Reti di Calcolatori

Livello di rete: protocolli di supporto

Universtità degli studi di Verona
Facoltà di Scienze MM.FF.NN.
A.A. 2010/2011
Laurea in Informatica

Acknowledgement

- *Credits*
  - *Part of the material is based on slides provided by the following authors*
    - *Douglas Comer, "Computer Networks and Internets," 5th edition, Prentice Hall*
    - *Behrouz A. Forouzan, Sophia Chung Fegan, "TCP/IP Protocol Suite," McGraw-Hill*, January 2005

Topics covered

- Address binding
- Error reporting
- Bootstrapping
- Address translation

ARP

Address Resolution

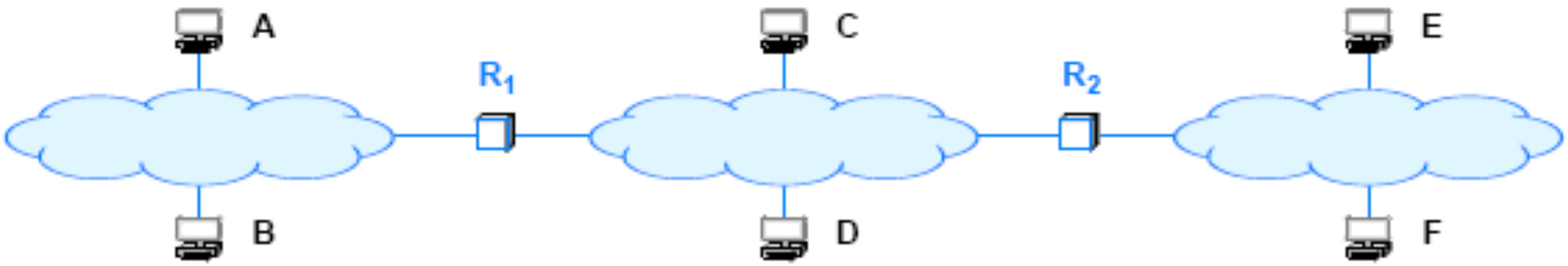
- A crucial step of the forwarding process requires a translation:
  - forwarding uses IP addresses
  - a frame transmitted must contain the MAC address of the next hop
  - IP must translate the next-hop IP address to a MAC address
- The principle is:
  - IP addresses are abstractions
    - provided by protocol software
  - Network does not know how to locate a computer from its IP address
    - the next-hop address must be translated to an equivalent MAC address

Address Resolution

- ❑ Translation from a computer's IP address to an equivalent hardware address is known as address resolution
  - And an IP address is said to be resolved to the correct MAC address
- ❑ Address resolution is local to a network
  - simple for Point-to-Point connections
  - need a protocol in the general case of shared access medium

Address Resolution

- One computer can resolve the address of another computer only if both computers attach to the same physical network
  - Direct delivery
  - A computer never resolves the address of a computer on a remote network
  - Address resolution is always restricted to a single network



