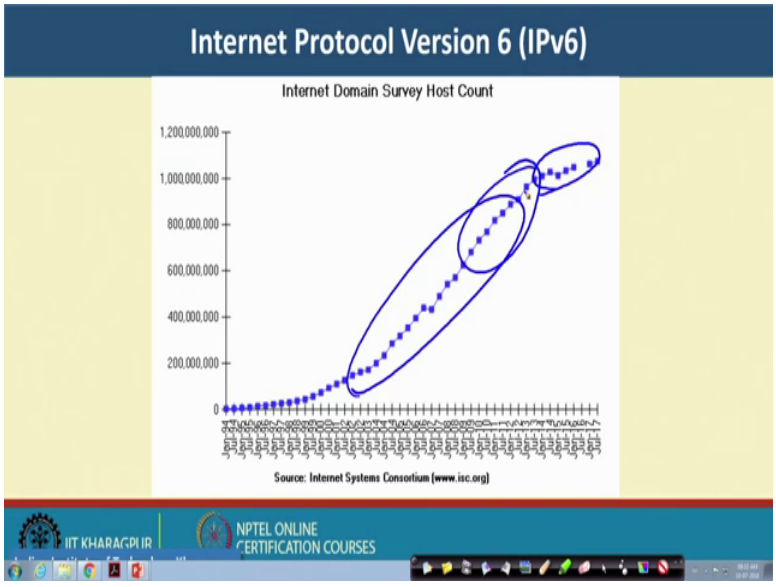
Computer Networks and Internet Protocol
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 30
IPv6 Addressing

Welcome back to the course on Computer Networks and Internet Protocols. So, in this course till now we have looked into, the details of the internet layer or the network layer and we have looked into the addressing scheme, which is used in the network and we looked into the details of IP version 4 addressing format; where the network uses a 32 bit IPv 4 address to individually identify each host.

Now, in this particular lecture today, we will move towards the most recent version of IP, the IP addressing scheme along with the IP protocol, which is called a IP version 6 or IPv6. So, we will first look into the short comings which are there for IPv 4. And then we will go to the design choices of IPv6 and the how IPv6 mitigates different problems, in which are associated with IPv 4 addressing. So, let us have a journey on IPv6 addressing.

(Refer Slide Time: 01:24)



So, first of all why do we require this new version of IP which is IPv6? So, if you look into the demand of internet addresses as there is with the grow of different devices in the internet; so, when the internet was first designed it was meant for military applications, as we have looked into the early days of internet history. And then people gradually

started using internet for normal, then general day to day usage. Now with this if you look into the grow of devices which we get connected to internet, then you will see that the number of devices are growing exponentially day by day

So, earlier we had the desktops which are getting connected to the internet. Now each person has 1 or even more than 1 devices; many of the cases it is more than 1 devices like you have your desktop you have your laptop, the mobile, phones, which you can get connected to the internet. And that way you require more number of IP addresses, because IP addresses associated with every network interface. And now a days we are moving towards the era of internet of things, where you have multiple small sensor devices mounted on single volt computers which are mounted on different places in a smart room or smart city or a smart hospital. And all of this tiny or the small devices they get connected to the internet.

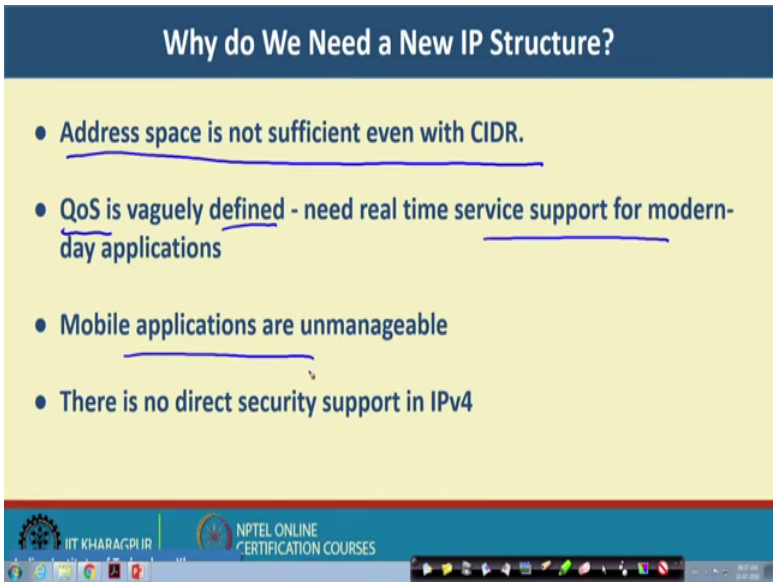
So, you connect a sensor to your fridge, to your ac, so, to your washing machine, even the doors, the lights, the smart lights, and then you can get data through those sensors and have a automated and smart operating of those devices. And all these devices are now getting connected over the internet. And whenever you will make a device to get connected over the internet, during that time device will obviously, require an address. Because our requirement is that we need to have unique IP address for all the devices which are getting connected in the internet. And that is why if you look into the trend of IP address requirement, in respect to years, so this graph is from January 94 to July 2017. Interestingly it is July 2017 is the time when IPv6 was standardized.

So, if you look into the growth of internet address which are there, you will see that there is a sharp increase in this growth. So, you have an exponential growth in the requirement of IP addresses. Now at this point, the things gets mostly saturated. So, whatever IP address we have, in the IPv4 address space with 32 bit addresses and as you know, we have we have discussed that these 32 bit IP address all though, theoretically it can support you 2 to the power 32 different IP addresses. But all this address are not useable for connecting a interface network interface with the internet. Because you have the reserved IP addresses, you have the special IP addresses, you have this broad cast IP addresses and the loop back IP addresses

Then you have this sub netting concept, where you need to allocate a set of IP addresses to the network address and then, individual host in the network. And because of all this reasons we are almost getting stagnant or we are almost getting saturated at the requirement of the IP addresses. So, the IP address space, which are available to us it is getting saturated. So, that is why you will see that, there is a drop in address usage in the recent years and this drop is not because the demand has become less but rather we do not have sufficient number of IP addresses in our hand. So, we are trying to manage with different ways like, using the network address translation NAT this kind of techniques that we discussed earlier.

So, what the take way message from this discussion is that, the IPv4 address that we have the total number of addresses are very limited and that is why, we need to have large pool of IP addresses, which can support global usage or global utilization with the help of a large number of addresses for a huge number of devices which are getting connected over the internet.

