Computer Networks and Internet Protocol

Prof. Sandip Chakraborty
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 51
ARP-RARP-BOOTP-DHCP

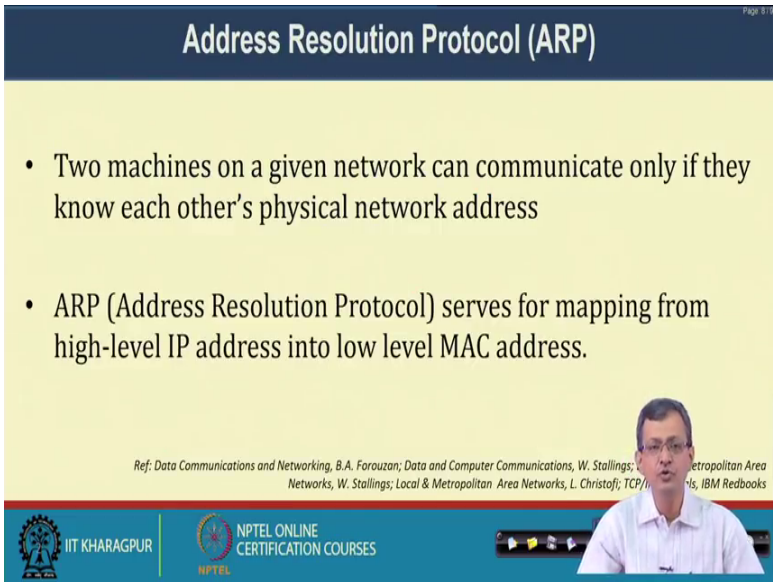
Hello. So we will be continuing our discussion on Computer Networks and Internet Protocol. So, we were discussing on layer 2 or data link layer phenomena. So, we have seen that aspects of flow control error control at layer 2 of the data link layer which is one of the major aspect of things. Apart from that the packets need to be switched or what we say frame needs to be forwarded at the layer 2 level.

As we understand that anything any upper layer packet finally, becomes it payload to this data link layer we needs to be forwarded to the next stop through these through the some layer to mechanisms all right or in other sense whatever the logical address space is there, we need to be resolved to the next of physical address to send the packet or the frame from one host to the next host next stop.

So, it can be router to router, router to switch, switch to router, system to switch and anything correct. So, that is why we will be today we will be looking at or may be into coming to lectures will be looking at different as protocols of the layer 2 phenomena, so namely ARP, RARP, BOOTP, DHCP. Some of these protocols also we might have discussed in our earlier lectures or at the when we were discussing at the top level things; nevertheless what I felt that this has direct linkages with our layer 2 level switching or data link level switching.

So, we need to we thought that it should discussed in the perspective of the layer 2 or data link layer right.

(Refer Slide Time: 01:59)



So, if you look at the first protocol which is predominant is the address resolution protocol, sometime which is also known as a companion protocol for our IP network or IP layer or what we say internet protocol in the layer 3.

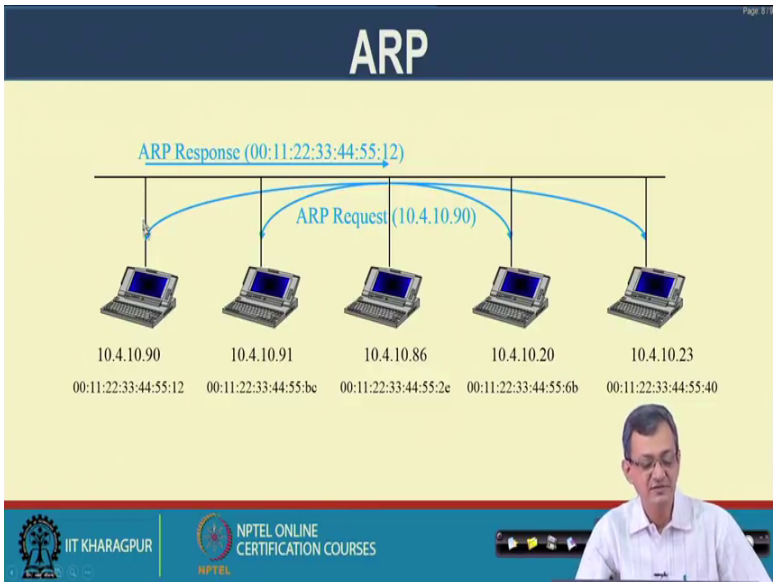
So, 2 machine on a given network can communicate only if they know each other physical address. So, this is bottom line. So, unless they know your physical address they cannot communicate, unless there is a physical connection you cannot communicate right.

So, first of all the connectivity should be there whether it is wired wireless whatever, but there should be a connectivity, the connectivity is not there whatever you do in the upper layer you cannot communicate all right.

Similarly, unless you know the physical address you cannot push it to the next stop. So, ARP serves or address resolution protocols serves for mapping from high level IP address to this low level MAC address or physical address sometimes known as loosely as network address also right or hardware address, so to say right.

So, that these ARP transform these from a logical address to this physical address.

(Refer Slide Time: 03:12)



Now, what is this ARP? So, what we see first of all? Every machine every system whether it is a PC or server or laptop or a router with multiple interfaces we come to that router etcetera.

Otherwise any devices or a printer which are which can be network enabled any devices which are network enabled has a logical address or IP address and a corresponding physical address. And typically we have seen that for IP v 4 this is a 4 byte address phase and this is a 6 byte address phase or the physical address and also we miland that this physical address of a device is unique; that is given by the hardware manufacturer on the things.

So, there are again I am repeating there are issues of cloning those physical address. So, we are not going to those complicacies, but physical address of a network device is a unique right. Whereas there can be multiple like logical address at the same time, but the router takes care of that how it to be there like these are private IP block.

So, private IP block can be same for 10 dot 4 dot 10 dot 90 can be in different places all right, but as private IP's are non routable, so there is not a problem of classing with other right; nevertheless physical addresses are unique.

Now, what I want to do if I want to send the packet from here to here, so only knowing this logical addressing will not suffice right. So, I need to know the physical address

from that particular packet or frame in terms of layer 2 to this thing right. So, if I only know the logical address I need to resolve that.

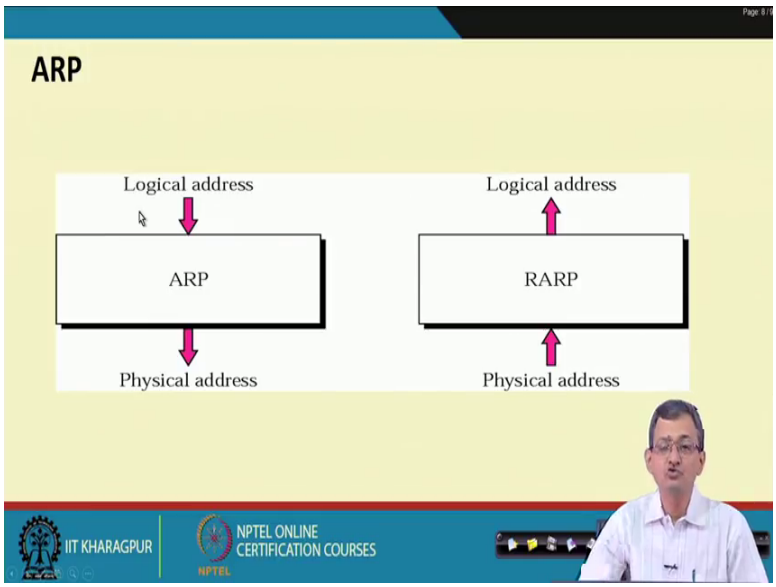
So, usually what happened? You when station a this is b you want to send to a station a wants know it is logical address or IP address and his physical address or MAC address, where as for the where it wants to say it needs its logical address or the IP address these IP address is known to this, but b's physical address is not known to it.