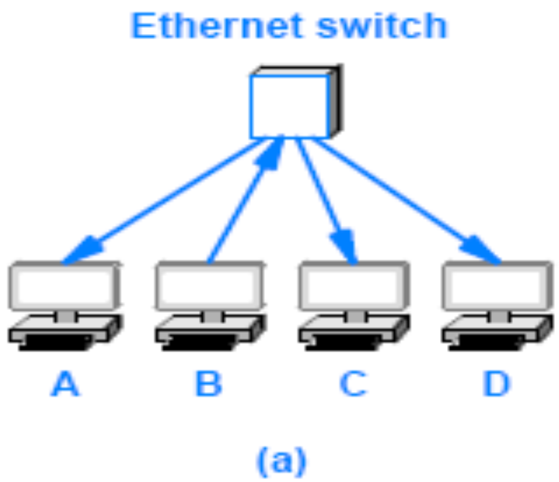
Address Resolution

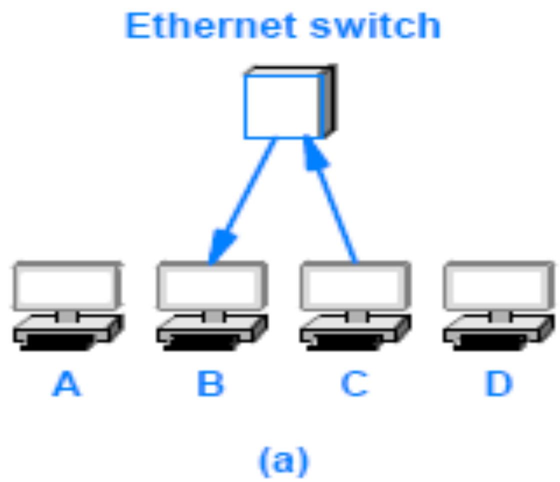
- How can a host know if the address to resolve is local?
  - if it is local, the dest. IP address should have the same NetID (prefix) of the source IP address
- What happens if the address is not local?
  - Indirect delivery
  - Host sends the request to a default Ethernet address
  - Alternatively, a local router can be configured to respond to ARP requests for the remote network.
  - ARP is used to find the MAC address of the next-hop router

The Address Resolution Protocol (ARP)

- ❑ What algorithm does software use to translate?
  - The answer depends on the protocol and hardware addressing
    - here we are only concerned with the resolution of IP
- ❑ Most hardware has adopted the 48-bit Ethernet
- ❑ In Ethernet ➔ Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP)





- Suppose B needs to resolve the IP address of C
- B broadcasts a request that says:
  - "I'm looking for the MAC address of a computer that has IP address C"
- The broadcast only travels across one network
- An ARP request message reaches all computers on a network
- When C receives a copy of the request it sends a directed reply back to B that says:
  - "I'm the computer with IP address C, and my MAC address is M"

ARP Message Format

- Rather than restricting ARP to IP and Ethernet
  - The standard describes a general form for ARP messages
  - It specifies how the format is adapted for each type of protocol
- Choosing a fixed size for a hardware address is not suitable
  - New network technologies might be invented that have addresses larger than the size chosen
  - The designers included a fixed-size field at the beginning of an ARP message to specify the size of the hardware addresses being used
- For example, when ARP is used with an Ethernet
  - the hardware address length is set to 6 octets
    - because an Ethernet address is 48 bits long

ARP Message Format

- To increase the generality of ARP
  - the designers also included an address length field
- ARP protocol can be used to bind an arbitrary high-level address to an arbitrary hardware address
- In practice, the generality of ARP is seldom used
  - most implementations of ARP are used to bind IP addresses to Ethernet addresses

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

- 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

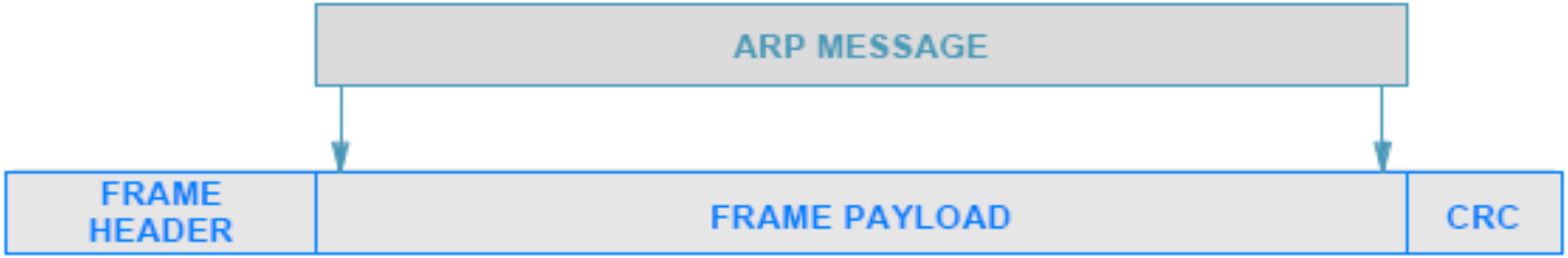
ARP Message Format

- OPERATION
  - 16-bit field that specifies whether the message
    - "request" (the field contains 1) or "response" (the field contains 2)
- 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

23.4 ARP Message Format

- An ARP message contains fields for two address bindings
  - one binding to the sender
  - other to the intended recipient, ARP calls it target
- When a request is sent
  - the sender does not know the target's hardware address (that is the information being requested)
    - field TARGET HADDR in an ARP request can be filled with zeroes
- In a response
  - the target binding refers to the initial computer that sent the request
  - Thus, the target address pair in a response serves no purpose
    - the inclusion of the target fields has survived from an early version of the protocol

