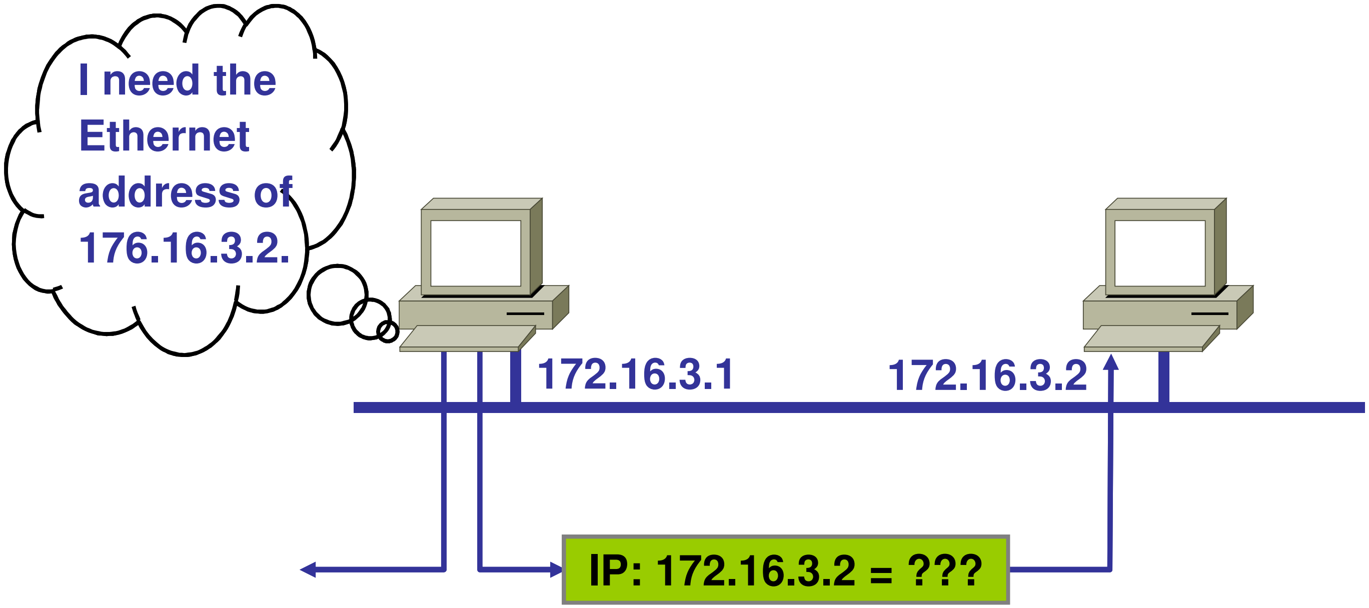
IT 4505
Section 3.3

IP support protocols

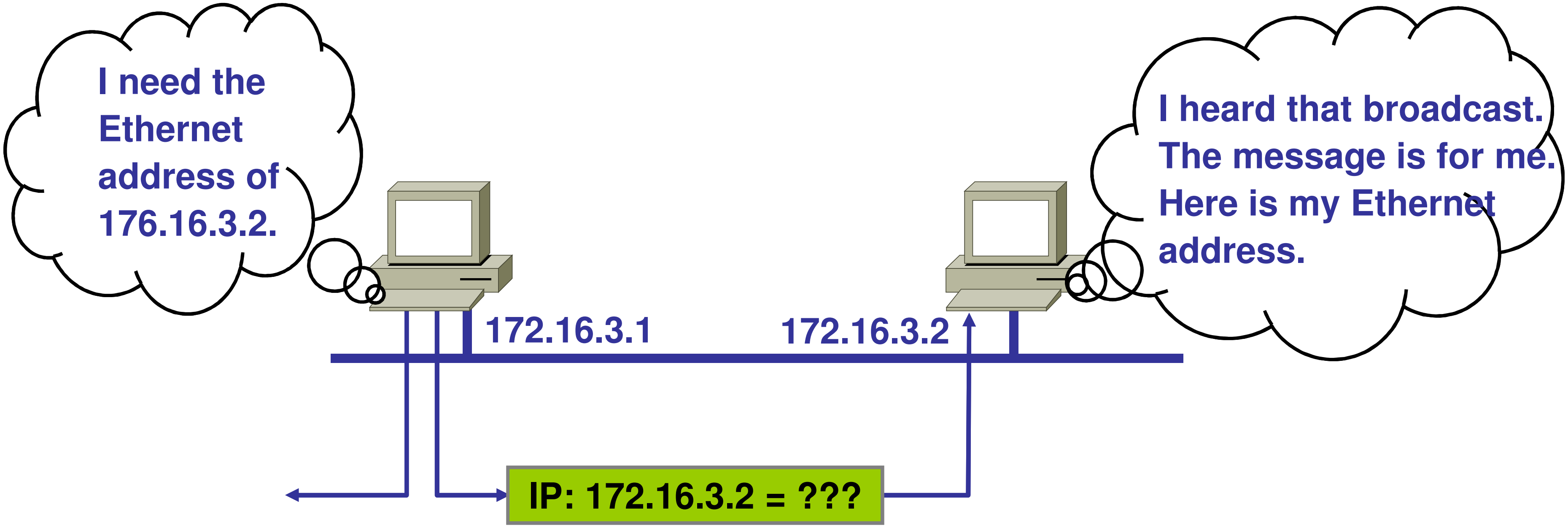
3.3.1 Address Resolution Protocol (ARP)



