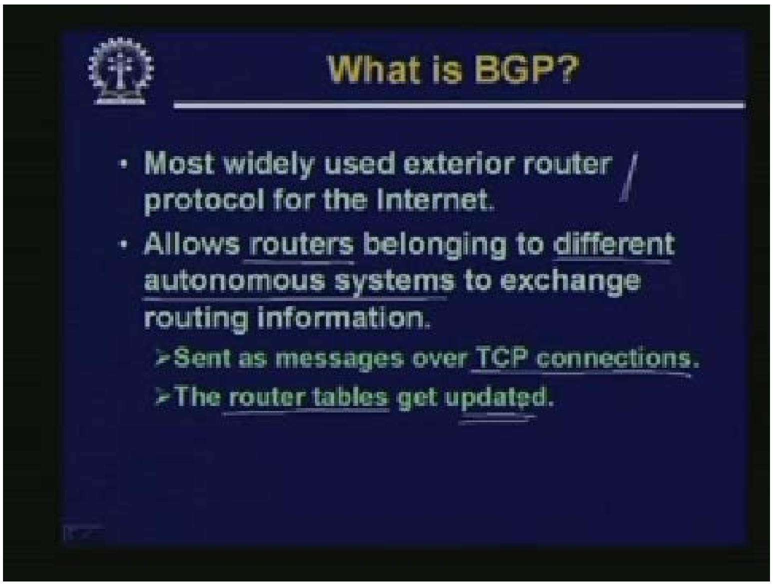
Internet Technology
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture No # 08

Internet Routing Protocols Part-II

In today's lecture we would be continuing with our discussion on internet routing protocols. Just to remind what we have discussing in our last class. We talked about autonomous systems which in a sense comprised of a collection of networks and routers which were essentially a part of a single organization. Now there can be a number of such autonomous systems all around the world. The basic concept behind this routing protocol is that there should be a class of protocols which could be operating within such autonomous system. Their primary purpose would be to have the routers update their routing table with whatever information they have with them. There are some protocols a couple of which we had discussed in our earlier class like the RIP and the OSPF which are used by the routers, which are inside the single autonomous system to update their routing tables. Now there if you recall there some kind of broadcast message was used where a router could send some information about some change to the network to all the other routers in the autonomous system.

This was possible because number one the en exact topology of the autonomous system was known to each of the routers because it is under the control of a single organization. And number two, the variation or the changes you can say the changes that can take us to the network are not that frequent. Today you would be talking about one of the most important so called exterior routing protocols where routers which are sitting in two or more different autonomous systems, they can exchange routing messages. Now different autonomous systems may actually mean communicating over a wide area network. So here a lot of you can say variations in the network topology congestion link status over a period of time are quite possible. So here the protocols which are used in the interior routing updates cannot not be used exactly so there has to be some modifications. So our topic of discussion today to start is the Border Gateway Protocol which is one such exterior routing protocol.

(Refer Slide Time: 03:22)

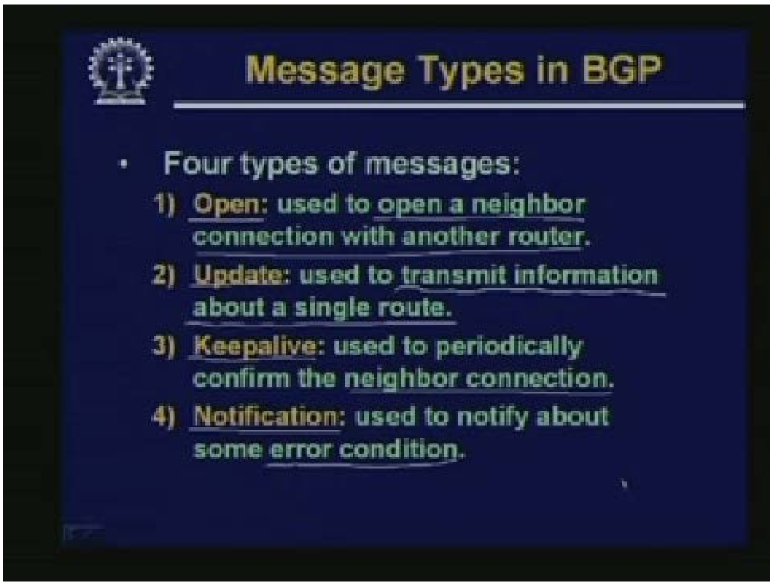


What is BGP?

- Most widely used exterior router protocol for the Internet.
- Allows routers belonging to different autonomous systems to exchange routing information.
  - ➢Sent as messages over TCP connections.
  - ➢The router tables get updated.

Now let us see what BGP actually is? The first thing I just mention that BGP is perhaps the only exterior routing protocols that is used extensively. Almost everywhere where it is used and the main purpose of BGP is to allow the routers which belong to different autonomous systems to exchange routing information among them so that their routing tables are kept updated in response to some changes in the network topology. Now these routing update messages are sent over TCP connections in the network. As a result as I had mentioned that the router tables get updated.

(Refer Slide Time: 04:18)



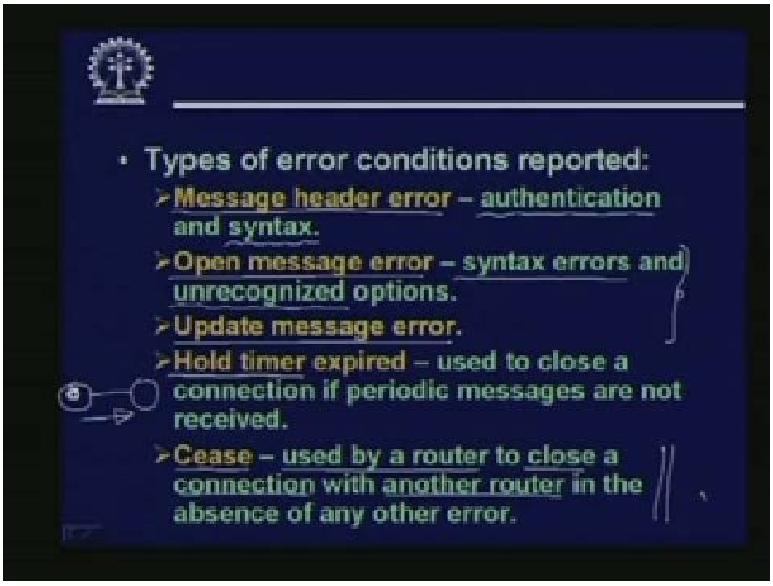
Message Types in BGP

- Four types of messages:
  1) Open: used to open a neighbor connection with another router.
  2) Update: used to transmit information about a single route.
  3) Keepalive: used to periodically confirm the neighbor connection.
  4) Notification: used to notify about some error condition.

Now let us see what are the kinds of packets and the other functionalities that BGP supports or provides. Broadly speaking there are four different types of messages that we have in BGP. First is the so called Open message. Now Open means two routers belonging to different autonomous systems. They agree upon the fact that they want to be neighbours. Suppose I am a router I want to be a neighbour of some other router belonging to some other autonomous system. This can be done by sending an Open message. So this Open message is used to open a neighbour connection with another router. This is the essential idea. Similarly, when information about some changes are to be communicated, it is this Update message type which is used. Update is used to transmit information about a single route which has undergone some change. This actually means that say I am a router, I suddenly find that I earlier knew of a route to some destination router say x. But I now have a better route or maybe a worse route also some of the link in my earlier route may have failed. So I have a modified route up to x. So I convey this information with to my neighbour or the neighbours wherever are they.

So I am not sending a broadcast message to everybody, I am only sending this to my neighbour routers. This is done by using the Update message. And in order to keep a connection intact or alive there is a Keepalive message type which is used to periodically confirm the neighbour connection. Which means that if two routers are neighbours they must send this Keepalive message periodically to each other. So they know that well the other side is active and is listening to whatever I am saying so this Keepalive message keeps the connection up and active. And finally to take care of the error conditions, there is a so called notifier or Notification message which can tell the neighbours about some error condition. Now this error condition maybe in the condition of the link it can be in connection with the status of a packet which is received. For example I have received a packet from my neighbour where I find that there are some errors, there can be checksum error or some header field is invalid. So in response to that I can send back a Notification message to the other side.

(Refer Slide Time: 07:25)



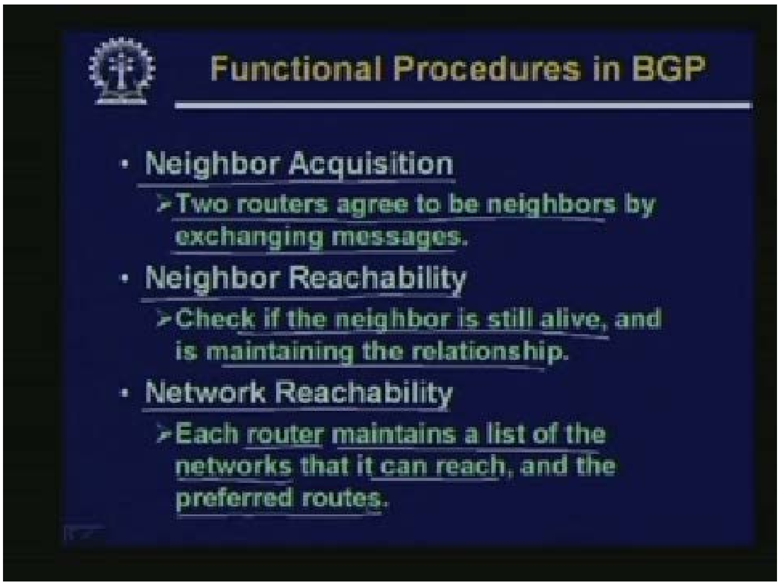
- Types of error conditions reported:
  - ➢ Message header error – authentication and syntax.
  - ➢ Open message error – syntax errors and unrecognized options.
  - ➢ Update message error.
  - ➢ Hold timer expired – used to close a connection if periodic messages are not received.
  - ➢ Cease – used by a router to close a connection with another router in the absence of any other error.

And through the Notification message the types of error conditions that can be reported are firstly there can be some errors in the message header. This can be with respect to authentication or with respect to its syntax. See authentication means in cases where you need some privacy, possibly some of some of the header fields will go encrypted. The receiver somehow finds that it is unable to decrypt it. So there must be something wrong; so either in the way it was encrypted or some changes had taken place while the message was being delivered and syntax maybe some general error in behaviour that can again happen due to some error in transmission. So message header error will take care of these two things. Similarly open message error, Update message error, these are some errors which take place in connection with the Open and Update messages.

These can be broadly classified into either syntax errors or some options which are invalid unrecognized options. These again should not occur under normal situations. If there is some error somewhere in transit something gets changed, then only this kind of errors will occur and will get detected. And in terms of the neighbour connections, there is the concept of a Hold timer. Suppose there are two neighbours. Suppose this is one neighbour and this is one neighbour. They have a connection between them. Now the idea of Hold timer is that say this fellow will be maintaining a timer. So whenever this neighbourhood connection is established this timer is set. So the timer actually counts how much time has elapsed since I have last received a Keepalive message from the other side. So if I do not receive a frequently enough Keepalive message from the other side, I can declare that somehow my connection is not active right.

Now so my neighbourhood connection will cease to exist. This is the Hold timer expired error condition. Finally Cease which is an explicit command which can be used to terminate a connection this command can be used by a router. To explicitly ask for closing a connection with another router which is its neighbour. So these, Cease kind of an event also will be going to the other side as a Notification message. So these are the kind of exception or error conditions which can be conveyed through a Notification message. Now talking about the broad functional procedures that BGP supports or handles there are three broad functional procedures.

