Internet Protocols

Supporting Protocols and Framing

Protocols and interfaces

- A **Protocol** is a set of rules required for two or more ***similar*** processes to communicate with each other.

- An **Interface** is a set of rules required for two or more ***dissimilar*** processes to communicate with each other.

- A protocol is a ***logical*** concept, while an interface is a ***physical*** one.

Functions of Protocol

1. Help in establishing necessary CONVENTIONS.
2. Help in establishing the STANDARDS.
3. Help in establishment of STANDARD DATA ELEMENTS

Layers and Their Functionalities

- The Physical Layer (Following parameters are specified)
  - Voltage and current levels
  - Timings of voltage changes – how many microsec a bit occupies
  - Physical data rates
  - Maximum transmission distances
  - Physical Connectivity – RJ45, SFP etc.
  - Connection types - (i) Point-to-point (ii) Multipoint
  - Physical topology – (i) Bus, (ii) Ring, (iii) Star (iv) Mesh etc. (Note: Physical topology indicates actual physical connectivity)
  - Digital and Analog singalling
  - Bit synchronization – (i) Synchronous (ii) Asynchronous
  - Bandwidth usage – (i) Broadband (ii) Baseband
  - Multiplexing on – (i) Frequency (ii) Time (iii) Statistical time division
- Network components
  - Connectors and cables
  - Electrical and data communication interfaces – NICs
  - Concentrators, hubs and repeaters
  - Modems, Transmission media converters etc.

Layers and Their Functionalities – Contd.

- The Link Layer
  - Media Access Control (MAC) Sub Layer – controlling the transmission
    - Logical topology – Bus, Ring
    - Media Access (i.e. Contention, Token passing, polling)
    - Addressing methodology – w.r.t. the actual physical device
  - Logical Link Control (LLC) sub layer – establishes and maintains the link for transmitting data frames from one device to another.
    - Transmission synchronization – Synchronous, Asynchronous, Isochronous
    - Connection services – Flow control and error handling
  - Responsibilities
    - Organizing the 1's and 0's supplied by physical layer into groups of logical information called 'frames'
    - Utilization of line links
    - Error notification (and correction)
    - Ordered delivery of frames
- Network components
  - Bridges
  - Network interface boards
  - Switches

Layers and Their Functionalities – Contd.

- The Network Layer
  - Providing connectivity and path selection between two end systems that may be located on geographically diverse ‘subnetworks’
  - ROUTING
  - Responsibilities
    - Addressing – Logical Network address and service address
    - Switching
      - Circuit Switching
      - Message switching
      - Packet Switching
    - Route analysis
    - Route selection
    - Connection services – Network layer flow, error handling and packet sequence control
    - Network services – Network layer translation.
- Network components
  - Router
  - Layer-3 switches

Supporting Protocols

- ARP / RARP
- BOOTP
- ICMP
- DHCP
- NAT

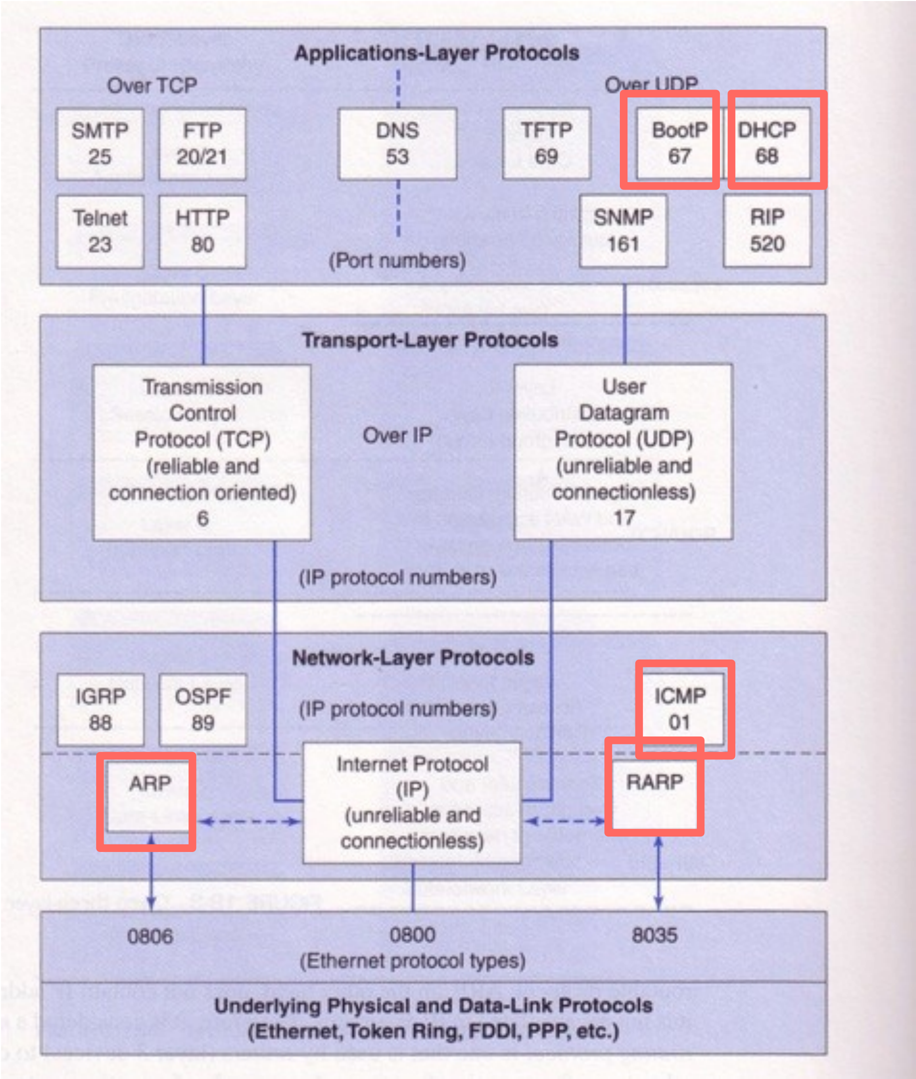
IP Supporting Protocols

IP protocol only deals with the data transfer (best-effort)

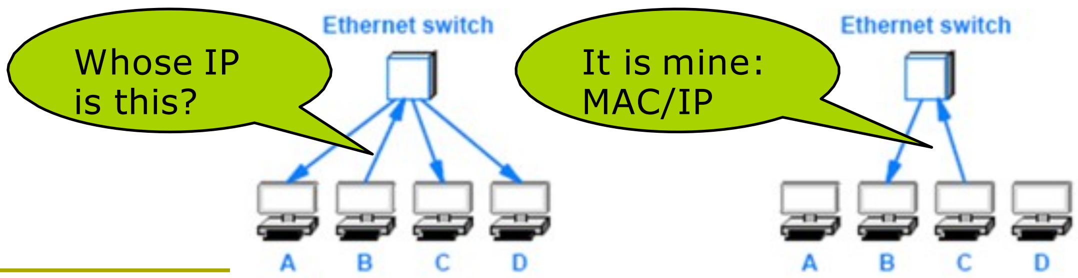
- Possible Errors that can happen and not detected by IP: Data lost, duplication, out-of-order
- However there are some error checking mechanisms:
  - CRC, TTL

