Network Adapter Bootstrap

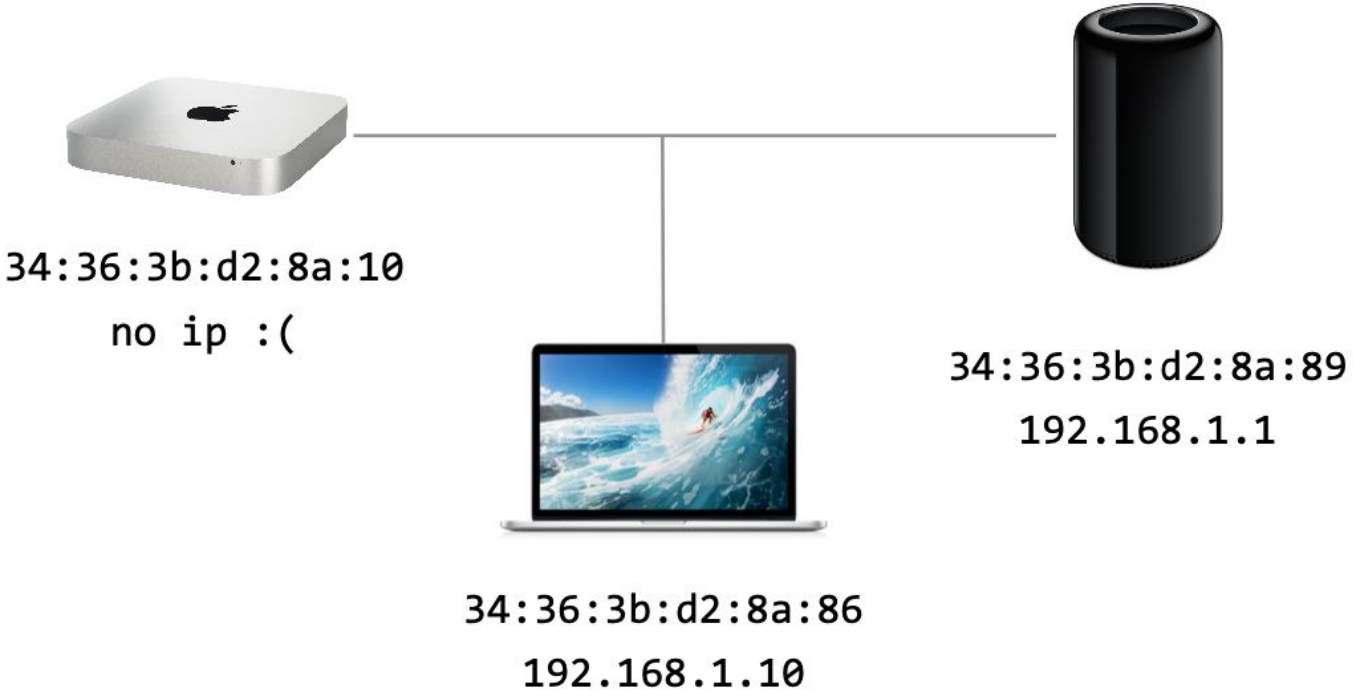
Two problems to solve:

1. Who am I? How do I acquire an IP address?
   Dynamic Host Configuration Protocol

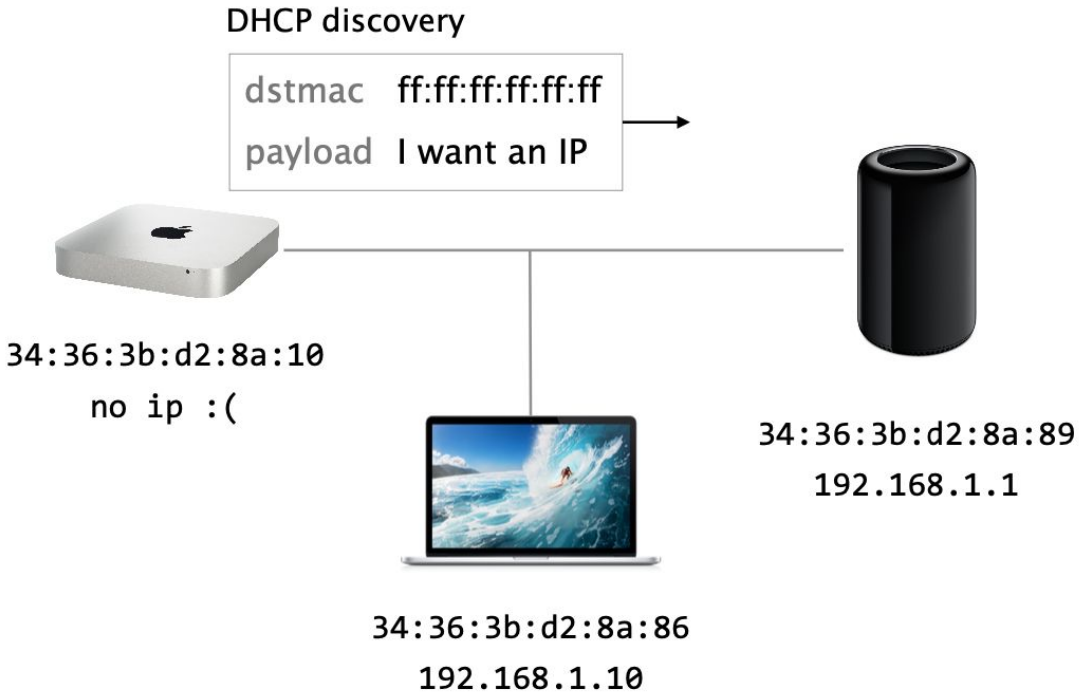
2. Who are you? Given an IP, how do I find which MAC to send to?
   Address Resolution Protocol

