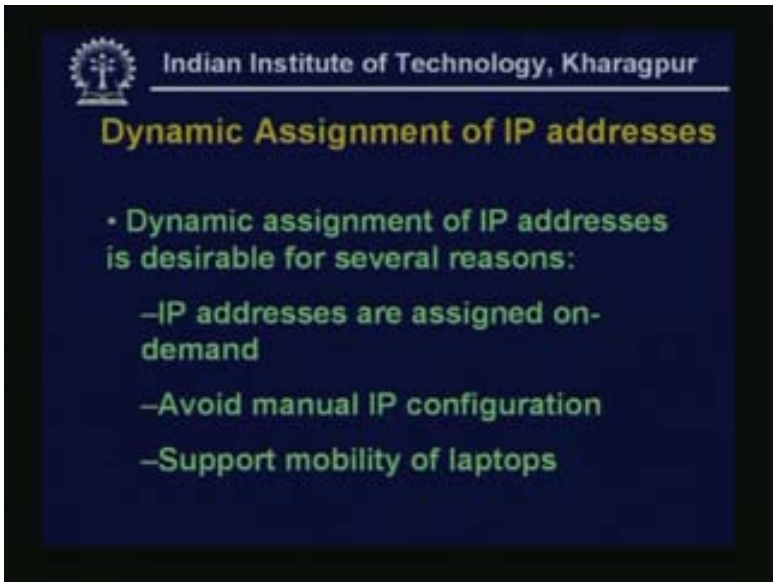
Computer Networks
Prof. S. Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture 33
DHCP AND ICMP

Good day. Today we shall talk about some protocols which are useful for controlling the network and also in keeping machines connected to the network. Specifically under the broadcast we will talk about DHCP and ICMP. There are some protocols associated with this so we shall discuss about it. DHCP is Dynamic Host Configuration Protocol. It is about configuring a host, configuring a machine may be a PC or some computers connected to the network.

(Refer Slide Time: 1:35-3:29)

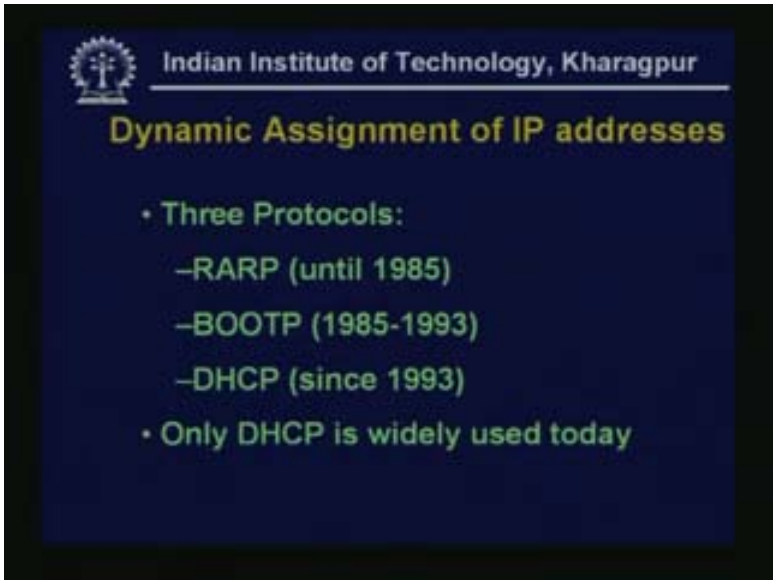


The chief motivation came from the dynamic assignment of IP addresses. The dynamic assignment of IP addresses is desirable for several reasons:
IP addresses can be assigned on demand.
For example, when you have a scarcity for real IP addresses then you keep a central pool of IP addresses and then as some computer comes on line it assigns an IP address from the pool and when it goes out those IP addresses are withdrawn and are given to some other machines.

Another place where it may be required is, suppose you have some kind of a RAS or Remote Access Server to which a number of machines should be connected via dial up connections then in that case you give them a temporary IP address for the connection. Now if somebody wants to visit some network with a laptop then they have to get a network address of that particular network therefore that network address has to be dynamically assigned.

IP addresses are assigned on demand.
It avoids manual IP configuration which is prone to errors.
It also supports mobility of laptops.

(Refer Slide Time: 3:30-3:59)

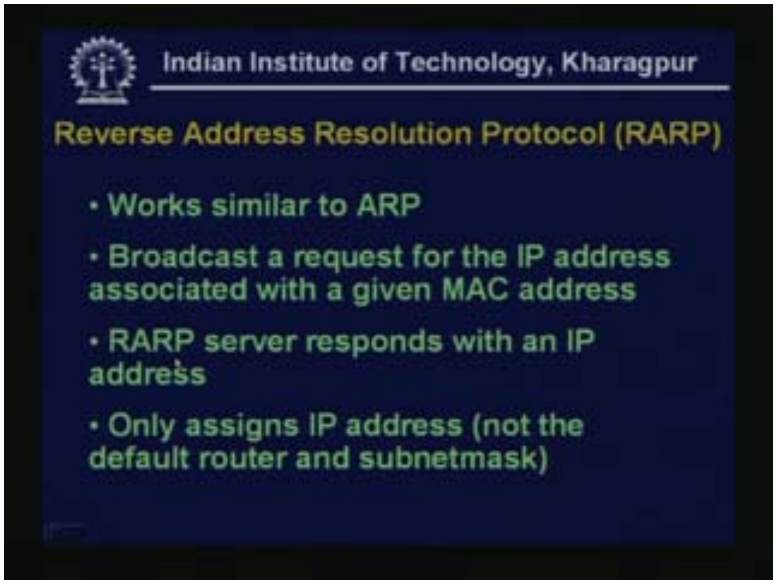


Dynamic assignment of IP addresses is done using three different protocols.

1. RARP: It was widely used up to 1985 and even beyond this period people kept using it.
2. BOOTP: Bootstrap protocol was used until 1993
3. DHCP: Is used after 1993 and currently this is in wide usage.

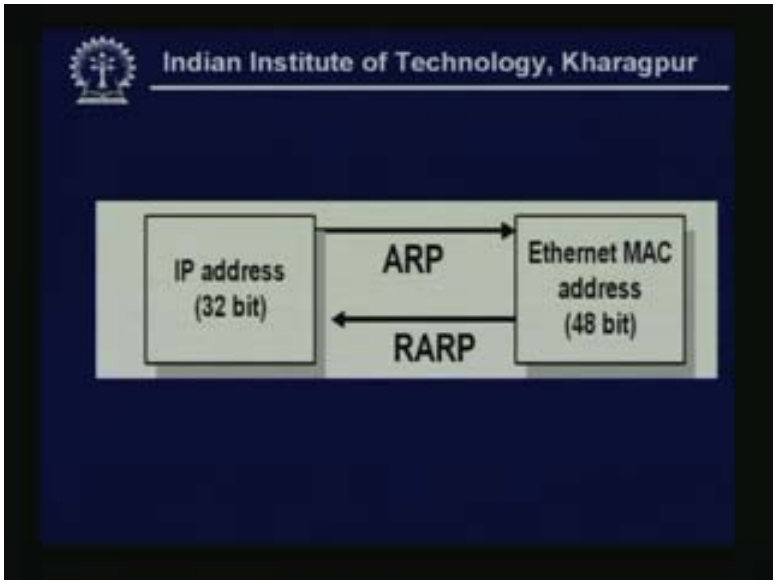
A Bootp client can also use DHCP server.

(Refer Slide Time: 4:08-5:33)



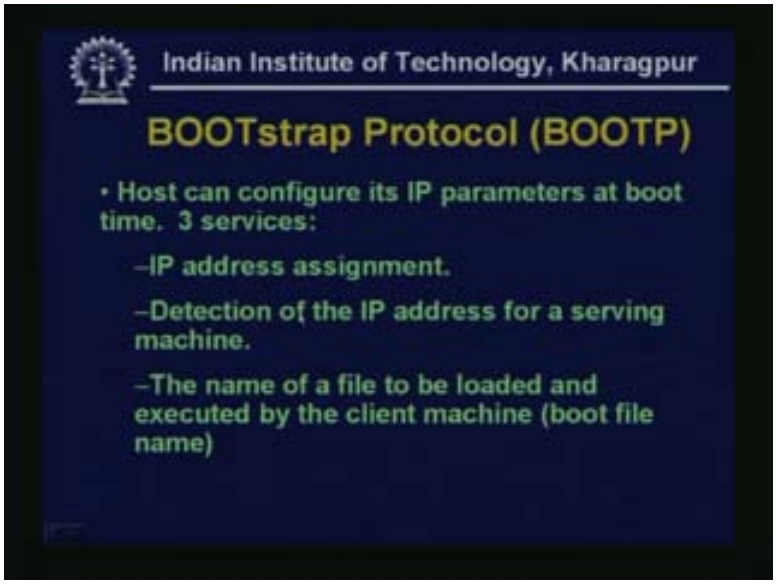
RARP is actually the reverse ARP Address Resolution Protocol. The problem is, given an IP address what is the MAC address. This is for mapping between the IP addresses and the MAC addresses. Finding the MAC address for the IP address is useful when you want to communicate over a LAN. RARP is the reverse of this. Given a MAC address, RARP finds IP address. This would be necessary in case you have something like disclosed work station which boosts the signal over the network. A disclosed work station has its own MAC address and it wants to get an IP address assigned. This is where RARP is typically used. RARP is used to broadcast a request for IP address associated with a given MAC address. RAP server responds with an IP address. It only assigns IP address and not the default router, subnet masks etc that are required and they are not a part of this server.

(Refer Slide Time: 5:34-5:46)



So IP address to MAC address is the ARP and Ethernet MAC address to IP address is the RRAP.

