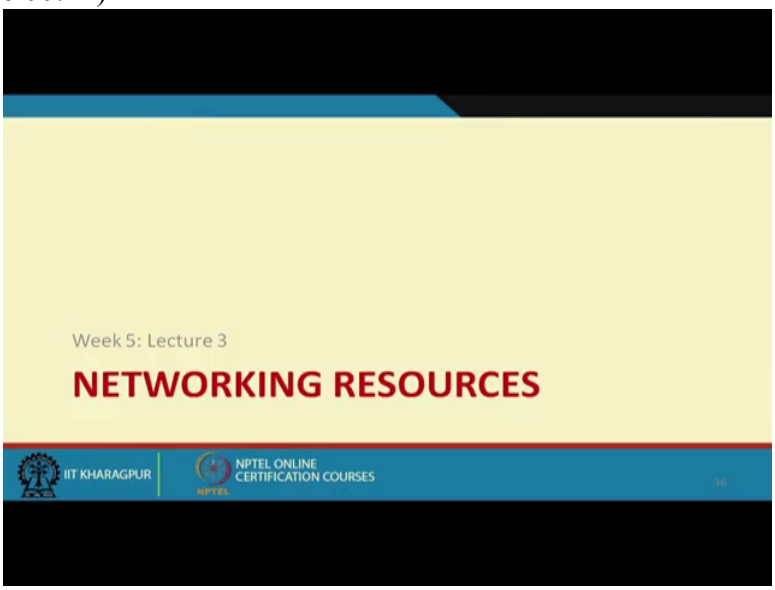
Course on E-Business
Professor Mamata Jenamani
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur
Module 05
Lecture Number 25
Networking Resources

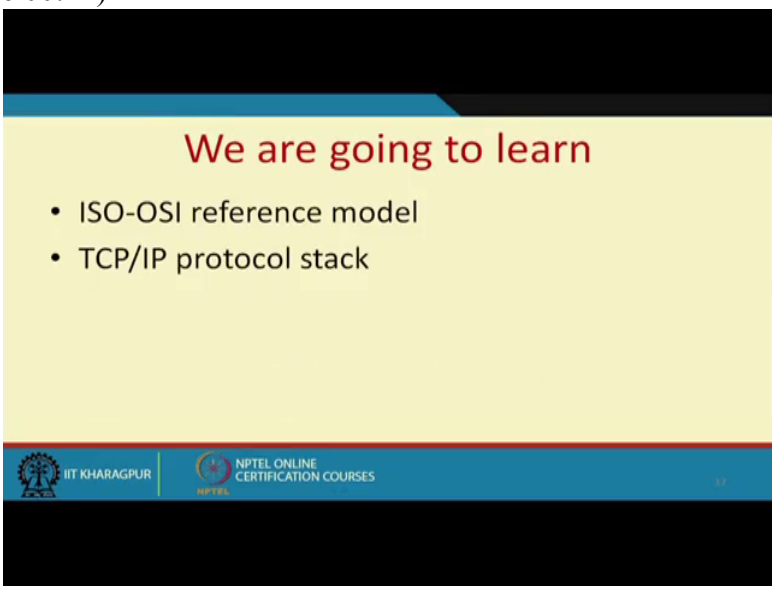
(Refer Slide Time 00:17)

We continue our discussion on infrastructure of e-business. So far we have discussed about what is internet and what is the basic web system architecture and what are various performance parameters, how web information systems will be judged and this work, this particular lecture we are going to learn about networking resources.

(Refer Slide Time 00:41)

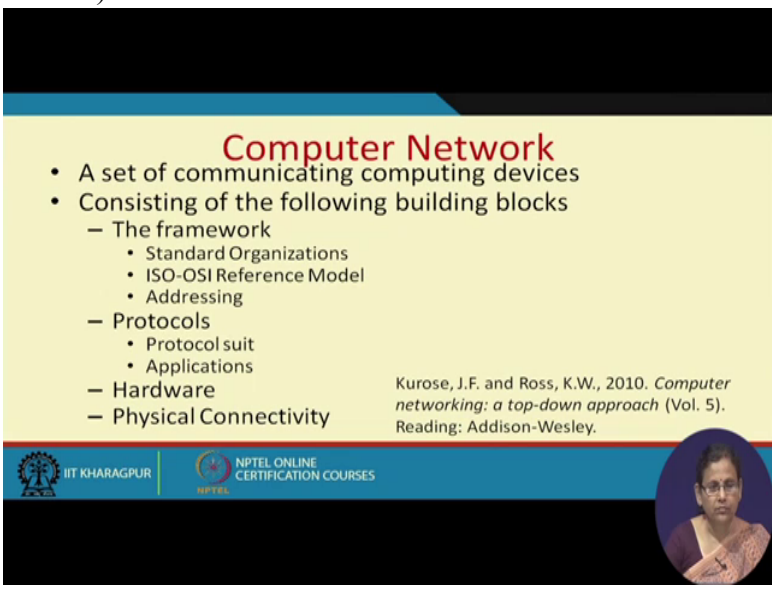


(Refer Slide Time 00:42)



So basically we will be covering two things, one is I S O/ O S I Reference Model and how T C P/ I P implements this particular model.

(Refer Slide Time 00:56)

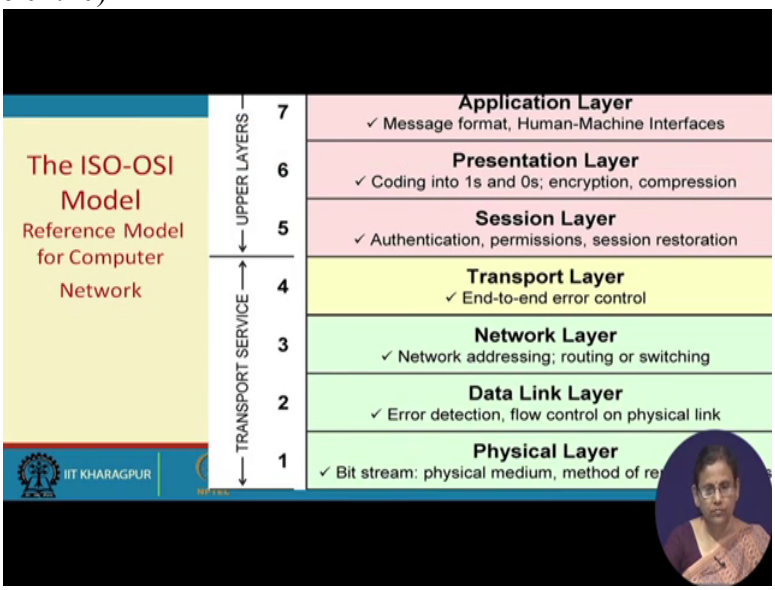


So coming to this computer network, it is a set of communicating computing devices consisting of many basic building blocks. First of all it has to have a framework under which we are going to talk about various standard organizations who are responsible for setting of, many organizations who are responsible for setting of the standards. Then under this, we are going to talk about this I S O/ O S I Reference model then we are going to talk about the protocols, hardware and physical connectivity. In fact this hardware and physical connectivity we will be talking when we discuss about computer hardware.

(Refer Slide Time 01:44)

There are many standard making bodies like I S O, I A B, I triple E who are responsible for setting up the standard because of which we are able to make two heterogeneous systems communicate with each other. They are responsible for designing protocols as well as computing devices and setting up, setting the communicating devices and setting up the standards so that we can make 2 different systems talk to each other.

(Refer Slide Time 02:20)



So if you look at the basic model of communication for, basic model of this client server based data exchange over the web the reference model proposed by these organizations, these specifically this I S O is Open System Interconnection model. So this is called a reference model of the computer network because this simply shows how logically various activities of

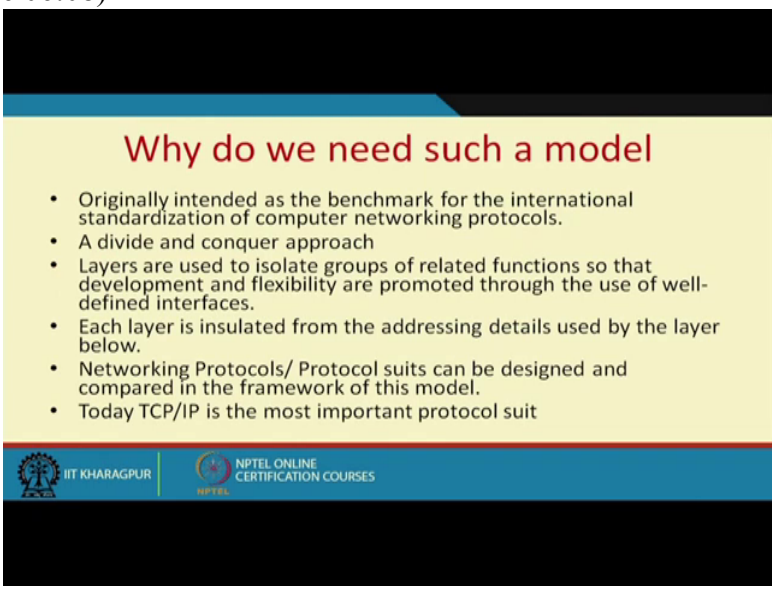
a network should be separated from each other. This is just a reference model and when it comes to implementation, this can be implemented by different protocols.