Addressing:

- 48-bit MAC (Ethernet) Address – Flat
- 32-bit Internet Address (IP) – Hierarchical

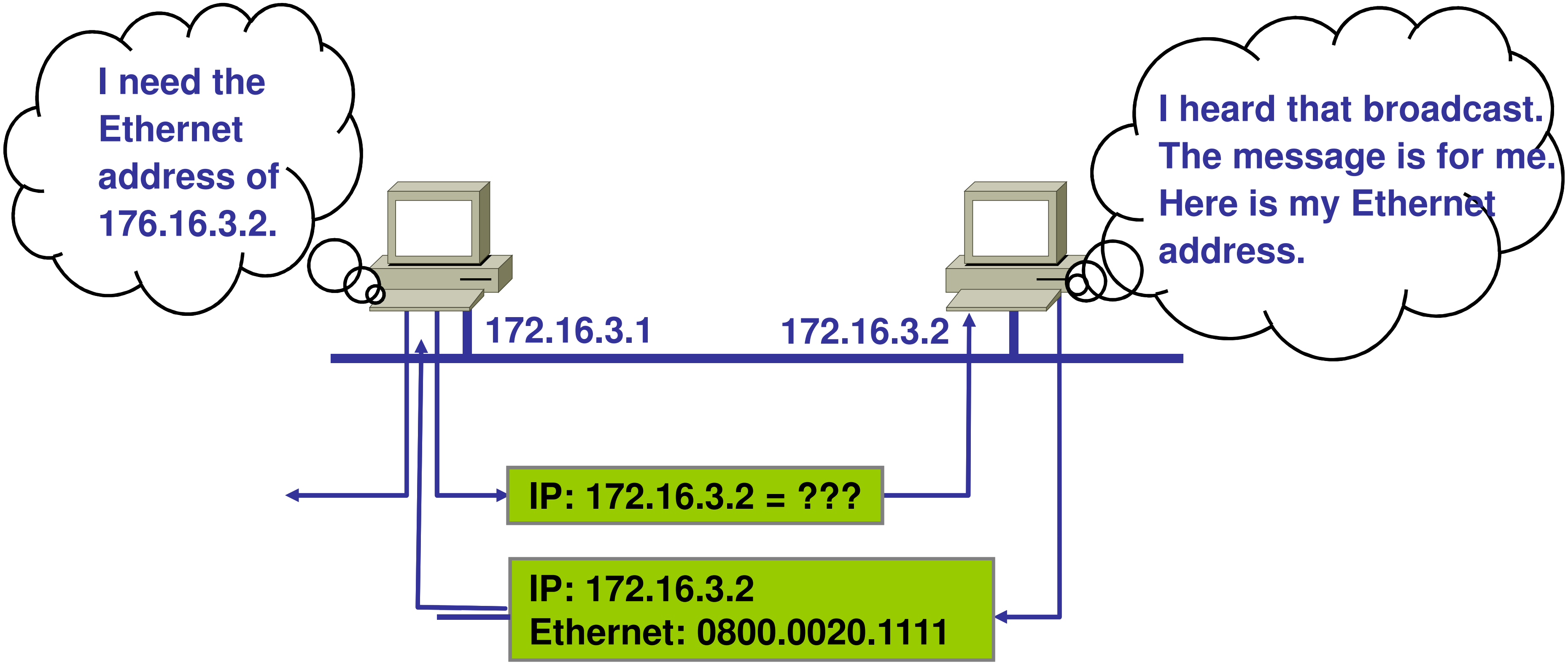
Address Resolution Protocol (ARP)



I need the Ethernet address of 176.16.3.2.

I heard that broadcast. The message is for me. Here is my Ethernet address.

Address Resolution Protocol (ARP)



I need the Ethernet address of 176.16.3.2.

I heard that broadcast. The message is for me. Here is my Ethernet address.