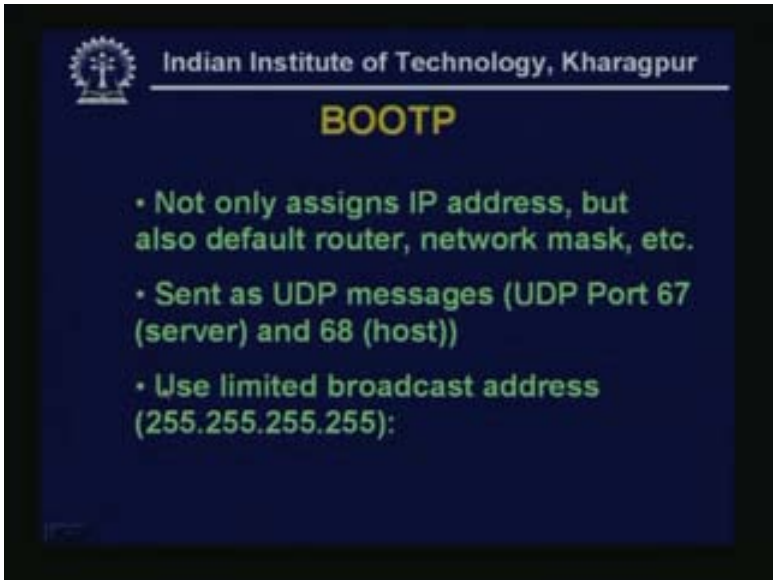
(Refer Slide Time: 5:45-6:39)



Let us see the improved version of RARP i.e. BOOTP.
BOOTP not only assigns IP addresses dynamically but also has some more functions. Host can configure IP parameters at boot time. Basically there are three services:
IP address assignment
Detection of the IP address for a serving machine

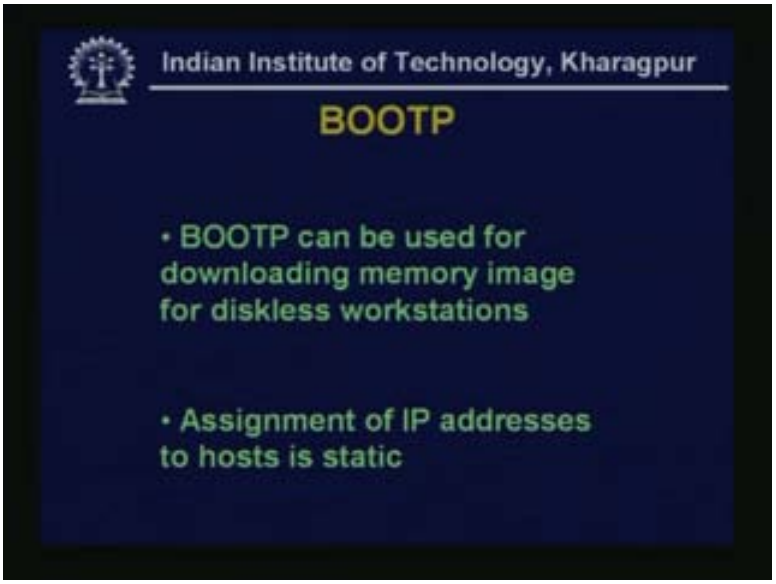
The name of the file to be loaded and executed by the client machine i.e. the boot file name This is the source from which it gets the name bootstrap protocol i.e. when the machine is booting up it not only gets an IP address but also gets the name of the file which can be loaded and executed. This is the bootstrap protocol or BOOTP.

(Refer Slide Time: 6:40-7:37)



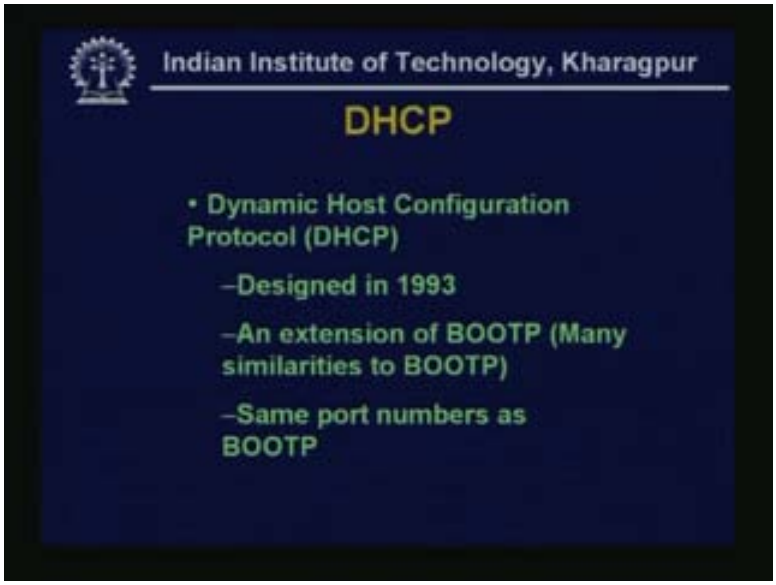
BOOTP not only assigns IP address but also default router, network mask, etc. Therefore whatever that particular machine requires for communication namely the addresses such as network, subnet mask, gateway etc are given by the BOOTP protocol. This is sent as an UDP message. So UDP port 67 is for server and UDP port 68 is for the host. Port 68 for host is required when you may want to find out a machine from bootstrap protocol which is already available on the network. And use limited broadcast address that is 255. 255. 255. 255. If you recall from our discussion about addresses this is a broadcast address where the broadcast is limited to this particular subnet or network.

(Refer Slide Time: 7:51-8:14)



BOOTP can be used for downloading memory image for diskless workstations. So whatever was the motivation for RARP the same thing can be done through BOOTP also. But assignment of IP address to hosts is static. This is one sort of drawback of BOOTP.

(Refer Slide Time: 8:16-8:52)



To make it dynamic we go to the dynamic host configuration protocol which is standard now and more versatile than RARP and BOOTP. It can do a lot of things apart from just giving the IP address. This was designed in 1993 as an extension of BOOTP with many similarities to BOOTP and same port numbers as BOOTP. That is why DHCP server can handle a few BOOTP clients.

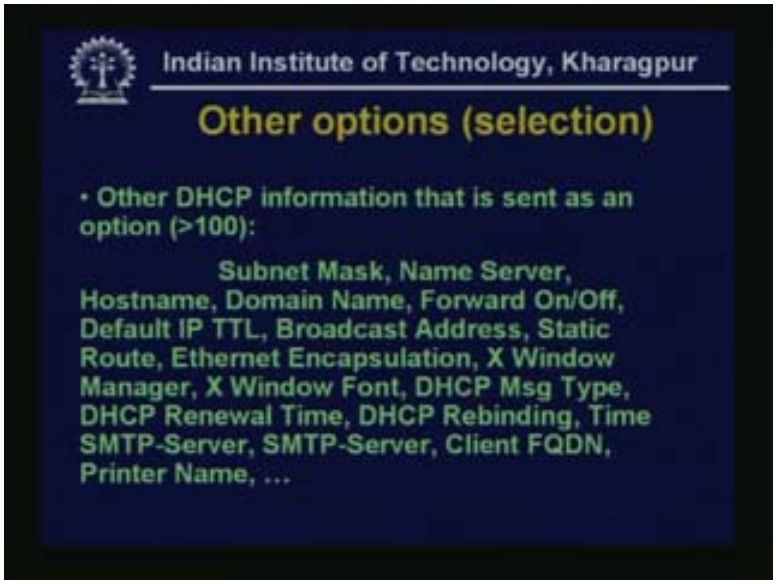
(Refer Slide Time: 8:52-10:05)

Extensions: There are lots of extensions especially with options. But these extensions support temporary allocation or leases of IP addresses. Leasing of IP address, suppose when we have a remote access server and when people are dialing what would happen is that, it would be given a particular IP address for a fixed amount of time. When its lease expires then that IP address may be withdrawn. And half way down the lease period if there is no great demand for IP address then the lease may be automatically extended or if there is a great demand the lease may be withdrawn also. This is for a temporary period of time and that is how it is dynamic. DHCP client can acquire all IP configuration parameters. Not only subnet mask and gateway addresses which are there in BOOTP but also other kinds of parameters can be downloaded from a DHCP server.

(Refer Slide Time: 10:16-10:23)

So DHCP is the preferred mechanism for dynamic assignment of IP addresses and DHCP can interoperate with BOOTP clients.

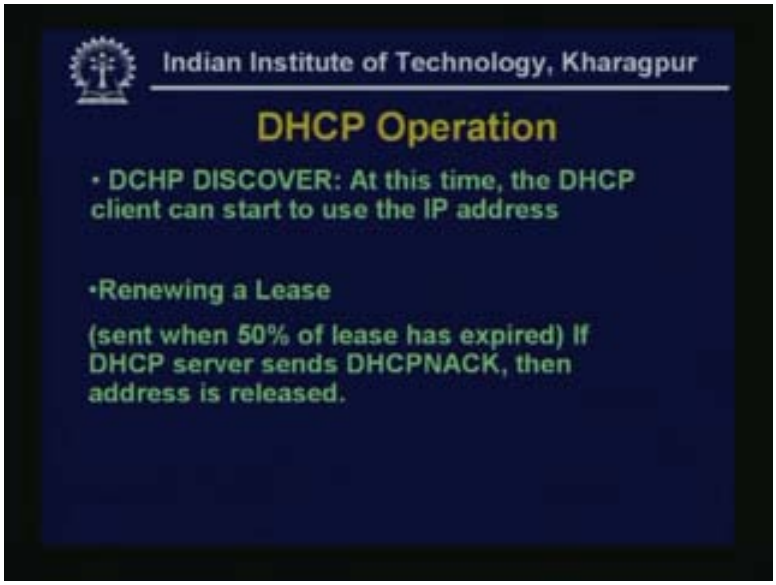
(Refer Slide Time: 10:24-12:17)



DHCP has a number of options. It is not possible to mention all the available options here. Other DHCP information is sent as an option so the number of options is actually greater than 100 which include things like subnet mask, name server, host name, domain name, forward on/off, default IP time to leave, broadcast address, static route, Ethernet encapsulation, x window manager, x window font, DHCP message type, DHCP renewal time, DHCP Rebinding, time server SMTP server, client FQDN, printer name etc. As the

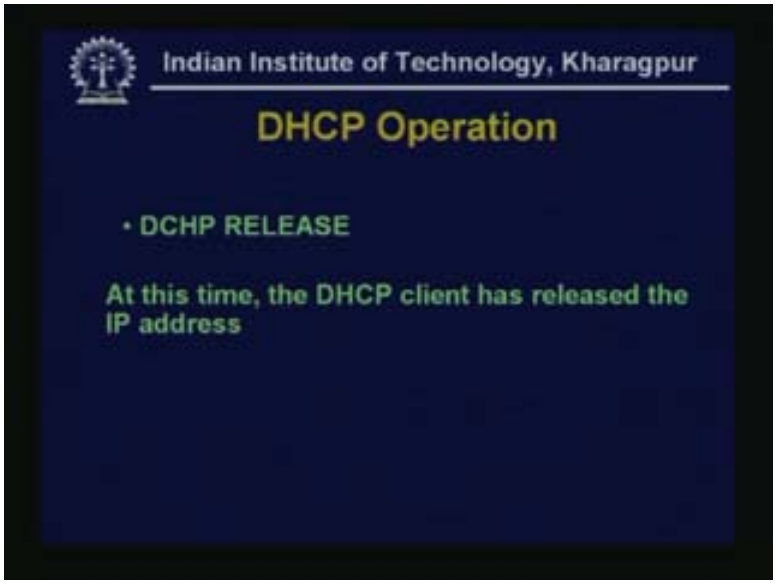
number of services given over a network grew it became important to give more information to the machines. Originally the machine was used just for communicating between two computers. Suppose there may be a centralized print service in the network and whenever you want to print something it can be done in the network. Similarly all other kinds of services became available in the local network as well as over wider networks. So all these would require some kind of configuration on the host end therefore such information can be transferred via this DHCP.