So, for that it requires a resolution or resolving the thing right. So, these IP ones I hit that give me this 10 dot 4 dot 90 91 MAC address it should response to the things all right or somebody else will tell me that this IP is these things right. So, there should be some address resolution protocol right that exactly ARP does.

So, like ARP request from here to here or here to here, so different level of ARP request when the file circling getting transferred right. So, I need to know the physical address of the both the parties to transfer the packet or frame.

So, ARP so if there is a ARP request ARP response with these, so somebody requesting this first terminal that what is your physical address. So, it will request response will be like that right.

(Refer Slide Time: 06:31)



So, in other sense as we have seen what we have done a logical address or the IP address to the physical address is the thing what ARP or address resolution protocol does all right.

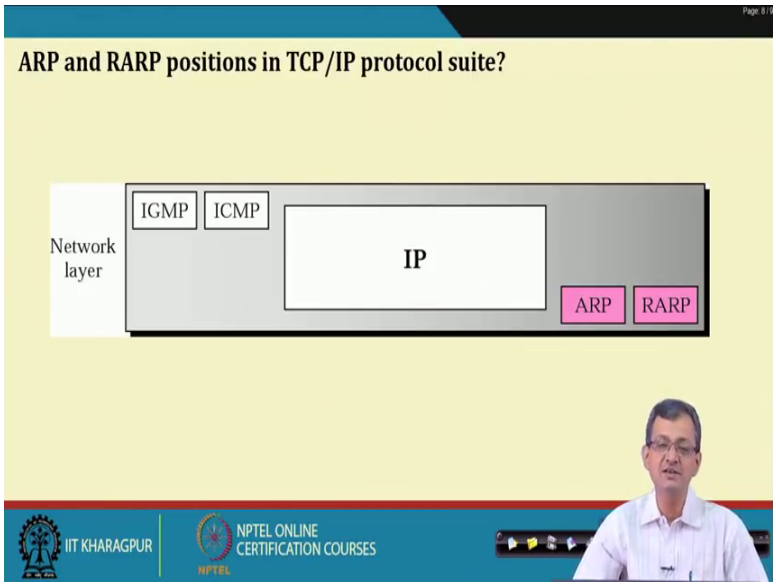
On the other hand, there is a concept of rewards ARP RARP all right. So, that is from if given a physical address a logical addressing I want to know the logical address right. Why this is required, will come to that right.

One of the thing what we can give that if I have a some sort of a terminal say term terminal or a systems where I have the physical address because, I have an inter phase cut, but somebody else need to give me the logical address, I do not know I have connected this terminal or a systems into this network and then I do not know that where the IP address is there. Either I ask the system administrator that give me the IP address and etcetera and he gives the thing or I somewhere other request to somewhere like a there may be a RARP server, where I request to give me a logical address.

So, this is my physical address give me a logical address of this network and then I consider as a all right. So, special it is true for dumb terminals which are which are do not have their own configure essence saved a on the request on the during the boot or bootstrap it request for the for the IP address and there will get connected to the things right.

So, in other sense, I require some rewards resolution right and there are some other scenarios where I want to know that what is the logical addressing of the things. I might have get a request from the things then I want to know that logical address of a particular system right. So, those are different scenarios where this RARP becomes important.

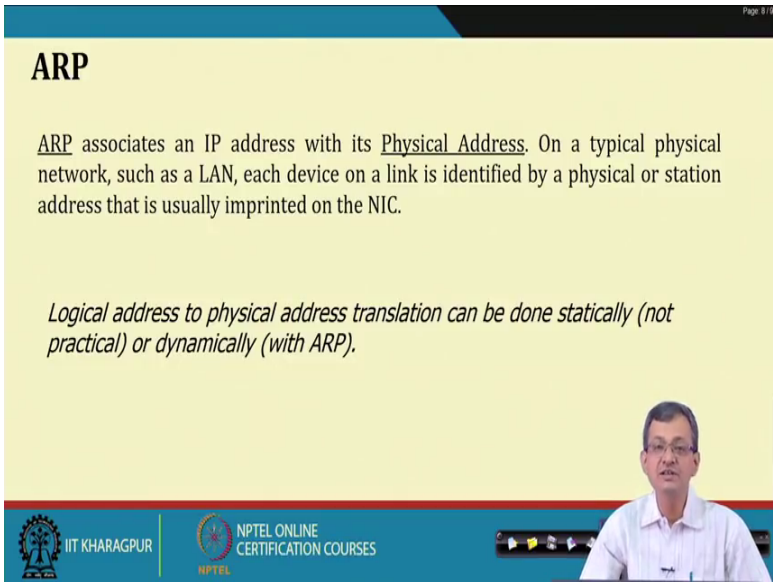
(Refer Slide Time: 08:34)



Now, as we were discussing in the TCP IP protocol suite where, this ARP or RARP sits all right. So, one way of looking at it, they are interface between the IP and the your MAC layer or data link layer all right. So, why these? Because, one side they are this ARP or RARP have that IP addresses, which is your legal address which is a phenomena of a network layer on the other side it has the physical layer things.

So, sometimes it is in some several literature is referred to as a company and protocol to IP. So, (Refer Time: 09:14) in doing a in doing some sort of a address resolution at the data link layer. So, ok, so this is there. So, in other sense in some of the literature will find that it is a protocol which is in between like IP and then down layer is the data link layer, so this is the in between nevertheless, it resolved IP 2 physical and physical to IP in the rewards.

(Refer Slide Time: 09:44)

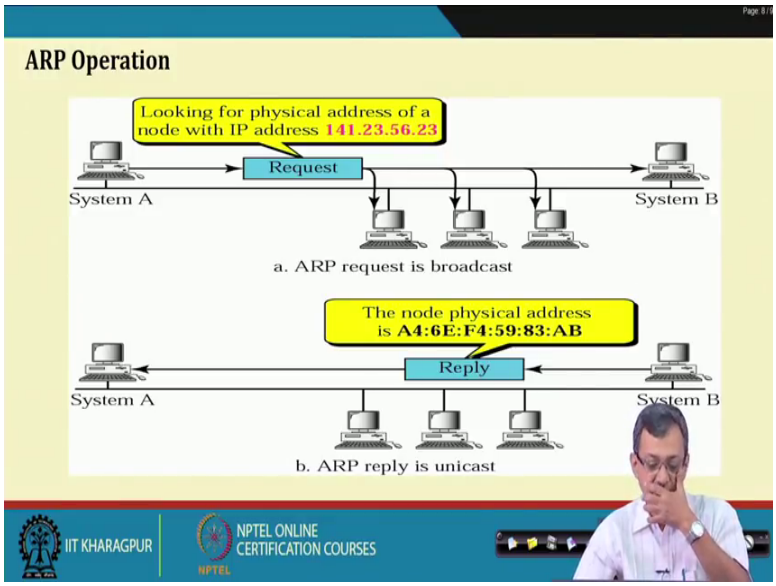


So, ARP associates an IP with its physical address or a typically physical network such as a LAN, each a LAN each device a on a link is identified by the physical or station address or network address that is usually imprinted on the NIC right, as you are discussing that NIC is the network interface card, which comes with the hardware address and this ARP associates help us in associating IP address with the physical address or the MAC address, hardware address, network address whatever we put or NIC imprinted address or NIC address.

