Lecture 17 Overview

- Last Lecture
  - Wide Area Networking (2)
- This Lecture
  - Internet Protocol (1)
  - Source: chapters 2.2, 2.3,18.4, 19.1, 9.2
- Next Lecture
  - Internet Protocol (2)
  - Source: chapters 19.1, 19.2, 22,1 22.2, 26.6

A Brief History of the Internet

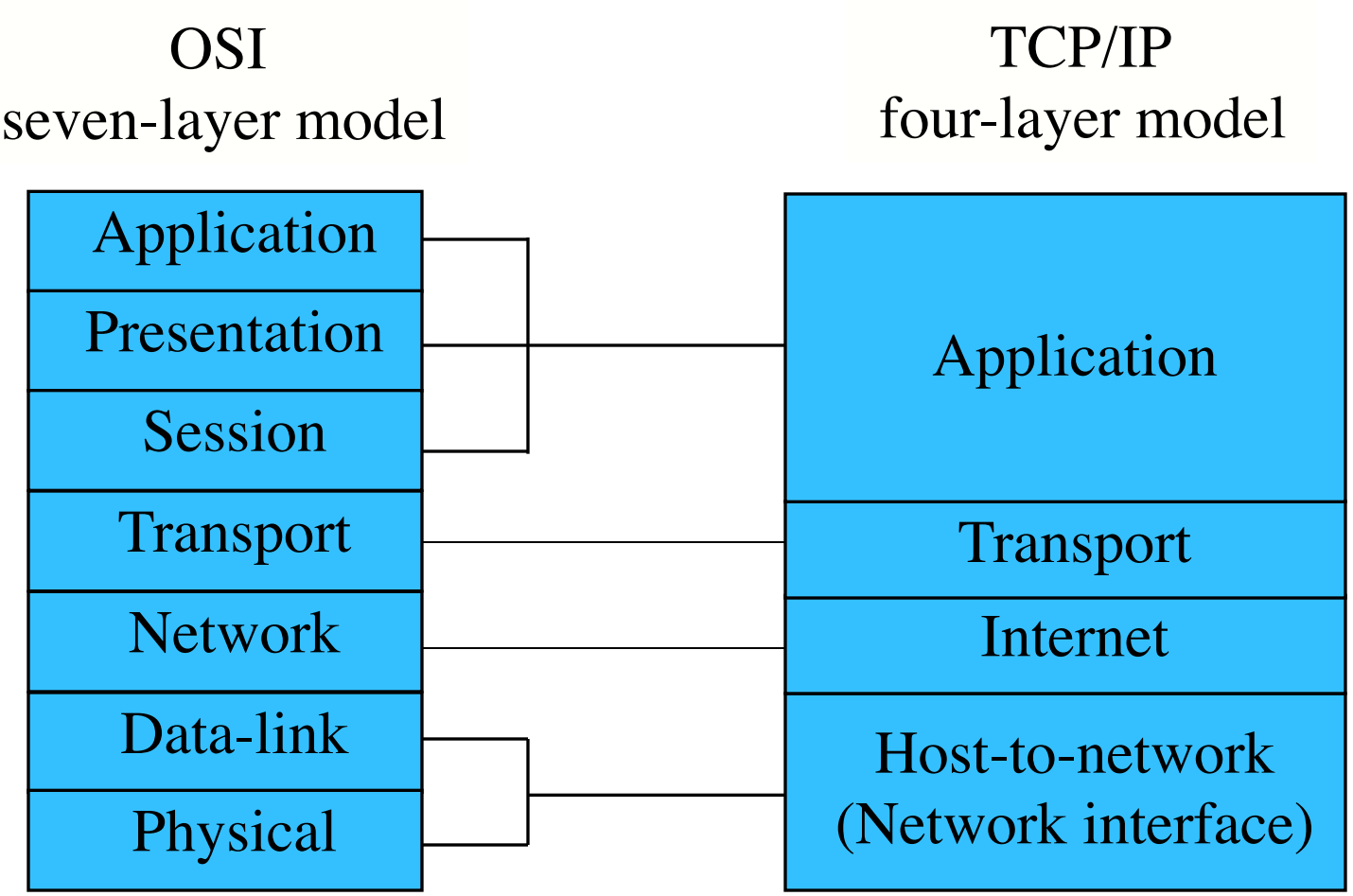
- Started in late 1960's by US Dept. of Defense, funded by Advanced Research Project Agency (ARPA).
- A packet-switching network used to connect research universities and military
  - Conventions developed by ARPA that specify how individual computers communicate across that network became TCP/IP.
- Size
  - 1969 - 4 sites, 1981 - 200 sites; 1996 - 100,000th network added in Internet; 1997 - 16M hosts; 1998 - 30M hosts; 2013- the estimated Internet users 2.802 billion (39% of world population); 2017- 3.8 billion (51.7%)
  - Internet world status: http://www.internetworldstats.com/stats.htm