(Refer Slide Time: 12:18-12:50)



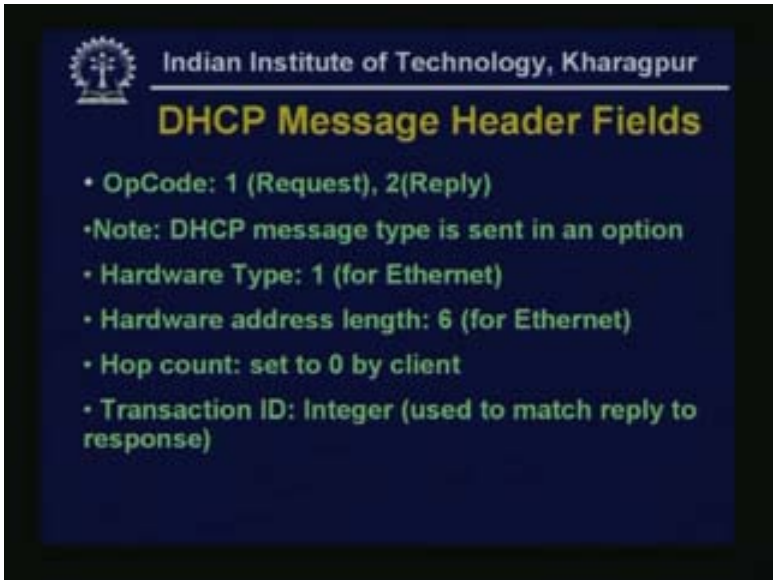
There are a number of DHCP operations. Let us discuss a few of them.
DHCP DISCOVER:
At this time the DHCP client can start to use the IP address.
Renewing a lease:
It is sent when 50% of the lease has expired. If DHCP server sends DHCPNACK then the address is released. Then you know your lease is not going to be renewed.

(Refer Slide Time: 12:49-12:55)



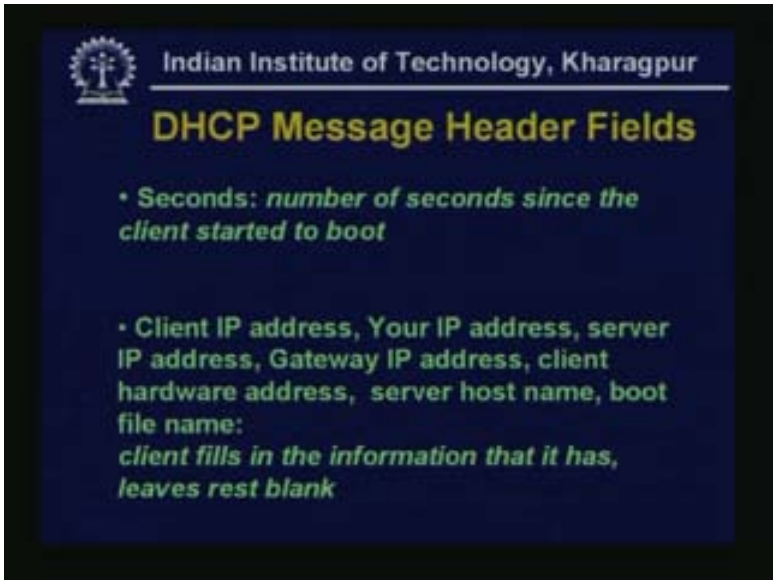
DHCP RELEASE: At this time the DHCP client has released the IP address, so the client has given it up.

(Refer Slide Time: 12:56-13:40)



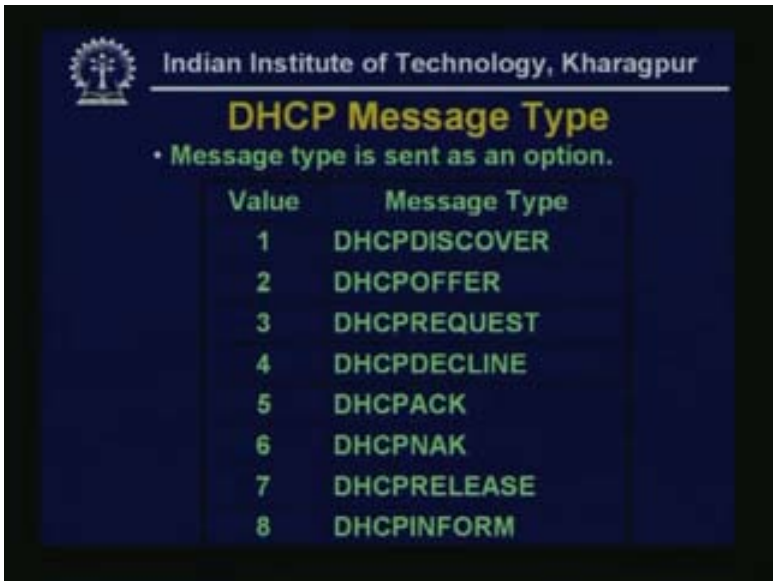
DHCP message header fields: In some fields there is an opcode. It may be a DHCP request from the client or it may be DHCP reply from the server. The DHCP message type is sent as an option. The hardware type of message is 1 for Ethernet and hardware address length is 6 for Ethernet. Hop count is set to 0 by client and transaction ID is an integer used to match reply to response if there is more then one request.

(Refer Slide Time: 13:38-14:30)



Seconds: It is the number of seconds since the client started to boot. Client IP address, your IP address, server IP address, gateway IP address, client hardware address, server host name, boot file name, etc. All these fields are available so when the client sends the request it would fill in whatever is known to it, maybe the MAC address is known to it. So it puts in the MAC address and all other fields are left blank. DHCP server will pick up the message that we broadcast and then fill up all the other necessary fields and then broadcast it back.

(Refer Slide Time: 14:29-14:50)

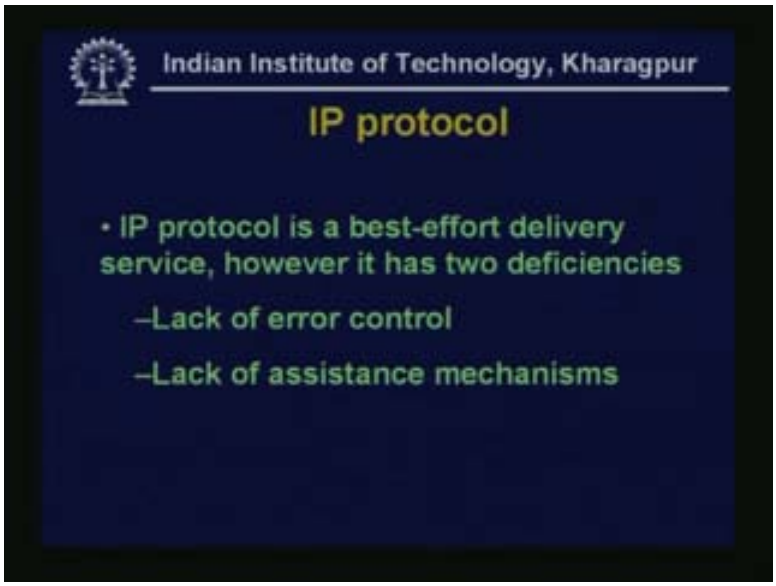


The following are the DHCP message types sent as an option:

DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPDECLINE
DHCP acknowledge
DHCP not acknowledge
DHCPRELEASE
DHCPINFORM and so on

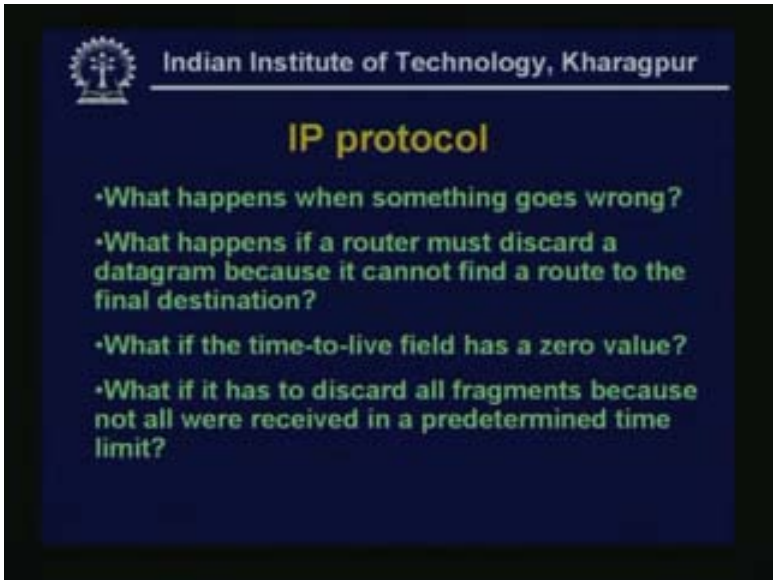
Our next topic is ICMP Internet Control Message Protocol. Let us see IP protocol and its deficiencies before that.