Now in this reference model if you can see there are 4 lower level layers who are responsible for transport service and there are 3 upper level layers who are responsible for organizing and presenting the content. So lowest level is your physical layer where the data actually moves through the physical medium like your cables and all. So here the data is treated as a bitstream and along with the data, your various, you know, various other addressing schemes, physical level addressing schemes are used to send it between 2 systems in certain manner. Then the second layer is actually your data link layer. This controls the, this acts as the flow control on the physical link. Now it also has certain kind of, certain kind of functionalities for detecting the error if at all it occurs during the physical flow.

Next level is your network layer. So in this network layer, network addresses are attached to the hosts so that they can be uniquely identified over the internet. So the routing and switching are 2 activities which take place in this particular network. Then there is transport layer which is responsible for end to end delivery and error control. Besides these 4 transport layer, 4 transport service layers, after the data reaches at the client's machine, then it is the responsibility of the server to make, bring it to a presentable form.

So in application layer, presentation layer and session layer takes care of these facts. The session layer's activity is authentication, providing permission, session restoration et cetera. For presentation layer, it is encryption and compression, and in case of application layer it is building a human machine interface for understanding what is sent through this transport layer.

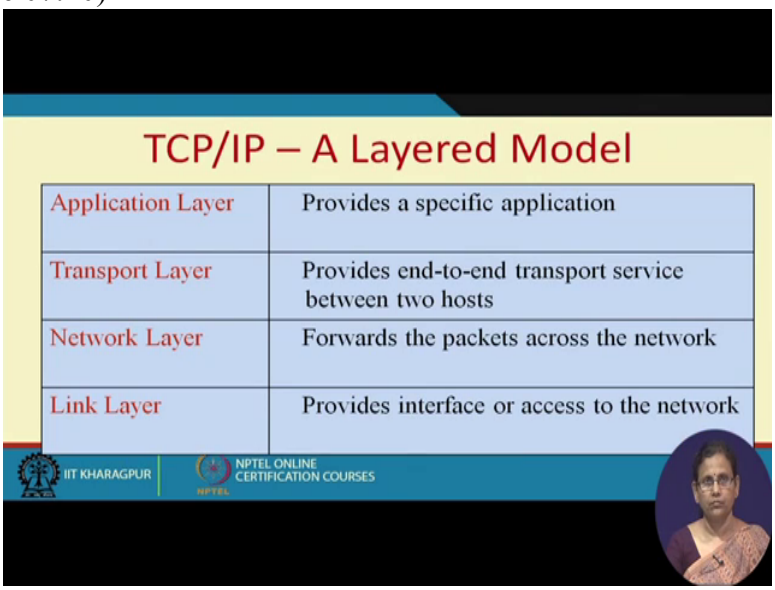
(Refer Slide Time 06:08)



Then the question is why do we need such a model? Now this particular model which was originally intended as a benchmark for international standard organization for computer networking protocols has been implemented in various forms but the idea of logically separating various activities within the layers still remains the same. So it follows a divide and conquer approach. The layers are used to isolate groups of related functions so that development and flexibilities are promoted through the use of well-defined interfaces. Each layer is insulated from the addressing detail used by the layer below. Various networking protocols and protocol suites can be designed and compared in the framework of this model and they can be made compatible if all of them follow this model.

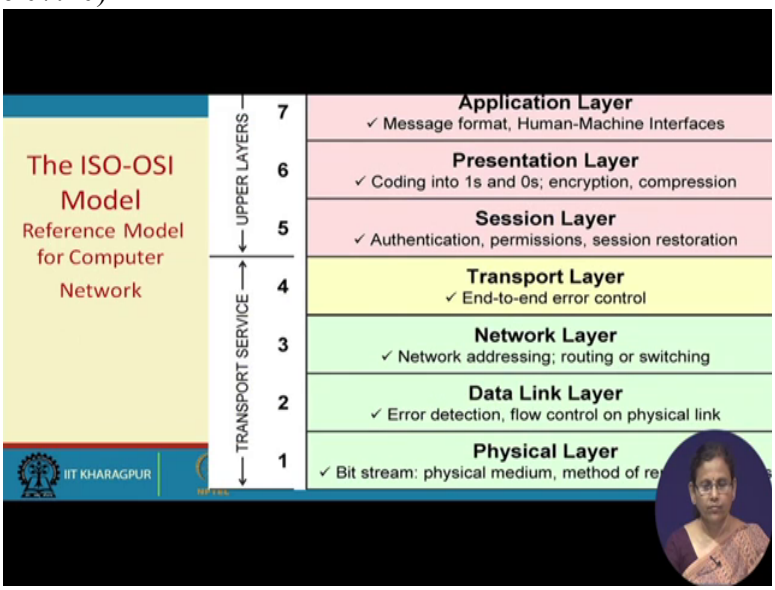
Now to implement this one, in today T C P/ I P is the most important protocol suite.

(Refer Slide Time 07:20)



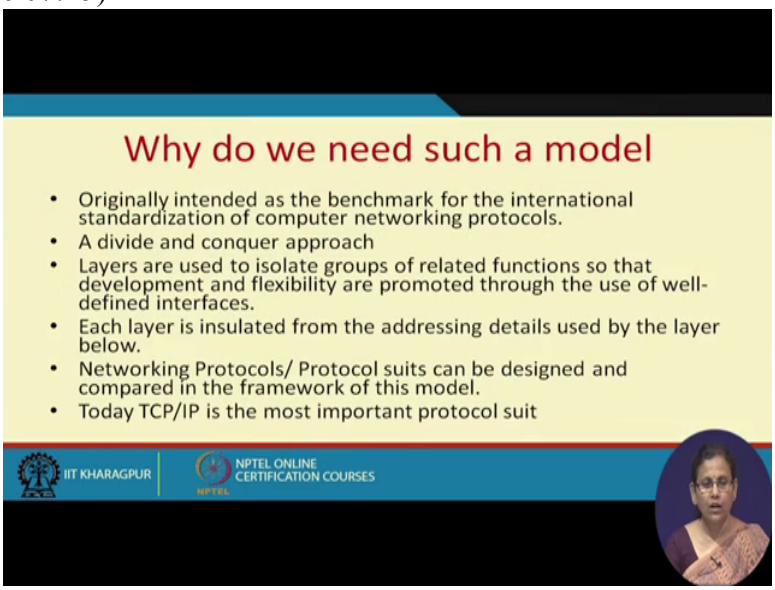
This T C P/ I P protocol suite consists of 4 layers. If you look at this, they are actually correspond to the, all of them correspond to the, three of them correspond to the transport layer of this,

(Refer Slide Time 07:40)



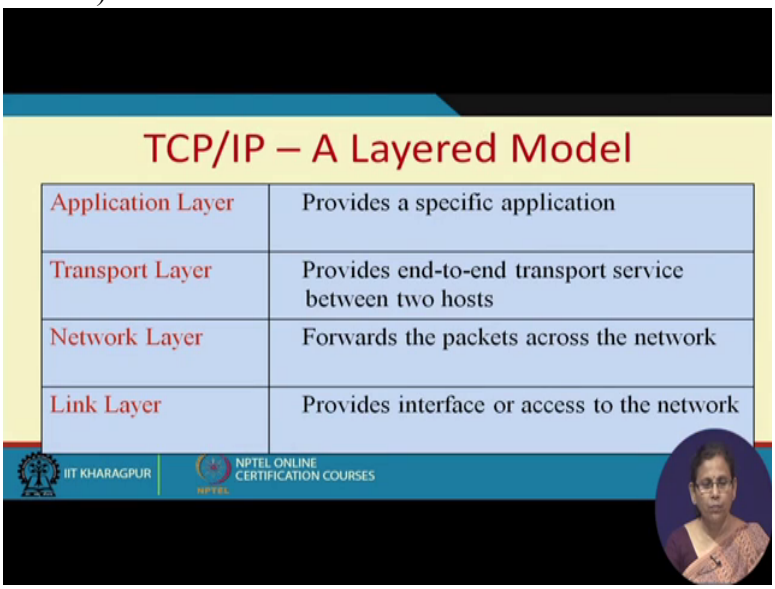
transport service layer of this, this I S O/ O S I model and the

(Refer Slide Time 07:45)