IP Supporting Protocols

We focus on the following Protocols: ICMP, ARP, RARP, BOOTP, DHCP



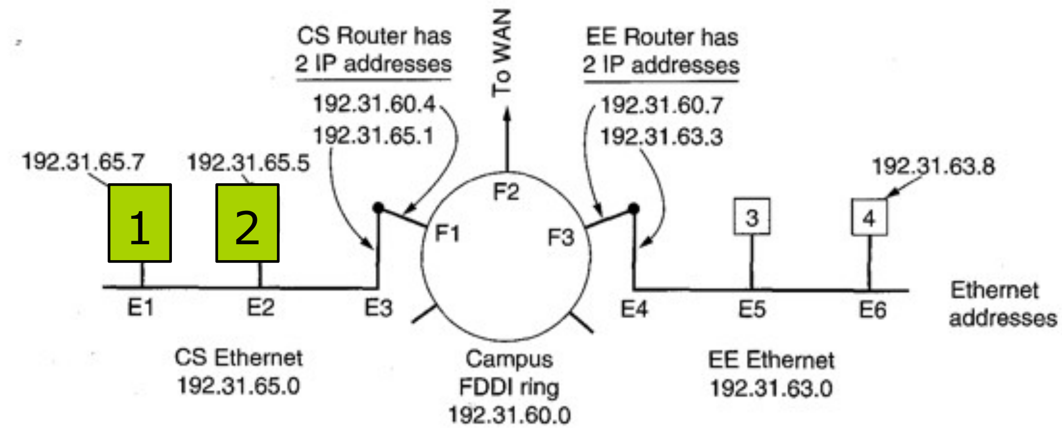
ARP



(Address Resolution Protocol)

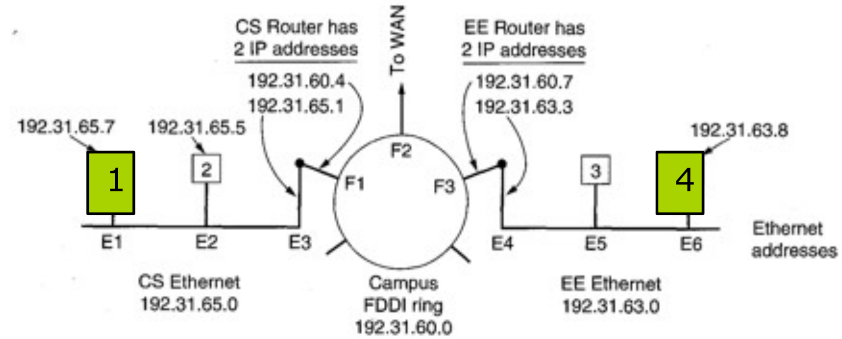
- Used to resolve network layer addresses into link layer addresses
- Exploits broadcast property of a LAN
- Each host on LAN maintains a table of IP subnetwork addresses
- If the address can not be found ARP broadcasts a request
  - Shouting: Who knows about this IP address?
- Other hosts listen and reply
  - The reply includes IP address and MAC (unicast)
  - Any interested host can learn about the new information

ARP Example



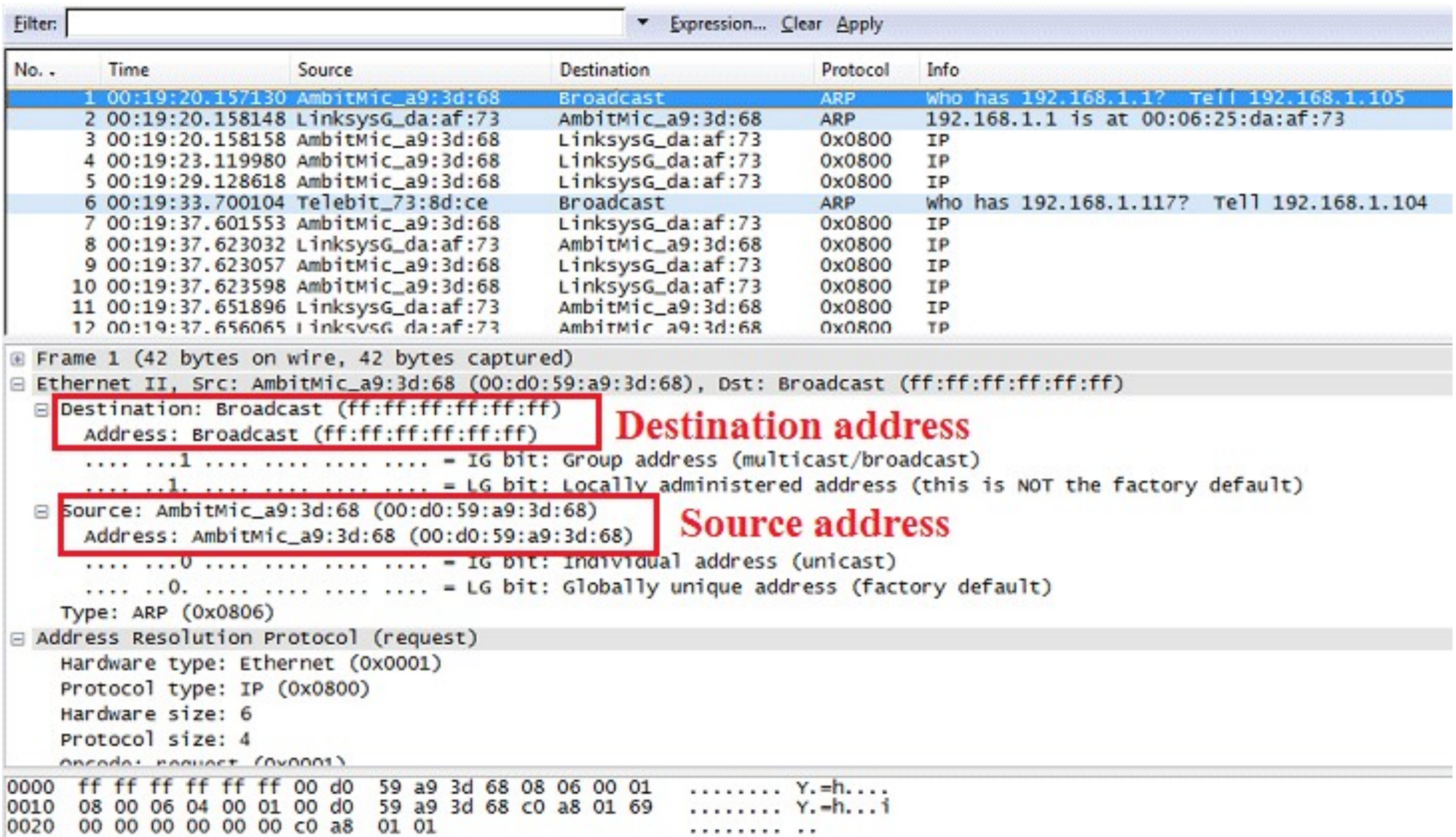
- Assume **1** is sending a message to **2** (192.31.65.5)
  - What is the MAC address for 192.31.65.5? Use ARP broadcast!
    - Host 2 responds to Host 1: it is E2
  - Host 1 maps IP and MAC;
    - Encapsulate the IP message in the Ethernet frame and sends it
  - Cashing can enhance ARP operation (Node 1 can cash the result)