(Refer Slide Time: 15:05-15:30)



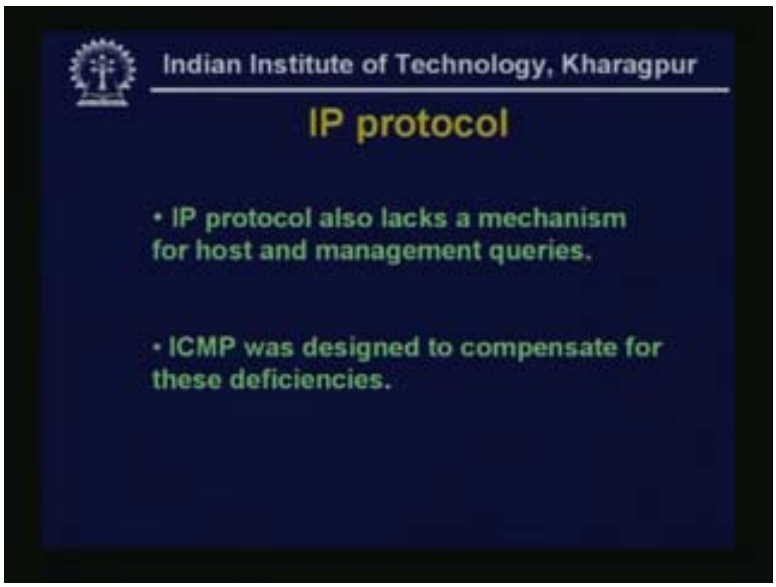
The internet is of course based on the Internet Protocol. IP protocol has some drawbacks. Though it is a best effort delivery service it lacks error control and lack of assistance mechanisms. Since IP is a best effort delivery at some point of time the effort may not be enough and routers ore other nodes on the network may have to drop packets and packets may not reach its destination on time and in proper order. First of all there is no error control and secondly if such errors do occur there is no message to the sources. Secondly, if you want to control the network for some reason, for example, may be the network is getting congested and so you want to do something about it, but IP does not have the mechanism. So, for all these purposes ICMP was brought in.

(Refer Slide Time: 16:36-16:55)



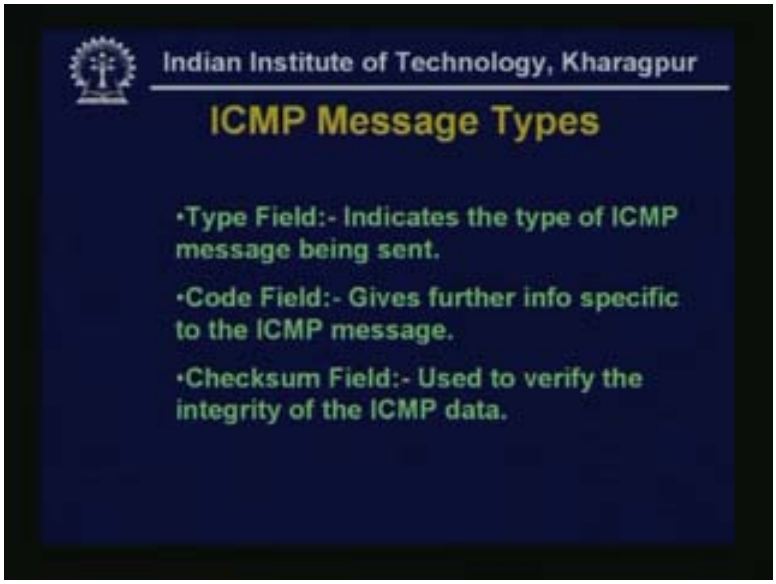
Therefore what happens if a router must discard a datagram because it cannot find a route to the final destination? What if the time to live field has zero value? What if it has to discard all the fragments because not all were received in a predetermined time limit? In all these cases IP has to discard a packet.

(Refer Slide Time: 17:05-17:24)



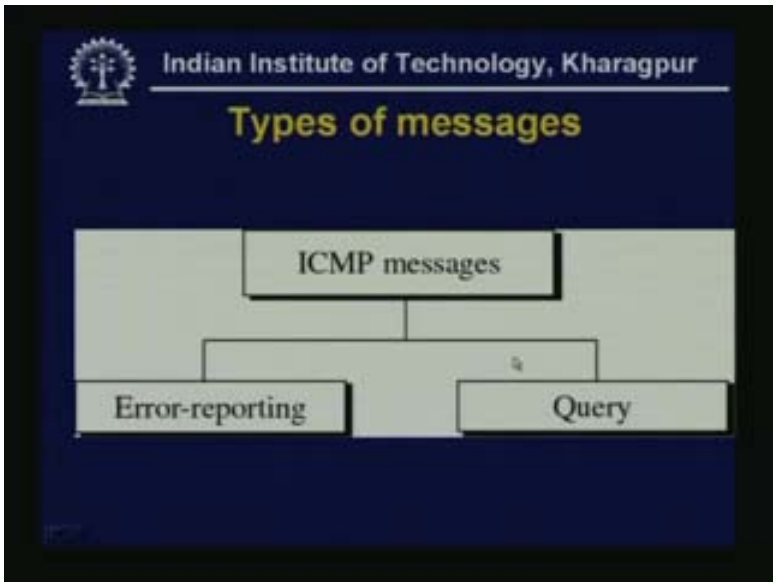
And similarly there are other situations. For example, may be it has reached the destination but the port is not available. So IP protocol also lacks a mechanism for host and management queries. So ICMP was designed to compensate for these deficiencies.

(Refer Slide Time: 17:25-18:01)



ICMP is a type field that indicates the type of ICMP message being sent and the type may be queries or errors. Code field gives further information specific to the ICMP message. For example, when an error occurs it tells what kind of error it is. Checksum field is used to verify the integrity of the ICMP data. So once again the checksum is included to control the error.

(Refer Slide Time: 18:00-18:24)

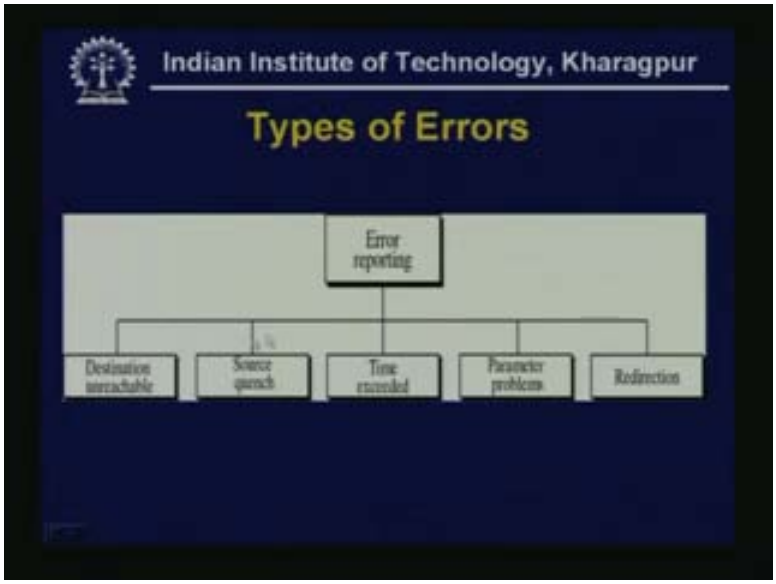


There are two types of ICMP messages. One is error reporting and the other is query response. If there is some error then the error reporting type of ICMP message would be generated and if there is a query another type of ICMP message would be generated.

(Refer Slide Time: 18:23-18:29)

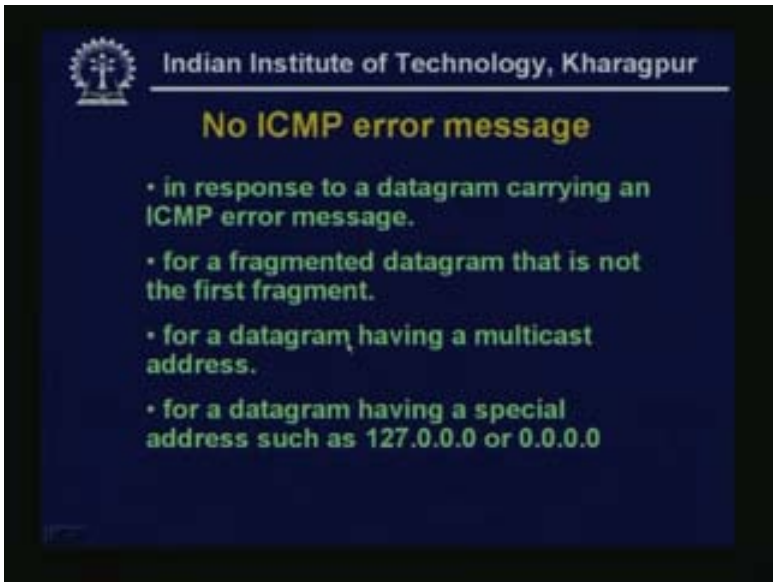
There is no effort in ICMP to correct the errors. This is the job of some other layer. So it does not really try to correct the errors but nearly reports the errors. The error messages are sent to the source. Suppose the datagram has been sent and something has happened to it and due to that there is an error, and now whoever drops that packet send an ICMP message back to the source. It may be a router on the way or may even be the final destination.

(Refer Slide Time: 19:23-19:50)



These are the various types of errors in error reporting. There may be a destination unreachable, there may be a source quench sending to first. Some of the important ones may be time exceeding, some may be parameters problem or redirection, etc.

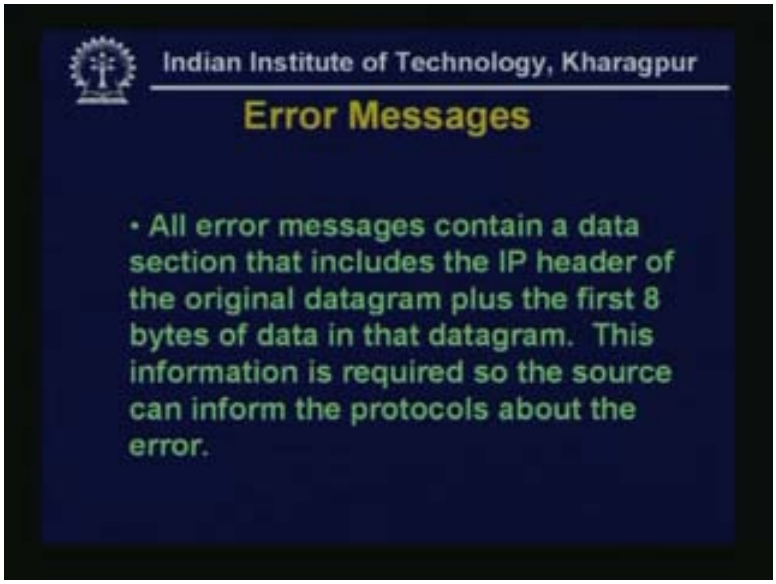
(Refer Slide Time: 19:51-21:29)



Please note that, no ICMP error message would be generated in response to a datagram carrying an ICMP error message. That means, somebody has generated an ICMP error message and it is traveling back to the source, and that error message itself gets an error and may have to be dropped on the way, then in such cases we do not generate another ICMP message. A little bit of problem happens due to congestion of networks. So if the network is very congested many packets may get dropped. And then if in response to dropping many packets you generate more packets then the congestion is not going to go away. So, ICMP error messages do not trigger other ICMP error messages for a fragment datagram that is not the first set of fragment.