So, logical address to physical address translation can be done statically, also I can keep a look up table that this is my logical address this is my setoff physical address (Refer Time: 10:32) it is fine, so long you are it is not dynamic all right. The same systems are there and everything configure then this is fine, not only it is state forward it is also sets time on this address resolution.

But in reality, it is not like that right. It is a you are looking for a dynamic network and it becomes a huge network, there means there is a change you need to change everywhere and type of things, so this ARP this dynamicity are brought in into the system.

(Refer Slide Time: 11:07)



So, as we are talking that is system A and there is a wants to know about some note say system B.

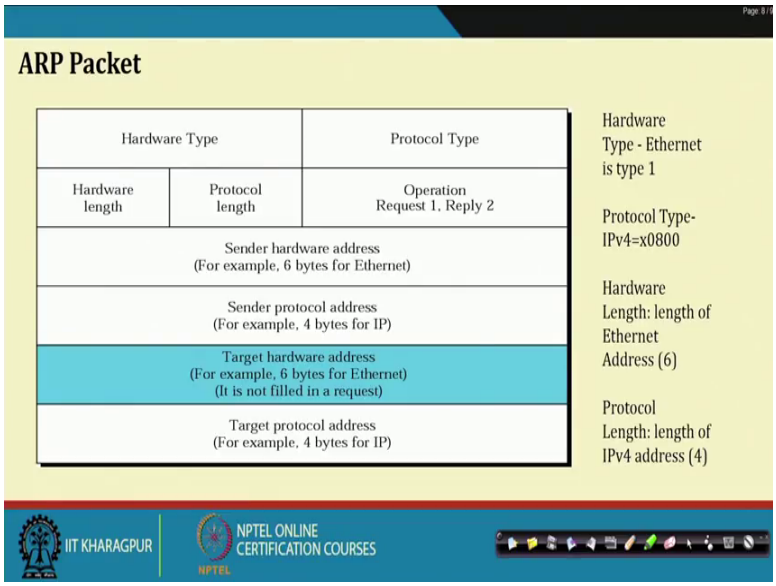
So, what it does because, system a does not know that which IP address what is the which one is the physical address all right. So, in a network, the A wants to send to some system B all right. So, it is in the same network. So, it is single hope away all right, but the A does not know what is the physical address of the things.

So, it cannot send the DLL at the data link layer or layer 2 frame to the B. So, what it first need to do, send the ARP request that say anybody is they are with this IP send me the physical address. So, ARP request is typically broadcast because, it is does not know that where the things will be there right.

Whereas, only one fellow will reply whose physical address which logical address matches with the IP and since the physical address, so it is ARP reply is unicast all right. So, it responses with the b's physical address that is A 4 6 E whatever.

So, whatever is there in the thing right. So, this is a example will find some literature.

(Refer Slide Time: 12:32)



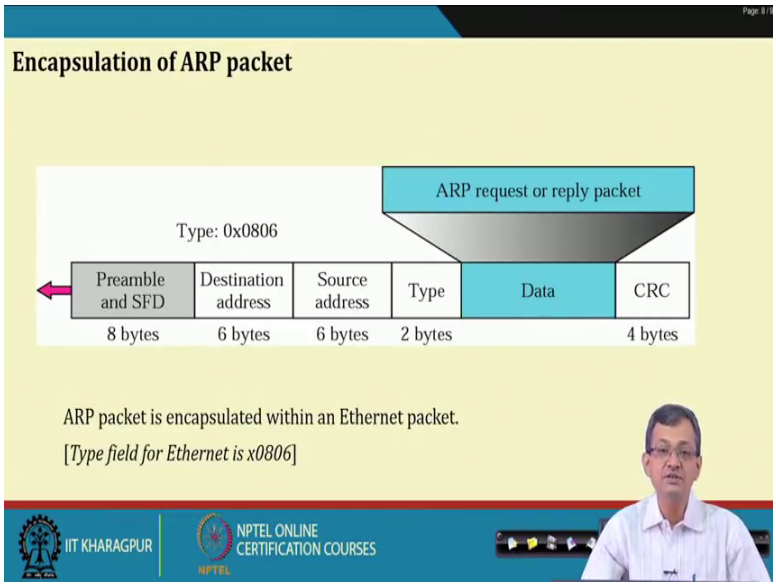
So, this ARP is ARP packet structure or packet format is like this. So, one is hardware type protocol type, hardware length, protocol length operation type that is one for request, 2 for reply all right and then what we require, sender hardware address, sender protocol address that is from the if A 2 B is hardware address b's processes hardware address and protocol address and then targets hardware address and the protocol address all right.

So, these are the things which are required out here. So, these are the things we require. But what happened that when you are sending a ARP request it is not known right. So, all 0's all right, so it is not known that what is the targets hardware address there exactly what the ARP request is looking for.

So, hardware address for ethernet type it is typically the value is 1, protocol type for IPv 4 which is predominant thing is 0 x that is 800, hardware length is the length of the ethernet address in this case 6, protocol length is the length of the IP address which is 4 all right.

So, these are the things which an operations is either request or response for request we send 1 and for response 2.

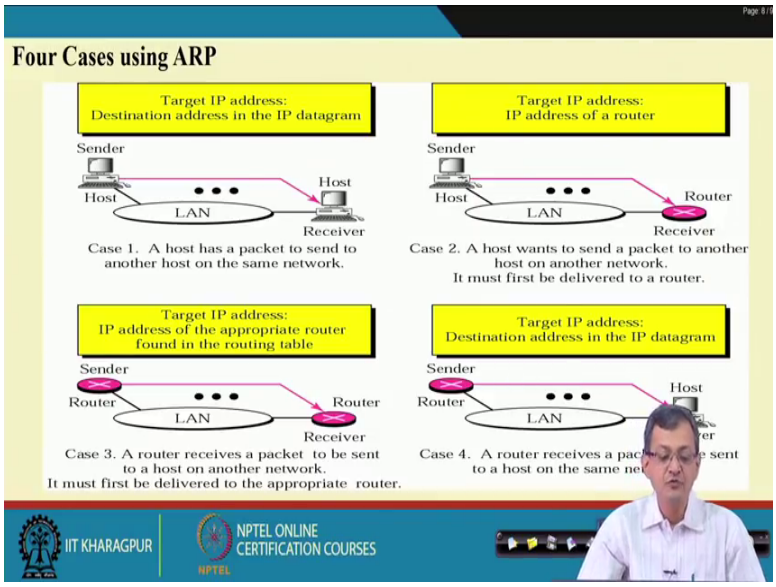
(Refer Slide Time: 14:09)



Now, how this ARP packet will be there? So, ARP encapsulation of the ARP packet, so ARP packet is encapsulated within an ethernet frame all right.

So, it becomes a payload into the things, rest you remember this preamble and SFD is 8 byte destination address and so and so forth are things are there, it is embedded into the thing all right. This is the ethernet frame all right. So, type field of the ethernet is 0 x 0 8 0 6.

(Refer Slide Time: 14:51)



So, 4 cases can be there right as we were discussing; one is that your host as a packet to send to another network on the same network all right another host on the same network it can be in the same network.