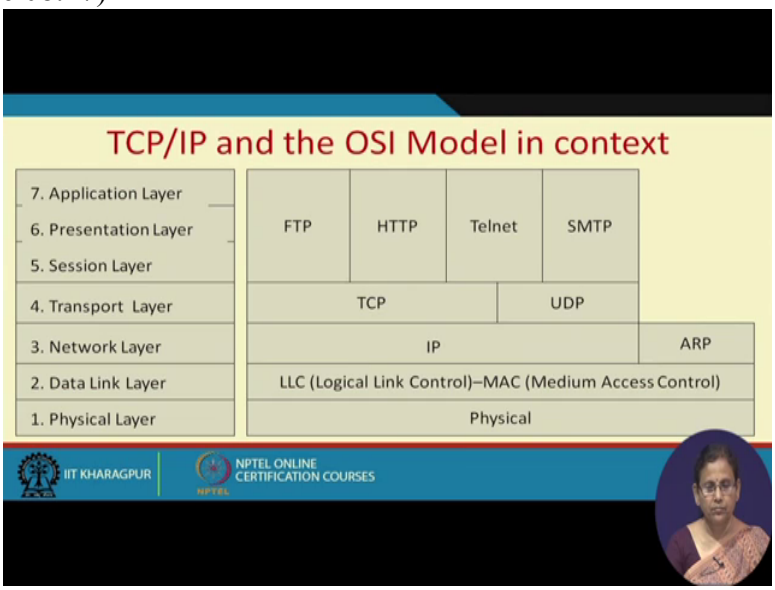
upper one

(Refer Slide Time 07:46)



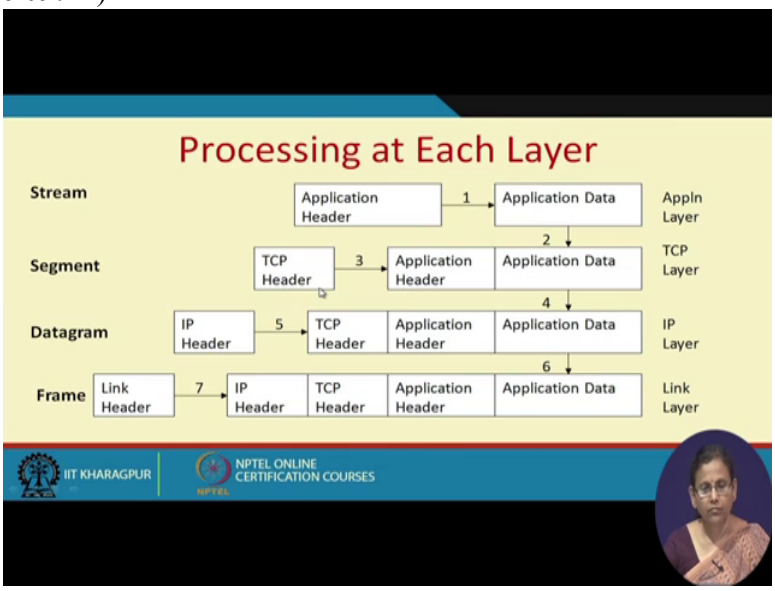
is for the application layer. So the activities are fairly the same. The link layer, they provide access to the physical part of the network. I mean it basically connects the physical network with that of the upper layer network. Then network layer is responsible for forwarding the packets in right direction. Transport layer provides end to end transport service between 2 hosts and application layer provides a special application like that of your H T T P and all.

(Refer Slide Time 08:27)



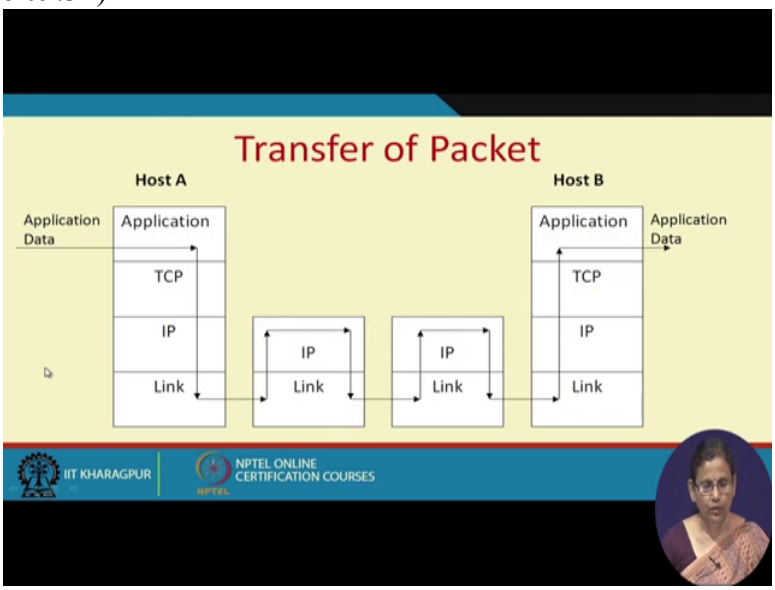
So if you compare this T C P/ I P and O S I model in right context we can see, in T C P/ I P, T C P/I P here in the network layer, in the data link layer it has some logical link control protocol and medium access control protocol, and physical layer is not a part of this T C P/I P then in the i p layer it has 2 protocols, Internet Protocol and A R P Protocol. Then in the transport layer it has T C P protocol and U D P protocol and there are many protocols which are in the application layer. So if you look at this, in all these application layer protocols of T C P/ I P this corresponding session layer, presentation layer and application layers are put together.

(Refer Slide Time 09:24)



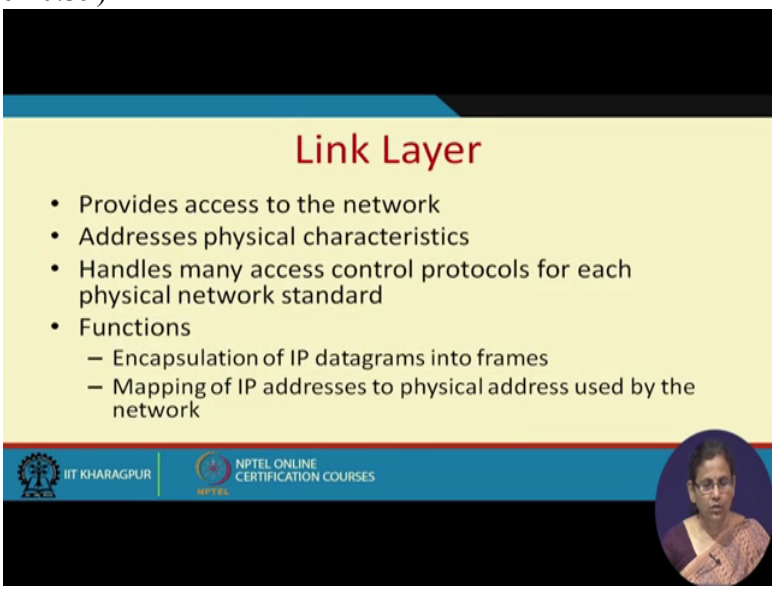
Now when the data passes through,

(Refer Slide Time 09:31)



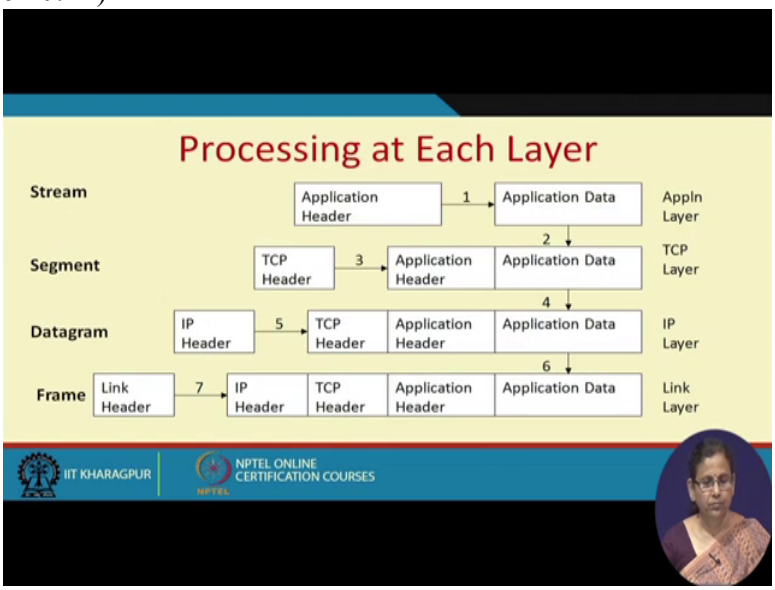
first of all, let us look at this. When the, from host 1 let's say your company server, your data packets are sent to the host B that is your client or may be it may be another server, the application data is sent through all these layers, each host will be having all its T C P/I P layers however when the data passes from the server, how the data goes? Data goes from server through various routers; it will be reaching the final destination. So these routers basically implement only the lower 2 layers of T C P/ I P and the data packet comes here, it goes through a number of routers then again it passes through all the layers in the receiving host then the application data which was sent from here gets regenerated at the host. Now,

(Refer Slide Time 10:39)