For example, the datagram may have been fragmented into a number of parts, may be fifty parts, now for each of them you generate an ICMP message. Then the ICMP message would be too many so it is only generated for the first fragment. For a datagram having a multicast address, once again we cannot send an ICMP messages to all members of the group and for a datagram with a special address such as 127. 0000 or with some address like 0.0.0.0.0 also no ICMP error messages are generated for these.

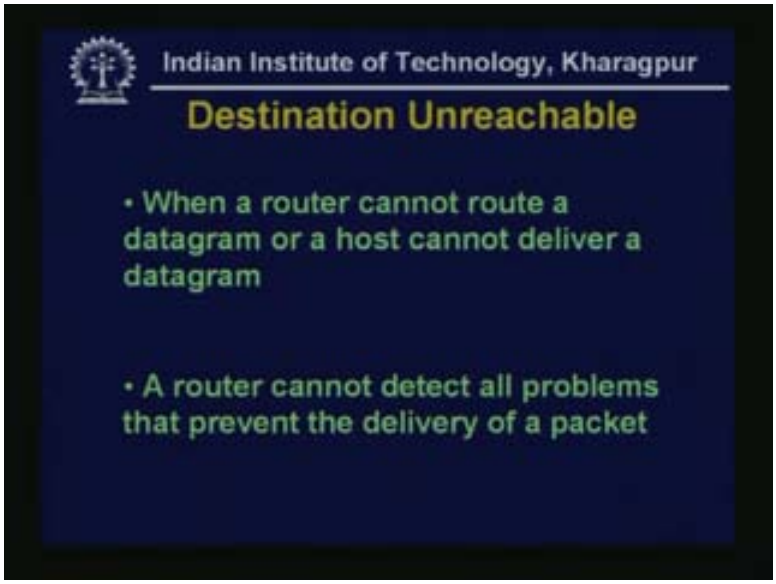
(Refer Slide Time: 21:30-23:15)



All error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. This information is required so that the source can inform the protocols about the error. From the original packet that was dropped the IP header of that original packet is sent back. First of all you need to know the source and know where you want to send back this ICMP message.

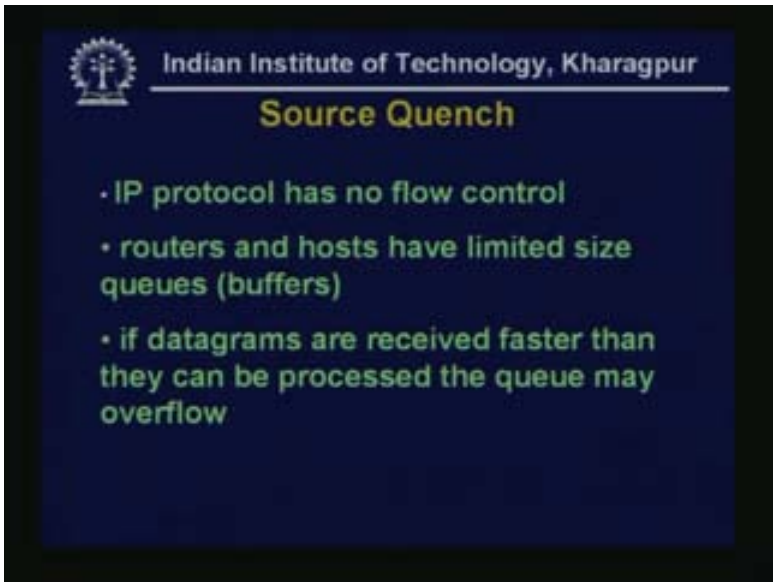
Secondly, even after this ICMP message gets back to the specific machine from which the original packet was generated. At this point it may have some error messages due to network intervening or this may have to do something with some process or application which is running on the source machine. So, after getting the message the host must know to which process it relates to. After the IP header what comes is the transport layer header so, a part of the transport layer header also goes back along with the ICMP message .This information is required so that the source can inform the protocols about the error.

(Refer Slide Time: 23:16-23:50)



Destination Unreachable: This is one type of an error message. When a router cannot route a datagram or a host cannot deliver a datagram, then in that case the destination is unreachable. A router cannot detect all problems that are preventing the delivery of a packet. So it is not always possible to exactly know why the destination is unreachable. But at least this information that the destination is unreachable, goes back to the source.

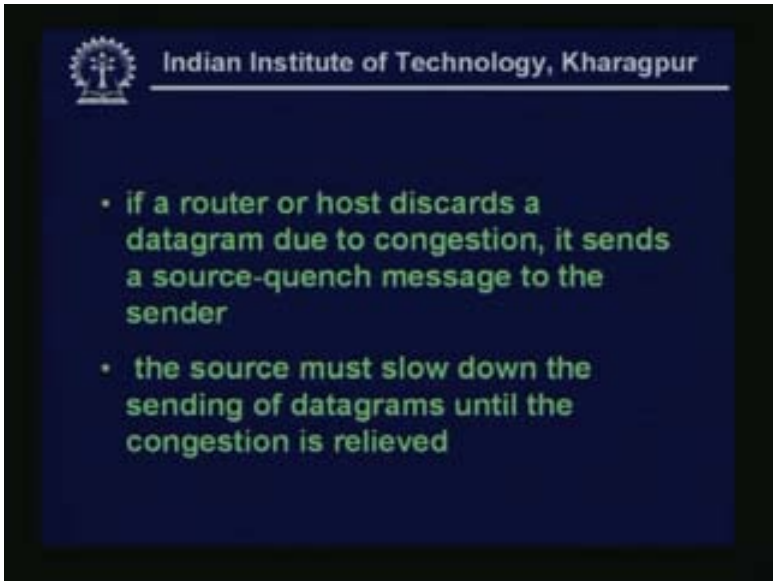
(Refer Slide Time: 23:51-25:30)



Source Quench: This is a crude attempt to implement some kind of flow control. IP protocol has got no flow control. Routers and hosts have limited size queues. So what happens is that, may be in an intermediate router and a number of packets have come up

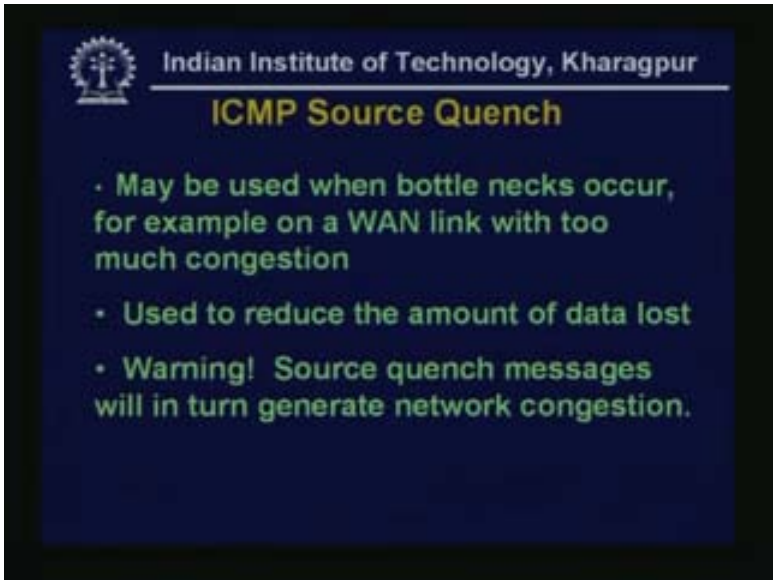
and certainly there is a flood of packets into one intermediate router from various directions. So what would happen is that its buffer is going to overflow and it will not be able to process because there is a limit depending on the speed of the router etc, there is a limit as to how fast packets can be processed and forwarded by an intermediate router and if other packets keep coming in, within that time they are going to be stored in the buffer where in the buffer might overflow. In that case the router cannot do anything else but to drop those packets. This router desperately wants to tell other people in the network to slow down on sending packets and that it cannot handle it because of overload. Basically it tries to slow down the flow of packets into itself. So it sends the source quench ICMP message towards the sources. If datagram is received faster than they can be processed the queue may overflow and in that case it asks the network to slow down.

(Refer Slide Time: 25:32-25:43)



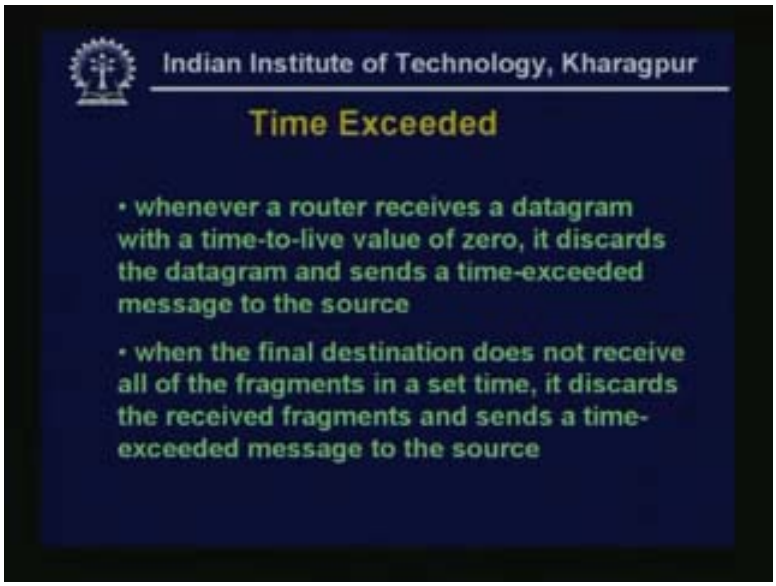
If a router or host discards a datagram due to congestion it sends a source quench message to the sender. The source must slow down the sending of datagram until the congestion is relieved.

(Refer Slide Time: 25:44-26:03)



This may be used when bottlenecks occur. For example, on a WAN link with too much congestion it is used to reduce the amount of data lost. But a warning is, source quench message will in turn generate network congestion. There were already too many packets in the network but you have sent a source quench packet towards the source which is just one hop towards the source was already getting packets from the source but will also get an ICMP message from the router just one hop down so it is having more packets now. So by this way congestion might travel towards the source but anyway finally it reaches the source and the source will hopefully slow down and all these will die.