(Refer Slide Time: 06:15)



Now, let us look into brief the problems which are associated with the IPv4 addressing; so why do we need a new IP structure, so, first of all as we have mentioned that the address space is not sufficient even with CIDR. So, this is the primary reason, that we require a larger address space but that is not the only requirement for us.

So, apart from the address space, there are multiple other problems which are associated with IPv4 addressing scheme. And as you know or as we have discussed that this IPv4 addressing scheme, it was initially designed for the standard desktop computers which are fixed and which does not required of the mobility support. So, during the early days of internet people where was not able to imagine that 1 day your devices which will mobile like the mobile phones which will move from one place to another place and that will need to get connected over the internet. And traditionally this IPv4 addressing scheme it does not support mobility.

So, there are way to make mobility support in IPv4 with the help of mobile IP, that is the variant of IPv4 address or what you can say that it is like a patch on top of the IPv4 address. But overall, the by default this IPv4 addressing scheme that does not support mobility and at the same time during the early days of the internet people was not bothered about security authentication this kind of aspect too much. So, during that time connectivity was the prime requirement.

So, as I have discussed some time back that, you should always read the paper of the history of DARPA internet protocol by, David Clark which actually talks about, the different requirements which where there in the mind of the DARPA people, when the internet was first designed. And during that time connectivity was the utmost requirement and a prime requirement and security, logging, auditing all these things where the secondary requirements. And because of that we had this IPv4 address, where connectivity was the major issue.

So, you need to uniquely identify every individual devices in the internet but the other goals like the security, the auditing that became the secondary goal and that was added as a patch on top of the IPv4 address. And another thing was the quality of service. So, IPv4 the quality of service was vaguely defined. We will look into the details that, what is mean by quality of service later on in some lectures.

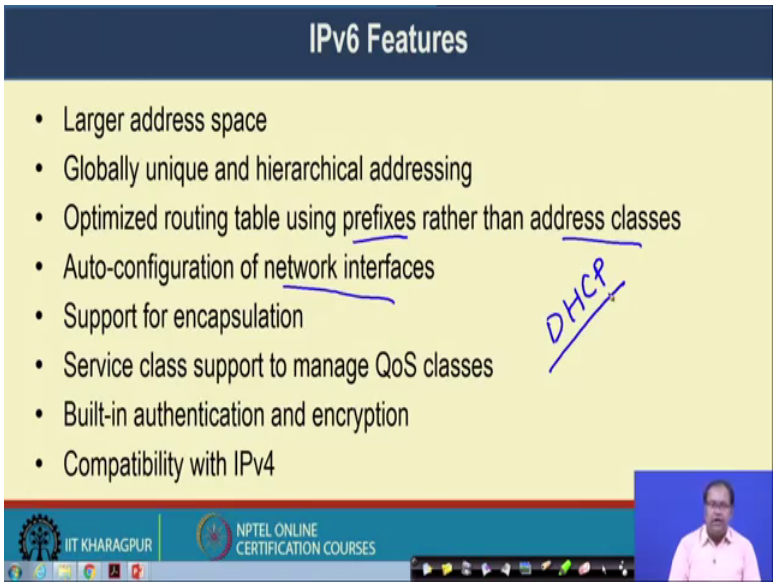
In brief quality of service is something like that, say initially when this IP addressing scheme was designed during that time people was only interested to transmit data traffic. But now days, we are transmitting multimedia traffic over the internet. So, we are transmitting voice data over voIP type of applications, we are doing video streaming.

So, interestingly the majority of the traffic in the internet now a days comes from the video traffic; from the video streaming kind of applications like YouTube, Netflix, this kind of applications. And whenever you are doing the video streaming, there are different kinds of video streaming, like this buffer video steaming, which is there in case of YouTube or hot star or that kind of application. And there is also kind of live video streaming like, what we do in case of Skype or live video chat. And all this type of multimedia applications, they require special services from the internet, because you need to transfer the data in a delay sensitive OS.

So, if your packet transfer takes too much of time, that will not sustain in the network. In IPv4 quality of service was not the prime goal and that is why the quality of service was vaguely defined in a IPv4. So, we need real time service support for modern day applications. And as I have mentioned that, mobile applications are in general unmanageable in IPv4 although, there are certain patch of mobile IP but that does not perform good in a real application and there is no direct security support in IPv4.

So, again that works like a patch on top of IP, using this transport layer security or secure socket layer kind of security module under transport layer and IP security kind of module on top of IPv4. Because there is no integrated support on IPv4 itself for this kind of application, QoS security mobility, the entire protocol became too complex and became unmanageable for a large internet.

(Refer Slide Time: 11:15)



Because of these reasons, we require a new IP structure and we gradually move towards this IPv6. Now, there is a interesting fact regarding IPv6. The draft version of IPv6 proposal it came sometime in December 1998. But then we took around 10 years to make the protocol standardized

So, the protocol became the IPv6 protocol became standardized just last year around July 2017. So, it took around 10 years to look into the different aspects of the protocol different internals of the protocol and to make it publish as a standardized protocol. So, the basic features of IPv6 are as follows: First of all it supports larger class of address space compared to 32 bit address in IPv4; we have 128 bit addresses space in IPv6.

Then, it uses a mechanism called globally unique and hierarchical addressing for efficient routing mechanism. In case of IPv4 we have seen that all though, we had the mind of having a hierarchical structure of the global internet, but ultimately we fail because of the unavailability of sufficient number address space and that is why we moved from the classful addressing which were there in initially. The classful addressing as you know that, it is a prefix based system. So, just by looking into the initial bits of IPv4 address, you can find out in which class it belongs to and accordingly you can find out the network address and the host address and then can do the route based on that.

But because this classful addressing was making wastage of address space and we require more number of address spaces, in the subsequent time. That is, why we gradually move from the classful addressing scheme to the classless addressing scheme and then, this classless inter domain routing or the CIDR kind of things.

With this, what happened that, this hierarchical architecture it was preserved locally, it was preserved within a network and in this subnet. But globally, this hierarchical architecture got broken. Also we have these private IP's and private lands in between by utilizing this NAT concept which actually violates or which actually moves little bit further from the global hierarchical structure. But with IPv6 address we try to build up a globally unique and hierarchical addressing scheme.