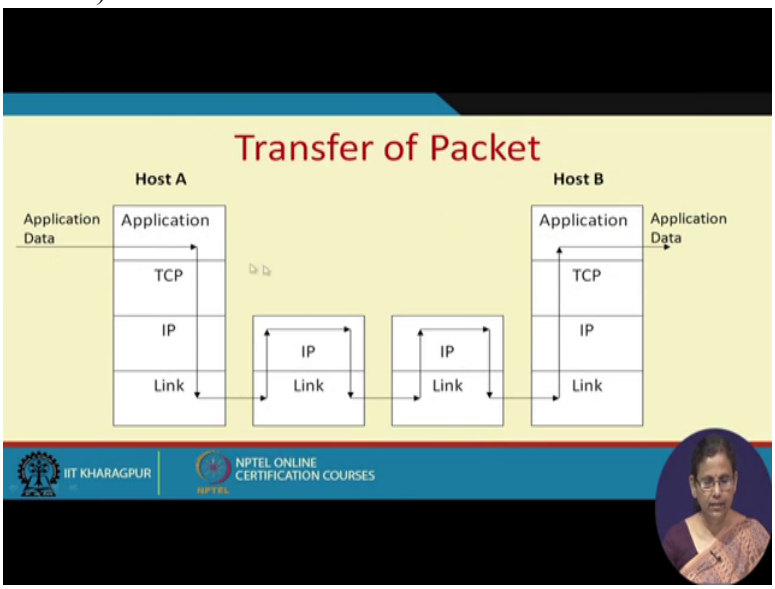
now

(Refer Slide Time 10:41)



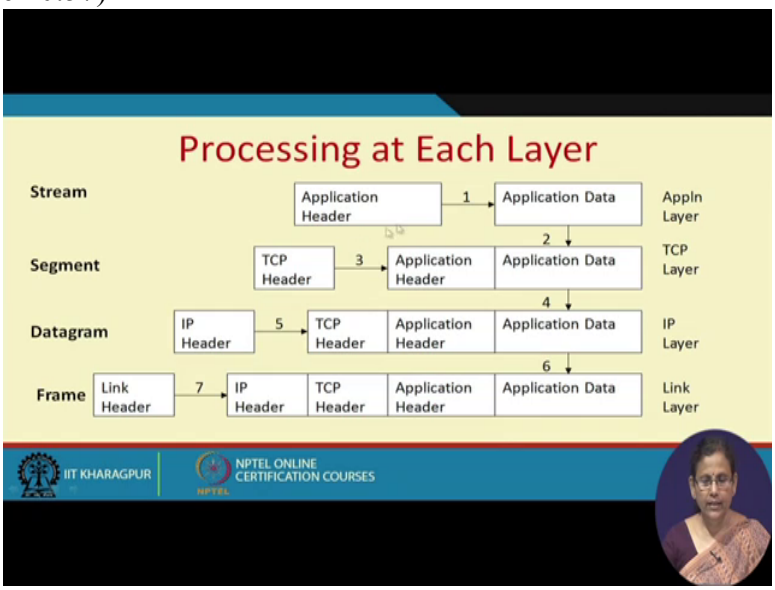
for making this transmission possible in the right manner, while the data passes from application layer to the lowest layer like here,

(Refer Slide Time 10:54)



from application to the lowest layer,

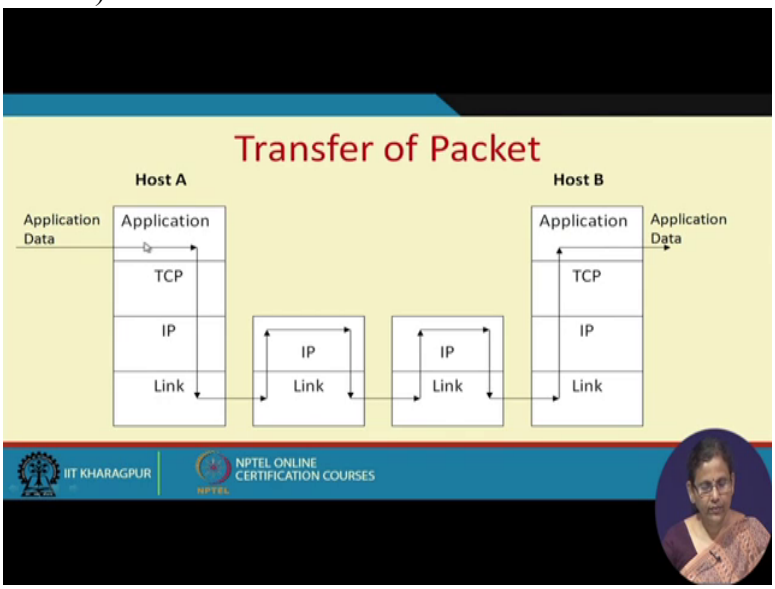
(Refer Slide Time 10:57)



each time some header is attached with the data. At the application layer, some application header is added. After addition of the application header it is called the data stream. Then after that, in T C P layer, again along with the application layer header, some T C P header is added. Then it is called a data segment. After that along with these 2 headers, one I P header is added. Then it is called I P datagram at I P layer, at Internet Protocol layer. Then in the next layer, in the link layer along with these 3 headers I P, T C P and application headers, one link header is attached.

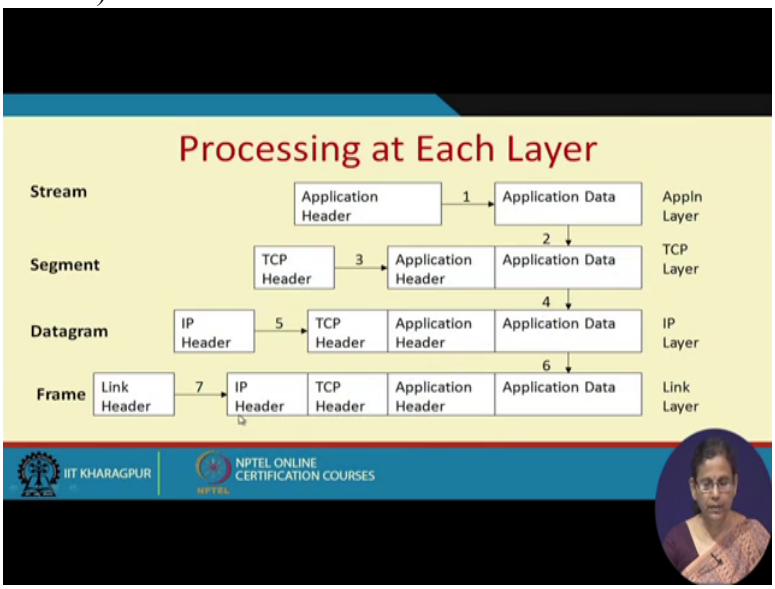
So when

(Refer Slide Time 11:45)



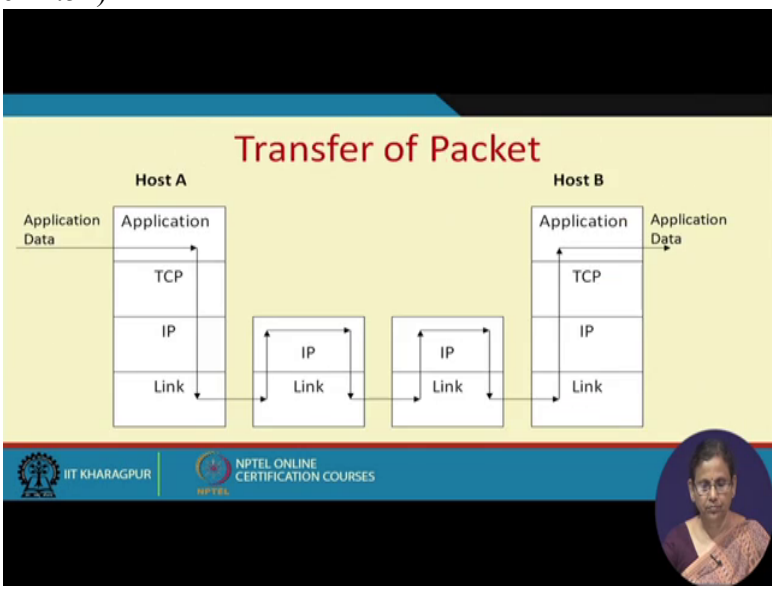
the data passes through all these layers, each layer some header gets attached. And when it passes through the router, the last 2 layers that is the link layer and I P layer, those are, those headers are removed and checked. By checking those headers, those headers contain the addressing details. So seeing these addressing details your router can now route these data packets. Again when it reaches the final host, because I P layer contains I P address which is unique for each machine, once it reaches this, this point the host B, each of the layers gets removed, each of the additional header which added gets removed and finally you get the data. By this

(Refer Slide Time 12:37)

