5.7 DHCP IP Address Management

Dynamic host configuration protocol (DHCP) is the successor to BOOTP. Unlike BOOTP, DHCP allows a host to obtain an IP address dynamically without the network administrator having to set up an individual profile for each device. All that is required when using DHCP is a defined range of IP addresses on a DHCP server. As hosts come online, they contact the DHCP server and request an address. The DHCP server chooses an address and leases it to that host. With DHCP, the entire network configuration of a computer can be obtained in one message. This includes all of the data supplied by the BOOTP message, plus a leased IP address and a subnet mask.

0-7 bits	8-15 bits	16-23 bits	24-31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 bytes)			
Seconds (2 bytes)		Flags (2 bytes)	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4 bytes)			
Chaddr (16 bytes)			
Server Host Name (64 bytes)			
Boot File Name (128 bytes)			
Vendor Specific Area (variable)			
DHCP Message Structure			

Figure (32) DHCP Message Structure

Field	Description
Op	Message operation code. Messages can be either DHCPREQUEST or DHCPREPLY.
Htype	Hardware address type.
HLen	Hardware address length.
Hops	Client places zero, this field is used by DHCP server to send request to another network.
Xid	Transaction ID.
Secs	Seconds elapsed since the client began the address acquisition or renewal process.
Flags	Flags
Ciaddr	Client IP address.
Yiaddr	“Your” (client) IP address.
Siaddr	IP address of the next server to use in dhcpstrap.
Giaddr	Relay agent IP address used in booting via a relay agent.
Chaddr	Client hardware address.
Server Host Name	Specifies particular server to get DHCP information from.
Boot File Name	Allows for multiple dhcp files to be used allowing hosts to run different operating systems.
Vendor Specific Area	Contains optional vendor specific information that can be passed to the host.

Figure (33) DHCP Message Structure Field Descriptions

The major advantage that DHCP has over BOOTP is that it allows users to be mobile. This mobility allows the users to freely change network connections from location to location. It is no longer required to keep a fixed profile for every device attached to the network as was required with the BOOTP system. The importance to this DHCP advancement is its ability to lease an IP address to a device and then reclaim that IP address for another user after the first user releases it. This means that DHCP offers a one to many ratio of IP addresses and that an address is available to anyone who connects to the network. A step-by-step description of the process is shown in Figures (34) through (48).

Laptop AA:EC:F9:23:44:19 is connected to the network.

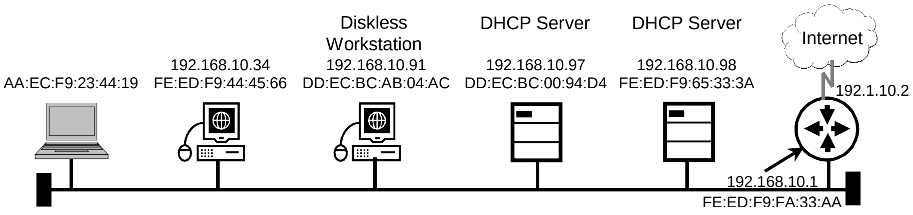
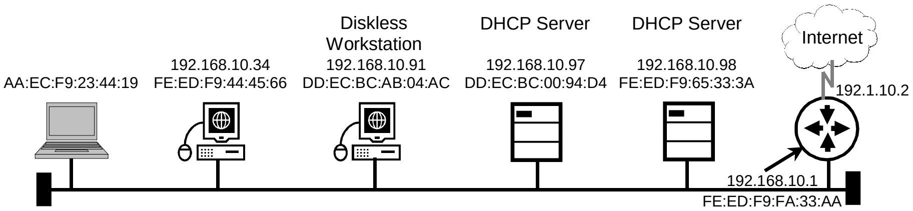


Figure (34) DHCP: Host Boots

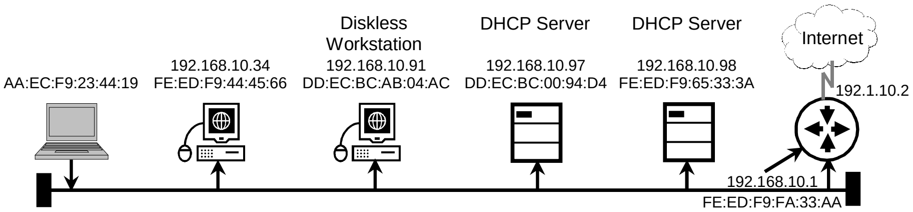
Laptop AA:EC:F9:23:44:19 generates a DHCP request.