Functionally, Every Connected Device Requires an IP

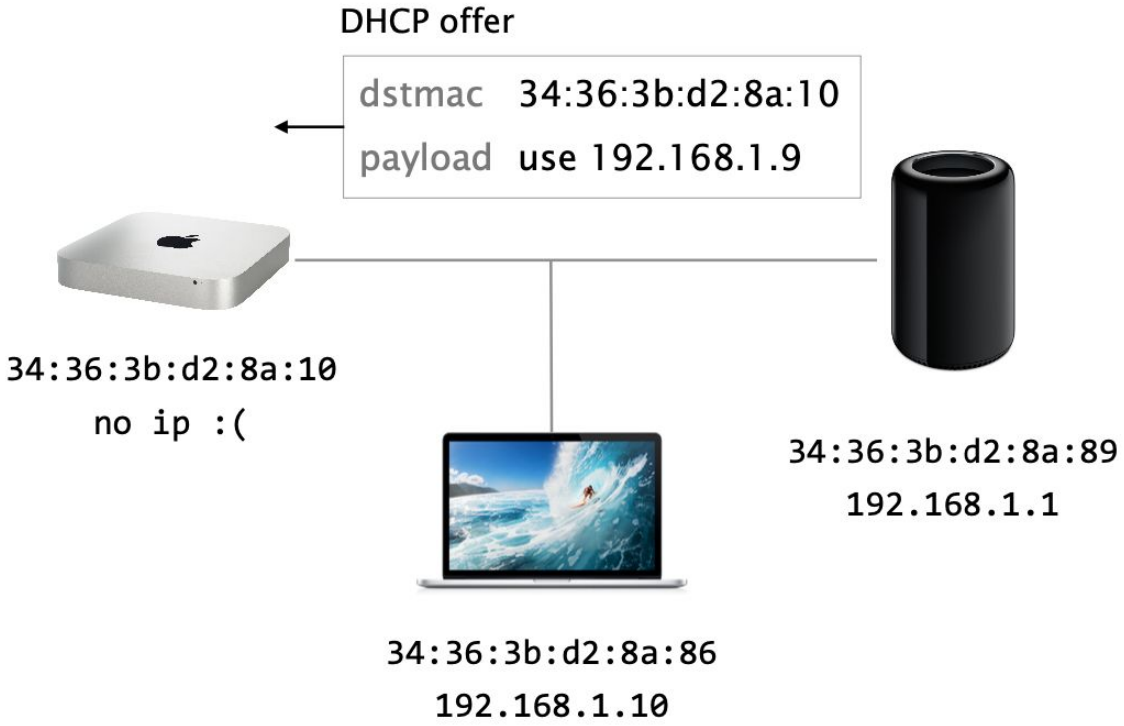
DHCP


34:36:3b:d2:8a:10
no ip :(
34:36:3b:d2:8a:89
192.168.1.1
34:36:3b:d2:8a:86
192.168.1.10