(Refer Slide Time: 10:55)



Functional Procedures in BGP

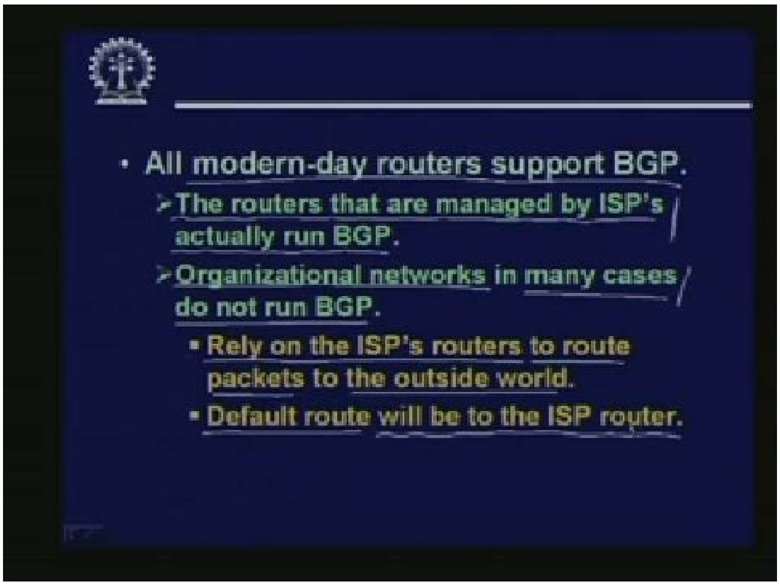
- Neighbor Acquisition
  - Two routers agree to be neighbors by exchanging messages.
- Neighbor Reachability
  - Check if the neighbor is still alive, and is maintaining the relationship.
- Network Reachability
  - Each router maintains a list of the networks that it can reach, and the preferred routes.

First is called Neighbour Acquisition, this I have just mentioned. That using the Keepalive message type two routers can agree to be neighbours and this is done by periodic exchange of

Keepalive messages. So they start being a neighbour by sending the Open message. But subsequently they have to keep sending the Keepalive message to each other periodically so that the connection remains established. Secondly once the neighbour is acquired you must check that the neighbour is reachable or not. Neighbour Reachability to check if the neighbour is still alive and maintaining the relationship. This again is ensured through those Keepalive messages and thirdly Network Reachability.

See in BGP, each router if you look at the routing tables of the routers they essentially will maintain information about a list of other networks. Suppose I have a packet which is destined to a network N1. So the routing table will tell that which outgoing link to follow in order to reach N1, this kind of information has to be there in all the routers. So Network Reachability will tell you whether you can reach. The other networks whose information are there in the routing table sometimes due to some error, due to some update messages, you can find that a particular network cannot be reached. So in if that kind of a scenario occurs you can simply drop that entry from the routing table. So Network Reachability ensures that all the networks in that listed in the table, it can be reached and which are the preferred next hops preferred routes.

(Refer Slide Time: 12:58)



- All modern-day routers support BGP.
  - The routers that are managed by ISP's actually run BGP.
  - Organizational networks in many cases do not run BGP.
    - Rely on the ISP's routers to route packets to the outside world.
    - Default route will be to the ISP router.

Now the point to note is that all modern day routers it can score or any other make they will support BGP. Because BGP has emerged as the defacto exterior, router update standard. So this is the fact that we see all round us. But one thing you should also remember that not everybody runs BGP. Typically the routers that are managed by the internet service providers or the ISP’s, they actually run BGP. For example, I may be referring to me as an individual or I may be referring to myself as an organization. Suppose I have obtained a network connection internet connection from an ISP like BSNL. So I get a connection from BSNL. So actually what does that connection mean? It can be dial up connection; it can be lease line connection. Whatever maybe the connection to my site, ultimately my connection will get terminated into some router port in the ISP side and that particular ISP must be running BGP.

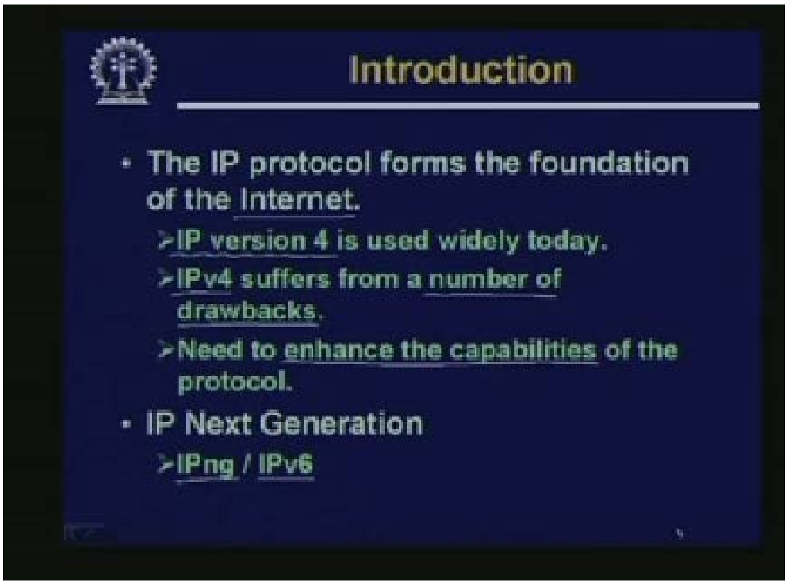
So that it can kept itself I mean it can keep its table updated with respect to changes that are happening to the outside world. Because if the router through which all my packets are going out is not updated regularly. There can be a problem, that means I may not be able route my packet in a proper way. So the ISP routers must always be running BGP. But however the organization networks there can be routers inside an organization also they in many cases do not run BGP. This is of course a choice it is not mandatory for them to run BGP. In that case what they do? They would rather rely on the ISP's routers to route the packets with the outside world. It means suppose I have an organization inside my organization. There can two or three routers but none of them is running BGP. Rather all our packets which are destined to an outside network will be sent to our ISP router and it will be the responsibility of the ISP router to route to properly.

So it is not that a router inside our organization will be running BGP and it will take a decision that where to send it from our organization. See this kind of a solution is very typical where an organization has a single or very few maybe two connections to the outside ISP's. So the internal router really do not have much option they will have to forward it to the ISP in anyway. And since the ISP router is running BGP in anyway, so you may not run BGP inside. This is the basic reason. So under this condition the default route of the router which is inside will be set to the ISP router. So if the destination does not match with an internal address, it will be directly sent to the router which is outside. Now let us shift our attention to a slightly different topic. Now if you recall when we had talked about TCP/IP earlier, we had basically talked about the IP version 4. We said that it is the most commonly used protocol that is being used in the network layer protocol in the internet.

IP version 4 is basically a datagram based service which takes responsibility or routing the datagrams from one source to a given destination. So each of the IP layers in the intermediate nodes take decision typically with respect to the IP address of the destination that means we have to forward the packet too. Now we had seen that this IP version 4 basically the way we address the host it is a 32 bit addressing scheme and the classical IP addressing scheme they assume that you break up the total 32 address space into 2 parts. One part will indicate the address of the network and the other part will indicate the address of the host of the computer within the network. Now there are three classes as you know class A, class B, class C, depending on the sizes of the networks you choose to use. There are other class less options also. You can go for variable length subnet mask you can go for class less internet domain routing.

So these are options available to you well which do not deviate from the IPv4 addressing scheme. But rather try to provide us you can provide a mechanism for more efficient utilization of the address space of the available address space. Now it was long felt that IP version 4 has already long lived its life. Now time is right to go for a change or some modification to a next higher version of the protocol. This IP version 6 which is the latest version of IP which has become means available as a standard since a long time. So lets us first look at this IP version 6. What it is all about 10? We shall be talking about the present status where we are IPv6.

(Refer Slide Time: 19:35)

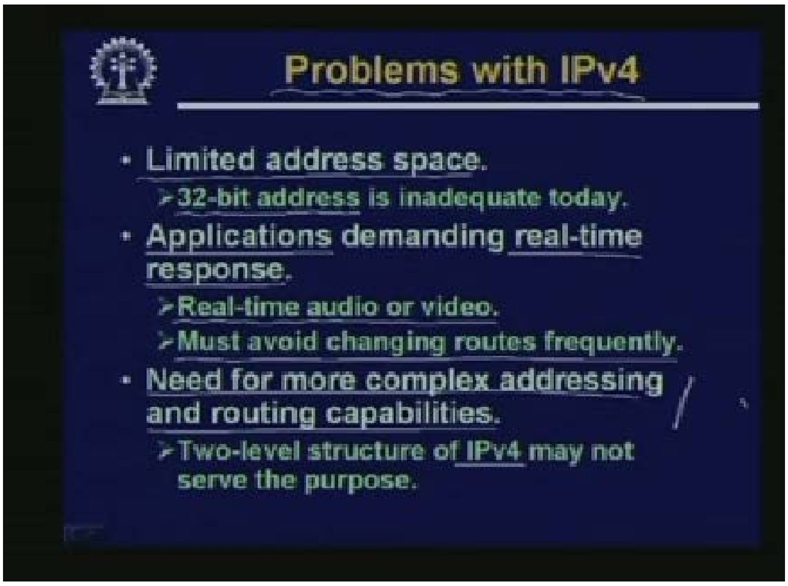


Introduction

- The IP protocol forms the foundation of the Internet.
  - IP version 4 is used widely today.
  - IPv4 suffers from a number of drawbacks.
  - Need to enhance the capabilities of the protocol.
- IP Next Generation
  - IPng / IPv6

Now I just mentioned that this IP protocol which we use in the internet so widely today. So the protocol which you mostly use is classical the IP version 4. We shall see shortly that IP version 4 at its existing, they suffer from a number of drawbacks. Therefore there is a need to enhance the capabilities of the protocol so as to overcome this drawback. So this IP, next generation which is sometimes also called IPng or in short IPng or IPv6. This is what has been proposed to address this issue. The issue that this IP version 4 is not capable of handling future needs. There are some disadvantages which we face with IPv4. How to overcome that? So let us see how these are done.

(Refer Slide Time: 20:42)



Problems with IPv4

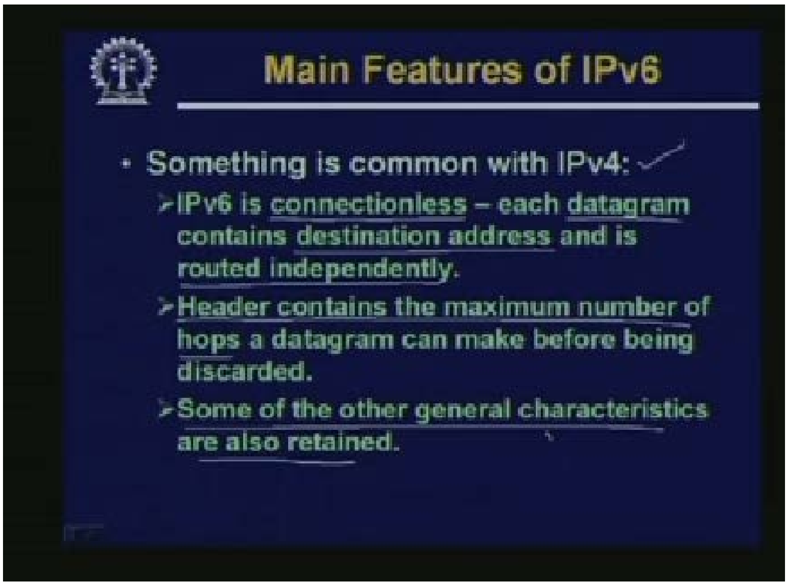
- Limited address space.
  - 32-bit address is inadequate today.
- Applications demanding real-time response.
  - Real-time audio or video.
  - Must avoid changing routes frequently.
- Need for more complex addressing and routing capabilities.
  - Two-level structure of IPv4 may not serve the purpose.

First let us very quickly look at some of the problems that IPv4 faces. Most important problem that IPv4 faces is the limited address space. We have only 32 bits available to us for addressing a node and as we see today, as we see, the state of the internet today we see that there are already close to billion computers that are connected and 32 bit addressing is grossly inadequate. We have formulated or framed a number of different ways to efficiently try to utilize the available address space. But still the time is very near, we will be absolutely tied up, we will not be able to expand the networks further because of our paucity or scarcity in the available address spaces. We use protocols like DHCP and other protocols to again efficiently utilize the available number of addresses that we have. But still these are all stop gap arrangements we have to have some solution.