Frame header	Packet Header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
AA:EC:F9:23:44:19	Unknown	2		Flags		:
Destination MAC	Destination IP	0				
FF: FF: FF: FF: FF: FF	225. 225. 225. 225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		AA:EC:F9:23:44:19				
		53	1	1		

Figure (35) DHCP: Message Structure Field Descriptions

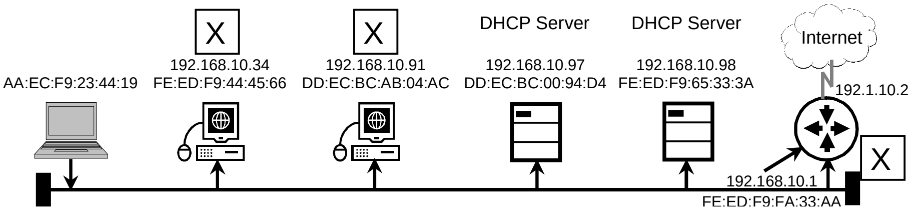
The DHCP request is transmitted by the laptop computer.



Frame header	Packet Header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
AA:EC:F9:23:44:19	Unknown	2		Flags		:
Destination MAC	Destination IP	0				
FF: FF: FF: FF: FF: FF	225. 225. 225. 225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		AA:EC:F9:23:44:19				
		53	1	1		

Figure (36) DHCP: Request Transmitted

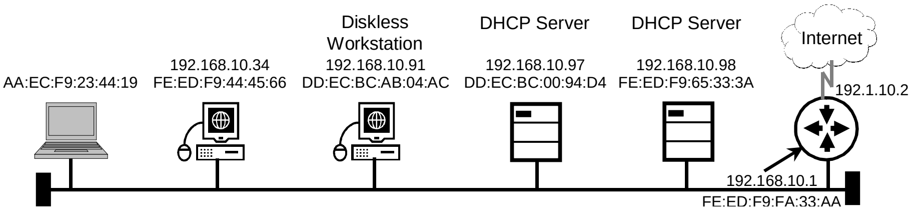
All devices pick up a copy of the frame, detect a broadcast MAC destination, strip off the frame header, and pass the packet up to the network layer. The devices detect that the IP destination is a broadcast IP address, strip off the packet header, and pass the reply data to the transport layer. All of the devices detect the DHCP request field as being a DHCP request. All devices except for the DHCP servers discard the request.



Frame header	Packet Header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
AA:EC:F9:23:44:19	Unknown	2		Flags		:
Destination MAC	Destination IP	0				
FF: FF: FF: FF: FF: FF	225. 225. 225. 225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		AA:EC:F9:23:44:19				
		53	1	1		

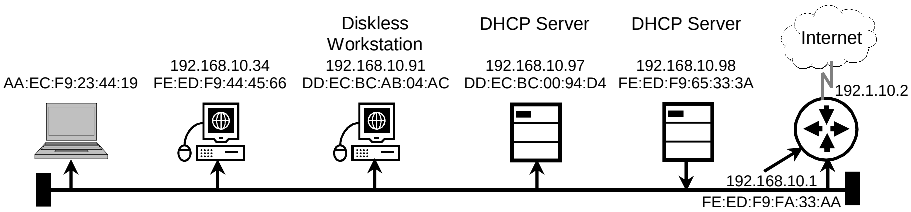
Figure (37) DHCP: Request Evaluated

The server prepares a DHCP offer to send back to the requesting device. This includes client IP address. DHCP server address, and default Gateway address. In the frame header, source and destination addresses are reversed. In the packet header, the DHCP server places its IP address in the source field and a broadcast address in the destination field. This is done to get the DHCP response packet back up to the transport layer to be processed. Only a broadcast will be passed since the client still does not know its IP address.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Figure (38) DHCP: Offer Prepared

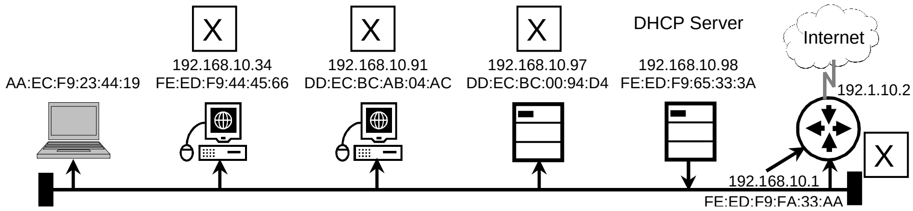


The DHCP server sends the DHCP reply frame back to the requesting device. All devices pick up the packet and examine it.

Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

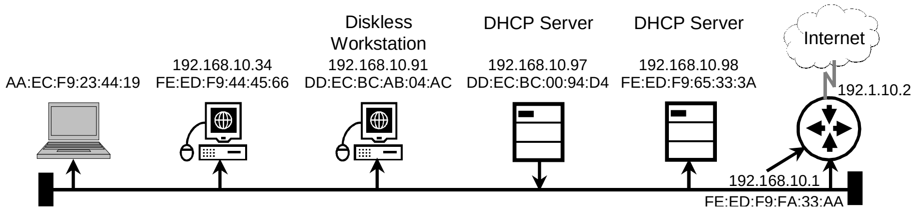
Figure (39) DHCP: Offer Transmitted

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Figure (40) DHCP: Offer Evaluated

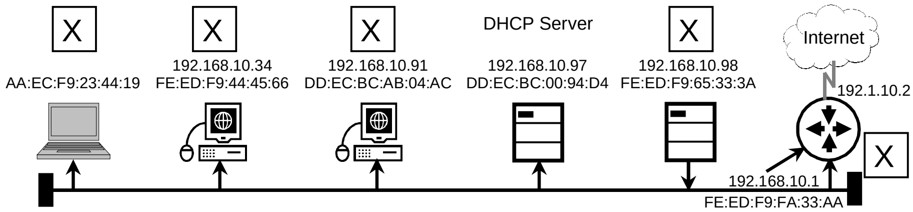


The second DHCP server sends the DHCP reply frame back to the requesting device. All devices pick up the packet and examine it.

Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
DD:EC:BC:00:94:D4	192.168.10.97	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.90				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Figure (41) DHCP: Offer Transmitted

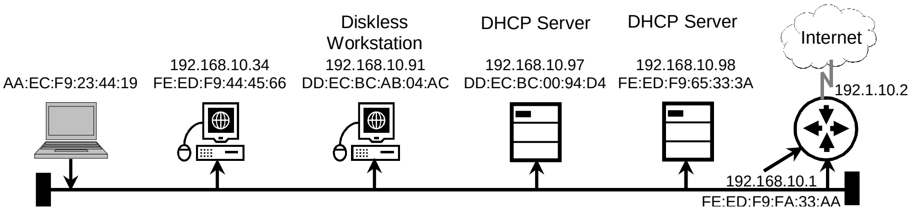
The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded. Since the laptop has already received a DHCP offer from another server, this offer is discarded.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
DD:EC:BC:00:94:D4	192.168.10.97	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.90				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Figure (42) DHCP: Offer Evaluated

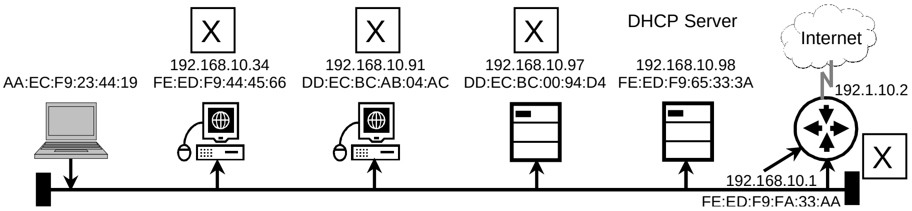
The laptop computer now sends a DHCP request addressed to the specific DHCP server that sent the accepted offer.



Frame header	Packet Header	1	1	6	0	CRC
Source MAC	Source IP	12				Check
AA:EC:F9:23:44:19	Unknown	2		Flags		:
Destination MAC	Destination IP	0				
FE:ED:F9:65:33:3A	192.168.10.98	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	3		

Figure (43) DHCP: Request Generated

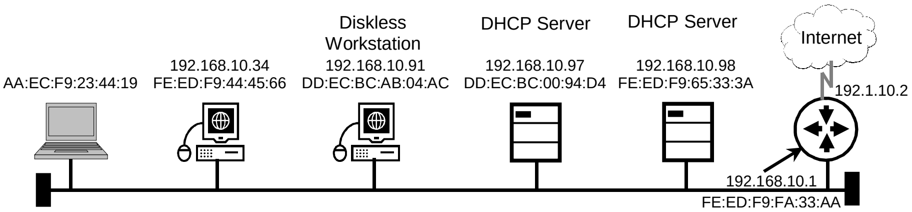
All devices pick up a copy of the frame and compare the MAC destination to their own. If there is no match, the devices discard the frame.



