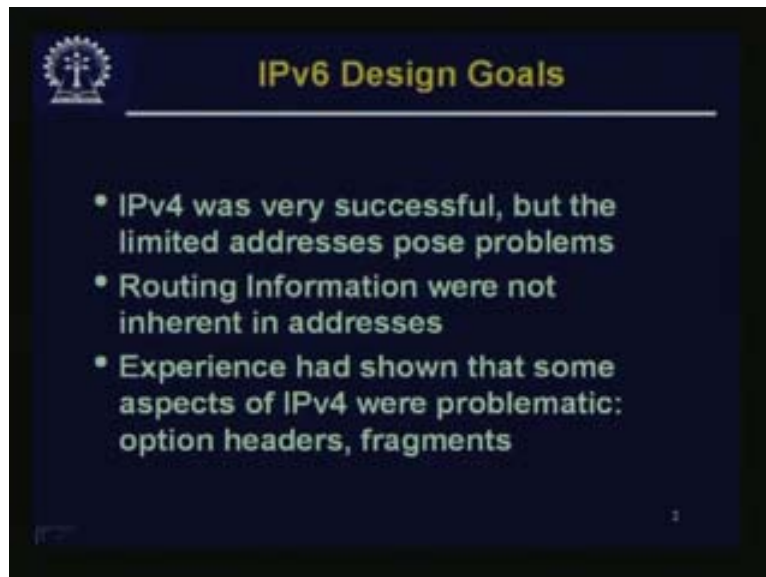


**Computer Networks**  
**Prof. S. Ghosh**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**  
**Lecture No: 29**  
**IP Version 6 & Mobile IP**

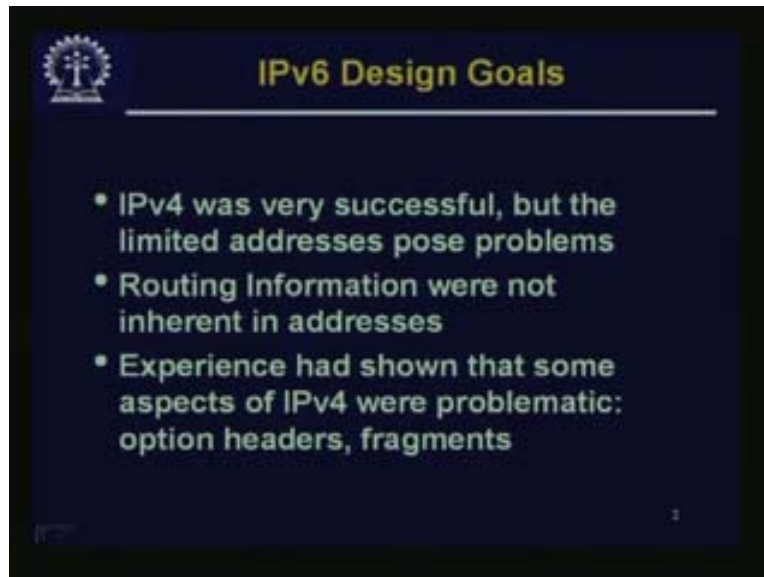
Good day, in the last lecture we discussed about IP version - 4 [IPv4]. That is the version of Internet Protocol that is now ubiquitous in the sense almost everywhere it is used. However, as this particular version became more popular than its originated thought then some problems about IPv4 came into focus and people started discussing about what is the next generation of Internet Protocol that would be there and after a lot of discussion etc people came up with this IP Version 6 [IPv6]. We will be doing a little discussion on IPv6 today. In the later part of the lecture we will be talking about mobile IP.

(Refer Slide Time: 01:38 – 01:37)



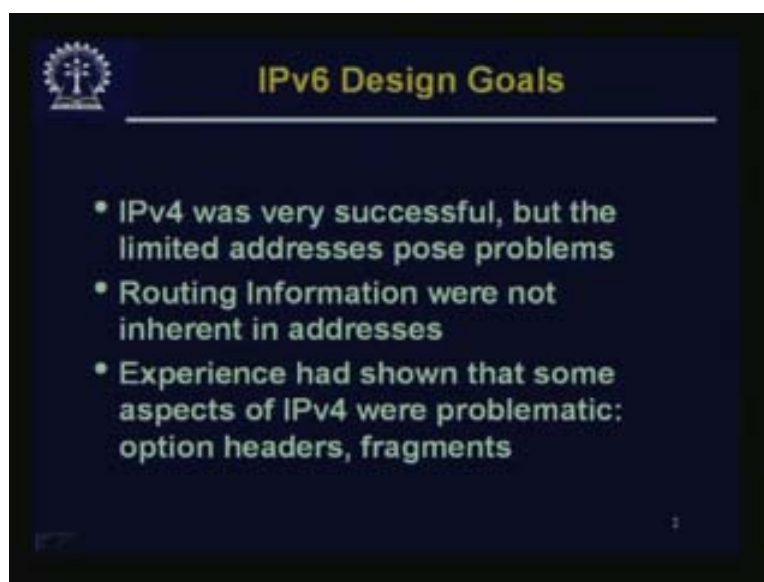
What was the design goal? As I mentioned, IPv4 was very successful, but the limited addresses posed problems. This was discussed earlier as how people are trying to fight with this problem using NATing/netting etc because so many machines are coming into the network these days and not only machines but in certain cases people are actually deploying all kinds of gadgets which should be connected to the network. If something is connected to the network and accessed from anywhere on the internet then it has to have an IP address. The pool of IP addresses we have in IPv4 is very limited and this is one of the major problems.

(Refer Slide Time: 02:34 – 02:47)



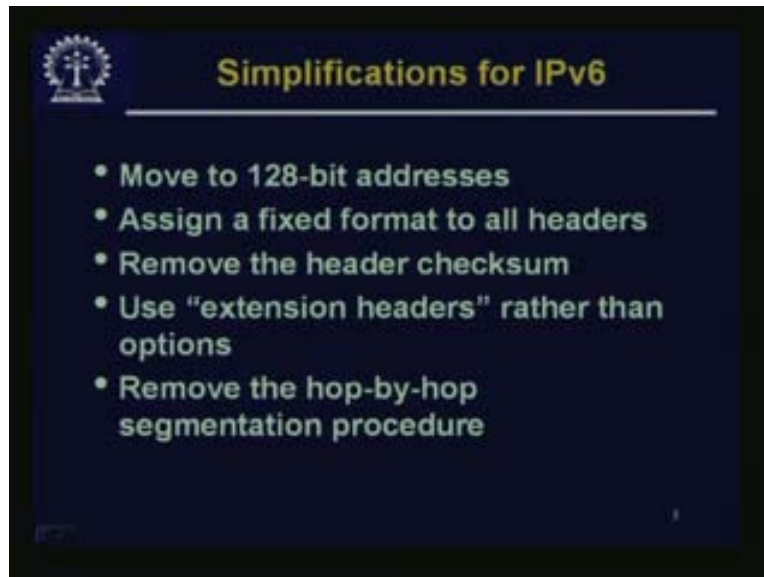
The second problem is, as mentioned earlier, the routing information were not inherent in addresses. For example, in a postal address, we have the Pin Code and in the pin code if the first digit is 7 then immediately we know that it is towards the East. If the first digit is 1 immediately we know that it is towards the North. So just by looking at that you can simply send the material to that direction. However, that has not been so because these IP addresses although they were based on networks which have larger chunks than hosts were distributed but then this could not be maintained at that time. If you could have some means of geographical information inbuilt into it then routing becomes easier and the routing table becomes smaller. Therefore, if the routing table is smaller routing speed becomes faster and so there are many advantages.

(Refer Slide Time: 03:43 – 04:07)



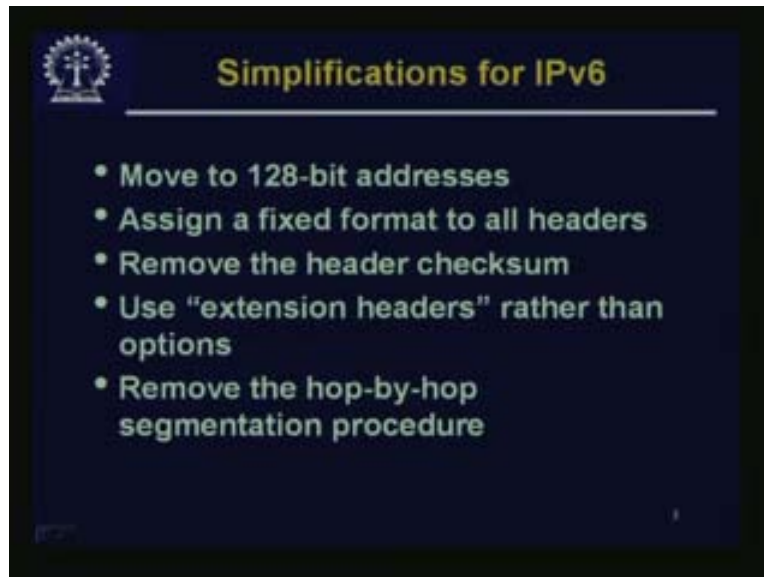
Thirdly, experience had shown that some aspects of IPv4 were problematic like Option headers and fragments etc were problematic then some type of service [TOS] which people never used, options also have a very limited utility because of its limited size and fragments was a problem. These were the basic issues.

(Refer Slide Time: 04:08 – 04:21)



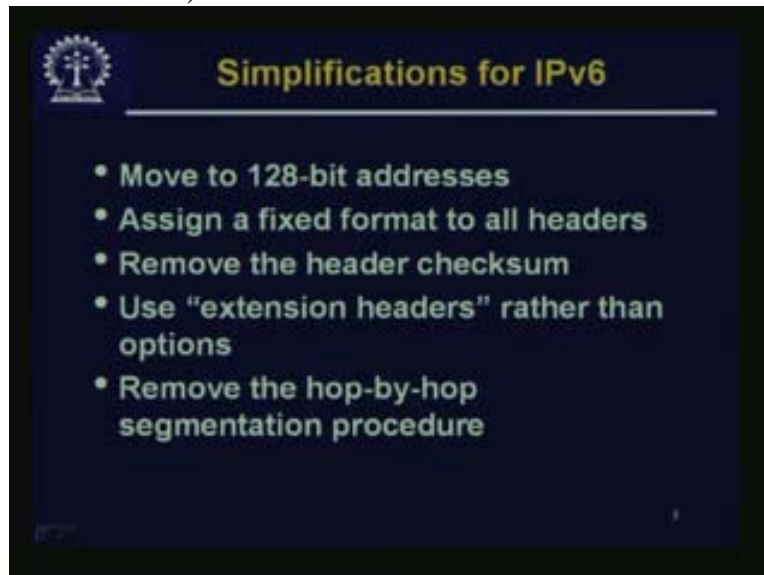
The simplification for IPv6 as mentioned was that to move to a 128-bit address. From 32-bits if you remember that IPv4 has as an address size of 32-bits whereas this is 128-bits. So in IPv4 in a theoretical maximum it is 2 power 32 (of course it is less than that but anyway the theoretical maximum is 2 power 32) addresses. Whereas here it is 2 power 128<sup>128</sup> addresses which is a very huge number. Even, if all the devices and computers you can think of are connected and given individual address space then also you will have a huge number of addresses to spare. This was done with the idea that we are not going to run into this problem of limited address space ever. The other point is, if you have so many bits, as I said that even after assigning numbers to all the devices and computers you will be left with some to spare so that can be used more intelligently.

(Refer Slide Time: 05:15 - 05:25)



Second point was to assign a fixed format to all headers. In IPv4 also, the essential part of it, the initial part of it, the compulsory part of it is fixed. But there are options and these options could be of various sizes so that is also removed.

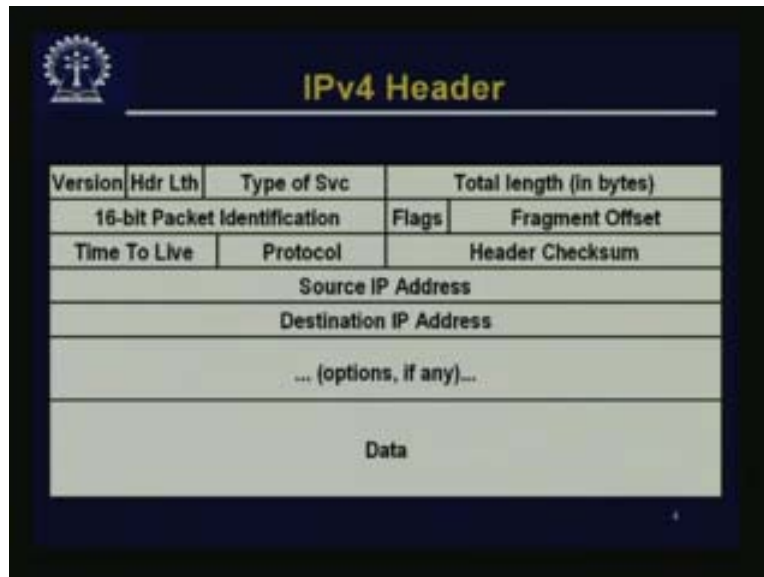
(Refer Slide Time 05:37 – 06:01)



Remove the header checksum which was not doing much anyway. Use extension header rather than options. Options were removed and we came to the concept of extension header that means headers followed by other headers, we will come to this later on. Remove hop-by-hop segmentation procedure. That means you do not segment it somewhere in between a packet that is traveling and then somewhere in between you try to fragment it. However, that was not a good idea, and because of this fragmentation you have to keep the fragmentation number, the packet

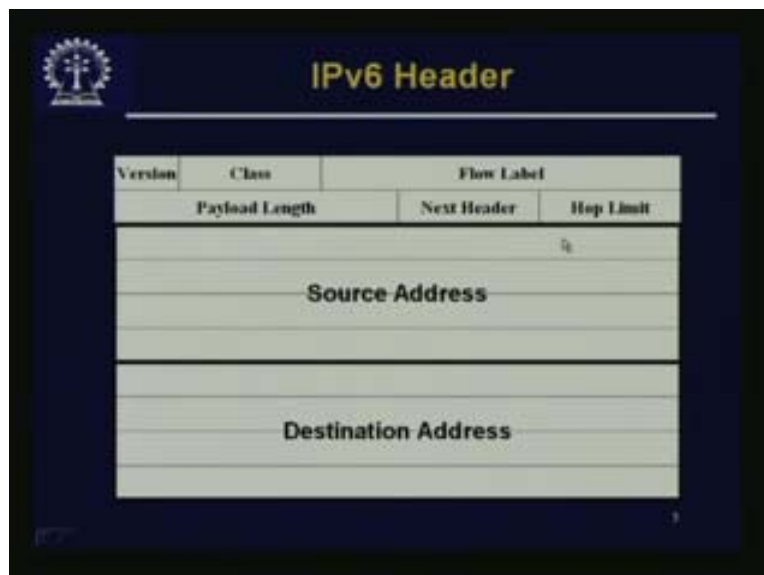
identification etc so all these are removed although fragmentation can be handled in some way. We will talk about that later.

