Communication Networks

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

Module - 12
Network and Transport Layer
Lecture - 57
ARP and DHCP

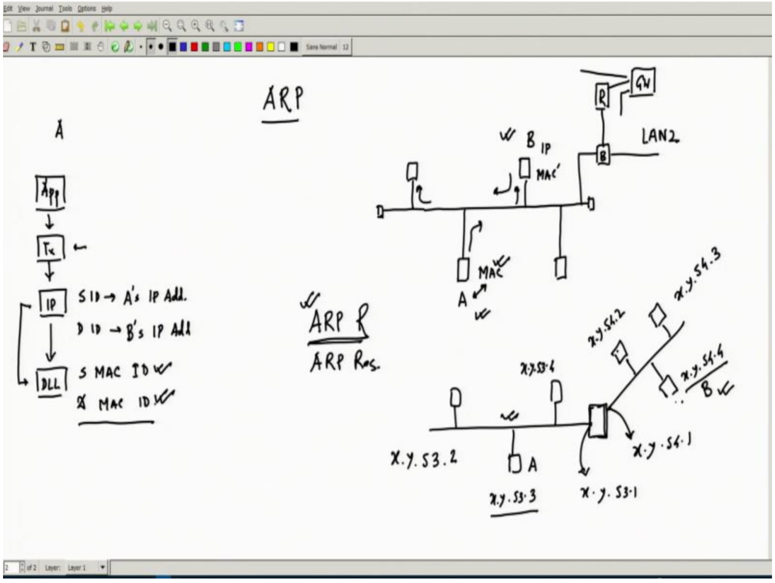
Ok, so we have started discussing subnet, we have understood how IP addresses can be handled in a more efficient way in a hierarchical manner. So, we have first classified IP addresses into class A, class B, and class C according to the size of the organization we can distribute these addresses and they can then configure the host.

So, basically, there is a classification that happens and there is a hierarchical kind of routing that will be happening. And then within the network ID also there might be subnetting which is something we have demonstrated with the help of a subnet mask and then subnet creation. We have already seen how people can manage IP addresses locally in an even better fashion.

This will really give an advantage in terms of routing speed; which means, deciding or searching through the routing table. The routing table size can be significantly reduced wherever it is not required. So, according to this classification of IP addresses and creation of subnet and then accordingly we can do very efficient routing. So, this is something we have seen.

Now, we would like to get into another concept which is called address resolution protocol and then probably further we will go into DHCP. But, we will say why IP addresses are limited in numbers and how they can be managed. So, we will try to look into that portion also, but let us first look into our ARP thing.

(Refer Slide Time: 01:58)



Let us call Address Resolution Protocol. What does this mean? Let us try to see first. So, let us say I have a LAN and within the LAN there are multiple stations LAN is properly terminated. Now, it is broadcast media we know that so let us keep it in that fashion only. Now, if this is the LAN ok, it has a simple hub or you can have this means that kind of a bus Ethernet bus with tapping you can realize it in any fashion ok?

In this LAN every station let us say this is part of a subnet ok. So, this might be connected to a bridge to another LAN that bridge might be further connected to a router local router which will be connected to the gateway ok something like that, and from the gateway there might be multiple such routers that can be connected internally ok.

So, each one of them may one one department, and each department might have multiple LANs also which are connected through a bridge. So, this might happen. So, let us say if this is the case this is the scenario. Now, over here what I want to do is a particular station let us say station A wants to communicate to another station B ok? This communication we want to facilitate through these layered protocols ok.

So, what will be happening? A has its application layer. So, if I try to see A what will be happening? It has an application layer that will generate a packet, and give it to its transport layer, The transport layer will append its header whatever that is still so far we do not know something it will append.

Then it will give to the IP layer, IP layer will add his header, ok this is where the problem starts. So, IP layer whenever he is trying to put his header he has to put this source ID which is A's IP address he knows that locally he must know his own IP address of course, it will be always there. You have also seen that; that is a very easy IP if you do immediately IP address will be coming up for this particular host.

So, you locally know your OS also knows it; it is there in your network card so it is all there. So, the IP address you will know the source ID, but the destination ID is something he has to also put. So, somehow he must get it if he wants to communicate with B only thing he needs to know is B's IP address.

If he does not know B's IP address then there is no communication. Because if I do not know whom I am communicating to then there is no communication that you can do. In telephony also if you do not know somebody's telephone number you cannot communicate right. So, that is always true. So, at least I have to know B's IP address this is something I must know somehow I will get that. Because then only I will be communicating, if you are communicating with the server you always know the server IP address.