Frame header	Packet Header	1	1	6	0	CRC
Source MAC	Source IP	12				Check
AA:EC:F9:23:44:19	Unknown	2		Flags		:
Destination MAC	Destination IP	0				
FE:ED:F9:65:33:3A	192.168.10.98	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	3		

Figure (44) DHCP: Request Transmitted

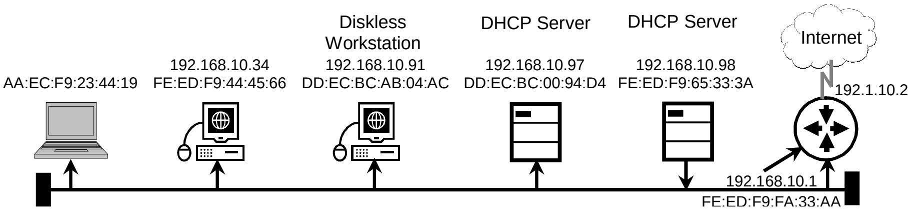
The DHCP selected server creates a DHCPACK.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Figure (45) DHCP: DHCPACK Created

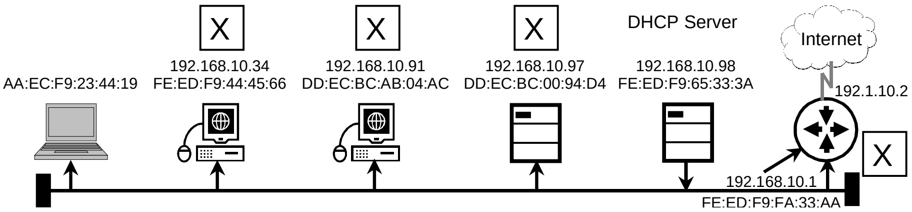
The DHCP server sends the DHCPACK frame back to the requesting device. All devices pick up the packet and examine it.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Figure (46) DHCP: DHCPACK Transmitted

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded.



Frame header	Packet Header	2	1	6	0	CRC
Source MAC	Source IP	12				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Flags		:
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	255. 255. 255. 255	192.168.10.35				
Field Type		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Figure (47) DHCP: DHCPACK Evaluated

The laptop computer now goes into the bound mode and starts to use the assigned IP address and other data passed with the DHCP offer message.

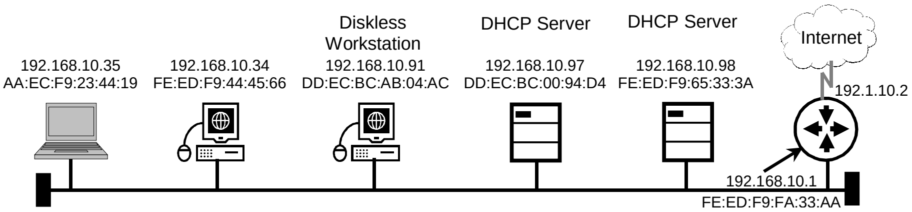
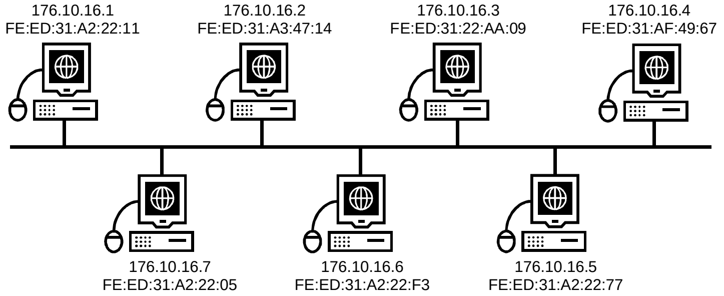


Figure (48) DHCP: DHCPACK Created

5.8 Problems in Address Resolution

One of the major problems in networking is how to communicate with other network devices.