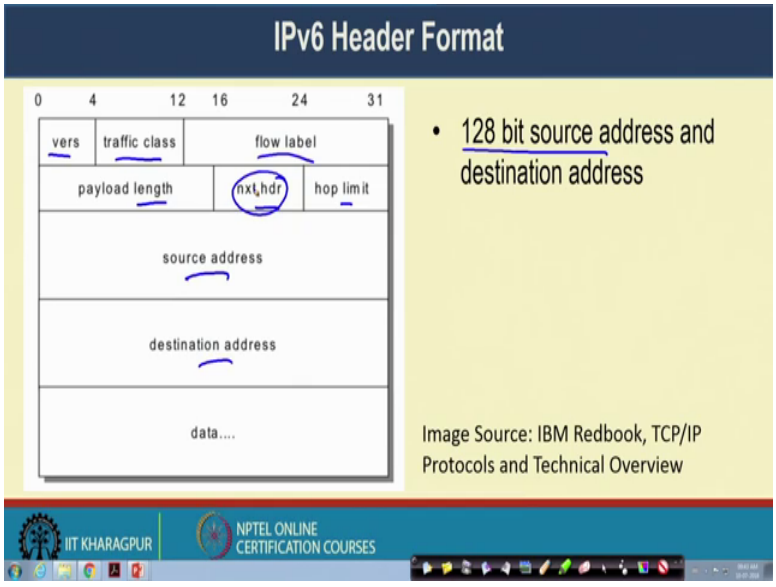
The third feature is the optimized routing table using prefixes rather than address classes. So, here you just look into the initial few bits of the address space and determine that in, which hierarchy, in which path of the hierarchy, the device belong to and accordingly

you route the packet in that path. That way you can optimize the routing table, rather than having this routing based on classful addressing.

Then the feature of auto configuration of network interfaces; that means, whenever you make a device life the network interface can automatically get an IPv6 address. So, whatever, we were you doing in IPv4 with the help of DHCP dynamic host configuration protocol; the same thing is implemented in IPv6 with the help of auto configuration. And that became a part of the IPv6, rather than having a different protocol like a DHCP which was there in IPv 6

Then the support for encapsulation; we will discuss this encapsulation in details. The service class support to manage quality of service classes. Then this built in authentication and encryption mechanism to support security and a backward compatibility with IPv4 so, that you can gradually migrate from IPv4 based system to IPv6 based systems.

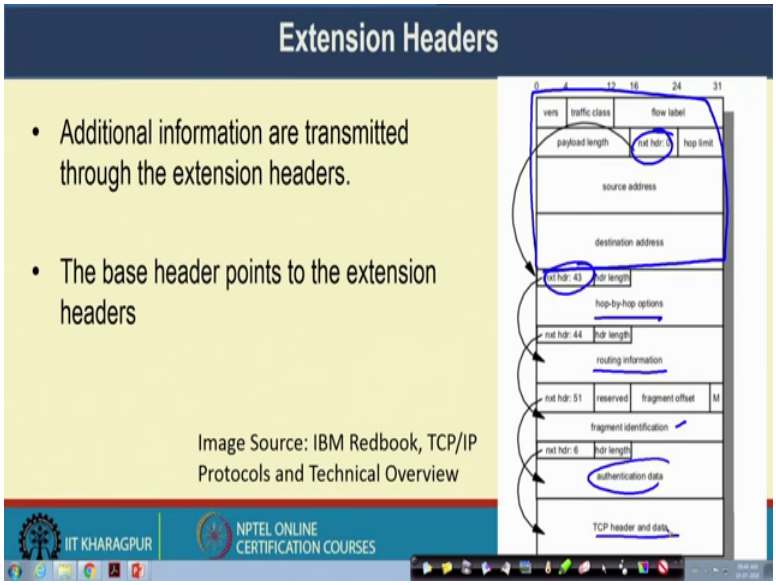
(Refer Slide Time: 15:19)



So, let us look into the header format of IPv6. So, in a case of IPv6, this is the header structure, in the header we use 128 bit source address and 128 bit destination address; the source and the destination address field. Along with that you have this traffic class field for supporting quality of service. This is the protocol version, then the flow level, leveling every flow based on its QoS classes, the payload length. The next header and the hop limit; so the next header is that in IPv6 you can have multiple optional headers, we

will come to that point. And the hop limits denote that, how many hop the packet should traverse because, before you discard the packet from the internet.

(Refer Slide Time: 16:17)



Now, this is the mandatory header structure of IPv6. Every IPv6 packet should have one mandatory header and along with one mandatory header, it can have multiple extension headers. So, these extension headers are used for special purposes. And with this mandatory header, so, in this diagram, this part is the mandatory header. In this mandatory header you have a pointer to the next header. So, this pointer actually points to the next header, in the total IP packet.

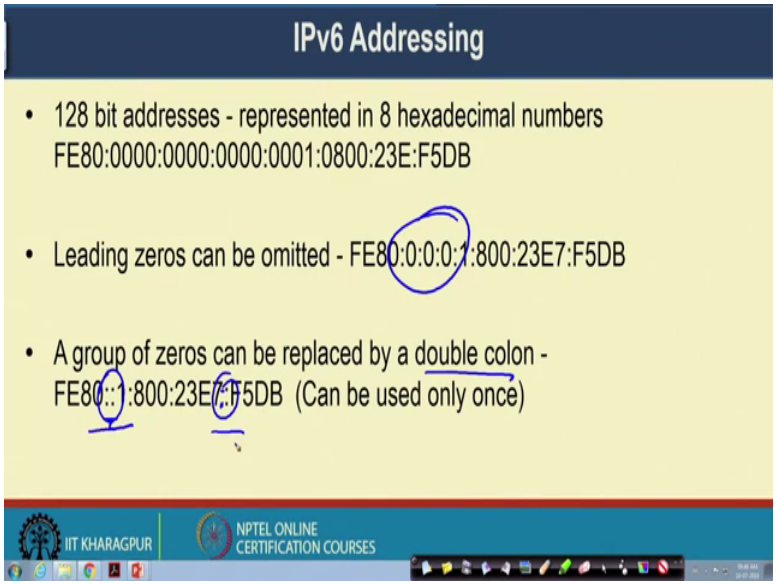
So, you have multiple, you can have multiple such extension header. One extension header can be you can put hop by hop option that whenever the packet traverse in each hop, how the packet will be treated there. Then, you can have a routing information embedded inside the inside the header itself. So, if you are applying something like source routing, where the source of the packet it will find out that in which the packet need to be traversed to reach at the destination, the source can put the entire routing information in the IP header packet. So, that is the routing information optional header.