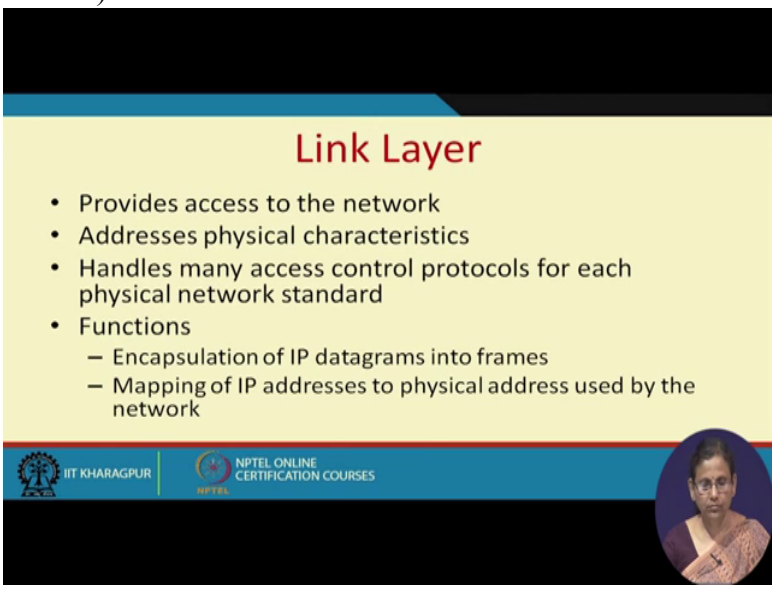


I mean when you again go up first at the link layer, this header is removed. Then at this layer I P header is removed. At this layer T C P header is removed. And application layer, application header is removed. So this is finally, this application data reaches the host.

(Refer Slide Time 12:54)



(Refer Slide Time 12:55)



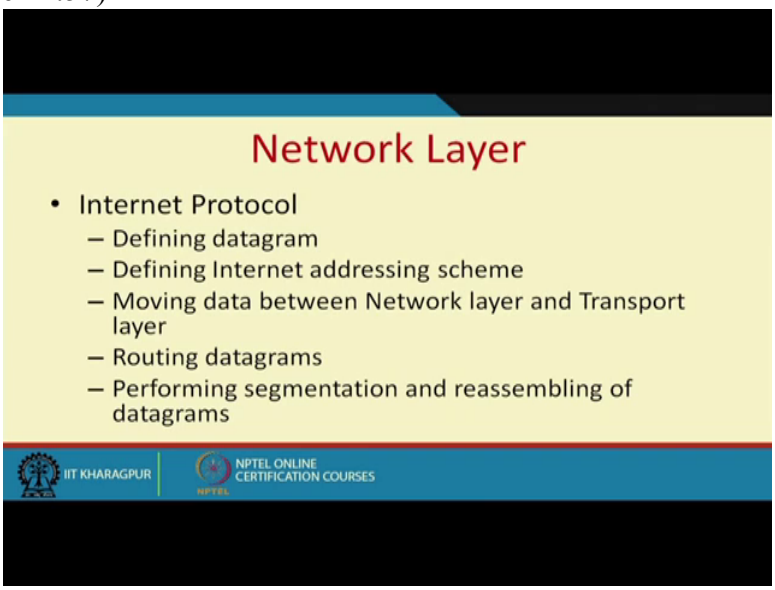
So let us look at the typical activities at each layer. This link layer provides access to the network. It addresses the physical characteristics of the underlying physical layer. Physical layer can be

(Refer Slide Time 13:19)

coaxial cable; it can be some kind of optical fiber cable. So what kind of protocol, how to handle this individual physical layer components and what kind of protocol will go for managing it is taken care of by this link layer. Now it handles many access control protocol, each protocol, for each of the physical network standard. Now what are its functions? The encapsulation of I P datagram in frames; by encapsulation of I P datagram we mean that when the data comes to this layer from the sender by this time, 3 headers have been already added. One is application level header. Second one is your trans, T C P header and I P Header. So with all these 3 headers it is called a datagram. It is called an I P datagram. So it encapsulates this I P datagram by adding one extra header. Then it is called a data frame. Now mapping of I P address to physical address is taken care of by this layer. Because again though I P address over the internet when you communicate with I P address, you are uniquely identified within a specific network, each computing device has its physical address. So there is some mapping between these physical address to I P address needs to take place.

Then in the network layer, you have one protocol

(Refer Slide Time 14:57)

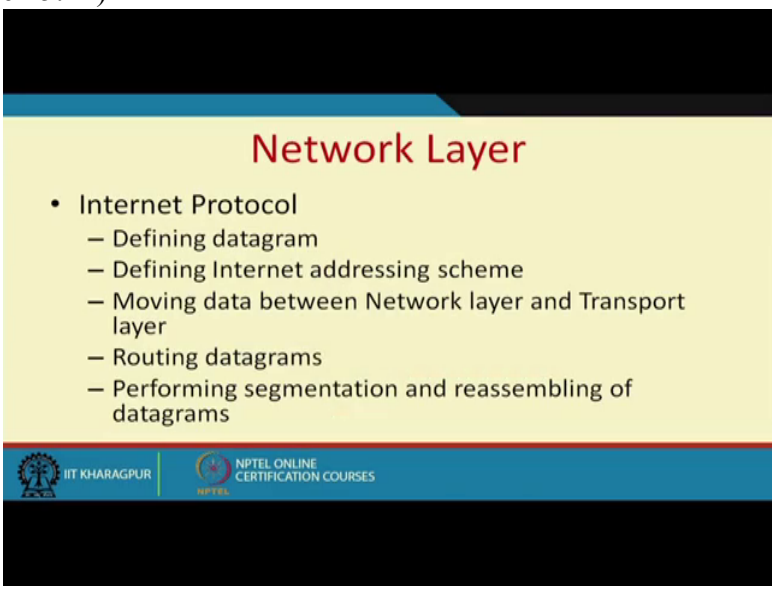


which is called Internet Protocol. This Internet Protocol as we have seen, this defines a datagram. By datagram we mean, the applic, the data that the sender is sending plus application header plus T C P header plus I P header. Taking all these 4 things together, we have, we define a datagram. Now this defines the internet, this layer defines the internet addressing scheme. Now moving the data between network layers and transport layers is the responsibility of this protocol. It helps, the network address that

(Refer Slide Time 15:36)

is attached here helps in routing the datagram. Now performing

(Refer Slide Time 15:41)

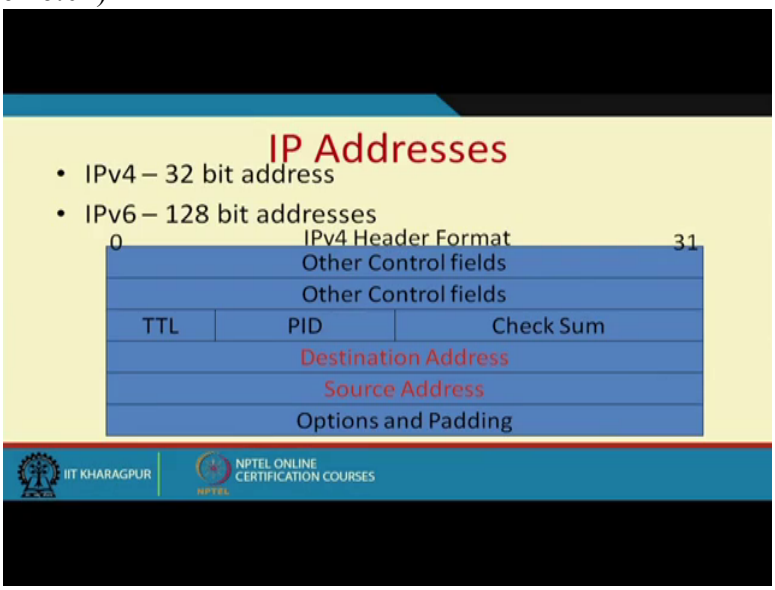


segmentation and reassembling of datagram,

(Refer Slide Time 15:44)

while sending from, sending from the sender, while getting from the sender and receiving at the other end, these activities is carried out in this layer.