(Refer Slide Time: 06:23 – 06:44)



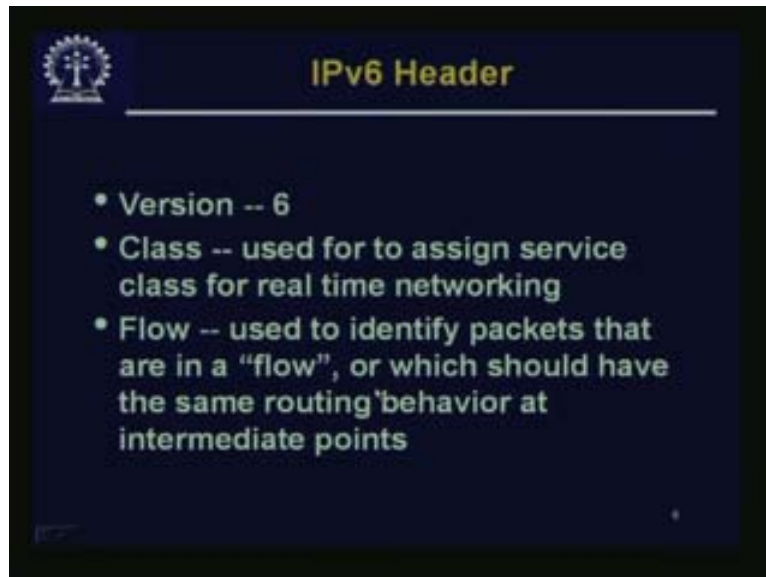
This was the original IPv4 header which we have already discussed like version header, length, type of service etc. This Type Of Service [TOS] was not very useful. Fragments etc came in because we allowed fragmentation which is not done here. Header checksum may go out but the source and destination IP addresses would be there. Let us come to the IPv6 Header.

(Refer Slide Time: 06:45 – 07:09)



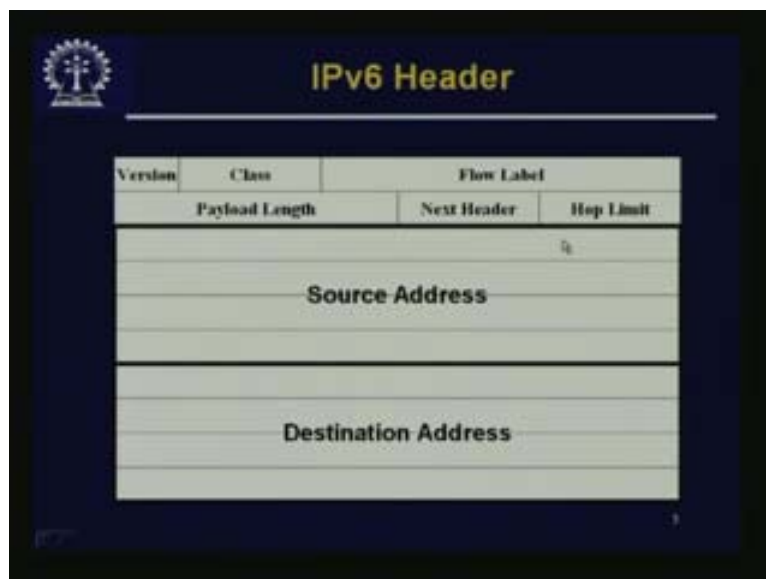
IPv6 Header is actually much simpler than the IPv4 Headers. We have a few fields and then the source address. Assuming that this is 32, previously IPv4 address was only one line but now you have four lines i.e. 128-bits for source address and 128-bits for destination address. Let us look at the fields.

(Refer Slide Time 07:10 – 07:27)



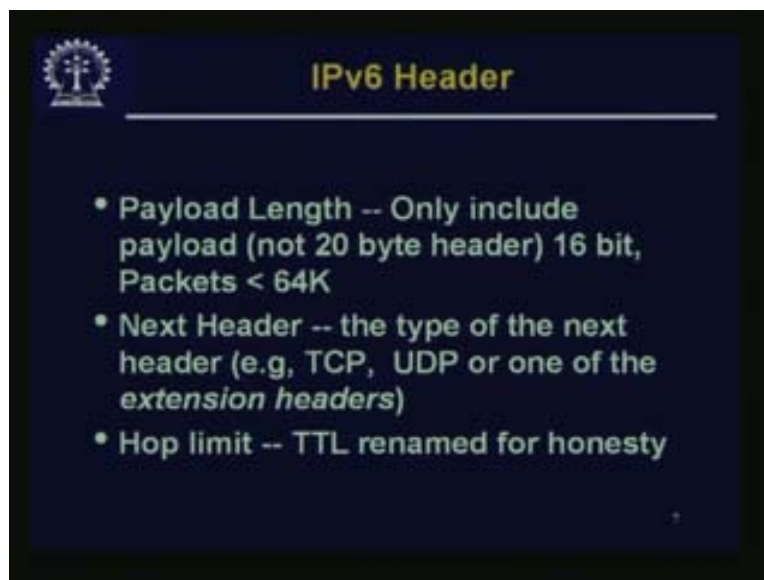
One is the version number. Previously it was 4 but now it is 6. Class: This is used to assign service class for real time networking. If you are doing some real time networking that can be indicated here. Then, there is a field called Flow: If you quickly look at it we have version, class, flow level.

(Refer Slide Time: 07:28 – 07:32)



Flow: Flow means given one particular source and another destination then for this particular source and destination pair there is a flow level. Flow means these two are likely to send large number of packets and all of them would belong to the same flow. This is not a virtual circuit identifier like ATM because in ATM the virtual circuit identifier and intermediate switch would just look at the virtual circuit identifier and switch it that way. This is not for that purpose at all rather this is for treating the packets with a particular flow level from a particular source and destination in the same way where all packets belonging to the same flow level in the intermediate router. For example, there may be class of service or all kinds of quality of service requirements for one particular flow that may require bandwidth reservation in between. Therefore such things can be handled using the flow level.

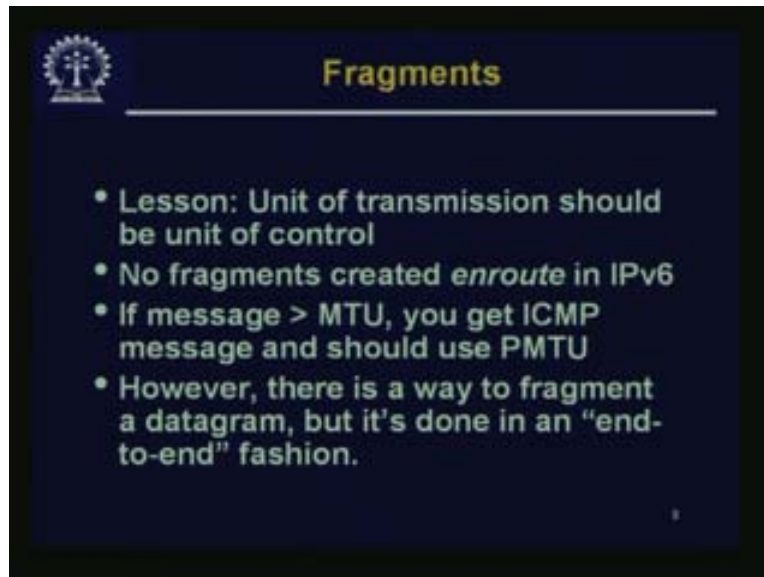
(Refer Slide Time: 08:45 – 09:31)



Payload Length: Only include the payload and not the 20-byte Header. This is 16-bits for that so packets are once again less than or equal to 64 k. Next Header; this gives rise to the possibility that there may be more than one header. If there are not any more IPv6 Headers then, at least the higher layer headers like TCP or UDP Headers could be there. There is a field called Hop Limit. This is really the TTL (Time to Live) which was present earlier in IPv4 but was used to just keep the count of the Hop and this is just renamed as Hop Limit.



(Refer Slide Time: 09:32 – 10:12)

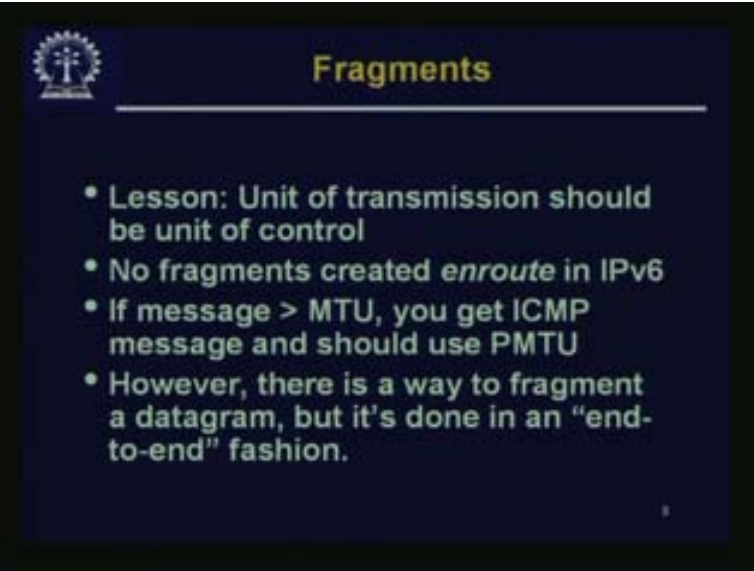


Fragments: One of the lessons we learnt in IPv4 was that the unit of transmission should be the unit of control so no fragments created en-route in IPv6. If message is greater than MTU the Maximum Transferable Unit then you get ICMP message, which is an Internet Control Message Protocol. We will talk a little bit more about ICMP later on. However, this is some kind of control message, which may be sent by a router to host etc. So, an ICMP message should use the path MTU. Let us see what is meant by this MTU and path MTU and how do you avoid transmission.

Suppose you are the source and you want to transmit a particular packet it so happens that en route it encountered a link where such a big packet cannot be accommodated. In IPv6 what this router will do is that it will drop the packet and send back an ICMP message saying that this MTU is so much which is for the next link. Now you will reduce your packet size at the source itself and try to send it again. But now it will definitely cross that particular link, it may get struck again in another link so again an ICMP message will come back but finally you will come to size of packet which will go through all the links. Now this is your path MTU. Now you can go on sending all your communication using this particular packet length and it will not be fragmented in between.



(Refer Slide Time: 11:17 – 11:36)

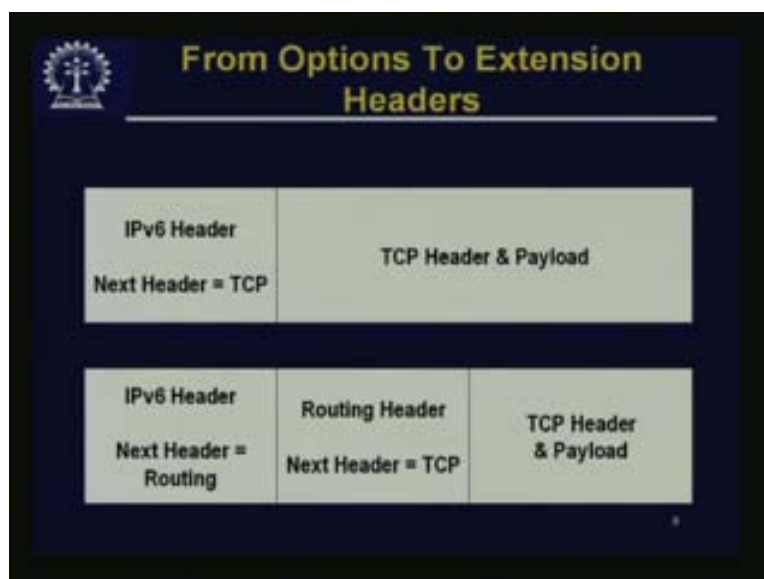


**Fragments**

- Lesson: Unit of transmission should be unit of control
- No fragments created *enroute* in IPv6
- If message > MTU, you get ICMP message and should use PMTU
- However, there is a way to fragment a datagram, but it's done in an "end-to-end" fashion.

This is a way to fragment a datagram but it is done in an end-to-end fashion. It may so happen that for some particular application all these smaller packets we have made should actually be made into bigger packets. So this is fragmentation in some sense so far as the application layer is concerned so there is a way to indicate that, there is a header for that.

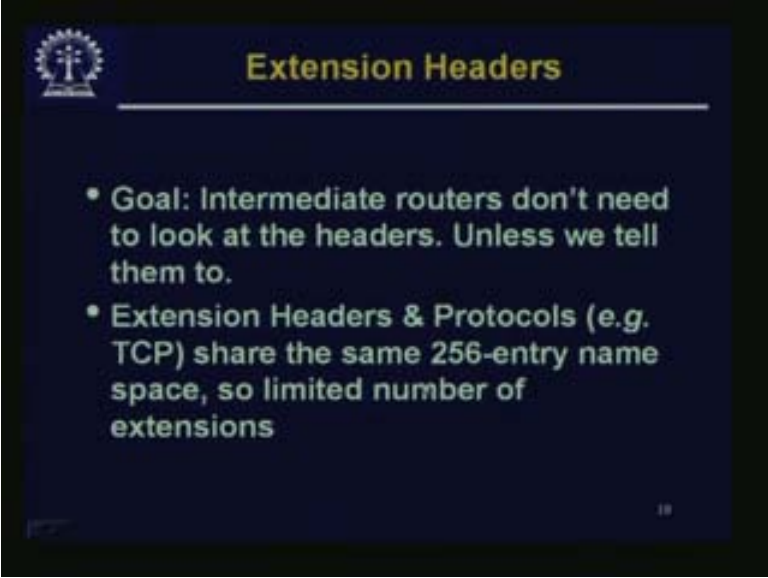
(Refer Slide Time: 11:46 – 12:29)



Finally we have removed the options from the IPv4 Header and we have come to this Extension Header. That means there may be more than one header. We could have this situation that IPv6 Header and next Header is said to be TCP. The Payload is the TCP Header and Payload itself. It could be that IPv6 Header, the Next Header is a Routing Header, which again is an extension

header for IPv6 Routing Header and the Next Header is TCP so the TCP header and payload comes here. So there may be more than one IPv6 Headers and Headers are of different types.