Then the fragment identification; if your IPv6 packet gets fragmented into multiple pieces, then this fragment information can contain in the fragment header. Then your authentication data as I have mentioned that authentication or the security became a

inbuilt part of the IPv6. So, the authentication information can be put inside the optional header. And then you have this TCP header and the corresponding data

So, that way, you can have such multiple extension header along with the mandatory header which will give you additional information about this, how the packet will be treated by the IP protocol.

(Refer Slide Time: 18:09)

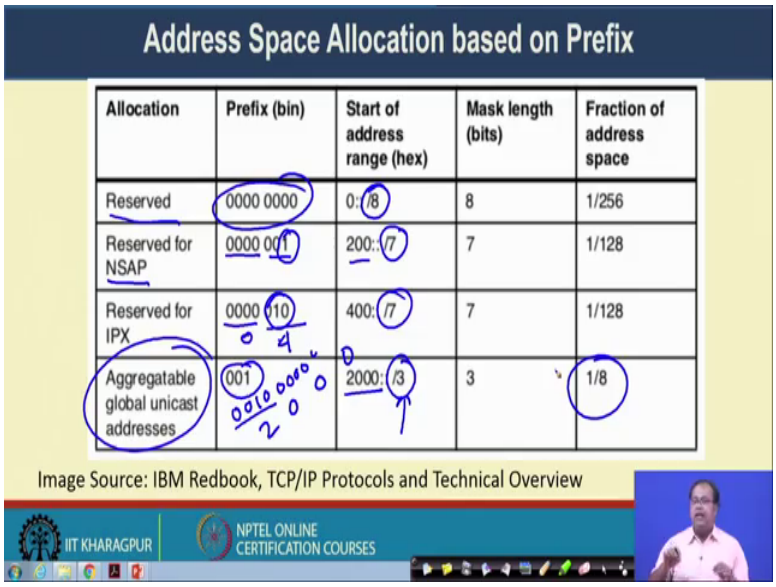


So, this is the format for the IPv6 addressing. So, as we have mentioned that, we use a 128 bit IP addresses it is represented in 8 hexadecimal numbers. So, every hexadecimal number is like FE80 then 0000. So, 16 bit binary that is, converted to the corresponding hexadecimal number and they are separated by a colon. So, that way, we represent this one 28 bit address in IPv6. Now this entire address we further reduce the total spaces, that is required to store an IPv6 address.

So, first of all if your hexadecimal number has all 0's, then you can replace it by a single 0. So, if, you have a single 0 that means, you have 4 consecutive 0, so all the bits in that part are 0's. Then if you have few consecutive 0's that consecutive 0's that can be replaced by a double colon. So, here these numbers of consecutive 0's are replaced by a double colon. But you need remember that, this double colon feature can be used only once, because if you have two different double colons; one say here and another double colon if I put here, then it will be difficult for you to find out that how many 0's are here and how many 0's are here.

So, that is why we cannot use it more than once, this double colons syntax we can use at most one. So, that you can find out that well here this it is, FE80 then it is 1. So, that means, it is 0001, then 8 0023E7 5FDB. So, you have 888 8 and 8 1 2 3 4 5 5 into 8, that many bits are there and remaining bits are 0, which will be placed here in the place of those two double colons. So, that way you can have a more optimized representation of the entire address in IPv6.

(Refer Slide Time: 20:19)



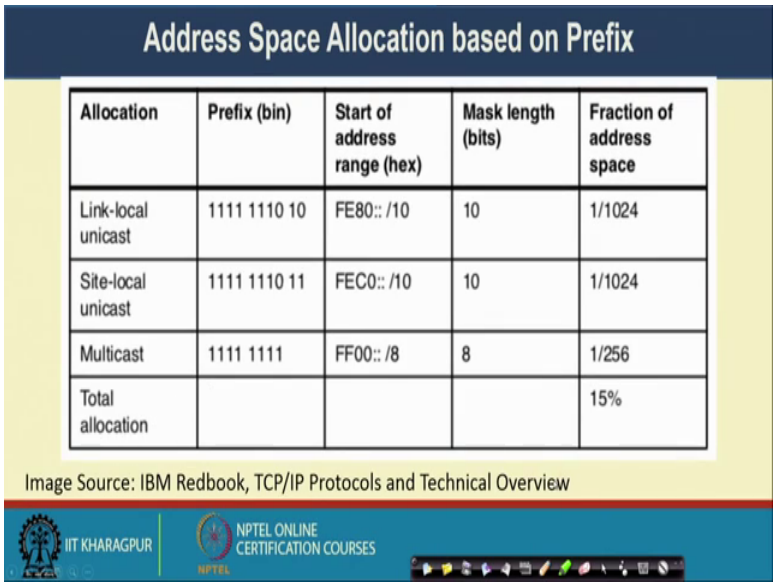
Now, this entre address space it is divided into multiple groups based on the prefix. So, this prefix actually determines that, how many addresses which fall into what group. So, if you look into the prefix values; that means, if the first 8 bits are 0's we can represent it as 0 then colon colon slash 8. So, this slash 8 represent the prefix and which was there in the CIDR concept as well, the concept of prefix that the first bits number of bits which will be used to identify the type of the address.