(Refer Slide Time 16:01)

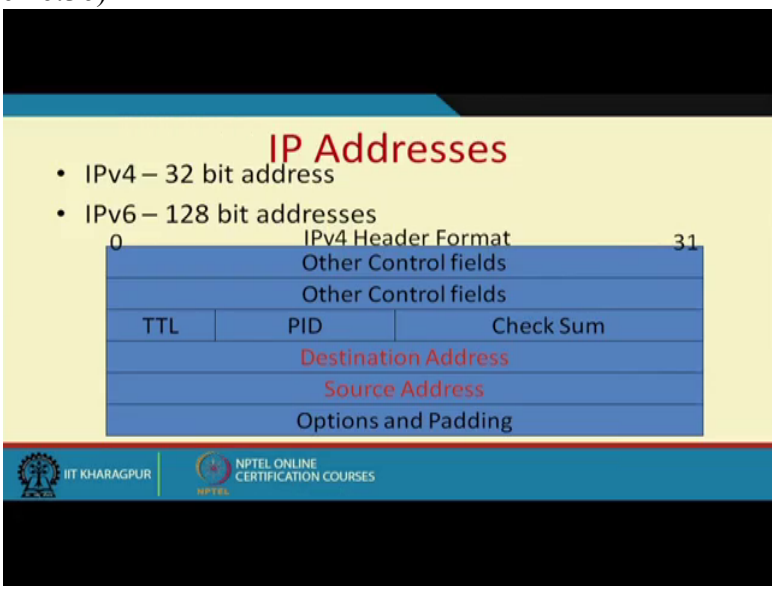


This is a typical I P address format. In fact I P addresses, there are 2 types of I P addresses. One is your I P v 4 which is the older format, which is a 32 bit address. Then you have I P v 6 which is a 128 bit address which is a newer form. In fact this I P v 6, the number of bits are 128 and it is so large that a large number of computing devices

(Refer Slide Time 16:29)

can be attached now to the internet. Then we have

(Refer Slide Time 16:36)

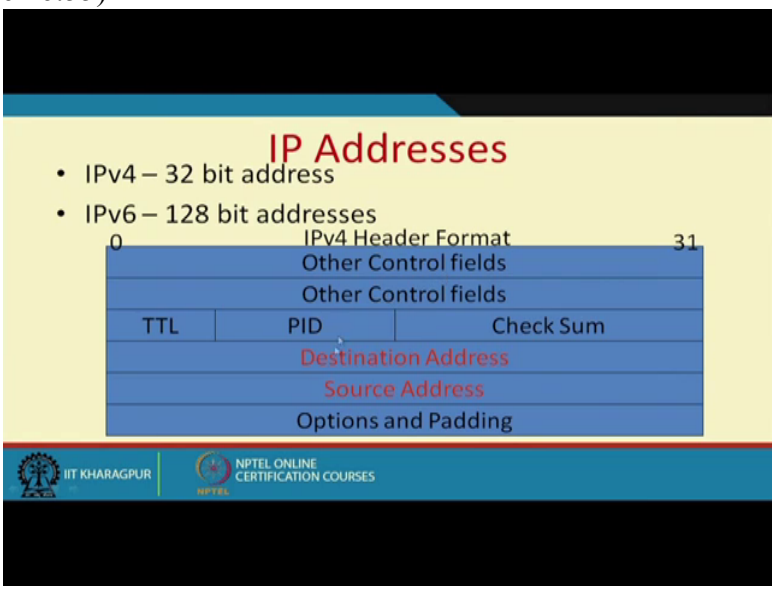


this I P v 4 format in which there are many fields. So though, because we are not going to discuss about details of this I P et cetera, but at least, at least 2 things I would like to let you know about here

(Refer Slide Time 16:54)

is that

(Refer Slide Time 16:55)

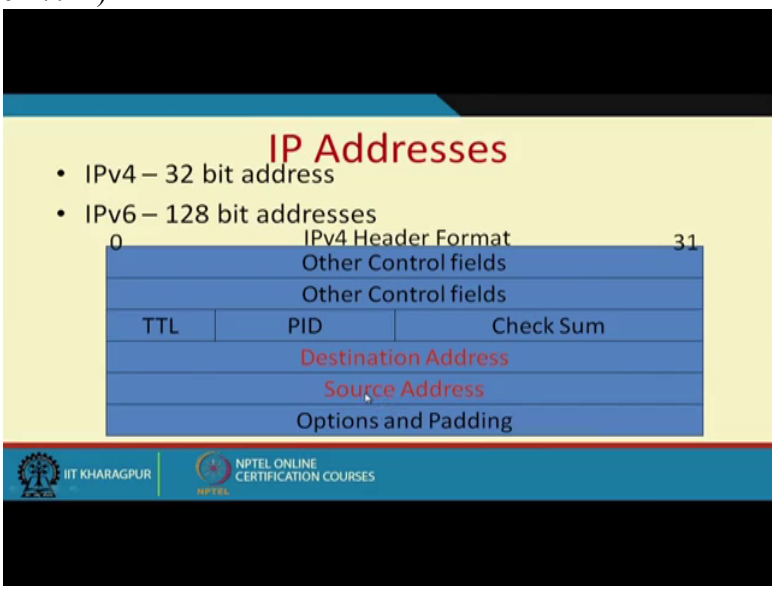


this contains this source address as well as destination address. This source address contains the I P address of the source

(Refer Slide Time 17:05)

and destination address is the I P address of the destination. So the routers, when

(Refer Slide Time 17:12)



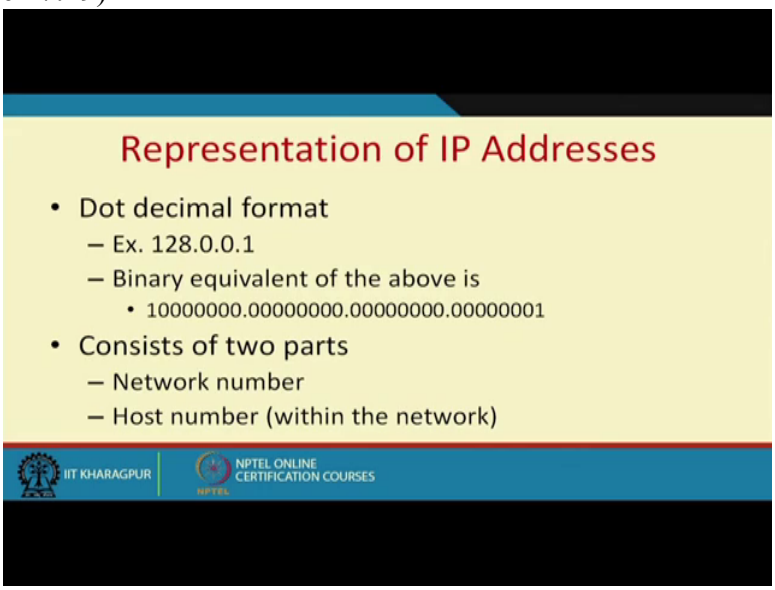
the data packets are sent, the routers in between know it is going from which address and it is going to which address. If you look at this, here each of this, the source address as well as destination address

(Refer Slide Time 17:28)

I P address are of 32 bit, 0 to 31 so they are all 32 bit each. So therefore we say that I P v 4 is a 32 bit address.

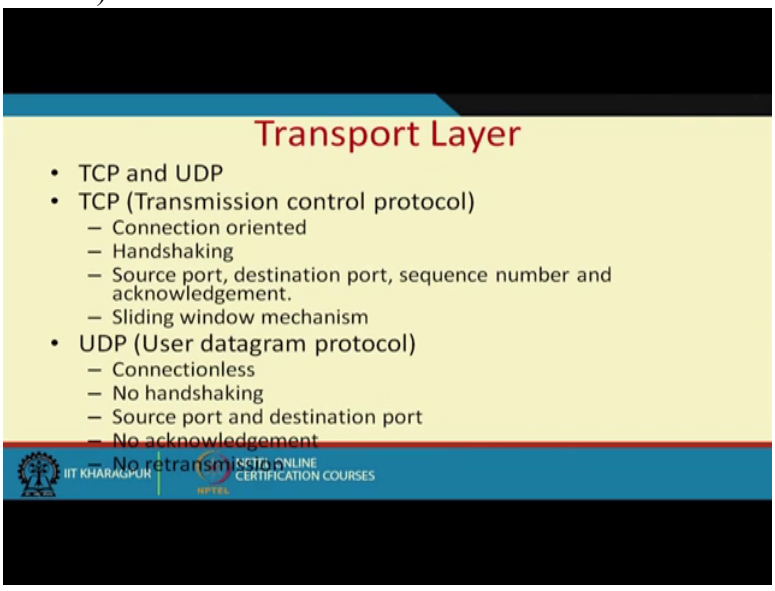
Now when in last class we discussed that this I P addresses every

(Refer Slide Time 17:49)



system in the internet are uniquely identified by its I P address and the converting this I P address to corresponding domain name is done by Domain Name System. Now this I P address in a dot decimal format has a form consisting of 4 parts. It is a 32 bit address so, 8, 8, 8, 8; 8 bits on each so it is a, it has 4 parts, 4 8-bit parts. So it, a part of this thing within the I P address is treated as the host number and the part is treated as the network number and accordingly the network's structure, local network is decided.

(Refer Slide Time 18:42)



Now this coming to to this transport layer; in transport layer we have 2 protocols T C P and U D P.