ARP Example

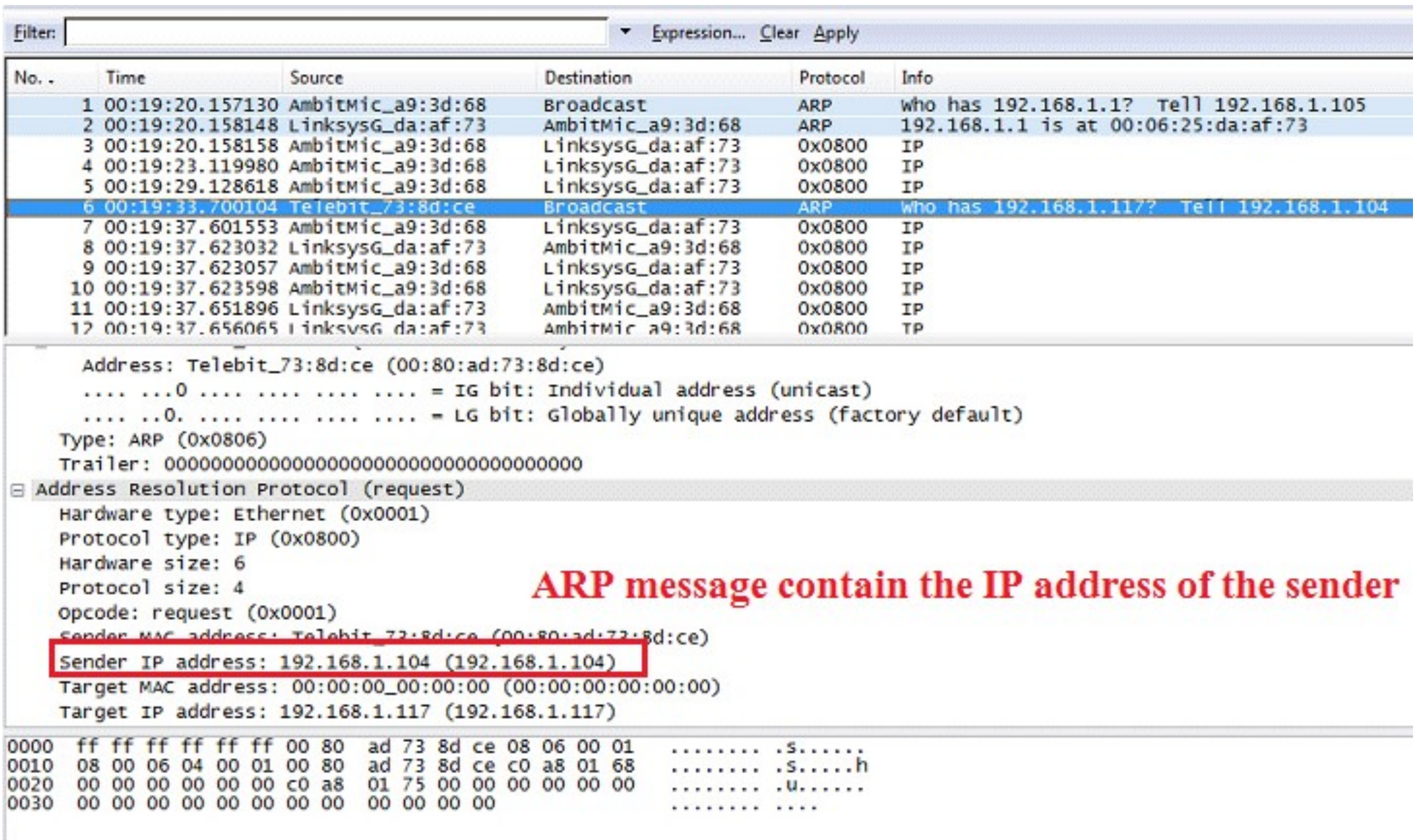


- Assume **1** is sending a message to **4** (rose@ee.sonoma.edu)
  - ee.sonoma.edu is the destination
  - Host **1** sends a message to Domain Name System (DNS): what is the IP address for ee.sonoma.edu? →192.31.63.8
  - What is the MAC address for 192.31.63.8? ARP cannot pass through the router!
- Two choices:
  1. Reconfigure routers to respond to ARP (Proxy ARP)
     - The ARP Proxy is aware of the location of the destination
     - Proxy offers its own MAC address
     - Thus, it acts on behalf of the node: "send it to me, and I'll get it to where it needs to go."
     - In this example the Proxy can be E4
  2. Send the message to the LAN router
     - Note that ARP is limited to a single network
     - In the example above, the address binding or resolution is done between Node 1 and E3; then between E3 and E4; then E4 and node 4 (via broadcast).
     - Node 4 will send back its MAC to node 1 (not found in ARP cache)
     - Each router looks at the IP address and passes it to the next node using the routing table

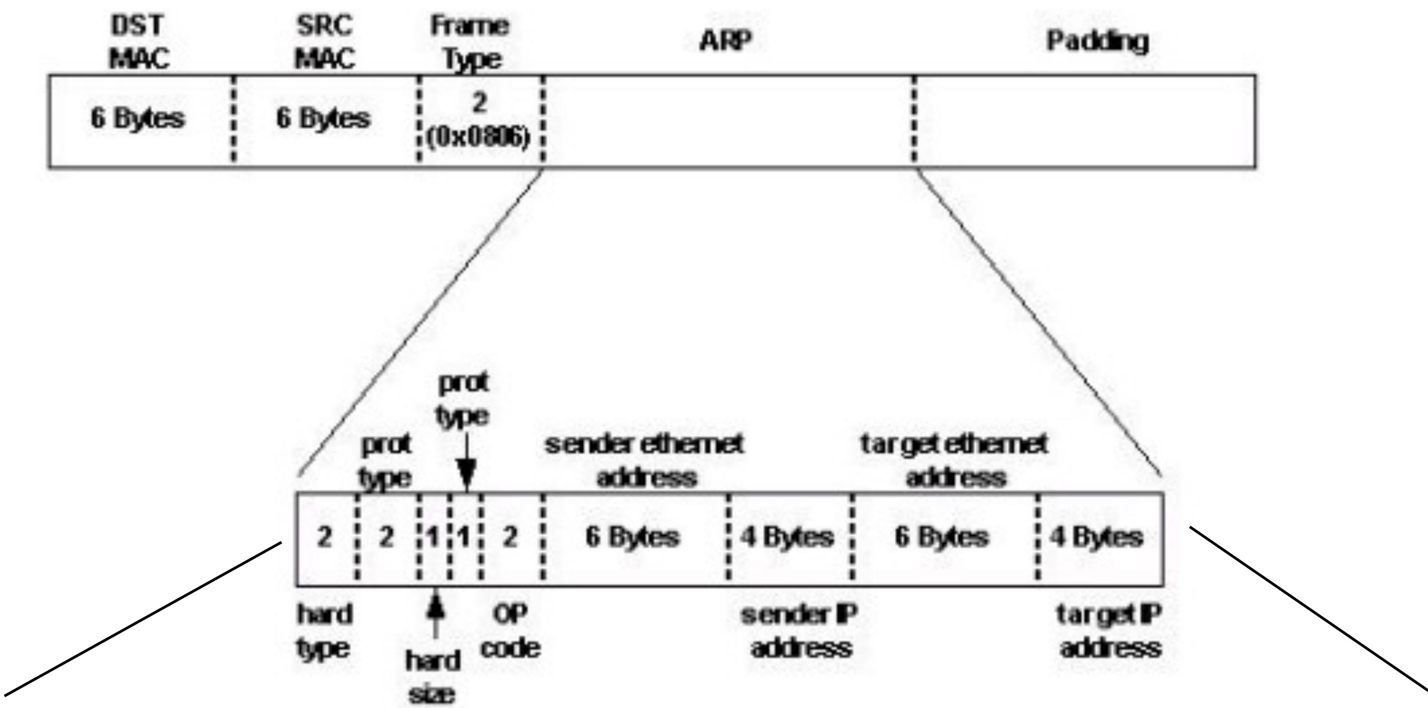
ARP Request Content - Broadcast



ARP Request Content –
Contains IP Address



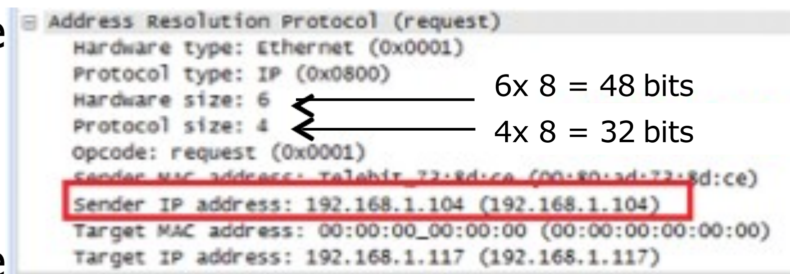
ARP Message Format



0	8	16	24 / 31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE	
HADDR LEN	PADDR LEN	OPERATION	
SENDER HADDR (first 4 octets)			
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)	
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)	
TARGET HADDR (last 4 octets)			
TARGET PADDR (all 4 octets)			