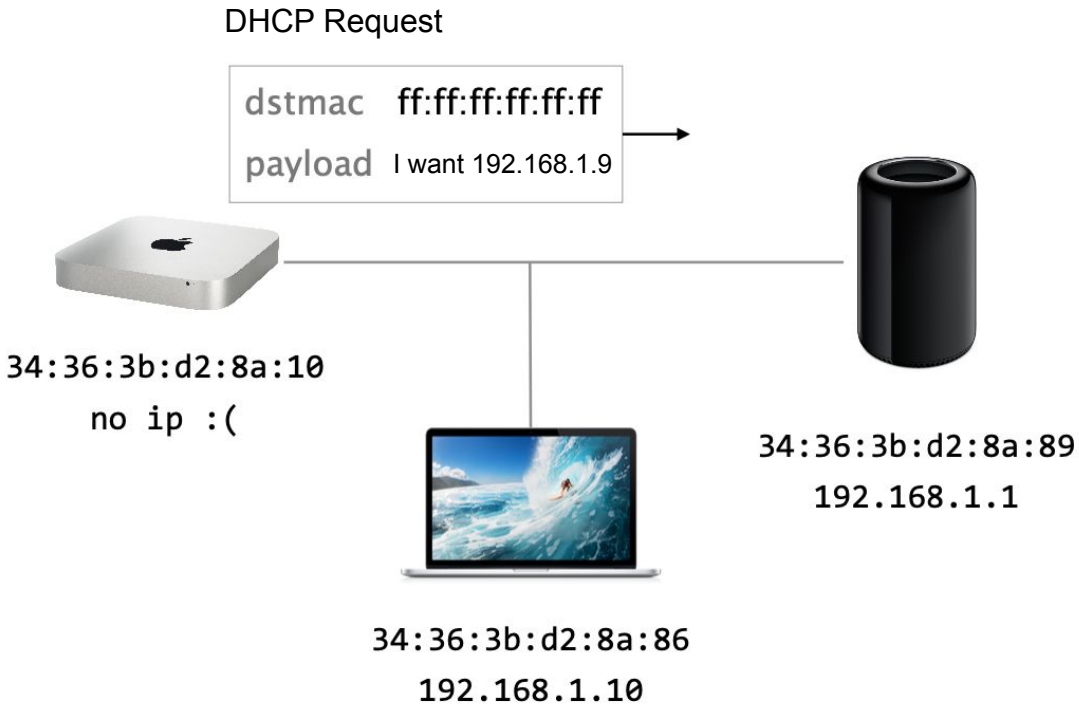
DHCP Discovery “Is the a DHCP Server out there?”using the Broadcast Address



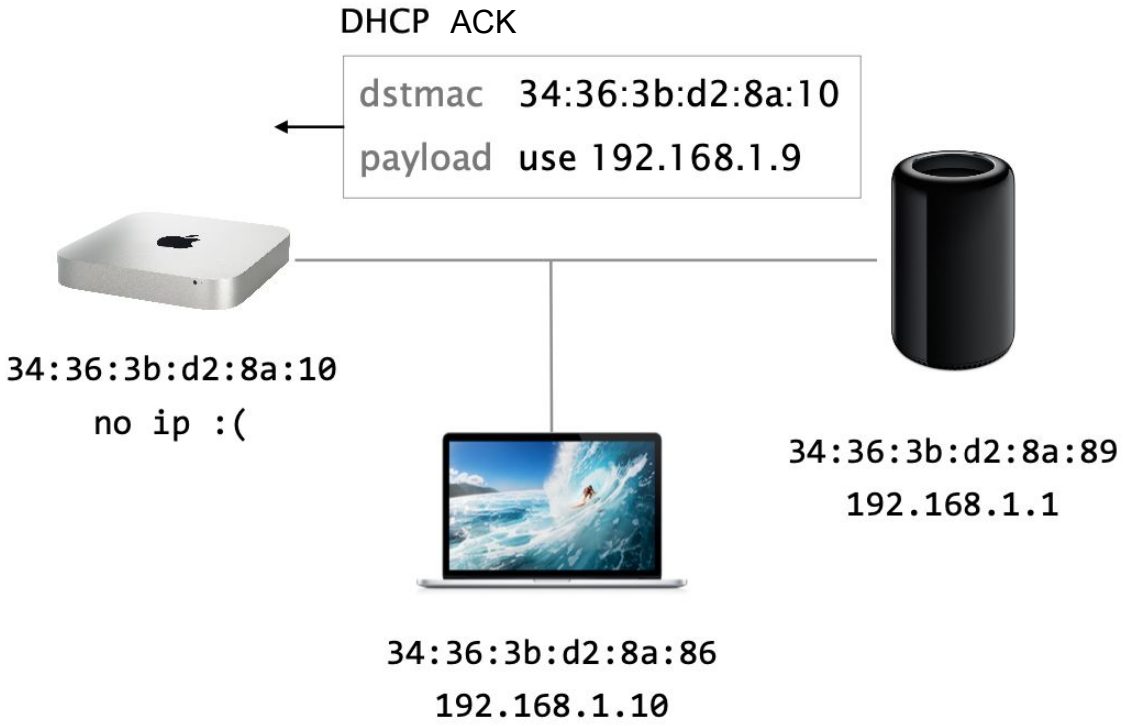
DHCP - Server (if there is one) Answers With an Offer