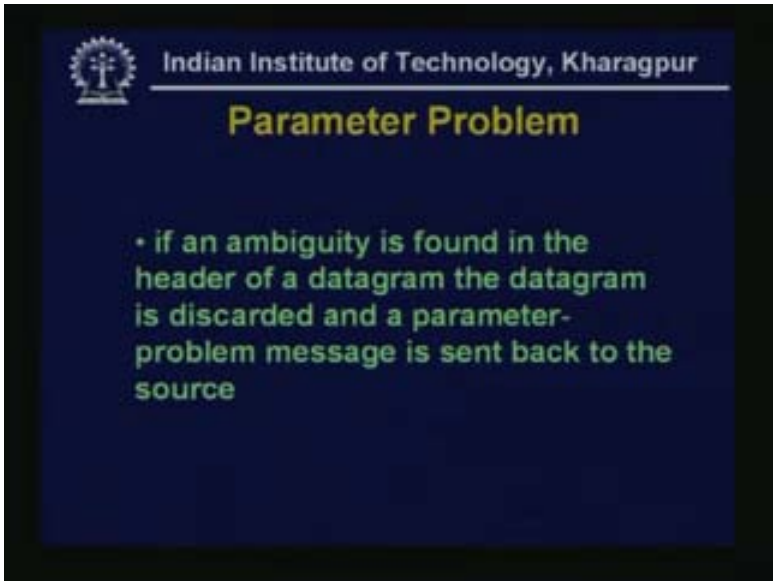
(Refer Slide Time: 26:48-27:18)



Time Exceeded: Whenever a router receives a datagram with a time-to-live value of zero that means it has been going round the network it discards the datagram and sends a time exceeded message to the source. When the final destination does not receive all of the fragments in a set time it discards the received fragments and sends a time exceeded message to the source. These are two different cases: One is that, in the destination all the fragments did not reach so there was a specified time after which it has to drop all the fragments and send a time exceeded message to the original source.

The other thing is that, when a router receives a datagram with the time-to-leave field which is zero. If you remember, keeping a time-to-leave field and decrementing it at every hop is quite important because suppose there were some packets which were floating around in the network and due to some trouble with the routing tables a loop has been formed, so, if you do not have this time-to-leave field it will go round and round at infinite term where they slowly burden the network. So, the solution to that was, after a certain number of hops the packet is dropped and when a packet is dropped a time exceeded message is sent to the source. There may be parameter problems.

(Refer Slide Time: 28:35-28:48)

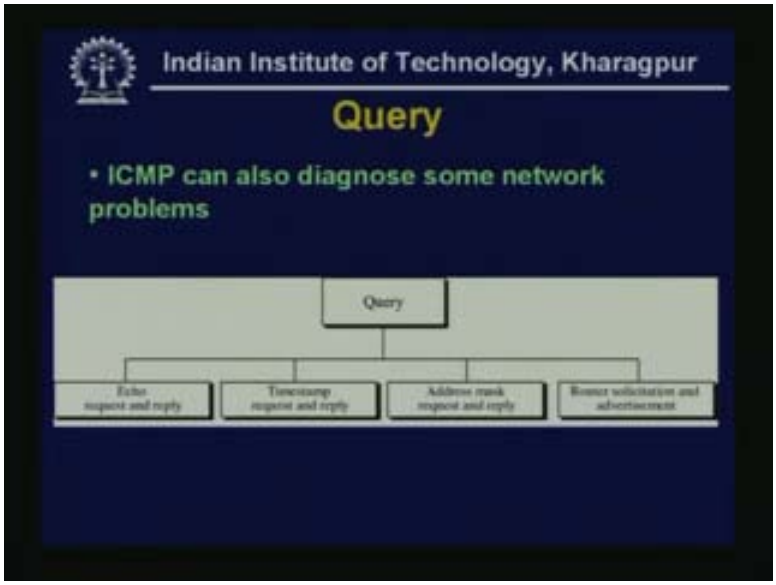


If an ambiguity is found in the header of a datagram the datagram is discarded and a parameter problem message is sent back to the source.

(Refer Slide Time: 28:47-28:59)

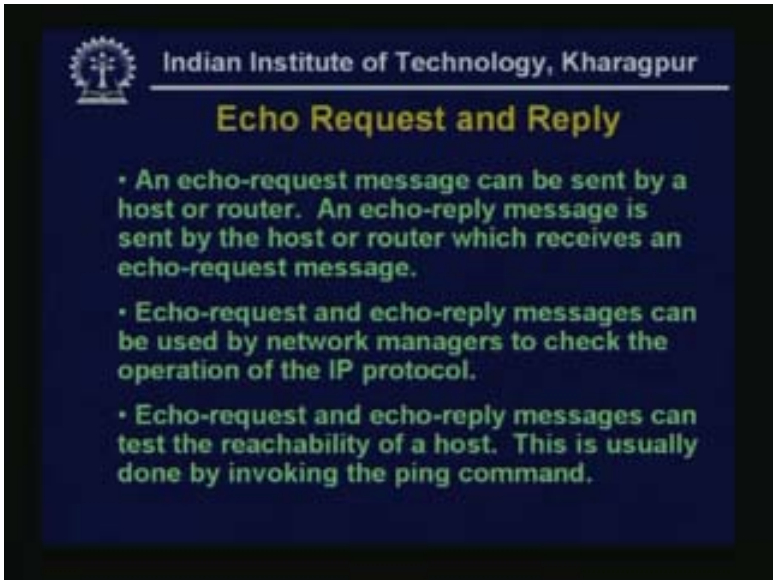
Redirection: A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message, so, actually this helps in routing.

(Refer Slide Time: 29:00-29:18)



Now let us come to queries. ICMP can also diagnose some network problems. For example, echo request and reply, time stamp, address mask, router solicitation and advertisements, these are example of queries. We will just see a few of these also.

(Refer Slide Time: 29:22-30:01)



Echo request and reply: Is used very often when you want to find out whether the network is up and running or not. An echo request message can be sent by a host or router. An echo reply message is sent by the host or router which receives an echo request message. The echo request and echo reply message can be used by network managers to check the operation of the IP protocol.

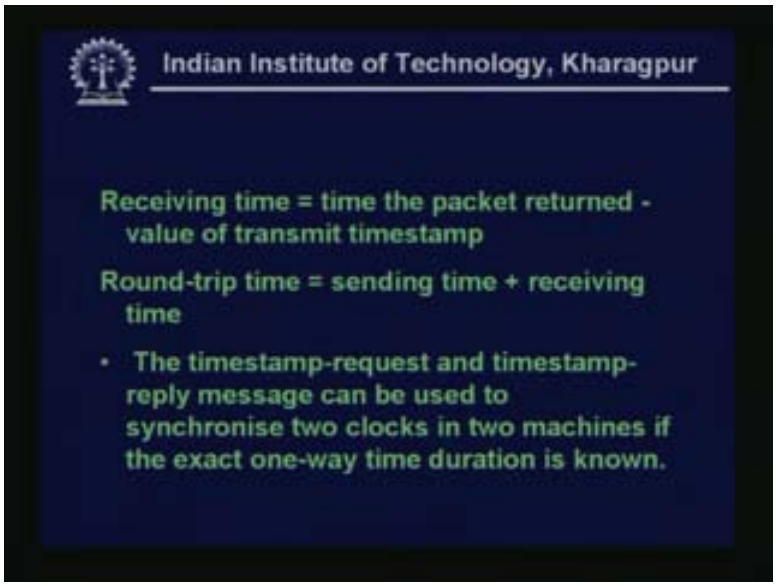
Echo request and echo reply message can test the reachability of a host. This is usually done by invoking the ping command. Later on we will get into more details of ping because that is one kind of command which even users quite often require. For example, if you are logged on and you find that you cannot reach your destination anywhere in the network then you have to find where the problem lies, is it in your local network or in the local subnet.

Therefore, in the local subnet you might ping that gateway to see whether you can reach up to the gateway. If your ping message goes up to the gateway and you get an echo reply then you know that up to that much the network is ok. And if you are ok up to the router you may want to ping the router in the entire network. Now the problem may be somewhere in the link outside. The problem may even be in the destination which you are trying to reach. So one way is to go probing the network, even by users is to use ping.

(Refer Slide Time: 31:16-31:47)

Timestamp Request and Reply: Timestamp request and timestamp reply messages can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized. So, sending time is equal to the value of receiving time stamp minus value of original time stamp. So this way you can get some idea about the round-trip time. There are other ways also.

(Refer Slide Time: 31:49-32:12)



So receiving time is equal to time the packet returned minus the value of transmit timestamp. Round-trip time is equal to sending time plus receiving time. So the

timestamp request and timestamp reply message can be used to synchronize two clocks in two machines if the exact one-way time duration is known.

(Refer Slide Time: 32:14-32:21)

Address-Mask Request and Reply: Enables a host to request and receive the network or subnetwork mask. It is useful for diskless stations at start up. But we have seen the DHCP is another way of handling this.

(Refer Slide Time: 32:23-32:43)

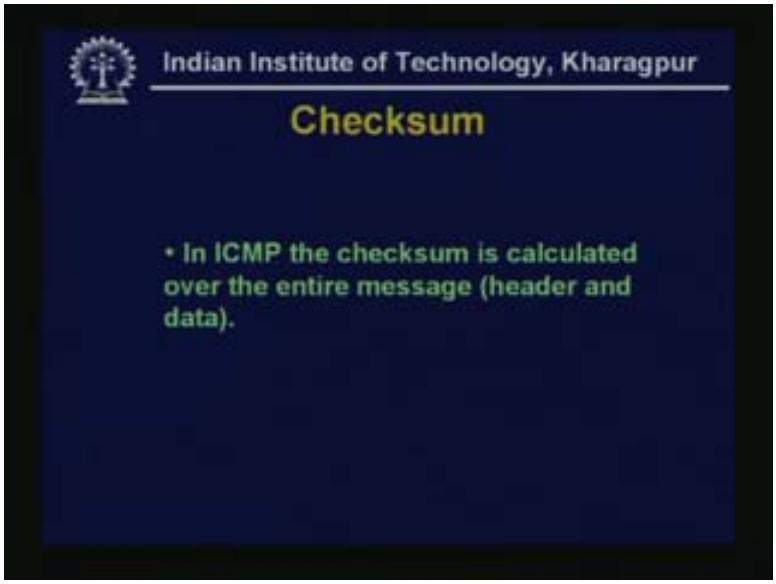
Router Solicitation and Advertisement: Allows request of routing information and the reply of this information. Routers can periodically send router advertisements without

being solicited. Suppose a router has just been connected to the network, anyway the routers have to run the routing protocol like the RIP or BGP, OSP etc, this means it needs to communicate to the neighboring routers, but how do the other routers know there is a new router in the group. So, one way is, as soon as the router gets connected it does some router solicitation and it advertises itself so that other routers get to know that and slowly the entire network becomes aware of this new router which is connected. Similarly, a link may go down and all kinds of other things may happen. So, the exchange of router information has to happen through some mechanism.