T C P which is called a transmission control protocol is a connection oriented protocol. It relies on hand=shaking for maintaining the end to end connectivity Then it has this source port, destination port, and sequence number and acknowledgement sent within its header, within its header so that corresponding, the connectivity between the corresponding sender and receiver can be maintained. It uses a sliding window mechanism. So now let us try explaining these terms in a more lucid manner. As I have told

(Refer Slide Time 19:39)

you this internet is actually a connectionless, H T T P is actually a connectionless protocol which means it does not maintain the state. So if you look at the T C P/ I P protocol stack, above T C P you have H T T P. So because H T T P is stateless, how does the, when you send the data in data packets and make it into small, small groups how is it possible that H T T P can, I mean the, when you send the data packets to the other host all of them are put together. Now let us try to understand the process of making this connectivity possible.

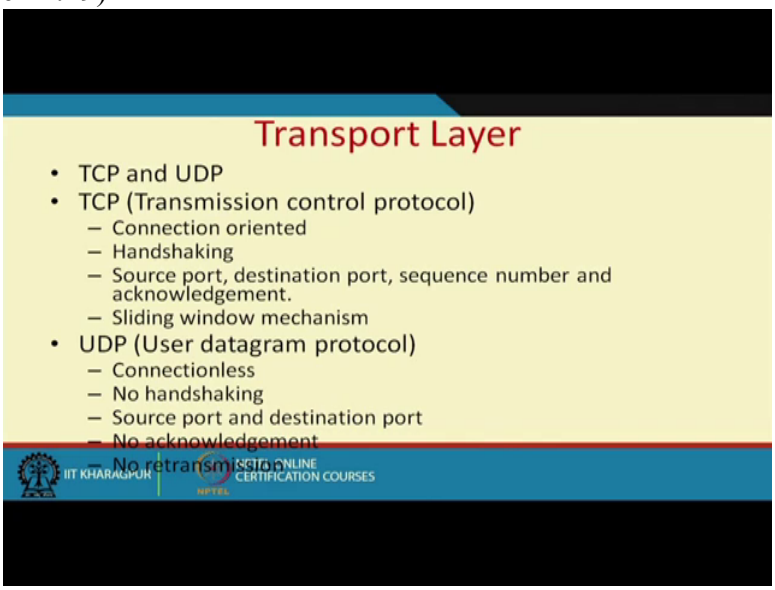
See internet is a connect; it is a packet switch network. There is no connectivity like a telephone network maintained between two hosts. So and moreover there is one more problem can happen. For example in your machine, you have opened 2 browser instances, in or that way, two tabs in the same browser. Now from one tab or one of the browser instance you send some request and second browser instance you send another request for another web page. So whenever these responses come, that the web pages come they come to the right tab or the right browser instance. So how does it happen? Each computer is uniquely identified, that's fine but within that computer there has to be some mechanism again which can identify

this individual web pages which are coming to different browser instances. So here this concept of port comes in. Each browser instance is associated with a different port number. So even if you send from the same computer, from two browser instances even if you send, when you send 2 requests, they not only come to the same machine but they also come back to the same browser instance. So this is the role of the port. So each application, networking application running has a unique port number associated with it.

Now let us try to understand the meaning of handshaking and how connection is maintained. Connection between the, the sender and receiver is maintained through handshaking. Now through handshaking as the name indicates, first the source, the sender sends a message to the destination to find out whether the destination is active or not. Then if the destination is active then the destination sends back a response. It shakes the hand. Then the source once again confirms that it knows the destination is up and tells the destination that it is going to send the data packets. Then the data packet, then afterwards the destination is prepared that some data packet is coming from such and such source so data packets keep coming.

Now as we have already told last class, internet is a best effort delivery network. That way every packet switched network is a best effort delivery network, which means due to network congestion, if some of the data packets are lost it is not, network does not take any responsibility for that. It is the responsibility of the host to resend these packets. Now the question is how the host will be knowing that data packets, some of the data packets are lost. So for that purpose a sliding window mechanism is implemented in

(Refer Slide Time 24:29)



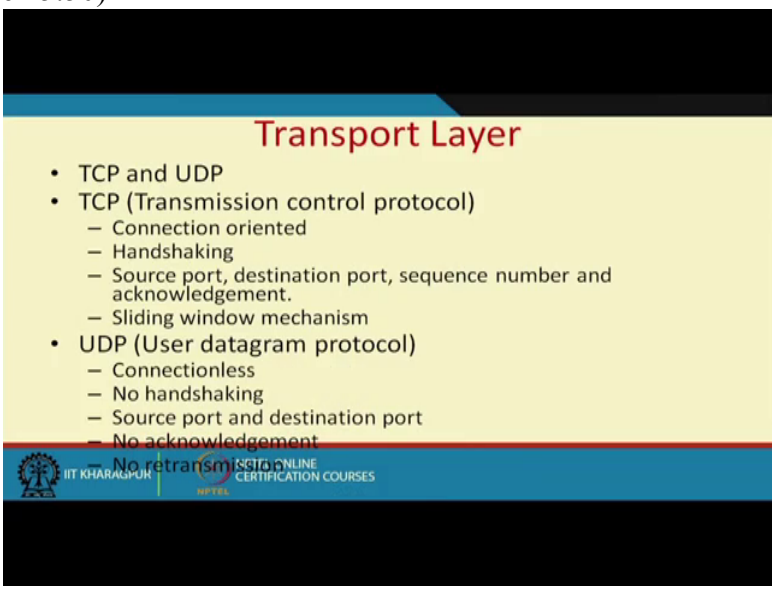
T C P. So in a simplistic manner this sliding window mechanism is the one in which the, because

(Refer Slide Time 24:45)

once the sender sends some data packets it will be receiving some acknowledgement from the receiver. So from the receiver, receiver's acknowledgement it can realize up to what number of data packets it has received. So if it finds that, it waits for some time and if it finds that for certain number of data packets the response is, the acknowledgement is not received then it immediately sends another chunk in a sliding window manner. And first 10, next 10 and if something is not responded then again it goes back and starts sending from the one for which the acknowledgement is not received.

Now this process though helps in making the connection possible between 2 resources, 2 hosts because of this handshaking and maintaining connection

(Refer Slide Time 25:50)

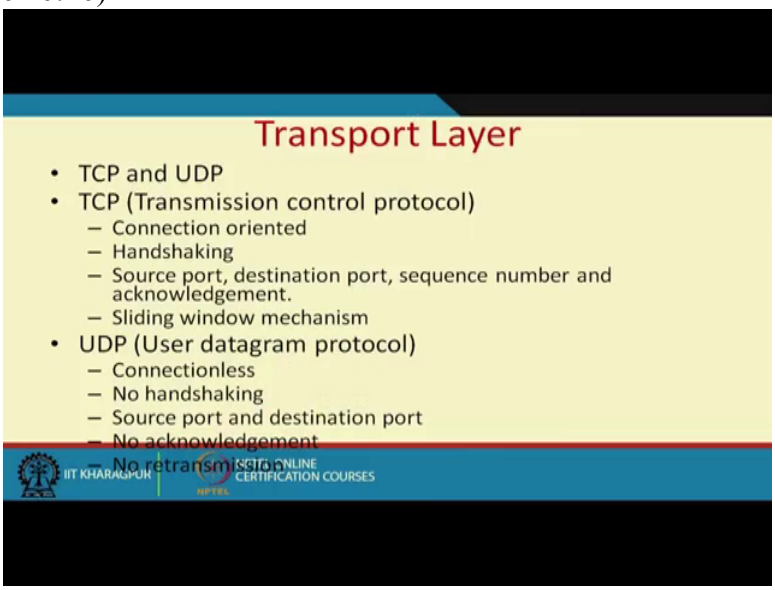


it is a bit slower protocol. Correspondingly there is another protocol in the transport layer which does not make this connection possible.

(Refer Slide Time 26:04)

So this particular protocol is called User Datagram Protocol. So this is a connectionless protocol. This does not waste time in handshaking. It has

(Refer Slide Time 26:16)

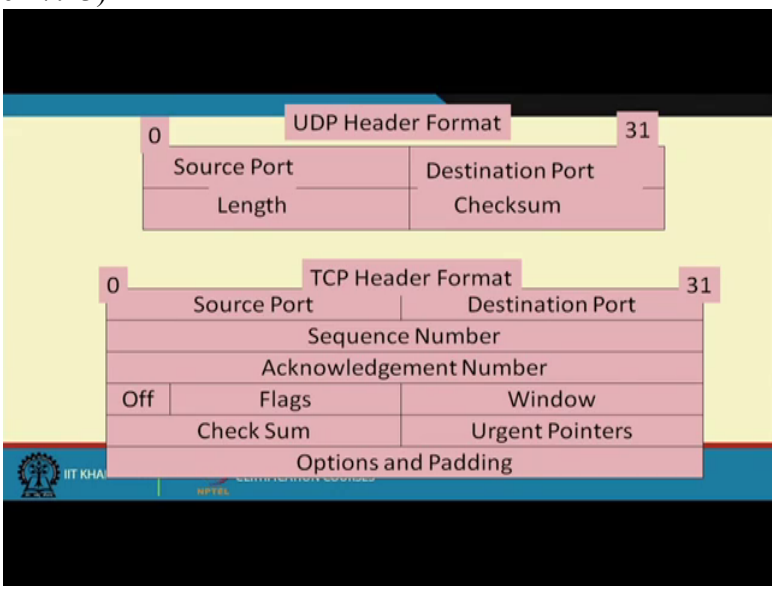


this source port and destination port attached with its header so that packet can be routed in the right direction and reach at the targeted application.