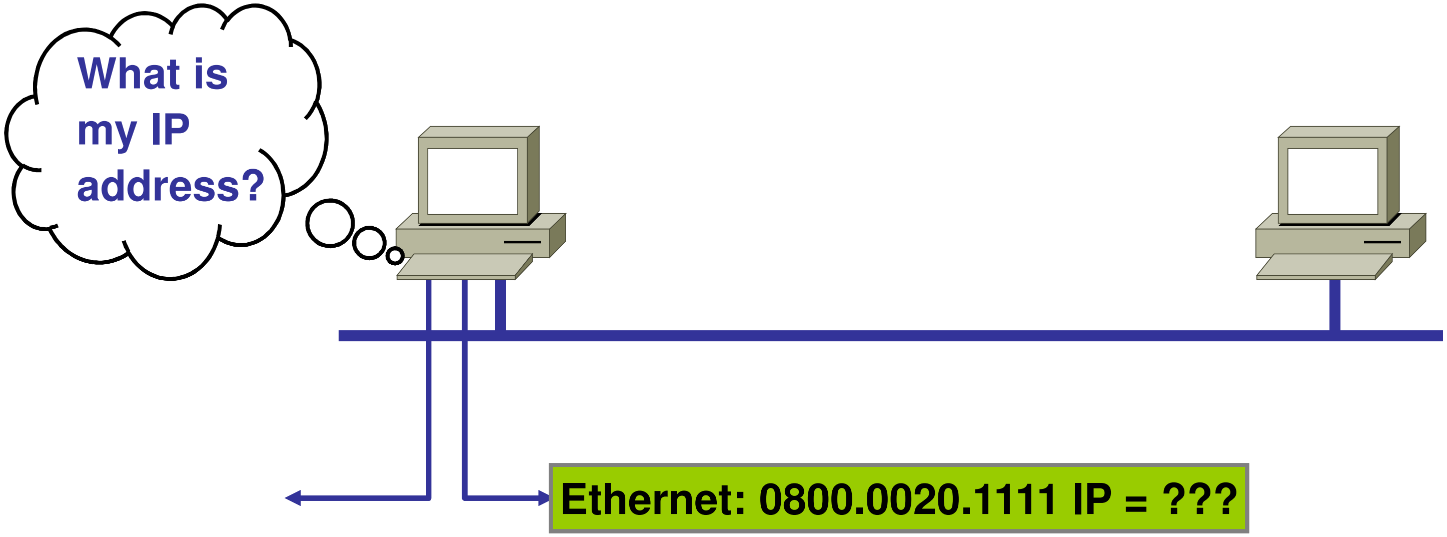
172.16.3.1

172.16.3.2

IP: 172.16.3.2 = ???