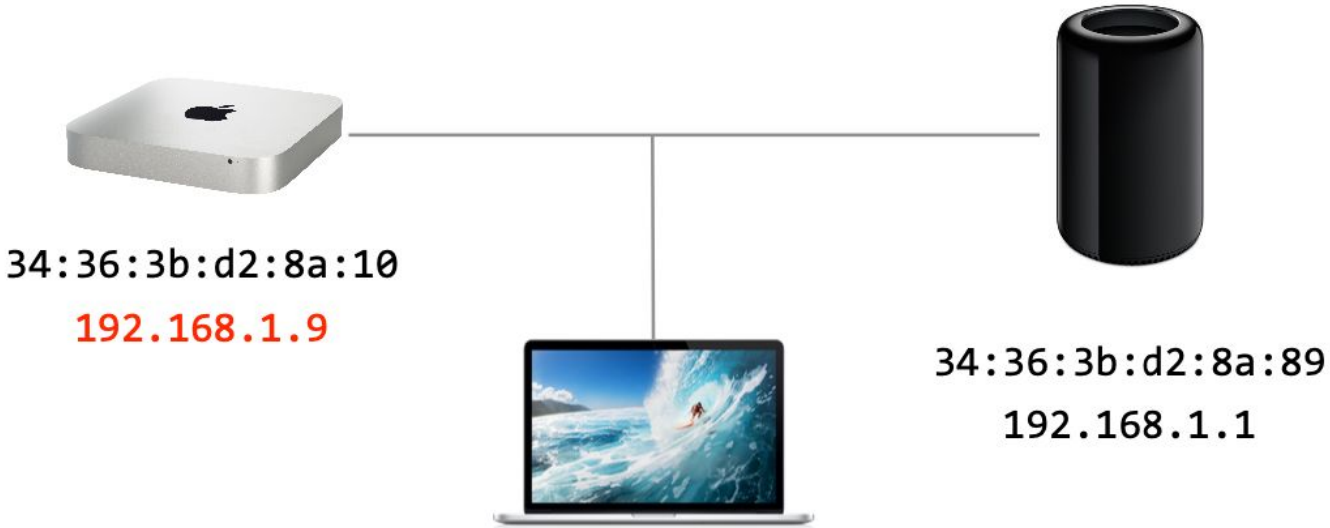
DHCP Request “Can I have this IP?”using the Broadcast Address



DHCP - Server Answers With an Acknowledgement



DHCP - Client Now Has an IP for the Lifetime of the Lease



DHCP

Download the pcap from https://teaching.pschmitt.net/EE449_Spring2023/exercises/dhcp.pcap

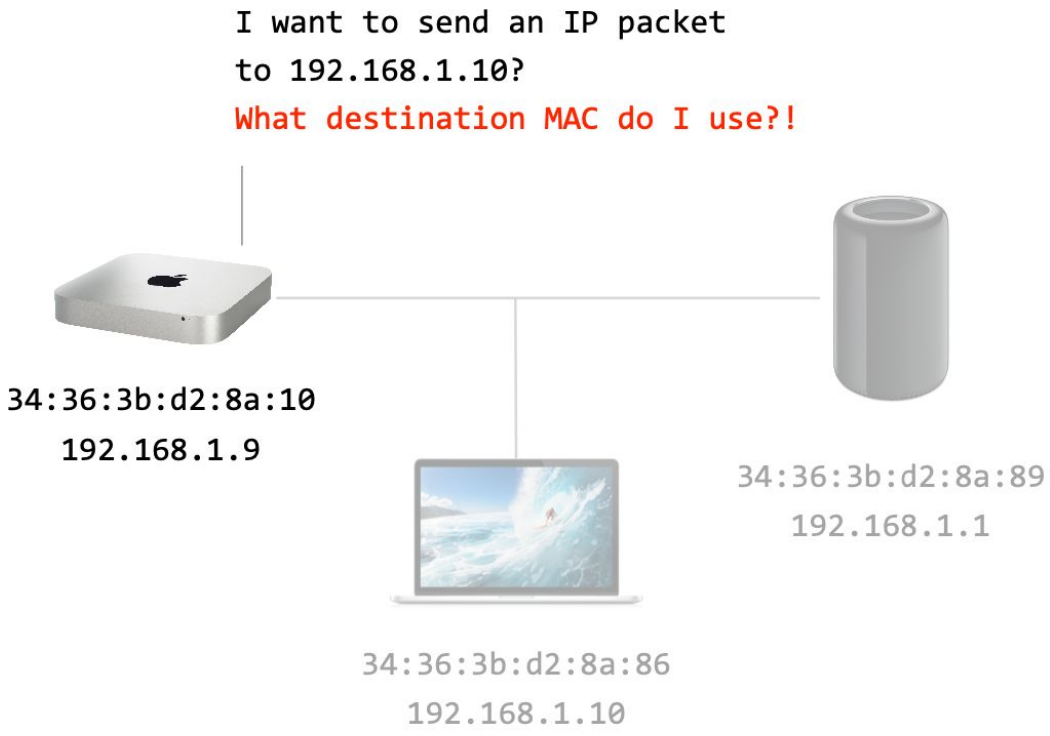
1. Are DHCP messages sent over UDP or TCP?
2. What is the link-layer (e.g., Ethernet) address of the host?
3. What values in the DHCP discover message differentiate this message from the DHCP request message?
4. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What is the purpose of the Transaction-ID field?
5. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange. If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange?
6. What is the IP address of the DHCP server?
7. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
8. Explain the purpose of the lease time. How long is the lease time in your experiment?