(Refer Slide Time: 12:29 – 13:01)

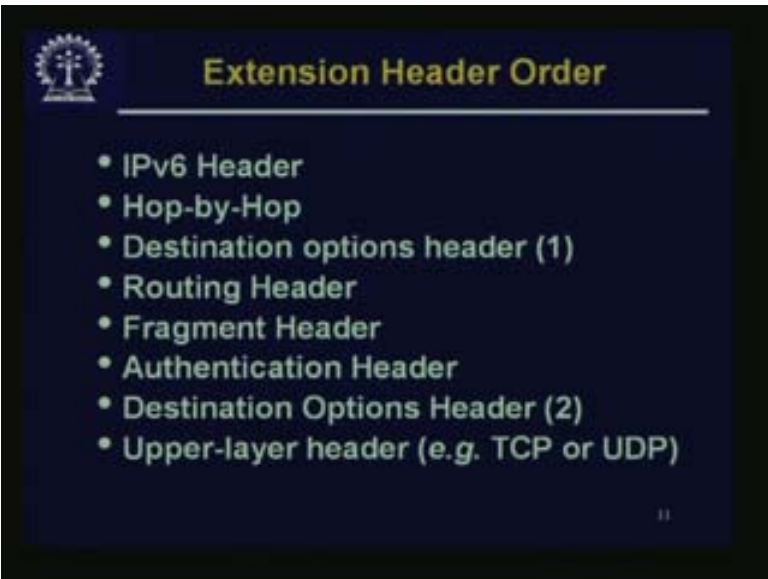


The slide is titled "Extension Headers" in yellow text on a dark blue background. It features a small logo in the top left corner. The main content is a bulleted list in white text. The first bullet point states the goal for intermediate routers. The second bullet point discusses the shared 256-entry name space for extension headers and protocols like TCP. A small number "10" is visible in the bottom right corner.

- Goal: Intermediate routers don't need to look at the headers. Unless we tell them to.
- Extension Headers & Protocols (e.g. TCP) share the same 256-entry name space, so limited number of extensions

Intermediate routers do not need to look at the Headers unless we tell them to. Specifically it has to look at some Headers but can ignore few other headers. It does not need to process all the information it should be fast. Extension Headers and Protocols, for example, TCP shares the same 256-entry name space i.e. 256-entry name space for the Headers. Hence there are limited number of extensions but this number is a big enough.

(Refer Slide Time: 13:02 – 13:33)

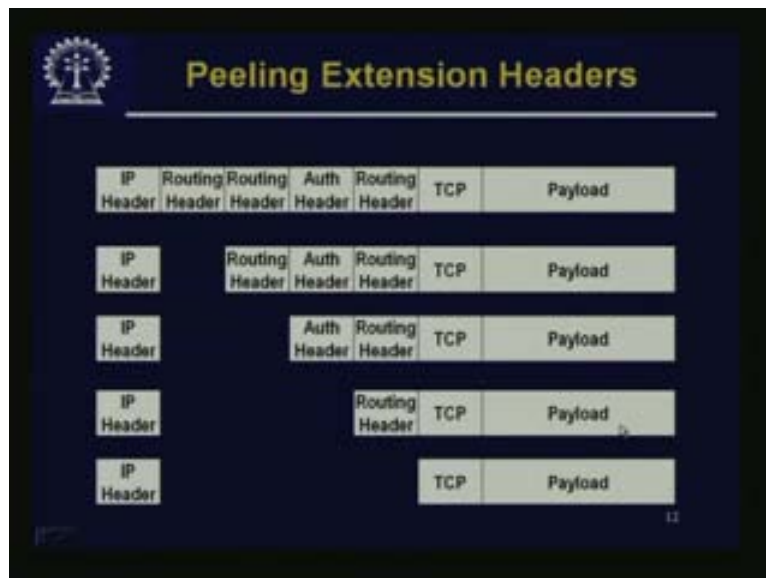


The slide is titled "Extension Header Order" in yellow text on a dark blue background. It features a small logo in the top left corner. The main content is a bulleted list in white text showing the sequence of headers in an IPv6 packet. A small number "11" is visible in the bottom right corner.

- IPv6 Header
- Hop-by-Hop
- Destination options header (1)
- Routing Header
- Fragment Header
- Authentication Header
- Destination Options Header (2)
- Upper-layer header (e.g. TCP or UDP)

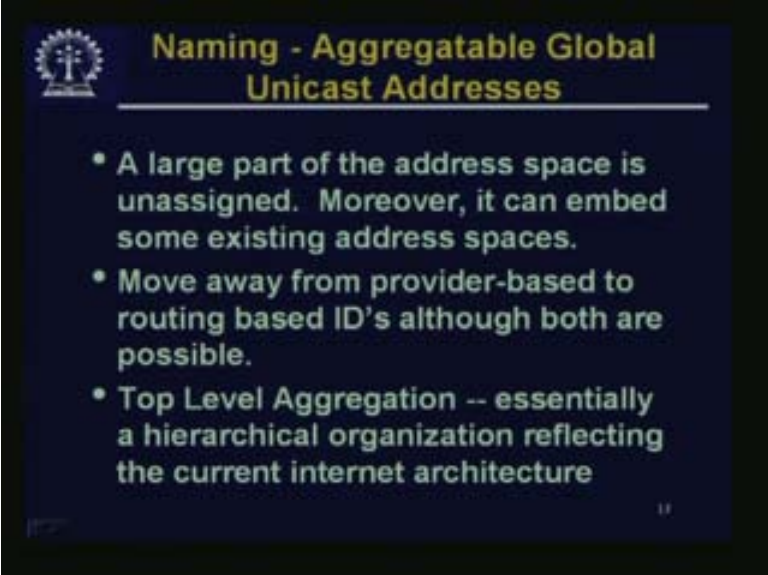
There is a certain order suggested that these Headers should occur in one particular order. One is, IPv6 Header the main header we talked about, An And the Extension Header called hop-by-hop Header, Destination Options Header, Routing Header, Fragment Header, Authentication Header, Destination Options Header, Upper-layer Headers if any that means TCP or UDP. Let us quickly discuss a few of them.

(Refer Slide Time: 13:34 – 14:21)



Payload may be encapsulated, payload followed by the Transport layer Header. Then there is a TCP, then a Routing Header, Authentication Header, another two Routing Headers, then IP header and so on. What you do is that you peel them one by one so that one Routing Header is peeled of because the Routing Header gives you information about how to route the packet something like source routing so that is peeled of may be in the next hop and this goes out. The IP Header remains and the routing header authentication header etc remains. You peel out one Header after another and finally you get to the TCP and the payload.

(Refer Slide Time: 14:22 – 14:38)



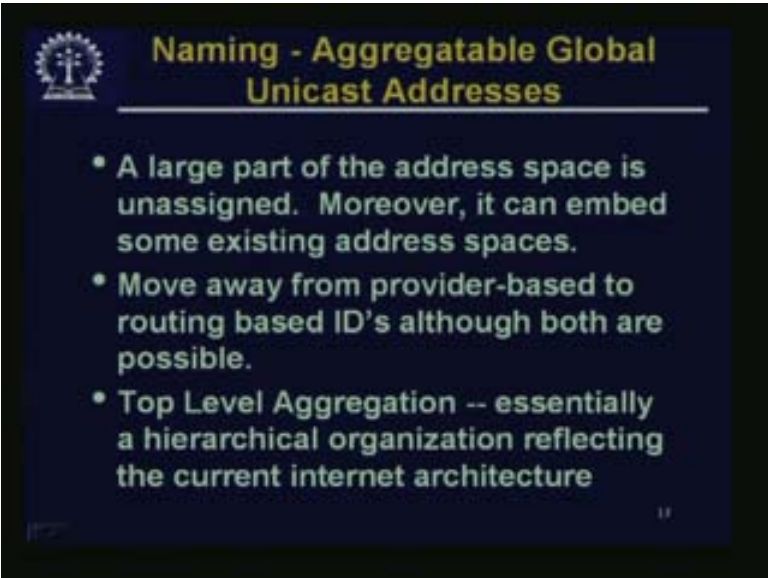
The slide features a dark blue background with a yellow title and white bullet points. In the top left corner, there is a small circular logo containing a stylized cross. The title is underlined. The bullet points are as follows:

- A large part of the address space is unassigned. Moreover, it can embed some existing address spaces.
- Move away from provider-based to routing based ID's although both are possible.
- Top Level Aggregation -- essentially a hierarchical organization reflecting the current internet architecture

At the bottom left, there is a small logo, and at the bottom right, there is a small number '11'.

Naming: A large part of the address space is unassigned. This means, at this point of time people thought it prudent to keep provision for some future requirement which we cannot envisage at this moment. So a large part of **the** name space is simply been kept unassigned.

(Refer Slide Time: 14:55 -15:08)

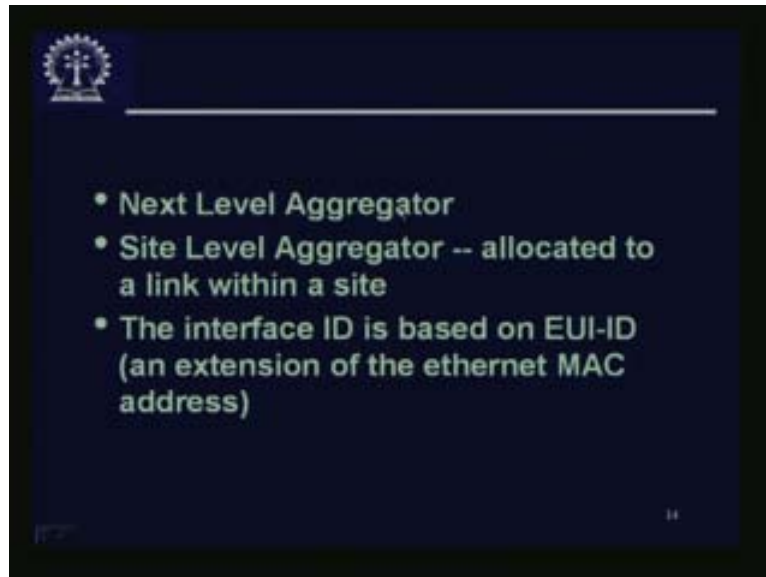


This slide is identical to the one above, featuring a dark blue background, a yellow title, and white bullet points. It includes the same circular logo in the top left and bottom left, and the number '11' in the bottom right.

There is a way now to move away from provider based routing, based ID's the two routing based ID's although both are possible. Previously what would happen is that the service provider would take a chunk of IP addresses and it is for his network. Now this could be distributed in various places. So, provider wise this loses the destination information. Whereas if you had done it geographically the routing would have been much easier, the routing table will also be smaller.

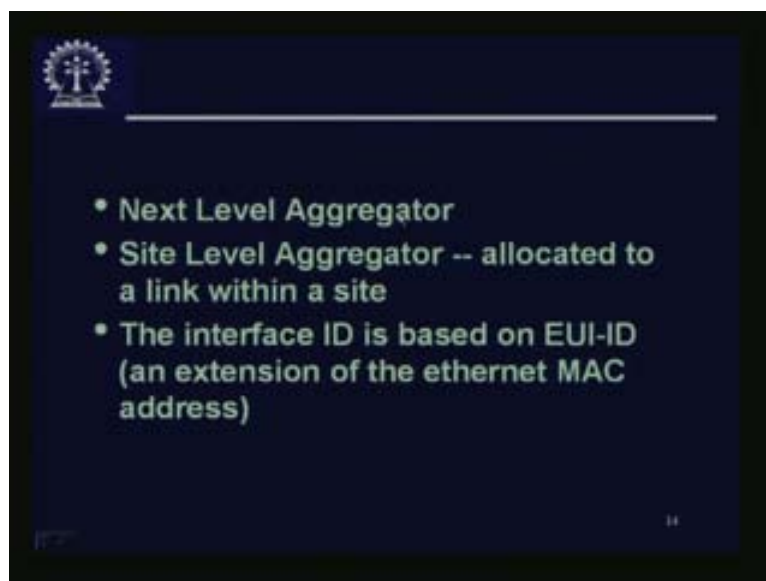
IPv6 keeps the option of both. So you can have provider based addresses and also geographic based addresses. There are various levels of aggregation like top-level aggregation which is essentially a hierarchical organization reflecting the current internet architecture.

(Refer Slide Time: 15:56 – 16:09)



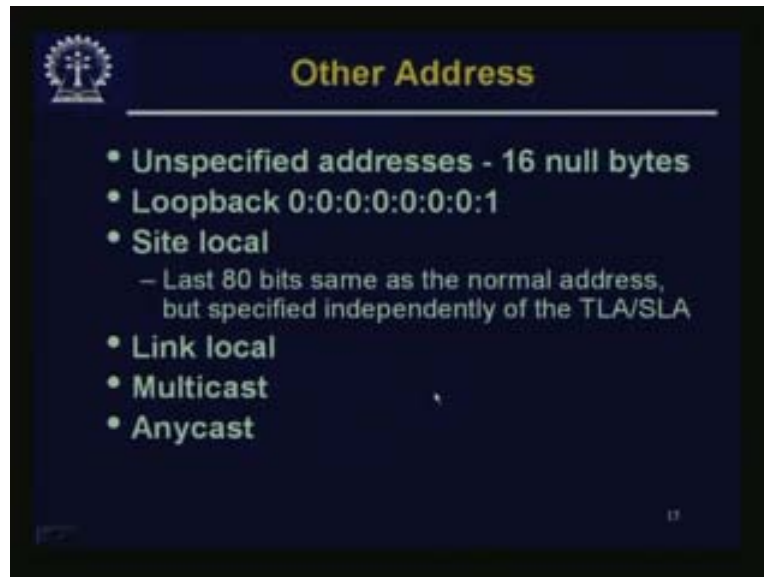
Then the Next Level Aggregator, then Site Level Aggregator allocated to a link or a link level or site level aggregator that is local. This means, at the link of the site level the rest of it may be common. It does not matter because it is strictly for local use that is something similar to a private IP and not for communication with others.