So, if this first 8 bits are 0's those this reserved class of address then, if this bit is a first 8 bit is 200; that means, 0000 followed by 0010. So, here your prefix is 7 bit first 7 bit. So, if you look into the first seven bit, if the last bit is 1, it is reserved for NSAP. If the bit is 10 in the address range, we can write it as 400; 400 because, this is 0 then, this becomes 4. If it is 400 then, this with this slash 7 prefix it is reserved for IPX protocol

Ah then, if the first 3 bits are 001; that means, this 001 means, the address is 0010 0000 then all 0's, that is the first hex part. So, the first hex part this becomes 2 and then all 4's

are 0's 2000 and your prefix is slash 3. If that is the case then, it is the aggregatable global unicast address, which is assigned to individual host in the network. And that is the 1 8th of the entire IPv6 address space that we have. So, that way we have a sufficient number of addresses that can be utilized for addressing every interface of a network

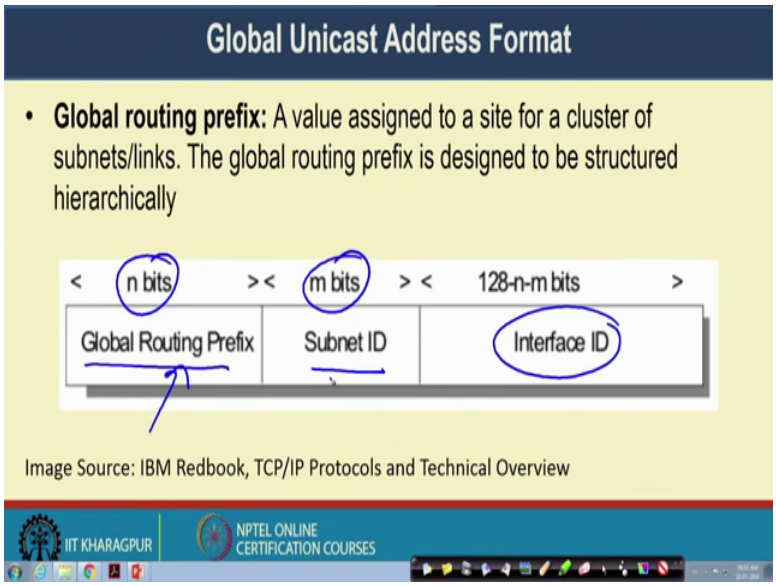
(Refer Slide Time: 22:37)



Then you have other classes like, the link local unicast, where the first few bits are 1111111010 with a 10 bit prefix. Then site local unicast again with a 10 bit if prefix the multicast address with the 8 bit prefix where all the first 8 bits are 1.

Ah. So, that way we have this multiple group of IP addresses, which are there in IPv6 and the interesting part is this global unicast address which are used in addressing every interface of individual devices.

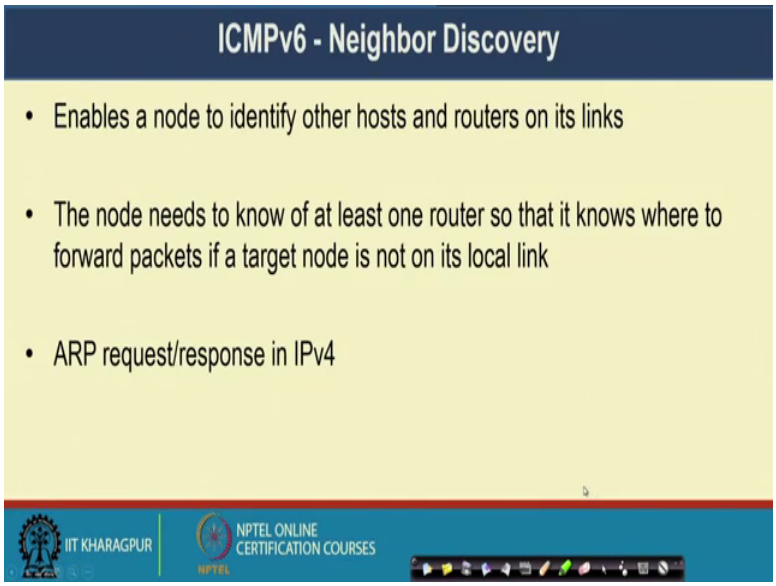
(Refer Slide Time: 23:18)



Now the global unicast address format in IPv6 this entire address is divided into 3 groups. You have a global routing prefix which is of n bits and then you have a subnet id of m bits and finally, 128 minus m minus m bits which are the corresponding interface id

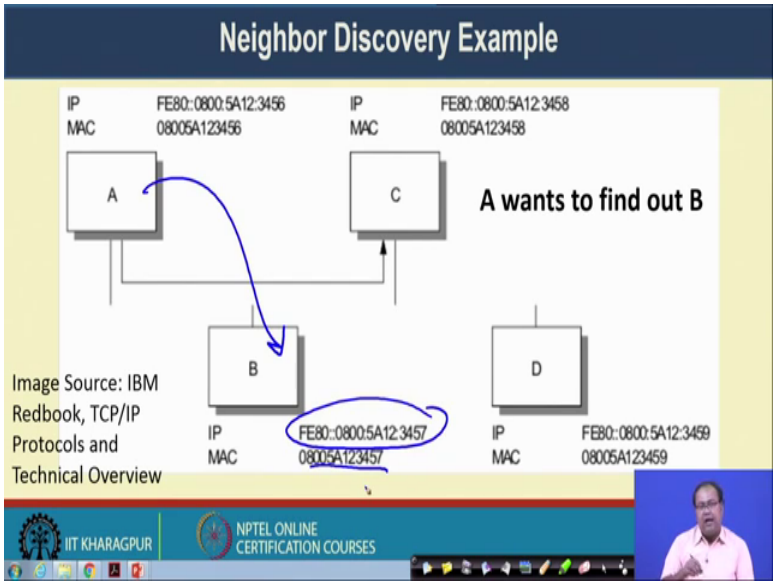
Now, this global routing prefix it is a value which is assigned to a site for a cluster of subnets of the links. The global routing prefix it is designed such that this entire network globally that can be structured hierarchically. So, the routing agencies they design these global routing prefix such that you can have this entire internet, you can structure the entire internet in a hierarchical way and then inside that individual level you can have the subnet ID, followed by the internet ID and your prefix the way we have noted it in CIDR, the same way the prefix is used to denote the globally routing prefix plus the subnet id.