(Refer Slide Time 26:30)

It does not send any acknowledgement but it is fast. So while sending the data where the sequence need not be maintained or if a part of data is by chance lost, it can be managed then U D P is used. Just imagine that a big map is being sent. Or some huge image file is being sent. If the image file is little blur because it has not all the data packets related to the image file is not received then it is acceptable but if some text message is sent and a part of text message is missing then it is not acceptable. So you can understand what is the implication of T C P and U D P.

(Refer Slide Time 27:23)

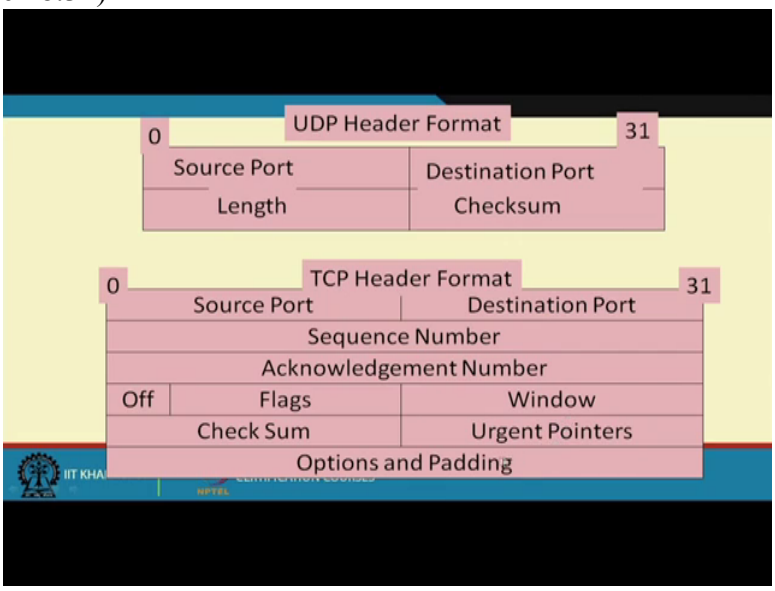


This is a typical T C P and U D P format. Here there are again many, many elements, many header elements but what we are actually talking about so far, it is the source address and the destination, source port address and destination port address which, after the data packets reach following its I P address, it reaches the right host. It is targeted to the right application. Then this sequence number is very important because you are sending the data sequences and it is the responsibility of the T C P to see that, to maintain the connection, to see that all the packets in the sequence are reached at the destination. And this acknowledgement number is something which comes back from the receiver telling that what all has been received so far. Then there are

(Refer Slide Time 28:28)

other controlling header

(Refer Slide Time 28:31)

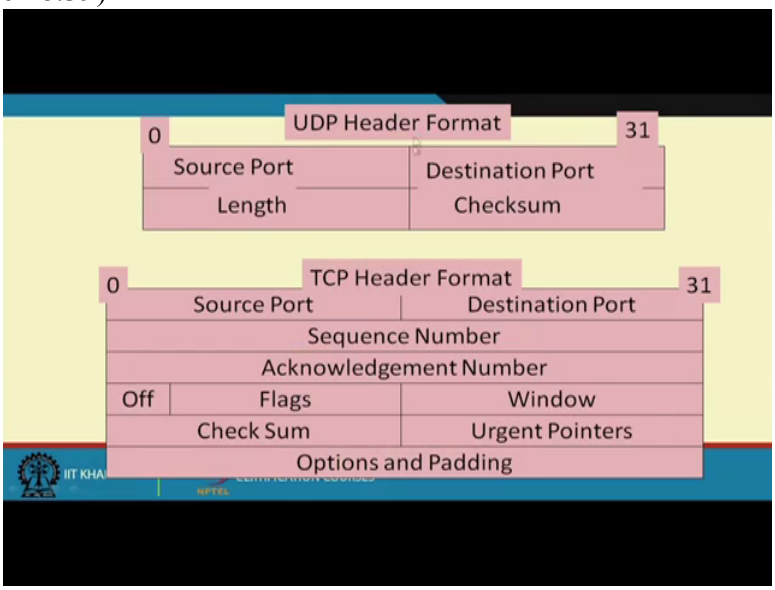


elements which we are not going to talk about but if you look at

(Refer Slide Time 28:35)

this U D P format what is missing here is this

(Refer Slide Time 28:39)



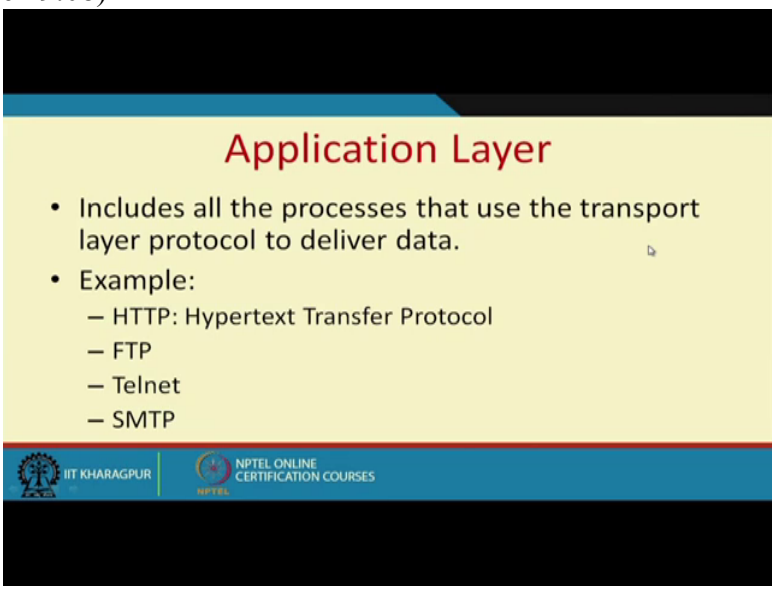
sequence number and acknowledgement number. But the source port and destination port is there so it is ensured that the if at all the data reaches at the receiver, if it is not lost in between definitely it will reach the right application. But if something is lost in between, this sequence number and acknowledgement numbers are not maintained so it is not the responsibility of

(Refer Slide Time 29:02)

U D P.

Then next layer is your

(Refer Slide Time 29:08)

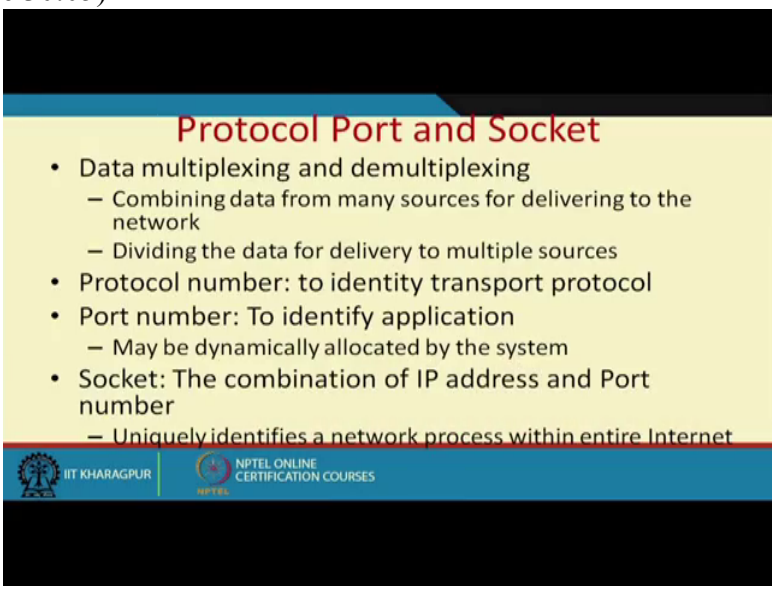


application layer. One of the application layer protocol we have already discussed about H T T P which is a stateless protocol. There are other application layer protocols as well like F T P, Telnet, S M T P et cetera. We are not going to have a lot of discussion on them because we are mostly interested in the H T T P protocol and sometimes possibly F T P for large file transfer et cetera.

(Refer Slide Time 29:32)

Now as I was telling you, each host in the network is uniquely identified by the I P address and each application within the host is uniquely identified by corresponding port. So if we put this port number and I P address together

(Refer Slide Time 30:05)



we call it a socket. A socket is a combination of I P address and port number. So your protocol number, besides this you also have the protocol number to identify the transport protocol, you have port number to identify the application and along with I P address your, once the request is made from the host, from a specific client or the browser instance it reaches the destination and the response is sent back to the right application, not only to the right host, to the right application as well. Thank you very much.

(Refer Slide Time 30:44)