DHCP

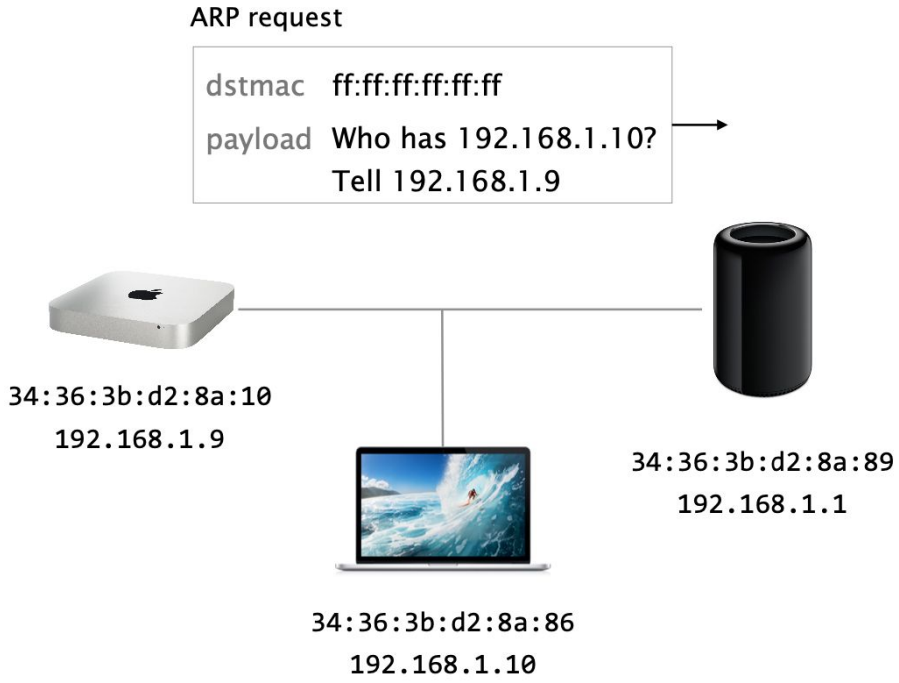
Download the pcap from https://teaching.pschmitt.net/EE449_Spring2023/exercises/dhcp.pcap

1. Are DHCP messages sent over UDP or TCP?
   UDP ports 67 and 68
2. What is the link-layer (e.g., Ethernet) address of the host?
   bc:d0:74:1a:75:19
3. What values in the DHCP discover message differentiate this message from the DHCP request message?
   Message type, Requested IP Address, DHCP Server, IP address lease time
4. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What is the purpose of the Transaction-ID field?
   0x9e03d8c2
5. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange. If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange?
   0.0.0.0->255.255.255.255; 192.168.86.1->192.168.86.123; 0.0.0.0->255.255.255.255; 192.168.86.1->192.168.86.123
6. What is the IP address of the DHCP server?
   192.168.86.1
7. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
   192.168.86.123 in the offer
8. Explain the purpose of the lease time. How long is the lease time in your experiment?
   The lease time is how long the server will hold the IP out of the pool from other potential users. Lease time is one day