This is of course one drawback. There is another big drawback there are many applications which depend real time response. Now you see that nowadays there are number of applications like video on demand online audio. That means you have IP telephoning there are these kinds of applications which demand real time response. But in the classical IP version 4 as I had mentioned that IPv4 is based on the datagram technology. A packet is sent independently it can follow any available path. Suppose I want to send speech signal as a sequence of packets, there is no guarantee that my speech signals will be arriving at a destination. Means uniformly spaced in time there can be unequal gaps between the different parts go my voice speech. Some packets may get lost in transit some packets may be reached out of order. So we can so here in terms of a response you may here some gaps in between speeches sometimes.

So IP version 4 does not do much to cater to these kinds of applications. They say that if it is real time application, if you do not find packets, simply reject it. It is perhaps the best solution. So it is better to have a small gap rather than hearing this voice once again later after something of the future has been spoken out. So that is not acceptable certainly, so real time response will demand that somehow you should avoid changing route frequently. Because if you change route frequently your real response cannot be guaranteed and again the third thing is that IP version 4 has a classical two-level addressing network and host. These simple two-level addressing may not be inadequate for modern day applications. As we shall see shortly there may be a need for having a more number of levels in addressing.

(Refer Slide Time: 24:22)

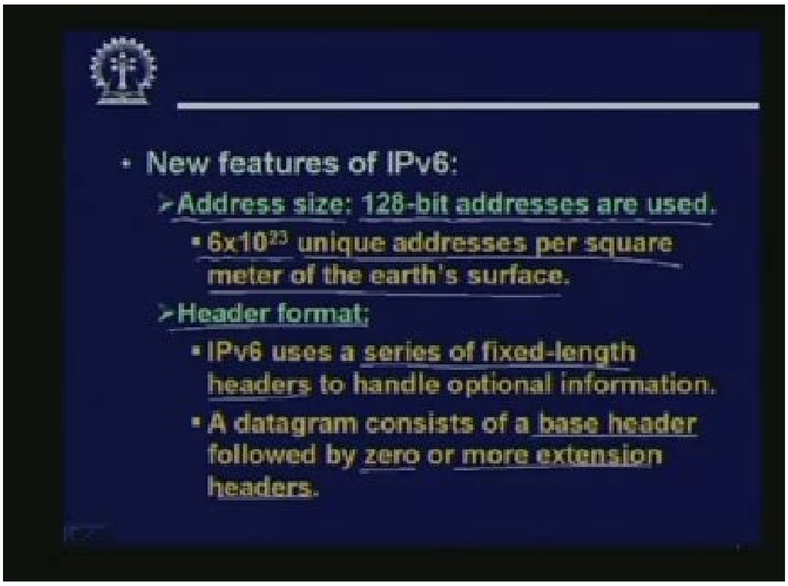


Main Features of IPv6

- Something is common with IPv4:
  - IPv6 is connectionless – each datagram contains destination address and is routed independently.
  - Header contains the maximum number of hops a datagram can make before being discarded.
  - Some of the other general characteristics are also retained.

Now, some of the main features of IPv6, of course something are there which are common to IP like it is also based on datagram technology it is a connectionless technology. Each packet or datagram will contain the destination address and will be routed independently. Secondly just like IPv4 the packet header will contain the maximum number of hops a datagram can meet. So at every hop the count will be decremented by one as soon as it reaches zero, the packet will be discarded. This is exactly what is done in IPv4. So here also something very similar is done. Some of the other general characteristics like fragmentation reassembly as the final destination. These are also kept the same as compared to IPv4.

(Refer Slide Time: 25:27)



- New features of IPv6:
  - Address size: 128-bit addresses are used.
    - $6x10^{23}$ unique addresses per square meter of the earth's surface.
  - Header format:
    - IPv6 uses a series of fixed-length headers to handle optional information.
    - A datagram consists of a base header followed by zero or more extension headers.

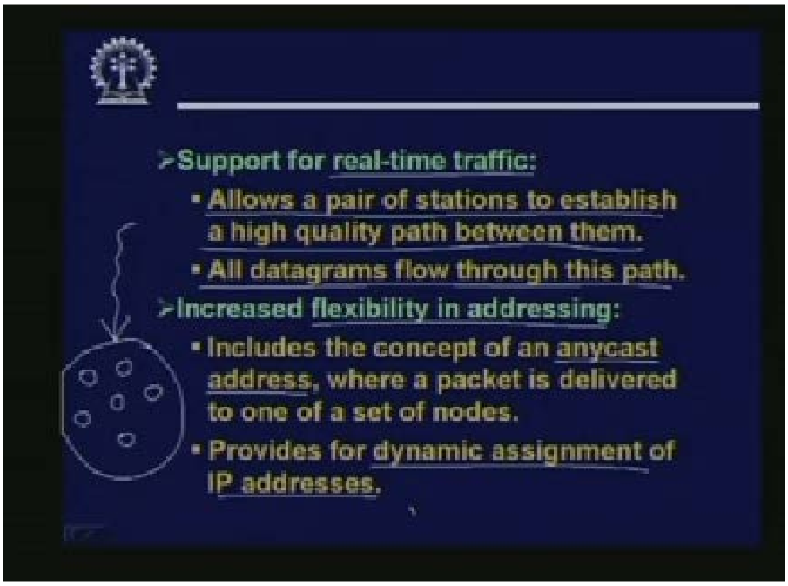
Talking of the new features, the most striking feature is the address size. Here from the 32 bit IPv4 address. We are moving on to a 128 bit address in IPv6. So how much or how big this

128 bit is address space. Let us try to have an idea, say 32 bits means 4 billion 2 to the power of 32. Approximately this we know but how much is 2 to the power 128 can we have a rough idea about that number that figure. Let us see if you compute 2 to the power 128 it come to close to 6 in to 10 to the power 23 addresses per square meter. This is not the total if you compute the whole circumference of the earth. If you take the whole circumference of the earth then with this 2 to the power of 128 different addresses in every square meter of the earth surface we can have 6 in to 10 to the power 23 addresses assigned.

So you can imagine how huge is this address space and what this number means is that, well approximately you can assign one address to one molecule on the earth surface. This is a staggering number, that means every molecule on the earth surface can be assigned an IP address 2 to the power of 128 means this much. So most likely in the foreseeable future if we start using this 128 bit addressing scheme. You shall not run out of addresses any more at least for the coming 10 or 20 years. Now there are some other changes also some new features of IPv6 because you recall in IPv4, we had a very well defined header. So all IPv4 packets use that same header. But in IPv6 the concept has become slightly different. IPv6 does not use a single header. But a series of headers, so all the headers are of fixed sizes. There is one header which is compulsory which is called the base header.

Following the base header you can have zero or more extension headers. Now extension headers are something which may or may not be present in a packet. Suppose if a packet needs to be fragmented then you need a fragmentation extend header. If you want to have some kind of encryption facility. So as to provide message secure your secrecy then you can have a security extension header. So these are the kind of extension header which is very specific to the needs that you have. But in addition to that we have one compulsory base header which will contain the basic information that you always require with a packet. So is the idea one base header followed by zero or more extension headers.

(Refer Slide Time: 29:11)



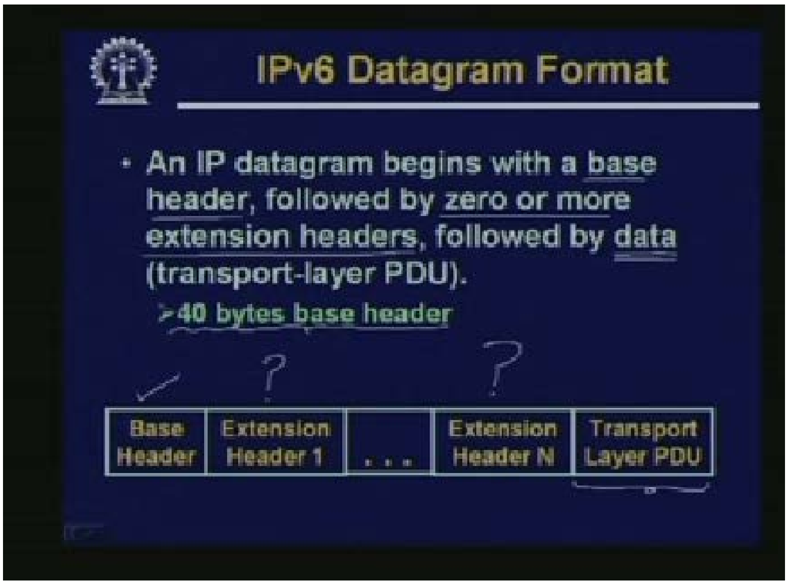
- Support for real-time traffic:
  - Allows a pair of stations to establish a high quality path between them.
  - All datagrams flow through this path.
- Increased flexibility in addressing:
  - Includes the concept of an anycast address, where a packet is delivered to one of a set of nodes.
  - Provides for dynamic assignment of IP addresses.

The third thing is that IPv6 supports real time traffic which means there is a facility to allow a pair of stations to establish a high quality path between them. For this purpose again you have a special purpose extension header. Suppose I want to establish a path with a destination between us, I want a 64kbps dedicated bandwidth. So I will try to establish a bandwidth where each of my intermediate nodes will give me a guarantee of this 64kbps bandwidth. So once this path is established I know that I have a guaranteed route where each of the nodes who are sitting in between they will guarantying me my required bandwidth this is called quality of service guarantee. This is guarantee and once such a path is established all datagrams will be forced to flow through is path. Because unless the datagrams flow through this path the guarantee of quality of service cannot be ensured.

And the last thing is that you have increased flexibility in addressing we will see it very soon. There are some new ways of addressing hosts which have been introduced which was not present in IP version 4. Like for example, a new concept called anycast address has been introduced. See anycast means suppose you have a number of computers, these computers can form a group. You can define an anycast address group with these set of computers. Suppose a packet arrives to this group with an anycast address, what this will mean is that this packet must be delivered to any one of the members of the group. This is unlike broadcast where the packet has to be sent to everybody. But here it is not that way here the packet needs to be delivered to exactly one member of that group. See these kinds of applications are very frequent nowadays.

We talk about internet search engines, we talk about the internet mail services and so on. But if you look a little carefully at these websites you will find that each of these websites will correspond to multiple IP addresses which means that there are so called mirror sites available. The name may be same the domain name, maybe same, but there are mirror sites. So when I want to contact such a site, so it would be very nice if I can have this any anycast addressing scheme. So that whatever I am going to send it will be reaching my nearest mirror. This is the idea and also you can have dynamic assignment of IP addresses very easily. This is of course a new feature which has been added. So here as and when you need an IP address can be assigned to you in a dynamic way. So these are some new features which IP version 6 has introduced. Now let us see the IPv6 datagram format how it looks like.

(Refer Slide Time: 32:54)



IPv6 Datagram Format

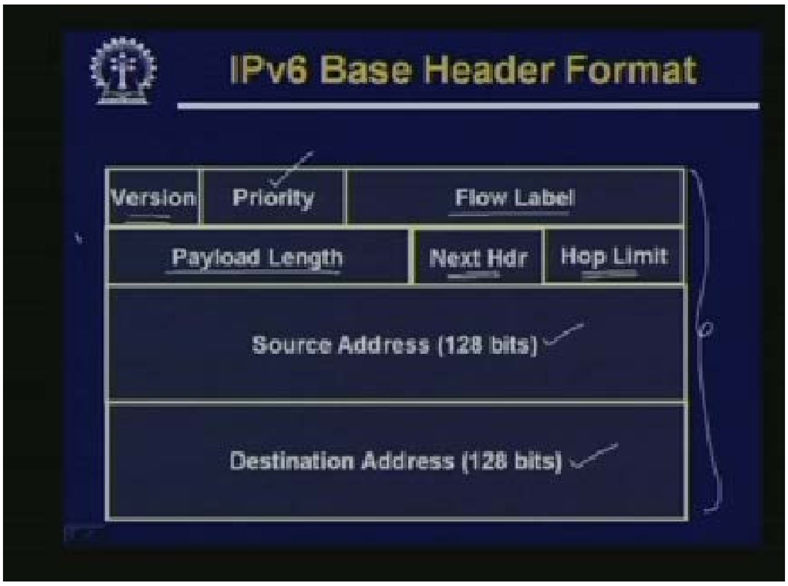
- An IP datagram begins with a base header, followed by zero or more extension headers, followed by data (transport-layer PDU).