Who Controls It

- Internet Activities Board
  - Internet Engineering Task Force (IETF)
    - Ongoing evolution of the TCP/IP protocols
  - Internet Research Task Force
    - Works on advancing network technology and long-term research
  - Network Information Center
    - Assigns network IP addresses
- RFC (Request For Comments)
  - Technical reports on protocols

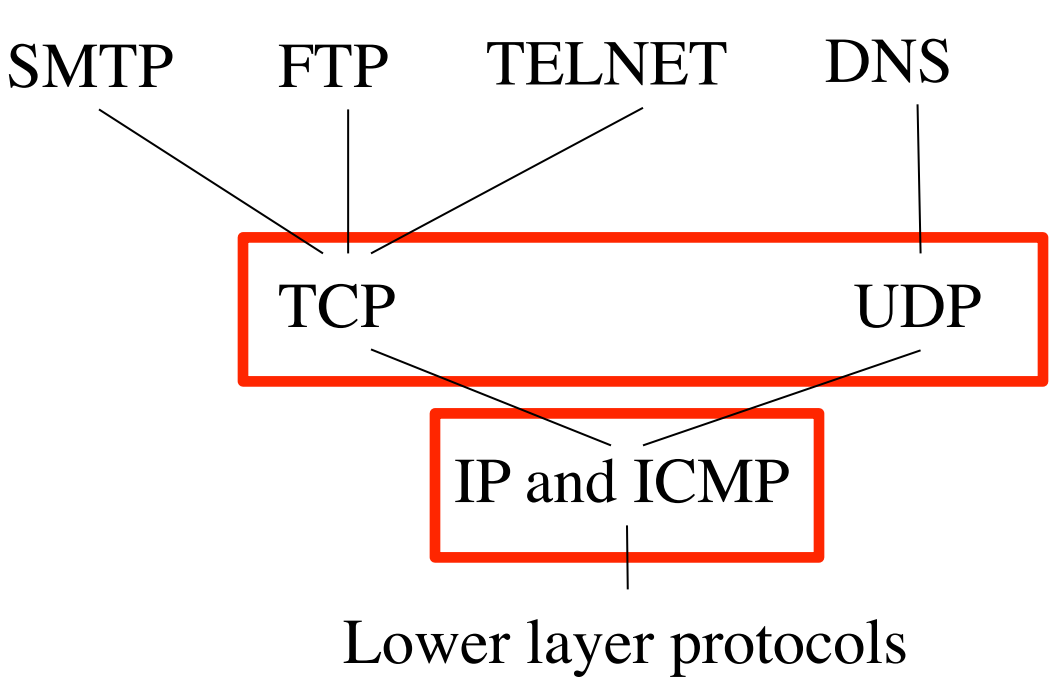
The Internet Model

- Also called the TCP/IP Reference model



TCP/IP Protocol Suite

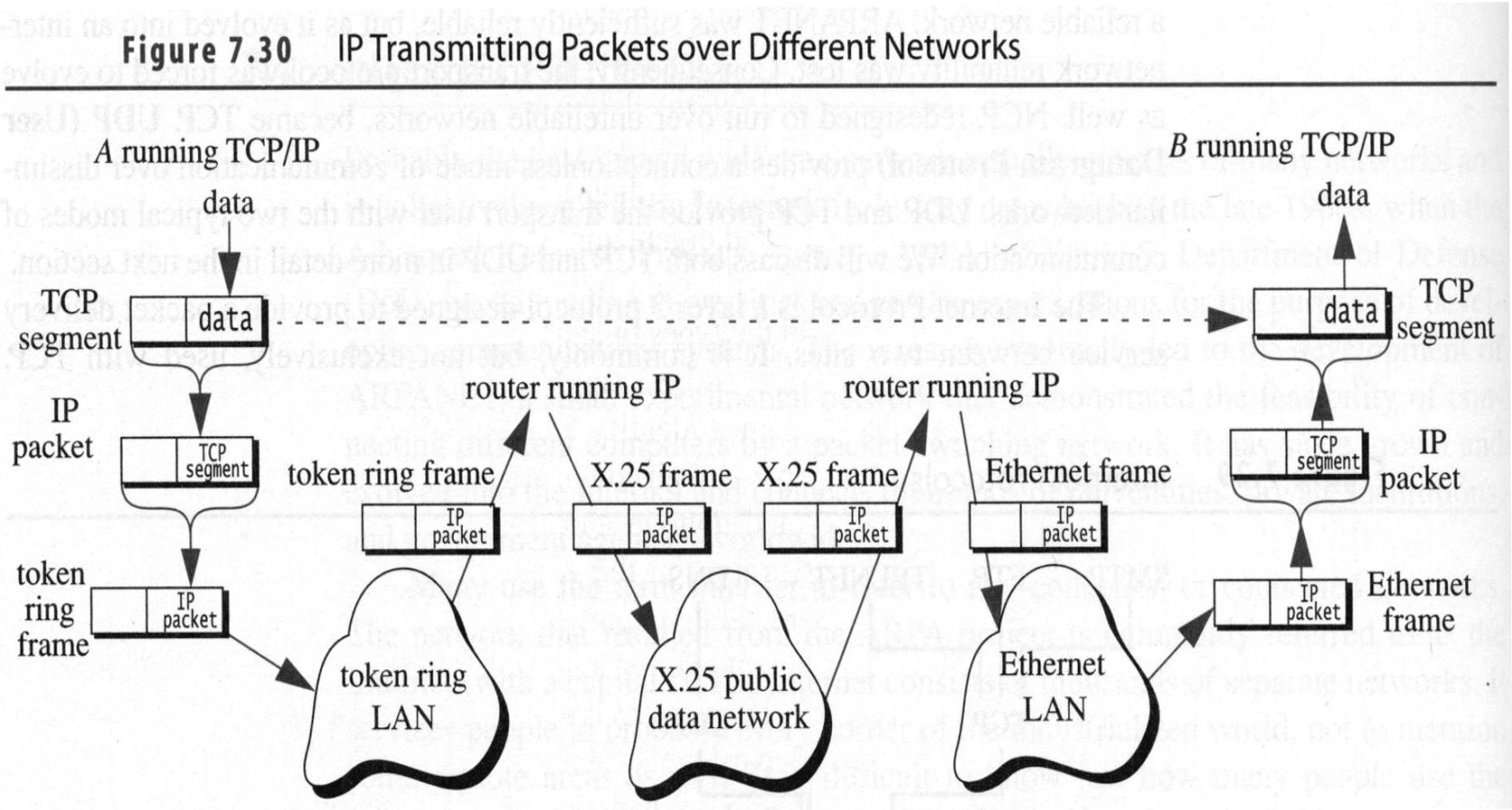
- The main protocols for the Internet
  - TCP: Transmission Control Protocol
  - IP: Internet Protocol