ARP Encapsulation



- ❑ When it travels across a physical network an ARP message is encapsulated in a hardware frame
  - e.g., Ethernet
- ❑ An ARP message is treated as data being transported
  - the network does not parse the ARP message or interpret fields

ARP Encapsulation

- The type field in the frame header specifies that the frame contains an ARP message
- A sender must assign the appropriate value to the type field before transmitting the frame
- A receiver must examine the type field in each incoming frame
- Ethernet uses type field 0x806 to denote an ARP message
- The same value is used for both ARP requests/ responses
  - Frame type does not distinguish between types of ARP messages
  - A receiver must examine the OPERATION field in the message to determine whether an incoming message is a request or a response

ARP Caching and Message Processing

- Sending an ARP request for each datagram is inefficient
  - Three frames traverse the network for each datagram
    - an ARP request, ARP response, and the data datagram itself
- Most communications involve a sequence of packets
  - a sender is likely to repeat the exchange many times
- To reduce network traffic
  - ARP software extracts and saves the information from a response
    - so it can be used for subsequent packets
  - The software does not keep the information indefinitely
    - Instead, ARP maintains a small table of bindings in memory

19

ARP Caching and Message Processing

- ARP manages the table as a cache
  - an entry is replaced when a response arrives
  - the oldest entry is removed whenever the table runs out of space or after an entry has not been updated for a long period of time
  - ARP starts by searching the cache when it needs to bind an address

20

ARP Caching and Message Processing

- If the binding is present in the cache
  - ARP uses the binding without transmitting a request
- If the binding is not present in the cache
  - ARP broadcasts a request
  - waits for a response
  - updates the cache
  - and then proceeds to use the binding
- The cache is only updated when an ARP message arrives
  - either a request or a response
  - A timeout is set (typically 20 min) to force the update: all information are deleted when a timeout occurs.

ICMP

Internet Control Message Protocol

- IP includes a companion protocol, ICMP
  - It is used to report errors back to the original source
- IP and ICMP are co-dependent
  - IP depends on ICMP to report errors
  - and ICMP uses IP to carry error messages
- Many ICMP messages have been defined

Internet Control Message Protocol

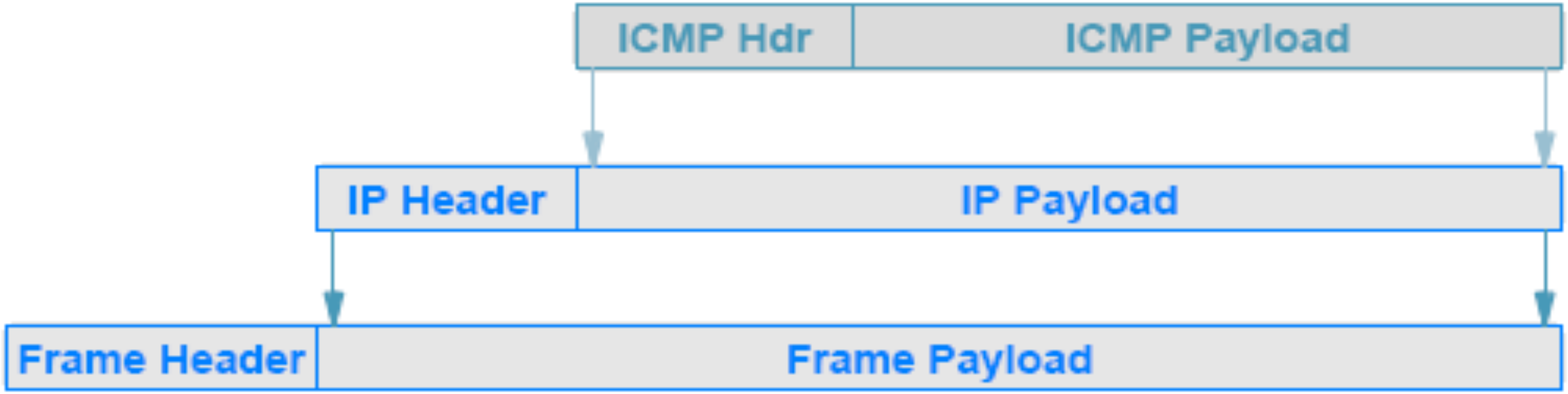
Number	Type	Purpose
0	Echo Reply	Used by the ping program
3	Dest. Unreachable	Datagram could not be delivered
5	Redirect	Host must change a route
8	Echo	Used by the ping program
11	Time Exceeded	TTL expired or fragments timed out
12	Parameter Problem	IP header is incorrect
30	Traceroute	Used by the traceroute program