(Refer Slide Time: 24:27)



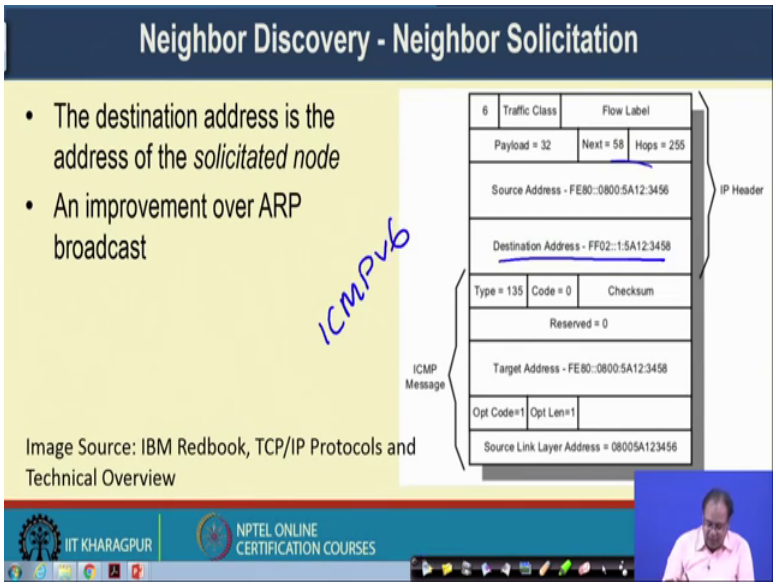
Well, now let us look into few features in IPv6; we look into a little detail. The first feature that we will discuss is neighbor discovery. So, neighbor discovery in IPv6 that was you can say it is a replacement of ARP in IPv4. So, it enables a node to identify the other host and routers on its links. The node they need to know of at least 1 router, so, that it knows, where to forward the packet. So, similar to the ARP protocol in IPv4, whenever you want to send to packet to another host you know its IPv6 address, but alongside you need to also know its MAC address. So, having a mapping from this IPv6 address to the MAC address that is, work done by this neighbor discovery protocol

(Refer Slide Time: 25:18)



Now, neighbor discovery protocol here is an example; like you say 4 devices A B C and D which have their IP address and the MAC address here, the IP address are the IPv6 addresses. Now say A wants to send some packet to B, now if he wants to send some packet to b a knows the say the IP address of B but A need to find out the MAC address of B. So, that it can find out that how to forward the packet to B. So, this is done with the help of this is the neighbor discovery protocol.

(Refer Slide Time: 25:54)



So, in case of neighbor discovery protocol what happens that, the node which wants to send the packets send a data here the node A in the preceding example, it sends a neighbor solicitation packet.

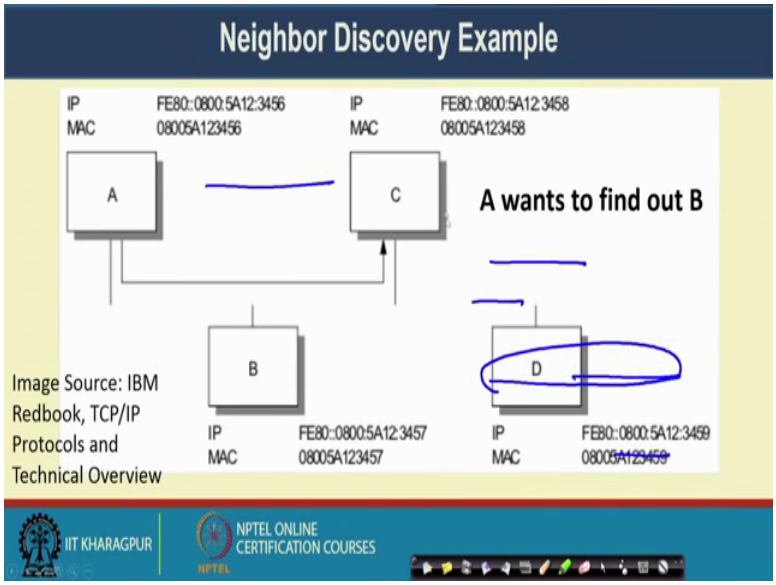
So, this neighbor solicitation packet, this is the structure of the neighbor solicitation packet, you have a source address field and the destination address field. This destination address field is an interesting feature that I will come in a couple of minutes So, this is your part of IP address IP address and this is the part of your ICMP message, that is the neighbor solicitation message in IPv6. So, the ICMP extension in IPv6 we call it as, ICMP version 6.

So, this is the ICMP message. So, in the ICMP message it is type 135; that means, it is a neighbor solicitation message. Then your target address is the given IPv6 address, so that means, this target address failed it tells you that you want to find out the MAC address

corresponds to this IPv6 address. And you have a source link layer address, so the MAC address of the source which is a part of the ICMP message

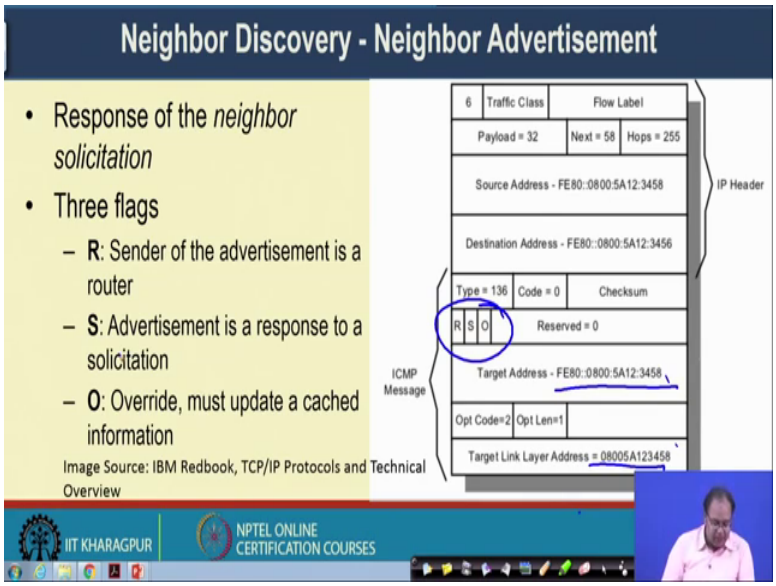
Here the interesting part is that, this destination address. So, this destination address is the address of the solicitated node. So, if you look into the ARP in IPv4, in case of ARP of IPv4, we actually broad cast the IPv4 ARP query. So, the query ARP query is broadcasted and the nodes which receive that, if they have the information they reply back otherwise, they further broadcast it. But in case of IPv6, we do not broad cast this query, rather we send to a targeted node. So, every node has associated with one solicitated node, the information of the solitcitated node is already available to the source node. So, it will send the query to only this solicitated node.

(Refer Slide Time: 27:56)



So, here in this preceding example, say node C is the solicited node of node A. So, node A will send the query to node C and then node C will find out the path to node B and then informing to node A ok.