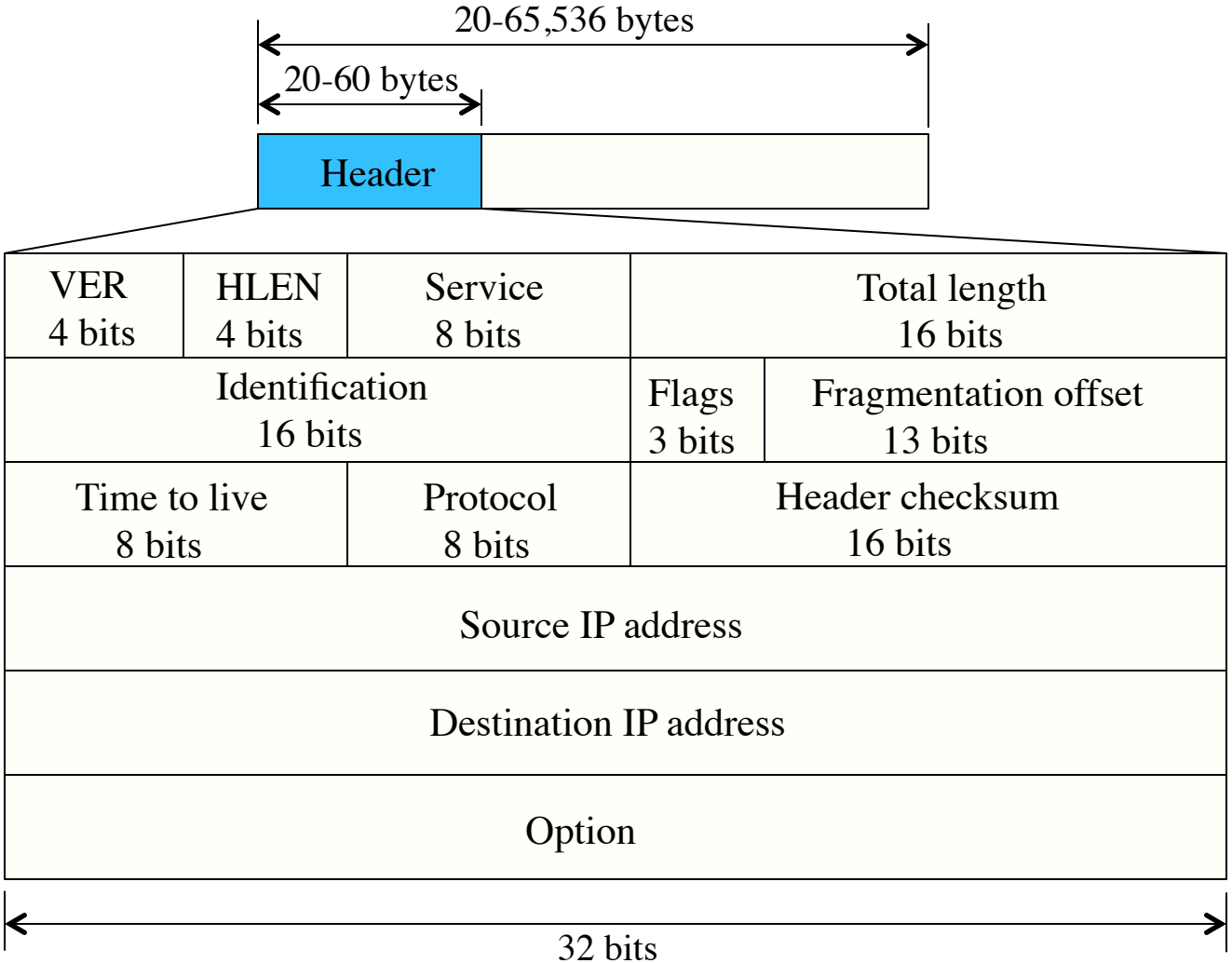
IP - Internet Protocol

- Unreliable connectionless protocol
- Use packet-switching
- Provide a datagram service between stations
  - Deliver a packet from source to destination
  - Routing decisions may be made for each packet
  - Packets are not guaranteed to arrive in order or via the same route
- IP takes care of network differences
  - Make sure IP packets can be transferred through different networks

IP - Internet Protocol (cont.)