So, that is what you do you want to do FTP or do you want to do remote login? So, you need to know to identify that server's IP address that is something you have to ok. Some additional thing also you might be might have to in transport layer you might have to identify some more things, but we will talk about that later. But, the IP address you have for this is something you really require ok.

Once you know that B's IP address is now the problem is this IP header you will be constructing no problem. You do fragmentation you do not do what version you are using all length you take and you construct the entire IP header the way we have described last to last class. So, you take that and then you append it and you give it to the DLL layer.

Now, what DLL layer have to do? Now, the DLL layer has to broadcast, but the problem is DLL also has a source ID and destination ID. This is like a duplication of addressing, but for the operation of the DLL layer, this is very important. Suppose it is an Ethernet protocol. So, he has to put this ID then only others will know who is communicating to whom so this is very essential. Suppose you have wireless then IDs are required because otherwise, you will not even know who is communicating.

Suppose somebody is sending the request to send an RTS message you will not even understand who is sending to whom, then how the destination will be able to send the CTS. Because he has to know what is the destination that must be there. So, the MAC ID is the source MAC ID and destination MAC ID that is essential.

Now, the problem is how many IDs will be actually collected this is really not a very good situation because generally what you know if A has a unique IP address. So, it has a unique MAC ID. So, this mapping of IP address to MAC address is always unique for a station whenever you allocate an IP address and the MAC ID will come with the network card only.

So, whatever DLL layer network card that you have installed has a because the manufacturer puts that ID. So, it is hardcoded and it is always unique globally. So, if that is the case this IP address and that MAC ID is always having a unified global identifier.

So, basically, I will be knowing my own MAC ID no problem with that, but what about this destination MAC ID? How do I know that? I will generally be not able to map these things ok? I will not know that because then generally we search for the IP address, but we never specify the MAC ID ok.

MAC ID can be anything it might not be that well organized like IP addresses like you do subnetting, you do networking and all those things mean net subnet than host. So, all kinds of hierarchical structures are there what kind of class of address do you take according to the structures that are being formulated?

Whereas, for MAC it can be meant at the whim of the manufacturer and which particular network card you buy from the store. So, it can be anything. So, it does not have a structure. So, therefore, this is something destination MAC ID I will not be really required, but what I know is that B’s IP address has a unique mapping with its own MAC address. Can I somehow get this, that is when this address resolution protocol works.

So, I know the IP address, but I want to now know what will be the MAC address. What I can do is something called this address resolution protocol ARP request, it is a broadcast message and it will be broadcasted to the LAN only ok? So, this will be broadcasted to the LAN and then I actually enquire that with this IP address whoever has this IP address what is his MAC address?

So, this request will be that only. So, the ARP request will be talking about ok. I have this particular IP address and this MAC address can you send me I am looking for this particular IP address what is his MAC ID? So, he will be broadcasting it and eventually if B is on the same LAN, it will be broadcasted over here he will see that this IP address for which he is asking for a MAC address that is matching with my IP address.

So, therefore, the MAC address he is looking for, he will insert that MAC address and send it back. So, that is called the ARP response. So, the ARP request you send is the broadcast message, and then the ARP response will be sent which is the unicast message. Because of that, you will see he knows now A, A’s MAC address and IP address because that has been already supplied.

So, while returning he can put this MAC address and he can put his IP address and send it back specifically to him because he was asking. The only thing is that with this particular process, you can also learn others can learn. Whenever he is sending that he might be sending it to A, but others also because of the broadcasting nature others also might be able to listen, and then from there they might learn this mapping.

So, other stations might be able to learn all these things while these things are going on. But, at least when you do not have a MAC ID of a particular corresponding IP address because you have never talked to that guy. So, you have never enquired. So, that and you have never seen because he has not sent any kind of ARP request or ARP response. So, that is why you have never listened to him and you could not figure out what is his MAC ID.

So, you can always issue this actively or otherwise passively if he has already sent some ARP request, to some other guy from there you might get his MAC ID and IP address. So, you can keep that in a local table MAC to IP mapping.

So, this is the cross-layer mapping as you can see from the IP I am trying to find out the DLL layer address or MAC address. So, this is something that is possible because there is unique mapping. So, this will always this will be giving you a unique value ok? So, this is something that we can do, but later on, we will see that IP addresses might become volatile.

That means a particular station not for all the time will have the same unique IP address. He might have for that time being in the entire universe he might have a unique IP address, but it might be changed later on he might get another unique IP address. We will talk about that when we talk about DHCP ok.