IP Address	MAC Address
178.10.16.2	FE:ED:31:A3:47:14
178.10.16.3	FE:ED:31:22:AA:09
178.10.16.6	FE:ED:31:A2:22:F3

Figure (49) LAN Transmission Address Resolution Issues

- Computer 176.10.16.1 is monitoring the Ethernet segment to update its ARP table with IP-MAC address pairs so that it can send data to other hosts on the LAN.
- Computer 176.10.16.2 prepares the data for transmission. To do that it checks the network cable to see if another computer is using it. If another station is using the cable, computer 176.10.16.2 will have to wait, as only one computer can transmit at a time. The cable is clear so computer 176.10.16.2 can transmit.
- Computer 176.10.16.2 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. Part of this process adds the IP-MAC source addresses to the ARP table. All devices except the one that the data was sent discard the data frame.
- Computer 176.10.16.3 prepares the data for transmission. It follows all the preparation steps.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames. Adding data to their ARP tables and discarding the frame if they were not the specified destination of the data.
- Computer 176.10.16.6 prepares the data for transmission.
- Computer 176.10.16.6 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames. They add data to their ARP tables and discard the frames if they were not the specified destination of the data. This shows the automatic process that is used on a normal Ethernet LAN for maintaining address associations.
- Computer 176.10.16.1 wants to send data to 176.10.16.4. It has its IP address, but data transmission also requires the MAC address of 176.10.16.4. How does it get that MAC address to perform the data transmission?

In TCP/IP communications, a datagram on a LAN must contain both a destination MAC address and a destination IP address. These addresses must be correct and match the destination MAC and IP addresses of the host device. If it does not match, the datagram will be discarded by the destination host. Communications within a LAN segment require two addresses. There needs to be a way to automatically map IP to MAC addresses. It would be too time consuming for the user to create the maps manually. The TCP/IP suite has a protocol, called Address Resolution Protocol (ARP), which can automatically obtain MAC addresses for local transmission. Different issues are raised when data is sent outside of the local area network.

Computer 192.168.10.34 needs to communicate with computer 192.168.1.1. How does it get the MAC address for 192.168.1.1, and would it do any good if it was able to get the MAC address? Remember that MAC addresses are only useful in a LAN. They will not be any help outside of the 192.168.10.0 network. So the MAC address of the router is needed to get the data out of the LAN and on to the WAN system.

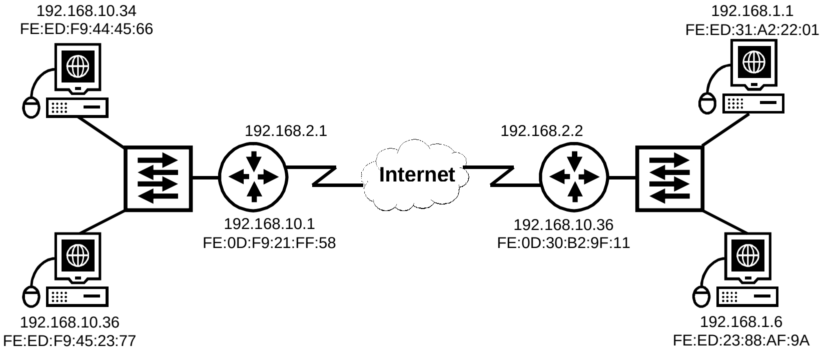


Figure (50) Non-Local Address Resolution Issues

Communications between two LAN segments have an additional task. Both the IP and MAC addresses are needed for both the destination host and the intermediate routing device. TCP/IP has a variation on ARP called Proxy ARP that will provide the MAC address of an intermediate device for transmission outside the LAN to another network segment.

5.9 Address Resolution Protocol (ARP)

With TCP/IP networking, a data packet must contain both a destination MAC address and a destination IP address. If the packet is missing either one, the data will not pass from Layer 3 to the upper layers. In this way, MAC addresses and IP addresses act as checks and balances for each other. After devices determine the IP addresses of the destination devices, they can add the destination MAC addresses to the data packets.

Some devices will keep tables that contain MAC addresses and IP addresses of other devices that are connected to the same LAN. These are called Address Resolution Protocol (ARP) tables. ARP tables are stored in RAM memory, where the cached information is maintained automatically on each of the devices. It is very unusual for a user to have to make an ARP table entry manually. Each device on a network maintains its own ARP table. When a network device wants to send data across the network, it uses information provided by the ARP table.