IP: 172.16.3.2
Ethernet: 0800.0020.1111

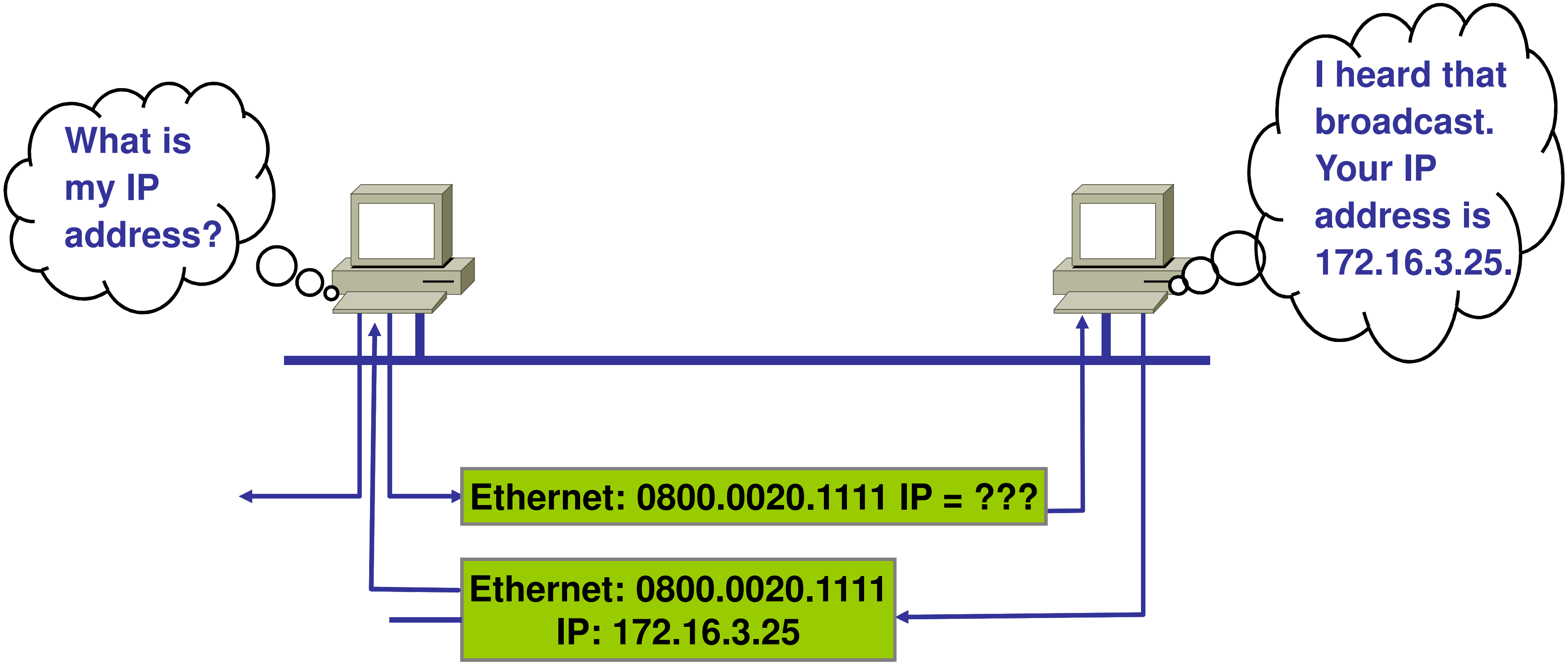
Reverse ARP



What is my IP address?

Ethernet: 0800.0020.1111 IP = ???

Reverse ARP


What is my IP address?
I heard that broadcast. Your IP address is 172.16.3.25.
Ethernet: 0800.0020.1111 IP = ???
Ethernet: 0800.0020.1111
IP: 172.16.3.25

3.3.2 Dynamic Host Configuration Protocol (DHCP)

- ❑ Allows client machines to receive an IP address, DNS information, etc automatically
- ❑ Before DHCP users had to type in all this information by hand, which is bad:
  - Easy to mistype something when entering by hand
  - Manually changing network configuration every time you move your laptop is a pain
  - Bootp resolved some of these issues
    - o … and DHCP still uses the same port as bootp

DHCP: Basics

❑ A client leases an IP address from a DHCP server for a given amount of time

❑ When lease expires, the client must ask DHCP server for a new address (clients attempt to renew lease after 50% of the lease time has expired)

❑ Typical leases may last for 30 seconds, 24 hours, or longer.

DHCP: Messages Overview

- Several messages are sent back and forth between a client and the DHCP server before it can successfully obtain an IP address

DHCP: DISCOVER

- ❑ Hardcoding the addresses of DHCP servers kind of defeats the purpose of automatic configuration

- ❑ Solution: A client using DHCP will broadcast a DISCOVER message to all computers on its subnet (address 255.255.255.255) to figure out the IP address of any DHCP servers

- ❑ Most routers are configured to pass this request within the campus or enterprise

DHCP: OFFER

- ❑ (Optionally) sent from server in response to a DISCOVER
- ❑ Contains an IP address, other configuration information as well (subnet mask, DNS servers, default gateway, search domains, etc)
- ❑ Note that all DHCP servers that receive a DISCOVER request may send an OFFER; since a client typically does not need > 1 IP address, more messages needed

DHCP: REQUEST

- ❑ Sent by client to request a certain IP address
  - Usually the one sent by an OFFER, but also used to renew leases. Also can be sent to try to get same address after a reboot
- ❑ This message is broadcast
- ❑ Most OSs by default will send a REQUEST for the first OFFER they receive – this means that if there is a rogue DHCP server on your subnet, most clients will *ignore* the OFFERs from the campus DHCP servers (since the OFFER from the rogue server gets to the user's PC first)!