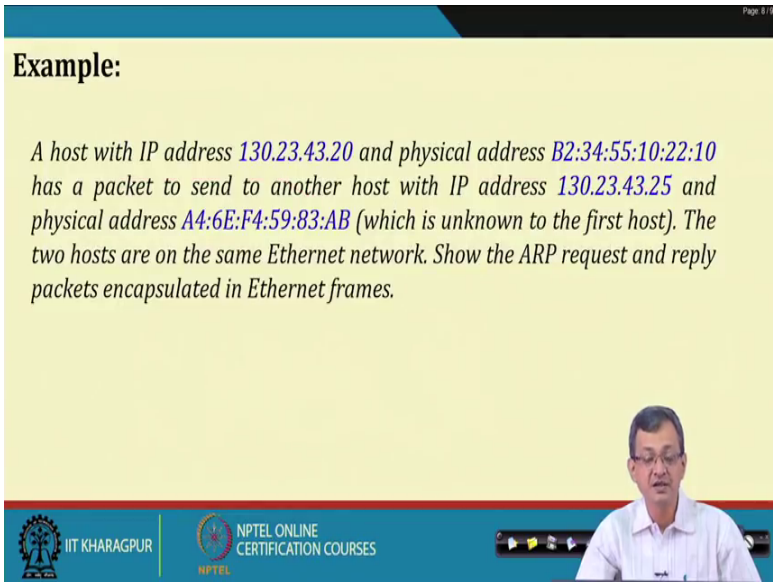
So, target IP address destination address in the IP datagram. Here the host want to send a packet to another host on the another network; that means, the host will send to the router right. So, it is on the other network, so it will send to the router. So, target IP address, IP address of a router in this case IP address of the in the IP destination address within the IP datagram in this case, the address is a router. Third may be the router receives a packet to be send to a host on another network.

So, it is a router to router, so that need to be resolve all right. So, and the final year router receives a packet sends to be the to the to the host; in other sense one is directly you can send to the host; host if it is in the same network or host to some layer 3 device and they are from it goes on and at the end of the things (Refer Time: 16:00) that is the to the host router. Another can be router to router intermediate communication or router to host on the thing right.

So, this is the 4 thing. Now incidentally if you look at the router, router has multiple interfaces correct. Typically a router has a 4 interfaces. So, 4 interfaces 4 IP address, 4 IP address and interface at it says that it has a 4 NIC card or in other sense 4 physical or hardware address.

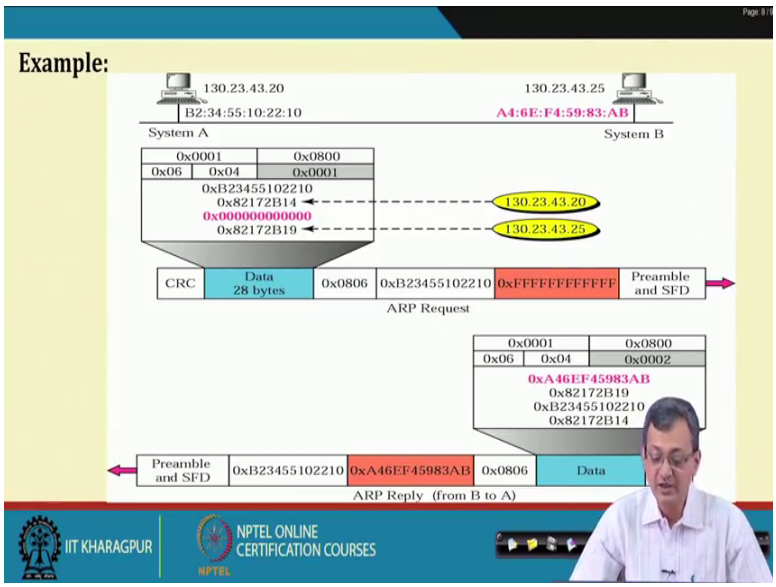
So, the router in return have may have multiple or will have multiple this sort of interfaces. Now it depends that where the connectivity is there which path it is following for that one router to another. So, there it depends that which particular interface hardware address need to be resolved to get the get back the hardware address, so that, the frame can be forwarded to the things. So, this 4 cases can handle all possible combinations.

(Refer Slide Time: 17:04)



Now, one example again from some (Refer Time: 17:06) if we look at a host with IP address 130 23 43 20 and physical address something has a packet or layer 2 frame to send to another host with IP address so and so and physical address so and so all right. The physical address at the beginning while that initial source system is sending to the destination is not known all right. The 2 host are on the same ethernet network, so that means, it does not require those router etcetera shows the ARP, I want to look at the ARP request and response.

(Refer Slide Time: 17:47)



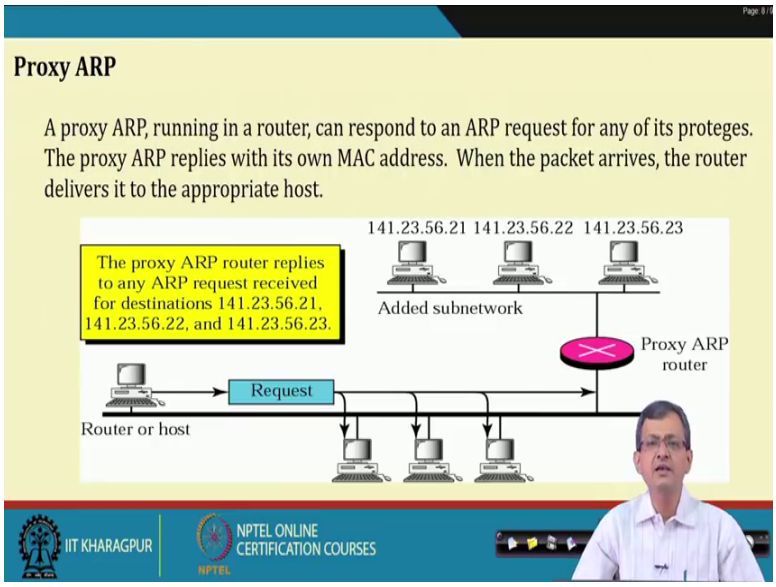
So, if you look at the ARP request path, so what it is happening? It does not know that what is the hardware address of the destination rest are known right, 130, 23, 43, 20 so, these are these are things which are embedded into the things right it is known 130, 23, 43, 20 in the x and it is also known that where 120, 23, 43, 25 is the destination that is sorry, this is also embedded and this hardware address only it is what is not known is this one right, the physical address of the things.

So, we make a ARP packet and forward it where it broadcast because, it does not know who is the owner of that IP address. Now on receiving one of the fellows whose things matches is response which is the instead of this is physical address of the thing all right. So, for it its own address becomes the whatever the address and the destination for it the destination becomes this hardware address and the IP etcetera.

So, you see this one is mapped to this and rest are there right corresponding mapped. And then, I then I know do not require a broadcast at the layer 2 level, then I can do a unicast because, I know that where to be send right. So, it becomes again ethernet packet and push into the network for a particular destination.

So, that is why, I can able to the things. So, this is a ARP request and corresponding ARP response on the things.

(Refer Slide Time: 19:24)



There is a concept called proxy ARP. So, this part is clear all right. So, just to before going to the procedure let me just repeat it. So, this was my protocol packet, what we get that once it is filled up, it filled a it is basically become a payload of the ethernet thing. We are considering the ethernet once that is there, there are there can be 4 cases; one is host to host, host to router, router to host and router to router.

So, this can be either in the same network or different network and based on the things will be there, then what we have trying to see that how this things are formed. So, I have that source having the IP and the hardware address whereas, the destination at the IP, but are not the hardware address. So, if the packet is filled up accordingly correct. So, this thing in the pink is that what it is not known and then once it is filled up, it is send to the network in a broadcast move because, the IP address is not known, who is the owner of this IP address is not known of destination.

So, once that is pushed, this fellow read this and response back resolve it whoever is the owner of the things resolved it in a unicast mode. So, this is a broadcast whereas, here we get as A B 2 A in a unicast mode. So, this is the bottom line of the ARP. So, at this address is resolved.

