Communication Networks
Prof. Goutam Das
G. S. Sanyal School of Telecommunication
Indian Institute of Technology, Kharagpur

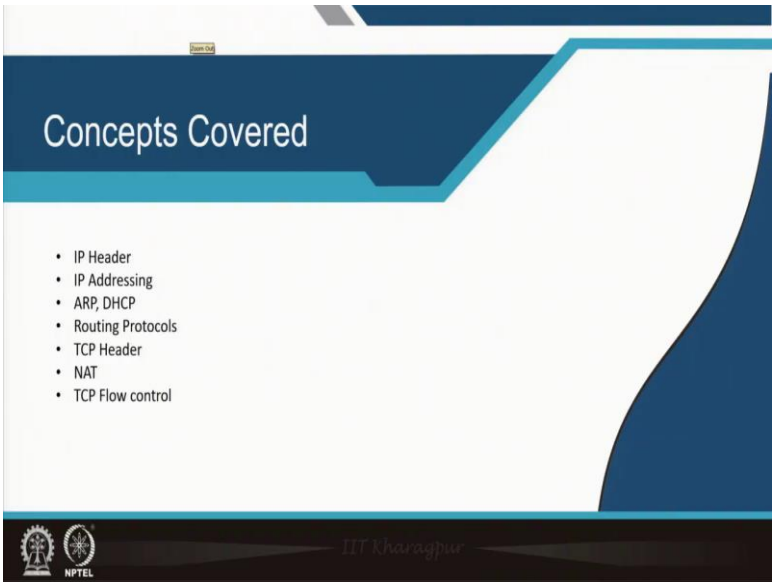
Module - 12
Network and Transport Layer
Lecture - 54
Internet Protocol

So today we are going to discuss about means we have finished our discussion of this DLL. So, now we will start discussing about other two layers of networking which are the Network Layer and Transport Layer which should be the end of this particular course.

So, we will try to see today it means we will be mostly concentrating on the IP layer the associated protocol, and how it helps in transferring packets end to end. So, that is something and it is the philosophy of course, and then we will start thinking means making decisions about how these two layers of DLL we have talked about that interlayer communication.

So, how DLL layer and IP layer work together toward some unified goal? So, that is also something we will try to see and we will try to see how these two things together along with a physical layer of course, actually do the whole networking. So, that is also something we will try to depict.

(Refer Slide Time: 01:30)

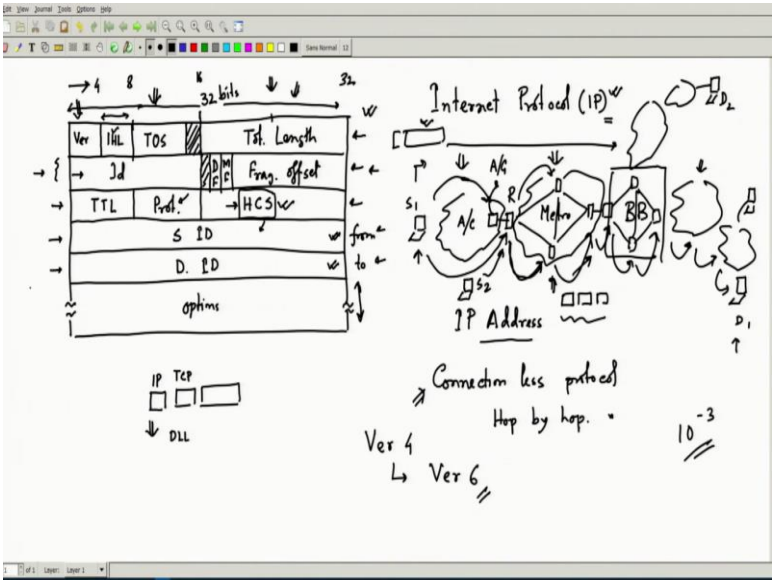


So, if you just try to see the topics that will be covered in this particular week. So, one will be the, of course, IP header, then IP addressing that is very important then this ARP, DHCP that is about address resolution kind of thing, and then some routing protocol. So, that should end our discussion about this network layer and then we will go to the transport layer.

Mostly we will discuss TCP which has been the predominant transport layer protocol probably and then we will discuss something about NAT which is again the interplay between the transport layer and the IP layer. So, we will talk about that also and then finally, we will end our course with the TCP flow control which is one of the most important parts of TCP actually the transport layer part.