ARP Message Format

0	8	16	24 – 31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE	
HADDR LEN	PADDR LEN	OPERATION	
SENDER HADDR (first 4 octets)			
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)	
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)	
TARGET HADDR (last 4 octets)			
TARGET PADDR (all 4 octets)			



- HARDWARE ADDRESS TYPE
  - 16-bit field that specifies the type of hardware address being used
  - the value is 1 for Ethernet
- PROTOCOL ADDRESS TYPE
  - 16-bit field that specifies the type of protocol address being used
  - the value is 0x0800 for IPv4
- HADDR LEN
  - 8-bit integer that specifies the size of a hardware address in bytes
- PADDR LEN
  - 8-bit integer that specifies the size of a protocol address in bytes
- OPERATION
  - 16-bit field that specifies whether the message

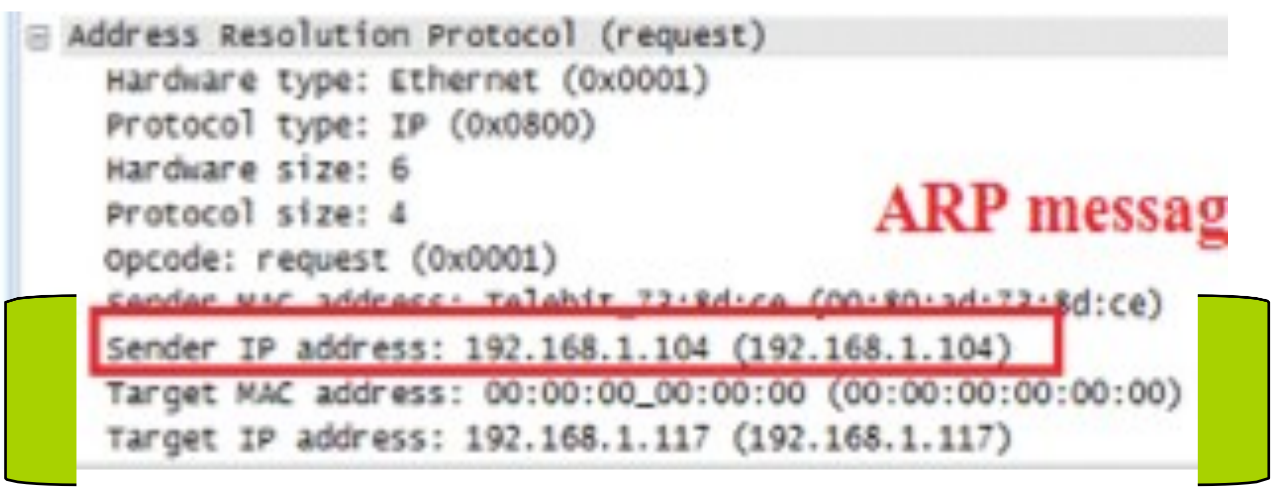
    request (the field contains 1) or

    response (the field contains 2)

ARP Message Format

0	8	16	24 31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE	
HADDR LEN	PADDR LEN	OPERATION	
SENDER HADDR (first 4 octets)			
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)	
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)	
TARGET HADDR (last 4 octets)			
TARGET PADDR (all 4 octets)			

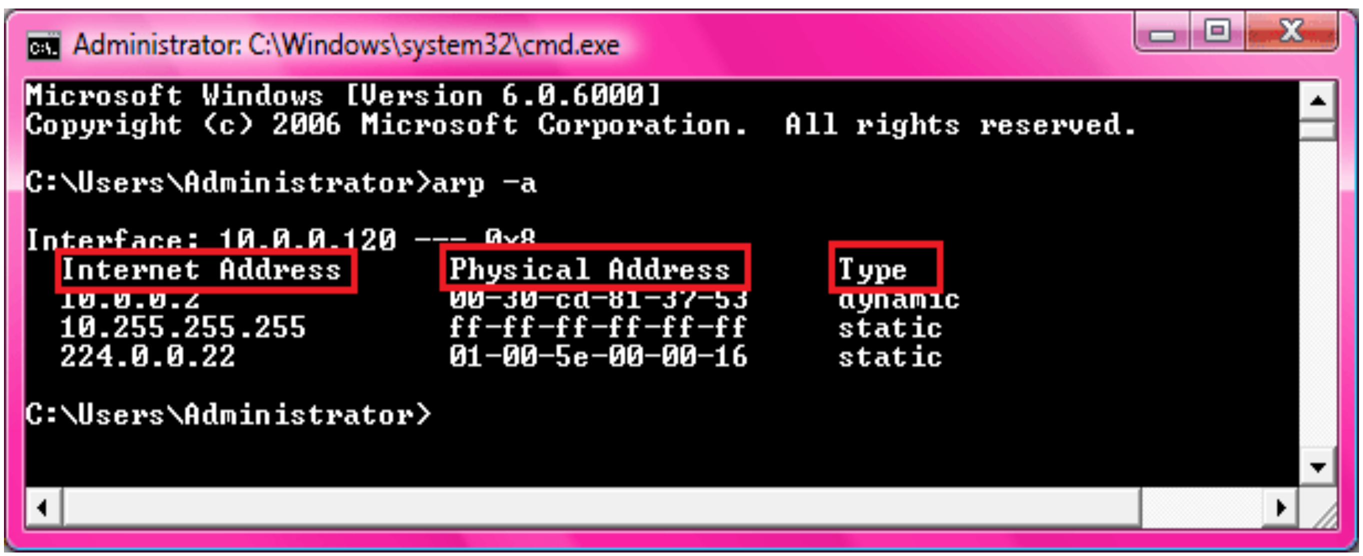
- SENDER HADDR
  - HADDR LEN bytes for the sender's hardware address
- SENDER PADDR
  - PADDR LEN bytes for the sender's protocol address
- TARGET HADDR
  - HADDR LEN bytes for the target's hardware address
- TARGET PADDR
  - PADDR LEN bytes for the target's protocol address



Notes

- ARP is encapsulated in Ethernet frame
  - In this case Ethernet type will be ARP
- Sending ARP for each message is not efficient
  - Thus, cache is used (create a small local table)
  - The cache is checked before broadcasting the request

Cashed Results:

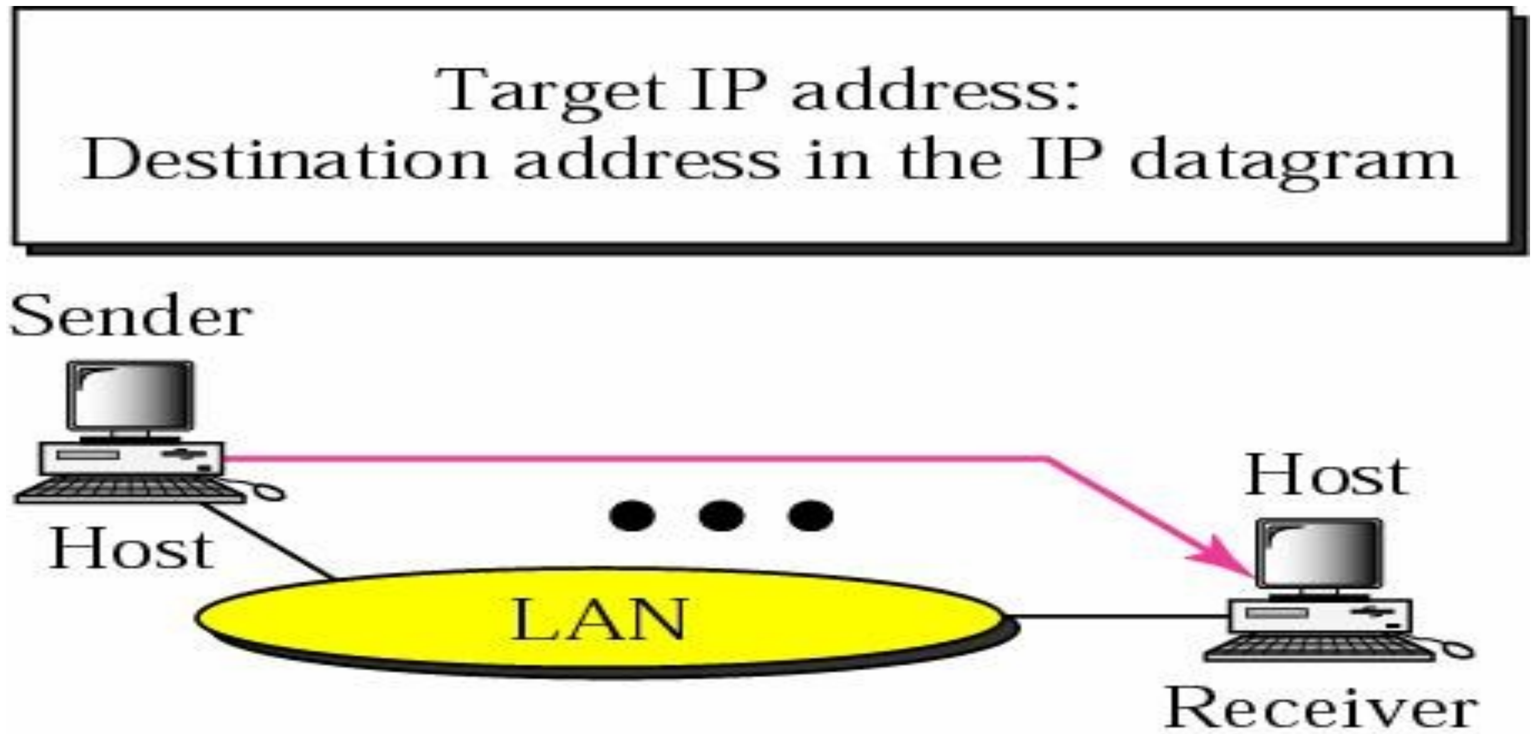


Four Cases to Use ARP

- ***Case 1:*** The sender is a host and wants to send a packet to another host on the same network
  - Use ARP to find another host's physical address

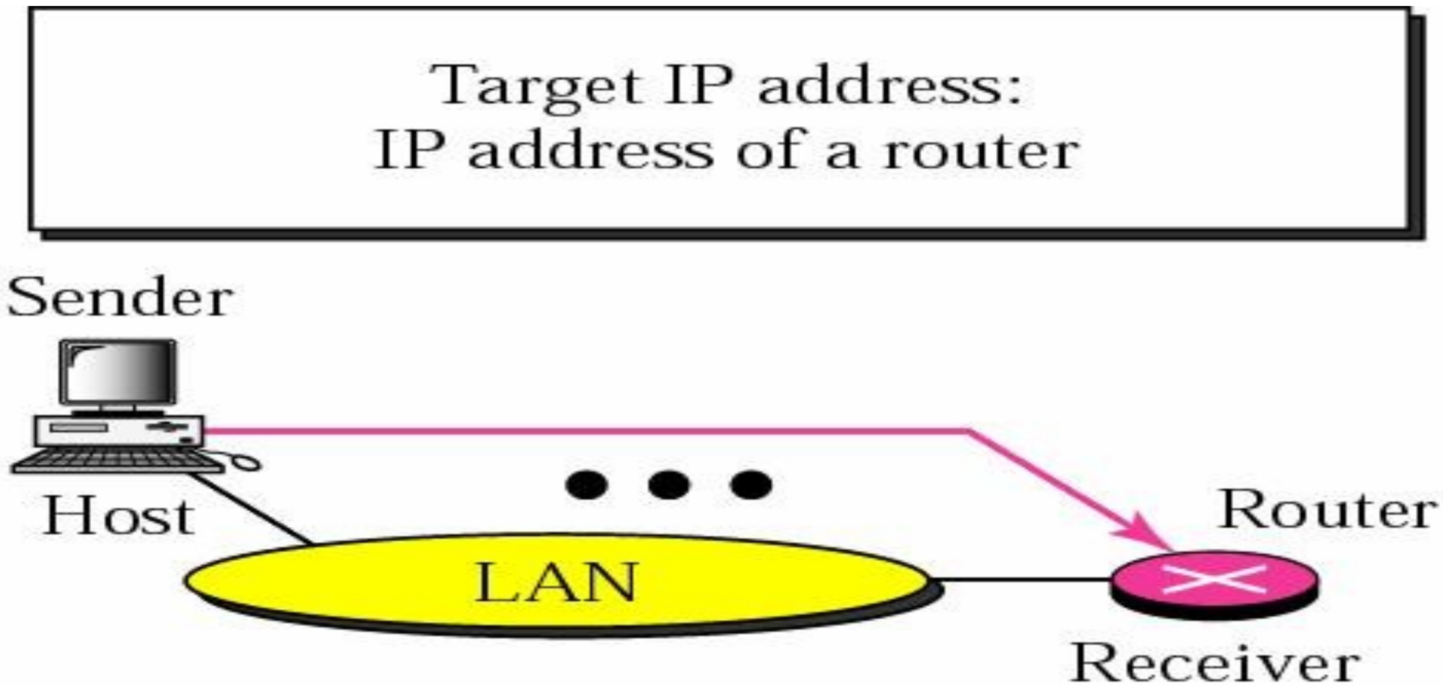
- ***Case 2:*** The sender is a host and wants to send a packet to another host on another network
  - Sender looks at its routing table
  - Find the IP address of the next hop (router) for this destination
  - Use ARP to find the router's physical address

Four Cases Using ARP: Case 1



Case 1. A host has a packet to send to another host on the same network.

Four Cases Using ARP: Case 2

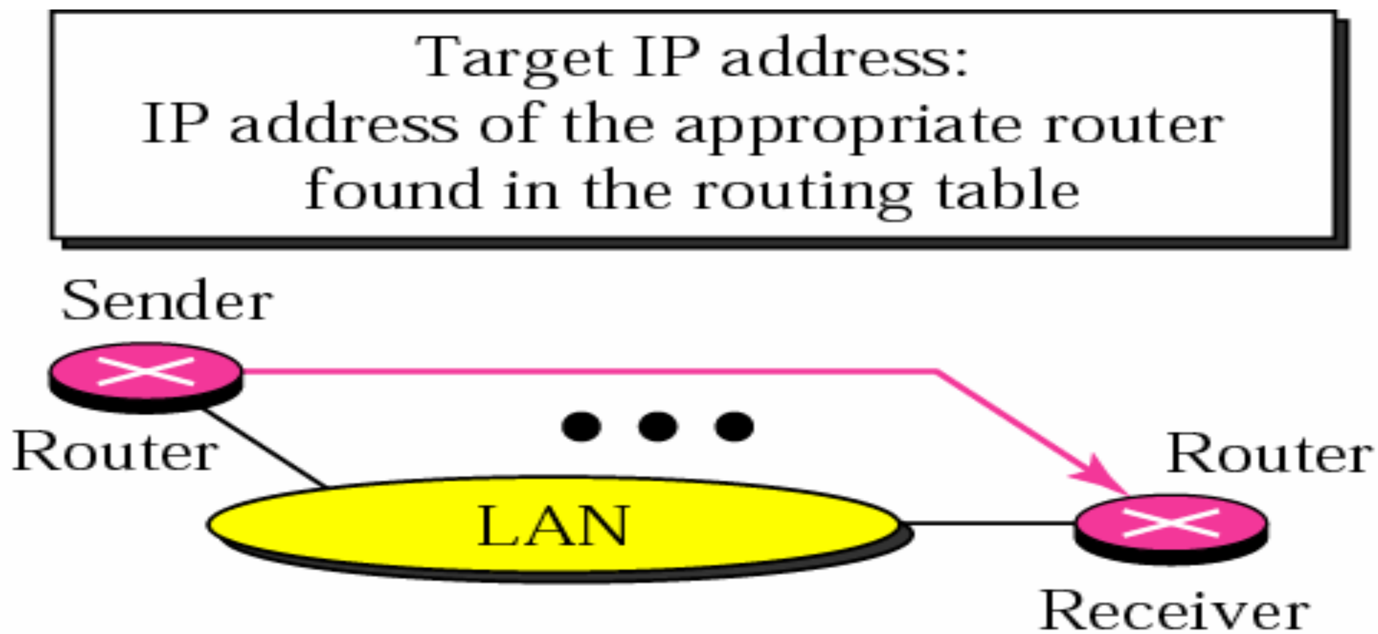


Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

Four Cases to Use ARP (Cont.)