(Refer Slide Time: 16:15 - 16:20)



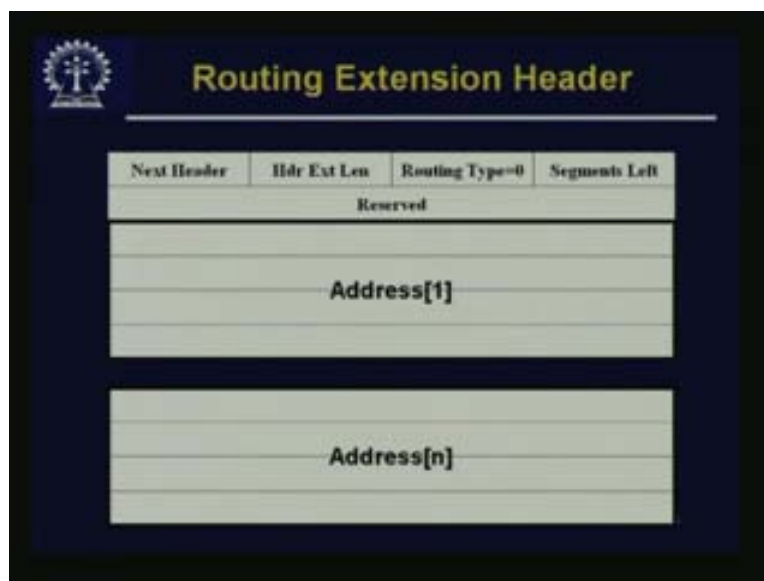
The interface ID is based on EUI ID, the extension of the Ethernet MAC address and even that can be embedded.

(Refer Slide Time: 16:29- 16:59)



There are some unspecified addresses. We need not bother about all this because IPv6 as of yet is not been deployed much. Only thing I would like to mention is about any cast. We have talked about Unicast, Broadcast and Multicast. Any cast is a concept something similar to multicast but in multicast there is a group where you can send some message to all the members of the group. In any cast you can send any message to any member of the group.

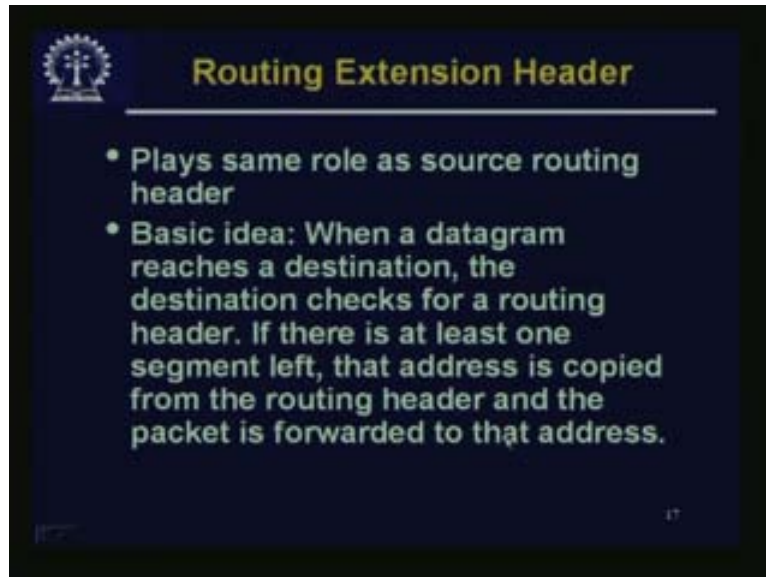
(Refer Slide Time: 17:15 – 17:41)





Let us look at some of the Routing Extension Headers. It has the next header, a Header length, a routing type etc. Now we have some address 1 to address n. There are some IP addresses, IPv6 addresses may be listed over here.

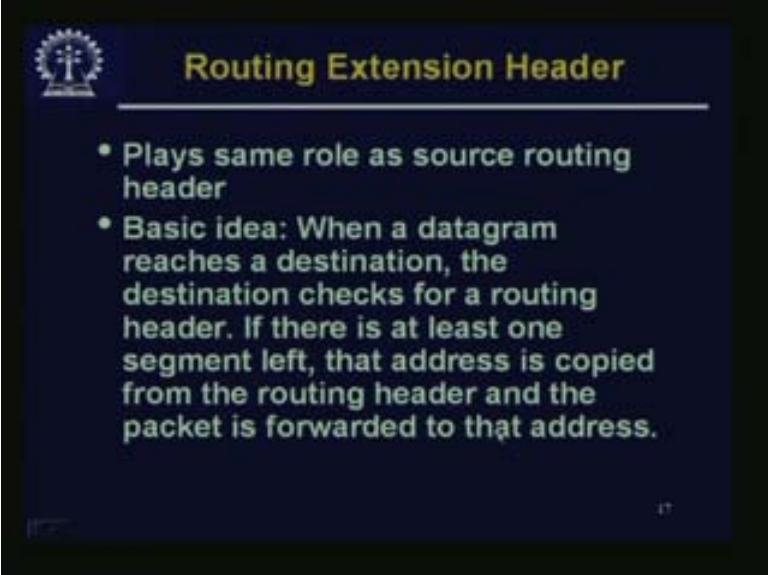
(Refer Slide Time: 17:42 – 17:55)



It plays the same role as source Routing Header. You remember that, in IPv4 options there is a way to give the routing from the source. That means you determine the routing from the source itself.. Such a facility is very important for protocols like BGP because BGP wants to dictate the route through which the packet should be routed. But the problem with IPv4 was that the Header length was very limited so you can go only up to a dozen or so may be 12 to 15 hops in the source routing. If it is beyond 12 to 15 hops you would run out of space in the header so you would not be able to specify that. Here you can have a routing header then you can have more than one routing header and this particular difficulty is obviated.



(Refer Slide Time: 18:42 – 18:54)



The slide features a dark blue background with a yellow title 'Routing Extension Header' at the top. To the left of the title is a small logo consisting of a gear with a cross inside. Below the title, there are two bullet points in white text. The slide number '17' is in the bottom right corner.

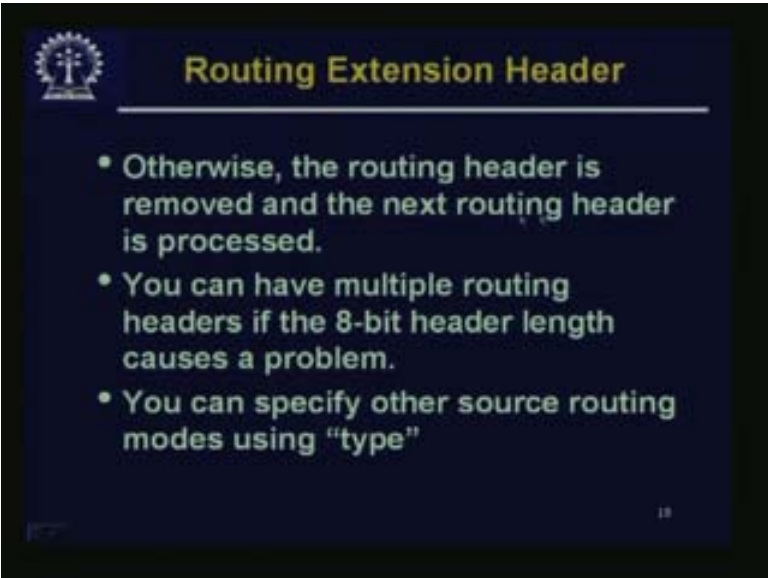
### Routing Extension Header

- Plays same role as source routing header
- Basic idea: When a datagram reaches a destination, the destination checks for a routing header. If there is at least one segment left, that address is copied from the routing header and the packet is forwarded to that address.

17

Basic idea is, when a datagram reaches a destination, the destination checks for a Routing Header. If there is at least one segment left, that address is copied from the routing header and the packet is forwarded to that address.

(Refer Slide Time: 18:55 – 19:17)



The slide features a dark blue background with a yellow title 'Routing Extension Header' at the top. To the left of the title is a small logo consisting of a gear with a cross inside. Below the title, there are three bullet points in white text. The slide number '18' is in the bottom right corner.

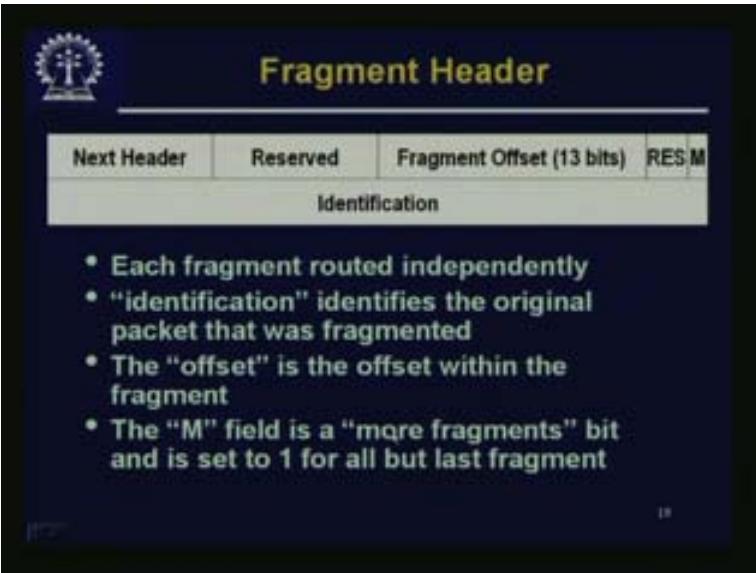
### Routing Extension Header

- Otherwise, the routing header is removed and the next routing header is processed.
- You can have multiple routing headers if the 8-bit header length causes a problem.
- You can specify other source routing modes using "type"

18

Otherwise, the routing header is removed and the next routing header is processed. You can have multiple routing headers if the 8-bit header length causes a problem. There is a Header length of 8-bits so you can go up to a length of 256 but then you can have multiple Routing Headers. You can specify other source routing nodes using type.

(Refer Slide Time: 19:18 – 19:46)



**Fragment Header**

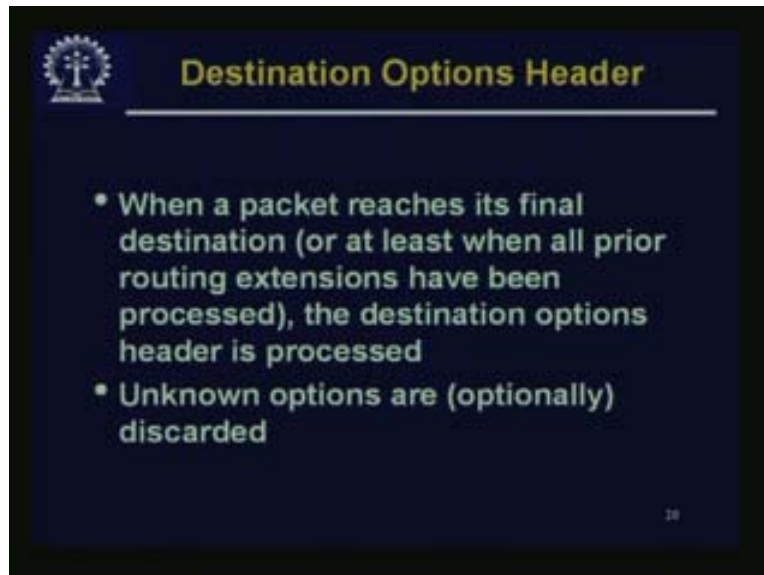
Next Header	Reserved	Fragment Offset (13 bits)	RES	M
Identification				

- Each fragment routed independently
- "identification" identifies the original packet that was fragmented
- The "offset" is the offset within the fragment
- The "M" field is a "more fragments" bit and is set to 1 for all but last fragment

19

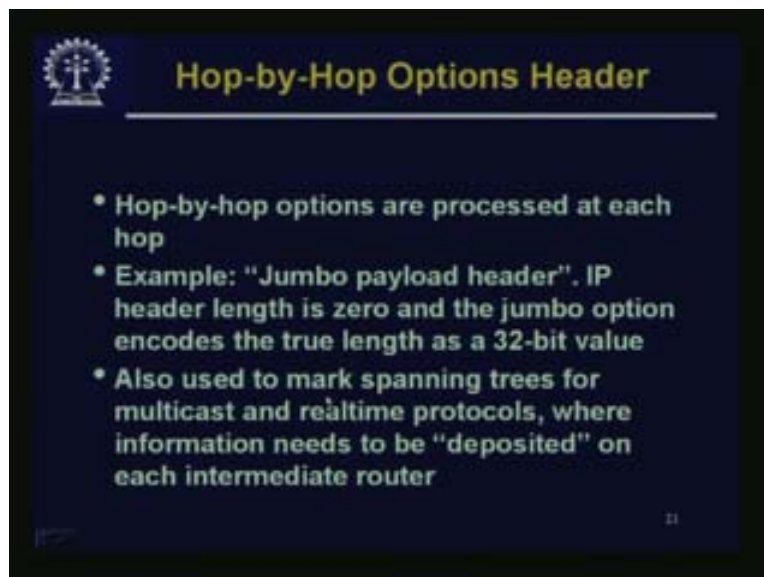
Fragment Header: Each Fragment routed independently. Identification identifies the original packet that was fragmented. The offset is the offset within the fragment. The M field is a more fragments bit **and** is set to one for all but last fragment. This is exactly similar to the way fragmentation was handled in IPv4. The difference over here is that the source sends it using the path MTU that means in the in between it is not fragmented and whatever fragmentation is done is done at the source and that information is carried in one header called Fragment Header. And those would need not fragment anything they will not use this header. So, all these extension headers are optional. You have to have the first IPv6 Header but all the extension headers are optional. Therefore, if you are not fragmenting then you will not use this header.

(Refer Slide Time: 20:23 – 20:39)



There is a Destination Options Header: When a packet reaches its final destination (or at least when all prior routing extensions are processed) the destination options header is processed. So, as an option the unknown options are discarded.

(Refer Slide Time: 20:40 – 21:23)



Hop-by-Hop Options Header: This is another one. The Destination Extension Header is looked at just at the end at the destination. In the hop-by-hop all these at intermediate hops you need to look at this hop-by-hop options header. They are processed at each hop, For example, the Jumbo payload header. The IP header length is 0 and the jumbo option encodes the true length as a 32-bit value. This is an option that you can have a very big packet traveling down. It is also used to

mark spanning trees for multicast and real time protocols etc. There may be things that you need to do at every hop.