(Refer Slide Time: 33:44-34:15)

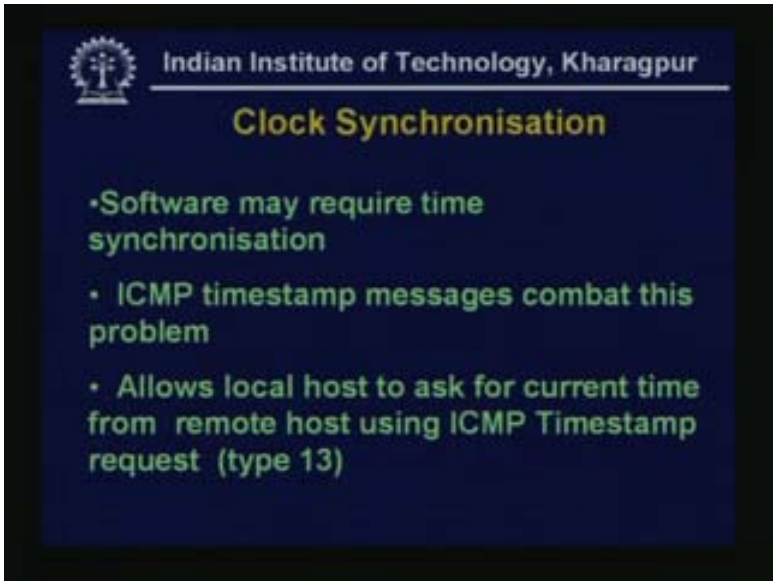
Router Discovery Message: Host can learn about available gateways to other networks. Host send the router solicitation message to begin the process using the multicast address of 224.0.0.2 as the destination. It can also be a broadcast message in case a router does not accept multicast messages. When a router receives the message it will advertise its available gateway.

(Refer Slide Time: 34:16-34:28)



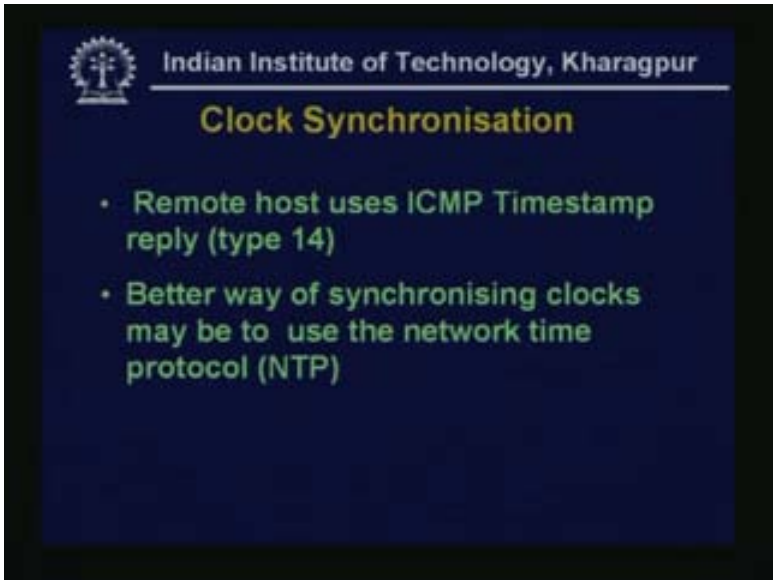
The checksum of the ICMP message: In ICMP the checksum is calculated over the entire message, that is the header and data combined. This is just to keep some control over errors.

(Refer Slide Time: 34:26-34:48)



Clock Synchronization: Software may require time synchronization. So ICMP time stamp message combats this problem. It allows local host to ask for the current time from a remote host using ICMP timestamp request. So it is type 13.

(Refer Slide Time: 34:47-35:04)



Remote host uses ICMP timestamp reply which is type 14. So, the better way of synchronizing the clocks is to use the network time protocol. The time is the UT Universal Time.

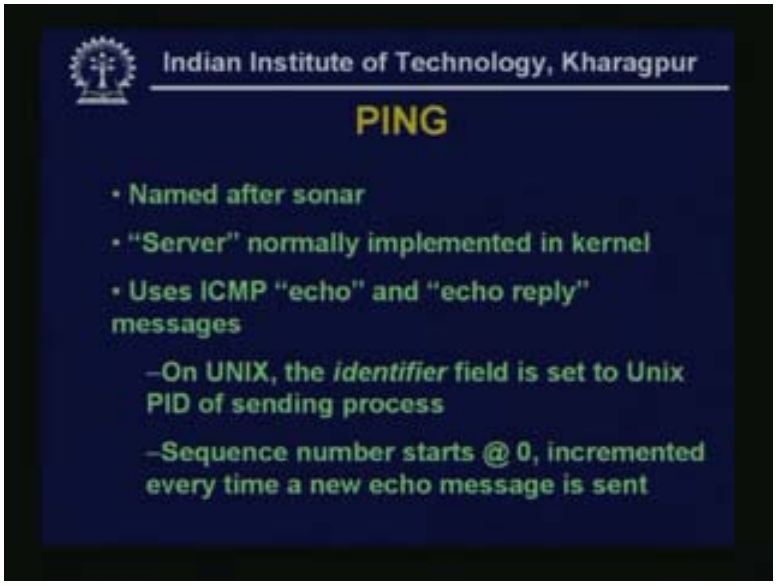
Ping and Traceroute:

(Refer side time: 35:15-35:55)

This is an overview. This is part of the ICMP messages. Ping sends an ICMP message to a remote host and lets you determine if that host is responding. Actually ping uses echo and echo reply for the ICMP message. Traceroute uses TTL fields to query all hosts

enroute to a specific destination. You can use traceroute to map a network. That means, if you want to know which is the route you are tracing then this helps you.

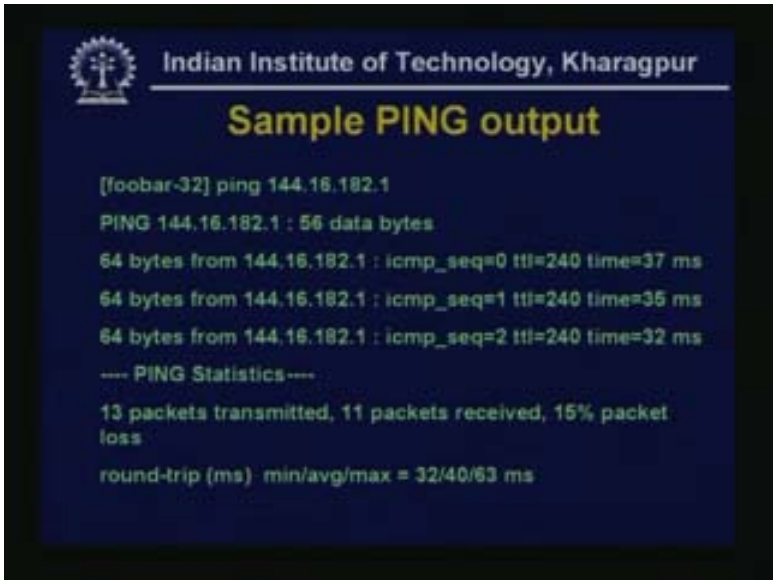
(Refer Slide Time: 35:58-36:46)



Ping is named after sonar. In sonar if you want to probe some place you send an ultra sound signal just like you do in radar and if it bounces of something you get a ping, so that is where the name comes from. If you want to send an echo request you expect an echo reply and that is your ping. So server normally implemented in kernel uses ICMP echo and echo reply messages. On UNIX the identifier field is set to UNIX PID or sending process. Sequence numbers starts at 0 incremented every time a new echo message is sent.

Actually, when you ping a machine not just one request is sent. The machine you are trying to ping or the channel may be noisy and if that happen then your echo request or the reply may get dropped in between. So, sending one request is not sufficient and may be three times or five times etc you can configure it, it sends echo request and it expects all the three or all the five replies. And if it receives none of them, then in that case it will say that hundred percent of packet loss or it may get two out of five so it will say sixty percent of packet loss or forty percent.

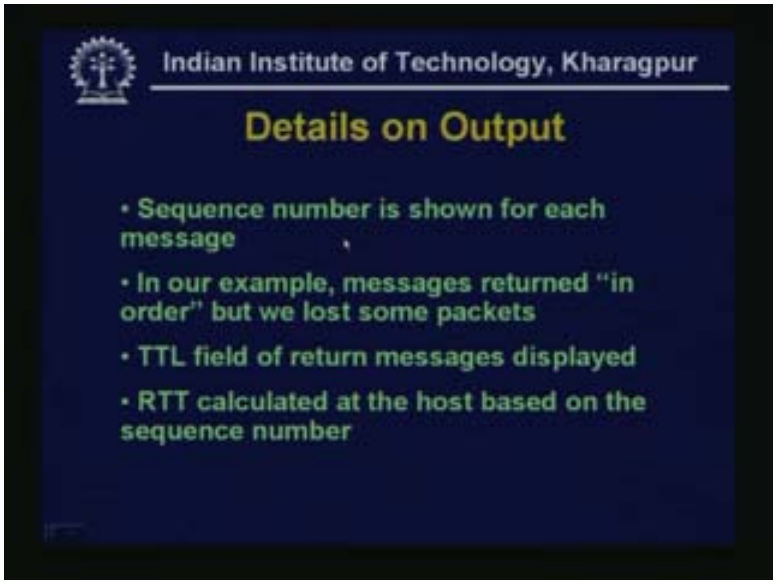
(Refer Slide Time: 36:37-39:46)



Let us see one example of ping. Suppose we ping a machine 144. 16.182.1, we have pinged this machine and then give the IP address over here. By the way if you have a name server on the network you could also put the name over there. Ping 144. 16.182.1, 56 data bytes is your data plus it will have some thing. So you may get a result like this: 64 bytes, this is what you are getting from the echo reply, 64 bytes from 144 16 182 1. ICMP sequence is equal to 0 time-to-leave is 240 and time is equal to 37 milliseconds. So it gives you some idea about how much time it takes.