Not only flow control there will be also congestion control and how TCP provides reliability on top of the IP datagram network which is not reliable which is hop by hop. We will start talking about these philosophies later on.

(Refer Slide Time: 02:27)



So, if we talk about this IP we have already talked about what is actually called the internet protocol or IP. This is layer 3 which is the networking layer that is responsible for delivering data from one particular address to another address or one particular destination source to another destination.

So, that is this layer's duty we have already talked about every layer has it is own duty like the data link layer which is actually the access part. It means we have already talked about that it is a duty somehow if the access is common. Then among multiple contenders, how do we resolve those contentions and how do you actually give meaningful transmission in the access part of the network?

Now, this internet protocol actually joins everything in the entire network end to end. And then it actually means thinking about delivering whatever you want to generate in any source of the network and then to the other part where the destination lies. So, we will try to see any protocol that is described we have seen that it is all about the header you add the header, and associated with that there will be some task.

So, over this particular protocol, we will try to understand how the header helps to do specific tasks and what are the specifications over there. And each node reading the header how they can decide things and what are the other things, they do on top of that header ok. So, that is something we will try to see.

So, their task with along with header and how this header specification, header reading, and header writing and this performing the associated task how that generates the whole networking task as a whole ok. So, before going into this protocol let us try to see what exactly is required from this protocol. So, that is something first we will try to describe. So, suppose what has happened is you have a network where this is the source node ok?

So, there is an access part of the network. So, let us say this is connected to some access part of the network then that will be again going and connecting to some metro part of the network. So, let us say this is the metro and then it might have the backbone. So, the backbone network then you can have another metro followed by access and then the destination node ok.

So, now this source node wishes to communicate to this particular destination node right. So, what will be happening in the access part of course, there will be some let us call that access gateway ok? So, this might be our if it is a wireless axis this might be the access point if this is Ethernet. So, whatever if there is a final switch that is connected to Ethernet that might be that switch ok.

So, followed by of course, it will be connected to the metro with a router we will talk about this router. So, far we have talked about these switches, but we still have not talked about these routers routers are those devices that actually operate up to layer 3. So, it goes beyond the DLL layer, it can read the header of the IP layer or the network layer ok.

So, there will be an associated router which we can call the means metro edge router or something like that. So, it is actually the gateway to the metro and after that, there will be multiple routers in the metro that will be interconnected through some form of networking and then there will be in the backbone.

There will be again means metro router that connects it to the backbone again backbone might have it is own networking which are all routers of different dimensions. So, they will be connected with some form of networking and it goes on like that. So, basically whenever we are talking about sending data from this sender to this destination what we will have to do is something like this generally all these sender destinations will have a unique ID which is called the IP address this has to be globally unique.

So, that is something that we will be putting in the header source ID and destination ID we will talk about that. So, the IP address is something that has to be unique like our earlier telephony number. So, this is something that has to be unique and every source and destination will be given this unique number. So, globally unique even though you will see later on when we will be discussing NAT it might not be always unique. So, that is something that might be locally unique, but might not be globally unique, but that is a different story ok?

But generally, our understanding is this source and destination have unique IP addresses, and with these IP addresses, we know they are means where are they located in the network ok? So, that is something that will be with this address only it is like a postal address. So, basically, if you give that address then that letter will be delivered like this here also this packet if you give that address it will be delivered.

So, in the place of address, you have to and from. So, this source ID is from part of our mailing and this destination ID is this 2. So, who is sending and to whom it is being sent that is being encoded inside the packet header? So, the header specifies this that has nothing to do with the datagram whatever you will be having actual data you append this.

So, that you know who is sending it and to whom it has to be sent ok? So, whichever destination you choose you choose that IP address. So, that is all you will have to do once you do that this internet protocol is a hop by hop or it is called a connectionless protocol or it is also called hop by hop protocol. What does that mean?

Now, this particular data has to be transferred to this destination, but directly it will not be done that way what will he will first give it to this router, this router, then decide which next router it has to go that is why it is called hop by hop. So, the source does not know about the destination he just puts this destination ID and he forgets about that he tells the network to do this entire forwarding ok.

So, basically, what he does is he just delivers this packet to the next hop and he is he washes his hand from this particular packet he does not care about this packet right now. So, inherently this does not have any reliability you actually do not know whether the packet will be delivered you are just hoping the network will somehow deliver this packet.