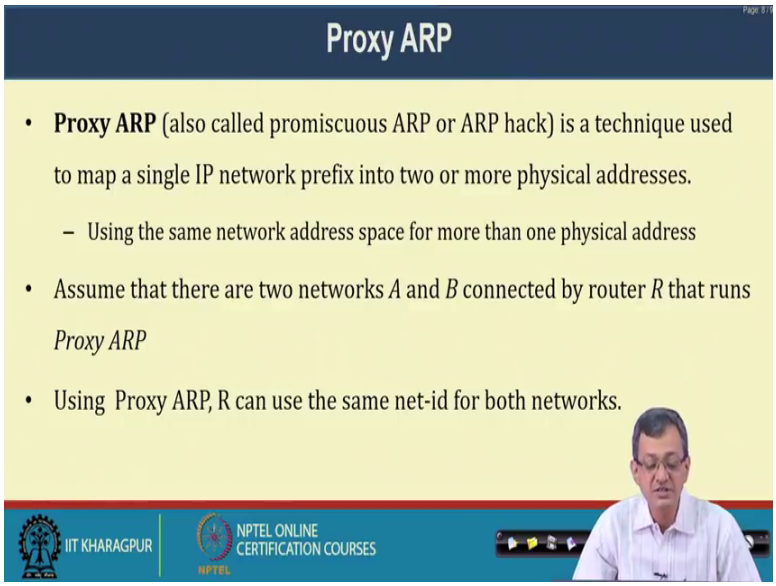
Now a proxy ARP running in a router can so there is a concept of proxy ARP. So, let us try to see what is a proxy ARP. So, at the term signifies if proxies for group of systems right. So, as if it proxies for group of systems. Now a proxy ARP running in a router can respond to an ARP request to for any type any of its proteges that is for its back in systems.

The proxy ARP replies with its own MAC address when the packet arrives and the router delivers it to the appropriate host. So, what it happens? There a proxy ARP typically running on a router it whenever there is a request come for a group of systems which is on the back off the router it responded with its own IP address. That means, it proxies or take care of the all the systems. So, it absorbs the packet and then push the packet to the rest of the network.

The proxy ARP router replies to any ARP request received right for the destination so and so, 141, 26, 56, 21, so there are 3 systems 21 22 23, so it proxies on the things.

So, on receiving the things it delivers the things and reply back and on their behalf. So, what it happens we will see that there are lot of advantages in there. Not only advantages in some of the cases, there is a requirement we need to do that. So, this is special case of ARP where one server is taking care of the things.

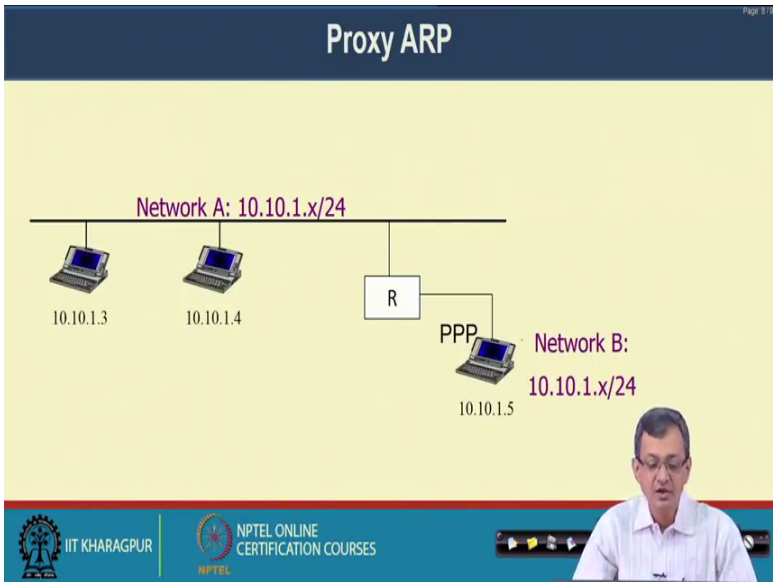
(Refer Slide Time: 22:30)



So, proxy ARP or sometimes call also promiscuous ARP or ARP hack is a technique used to map a single IP network prefix 2 1 or more physical address all right, using the same network address space for more than one physical address all right. Assume that there are two network A B connected by a router R that runs a proxy ARP.

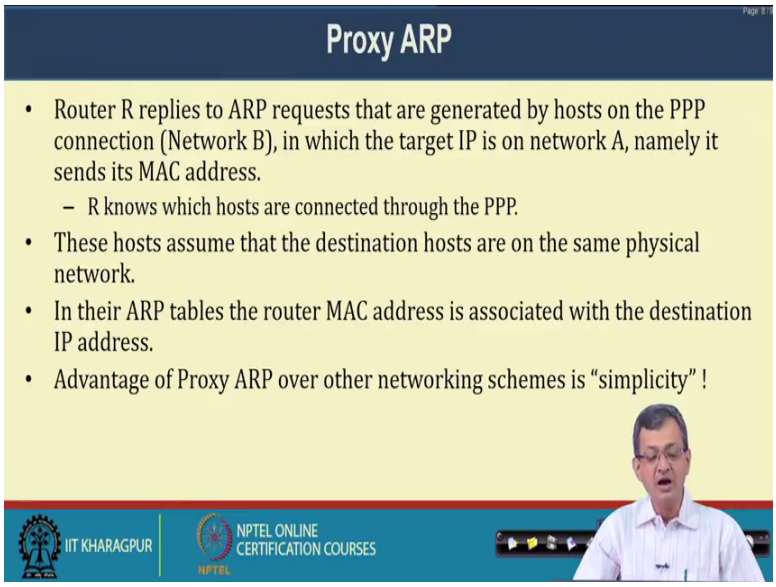
So, using proxy ARP R can use the same network id for both the networks all right. So, this is the thing it can do the proxy ARP.

(Refer Slide Time: 23:10)



So, it is take a with a sub net marks. So, it with this particular router with a proxy ARP, another network may be a PPP network, network B is so and so forth. So, this these takes care connects those 2 network or proxying for the both the network A and B all right.

(Refer Slide Time: 23:36)



So, router R replies to ARP requests that are generated by the host on the PPP network right. There is a network B and in which the target IP is on the network A namely it sends the MAC address of the thing right.

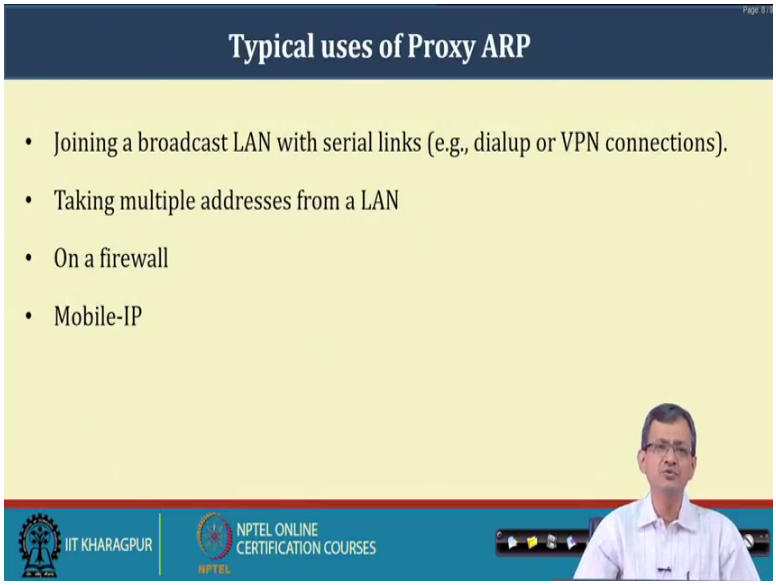
So, R knows which host are connected through PPP and so and so forth all right. So, these hosts assume that the destination host on the same physical network right. In their ARP tables, the router MAC address is associated with the destination IP address right. Advantage of the proxy ARP over the networking scheme is simplicity of handling so many things.