But, for the time being, this is what happens. So, this is very nicely resolved I have no issues, but now the problem comes you know what will happen if this particular station A is trying to transmit to another station the IP address that he is looking for that B is residing on some other subnet ok?

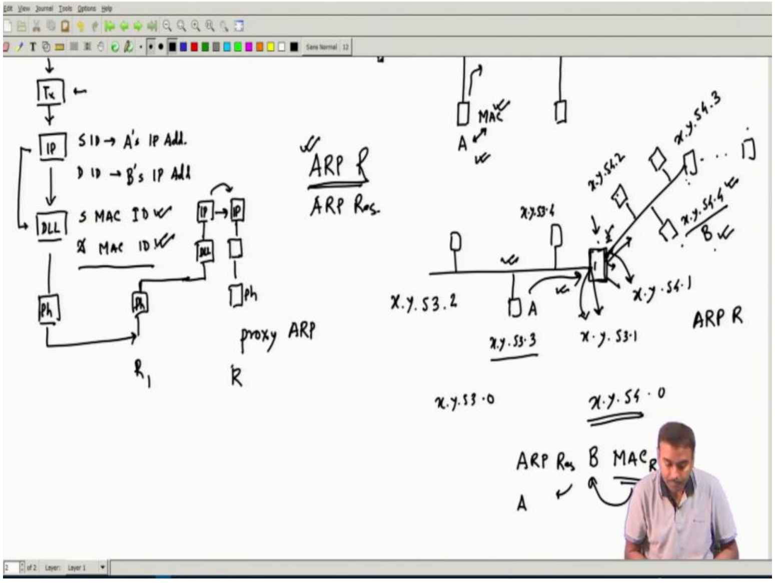
So, let us say I have a LAN and I have a router another LAN is connected to that router and this is the subnet. Let us call that x dot y dot 53 dot something. So, all hosts will be having that and this might be x dot y dot 54 probably something like that ok.

So, the router will have a port on each side. So, each of these ports will get an IP address. So, that will be x dot let us say y dot 54 dot let us say 1, this station will be x dot y dot 54 dot 2 something like that 54 dot 3. This might be x dot y dot 54 dot 4 something like that. Over here this routing port will get an address x dot y dot 53 dot 1 let us say ok. It might be 1 2 whatever you want to allocate and this will be accordingly 53 dot maybe 2. This will be x dot y dot 53 dots 3, this will be 4 x dot y dot 53 dots 4 something like that.

Now, if suppose this is A and this wish to communicate to this is B ok. Now, even if he broadcasts this ARP request because it is restricted within this LAN this particular LAN only. So, this will never be heard by B and B will not be. So, basically, he will say this is my source ID and I am looking for this destination ID and I want the corresponding MAC address because I do not know.

So, ARP request he will be sending, but that will never be broadcasted to B; B will never listen to it. So, B will not be able to give a response back. So, in this particular critical scenario, what do we do? How do we resolve this issue? How do we actually solve this particular mechanism?

(Refer Slide Time: 15:59)



So, the thing is very simple what you can do is a concept called proxy ARP. In that proxy ARP what will be happening? With this particular router in this port, he will be able to understand that the means IP address he is looking for is not even in this particular LAN or in this subnet. He can immediately put a subnet mask, he will be getting that the IP address he is looking for is x dot y dot 54 dots 0 something like that ok? So, he will after doing subnet masking he will get that.

He knows that over here in this LAN the subnet is x dot y dot 53 dot 0. So, therefore, in this subnet, if I broadcast this message nobody will answer and the router will understand. Because from his routing table entry, he knows that whatever I have connected to this subnet that is this particular station he is looking for in the ARP request is not nonexistent. So, he will work like a proxy ARP.

What he will do? He will now become the proxy or relay. What he will do? He will actually say that for this B whatever MAC ID this router port has let us call that MAC router 1 ok. So, this is port 1. So, MAC router 1 will be now taken as the MAC ID of B as if it is a wrong notion, but it will work.

As you can see with this he will be constructing his ARP response and he will send it to A. Now, A what he will understand, A will understand that ok. For if I wish to send a packet to B in the IP, I will be putting destination ID B. So, that is correct.

But, in the MAC I will be putting the MAC ID of this one and what will happen is the packet will be delivered to him his MAC layer will get that packet because his MAC ID is there he will take that and give it to the upper layer IP layer. So, station this physical layer for station 1, will go through this and then it will go through the physical layer of the router on this particular port.