So, your duty is just to give it to the next router the next router also duty is not to deliver the whole packet to the destination he will also do the same thing he will just deliver it to the next router. So, it will just keep on going. So, like this, it will keep on happening, and then finally, it will reach the destination that is why it is called connection-less protocol because you do not establish any connection between source and destination that also helps us in terms of you if you remember at the beginning of this course.

We started discussing about this circuit switch network and packet switch network this is packet switch network. So, therefore, we do not really create connection end to end connectivity we do not create what we create we only think about the next hop and the next router. We think that he will be intelligent enough to route it to the next destination which will be closer to the destination.

So, that is in some manner ok conceptually it is closer to the destination. So, distance it might be closer to the destination, or delay it is closer to the destination. That means, if I forward this packet to this router instead of this router I will probably reduce the delay overall delay of the packet delivery.

So, they intelligently do just these things every router is concerned about his own hop, not the end destination and somehow in a distributed fashion, they do a very nice job. So, for every package that is being routed at the same time what might happen is there might be another station which is another source he might be looking for another destination connected somewhere it might be also connected over here. There might be another metro access followed by another destination.

So, it might happen that he wants to now source 2 this. So, if source 1, destination 1, and source 2 want to send it to destination 2 this might also happen. So, if that has to happen these 2 packets simultaneously will be routed. So, as you can see this router will handle both the packets ok. One packet will come from here another packet will go from here.

So, both this packet he will handle and then accordingly he will decide because both the packets have unique IDs the source ID and destination ID are not the same. They have different ID seeing those IDs somehow routers will be rooting them to the next hop in an intelligent manner. So, that if you take all these routers decision finally the packet will be correctly delivered to the destination.

So, that is why it is called connectionless protocol it is, of course, it is part of packet switching. So, it does facilitate our statistical multiplexing very nicely because nowhere you are establishing a connection you are not putting a complete link you are not reserving anything.

So, you are just delivering to the next hop next router again putting them in a buffer, and then whenever there is availability they will forward it to the next router and every router takes this intelligent decision of where it has to forward. So, that it goes towards the destination that is the whole idea of IP routing ok?

So, that is why it is called connectionless protocol it has no reliability whatsoever I do not know if a source is transmitting a packet. I do not know whether the packet has been delivered or not if some router is faulty it might be clubbed over there it might be lost over there. So, you will see later on because this particular layer IP layer does not have any reliability.

So, we had to put another layer above that which is the TCP layer or which is a transport layer we will start putting reliability on top of it and that is why that will be more of a connection-oriented networking you will see that later on when we will be discussing about TCP.

So, TCP governs this reliability on top of a nonreliable IP transport sorry IP network layer protocol which is a hop-by-hop. I really do not know whether my packet is finally, delivered to the destination network keeps absolutely no monitoring about this that is the job of the layer above ok which provides this reliability.

We will when we discuss TCP along with IP and TCP. We will actually discuss why this philosophy has been proposed, why not some other philosophy, and why not providing reliability from the means network layer itself. Why this has been divided, and subdivided, why is this entire task of reliably transferring packets from one source to another destination and another source to their respective destination? Why this has been divided into two tasks; one is just delivering the packet and the other one is adding reliability on top of that.

So, that is something we will try to appreciate right now we know that these two layers do this together. But this has been separated out and the IP layer has deliberately taken

this connection-less protocol there are benefits of that we will talk about that later on. But we have at least understood what will be the philosophy of this IP packet forwarding.

So, this kind of packet forwarding is called store and forward. So, every router that it does actually store the packet in it is a buffer. So, whenever it arrives, it stores the packet in it is buffer then it reads the header from the header and the most important part it reads is which destination ID it is looking for.

So, where I have to send accordingly we will later on know that there will be a routing table which will be there in the router every router will have that from that routing table he will understand. What will be the next router he should forward this towards that destination? So, he can he can actually expedite the process of forwarding this packet toward that destination.

So, he will make a decision from his routing table on how he updates his routing table which is a separate issue which is the routing protocol we will talk about that later also. So, he takes that decision and then forwards the packet to the next hop that is all he does he does not do anything else. So, that is why it is called stored and forward, and of course, in between he takes that routing decision.

So, he stores the packet reads the header does the routing then there whenever the link is available he forwards that packet with the help of statistical multiplexing. So, that is exactly what every router does. So, every router will keep on doing that hop by hop and after a multiple number of hops, it will finally, reach the destination ok.

So, let us try to see how means whenever we define a protocol we have already talked about that there should be a header. So, how the header of IP which will be appended along with the IP data means whatever data will be given by the transport layer it will append this header on top of that data.