(Refer Slide Time: 21:25 -21:56)

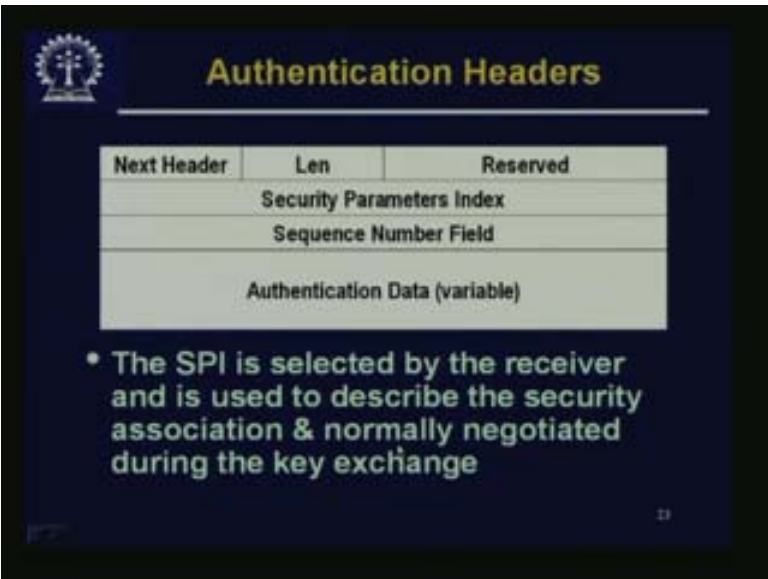


**Security Associations**

- **Authentication & encryption requires that senders and receivers agree on**
  - A key
  - An authentication or encryption algorithm
  - Set of ancillary parameters such as the lifetime of the key or details about the algorithm
- **This is a security association**

Security is another area that was in focus. Security Association: We will talk about network security etc at length later on. There is a way to put authentication and encryption requires that senders and receivers agree on a key for encryption and decryption. In addition, authentication or encryption algorithm, and set of ancillary parameters such as the lifetime etc. This is called security association.

(Refer Slide Time: 21:57 – 22:17)



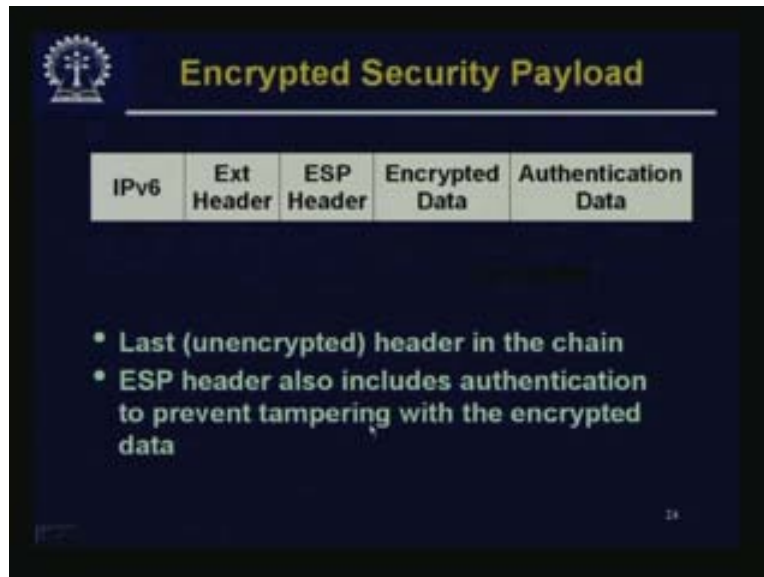
**Authentication Headers**

Next Header	Len	Reserved
Security Parameters Index		
Sequence Number Field		
Authentication Data (variable)		

- **The SPI is selected by the receiver and is used to describe the security association & normally negotiated during the key exchange**

Now, you have an Authentication Header where the security parameters may be mentioned namely the sequence number field, next Header, length and reserved. The SPI is selected by the receiver and is used to describe the security association where everything is normally negotiated during the key exchange.

(Refer Slide Time: 22:18 – 22:53)



There is Encrypted Security Payload. Headers entirely cannot be encrypted because then the intermediate routers will not be able to handle it. The last unencrypted header in the chain, this is an Encrypted Security so there would be encrypted data and authentication data, Also the ESP (Encrypted Security Payload) Header ESP header will be there. ESP Header also includes authentication to prevent tampering with encrypted data. We will talk in details about security in a later lecture.

To conclude this discussion about IPv6 this is really one scheme where people will not be running out of IP addresses. Then a funny thing happened in the sense that many of the hardware vendors like routers etc rather modified their design in order handle IPv6. However, actually what happened was that everybody is waiting for all others to switch from IPv4 to IPv6. When you switch you may have problems with some of your software or a lot of your software.

If you only switch over to the other version that would not do because the rest of the world will still go with IPv4. You can still operate it through some bridge, through an IPv4, IPv6 etc but then nobody wants to do it unless other people are doing it. That is how everybody is held back for quite a few years. But one thing is that if there are ubiquitous kind of networking, in the sense that, not only your computers but all your devices like refrigerator, TV and Air Conditioner and everything in the house is networked then we will require a huge number of network addresses. Then people will not have any option but to actually make the move.

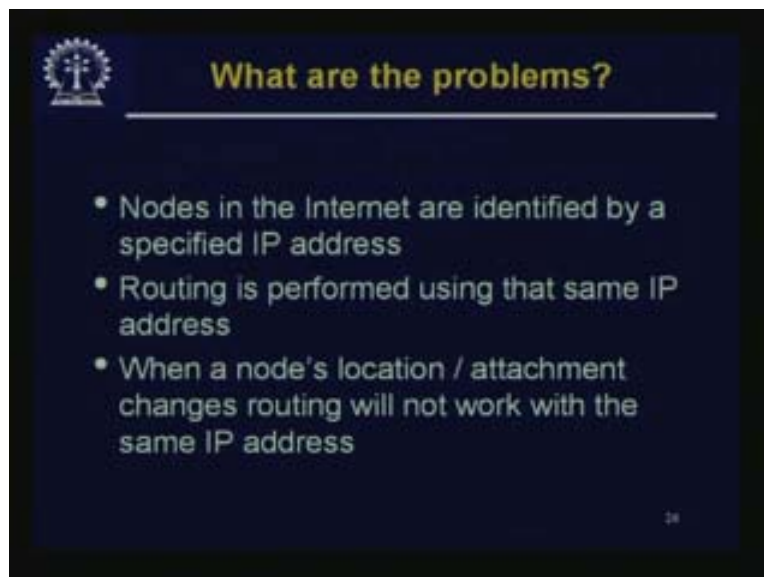
Right now everybody is sort of waiting for other people to make the move. Next, we will come to the topic of mobile IP. What is mobile IP? Mobile IP means, now there are many network

attachable devices. It is not only the laptop computers people are carrying everywhere. Even apart from laptop computers there can be all kinds of devices including hand held devices which can be connected to a network.

Now what is the problem if all these mobile devices are connected to the network? There is no problem as such, whenever you go there have to be some way in which a physical connection is made. That connection may be wireless in the case of mobile. The wireless connection is very attractive but otherwise you may go to some other place and actually connect a wire over there, it may be wired also, although wireless is more dominant but the trouble is what happens to the IP address? Your device has a particular IP address and that would have worked fine when you were at your home base. But you have moved from your home base to some other place.

Now, if somebody wants to talk to you he will be using your IP address and that is what he is familiar with. For example, all the name servers etc will have the IP address corresponding to the URL if you have a URL and that is not going to change. They are going to try to use your old IP address but by using your old IP address they will land in your home network where you are no longer available. This is the problem of mobile IP. When a particular network attached device moves from one network or one sub network to another network then how would you keep communicating? That is the problem of mobile IP.

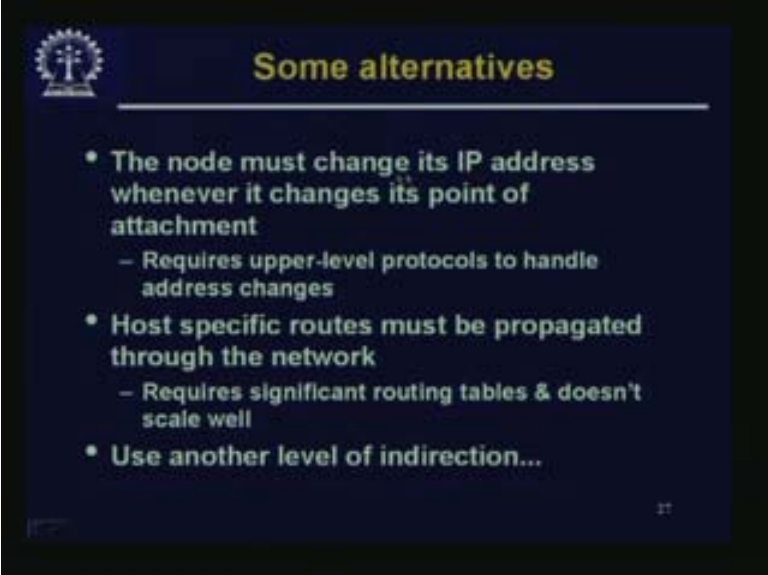
(Refer Slide Time: 25:36 – 26:59)



These are the problems as I just now discussed. Nodes in the Internet are identified by specified IP address. Routing is performed using that same IP address. When a node's location or attachment changes then routing will not work with the same IP address. That is a simple point.



(Refer Slide Time: 27:00 – 27:18)

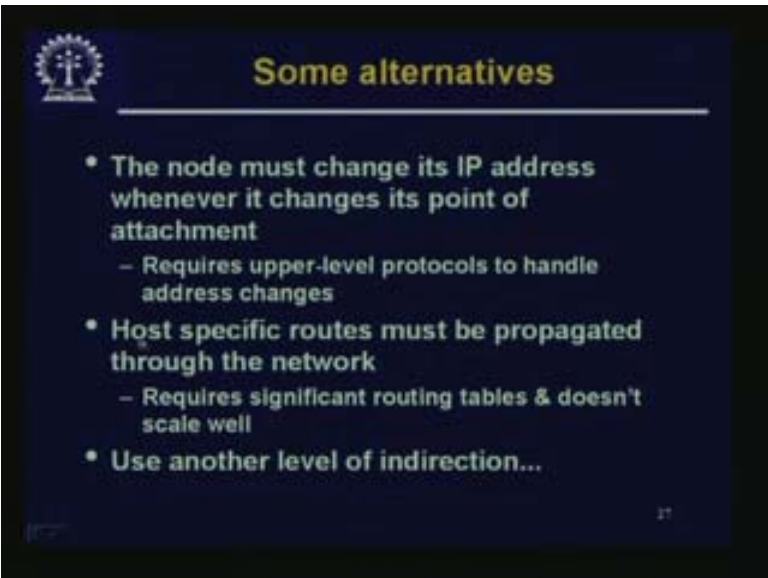


### Some alternatives

- The node must change its IP address whenever it changes its point of attachment
  - Requires upper-level protocols to handle address changes
- Host specific routes must be propagated through the network
  - Requires significant routing tables & doesn't scale well
- Use another level of indirection...

What are the alternatives? One is that, the node must change its IP address whenever it changes its point of attachment. It requires upper level protocols to handle address changes, that is one problem. This means, if it is to be made automatic then it has to be automated by a higher-level protocol which really sort of violates this layered architecture, that is one point. More importantly, what would happen is that the others who want to communicate with you know your IP address. They do not know that it has changed in the meanwhile so they would still try to communicate with the old IP address.

(Refer Slide Time: 27:43 – 28:54)



### Some alternatives

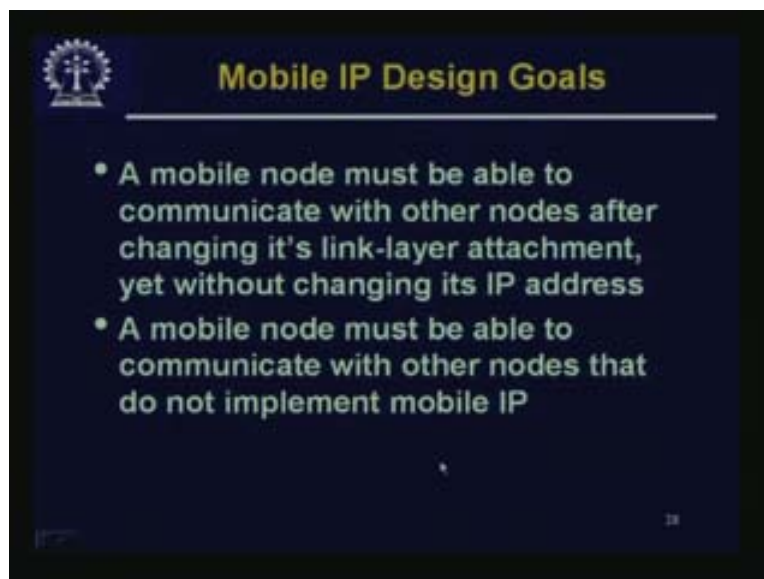
- The node must change its IP address whenever it changes its point of attachment
  - Requires upper-level protocols to handle address changes
- Host specific routes must be propagated through the network
  - Requires significant routing tables & doesn't scale well
- Use another level of indirection...



The other thing was that, Host specific routes must be propagated through the network. This is another possibility because from your IP address if somebody is trying to contact you from outside he first looks at the network part of the address and allows them into your network, then within the network, you have this ARP and other protocols to help you to get the MAC address and reach you directly. So the routing table essentially keeps track of all the networks as many as they can depending on what size the router is.

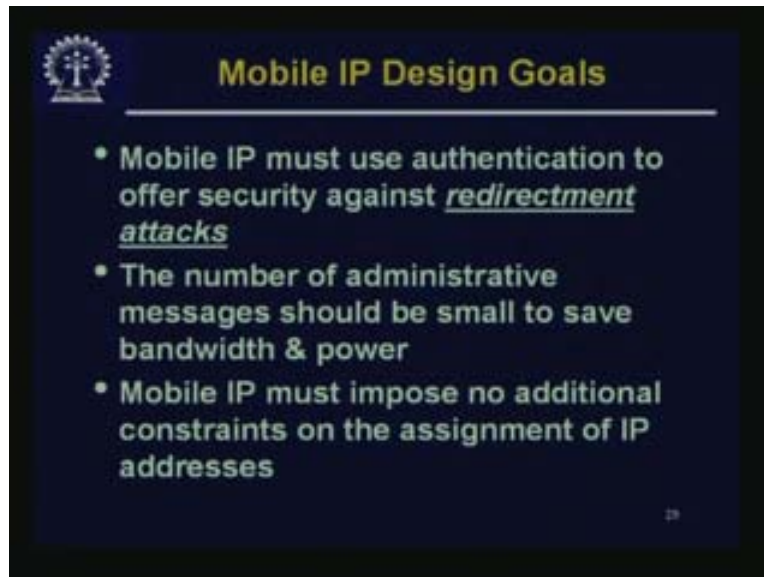
The big routers keep track of many networks, the small routers keep track of only a few network addresses. If these entries were against Host then the routers might dynamically change their entry etc and route it directly to that host. However, even handling so many millions of networks is becoming a problem so handling billions of hosts in the routers is simply out of question. The solution to this is to use another level of indirection and that is what we do in mobile IP as I have just now shown.