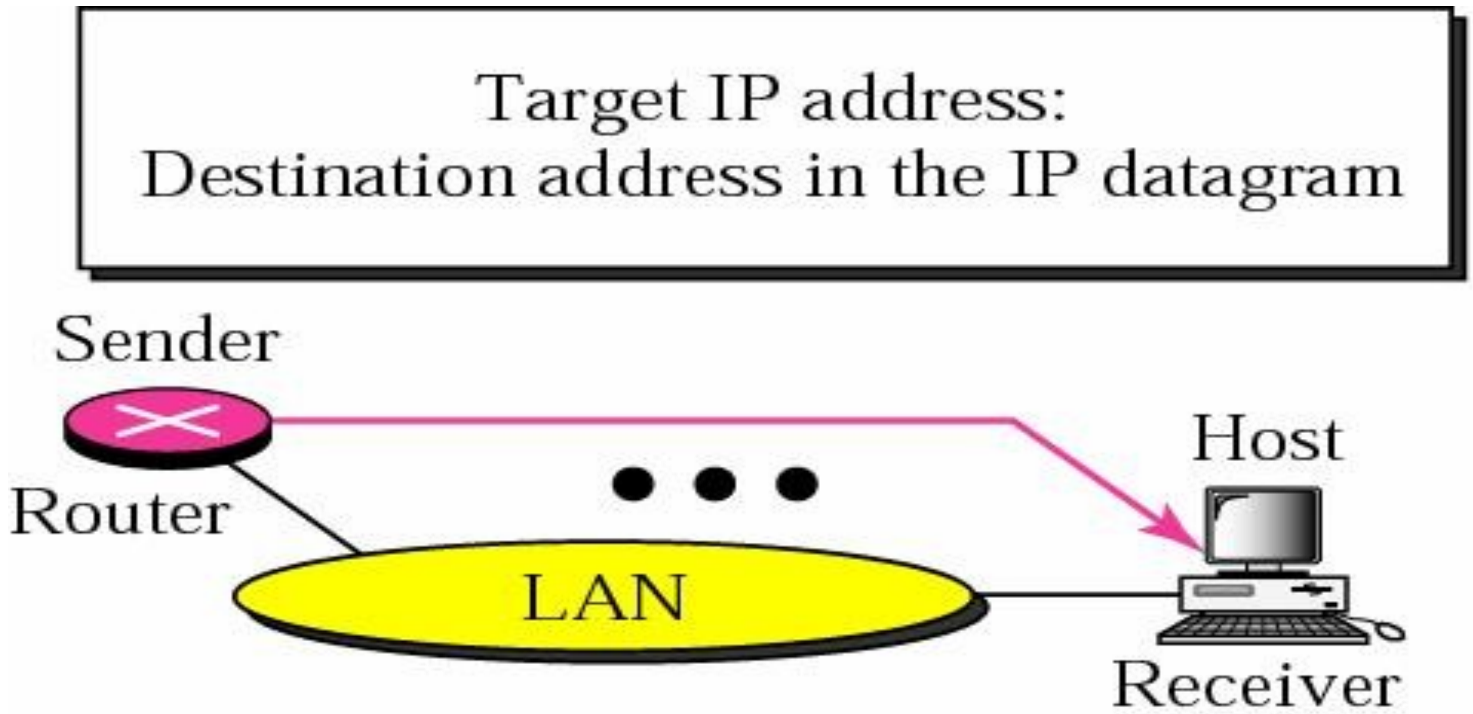
- ***Case 3:*** the sender is a router and received a datagram destined for a host on another network
  - Router check its routing table
  - Find the IP address of the next router
  - Use ARP to find the next router's physical address
- ***Case 4:*** the sender is a router that has received a datagram destined for a host in the same network
  - Use ARP to find this host's physical address

Four Cases Using ARP: Case 3



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

Four Cases Using ARP: Case 4



Case 4. A router receives a packet to be sent to a host on the same network.

Proxy ARP

- Used to create a subnetting effect
- A router running a proxy ARP
  - Its ARP acts on behalf of a set of hosts
  - If it receives an ARP request message looking for the address of one of these host
    - The router sends an ARP reply announcing its own hardware (physical) address
  - After the router receives the actual IP packet
    - It sends the packet to the appropriate host or router