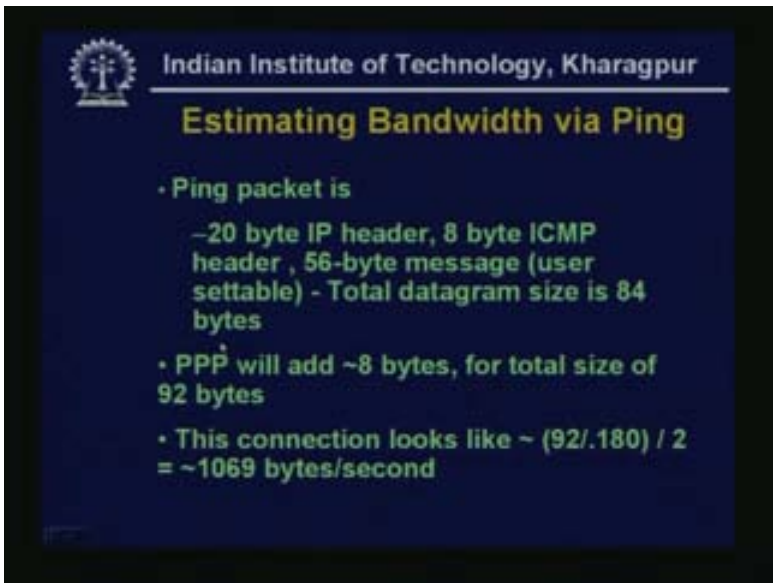
Then another packet has came back as an echo reply 64 bytes from the same machine, sequence number 1 and time is so much. For each packet it receives back as reply it is going to print a line like this and then finally it will give you a statistics as something like this: 13 packets transmitted, 11 packets received which means that it had originally sent 13 packets and it got only 11 packets back so 2 packets must have got lost. Therefore it is a 15% packet loss. And the round-trip time you may calculate the mean, average, max. So, from the ping you can get an idea about the round-trip time.

(Refer Slide Time: 39:51-40:12)



Some details on the output sequence number are shown for each message. In our example message returned in order but we lost some packets. They may be returned due to out of order. Also TTL field of return message is displayed and round-trip time is calculated at the host based on the sequence number.

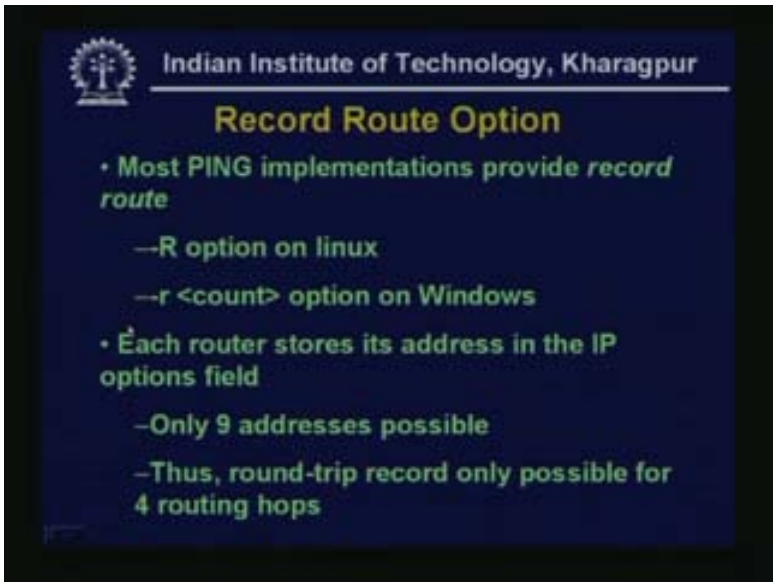
(Refer Slide Time: 40:14-41:45)



We can estimate not only the round-trip time but also the bandwidth using ping. But this works only for few hops. If it is beyond a number of hops your ping will not work. The ping packet can estimate the bandwidth in this way: 20 byte IP header, 8 byte ICMP header, 56 byte message this can be set by the user, so the total datagram size is that plus

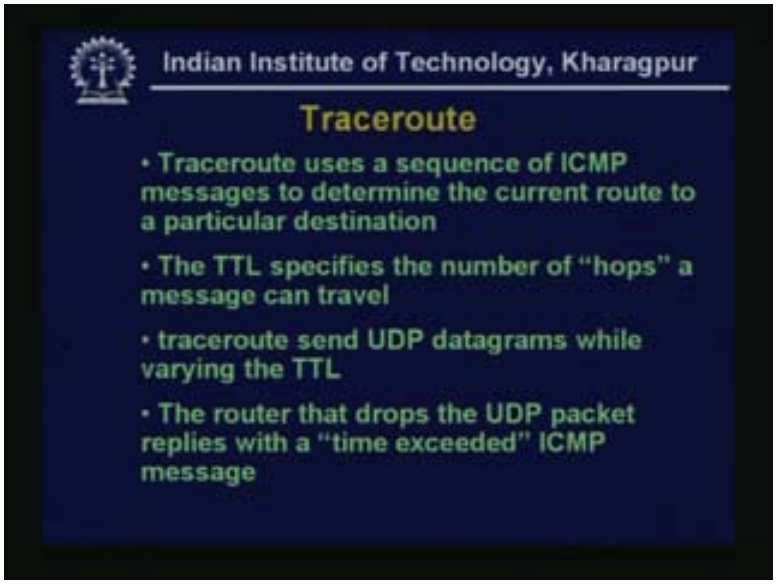
76 plus 8 is equal to 84 bytes so 84 bytes were sent. Now, if it was sent through PPP it will add about 8 bytes so the total size will be 92 bytes. So this connection looks like 92/.180/2 that is about 1069 bytes per second. What is this 0.180? It is 92 bytes so this is time. This gives you some idea about what kind of bandwidth you have. In this particular case the bandwidth is not that much but it is only about 1069 bytes per second. This is a very crude estimate but you can get some kind of feel about your immediate locality.

(Refer Slide Time: 41:56-42:23)



Record Route Option: Most ping implementations provide record route which is – R option on linux, – r option on windows. Each router stores its address in the IP options field, only 9 addresses are possible. Thus round-trip is only possible for 4 routing hops. So you can take only 4 hops and within those 4 hops you can find out that how your message went and how it came back. That is, may be it came back through different paths or it could have returned in the same path etc. You can actually trace the route and because of the limitation on the size that is on the number of addresses you can store you can only route or map the network in your immediate locality. But if you want to go beyond this then you have to use something else called Traceroute.

(Refer Slide Time: 43:12-46:16)

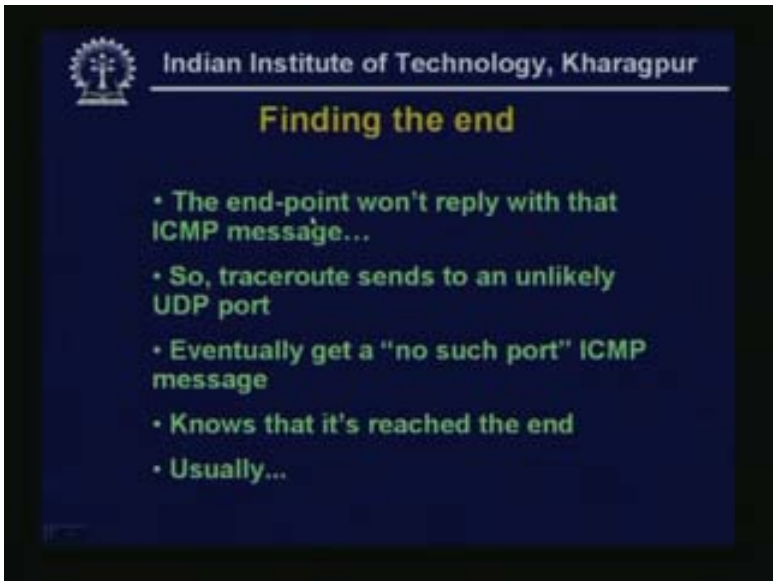


Traceroute uses a sequence of ICMP messages to determine the current route to a particular destination. This is actually done in an iterative fashion. Suppose I want to traceroute to a distant machine whose IP address is known. Then I will send a message to that machine but with a very small number for the time-to–live. Therefore what will happen is that my message will take so many hops but then it has not reached the destination so may be it must have just started and it will be somewhere in the beginning so its time-to-leave is going to become 0.

As soon as the time-to-live becomes 0 the intermediate node may be that router will have to drop the packet and it sends an ICMP message back to the source. Now my program gets this ICMP message and now it sends the same dummy message to the destination after increasing the time-to-live by one unit. Now it is going to pass that router that had dropped the packet in the previous instant and so it will go one more hop and then the packet will get dropped so that router is now going to send an ICMP message back to the source. Now we will know which router is on the way. Therefore by this way iteratively you keep on increasing the time-to-leave one by one and you trace the entire route, that is, you map it out.

But let us see what happens when it reaches the destination? When it reaches the destination what happens is that this message is sent to a very unlikely port, a randomly selected port. Most probably the destination machine will not know about this port so it will say that the port is unreachable and then that ICMP message will come back. Now we know that we have reached the destination. Hence this way we have traced the entire route one by one from the source to the destination. Traceroute uses a sequence of ICMP messages to determine the current route to a particular destination. The TTL specifies the number of hops a message can travel. Trace route sends UDP datagrams while varying the TTL. The router that drops the UDP packet now replies with a time exceeded ICMP message.

(Refer Slide Time: 46:20-46:40)



The end point will not reply with that ICMP message because it has already reached there. So traceroute sends to an unlikely UDP port. Eventually get a no such port ICMP message. It knows that it has reached the end.

(Refer Slide Time: 46:41-46:46)

So this is the reference about ICMP messages. Actually these are not the only internet control message protocols but there are a number of others which we did not discuss. We just discussed a few of them. There are other protocols like DHCP, BOOTP, RARP, ARP. For example, they help in running the network in a better fashion. ARP protocol is

a low level protocol. Then we have this RARP, BOOTP and DHCP for assigning a network. This ICMP helps in controlling the network operation and giving error messages. Then there is another side protocol which we will discuss in the next class namely IGMP which is internet group management protocol. So, that is another part of routing that we have not discussed as yet.