≻40 bytes base header

✓	?		?	
Base Header	Extension Header 1	. . .	Extension Header N	Transport Layer PDU

Well as I had mentioned earlier that an IP datagram will always begin with a base header followed by zero or more extension header and finally you will be having the data path. This data path will be coming from the layer on top of IP. Typically on top of IP you have the TCP layer. So the TCP layer will be sending a chuck of data to IP for transmission. So actually this data is sometimes called the transport layer protocol data unit or PDU. So this data that we are showing in this diagram at the end this is the transport layer PDU before it you have a mandatory base header. But these extension headers are all optional. You may or may not require depending on what you are trying to do this extension headers maybe present may not be present and the thing to note is that the base header has a size of 40 bytes. In fact all the other extension headers are also of the same size 40 bytes base headers.

(Refer Slide Time: 34:07)



IPv6 Base Header Format

Version | Priority | Flow Label

Payload Length | Next Hdr | Hop Limit

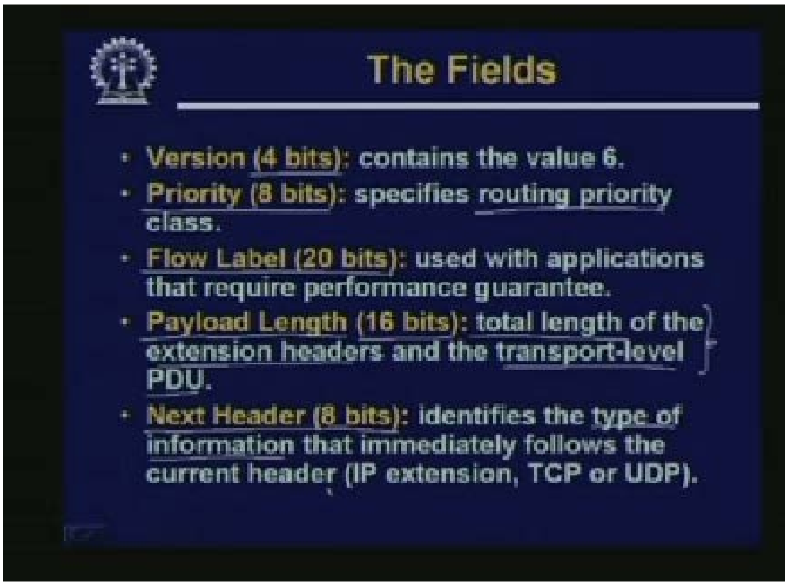
Source Address (128 bits)

Destination Address (128 bits)

So let us see what does the base header contain? The base header contains some fields Version for IPv6. This Version field will contain a number 6 priority. Well you can assign priorities to your packets. If a packet has a higher priority if it is assigned a higher priority, then the routers will give priority to your packet for transmit. Then you can have something called Flow Label, this is used for Flow control. Payload Length, this is the total size of the packet. Next Header we shall be talking about. Hop Limit this is what I had mentioned earlier this field is initialized with the maximum number of hops the packet can take. So whenever this packet hops from one to another the Hop Limit or hop count gets decremented as soon as it reaches zero.

The packet is discarded the idea is that this hop count is set to some maximum value and the nominal path length should not exceed that. If due to some reason the path length actually exceeds it. This will mean that either the packet was somehow routed in the wrong direction or it has some gone into a routing loop it is circulating in a circular path loop and in addition we have the Source Address and Destination Address. Both are 128 bits. So this total header size is 48 40 bytes, out of them the Source and Destination addresses will consume 16 and 16, 32 bytes. Remaining 8 bytes are for the other headers. Now let us see what the other (36:09) header their sizes and their functions are.

(Refer Slide Time: 36:11)



The Fields

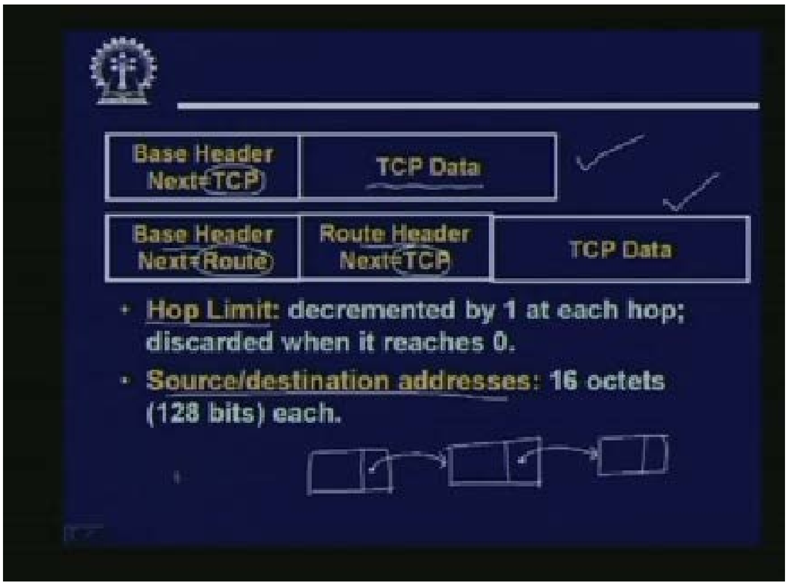
- Version (4 bits): contains the value 6.
- Priority (8 bits): specifies routing priority class.
- Flow Label (20 bits): used with applications that require performance guarantee.
- Payload Length (16 bits): total length of the extension headers and the transport-level PDU.
- Next Header (8 bits): identifies the type of information that immediately follows the current header (IP extension, TCP or UDP).

Version-I, I told it will contain the value 6 because this is IP version 4, this is a 4 bit field. 4 bit represent 6 you may need 3 bits only. But these 4 bits have been kept for future expansion. Maybe sometime later you may be having version 8, version 10 like that. So 4 bits are kept, Priority as I have told this specifies the routing priority Flow Label. Well this I am telling what this actually means? This ensures some sort of flow control and quality guarantee this field is used with applications that require performance guarantee. See suppose I go back to the example, I had said I need to establish a 64 kbps link with the destination.

So when the path gets established, so all the intermediate nodes are informed about my, I can say my willingness that I want to establish a path through you and I want a guaranteed bandwidth of 64kbps. Now I also mentioned that in order to have this feature all the datagrams must follow the same path. So essentially we are talking about something which is similar to a virtual circuit. So although we are talking it in terms of a datagram but since we are restricting the path, the path has to be the same. So it is effectively something like a virtual circuit and this Flow Label is actually something like a virtual circuit number. So if the packet contains that number every intermediate node on the router can find out well. This is the Flow Label number 10 which means I have to forward it to this node.

So this is very similar to the virtual circuit number actually and the next field is the Payload Length which is 16 bits, 2 bytes. This contains the total length of the extension headers plus the data path. Since it is 16 bits the total size of the datagram can be 64 kilobytes next header. It is an 8 bit field. It actually identifies that if there are some extension headers following, what is the type of extension header; it identifies the type of information that immediately follows the current header. There can be a number of different header types that follows the present base header. It is like a pointer to the next extension header the next header field essentially works as a link. It is like a link list the headers are maintained like a linked list.

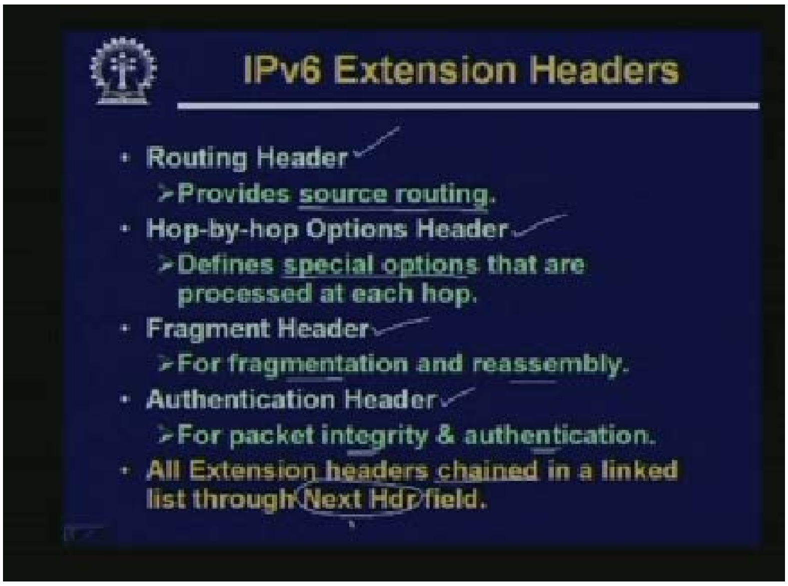
(Refer Slide Time: 39:14)



- Hop Limit: decremented by 1 at each hop; discarded when it reaches 0.
- Source/destination addresses: 16 octets (128 bits) each.

So this diagram will show you this suppose you have in the first example, you have a packet with only the base header, nothing else. So you have the base header followed by the data which is the TCP data the data which has come from the TCP layer. So in the next header field the value TCP will be stored this will mean that the next whatever is following the base header is the TCP data. But in the next example say we have a scenario where in addition to the base header we have another header which is a routing header which is used to establish a high quality path. For example, so in this case the base header will have the next pointer as of type route. The route header we have the next one of type TCP. So essentially what it means that all the headers are like the nodes of a link list and there is a connection from one to the other. So starting from the base header you know that what is the next type of the header. If there is a header you process it otherwise you can straight away go to the TCP data and so on. So Hop Limit I have mentioned and Source destination address also I have mentioned.

(Refer Slide Time: 40:50)



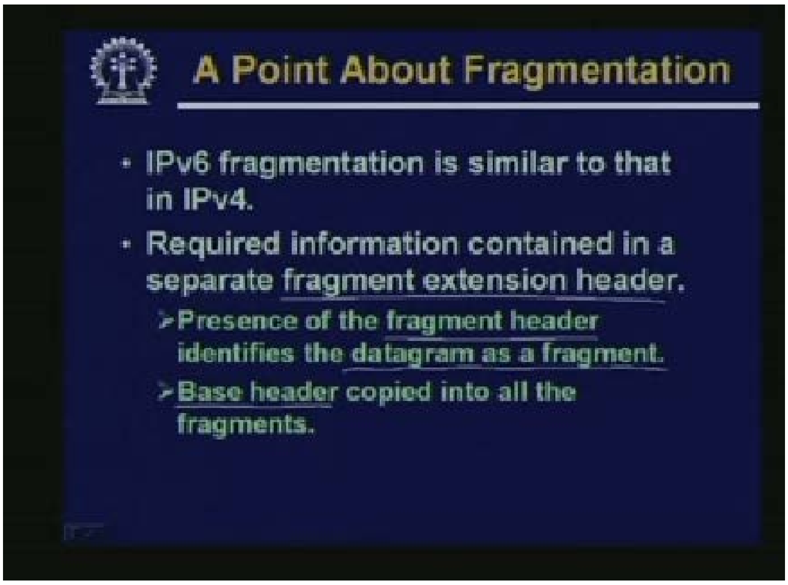
IPv6 Extension Headers

- Routing Header
  - Provides source routing.
- Hop-by-hop Options Header
  - Defines special options that are processed at each hop.
- Fragment Header
  - For fragmentation and reassembly.
- Authentication Header
  - For packet integrity & authentication.
- All Extension headers chained in a linked list through Next Hdr field.