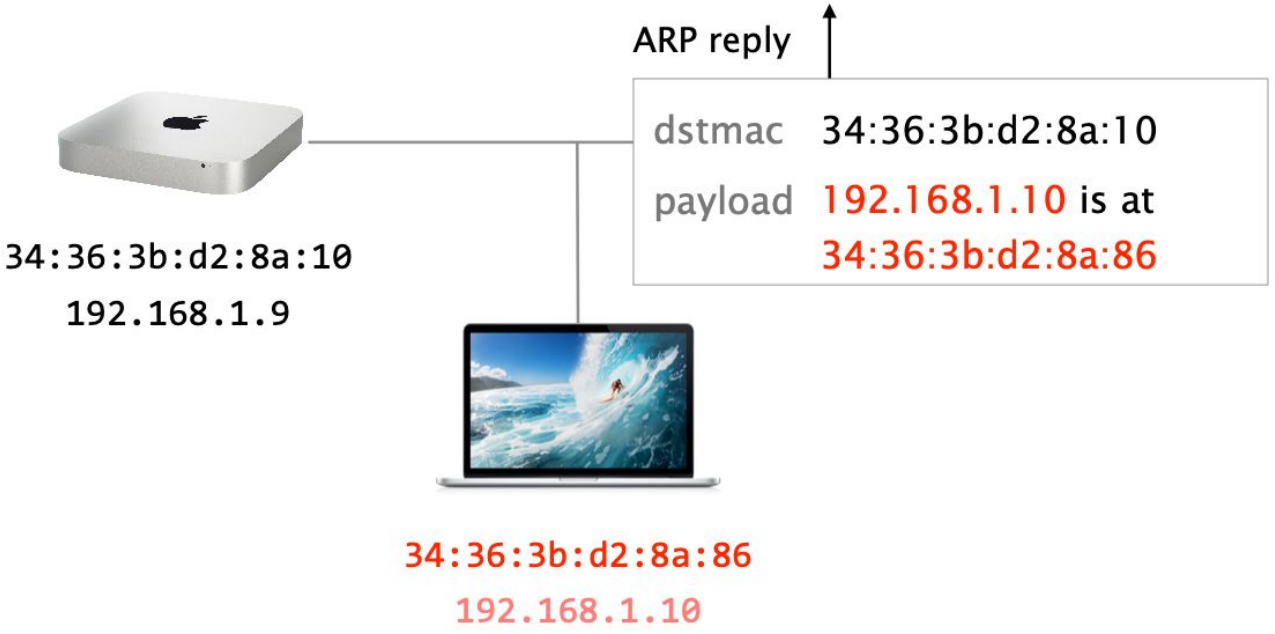
Address Resolution Protocol (ARP) Enables Hosts to Discover MACs Associated with IPs



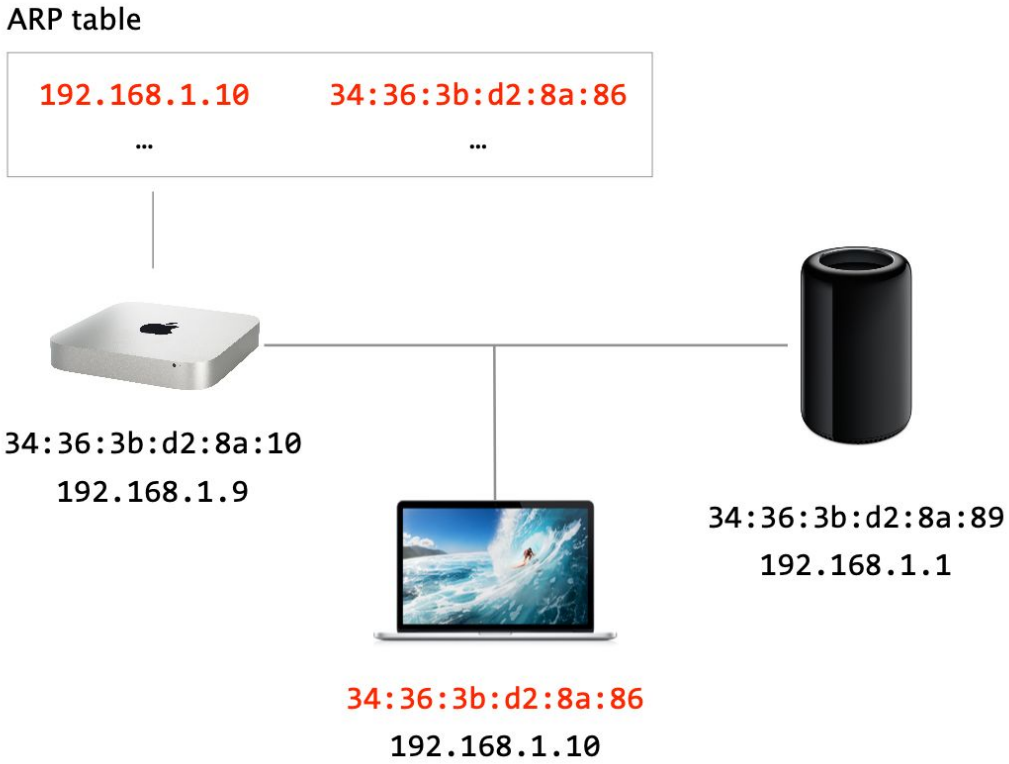
Address Resolution Protocol (ARP) Enables Hosts to Discover MACs Associated with IPs