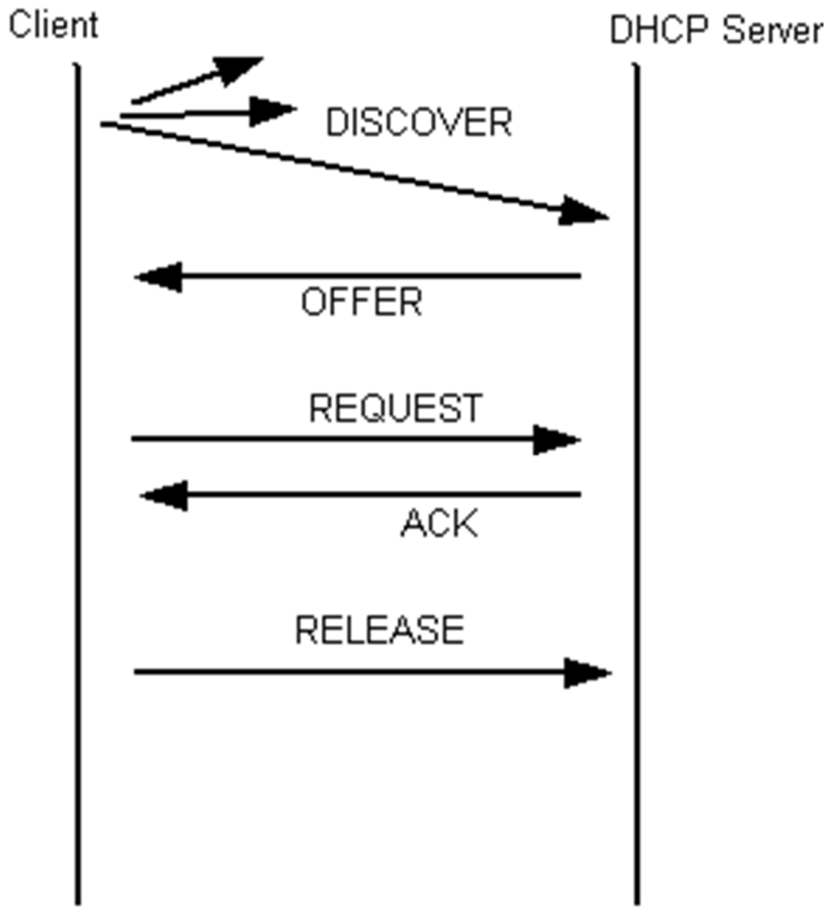
DHCP: ACK/NACK

- ❑ Sent by server in response to a REQUEST
- ❑ ACK: Request accepted, client can start using the IP it REQUESTed
- ❑ NACK: Something is wrong with the client’s REQUEST (for example they requested an IP address they’re not supposed to have)

DHCP: RELEASE

- Sent by client to end a lease
- Not strictly required, but is the “polite” thing to do if done with the IP (could just let the lease expire)
- Some clients may not send RELEASEs in an attempt to keep the same IP address for as long as possible

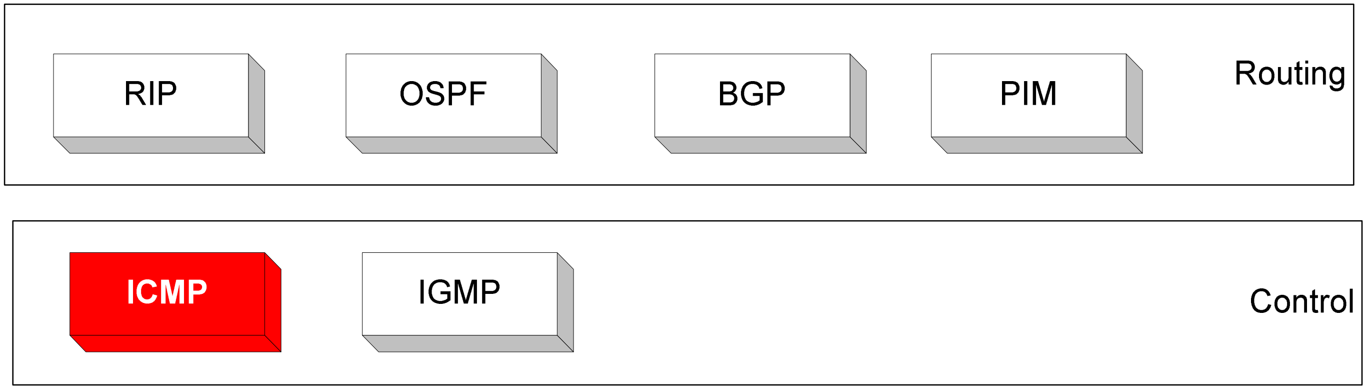
DHCP: Big Picture



3.3.3 Internet Control Message Protocol (ICMP)

Overview

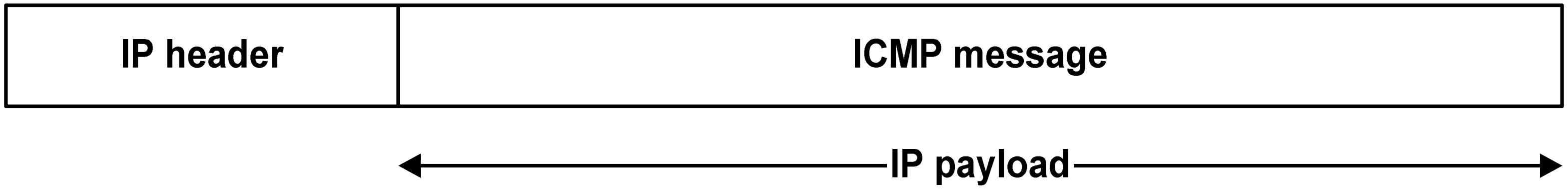
- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
  - Control functions (ICMP)
  - Multicast signaling (IGMP)
  - Setting up routing tables (RIP, OSPF, BGP, PIM, …)