So, router port 1 physical layer will give it to his MAC layer ok? So, his MAC layer will take it in the vertical communication his MAC layer will take it. Because it matches his ID, so this is having his MAC ID. And then from there, he will give it to the IP layer. Now, the IP layer will do the routing.

So, basically over here if I see that will be going to his DLL from there it will go to the IP layer. Now, the IP will know which port to forward it to because he will be reading his routing table and he will know that ok if there are multiple ports on this port it has to be forwarded. So, R let's say this is the second 2.

So, R 2 IP layer he will forward it; he will not go beyond this because in the in-between in the router, I do not have to go to the transport layer and application layer. So, it will never go up to the transport layer or application layer in the intermediate nodes. So, if it is a layer 2 switch then it will go up to layer 2 only it will not go beyond that. If it is a router then it will go up to layer 3 and it will not go beyond that.

So, this is how the functionality will be going on then he will transfer it to the IP layer of the corresponding network card of the other port which port he thinks according to his routing table that packet should be forwarded. From there it will again go to the DLL layer and come to the physical.

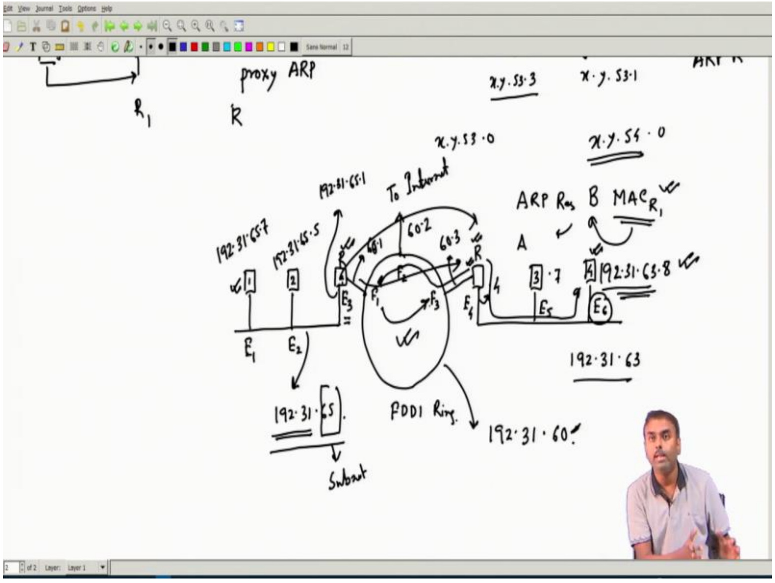
Now, on the other side when he is trying to send the packet suppose this particular thing does not know what the MAC ID of that B. But, now he can broadcast the ARP request that he can do because now it is broadcasted in the correct MAC. He has already resolved that he can broadcast it. Then B will listen to that B will reply to this port, this port will know and then forward that packet in the MAC layer means in the physical layer with that MAC ID.

So, therefore, B will receive the packet. So, this is how the address resolution goes on. So, basically, the proxy ARP is the router port that is connected to that particular subnet it will act as if he is the one who is receiving the packet. He will pull the transmitter, but he will do his job also. Because at the upper layer he will route it to the proper router routing port and from there again address resolution will go on and things will be smoothly working.

Even though that MAC ID was not available in your particular LAN still you are capable of through this proxy ARP's you will be capable of transferring it to any network. So, if it is connected to another router and connected to another router they will keep on doing this till it reaches the destination. So, all those routers will be acting as if they are the proxy ARP.

So, they will keep on doing that the other router will understand he will again act as a proxy ARP for this particular router. So, from this router to this router, this router will again act as a proxy ARP and send the MAC ID himself so that the packet is forwarded to that particular router. So, if it happens like this. So, multiple routers are connected then this is how things will be resolved.

(Refer Slide Time: 22:19)



So, I can give you a very simple example which you can do yourself also let us say I have a connectivity like this. So, I have an Ethernet LAN where two stations are connected to station 1 and station 2 and this is connected to a router. So, this is the router this router has 2 ports and then that router is connected to a ring again it is a metropolitan area network. So, it is called an FDDI ring.

So, again it is also a kind of means at layer 2 it operates it is like Ethernet, but it is actually a ring topology and over there packet transmission can go on between stations ok? So, let us say I have one particular link that is going to the internet or to the wide area network there can be another port ok?