So, the application layer will give some amount of data then the transport layer will add the TCP header, and then the IP layer will add its IP header and then it will deliver this to the corresponding DLL layer of the same node. So, that is what will be happening. So, IP layer we will just add this header what are the fields of this header and what do they do

we will not go into the details of everything, but some of the things we will start describing over here. So, if you see this is a typical header that I have already drawn ok.

So, I have drawn this header of course, in a square matrix kind of thing, but it will not be like that it will be this is actually 32-bit. So, this part is 32-bit ok. So, I have subdivided it is actually 132 bit, 32 bit and the next 5 this one mixes the header there is an option field that we might keep we might not we will not discuss that due to the time crunch.

So, that is not that important also ok. So, I have shown it this way, but actually, it will be a bit stream. So, it will start from here like the television screen the way we scan that. So, it will go up to this 32-bit, and then it will again start from this side and it will go from this direction.

So, always it goes from this direction to this direction one row it picks then the next row then the next row like this it will be a series of bit streams for ease of demonstration we have depicted it in a square box kind of pattern ok. So, you understand what exactly is happening.

So, the first field which is actually. So, this is 32-bit this is actually a 16-bit mark. So, that is the 16. So, if you take from 1 to 1616 to 32 this is 8 bit mark this is 4 bit mark ok. So, if you see the first 4 bit specifies the version currently mostly IP version 4 is being used.

So, we are generally using version 4, but it has been actually upgraded to version 6 IP V 6 is already being used, but not everywhere still IP V 4 is predominant. So, we will talk about mostly version 4 version 6 is almost similar just enhancing some of the fields and it has a little longer header ok.

So, this version actually specifies which version we are taking for 4 there is a unique identifier 4-bit identifier and for an 8-6, there will be another identifier any future version that comes will have a different identifier. So, why does this version have to be specified it is again a very important philosophy of networking that whenever you upgrade your network from version 4 to version 8 6.

Let us say you always assume that some of the versions or some of the network tools or network components of that version are already there they have been used their serve

their purpose. So, suddenly overnight you will not be completely taking them away from the network and you will not be completely installing a new network this is not expected.

So, generally, networking development goes scale by scale or gradually it happens. So, basically, whatever is there overnight you do not throw the entire thing entire infrastructure that will be too costly. So, basically on that infrastructure slowly one by one you actually modify this. What does that mean? That means the interoperability and backward compatibility of these kinds of terms are very important or coexistence they are very important.

So, whenever you have a network it must have both things they must coexist if they coexist some of the things suppose IP version 4 is there all routers are of version 4 now you want to install a version 8 router F, and version 8 router in some portion of the network. You install them, but those routers will have the capability of reading both version 6 and version 4.

So, they will have the capability of both therefore, some of the IP version 4 packets that are coming from other sections of the network will be capable of reading that. But how do they discriminate these 2 packets that is where these particular fields come as handy. So, whatever will be specified over there if it says version 4 or if it gives the unique idea of version 4, then it will be version 4. If it is a unique idea of version 6 then it will be version 6.

So, remember whenever you are doing networking designing you will have to keep this in mind always. Keep things backward compatible keep provision for coexistence and whatever new you are installing that must be as I have said backward compatible. That means it should have the capability of the new one as well as the older one.

Because networking is all about everybody being able to talk to everybody else now you install a new network among a few users. Now if that is standalone then it will be an isolated island where those users only can talk to each other. Because the entire network protocol is an upgraded version and it cannot understand the earlier version then you have a big problem. Because you are creating an island and it cannot communicate to anybody else that is not the purpose of networking. Networking has the purpose of providing communication between any user any two users should be able to freely talk.

So, therefore, whenever you do this networking upgradation that is for your own purpose, but the user will not understand that they only need connectivity. So, you have to provide this backward compatibility. So, that is why as you can see from the header people have started thinking about that record compatibility. So, that is why that version field has been specified.

So, any packet that is coming with version 4, so will have a version 4 identifier at the beginning. So, any header IP header that is being read first will read the version according to that version reading whatever unique ID they will get. If it is version 4, they will read the entire header according to the version fare 4 protocol or specification. If it is written as version 6, they will read the entire header according to version 6 specifications. So, this is how they will discriminate between version 4 and version 6.

So, the next field again another 4-bit field which is called IP header length. So, there this is happening because I have put these options ok. If the option fields are varying then the IP header is no longer a fixed header even if it is version 4, it might not be fixed. So, that is why I have to specify the header length.