Now IPv6 extension header there are a number of different header types possible some of these have been shown here. First one is the routing header which provides the so called source routing. Source routing means the source can specify the path. The datagram has follow suppose I am sending a packet to destination and I know that if the packet follows this particular route then it will be good for me. There will be less congestion; the packet delivery speed will be higher so I can specify that please follow this path. So if it is a source routing packet then the IP layers in between they will not try to carry out any routing decision on their own. They will simply follow my instructions which I have sent along with the packet.

So you have a so called hop by hop options header. So here you can specify a number of special options. So I am not going into details but the number of options can be varied. So these options can be processes at each hop. So in case the packets get fragmented you have Fragment header, so for fragmentation and reassembly the fragment headers are used for security applications, you can have an authentication header where packet integrity and authentication can be taken care of. That means to verify the source of the packet to verify that the packet has not been modified and as I had mentioned that all the extension headers are chained in a link list, by using the Next Header field which is present in every header base header as well as the extension headers they are connected as a link list right.

(Refer Slide Time: 42:50)

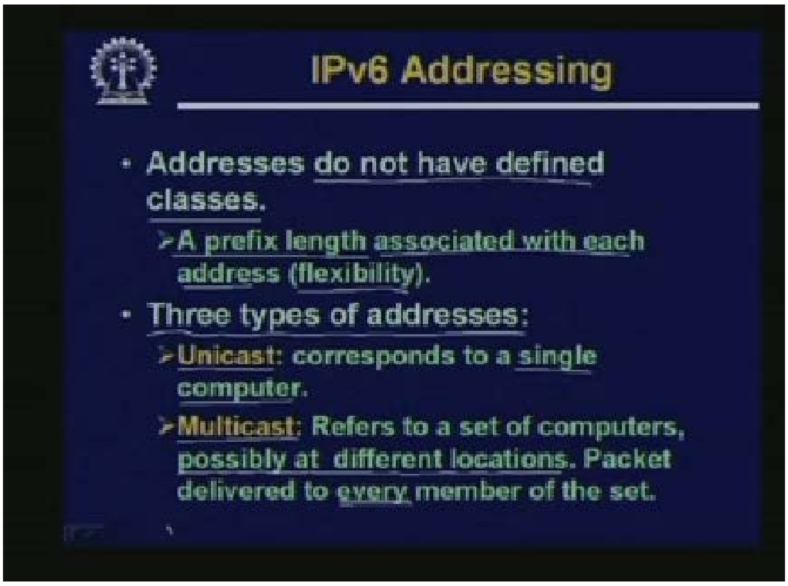


A Point About Fragmentation

- IPv6 fragmentation is similar to that in IPv4.
- Required information contained in a separate fragment extension header.
  - ➢Presence of the fragment header identifies the datagram as a fragment.
  - ➢Base header copied into all the fragments.

Regarding fragmentation, well IPv6 and IPv4 fragmentation are similar. But in IPv6 the only difference is that fragmentation information is not stored in the base header; rather it is stored in a separate fragment extension header. Now if in a packet you find that the fragment header is present. This means that the present packet has to be a fragment. So just by looking at the presence of the fragment header you can actually confirm whether the packet corresponds to a fragment packet or not. And well if a packet gets fragmented then the base header gets copied into all the fragments. The optional fragment header along with the offset and other information will get appended or added to the different fragments. And that is done exactly in the same way as in IPv4. So there is not really much difference out there.

(Refer Slide Time: 43:59)

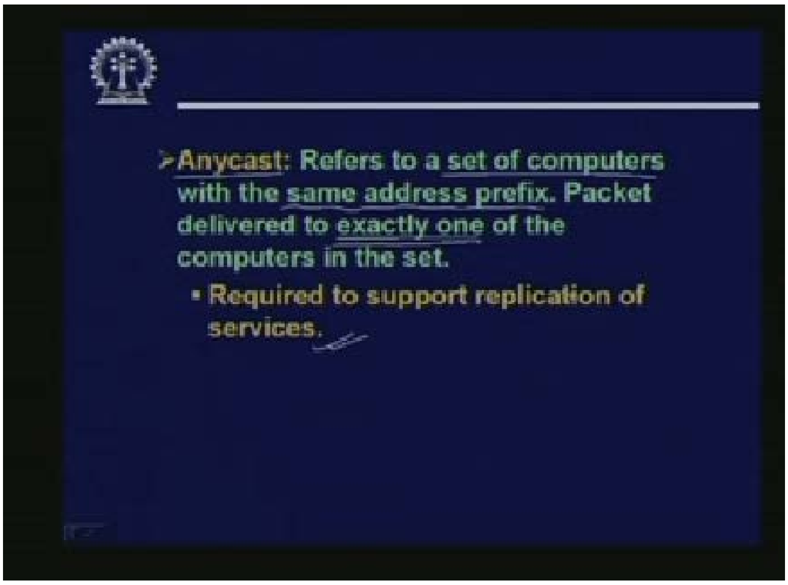


IPv6 Addressing

- Addresses do not have defined classes.
  - ➢A prefix length associated with each address (flexibility).
- Three types of addresses:
  - ➢Unicast: corresponds to a single computer.
  - ➢Multicast: Refers to a set of computers, possibly at different locations. Packet delivered to every member of the set.

Talking about IPv6 addressing how we specify address of a host. So unlike IPv4 here you do not have any defined classes like that A B C. Rather you can specify a prefix length with each address like you can see say CIDR class less internet domain routing. So you have seen CIDR provides enough flexibility. Depending on my requirement I can specify a prefix length and the last few bits I can use as my host addresses in my network that can provide with a lot of flexibility. But here it is more general as we shall see very shortly and in terms of the types of addresses there are three types one is of course Unicast. But the destination is a single computer. Multicast where the destination maybe a set of computers but they may not belong to the same LAN. They may possibly belong to different locations. Now if it is a Multicast address then the packet will be delivered to every member of the set this is Multicast.

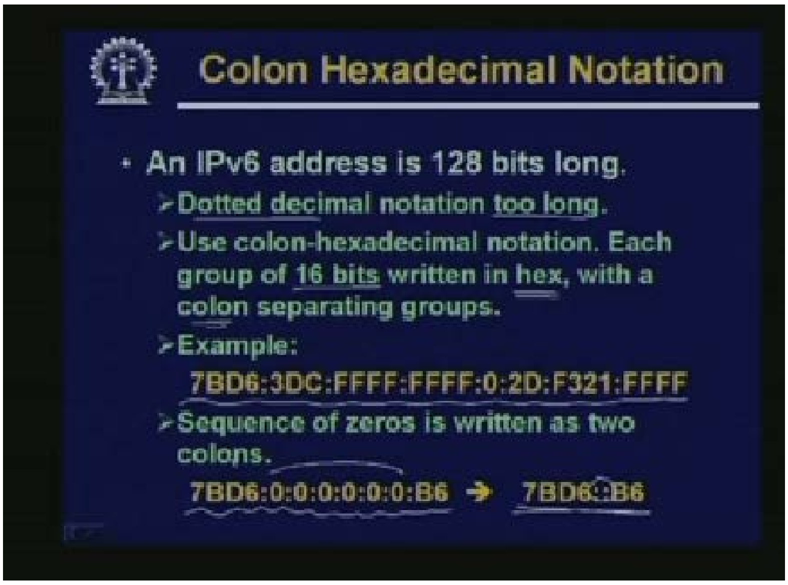
(Refer Slide Time: 45:19)



- Anycast: Refers to a set of computers with the same address prefix. Packet delivered to exactly one of the computers in the set.
  - Required to support replication of services.

Now in contrast I just mentioned you can also have Anycast where again you also have a set of computers. And Anycast you can say address all the computers must have the same address prefix and packet will be delivered to exactly one of these computers. So this Anycast as I had mentioned, this is typically used to support replication of services or mirrors in system.

(Refer Slide Time: 45:50)

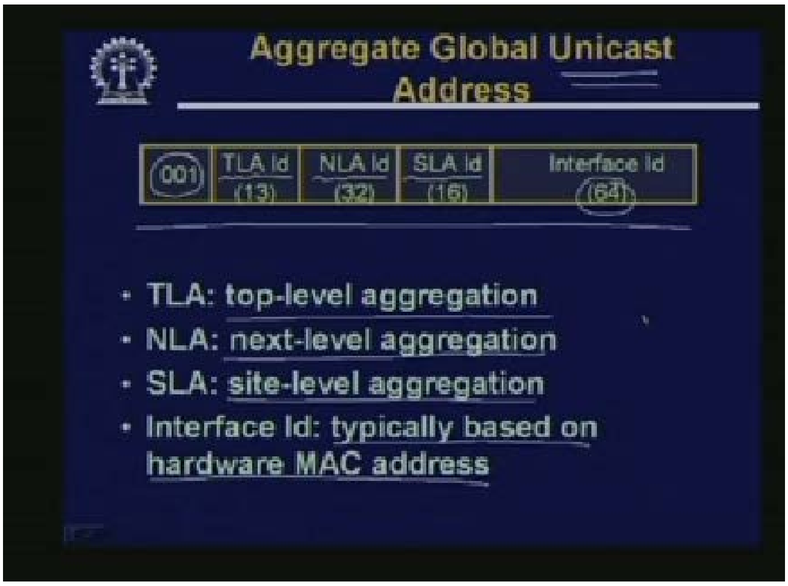


Colon Hexadecimal Notation

- An IPv6 address is 128 bits long.
  - Dotted decimal notation too long.
  - Use colon-hexadecimal notation. Each group of 16 bits written in hex, with a colon separating groups.
  - Example:
    7BD6:3DC:FFFF:FFFF:0:2D:F321:FFFF
  - Sequence of zeros is written as two colons.
    7BD6:0:0:0:0:0:0:B6 → 7BD6::B6

Now IPv6 address is normally expressed in the so called Colon Hexadecimal Notation. The dotted decimal notation like IPv4 will be too long to use. Colon hexadecimal notation works like this. The whole 128 bit address you divide into groups of 16 bits and write each of them down separately in hexadecimal and instead of dot we use a colon to separate them. This is an example of an IPv6 address. Now in practice you will find that most of the addresses you will have will contain lots of zeros like this. Now it is possible that there are a set of consecutive. You can say hex blocks which are all zeros. So in this case you can write it in a compact notation where all these consecutive zeros can be written as double colon two colon written as two colons. So this is a compact way of writing this down.

(Refer Slide Time: 46:57)



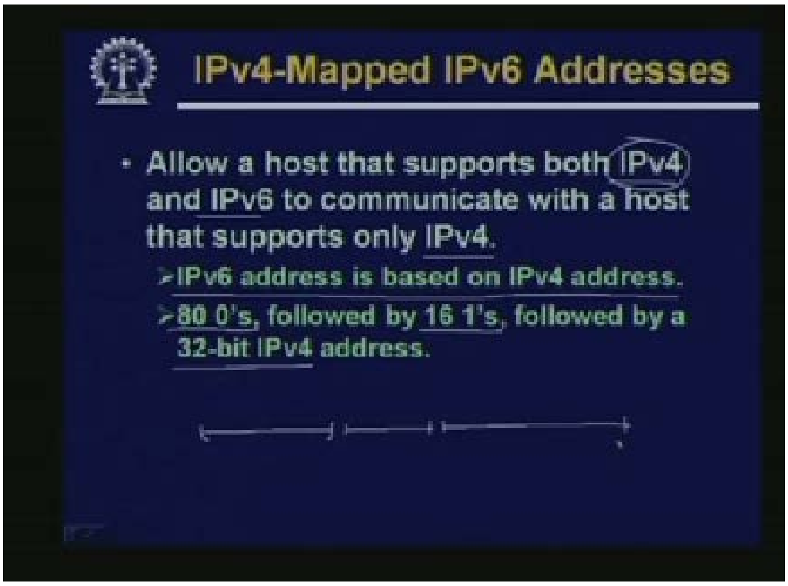
Aggregate Global Unicast Address

001	TLA Id (13)	NLA Id (32)	SLA Id (16)	Interface Id (64)

- TLA: top-level aggregation
- NLA: next-level aggregation
- SLA: site-level aggregation
- Interface Id: typically based on hardware MAC address

And you can have Aggregate Global Unicast Address. This means that the total IPv6 address you can divide as follows. Well, you usually start with 001 indicating that it is a Unicast address. All Unicast address will start with 001. You can have top-level aggregation. This can refer to the top-level internet provider. There are 13 bits for it; you can have next-level aggregation. This can be country level internet service provider you can have site-level aggregation. You can city based internet service provider, you can have a number of different levels of hierarchy and at the end you have 64 bits to represent your computer. So what I has been suggested is that these 64 bits can be used to represent MAC addresses directly. So that there is no chance of replication 2 ad 2 computers can never have the same address. So by these kind of hierarchal facility you can very well or means you can assign the addresses in a very structured way and simply by looking at the address you can very easily know that to which hierarchy your address belongs to, you can know of your country which ISP you belong to and so on.