(Refer Slide Time: 28:15)

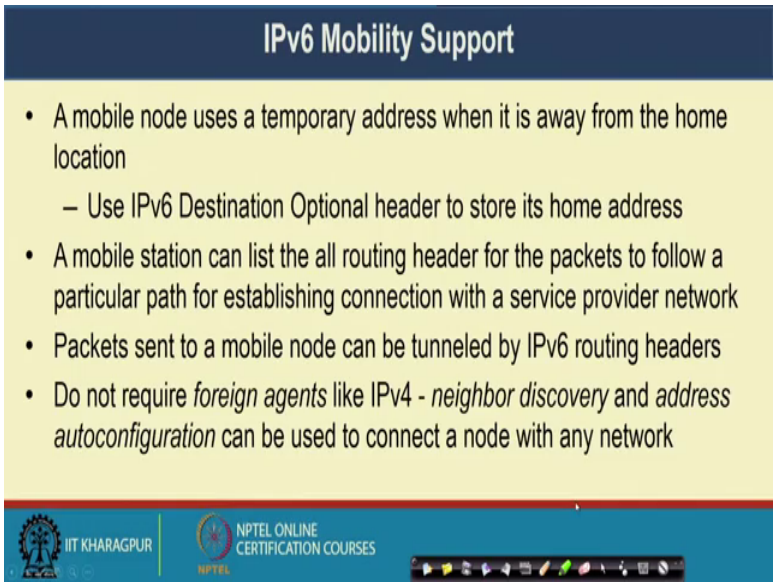


Now this response to the neighbor solicitation message is the neighbor advertisement message. In the neighbor advertisement message, you include the target address, the target IPv6 address and the corresponding target link layer address. So, this is the address for node B and you send the MAC address of node B the neighbor advertisement message.

Now, one feature is that, the it is not like that neighbor advertisement are only send as a response to neighbor solicitation. Whenever you are sending a neighbor solicitation during that time you will get a advertisement. But apart from that every node periodically send this neighbor advertisement message, so that they can formed a one half link connectivity.

Now, here because of this you can see there are 3 flags. So, this flags are the R flag means, the sender of the advertisement is a router, the S flags means, the advertisement is a response to a solicitation and O means override; that means, the source of the solicitation it must update the cash, with this new information.

(Refer Slide Time: 29:20)



Ok, now coming to the mobility support in IPv6, so in case of IPv6 mobile node, it uses a temporary address, when it is away from the home location. So, it use this IPv6 destination optional headers, to store the home address home address means, where it was initially connected. Now the mobile station it can least all the routing header, for the packets to follow a particular path for establishing a connection with a service provider network

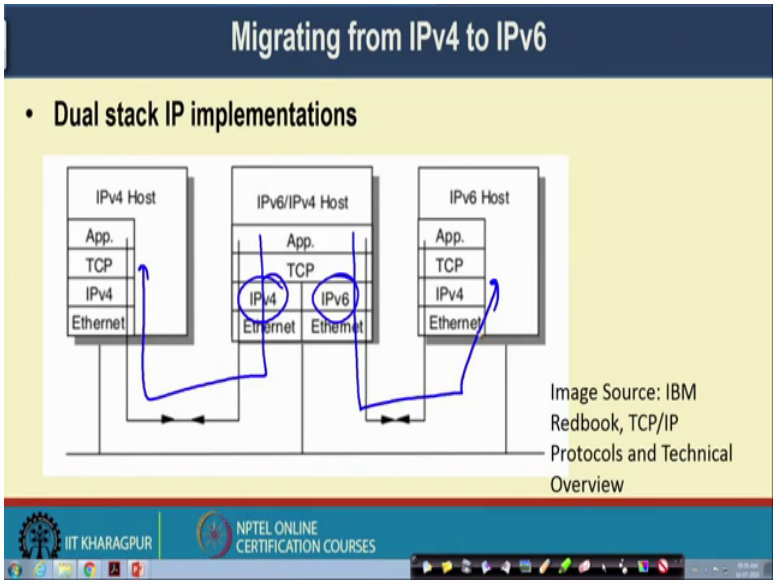
So, as you have seen that the advantage of IPv6 is that, you can add a additional number of optional headers to support this mobility. With this optional header you can add this additional information like whenever a node is moving from one location to another location, how the packet would be forwarded to this node, that can get embedded with this routing header information

Now, the packet sends to a mobile node, it can be tunneled by IPv6 routing headers and we do not require the foreign agents like IPv4. So, if you look into the IPv4 for mobility support, in IPv4 mobility support you have a foreign agent, that is a designated router and that designated router will actually make a mapping between the original address of the machine and the when the node has moved to a different subnet the new address corresponds to this mobility location. So, we do not require a foreign agent here in IPv6. We have the neighbor discovery protocol and the address of a configuration mechanism that can be used to directly connect a node to any subnet. So, the node will get a new IP

address IPv6 address with the help of this neighbor discovery and interface or address auto configuration

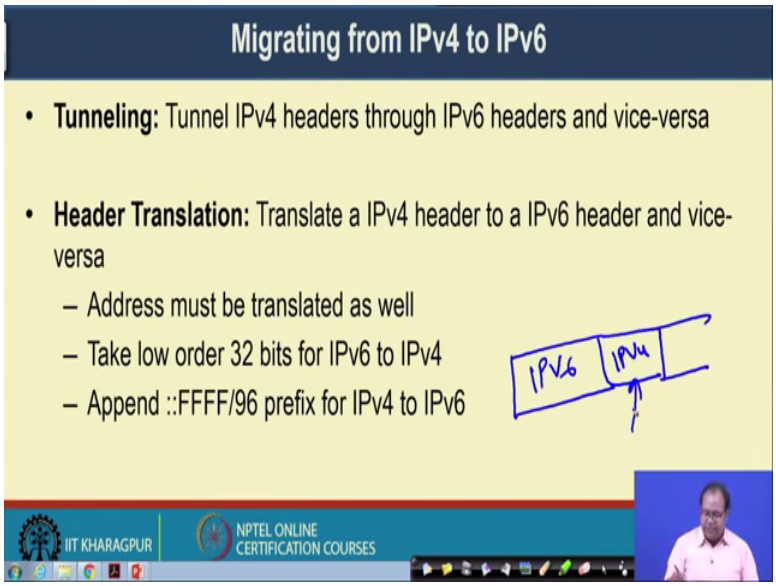
Now the interesting fact is that, you cannot migrate from IPv4 to IPv6 in 1 day because, currently all the machines are majority of the machines in the internet is support IPv4. And IPv6 as a huge new set of features now if, you want to migrate from IPv4 to IPv6 how will you do that? There are broadly three ways of doing that one is the dual stack support in case of a dual stack support. You have a support for both IPv 4 and IPv6 in the same protocol stack.