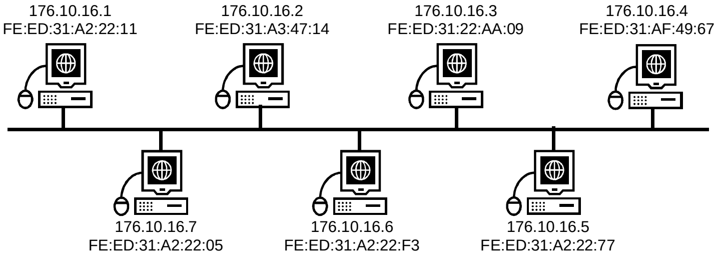
When a source determines the IP address for a destination, it then consults the ARP table in order to locate the MAC address for the destination. If the source locates an entry in its table, destination IP address to destination MAC address, it will associate the IP address to the MAC address and then uses it to encapsulate the data. The data packet is then sent out over the networking media to be picked up by the destination device.

ARP Table Entry		
Internet Address	Physical Address	Type
68.2.168.1	00-50-57-00-76-84	Dynamic

ARP Table 198.150.11.36	
MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Figure (51) ARP Table Entry

There are two ways that devices can gather MAC addresses that they need to add to the encapsulated data. One way is to monitor the traffic that occurs on the local network segment. All stations on an Ethernet network will analyze all traffic to determine if the data is for them. Part of this process is to record the source IP and MAC address of the datagram to an ARP table. So as data is transmitted on the network, the address pairs populate the ARP table. Another way to get an address pair for data transmission is to broadcast an ARP request.



ARP Table	
IP Address	**MAC Address**
178.10.16.3	FE:ED:31:22:AA:09
178.10.16.6	FE:ED:31:A2:22:F3
178.10.16.5	FE:ED:31:A2:22:77
178.10.16.2	FE:ED:31:A3:47:14

Figure (52) ARP Table Functions

- Computer 176.10.16.1 is monitoring the Ethernet segment to update its ARP table.
- Computer 176.10.16.2 prepares the data for transmission. To do that it checks the network cable to see if another computer is using it. If another station is using the cable, computer 176.10.16.2 will have to wait, as only one computer can transmit at a time. The cable is clear so computer 176.10.16.2 can transmit.
- Computer 176.10.16.2 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. Part of this process is to add the IP-MAC source addresses from the data to the ARP table.
- Computer 176.10.16.3 prepares the data for transmission. It follows all the preparation steps.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.6 prepares the data for transmission.
- Computer 176.10.16.6 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- Computer 176.10.16.5 prepares the data for transmission. Notice the first pair in the ARP table, it is reaching its timeout value. If a computer does not transmit data for a certain length of time, their IP-MAC pair is dropped from the ARP table.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment. The first value in the ARP table exceeded the timeout value so it is removed. The ARP table is dynamically updated. It adds and removes entire based on segment activity and timeout values.
- Again all hosts on the segment analyze the incoming frames. New values are added to the ARP table.
- Computer 176.10.16.2 prepares the data for transmission.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. The IP-MAC pair for 176.10.16.2 is added back into the table. If this transmission had come before the

timeout value was exceeded, the pair would not have been removed from the table, the timeout value would have just been reset.

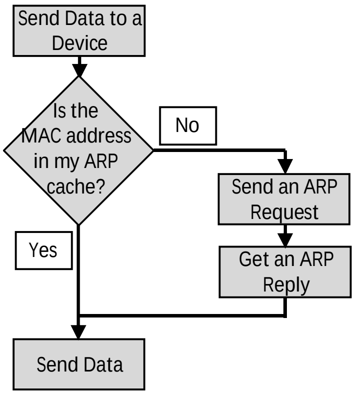
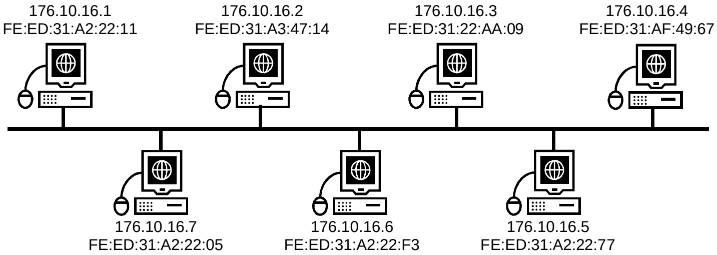


Figure (53) The ARP Process

The computer that requires an IP and MAC address pair broadcasts an ARP request. All the other devices on the LAN analyze this request. If one of the local devices matches the IP address of the request, it sends back an ARP reply that contains its IP-MAC pair. If the IP address is for the LAN and the computer does not exist or is turned off, there is no response to the ARP request. In this situation, the source device reports an error. If the request is for a different IP network, there is another process that can be used.