So, those 4 bytes will be able to specify how many option fields I am padding over there and what is the overall length of the IP header. So, whenever I read this IP header, next by reading this IP header length he will be able to calculate how far the header is there and where the actual data starts this is very important. Otherwise, I will not be able to know where the header ends and where the data field actually starts.

So, therefore, that has to be specified after that there is a type of service this is for priority IP has specified different kinds of priority classes there is a dip serve integrated service. So, different kinds of priorities have been provided so that different classes of traffic like voice video and all kinds of other classes can be handled for the time being. We will skip this part that is we will not be taking our focus into that particular part that is a big discussion again about how IP provides this priority or class of service and how it handles those things.

Next is the total length it is 16 bits ok. So, with this 16-bit, we specify what will be the total length already we have specified the header length over here. But this is header plus data what is the length? Because when IP packets are coming we will be seeing a bit

stream we do not know exactly where the header starts and where the packet will be ending.

So, from starting point to find out the ending point we need to really know what is the overall length of the packet. So, this particular byte specifies for this particular packet whichever packet I am appending this header what is the length of that. So, this is because I have a total length field so; that means, that and IP datagram can be of a variable size it does not have to be fixed I can specify whatever length I want to put and accordingly the length will be put ok.

The next 32-bit filled the next row, this is all about fragmentation. So, this is something we need to discuss IP data sometimes might happen it might go through some of the networks where it cannot handle very long packets ok? So, if you have a wireless link if you give a very long packet. Then what might happen most of the packet will be erroneous because the bitter rate is not that low it might be of the order of 10 to the power minus 3. So, for every 1000 bits it might have an error.

So, if your packet size is too big then most of the packet will be erroneous you will be just wasting time retransmitting. So, if there is a means wireless link in between and IP works on that remember IP layer works on top of the DLL and physical layer this DLL physical layer can subside or can hide what particular media layer is operating underline.

So, IP can operate in different kinds of media layers. So, this networking that I am constructing it might happen that the first part is wireless second part is let's say fibre optic third part might be or some third part might be a satellite. So, all kinds of links can come, but IP will still operate on top of them. Because it abstracts all those layer-specific details in the physical layer and data link layer.

So, the physical and data link layer will hide all these things IP layer can operate on top of that only thing is that I need to know if the layer is not that reliable. Suppose it is it is basically the underlying layer is wireless media then it is not that reliable. So, the IP header length has to be restricted. So, this is something which we will be doing over here ok because sometimes it might be restricted.

So, it might happen that in that particular layer I have a big IP packet coming I might have to fragment that packet into smaller packets this is something in between routers

can also do. So, basically source gives a packet a big chunk of the packet with an IP header and all those things then the in-between nodes might decide ok this particular packet has to be fragmented.

So, he makes smaller fragments and then delivers them. So, that it becomes easier for him to deliver it without error or he does not have to do too many retransmission. So, he does that and of course, it will be length at the end it will be again defragmented. That means, one of these packets will be again added together to construct that original packet.

So, this fragmentation and defragmentation that is being handled over here we will talk about a little bit more detail. This is the error control. So, this will tell you whether the packet and the packet header are ok. So, this is sorry not per packet for the header whether the header is erroneous or not because if the header becomes erroneous 1 bit of the header becomes erroneous. Then you do not know whether you are doing the right thing or not.

So, suppose one bit of the destination ID becomes erroneous then you do not know whether the right destination you are going to. So, therefore, this header checksum actually provides you whether it is this are the redundant bit that you add with your error detection.

So, that will detect like parity bits actually that will detect whether there is an error in the header because it can detect. So, immediately you can see that that packet is basically not good because the header is already erroneous. So, I cannot take any decision. So, you can discard that packet. So, this is something you will be able to do.

So, the header checks some does the protocols specified above the layer and what protocol it is handling. So, we will talk about that later when we will be discussing TCP; TTL is a time to leave which is a field that might not be that much required this is for packet looping we generally avoid packet looping by this field. But we will not be discussing this part because this is not very interesting and next we have this source ID and destination ID.

So, in the next class what we will try to do? We will talk about this source ID destination idea and the fragmentation part. So, how IP with that header does the fragmentation is

something we will be discussing and we will also see this addressing. What kind of address is being implemented for IP that is for version 4 then we will try to see with that addressing how the networking is being built up ok. So, that is something we will start talking about in the next class.

Thank you.