(Refer Slide Time: 48:16)

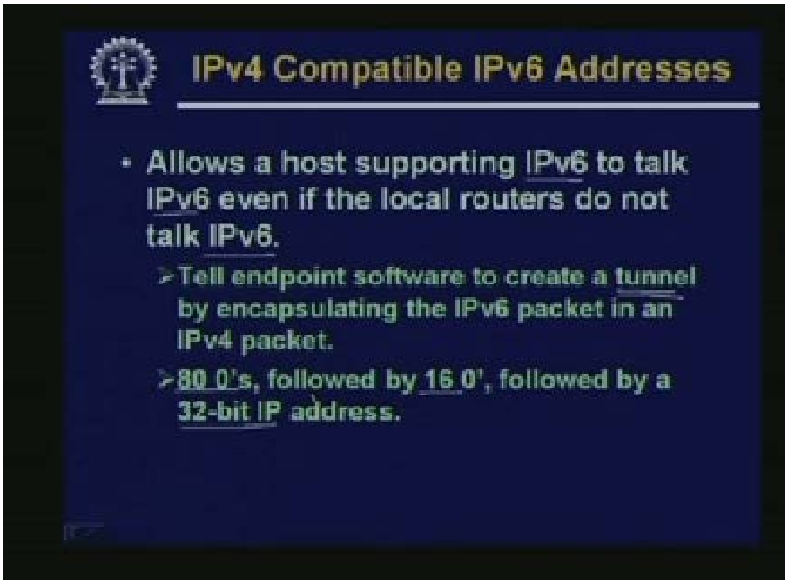


IPv4-Mapped IPv6 Addresses

- Allow a host that supports both IPv4 and IPv6 to communicate with a host that supports only IPv4.
  - IPv6 address is based on IPv4 address.
  - 80 0's, followed by 16 1's, followed by a 32-bit IPv4 address.

And there is something called IPv4 Mapped IPv6 address. This will allow a host that supports both IPv4 and IPv6 to communicate with a host which understands only IPv4. Here there is a convention of the address. The first 80 bits of the address will be 0’s followed by 16 1’s followed by a 32 IPv4 address of that machine. So the IPv6 address is basically derived from the IPv4 address. This is how you write first there will be a sequence of then there will be a sequence of once. Then the actual IP address 32 bits.

(Refer Slide Time: 48:57)

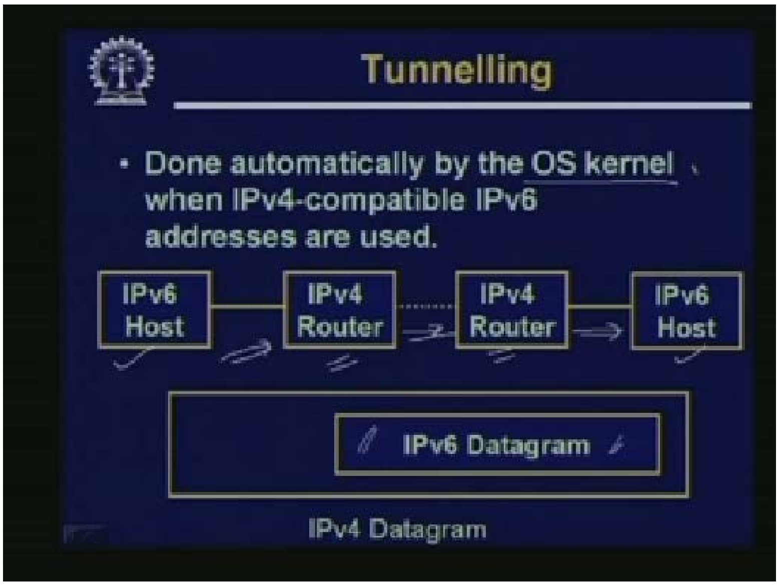


IPv4 Compatible IPv6 Addresses

- Allows a host supporting IPv6 to talk IPv6 even if the local routers do not talk IPv6.
  - Tell endpoint software to create a tunnel by encapsulating the IPv6 packet in an IPv4 packet.
  - 80 0's, followed by 16 0', followed by a 32-bit IP address.

After that you can have something called IPv4 compatible IPv6 addresses. Here a host supporting IPv6 can talk IPv6 even if the intermediate routers do not support IPv6. So this uses tunnelling, the IPv6 packet can tunnel through an IPv4 network. Here the convention is that 80 plus 16, 96 0's are there in the beginning followed by the IP for IP address it is 32 bits.

(Refer Slide Time: 49:35)

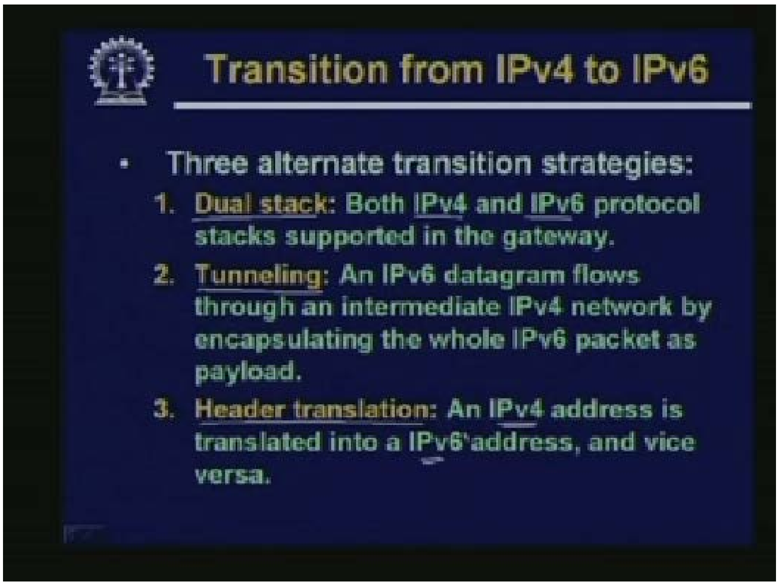


Tunnelling

- Done automatically by the OS kernel when IPv4-compatible IPv6 addresses are used.

So this looks like this. You have the IPv6 host, IPv6 there are number of intermediate routers which understand only IPv4 use tunnelling where the IPv6 packet or datagram is treated as the data you create an IPv4 datagram on top of it and send it here, here, and here. So the final IPv6 host will take out the IPv6 datagram and will extracting the data from here. This is typically done automatically by the OS kernel which supports IPv6.

(Refer Slide Time: 50:06)

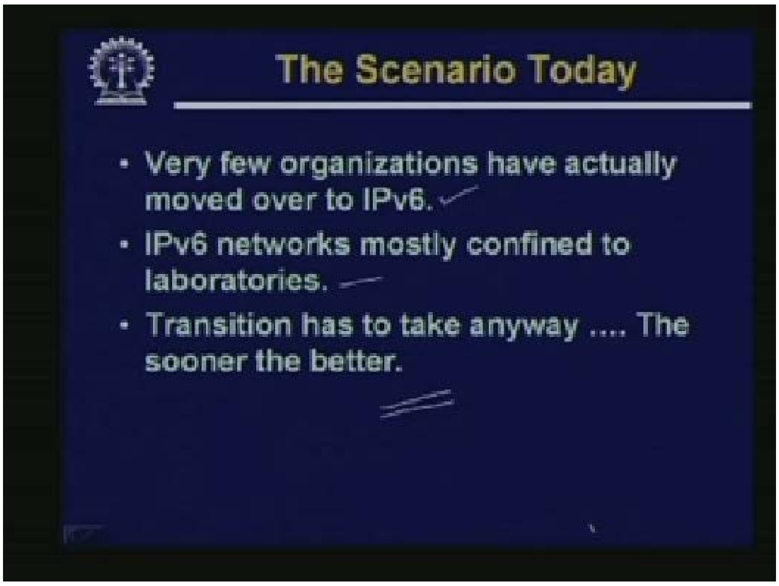


Transition from IPv4 to IPv6

- Three alternate transition strategies:
  1. Dual stack: Both IPv4 and IPv6 protocol stacks supported in the gateway.
  2. Tunneling: An IPv6 datagram flows through an intermediate IPv4 network by encapsulating the whole IPv6 packet as payload.
  3. Header translation: An IPv4 address is translated into a IPv6 address, and vice versa.

And to talk about the transition, well you can have a system of where you have both IPv4 and IPv6 protocol you can have Tunnelling which we have just mentioned. You can have Header Translation where a gateway will automatically translate an IPv4 header to an IPv6 address. These are the different kinds of options that you have when you want to do a transition from IPv4 to IPv6.

(Refer Slide Time: 50:40)

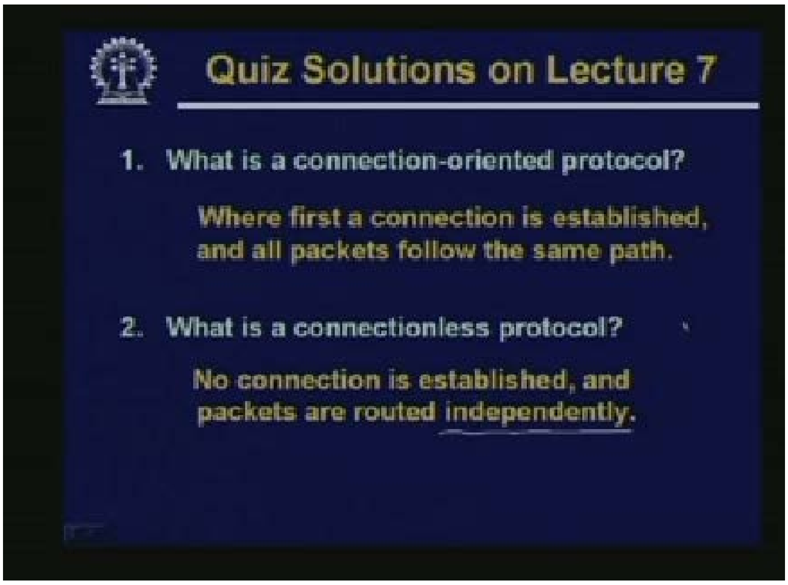


The Scenario Today

- Very few organizations have actually moved over to IPv6.
- IPv6 networks mostly confined to laboratories.
- Transition has to take anyway .... The sooner the better.

But the modern day scenario is that very few organizations are actually moved to on to IPv6 because of some compatibility issues. Most of the IPv6 networks are confined to labs. But the transition has to take anyway. So we have to gear up for the future and find out that when earliest we can carry out the transition. So with this we conclude our lecture. Now let us quickly look through the solutions.