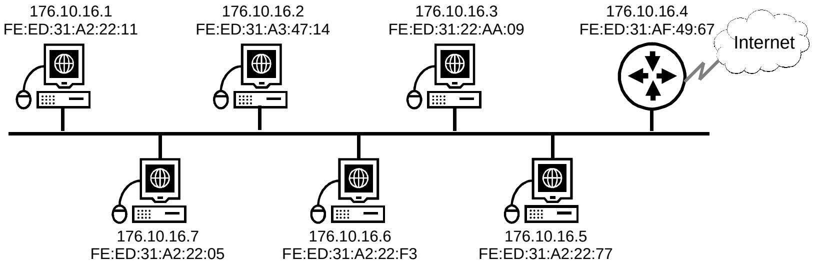
ARP Table	
IP Address	**MAC Address**
178.10.16.3	FE:ED:31:22:AA:09
178.10.16.6	FE:ED:31:A2:22:F3
178.10.16.5	FE:ED:31:A2:22:77
178.10.16.2	FE:ED:31:A3:47:14

Figure (54) ARP Request

- Computer 176.10.16.1 needs to send a data transmission to computer 176.10.16.4.
- Computer 176.10.16.1 prepares the data for transmission to computer 176.10.16.4. As it is building the frame for transmission. It finds that the IP-MAC pair for 176.10.16.4 is not in its ARP table. Computer 176.10.16.1 needs this pair, so it must do an ARP request to get it.
- Computer 176.10.16.1 discards the process of encapsulation for the data transmission and instead creates an ARP request to get the MAC address of computer 176.10.16.4.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination IP address of the incoming frames.
- Computer 176.10.16.4 prepares the ARP reply data for transmission.
- Computer 176.10.16.4 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.1 prepares the data for transmission.
- Computer 176.10.16.1 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames.

- Computer 176.10.16.2 prepares the data for transmission.
- Computer 176.10.16.4 processes the data transmission.

Routers do not forward broadcast packets. If the feature is turned on, a router performs a proxy ARP. Proxy ARP is a variation of the ARP protocol. In this variation, a router sends an ARP response with the MAC address of the interface, on which the request was received, to the requesting host. The router responds with the MAC addresses for those requests in which the IP address is not in the range of addresses of the local subnet.



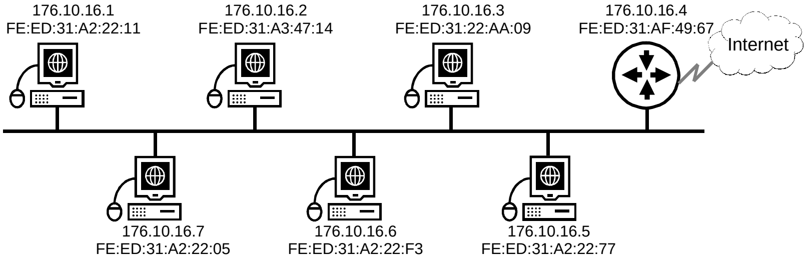
ARP Table	
IP Address	MAC Address
178.10.16.3	FE:ED:31:22:AA:09
178.10.16.6	FE:ED:31:A2:22:F3
178.10.16.5	FE:ED:31:A2:22:77
178.10.16.2	FE:ED:31:A3:47:14

Figure (55) Proxy ARP Request

- Computer 176.10.16.1 needs to send a data transmission to computer 176.10.16.4.
- Computer 176.10.16.1 prepares the data for transmission to computer 176.10.16.4. As it is building the frame for transmission. It finds that the IP-MAC pair for 176.10.16.4 is not in its ARP table. Computer 176.10.16.1 needs this pair, so it must do an ARP request to get it.
- Computer 176.10.16.1 discards the process of encapsulation for the data transmission and instead creates an ARP request to get the MAC address of computer 176.10.16.4.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them.
- All devices except router 176.10.16.4 drop the frames because they do not match the destination IP address of the incoming frames.
- Router 176.10.16.4 compares the address with its Ethernet interface IP address. The calculation reveals that this packet is going outside of the LAN. Since this router has proxy ARP enabled, it prepares an ARP reply to the requesting host with its MAC address and the IP address of the destination device.
- Router 176.10.16.4 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.1 prepares the data for transmission.
- Computer 176.10.16.1 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames.
- Router 176.10.16.4 processes the data for transmission to forward to the next network hop.
- Computer 176.10.16.4 processes the data transmission.