Address Resolution Protocol (ARP) Enables Hosts to Discover MACs Associated with IPs



Address Resolution Protocol (ARP) Enables Hosts to Discover MACs Associated with IPs



ARP

ARP is stateless

- Hosts will automatically cache any ARP replies they receive, regardless of whether network hosts requested them.
- Even ARP entries that have not yet expired will be overwritten when a new ARP reply packet is received.
- There is no method in the ARP protocol by which a host can authenticate the peer from which the packet originated.
    - Allows ARP spoofing

ARP

Download the pcap from https://teaching.pschmitt.net/EE449_Spring2023/exercises/arp.pcap

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

2. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

3. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

4. What would happen if, when you manually added an entry to the ARP table, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

ARP

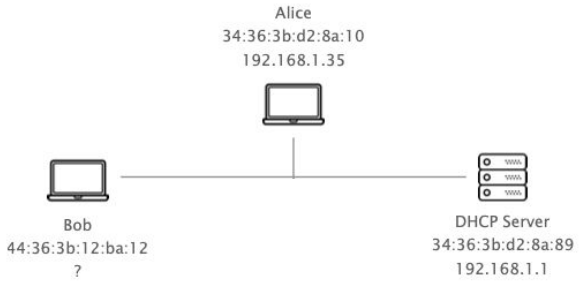
Download the pcap from https://teaching.pschmitt.net/EE449_Spring2023/exercises/arp.pcap

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
   Src: bc:d0:74:1a:75:19, Dst: ff:ff:ff:ff:ff:ff
2. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
   Target IP address
3. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
   Sender MAC Address
4. What would happen if, when you manually added an entry to the ARP table, you entered the correct IP address, but the wrong Ethernet address for that remote interface?
   The frames for that IP destination would be addressed using the ARP table entry, no NIC would process the frame (because it wouldn’t match them)

DHCP + ARP

The three hosts Bob, Alice and Eve are all connected to the same network, which has a DHCP server.

Bob just connected to the network and wants to send important IP packets to Alice. Bob only knows the IP address of Alice (192.168.1.35) and his laptop is not yet configured with an IP address.



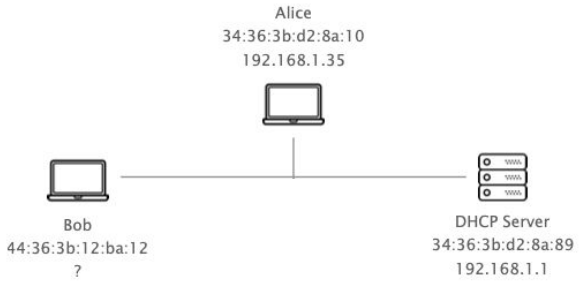
Question: Explain all the steps that are necessary such that Bob's computer can finally send packets to Alice.

SRC MAC	DST MAC	Message Type	Message Content

DHCP + ARP

The three hosts Bob, Alice and Eve are all connected to the same network, which has a DHCP server.

Bob just connected to the network and wants to send important IP packets to Alice. Bob only knows the IP address of Alice (192.168.1.35) and his laptop is not yet configured with an IP address.



Question: Explain all the steps that are necessary such that Bob's computer can finally send packets to Alice.

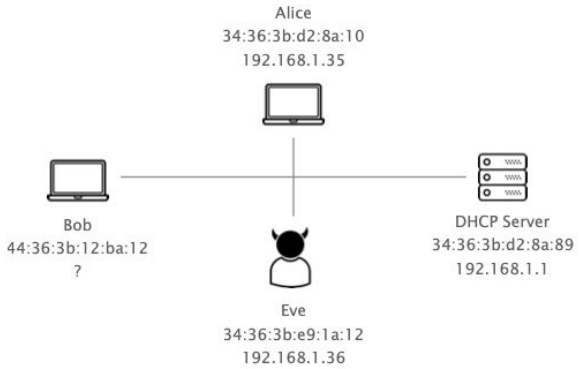
SRC MAC	DST MAC	Message Type	Message Content
44:36:3b:12:ba:12	ff:ff:ff:ff:ff:ff	DHCP discovery	I need an IP address
34:36:3b:d2:8a:89	44:36:3b:12:ba:12	DHCP offer	use 192.168.1.37
44:36:3b:12:ba:12	ff:ff:ff:ff:ff:ff	ARP request	Who has 192.168.1.35 Tell 192.168.1.37
34:36:3b:d2:8a:10	44:36:3b:12:ba:12	ARP reply	192.168.1.35 is at 34:36:3b:d2:8a:10

DHCP + ARP

The three hosts Bob, Alice and Eve are all connected to the same network, which has a DHCP server.