(Refer Slide Time: 28:55 – 29:00)



Mobile IP Design Goals: A mobile node must be able to communicate with other nodes after changing its link layer attachment. Changing its link layer attachment is changing the attachment to the network or sub network to which it was originally attached yet without changing its IP address where its IP address remains the same. This is the problem. A mobile node must be able to communicate with other nodes that do not implement mobile IP. This is the other requirement. It means, you may do something very sophisticated and special in your hand held device but the point is that still it should be able to communicate with millions of other hosts who do not have any special arrangement for communicating with mobile IP. Therefore, you cannot do anything on the other end.

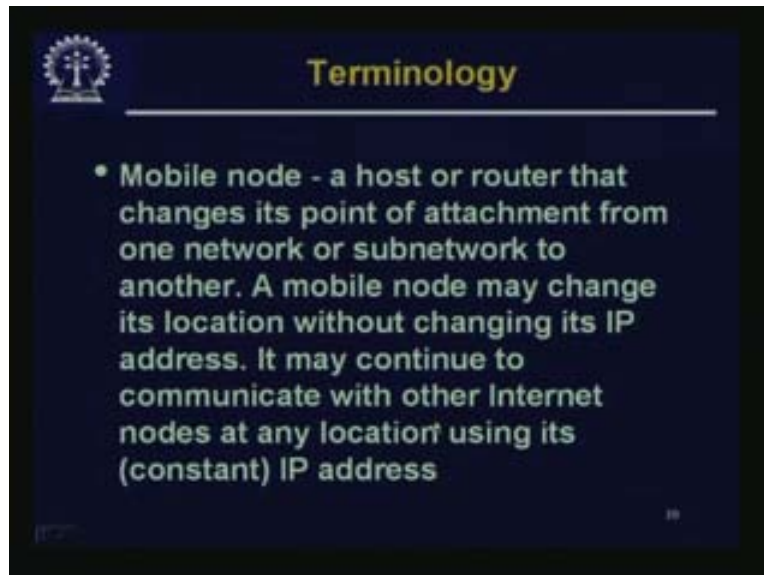
(Refer Slide Time: 29:49 - 31:39)



Another point is that, this is a sort of security concerned that mobile IP must use authentication to offer security against Redirectment Attacks. The point is, when you are in your own network you can try to authenticate it apart from any other security arrangement that is present like your password may be at a higher layer. But the point is that it is also possible that you allow communication with that particular host which is in that network, So you will set up your firewall or router policy in such a way that, that particular communication will be allowed, may be communication from others will not be allowed. But the point is, if this fellow has moved to another network then you will not be able to do it using the network address, that is one aspect.

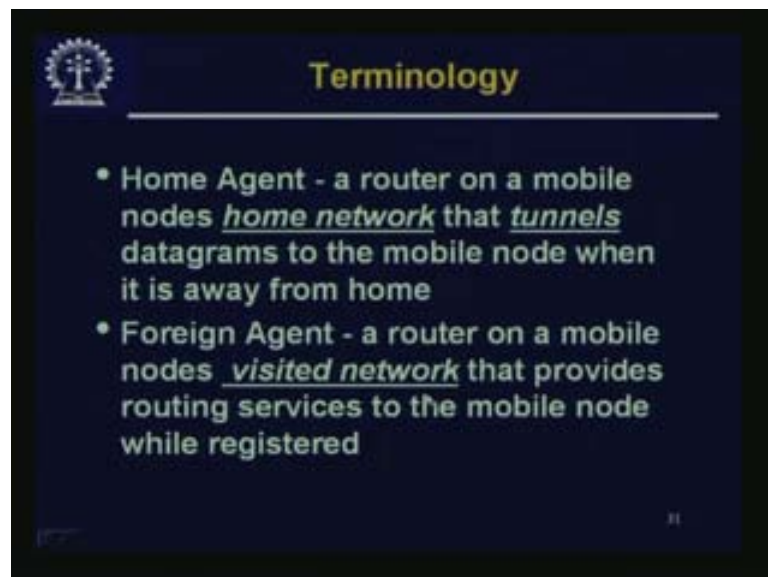
The other point is, other people may fake from other places. For example, suppose I want to communicate with Mr X, then Mr Y from some other place may rather try to spoof; in the sense, they may try to show that he is actually Mr X. So I will think that I am communicating with Mr X but actually I am communicating with Mr Y. Therefore, anything might happen and security concern is an issue. The number of administrative messages should be small to save bandwidth and power. You cannot have a huge overhead for doing this, Mobile IP must impose no additional constraints on the assignment of IP addresses, this is another important issue.

(Refer Slide Time: 29:49 - 32:09)



Before describing how this mobile IP is implemented, let us discuss about some Terminology. One is the Mobile node that is a host or router that changes its point of attachment from one network or sub network to another. A mobile node may change its location without changing its IP address. It may continue to communicate with other internet nodes at any location using its own constant IP address.

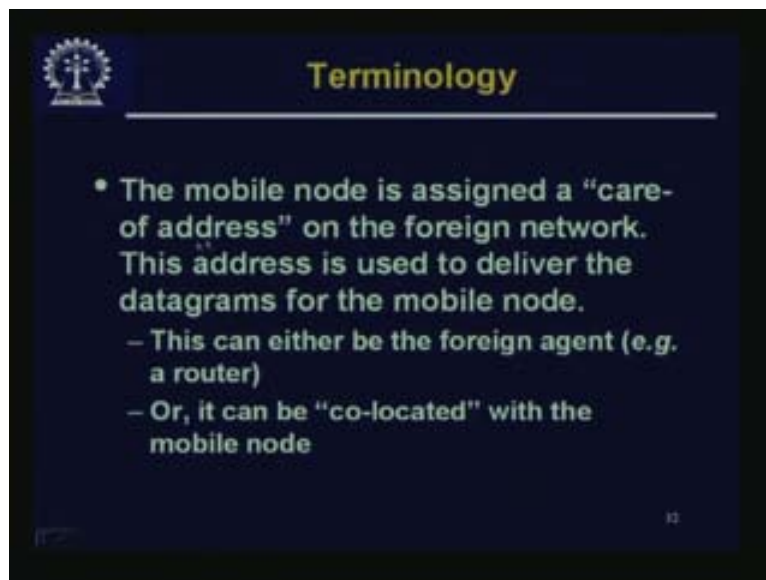
(Refer Slide Time: 32:09 - 32:42)



Home Agent: This is required in order to support mobile IP. Home Agent is a router on a mobile nodes home network that tunnels datagrams to the mobile node when it is away from home. You can immediately get the idea of how it is done. The point is that, this particular mobile device has

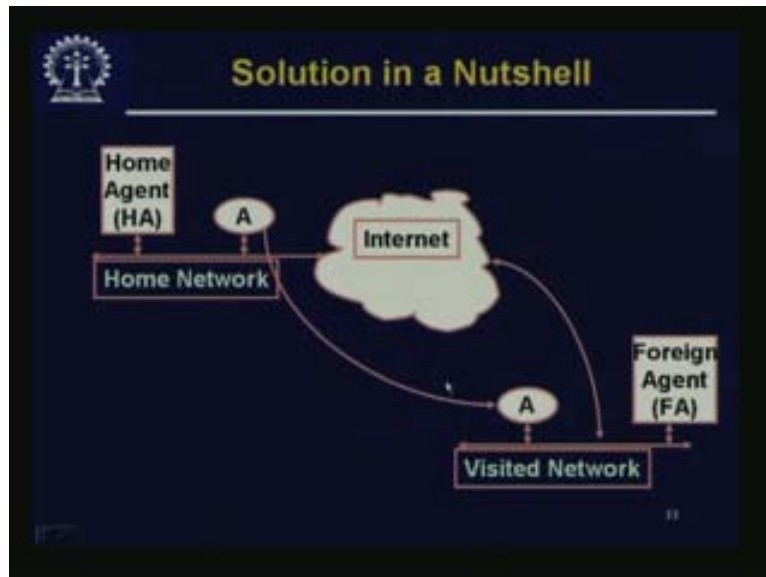
a home network and that home network has a router and that supports mobile IP. What that home network router would do is whatever communication is supposed to be received by this particular mobile device will come to its home network. The router will accept that communication on behalf of this mobile host that may now be away somewhere else. Then it would be the job of the router to send that communication back to that particular mobile host. Not only you require a home agent, that means, some router helping you and your home network, then you require a foreign agent. A router on a mobile nodes visited network means the network to which it is currently physically connected provides routing services to the mobile node while it is registered. For getting this service you must register with this foreign agent.

(Refer Slide Time: 32:43 - 34:13)



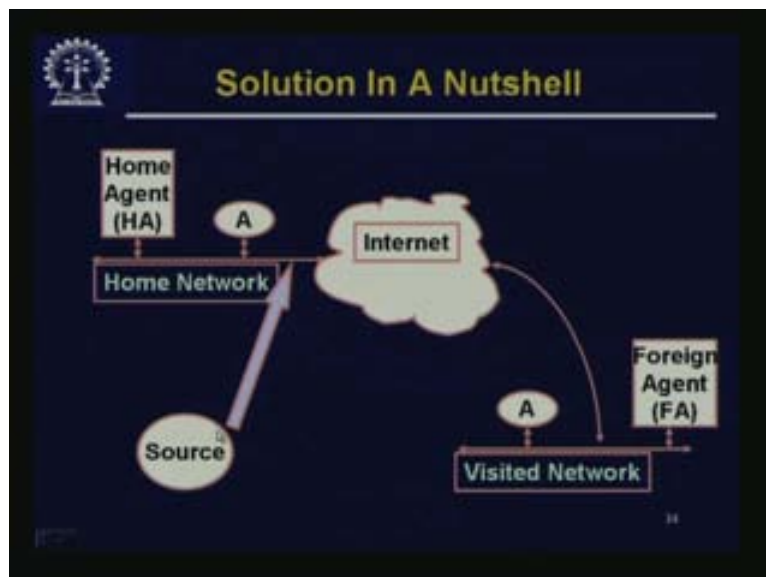
The mobile node is assigned a care of address. This is a new address. One is the mobile nodes own IP address which is remaining constant that actually belongs to the network in its home base. It also has a care of address on the foreign network. This address is used to deliver the datagrams for the mobile node. This address can either be the foreign agent where the Foreign Agents address may be this care of address or it can be co-located with the mobile node.

(Refer Slide Time: 34:13 to 34:50)



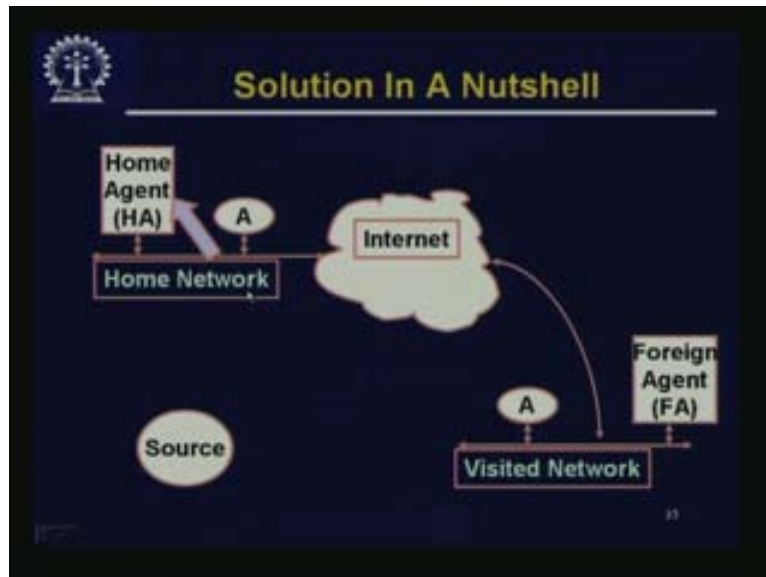
This is the idea you have, this is the home network of the device of A. Now A has moved to another network so this is the visited network of A. In the home network A has a home agent which will help you in this mobile communication. In the visited network it looks for and finds a foreign agent that will help you for this communication. This foreign agent will give that care of address and then both of them will be connected to the internet.

(Refer Slide Time: 34:51 - 35:00)



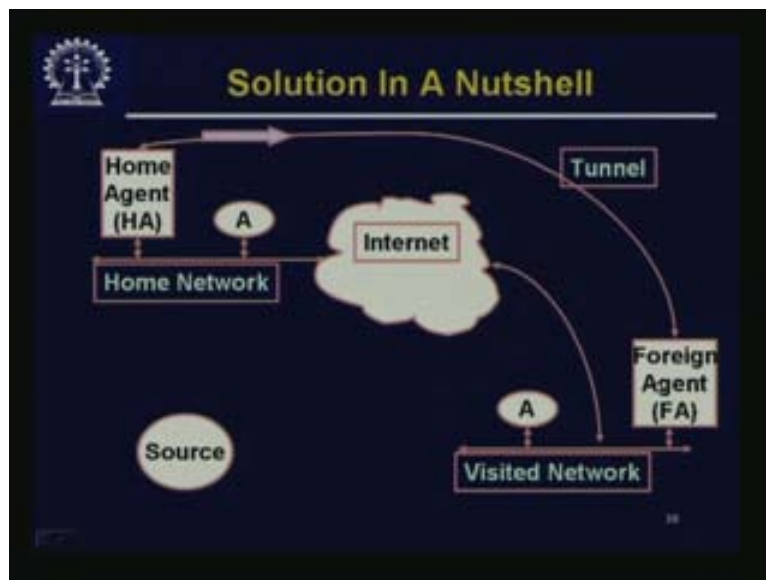
Suppose some source wants to send something to A, naturally it will use A's original IP address so it will be routed to the home network of A.

(Refer Slide Time: 35:01 - 35:15)



What will happen is that then the home network will send it to the home agent. The home agent knows that A is no longer here but it is somewhere else and the home agent also knows the care of address given by the foreign agent.