So, what it happening that in doing so, it as if things that it is in the same network. So, A things on the thing and then send the ARP request to that router and which in turns replies back on this B and on the other sense, it also takes care of the other part of the thing; that is the network A, so it proxies on the both the side.

So, what it becomes say I want to increase a system, decrease a system, so long I am handling within the network marks, I do not bothered about updating the ARP table etcetera. So, this is one major advantage of handling this type of things right.

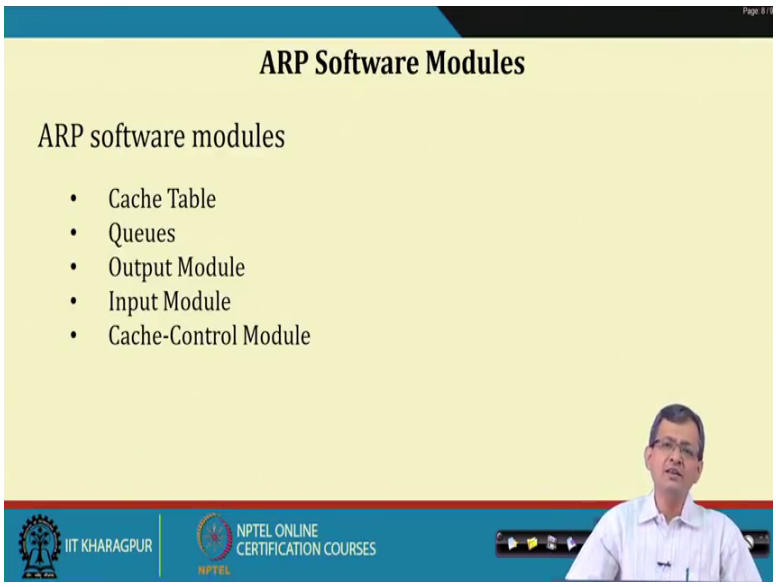
So, and secondly, that the manageability is now concentrated within how to handle this router. Not only that if we look if we thing little allowed that or if we think little on the broader aspect what you see that, now I have a handler or I have somewhere I can basically control this who can access what or if I want to keep something allow that this proxy ARP itself can be there. And in other sense, I can also restricting this broadcasting thing to a large thing right. So, the broadcasting and congesting the network on a larger this is a unable to restrict that.

(Refer Slide Time: 25:46)



So, there are typically uses like joining a broadcast LAN with a serial network dialup VPN etcetera where it will be a very helpful otherwise this interoperability etcetera has to be handled that how this IP addresses will be address and so and so forth. Taking multiple addresses from a LAN and making means more than 1 addresses from a LAN and handling them on a firewall I can have some sort of a firewall level, what we say operations into the things. There are issues of mobile IP's right those IP which are mobile IP's where also it will be very helpful so that, I can have handling this mobile IP will be much easier.

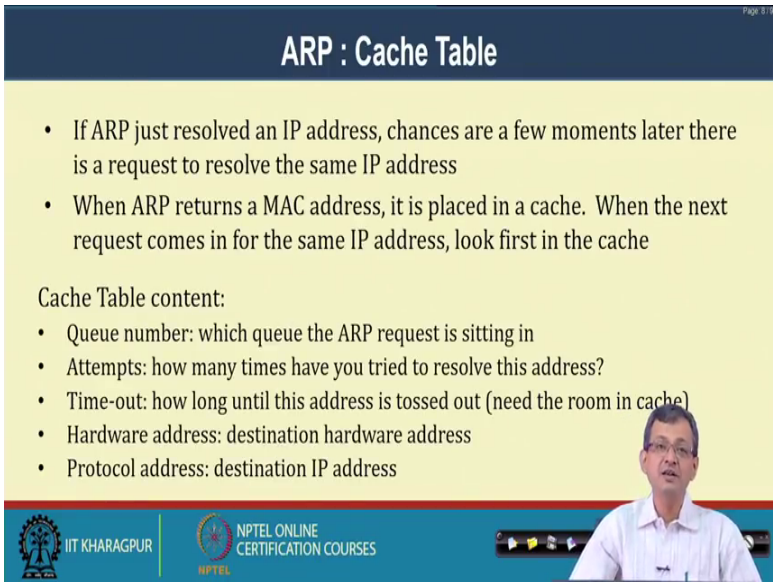
(Refer Slide Time: 26:37)



So, if you look at the ARP module per say all right, what that ARP want to will have? One is that, I sends requires sender things, but from the operational point of view they not then that may not be very cache or helpful right. Once so what are the things it will be there? There can be a cache table with caching that what are the recent resolution.

So, that if there is request coming within a shorter time period, it can reply from that cache only, there can ARP queue output module input module and cache control module. So, these are the typical modules which is there in a ARP suite all right or what I can say ARP software package.

(Refer Slide Time: 27:25)

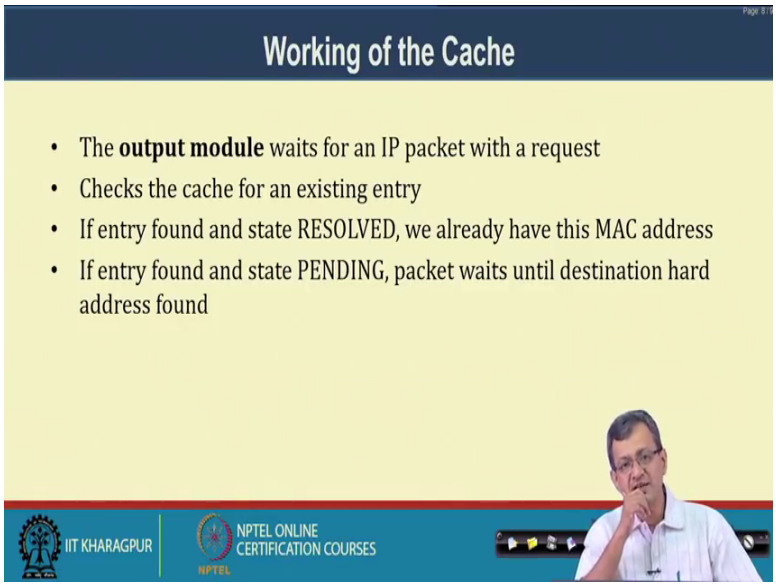


So, cache table if the ARP is just resolved an id address chances that are few moments later there is a request to resolve the same IP address.

When ARP returns the MAC address is placed on the cache. When the next request come for the same IP address look at its cache and reply back. So, it saves time saves network bandwidth and so and so forth.

So, cache table typically contained a queue number which queue the ARP request is sitting in, attempts how many times have it has been tried for the resolution timeout, how long you can go on trying before the things that it is flashed out, hardware address destination hardware address and protocol address the IP address. So, IP address versus hardware address is the mapping function and there are other things which needed to manage those things.