(Refer Slide Time: 51:10)



Quiz Solutions on Lecture 7

1. What is a connection-oriented protocol?

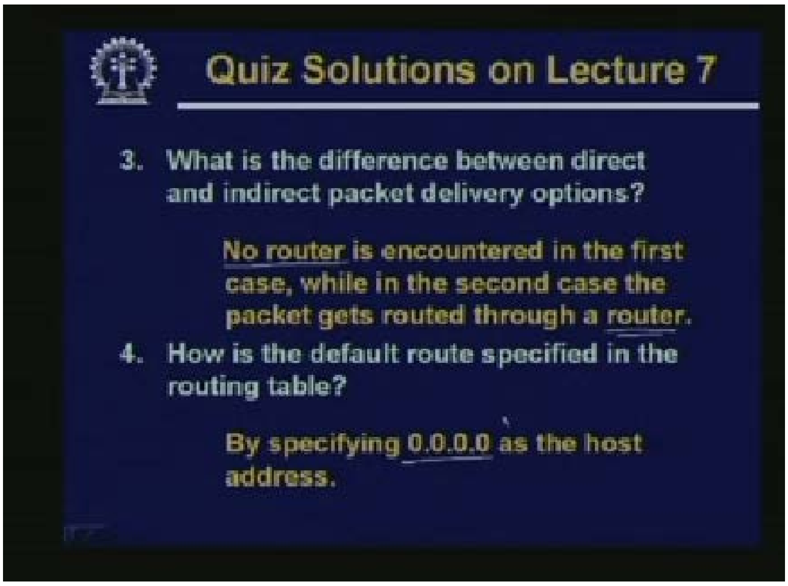
   Where first a connection is established, and all packets follow the same path.

2. What is a connectionless protocol?

   No connection is established, and packets are routed independently.

To the quizzes of our last class the questions are fairly simple. What is a connection-oriented protocol? Basically this means that where first a connection is established then the packets are sent and a connectionless protocol where you do not establish a connection and packets are routed in an independent way. It is basically virtual circuit and datagram kind of approach.

(Refer Slide Time: 51:35)



Quiz Solutions on Lecture 7

3. What is the difference between direct and indirect packet delivery options?

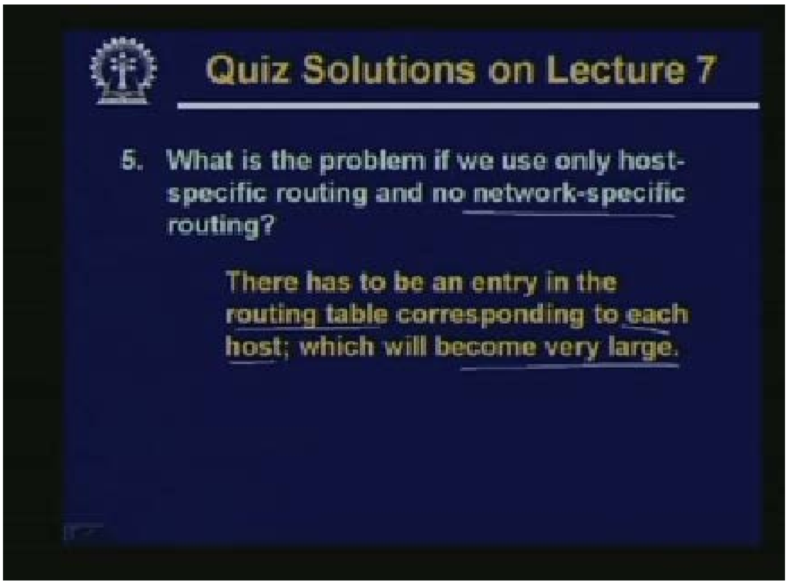
   No router is encountered in the first case, while in the second case the packet gets routed through a router.

4. How is the default route specified in the routing table?

   By specifying 0.0.0.0 as the host address.

What is the difference between direct and indirect packet delivery? In direct packet delivery no router is encountered in between. But in indirect, the packet may have to go through intermediate routers. This is the difference. How is the default route specified in the routing table? By specifying as the address 0.0.0.0, that will mean default.

(Refer Slide Time: 52:04)



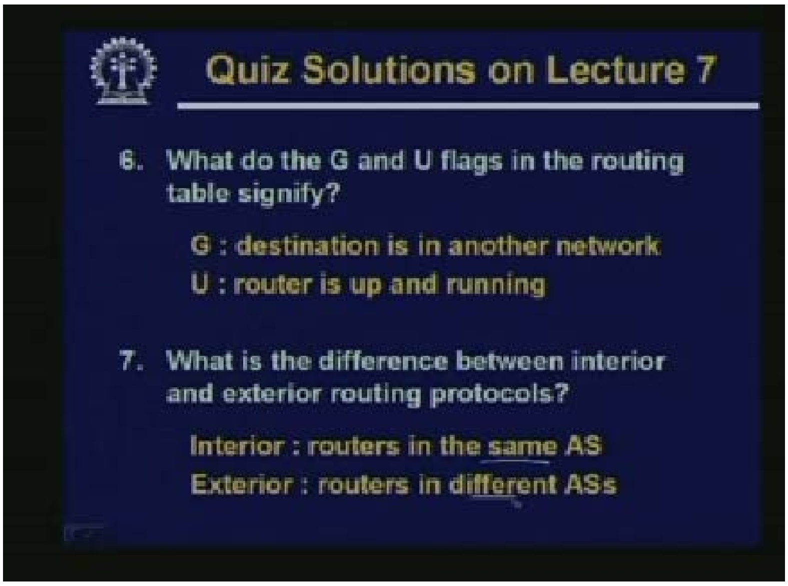
Quiz Solutions on Lecture 7

5. What is the problem if we use only host-specific routing and no network-specific routing?

   There has to be an entry in the routing table corresponding to each host; which will become very large.

What is the problem if we use only host-specific routing and no network-specific routing? The problem is that there has to be an entry in the routing table corresponding to each host which can become very big the routing table can become very large. That is why we have to go for network-specific routing. Because in host-specific if there are 1000 hosts, then the routing table has to contain 1000 entries.

(Refer Slide Time: 52:26)



Quiz Solutions on Lecture 7

6. What do the G and U flags in the routing table signify?

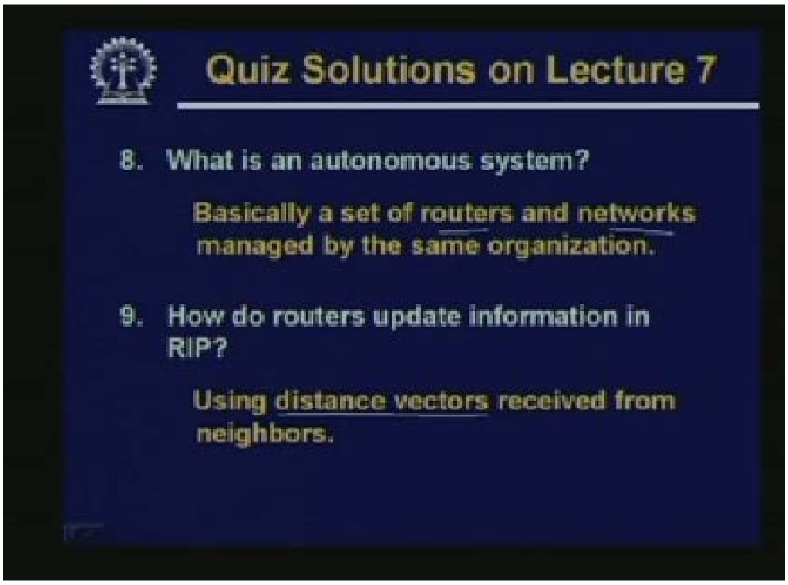
   G : destination is in another network
   U : router is up and running

7. What is the difference between interior and exterior routing protocols?

   Interior : routers in the same AS
   Exterior : routers in different ASs

G and U flags what do they signify? G means destination is in another network; U means router is currently up and running. Difference between interior and exterior routing protocols. We have told this many times for Interior protocols router are in the same autonomous system; exterior they are in different autonomous systems.

(Refer Slide Time: 52:48)



Quiz Solutions on Lecture 7

8. What is an autonomous system?

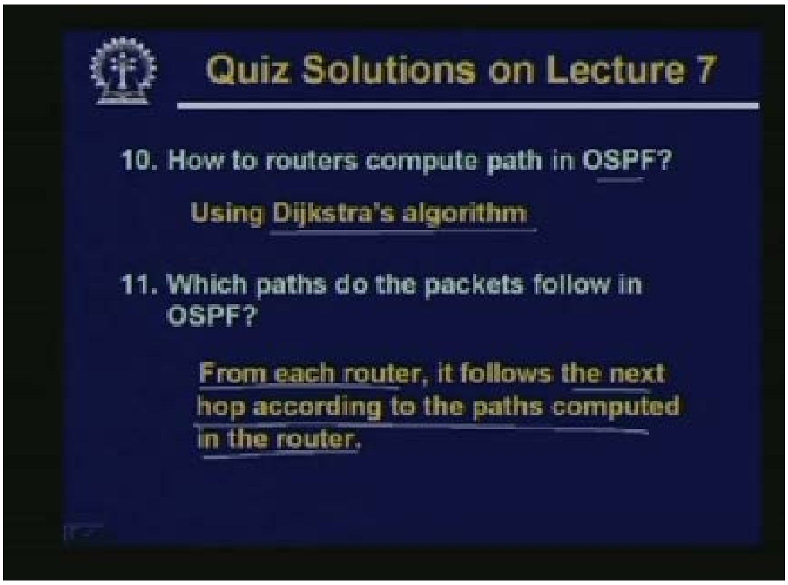
Basically a set of routers and networks managed by the same organization.

9. How do routers update information in RIP?

Using distance vectors received from neighbors.

What is an autonomous system? They are a set of routers and networks which are managed by the same organization. How do routers update information in RIP? They use distance vector routing by using distance vector received from the neighbours they update their tables.

(Refer Slide Time: 53:06)



Quiz Solutions on Lecture 7

10. How to routers compute path in OSPF?

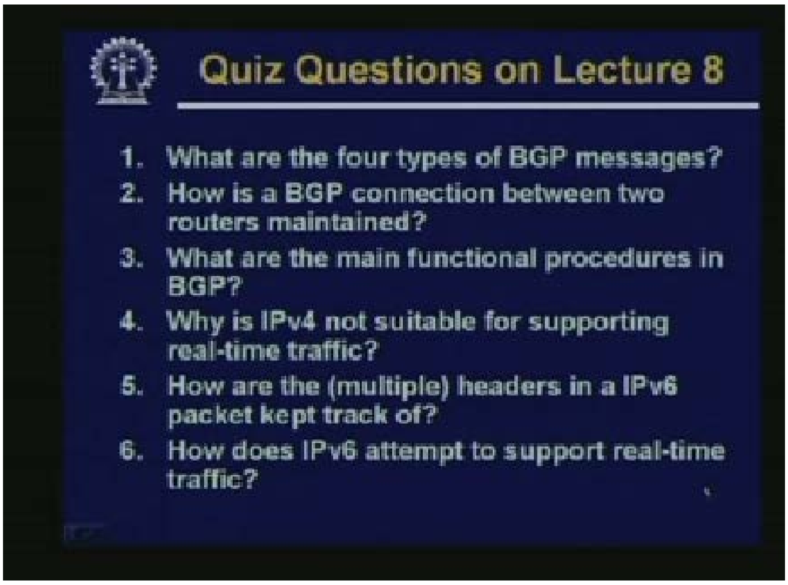
Using Dijkstra's algorithm

11. Which paths do the packets follow in OSPF?

From each router, it follows the next hop according to the paths computed in the router.

How do routers compute path in OSPF? Well OSPF uses the shortest path algorithm Dijkstra's algorithm to compute the shortest path. Because OSPF every router has complete information about the network they can optimally compute the shortest path. Which paths do the packets follow in OSPF? Well, OSPF from each router it follows the next hop according to the paths computed in the router. Because the Dijkstra's algorithm computes the shortest path. But it only keeps information about the next hop with respect to the shortest path and regarding questions from today's lecture. These are some questions.