Internet Control Message Protocol (ICMP)

Overview

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
  - Error reporting
  - Simple queries

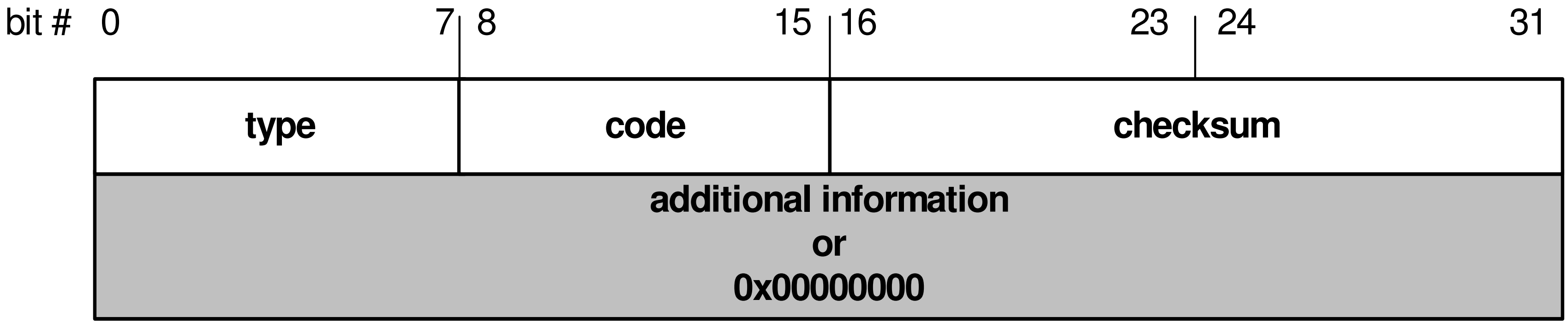


IP header | ICMP message

IP payload

- ICMP messages are encapsulated as IP datagrams:

ICMP message format



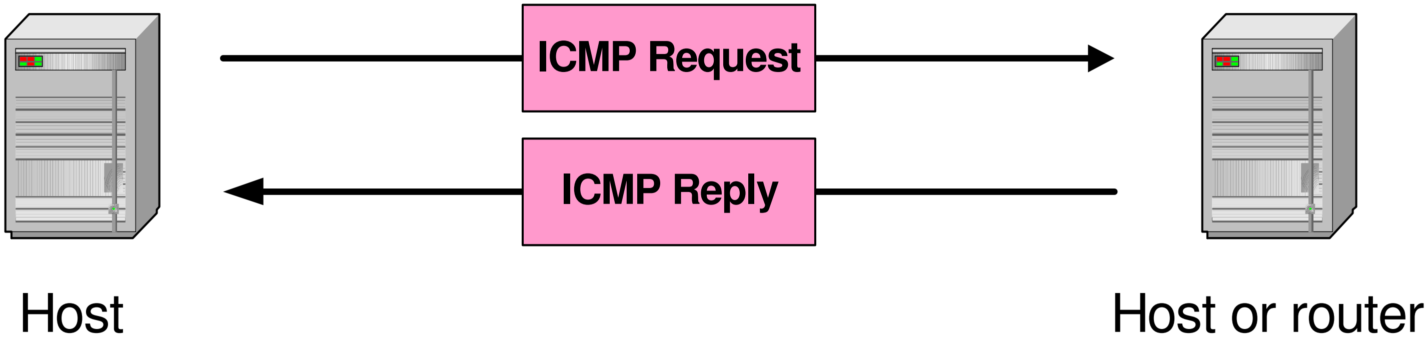
bit # 0 … 7	8 … 15	16 … 23	24 … 31
type	code	checksum	
additional information or 0x00000000			

4 byte header:

- Type (1 byte): type of ICMP message
- Code (1 byte): subtype of ICMP message
- Checksum (2 bytes): similar to IP header checksum. Checksum is calculated over entire ICMP message

If there is no additional data, there are 4 bytes set to zero.
→ each ICMP messages is at least 8 bytes long

ICMP Query message



ICMP query:

- Request sent by host to a router or host
- Reply sent back to querying host

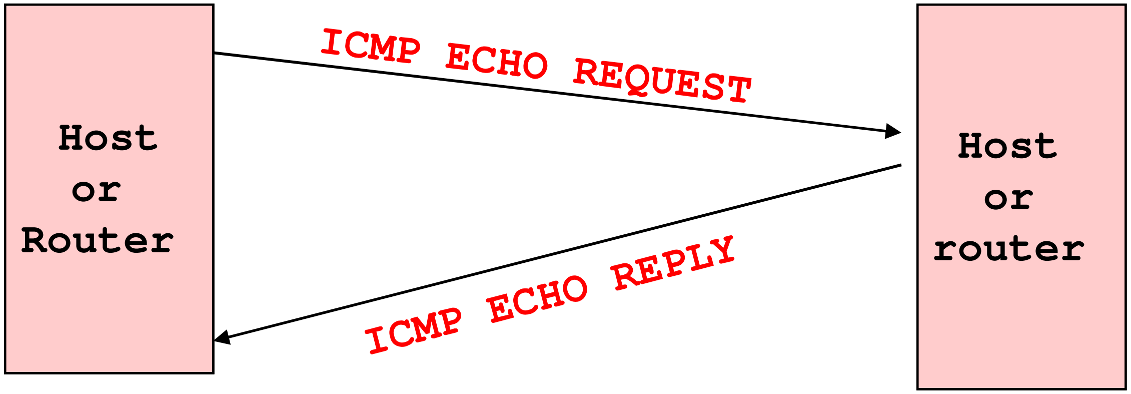
Example of ICMP Queries

Type/Code:	Description
8/0	Echo Request
0/0	Echo Reply
13/0	Timestamp Request
14/0	Timestamp Reply
10/0	Router Solicitation
9/0	Router Advertisement

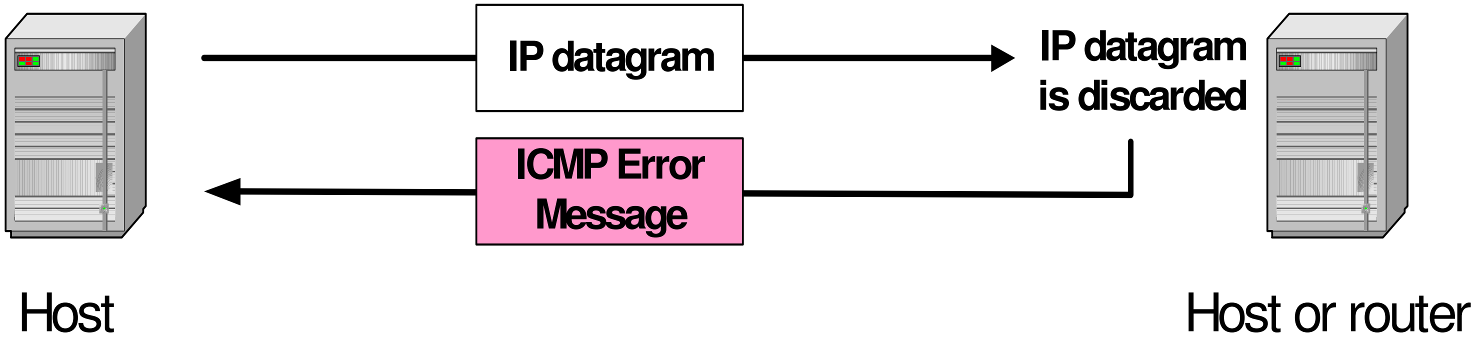
The ping command uses Echo Request/ Echo Reply

Example of a Query: Echo Request and Reply

- Ping's are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Ping'ed host responds with an ICMP Echo Reply