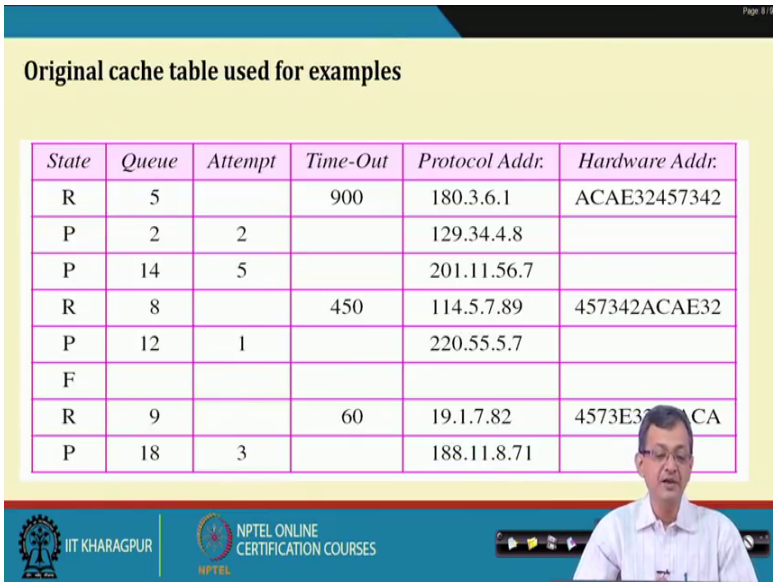
(Refer Slide Time: 28:19)



So, working of the caches state forward, there output module waits for an IP packet for a request. Checks that cache for an existing require, if the entry is resolved that is or sometimes say that is the entry becomes R, we have already have this MAC address. If the entry found and the state is pending packet waits until the destination hardware address is found I think.

So, either it can be resolved or it is in a pending state.

(Refer Slide Time: 28:47)

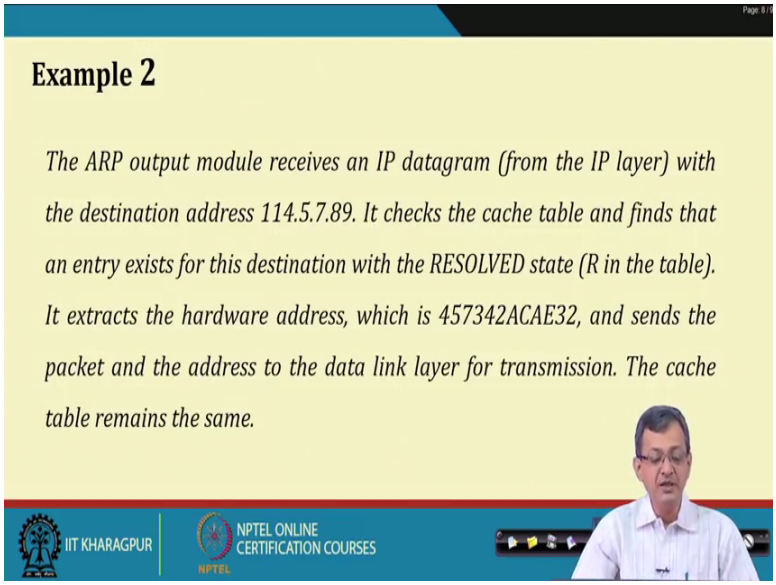


State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3 CA
P	18	3		188.11.8.71	

So, like typically original cache table used for those examples if you look at or some example scenarios like we say that there is a state is resolved, queue is 5 time out time is 9 out 900 after which it will be flashed out, protocol IP is this and the hardware address is this.

So, within that if there is request come, so if it is a pending, so is there it is still pending, pending resolve some of the things and this time out period is going on. So, after the time out period goes off that assists flashed out. So, that it is a older version of the things.

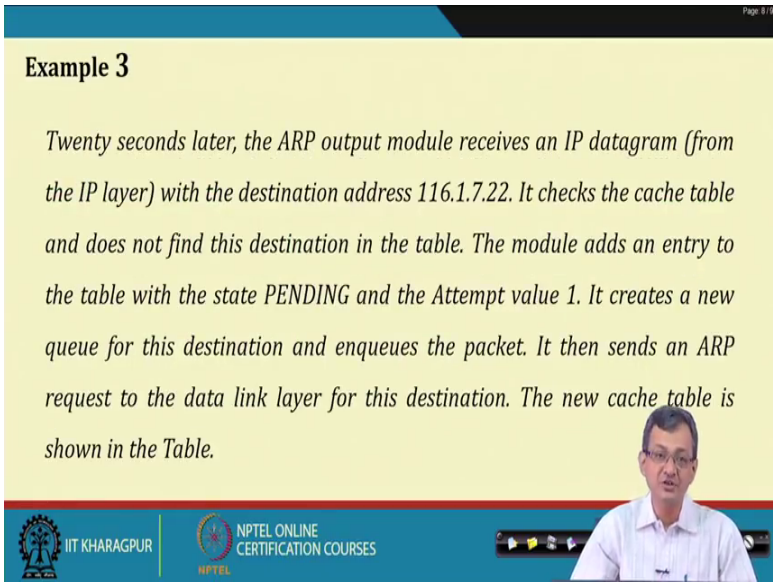
(Refer Slide Time: 29:30)



So, ARP output module receives an IP address from a IP layer with the destination address and so and so forth all right. So, it is getting a module that 114 dot 5 dot 7 dot 89 it is there, 114 dot 5 dot 7 dot 89, it is already resolved and resolved state and or within the time period. And finds that there existing there in the revolved state R table it extract the hardware address whatever the hardware address and sends to the packet and the address to the data link layer for transmission.

This cache table remains the same. So, it is nothing to change it goes on doing that.

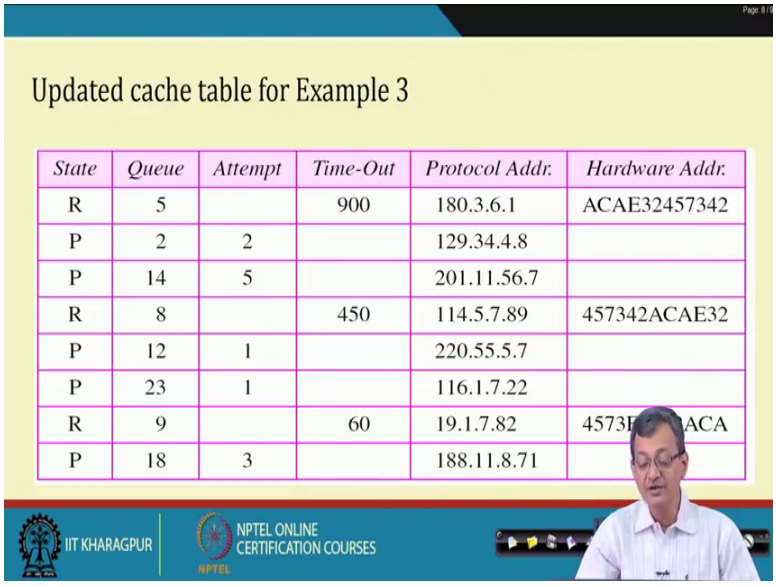
(Refer Slide Time: 30:15)



So, scenario 3, the 20 seconds later ARP modules received a IP datagram from for the destination 116 dot 1 dot 7 dot 22, it is there 116 dot it is not there right. It checks the table and find that the destination addresses not present in the table right.

So, it creates a so the module adds a new entry for the state pending with the state pending and attempt is one. It creates a new queue in the destination enqueues the packet, is then sends a ARP request to the data link layer for the destination the new cache table will be looking like this.