Another method to send data to the address of a device that is on another network segment is to set up a default gateway. The default gateway is a host option where the IP address of the router interface is stored in the network configuration of the host. The source host compares the destination IP address and its own IP address to determine if the two IP addresses are located on the same segment. If the receiving host is not on the same segment, the source host sends the data using the actual IP address of the destination and the MAC address of the router. The MAC address for the router was learned from the ARP table by using the IP address of that router.

If the default gateway on the host or the proxy ARP feature on the router is not configured, no traffic can leave the LAN. One or the other is required to have a connection outside of the LAN.



ARP Table	
IP Address	MAC Address
178.10.16.3	FE:ED:31:22:AA:09
178.10.16.6	FE:ED:31:A2:22:F3
178.10.16.5	FE:ED:31:A2:22:77
178.10.16.2	FE:ED:31:A3:47:14
178.10.16.2	FE:ED:31:A3:47:14

Default Gateway	
IP Address	MAC Address
178.10.16.4	FE:ED:31:AF:49:67

Figure (56) Default Gateway

- Computer 176.10.16.1 needs to send a data transmission to computer 199.11.20.5.
- Computer 176.10.16.1 prepares the data for transmission to computer 199.11.20.5. As it is builds the frame for transmission. It finds that the IP-MAC pair for 199.11.20.5 is not in its ARP table. With the default gateway set on this computer the destination address is compared with the hosts source address. The calculation shown that the destination is on another network. So the host builds the data frame using the destination IP address and the default gateways MAC address.
- Computer 176.10.16.1 transmits its data frames through the network cable segment.
- All hosts on the segment analyze the incoming frames.
- All computers except for router 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames.

5.10 Routing

Routing protocols determine the paths that routed protocols follow to thief destinations. Examples for routing protocols include Routing *Information Protocol* (RIP), the *Interior Gateway Routing Protocol* (IGRP), the *Enhanced Interior Gateway Routing Protocol* (EIGRP), and *Open Shortest Path First* (OSPF).

Routing protocols enable routers that are connected to create a map, internally, of other routers in the network or on the Internet. This allows routing (i.e. selecting the best path, and switching) to occur. Such maps become part of each router’s routing table.

There are several methods to inter route information into a routing table. The most primary method is called “*Static Routers*”, where the routing information is entered manually into the tables. This is quite a difficult task especially for large or changing networks. Static routers are practically useful whenever the network administrator wants to control which path a router will select. For example:

- To test a particular link in the network.
- To conserve wide area bandwidth.

- When there is only one path to the destination network in order to prevent routers from trying to find another way to this network if the connection fails.

The other type of building routing tables is the "*Adaptive or Dynamic Routing*" which occurs when routers send periodic routing update messages to each other. Each time a router receives a message containing new information; it recalculates the new best route, and sends the new update information to other routers. By dynamic routing, routers can adjust to changing network conditions.

5.10.1 Routing Information Protocol (RIP)

The most common method to transfer routing information between routers that are located on the same network is RIP. This protocol calculates distances to a destination. RIP allows routers that use this protocol to update their routing tables at programmable intervals, typically every 30 seconds. However, because it is constantly connecting neighboring routers, this can cause network traffic.

Features of RIP:

- Distance vector routing protocol.
- Only metric is the number of hops.
- Maximum number of hops is 15.
- Update every 30 seconds.
- Doesn't always select fastest path for packets.
- Generates lots of network traffic with updates.

5.10.2 Interior Gateway Routing Protocols (IGRP)

IGRP and EIGRP are routing protocols that were developed by CISCO System, Inc. to address problems associated with routing in large multiple vendor networks that were beyond the scope of protocols such as RIP.

Features of RIP:

- Distance vector routing protocol.
- Determines the best path depending on the following factors (hop count, bandwidth, load, delay, & reliability). The waits of these factors are set by the network administrator to allow IGRP to automatically calculate the best path.
- Maximum number of hops is 255, which means that it can work in larger networks in world.

5.10.3 Open Shortest Path First (OSPF)

It aims to determine the optimum path, because this protocol actually uses several criteria to determine the best route to a destination. These criteria include cost metrics, which factor in such things as route speed, traffic, reliability, and security.