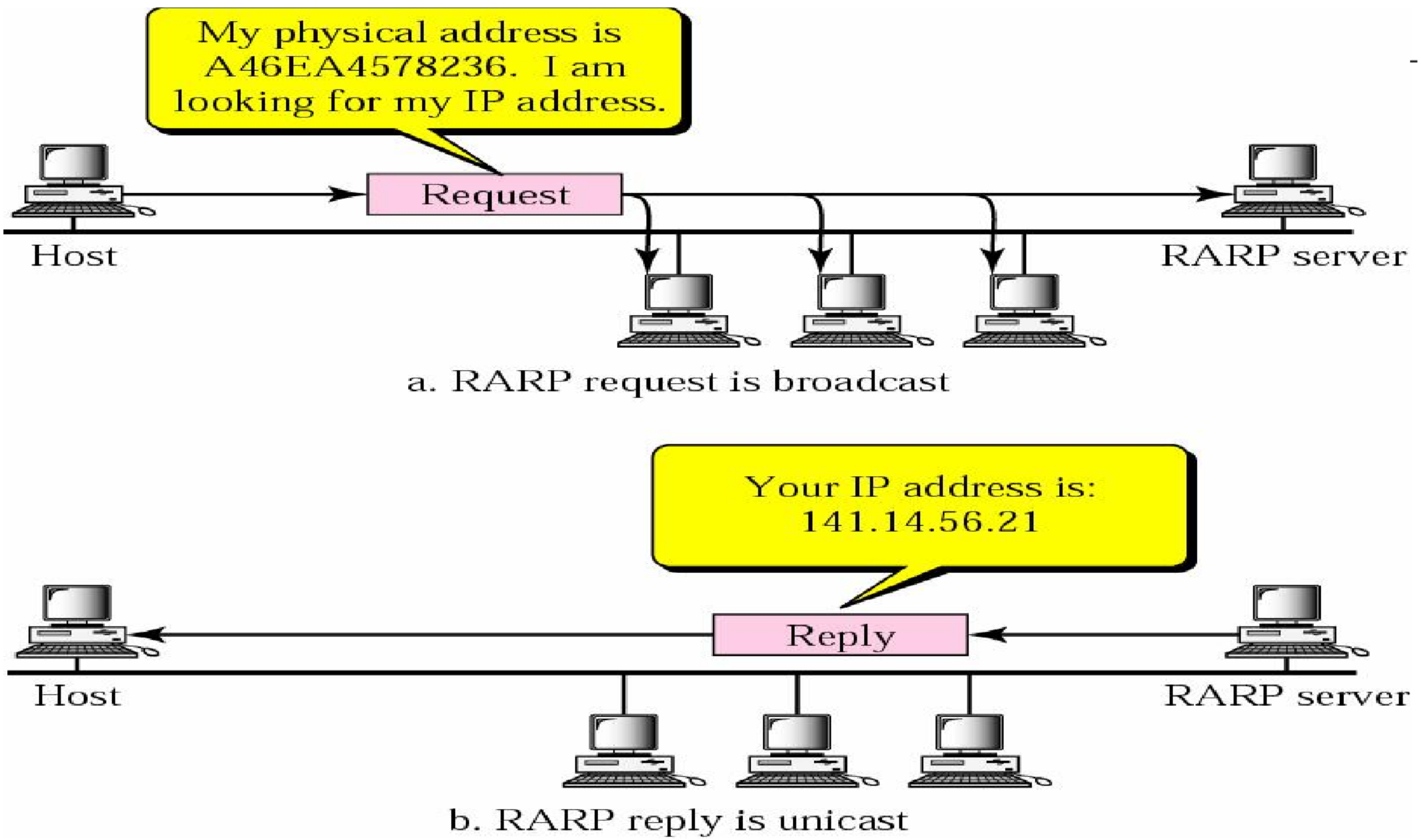
Gratuitous ARP

- ARP message for its own IP address
- Used during bootstrap time to check if no other host is configured with the same IP address.

Reverse ARP

- A diskless machine is usually booted from ROM
- It cannot include the IP address
  - IP address are assigned by the network administrator
- Obtain its logical address by the physical address using the RARP protocol

RARP Operation



Alternative Solutions to RARP

- When a diskless computer is booted, it needs more information in addition to its IP address
  - The subnet mask
  - The IP address of a router
  - The IP address of a name server
- RARP cannot provide this extra information
- Two protocols, BOOTP and DHCP, can be used instead of RARP

RARP and BOOTP

- Reverse ARP translates the Ethernet address to IP address
  - A diskless machine when it is booting can ask: My MAC is 12.03.23.43.23.23; what is my IP?
- RARP broadcasts the question (destination address is all one)
  - Not passed through the router!
- Major issue: Each LAN needs a RARP server!
- Bootstrap protocol uses UDP and forwards over routers
  - BOOTP is usually used during the bootstrap process - when a computer is starting up
  - Mapping must be done manually in each router!

Dynamic Host Configuration Protocol

- DHCP allows a computer to join a new network and obtain an IP address automatically
  - The concept has been termed plug-and-play networking
- Replaces BOOTP and RARP
  - Extension of BOOTP data format
- DHCP uses UDP
  - UDP port 67 for sending data to the server
  - UDP port 68 for data to the client
- DHCP communications are connectionless in nature

Dynamic Host Configuration Protocol

- DHCP has four basic phases:
  - IP discovery, IP lease offer, IP request, and IP lease acknowledgement
- First DHCP server must be discovered
  - The client broadcasts messages on the physical subnet to discover available DHCP servers
- IP Lease Offer
  - When a DHCP server receives an IP lease request from a client, it reserves an IP address for the client and extends an IP lease offer by sending a DHCP OFFER message to the client

No.	Len	Time	Source	Destination	Protocol	Info
1	314	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID
2	342	0.000295	192.168.0.1	192.168.0.10	DHCP	DHCP Offer - Transaction ID
3	314	0.070031	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID
4	342	0.070345	192.168.0.1	192.168.0.10	DHCP	DHCP ACK - Transaction ID

http://wiki.wireshark.org/DHCP

Dynamic Host Configuration Protocol

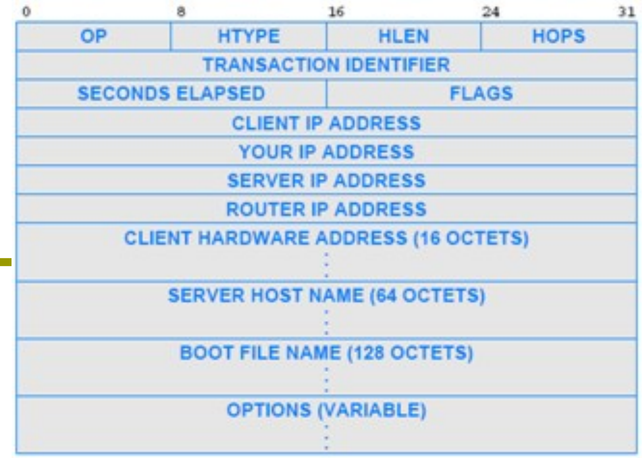
- A client can receive multiple offers from difference servers
  - Thus, it must request an IP address
- DHCP sends a Request packet to the DHCP server and receives a DHCP Reply
  - What is the IP address for this MAC?
  - It can also request its previous IP address!
- Even when an IP address is assigned, how long is it good for?
  - Before the IP address is removed find another IP address….called Leasing
- When the DHCP server receives the Request from the client, the configuration process enters its final phase
  - a DHCPACK (ACK) packet is sent to the client

No.	Len	Time	Source	Destination	Protocol	Info
1	314	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID (
2	342	0.000295	192.168.0.1	192.168.0.10	DHCP	DHCP Offer - Transaction ID (
3	314	0.070031	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID (
4	342	0.070345	192.168.0.1	192.168.0.10	DHCP	DHCP ACK - Transaction ID (

DHCP

- DHCP includes several important details that optimize performance, such as the following:
- Recovery from loss or duplication
  - DHCP is designed to insure that missing or duplicate packets do not result in misconfiguration
  - If no response is received
    - a host retransmits its request (remember DHCP uses UDP!)
  - If a duplicate response arrives
    - a host ignores the extra copy
- Caching of a server address
  - once a host finds a DHCP server
    - the host caches the server's address
- Avoidance of synchronized flooding
  - DCHP takes steps to prevent synchronized requests
  - Synchronization can occur when all computers boot up at the same time!