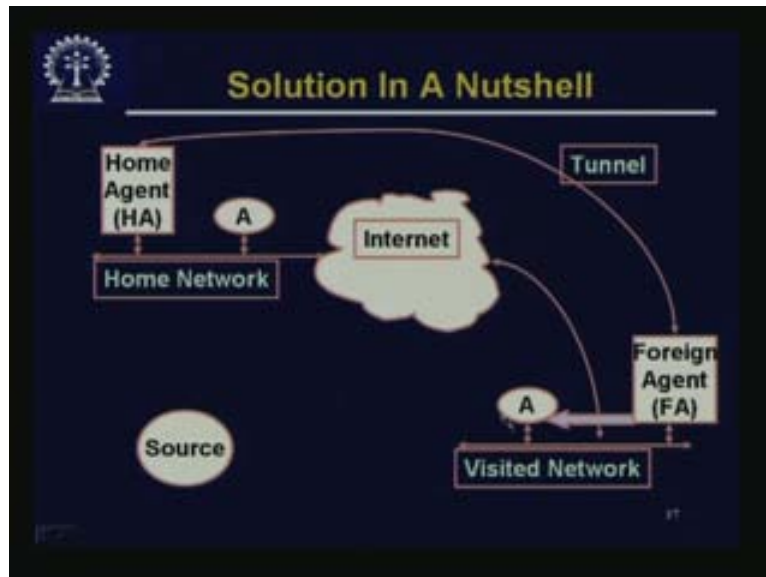
(Refer Slide Time: 35:16 - 35:25)



He tunnels the communication to the foreign agent using the care of address.

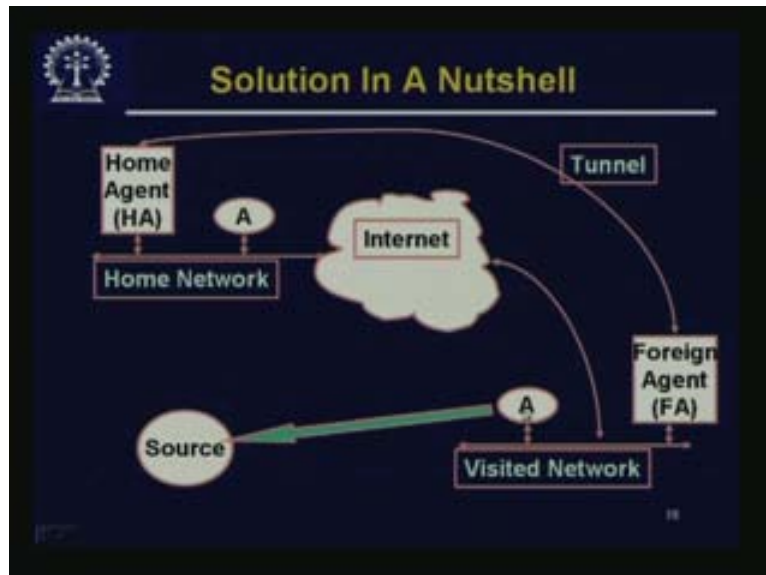


(Refer Slide Time: 35:26 - 35:33)



Then the foreign agent will deliver the message to A because foreign agent knows the A's current location, MAC address etc where it can communicate.

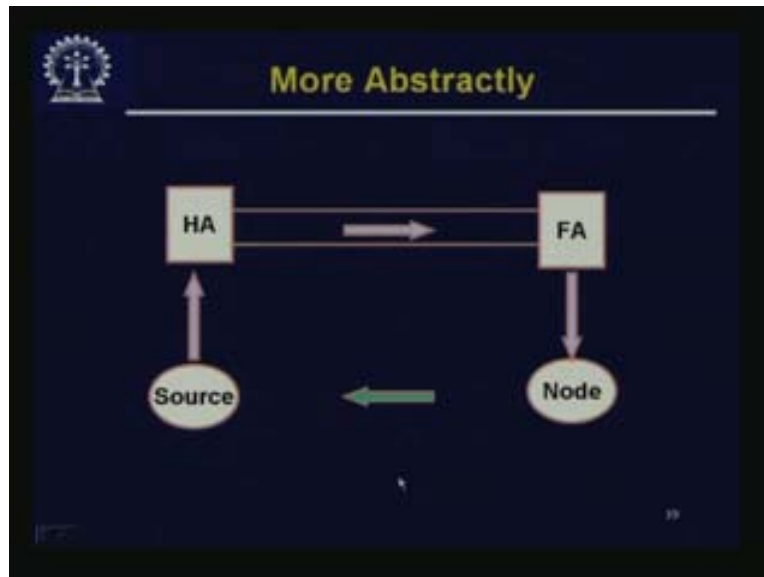
(Refer Slide Time: 35:34 - 35:52)



Now **A** replies to C but this can go straight. This need not go in the circuitous manner because he is using the IP address of the source of the original communication so A can send this reply directly back to the source. Hence, this need not go through the entire process.

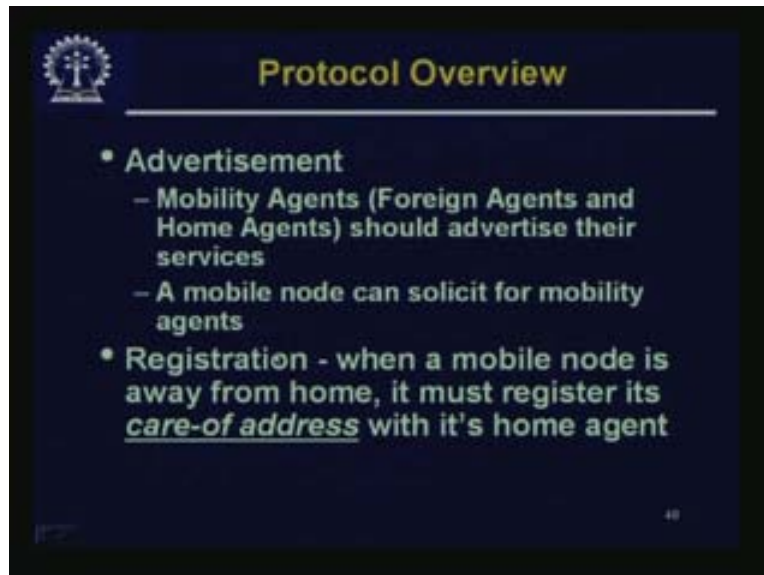


(Refer Slide Time: 35:52 - 36:05)



This is the solution in a nutshell, From the source, it goes to the home agent, to the foreign agent, to the node and from the node it directly goes back to the source for the return communication.

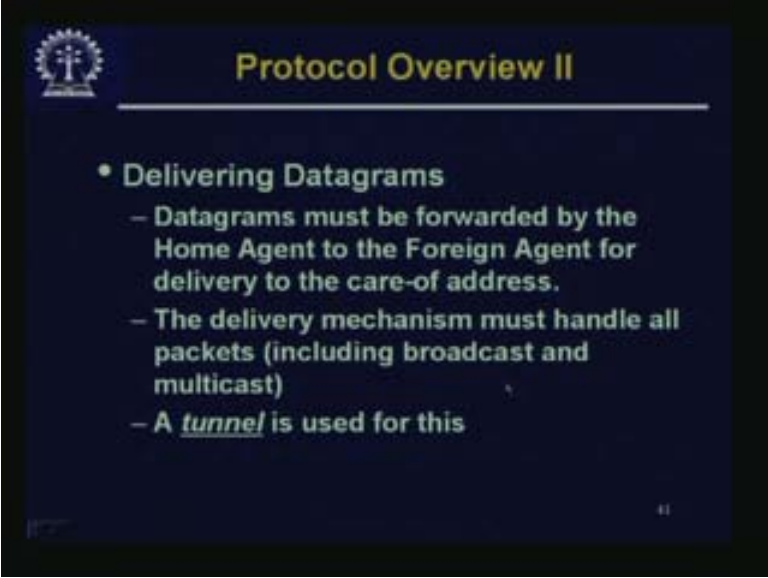
(Refer Slide Time: 36:05 - 37:06)



A small overview of the Protocol, you have advertisement. That means the mobile agents the so-called foreign agents and home agents should advertise their services. That means the mobile node comes to know that this foreign agent **or** home agent is available, that this service is available. Otherwise, a mobile node can also solicit for mobility agents and that is possible. Registration: When a mobile node is away from home it must register its care of address with its home agent. So, not only it must set up some arrangement with the foreign agent to give it an

address but also that address has to be sent to the home agent so that, whatever the home agent tunnels it will tunnel it straight to that care of address.

(Refer Slide Time: 37:06 - 37:23)



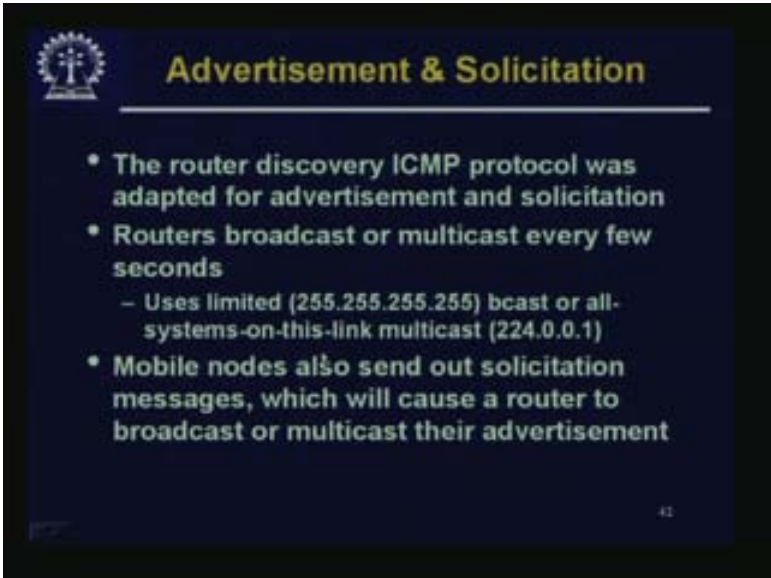
The slide is titled "Protocol Overview II" in yellow text on a dark blue background. It features a small logo in the top left corner. The main content is a bulleted list in white text. The first bullet point is "Delivering Datagrams". The second bullet point is "Datagrams must be forwarded by the Home Agent to the Foreign Agent for delivery to the care-of address." The third bullet point is "The delivery mechanism must handle all packets (including broadcast and multicast)". The fourth bullet point is "A tunnel is used for this". The slide number "41" is in the bottom right corner.

## Protocol Overview II

- Delivering Datagrams
  - Datagrams must be forwarded by the Home Agent to the Foreign Agent for delivery to the care-of address.
  - The delivery mechanism must handle all packets (including broadcast and multicast)
  - A tunnel is used for this

Delivering Datagrams: Datagrams must be forwarded by the home agent to the foreign agent for delivery to the care-of address. The delivery mechanism must handle all packets including broadcast and multicast. A tunnel is used for this analogy. In a little while, let us see what a tunnel means.

(Refer Slide Time: 37:23 - 38:05)



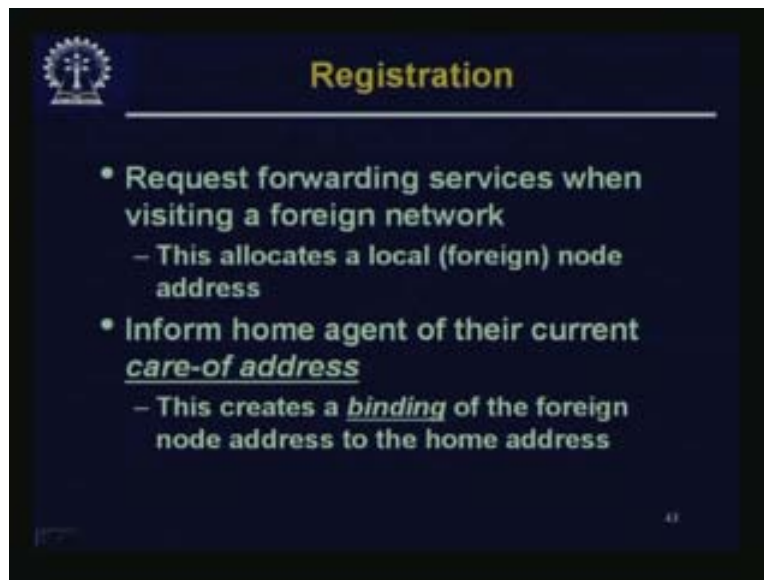
The slide is titled "Advertisement & Solicitation" in yellow text on a dark blue background. It features a small logo in the top left corner. The main content is a bulleted list in white text. The first bullet point is "The router discovery ICMP protocol was adapted for advertisement and solicitation". The second bullet point is "Routers broadcast or multicast every few seconds". The third bullet point is "Uses limited (255.255.255.255) bcast or all-systems-on-this-link multicast (224.0.0.1)". The fourth bullet point is "Mobile nodes also send out solicitation messages, which will cause a router to broadcast or multicast their advertisement". The slide number "42" is in the bottom right corner.

## Advertisement & Solicitation

- The router discovery ICMP protocol was adapted for advertisement and solicitation
- Routers broadcast or multicast every few seconds
  - Uses limited (255.255.255.255) bcast or all-systems-on-this-link multicast (224.0.0.1)
- Mobile nodes also send out solicitation messages, which will cause a router to broadcast or multicast their advertisement

Advertisement and Solicitation: The router discovery ICMP protocol was adapted for advertisement and solicitation so not much of a change was required. We will look at the details of ICMP protocol later. The routers broadcast or multicast every few seconds. So it uses limited broadcast or all systems on this link, multicast kind of an address for giving this because they cannot use the IP address directly because it is an advertisement. Mobile nodes also send out solicitation messages that will cause a router to broadcast or multicast their advertisement.

(Refer Slide Time: 38:05 - 38:39)



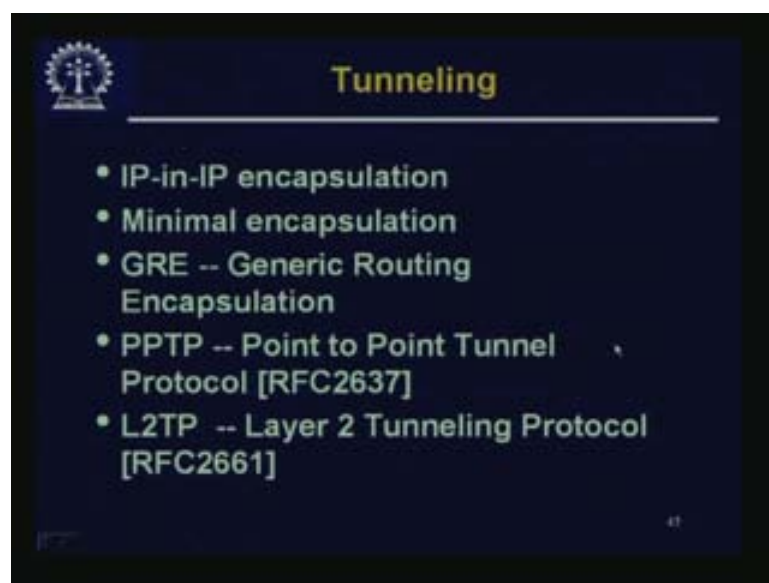
Registration: Request forwarding services when visiting a foreign network. This allocates a local foreign node address. That means a care **of** address is required. Inform home agent of their current care of address. This creates a binding of the foreign node address to the home address in the home agent. If anything comes destined for the original home address then this can be tunneled to the care of address.