24

Internet Control Message Protocol (ICMP)

- ICMP contains two message types:
  - messages used to report errors
    - e.g., Time Exceeded and Destination Unreachable
  - messages used to obtain information
    - e.g., Echo Request and Echo Reply
- Echo Request/Reply are used by the ping application to test connectivity
  - When a host receives an echo request message
    - ICMP software on a host or router sends an echo reply that carries the same data as the request

ICMP Message Format and Encapsulation



- ICMP uses IP to transport each error message:
  - when a router has an ICMP message to send
    - it creates an IP datagram and encapsulates the ICMP message in it
  - the ICMP message is placed in the payload area of the IP datagram
  - the datagram is then forwarded as usual
    - with the complete datagram being encapsulated in a frame for transmission

26

ICMP Message Format and Encapsulation

- ICMP messages do not have special priority
  - They are forwarded like any other datagram, with one minor exception
- If an ICMP error message causes an error
  - no error message is sent
- The reason should be clear:
  - the designers wanted to avoid the Internet becoming congested carrying error messages about error messages

DHCP

IP addressing: CIDR

CIDR: Classless InterDomain Routing

- subnet portion of address of arbitrary length
- address format: a.b.c.d/x, where x is # bits in subnet portion of address

subnet part | host part

11001000 00010111 0001000**0 00000000**

200.23.16.0/23

IP addresses: how to get one?

Q: How does a *host* get IP address?

- hard-coded by system admin in a file
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

DHCP: Dynamic Host Configuration Protocol

Goal: allow host to *dynamically* obtain its IP address from network server when it joins network

Can renew its lease on address in use

Allows reuse of addresses (only hold address while connected an "on")

Support for mobile users who want to join network (more shortly)

DHCP overview:

- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

Protocol Software, Parameters, and Configuration

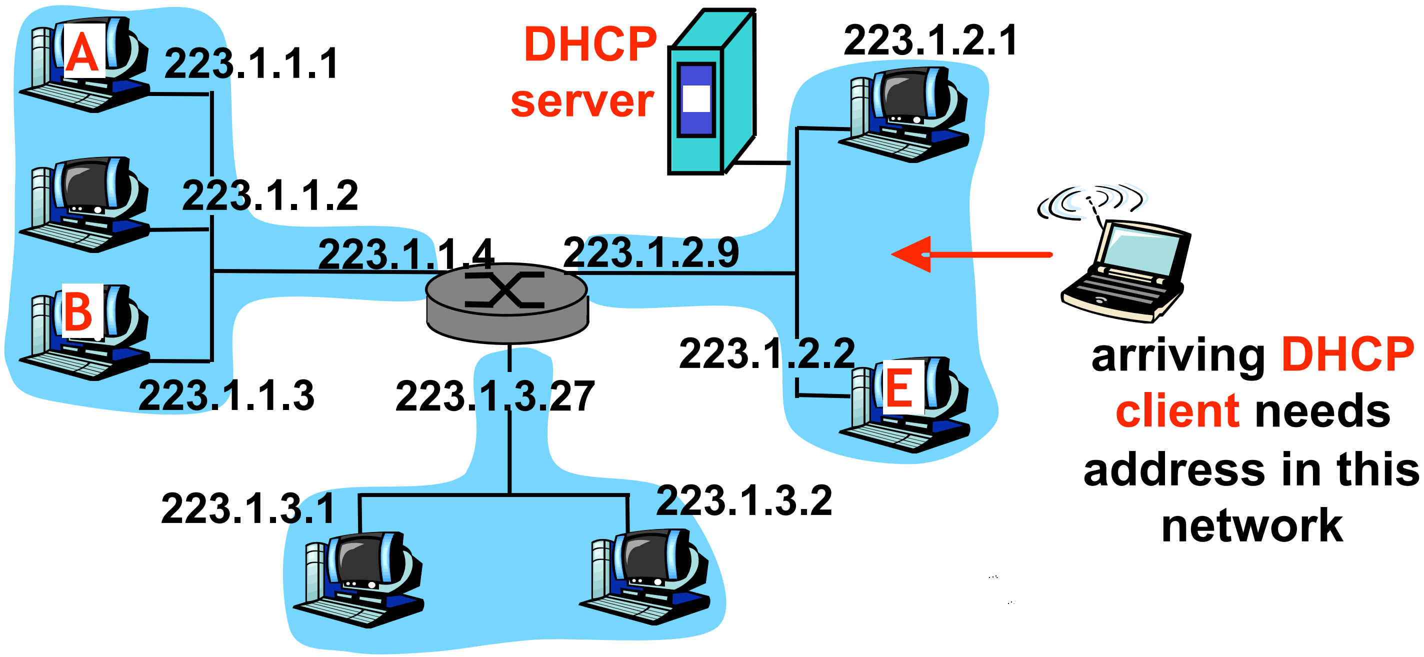
- Once a host or router has been powered on, OS is started and the protocol software is initialized
- How does the protocol software in a host or router begin operation?
- For a router, the configuration manager must specify initial values for items such as
  - the IP address for each network connection
  - the protocol software to run
  - and initial values for a forwarding table
  - the configuration is saved, and a router loads the values during startup
- Host configuration usually uses a two-step process, known as bootstrapping
  - A protocol was invented to allow a host to obtain multiple parameters with a single request, known as the Bootstrap Protocol (BOOTP)
  - Currently, DHCP is used to take care of most configuration needed