(Refer Slide Time: 31:35)



So, if you are communicating with the IPv4 machine, then you use the IPv4 stack, this part of the stack to communicate with the IPv4 machine. If you are communicating with the IPv6 host they would then, you use this IPv6 stack to communicate with the IPv6 host; so, that means, the single machine should have both the IPv4 stack as well as the IPv6 stack. The second mechanism is tunneling.

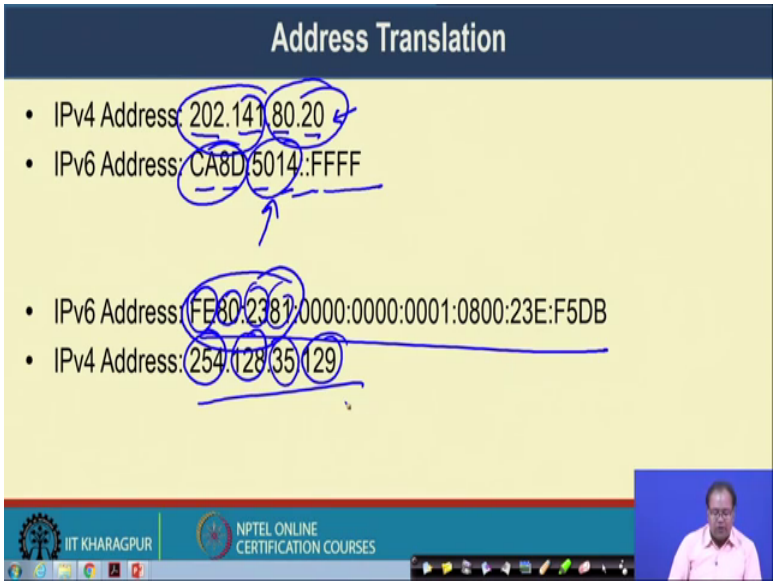
(Refer Slide Time: 32:08)



The tunneling mechanism says that you tunnel the IP 4v 4 headers through IPv6 headers. That means, the tunneling mechanism says that, you have a IPv4 header. So, whenever you want to send it to IPv6 a host, you add up an IPv6 header along with the IPv4 header.

Now, if you are sending it to IPv4 host these part of the header will be red, if you are sending it to the IPv6 header this part of the header will be red out. Then the concept of header translation, it says that you translate a IPv4 header to IPv6 header. That means, you have a IPv4 header and you create a corresponding IPv6 header, by converting the values in the IPv6 format and then add it with the original packet

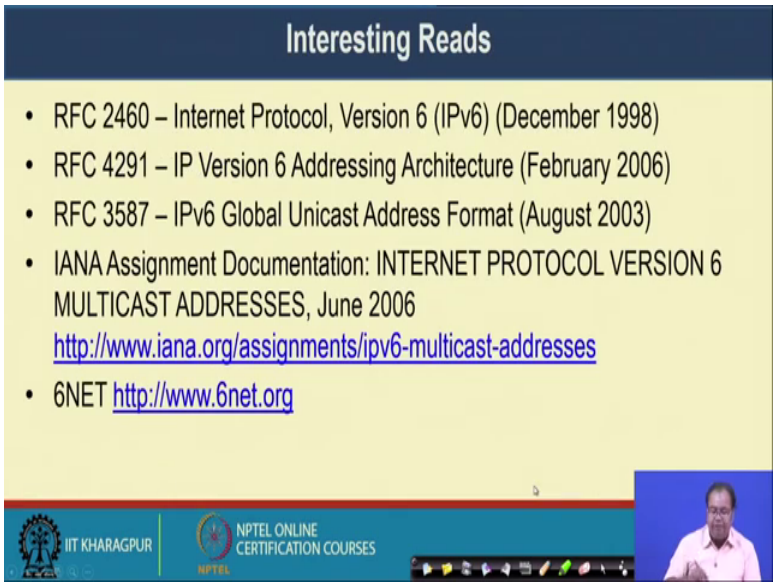
Now, whenever you are doing a header translation, for an important requirement is that your address must be translated. That means you should be able to translate the IPv6 address to IPv4 address and the vice versa. So, to make this conversion if you want to make a conversion from IPv6 to IPv4 then, you take the low order 32 bit address to make the corresponding IPv4 address. If you want to convert from IPv4 to IPv6 you have 32 bits, you require additional 96 bits, you put all this 96 bits as initial 0's and then all 1's for the last hex part. (Refer Slide Time: 33:35)



So, an example is here. Say this is your IPv4 address. If this is the IPv4 address, this is your corresponding IPv6 address. So 202 corresponds to CA 141 corresponds to 8D, 80 corresponds to 50 20 corresponds to 14. So, note that this is in the decimal notation and this is in the hexadecimal notation.

So, we take this 16 bits and convert it to a hex format. Then we take this 16 bit and convert it to a hex and then all 0's followed by last ones. And if you have a IPv6 address like this to convert it to a corresponding IPv4 address, you take the lower order 32 bits that means this part of the IPv 6 address and convert it to the corresponding IPv4. So, FE means 254, 80 means in hex means 128 23 in hex means 35, 81 in hex means 129. So, your address is 254.12.35. So, that is all about IPv6 that we wanted to discuss here, but I have not discussed all the details.

(Refer Slide Time: 34:34)



So, the IPv6 details are much more than what I have covered, I have just tried to give you a basic introduction about IPv6. So, to know more about this IPv6 here are some pointers that you can follow, the RFC's. So, this RFC's are these RFC 2460, RFC 4291 and RFC 3587. This discuss about a various aspects of the IPv6 in details. And then I have pointed two different links, one is the IANA documentation; that talks about the IPv6 addresses, multicast addresses and another is the 6NET website. The 6NET is a project that worked on the design and development of IPv6.

So, you can visit the 6NET website to look into their white papers the documentations which are there to know more about different features in IPv6. So, that is all about IPv6 and I will say that it is a very brief introduction about IPv6 there are much more details. So, please explore the pointers which are given at the end of this slide to know more about IPv6 addressing format.

Thank you for attending this class.