(Refer Slide Time: 38:05 - 39:16)



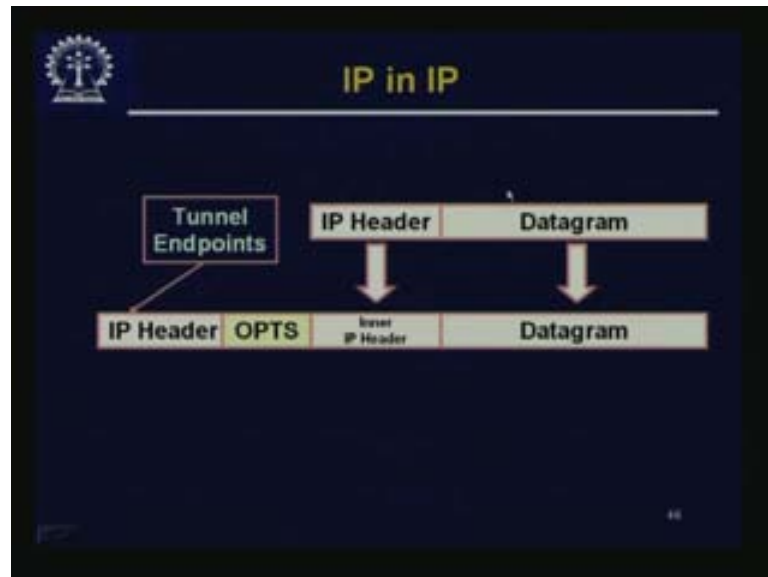
This is one small but important point that this binding has to be renewed from time to time. Bindings have lifetimes. This is important because mobile node may be rude and just go away without informing anybody and that registration will rather last forever, it cannot last forever. It is best that it dies down after sometime. If the mobile agent continues in the same location for more time, it is going to renew this binding from time to time. And of course you have to deregister when they return home.

(Refer Slide Time: 39:16 - 39:26)



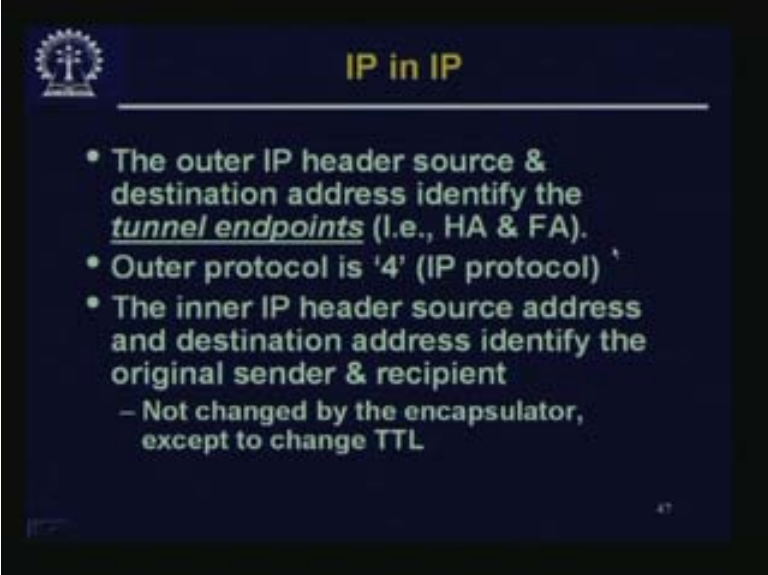
Tunneling: There are various methods of tunneling. We will just discuss this IP-in-IP encapsulation and minimal encapsulation.

(Refer Slide Time: 39:16 - 39:26)



This is IP-in-IP: This was the original message sent from the source and this is what landed in the home network of the destination. If you remember, in the diagram the destination was marked as A. This IP header will contain the actual address of A and this is the datagram. What it does is, when it lands into the home agent the home agent knows that this has to be sent somewhere else. It keeps the inner IP header and datagram intact. This whole thing is considered now as a payload and then you add another IP header with some options if necessary. This IP header will have as its destination the tunnel endpoints, the tunnel destinations which is supposed to be the care of address. In the packet the original packet is still there, this inner IP header and the datagram etc and this whole thing is encapsulated as if this is a payload and sent to the foreign network in the care of address. It will reach the foreign agent and the foreign agent will then send this part to the mobile node who is currently connected and its MAC address is known to the foreign agent. The mobile agent or the mobile node will receive a whole packet including this inner IP header. So you do not require any kind of change in the software which handles it just like a normal packet. It is as if he was in the home network and got this is original packet.

(Refer Slide Time: 41:15 - 41:50)

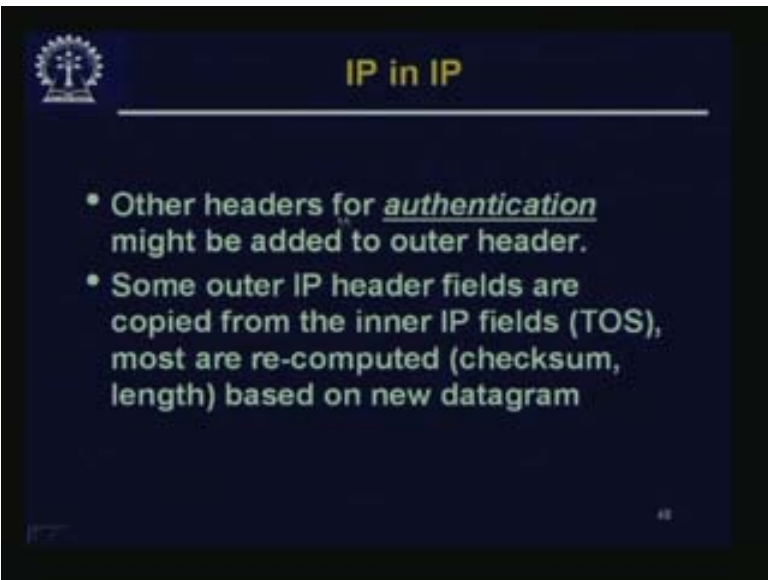


The slide is titled "IP in IP" in yellow text at the top center. In the top left corner, there is a logo of a gear with a cross inside. The slide has a dark blue background with white text. It contains a bulleted list of three points. The first point states that the outer IP header source and destination addresses identify the tunnel endpoints (HA & FA). The second point states that the outer protocol is '4' (IP protocol). The third point states that the inner IP header source and destination addresses identify the original sender and recipient, with a sub-bullet indicating that these are not changed by the encapsulator except to change the TTL. The slide number "47" is in the bottom right corner.

- The outer IP header source & destination address identify the tunnel endpoints (i.e., HA & FA).
- Outer protocol is '4' (IP protocol)
- The inner IP header source address and destination address identify the original sender & recipient
  - Not changed by the encapsulator, except to change TTL

The outer IP header source and destination address identify the tunnel endpoints. The source would be the home agent and the destination would be the foreign agent. The outer protocol is 4 that is the IP protocol. The inner IP header, the source address and destination address identify the original sender and recipient, this is not changed by the encapsulator except to change the time to live. So for time to live you have to look at the TTL and then make the necessary changes. This whole thing is put in the payload.

(Refer Slide Time: 41:51 - 42:16)



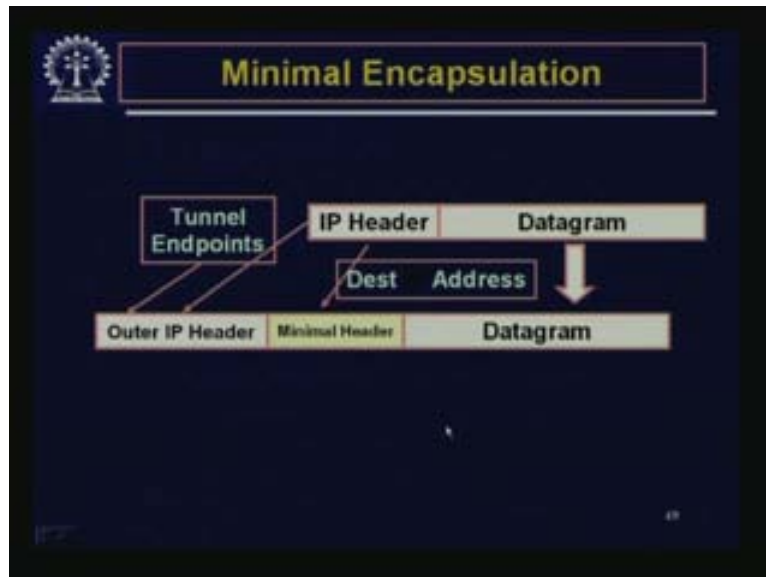
The slide is titled "IP in IP" in yellow text at the top center. In the top left corner, there is a logo of a gear with a cross inside. The slide has a dark blue background with white text. It contains a bulleted list of two points. The first point states that other headers for authentication might be added to the outer header. The second point states that some outer IP header fields are copied from the inner IP fields (TOS), most are re-computed (checksum, length) based on the new datagram. The slide number "48" is in the bottom right corner.

- Other headers for authentication might be added to outer header.
- Some outer IP header fields are copied from the inner IP fields (TOS), most are re-computed (checksum, length) based on new datagram

Other headers for authentication might be added to the outer header in order to handle all these security concerns. Some outer IP header fields are copied from the inner IP fields. For example,

type of service etc most are recomputed like checksum length etc may change based on the new datagram.

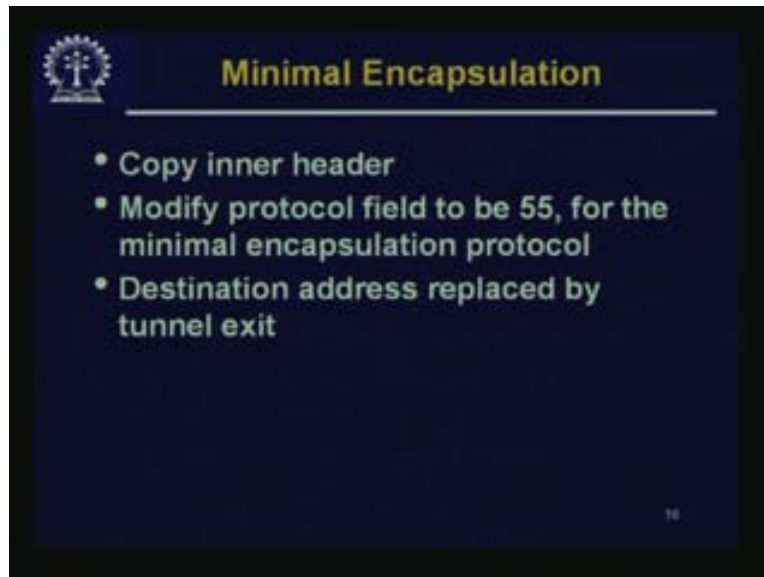
(Refer Slide Time: 42:17 - 43:09)



The other option is the minimal encapsulation. Minimal encapsulation means that you do not keep the entire IP header intact here. So, what you want to do is that, you want to retain the minimal information in the minimal header and then construct an outer IP header. For the outer IP header the tunnel endpoints as the source and destination address would still be there and some of the stuff from the IP header will come here. The destination address will be there in the minimal header. You have to make some deconstruction and reconstruction at both places. The size is a bit smaller so the overhead may be a bit smaller but it may not be such a big deal.

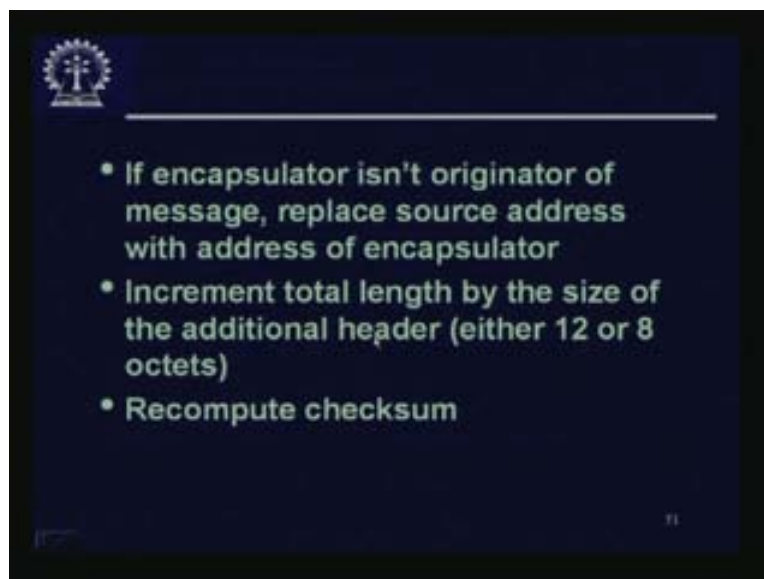


(Refer Slide Time: 43:10 - 43:30)



In Minimal Encapsulation, we copy inner header. Modify protocol field to be 55 for the minimal encapsulation protocol because on the other side it must know which protocol it is following. If it is following minimal encapsulation then it has to do something. Destination address is replaced by the tunnel exit.

(Refer Slide Time: 43:31 - 43:50)



If encapsulator is not the originator of message, replace source address with address of encapsulator. Then increment total length by the size of the additional header by 12 or 8 octets and then re-compute the checksum. This is called mobile IP in one way in which mobility can be

handled and your IP address can be recomputed. There are other possibilities and other ways of handling mobility.

For example, this has an overhead that any communication from the source to the intended host that has moved, now has to go through this triangular path. Will it continue to do so or whether after first communication there would be some protocol to exchange their new IP addresses etc? Then, they can communicate directly, that would avoid this triangular path. The other problems with triangular path may be apart from higher overhead. It may exceed the hop limit, as networks are **growing** it may increase the hop limit and you may never reach whereas if it had gone directly then it would have reached.

Other options could be just like you do handoffs in cellular from one base station to another. In the case of cellular networks what is happening is that, you are always in connection with some base station, may be even more than one base station. If you are moving away from one **base** station when the signal strength drops then it goes to the realm of another base station, and the other base station automatically picks up and does some kind of registration. When this is done, the communication remains direct. But, if you want to change the IP address in such a dynamic fashion then there has to be an integrated system running everywhere which is using this protocol. Mobile IP is a way of handling mobility with minimal change to others and the problem is that this has a significant overhead. In the next class we will be moving into the next higher layer which is the Transport Layer the TCP and UDP, thank you.