32

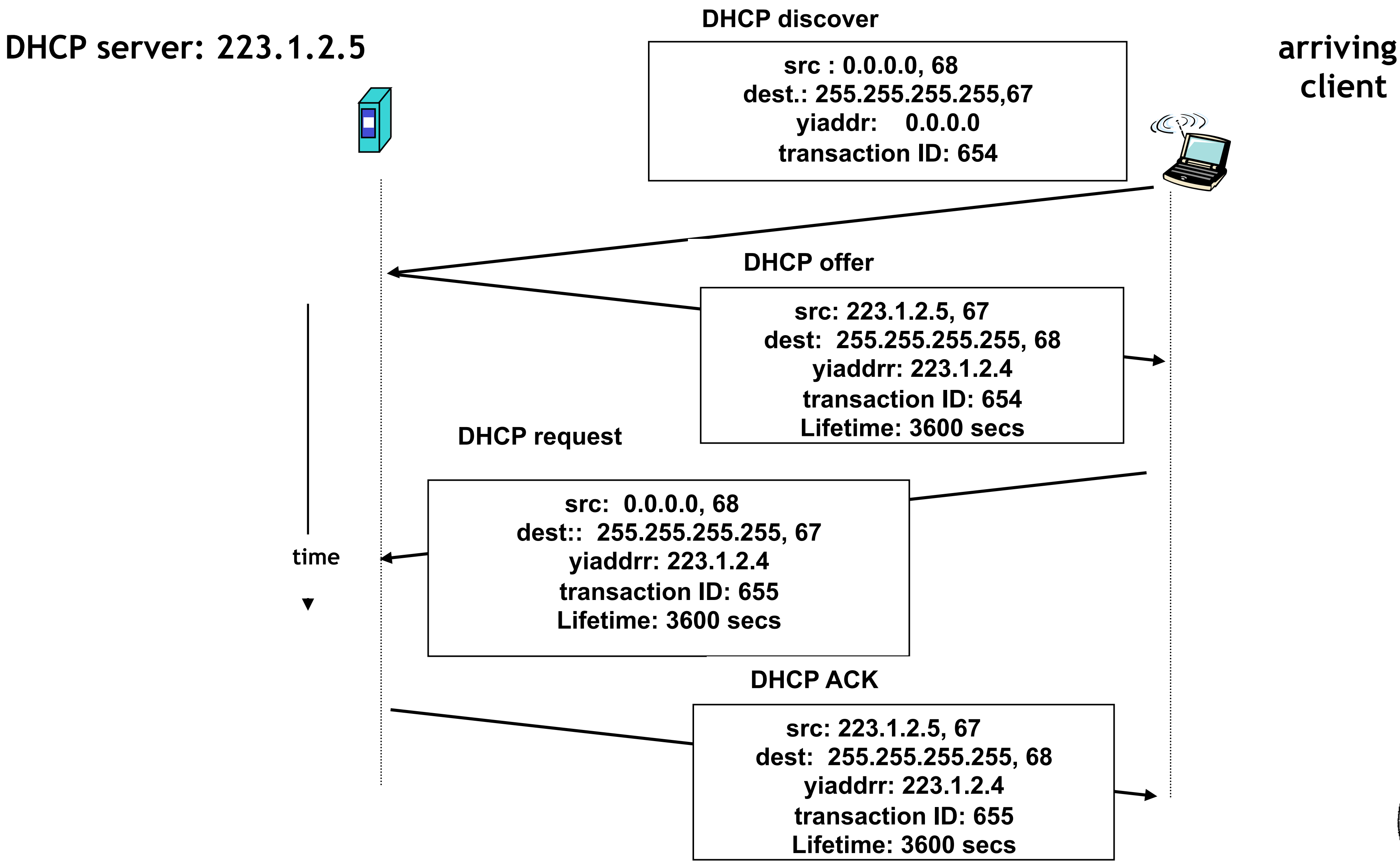
Dynamic Host Configuration Protocol (DHCP)