Bob just connected to the network and wants to send important IP packets to Alice. Bob only knows the IP address of Alice (192.168.1.35) and his laptop is not yet configured with an IP address.

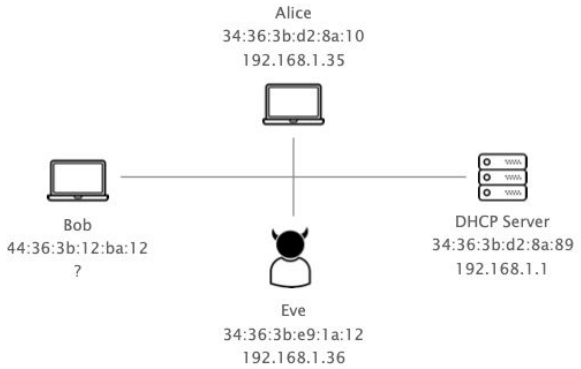
Question: Eve is very interested to find out what Bob is sending to Alice. What could she do to intercept Bob's packets?



DHCP + ARP

The three hosts Bob, Alice and Eve are all connected to the same network, which has a DHCP server.

Bob just connected to the network and wants to send important IP packets to Alice. Bob only knows the IP address of Alice (192.168.1.35) and his laptop is not yet configured with an IP address.



Question: Eve is very interested to find out what Bob is sending to Alice. What could she do to intercept Bob's packets?

Solution: When Bob sends the ARP request to learn the MAC address of Alice, Eve also receives it as it is destined to the MAC broadcast address (ff:ff:ff:ff:ff:ff). If Eve can send a fake reply to Bob before Alice does so, she can make Bob believe that her MAC address is the one of Alice. This is ARP spoofing.

Link Layer

1. What is a link?
2. How do we share a network medium?
3. How do we identify link adapters?
4. What is Ethernet?
5. How do we interconnect segments at the link layer?

Ethernet

was originally a broadcast technology (based on Aloha)

- each packet was received by all attached hosts

is *the* dominant wired LAN technology

- by far the most widely used

kept up with the speed race

- from 10 Mbps to 400 Gbps (next: 800 Gbps and 1.6 Tbps)

Ethernet Topology

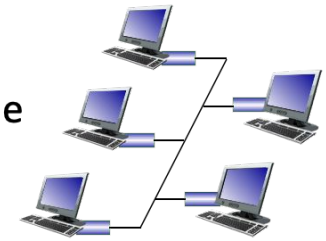
bus: popular through mid 90s

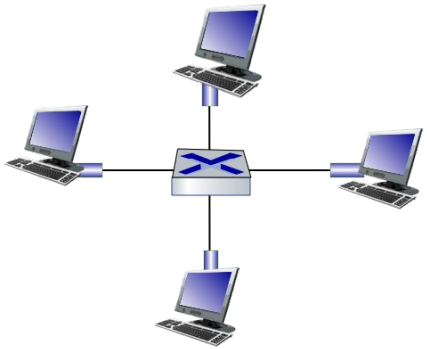
- all nodes in same collision domain (can collide with each other)

switched: prevails today

- active link-layer 2 switch in center
- each “spoke” runs a (separate) Ethernet protocol (nodes do not collide with each other)

bus: coaxial cable





switched

Ethernet Frame

sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

preamble:

- used to synchronize receiver, sender clock rates
- 7 bytes of 10101010 followed by one byte of 10101011

Ethernet Frame

sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

- addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- type: indicates higher layer protocol
  - mostly IP but others possible, e.g., Novell IPX, AppleTalk
  - used to demultiplex up at receiver
- CRC: cyclic redundancy check at receiver
  - error detected: frame is dropped

Ethernet Offers Unreliable, Connectionless Service

unreliable	Receiving adapter does not acknowledge anything Packets passed to the network layer can have gaps which can be filled by the transport protocol (TCP)
connectionless	No handshaking between the send and receive adapter

Ethernet CSMA/CD

1. NIC receives datagram from network layer, creates frame

2. NIC senses channel:
   a. if idle: start frame transmission.
   b. if busy: wait until channel idle, then transmit

3. If NIC transmits entire frame without collision, NIC is done with frame

4. If NIC detects another transmission while sending: abort, send jam signal

5. After aborting, NIC enters binary (exponential) backoff:
   a. after mth collision, NIC chooses K at random from {0,1,2, …, 2m-1}. NIC waits K·512 bit times, returns to Step 2
   b. more collisions: longer backoff interval

Link Layer

1. What is a link?
2. How do we share a network medium?
3. How do we identify link adapters?
4. What is Ethernet?
5. How do we interconnect segments at the link layer?