So, these are the ports of that ring where power can be tapped, this is connected to another router and it is connected to another LAN station 3, station 4 something like that. FDDI port 1, port 2, port 3 ok. Remember this is a particular subnet. So, let us call that subnet some 192 dots and 31 dots. Let us say 63 ok this is that subnet.

Then this FDDI ring also has a subnet which is 192 dots 31 dots 60 dots 60 and dot another thing whatever will be coming. So, that is this subnet and this has another subnet which is 192 dot 31 dot 65. So, as you can see it is a class B address. So, this is a network, and then the next one is the subnet followed by there will be host all these hosts will have the same network subnet and it will have some host ID.

So, 1 and 2 will have some host ID. So, we can give some ID let us say 192 dot 31 dot 65 dot 7. Probably this is then this might be 192 dot 31 dot 65 dot 5 because the router has one port that is connected to this subnet. So, this port must get a corresponding ID 192 dot 31 dot 65 dot 1 probably, now FDDI ring has 60. So, all these ports actually will be getting their own FDDI address. So, it might be this might be 65 dot 1 this might be 60 ok.

So, wherever it is connected it depends on where it is connected. So, because this is connected to oh sorry not 65; 60 dot 1, because this is 60; so 60 dot 1. This will be maybe 60 dot 2; this will be probably 60 dot 3 something like that and this port and this ID's will be again with 63.

So, 192 dots 31 dots 63 dots let us say 8 this might be dot something like 7 and this might be dot 4 this particular port is ok. So, they will all have these things 192 dots 31. Now, if a station might have its unique MAC ID let us say this is having E 1, this is having E 2, this is having this one is having E 3, and so on ok? So, like that they will have let us say E 4, E 5, E 6, they will have MAC ID.

Now, if a particular station 1 wishes to communicate to this guy he has to actually go through three LANs like I was demonstrating. So, first, he will be his proxy ARP, and this router will become the proxy ARP. So, he will give E 3 for this ID, he is trying to reach this particular guy 192 dot 31 dot 63 dot 8, his MAC ID should be E 6, but proxy ARP will tell that that ID has a corresponding MAC ID which is E 3.

So, immediately station 1 will send all the packets to him, now he will go to layer 3 he will see where it has to be routed. So, he will see that it has to be if he has to reach over here he has to give it to him this router next through this FDDI ring. Again in the FDDI ring, there will be this proxy ARP this router will act as a proxy ARP.

If you wish to resolve it or this address resolution you want to do then you will be again broadcasting an ARP request and this guy will be volunteering to give him a reply with his own MAC ID for the same ID again you can see.

Every time a proxy ARP will be telling his MAC ID as if that is the MAC ID of that corresponding IP address only thing is that from layer 3; they have a clear bird's eye vision of where it has to be forwarded. So, therefore, they know ok from their routing table in a distributed fashion. Even though it is distributed in a distributed fashion they will be able to know who should be connecting to whom next and he should be connecting to whom next and so on they have the entire routing.

So, therefore, they will know who should be the next one who reply. So, whenever you give this IP address it will go to that particular router and that router will respond back with his MAC ID as if you have to just send it to that router only and you keep doing that. So, FDDI is again another DLL layer ok? So, it is a ring protocol and it has it is own protocol ok.

So, again through that protocol that MAC layer packet will be forwarded over here, and then from that again it will be broadcasting and it will finally, reach the destination. So, this is how through the proxy ARP or ARP request and ARP response the entire network operates and overall you will know how the IP address and MAC address together very nicely interoperate and both these layers function in a manner.

So, from end to end, you can still get connectivity meaningful connectivity. Even though layer 2 is operating within its own vicinity it is resolving things. So, in the layer 2 router, he knows he has to forward this packet to this packet, but in layer 2 you are also resolving that this guy has to forward to this guy ok? Because of this ARP proxy ARP and ARP response and request.

So, this will always happen which is pretty much the discussion of ARP. So, what we will try to do in the next class? We will try to talk about this IP address crunch and then with that crunch how do we really mean get away that get away with that crunch even though there are a limited number of IP addresses and how we can really efficiently utilize them?

So, when IP V 4 is there I have a restricted number of IP addresses still I can still cooperate. So, this is what we will be discussing there are multiple strategies for that. So, we will talk about those strategies and then we will one of them DHCP we will talk about that. NAT is again a functionality of cross-layer like ARP was a cross-layer thing NAT is another cross-layer between the transport layer and IP layer.

But, that also resolves some of the IP address crunch ok. Locally you can start using locally unique IP addresses which is which are not globally unique. So, this is something which we will be seeing in the next class ok?

Thank you.