DHCP Format



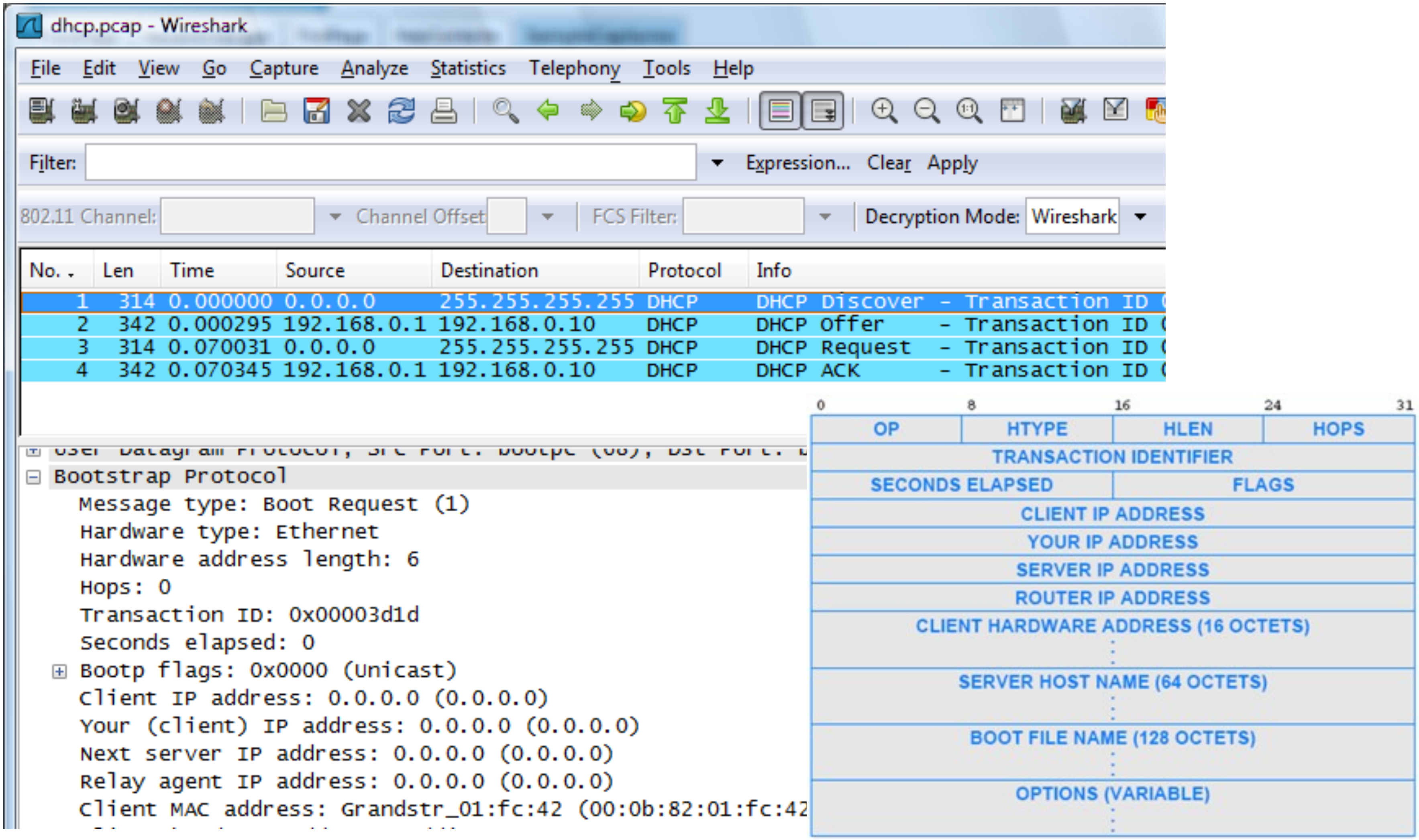
DHCP adopted a slightly modified version of the BOOTP message format

DHCP message format

- OP specifies whether the message is a <u>Request or a Response</u>
- HTYPE and HLEN fields specify the network hardware type and the length of a hardware address
- FLAGS specifies whether it can receive <u>broadcast or directed replies</u>
- HOPS specifies how many hops to the <u>server</u>
- TRANSACTION IDENTIFIER provides a value that a client can use to determine if an incoming response <u>matches its request</u>
- SECONDS ELAPSED specifies how many seconds have elapsed since the host began to boot

- See next slide for Example….→→

DHCP Phases



dhcp.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
802.11 Channel:
Channel Offset
FCS Filter:
Decryption Mode: Wireshark
No. Len Time Source Destination Protocol Info
1 314 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID
2 342 0.000295 192.168.0.1 192.168.0.10 DHCP DHCP Offer - Transaction ID
3 314 0.070031 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID
4 342 0.070345 192.168.0.1 192.168.0.10 DHCP DHCP ACK - Transaction ID
Bootstrap Protocol
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x00003d1d
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42
0
8
16
24
31
OP
HTYPE
HLEN
HOPS
TRANSACTION IDENTIFIER
SECONDS ELAPSED
FLAGS
CLIENT IP ADDRESS
YOUR IP ADDRESS
SERVER IP ADDRESS
ROUTER IP ADDRESS
CLIENT HARDWARE ADDRESS (16 OCTETS)
SERVER HOST NAME (64 OCTETS)
BOOT FILE NAME (128 OCTETS)
OPTIONS (VARIABLE)

No.	Len	Time	Source	Destination	Protocol	Info
1	314	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID (
2	342	0.000295	192.168.0.1	192.168.0.10	DHCP	DHCP Offer - Transaction ID (
3	314	0.070031	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID (
4	342	0.070345	192.168.0.1	192.168.0.10	DHCP	DHCP ACK - Transaction ID (

Request and ACK

DHCPREQUEST

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67			
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0x00000000			
SIADDR (Server IP Address)			
0xC0A80101			
GIADDR (Gateway IP Address)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			

Client

Client uses Port 68

Assuming the client is choosing the offered IP address form the server

Server IP Address

DHCPACK

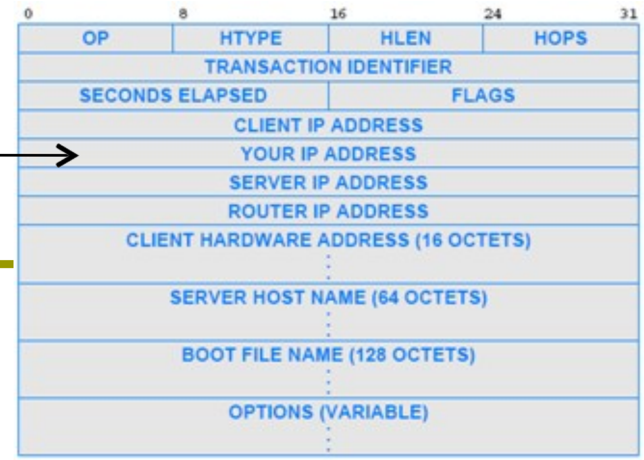
UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68			
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS			**FLAGS**
0x0000		0x0000	
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0xC0A80164 Client's NEW IP Address			
SIADDR (Server IP Address)			
0xC0A80101			
GIADDR (Gateway IP Address switched by relay)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			

Server

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client.

DHCP

Server fills it

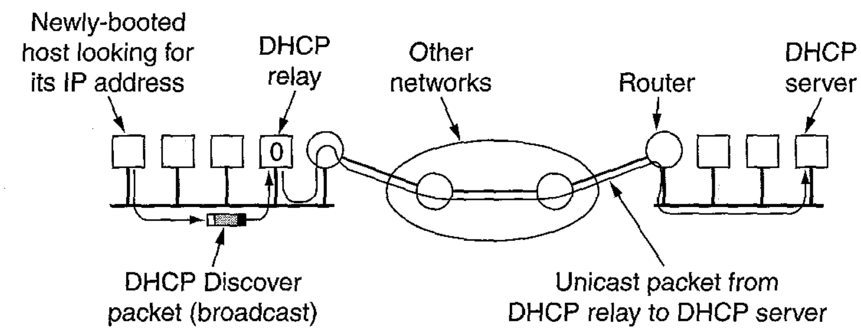


- Later fields in the message are used in a response to carry information back to the host that sent a request
  - if a host does not know its IP address, the server uses field YOUR IP ADDRESS to supply the value
  - server uses fields SERVER IP ADDRESS and SERVER HOST NAME to give the host information about the location of a server
  - ROUTER IP ADDRESS contains the IP address of a default router
- DHCP allows a computer to negotiate to find a boot image
  - The computer is boot up, request and OS
  - the host fills in field BOOT FILE NAME with a request
  - The DHCP server does not send an image
    - The host uses TFTP

Early Release

- The user can end the lease through a process called early lease termination or lease release
- This is a very simple, unidirectional communication
  - The client sends a special DHCPRELEASE message unicast to the server that holds its current lease
  - The server then records the lease as having been ended
  - It does not need to reply back to the client (no ACK)
- Client can just assume that the lease termination has been successful
- Having clients send DHCPRELEASE to end a lease is considered a *courtesy*, rather than a requirement
- DHCP servers are designed to handle the case where a client "disappears" without formally ending an existing lease
  - Sending a DHCPRELEASE is clearly more efficient, however!

Indirect DHCP Server Access Through a Relay



- DHCP broadcasts on the local network to find a server
- DHCP does not require each individual network to have a server
  - Instead, a DHCP relay agent forwards requests and responses between a client and the server
- At least one relay agent must be present on each network
  - The relay agent must be configured with the address of the appropriate DHCP server
- When the DHCP server responds
  - The relay agent forwards the response to the client