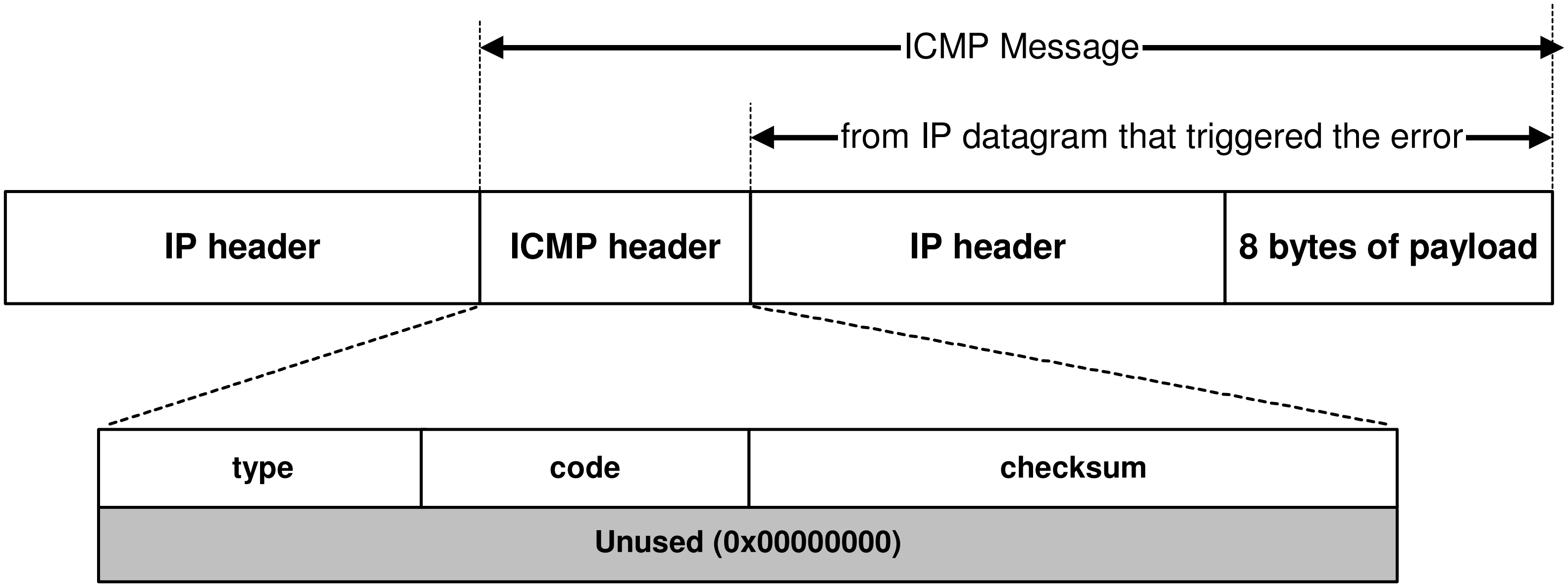


ICMP Error message



- ❑ ICMP error messages report error conditions
- ❑ Typically sent when a datagram is discarded
- ❑ Error message is often passed from ICMP to the application program

ICMP Error message



ICMP Message

from IP datagram that triggered the error

IP header	ICMP header	IP header	8 bytes of payload

type	code	checksum
Unused (0x00000000)		

❑ ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)

Frequent ICMP Error message

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

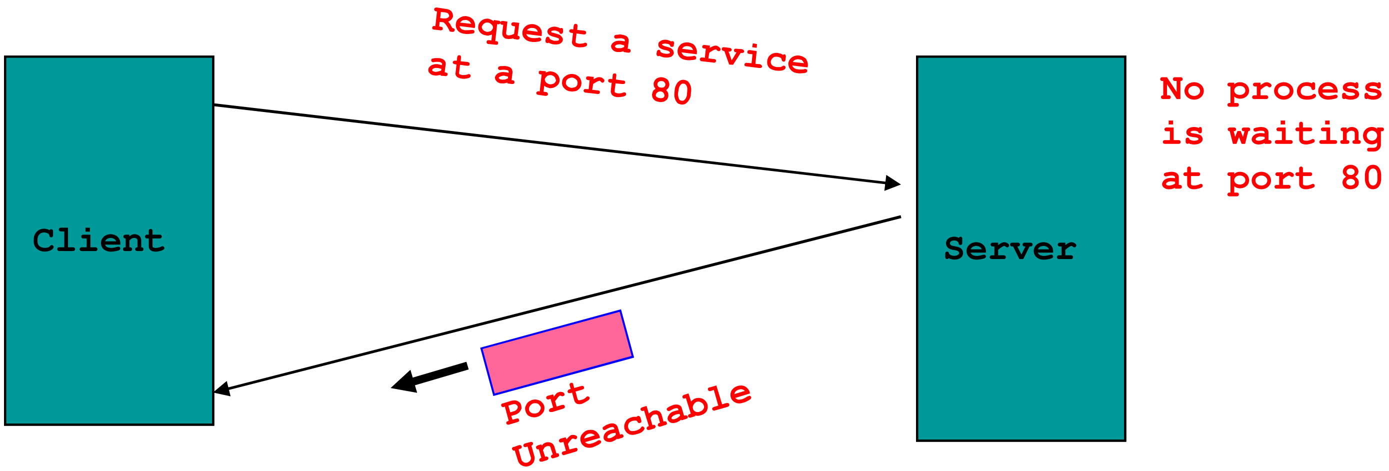
Some subtypes of the “Destination Unreachable”

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

Example: ICMP Port Unreachable

- RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.

- Scenario:


Request a service at a port 80
No process is waiting at port 80
Client
Server
Port Unreachable