- Various mechanisms have been created to allow a host computer to obtain parameters
- An early mechanism known as the Reverse Address Resolution Protocol (RARP) allowed a computer to obtain an IP address from a server
- ICMP has Address Mask Request and Router Discovery messages
  - can obtain the address mask used and the address of a router
- Each of the early mechanisms was used independently
  - requests were broadcast and a host typically configured layers from lowest to highest
- DHCP allows a computer to join a new network and obtain an IP address automatically
  - The concept has been termed plug-and-play networking

DHCP client-server scenario



DHCP client-server scenario



Dynamic Host Configuration Protocol (DHCP)

- When a computer boots
  - the client computer broadcasts a DHCP Request
  - the server sends a DHCP Reply
    - DHCP uses the term offer to denote the message a server sends
    - and we say that the server is offering an address to the client
- We can configure a DHCP server to supply two types of addresses:
  - permanently assigned addresses as provided by BOOTP or
  - a pool of dynamic addresses to be allocated on demand
- Typically, a permanent address is assigned to a server, and a dynamic address is assigned to an arbitrary host
- In fact, addresses assigned on demand are not given out for an arbitrary length of time

Dynamic Host Configuration Protocol (DHCP)

- DHCP issues a lease on the address for a finite period
  - The use of leases allows a DHCP server to reclaim addresses
- When the lease expires
  - the server places the address to the pool of available addresses
- When a lease expires, a host can choose to relinquish the address or renegotiate with DHCP to extend the lease
  - Negotiation occurs concurrent with other activity
- Normally, DHCP approves each lease extension
  - A computer continues to operate without any interruption
  - However, a server may be configured to deny lease extension for administrative or technical reasons
  - DHCP grants absolute control of leasing to a server
  - If a server denies an extension request
    - the host must stop using the address

DHCP Protocol Operation and Optimizations

- 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
  - 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

38

DHCP Message Format

- DHCP adopted a slightly modified version of the BOOTP message format
  - OP specifies whether the message is a Request or a Response
  - HTYPE and HLEN fields specify the network hardware type and the length of a hardware address
  - FLAGS specifies whether it can receive broadcast or directed replies
  - HOPS specifies how many servers forwarded the request
  - TRANSACTION IDENTIFIER provides a value that a client can use to determine if an incoming response matches its request
  - SECONDS ELAPSED specifies how many seconds have elapsed since the host began to boot
  - Except for OPTIONS (OP), each field in a DHCP message has a fixed size

39

DHCP Message Format

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) ⋮			

DHCP Message Format

- 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
  - To do so, the host fills in field BOOT FILE NAME with a request
  - The DHCP server does not send an image

Summary

What happens when a machine (end host)…

- … is switched on
  - it obtains its IP address via DHCP
    - the IP address may be set also manually
- … wants to send a message to another host on the same network
  - it obtains the IP address from the DNS
    - DNS: something that translate human readable strings (e.g. www.google.com) into IP addresses
  - it checks if the address belong to the same network
    - check the NetID (IP prefix) in the IP address
  - if the dest belong to the same network, it checks the ARP cache
  - if the dest. IP is not in ARP cache, it sends an ARP request
  - when the source has the MAC address, it sends a frame
- … wants to send a message to another host on another network

  ➔ topic of the next classes