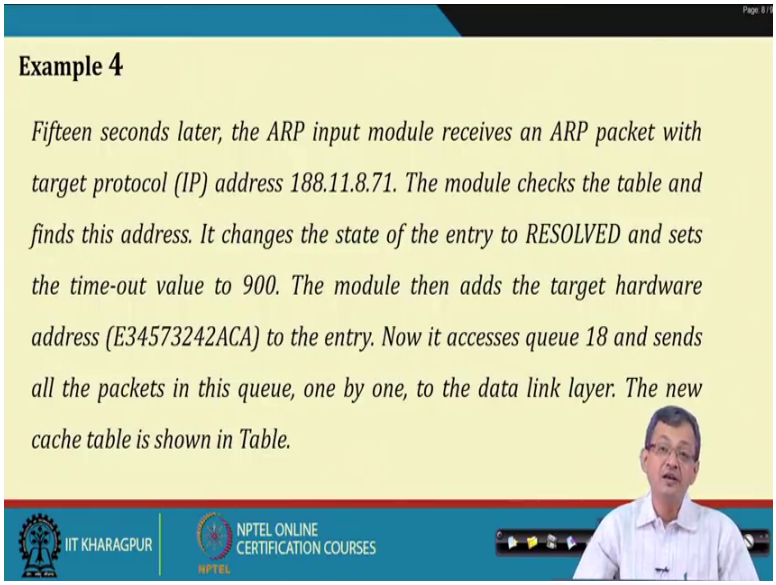
(Refer Slide Time: 30:57)



State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573[illegible]ACA
P	18	3		188.11.8.71	

So, there is a new entry of 116 dot 1 dot 7 dot 22 right. 116 dot 1 dot 70 this with a P entry and there is a new queue is there with that attempt is 1 all right.

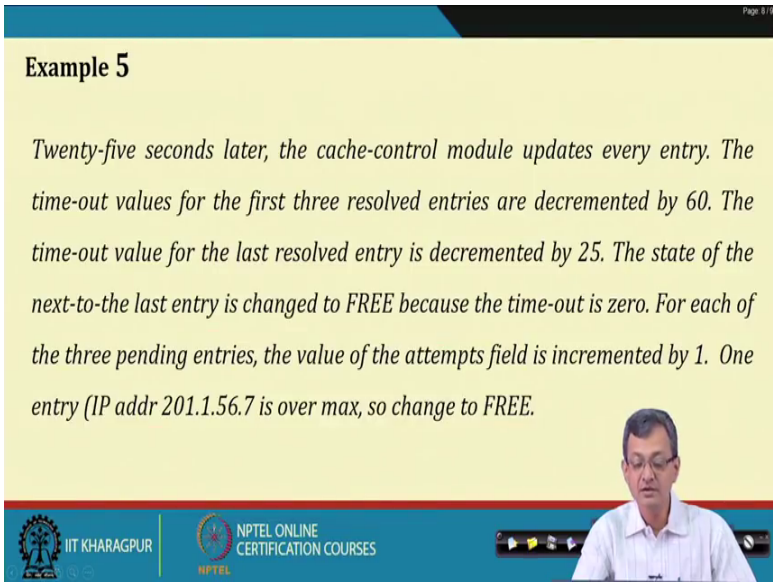
(Refer Slide Time: 31:13)



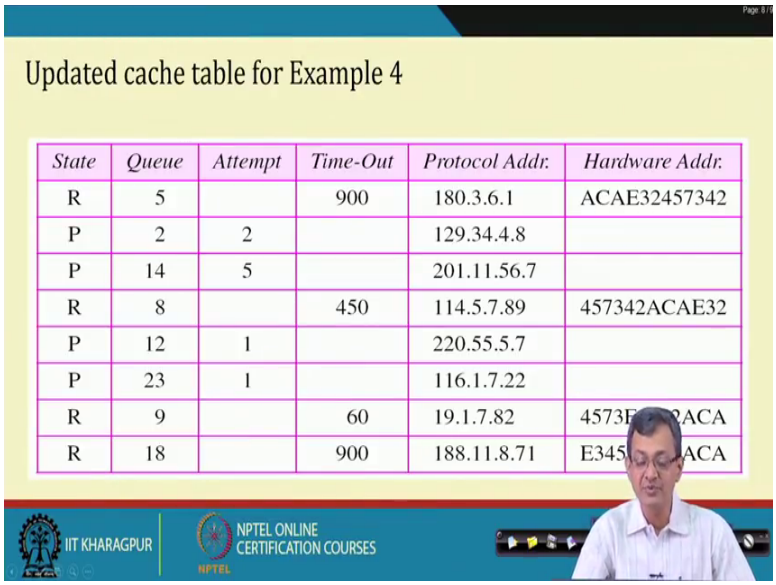
Example 4, fifteen seconds later the ARP input module receives a ARP packet with target IP 118 dot 11 dot 8 dot 71 right. Let us check whether, it is there 118 dot 11 dot 8 dot 71, it is that the module checks the table, if the it changes the state to resolved right. ARP modules receives a packet with a target IP this is the module resolved and sets the second and 900, the module adds the IP address sorry MAC address or the hardware address these to the entry.

Now, it accesses it accesses queue 18 and send the packet to the queue the new entry is there. So, what is there, it was in a pending state now, it receives the thing what that is sorry 118 dot 11 dot 8 dot 71, 118 dot 11 dot 71 and then it resolves the with a IP address MAC address like this.

(Refer Slide Time: 32:09)



(Refer Slide Time: 32:12)

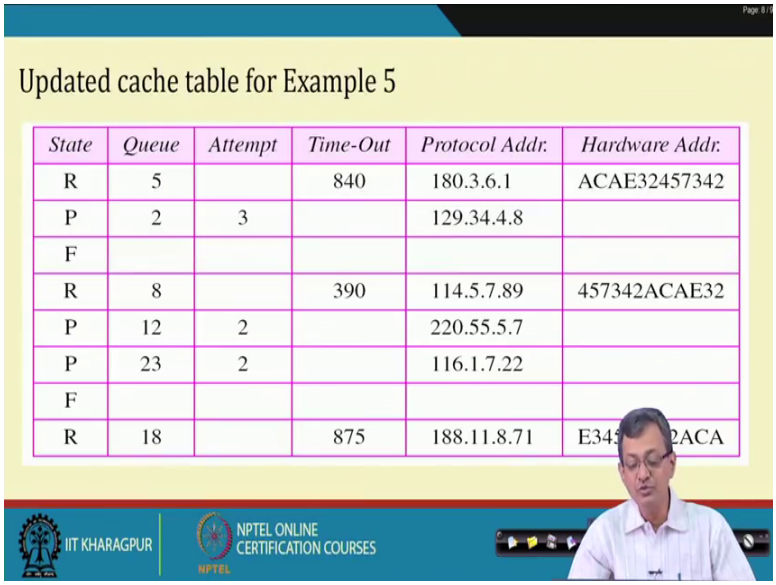


And there may be a some 25 seconds later, the cache control module updates every entry the time out values for the 3 resolved entries are decremented by 60. And the timeout for the last resolved decremented by 25, the state of the entry is resolved to free because the timeout is 0 right.

So, for each of the 3 pending, so what we are doing? It some sort of a house keeping thing. So, once it is there, it checks the timeout decrease decrements the timeout or if it is

the timeout, I expired it flash out the things and make it free and then the new table becomes like this all right.

(Refer Slide Time: 32:53)



So, it goes on doing this so that. So, you see this table handles this IP with a MAC address right and also it go on updating it over a on a periodic basis. Now any request come first consult the table all right. So, this is important, this ARP cache table or ARP table is important because, it gives it mix a proper maintenance of the things, mix the overall communication process at the data link layer if you send in other sense, at the all the upper layer things much efficient to handle this right.

So, what will we have seen now that how a higher level address, while packet coming from the higher level or this address need to be resolved to the hardware address, so that it can be transferred to the things all right, to the next stop. So, I again repeat we all though will or know that in order to transfer I need to require at a that layer that level, that is layer to level hardware resolutions. Once it is done, the packet is forwarded or switched from to the next stop. So, with these let us conclude our this present lecture and we will continue with this discussion in the subsequent lectures.

Thank you.