(Refer Slide Time: 53:53)

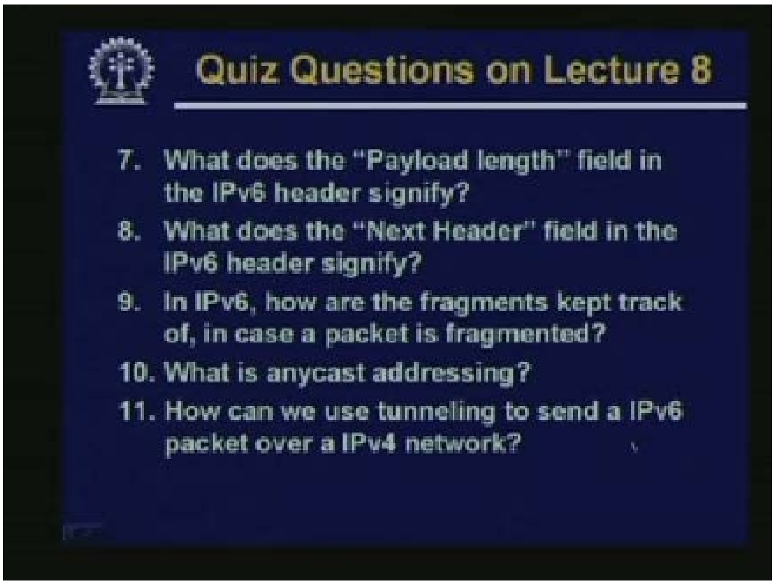


Quiz Questions on Lecture 8

1. What are the four types of BGP messages?
2. How is a BGP connection between two routers maintained?
3. What are the main functional procedures in BGP?
4. Why is IPv4 not suitable for supporting real-time traffic?
5. How are the (multiple) headers in a IPv6 packet kept track of?
6. How does IPv6 attempt to support real-time traffic?

What are the four types of BGP messages?
How is BGP connection between two routers maintained?
What are the main functional procedures in BGP?
Why is IPv4 not suitable for supporting real-time traffic?
How are the multiple headers in an IPv6 packet kept track of?
How does IPv6 attempt to support real-time traffic?

(Refer Slide Time: 54:17)



Quiz Questions on Lecture 8

7. What does the "Payload length" field in the IPv6 header signify?
8. What does the "Next Header" field in the IPv6 header signify?
9. In IPv6, how are the fragments kept track of, in case a packet is fragmented?
10. What is anycast addressing?
11. How can we use tunneling to send a IPv6 packet over a IPv4 network?

What does the Payload length field in the IPv6 header signify?
What does the Next Header field signify?
In IPv six how are the fragments kept track of in case a packet is fragmented?
What is anycast addressing?
How can we use tunnelling to send an IPv6 packet over a IPv4 network?

So with this we come to the end of today’s lecture. Thank you.

(Refer Slide Time: 54:47)

Preview of next lecture

Preview of next lecture.

(Refer Slide Time: 54:49)

Lecture No. # 09

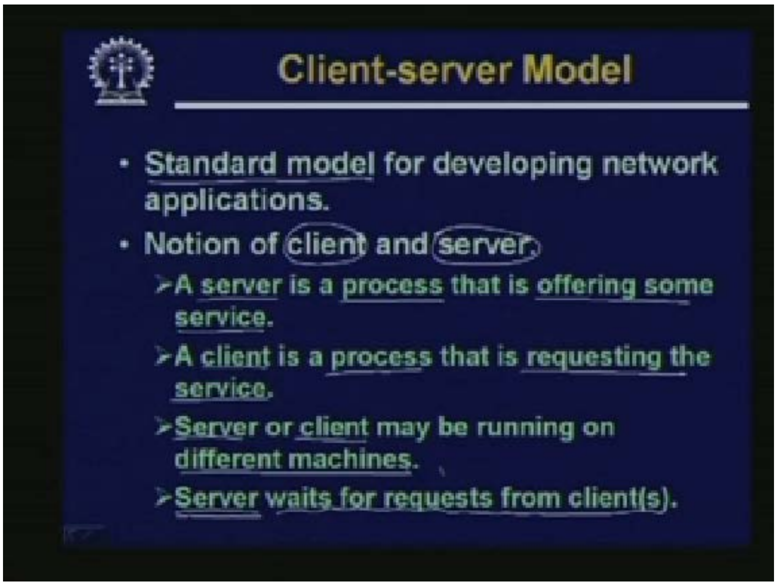
Client Server Concepts

DNS, Telnet, FTP

Client Server Concepts DNS, Telnet, FTP.

In this lecture, I would like to touch upon the very important concept which is used widely in the internet now days. You must have heard about the term, Client Server Concept, Client Server programming. In fact most of the internet applications that we see today, that we use today, they are based on this kind of client-server programming. So first I try to explain what this client-server programming concept is all about. Then we shall be specifically looking at some of the applications of the internet. So client server concepts and some of the applications are the topic of our discussion today.

(Refer Slide Time: 55:44)

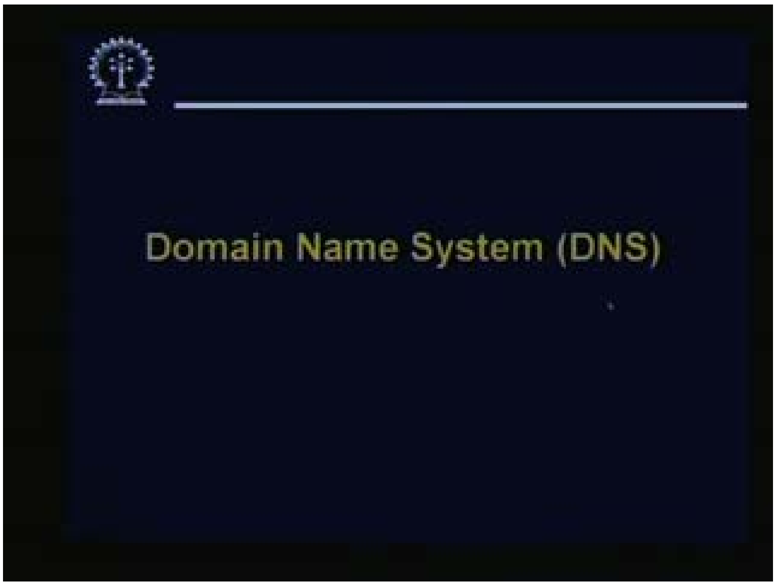


Client-server Model

- Standard model for developing network applications.
- Notion of client and server.
  - A server is a process that is offering some service.
  - A client is a process that is requesting the service.
  - Server or client may be running on different machines.
  - Server waits for requests from client(s).

So first see what the client server model is all about. This is a standard model for developing network applications today. Now as the name implies there is the notion of a client, there is the notion of a server. The basic idea is that a server is a program or which is sometimes called a process. A program in execution is called a process a server is a process which is continuously running and it wants to offer some services to clients. So my purpose of telling all these things was to give you a rough idea about what this client server concept is all about and I have told you all the internet applications that you see they are all based on the client server concept. Now I will start with one of the most important applications which will in itself is not an independent application. But is used by many other practical applications that is the so called Domain Name System or DNS.

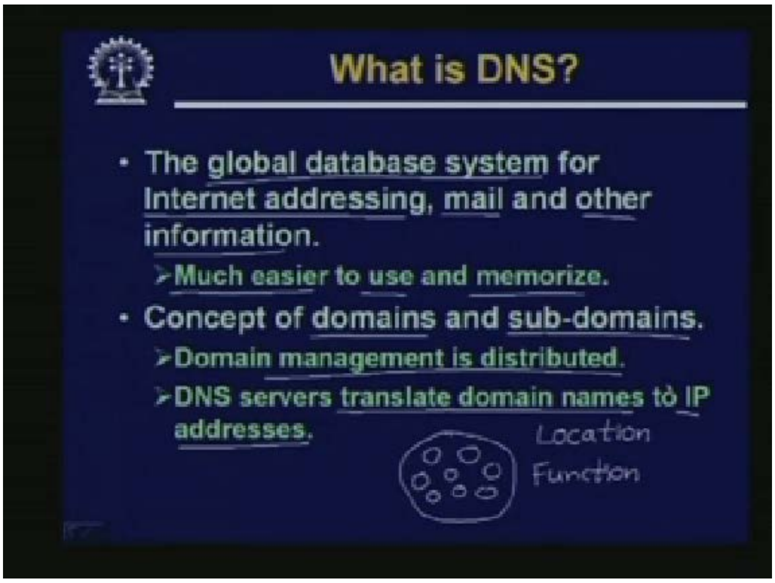
(Refer Slide Time: 56:56)



Domain Name System (DNS)

This is you may have heard, this is a very important service which is provided in the internet in LAN's in different areas.

(Refer Slide Time: 57:08)



What is DNS?

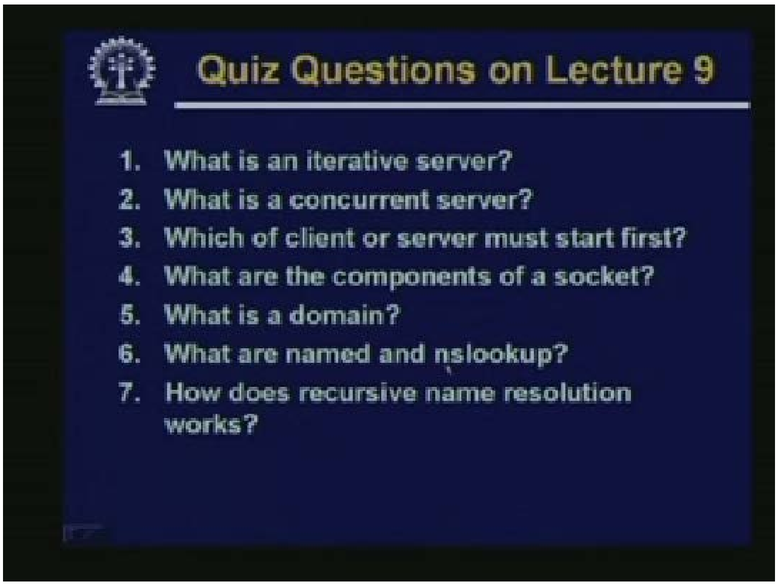
- The global database system for Internet addressing, mail and other information.
  - ➢Much easier to use and memorize.
- Concept of domains and sub-domains.
  - ➢Domain management is distributed.
  - ➢DNS servers translate domain names to IP addresses.

Location

Function

Basically the domain name system is a global database system for internet addressing mail. Other see, here this need not be restricted to internet and mail it can refer to World Wide Web, Telnet, FTP, any kind of application you use today. You typically use a name you do not always use an address. The purpose of the DNS essentially is to convert from a name into an address. So this is how it works. Now the advantage of using DNS is that see the using names rather than addresses is much easier to use easier to memorize. Like for example I am giving you, one practical I can say example, say the mail server of the computer science and engineering department of IIT Kharagpur. That can be referred to by a name cse, the full name is cse.iitkgp.ernet.in. Well you are familiar with names of this type. Now this kind of a name is easier to memorize, but I also know that the IP address of the cse machine is 144.16.192.57. Of course you cannot remember many such addresses with numbers you may tend to forget. But using names is much more easier because it is more English like more easy to memorize. So now some questions from today's lecture.

(Refer Slide Time: 58:58)



Quiz Questions on Lecture 9

1. What is an iterative server?
2. What is a concurrent server?
3. Which of client or server must start first?
4. What are the components of a socket?
5. What is a domain?
6. What are named and nslookup?
7. How does recursive name resolution works?

What is an iterative sever?
What is a concurrent server?
Which of client or server must start first?
What are the components of a socket?
What is a domain?
What are named and nslookup?
How does recursive name resolution works?