IPv4 Packet Format



IPv4 Packet Fields

- Version (4 bits)
  - Version of IP that created the packet
  - IPv4, may be totally replaced by IPv6 in the future
- Header length (4 bits)
  - Number of 32-bit words in the packet header
  - Minimum 5, maximum 15
- Type of service (8 bits)
  - Allows the host to tell the subnet what kind of service it desires (reliability and speed)
- Packet length (16 bits)
  - Length of the entire IP packet. Max 64KB.

IPv4 Packet Fields (cont.)

- Identification (16 bits), flags (3 bits), fragment offset (13 bits)
  - When the packet is too big, these fields are used for breaking a packet into multiple packets at routers and reassembling them at the destination.
- Time to live (8 bits)
  - Originally designed to hold a timestamp, and the packet is discarded when the value becomes zero (require synchronization among all machines).
  - Today, this field is used mostly to control the maximum number of hops visited by the packet. Each router decreases the value by one and discards the packet if the value becomes zero.
  - Can be used intentionally to limit the journey of the packet, e.g. to confine the packet to the local network.
- Protocol (8 bits)
  - Specifies the next higher layer protocol. Used at destination to give data to the appropriate entity.

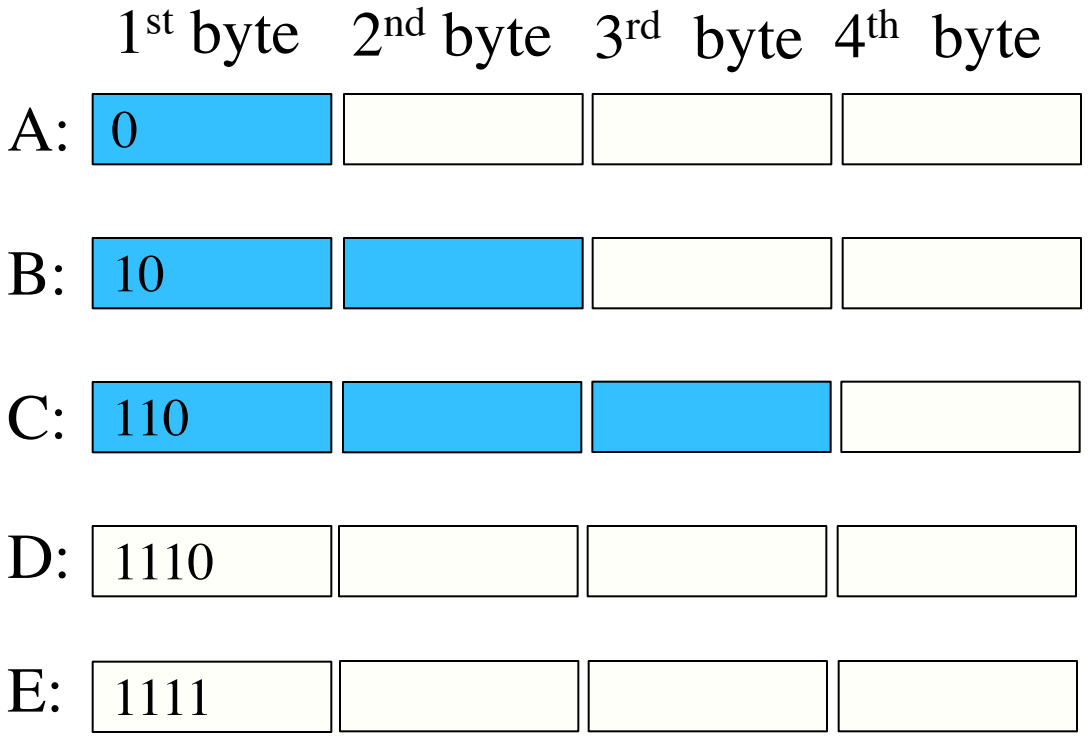
IPv4 Packet Fields (cont.)

- Header checksum (16 bits)
  - Error detection for the packet header. IP only worries about errors at its level.
- Source and destination IP addresses
  - 32 bit fields for the addresses
- Options
  - record route, source route, timestamp
- Padding
  - Makes header end at a 32 bit boundary
- Data
  - Data provided by higher layer

IPv4 Address Classes

- IPv4 address structure: two main components

- IPv4 addresses are divided into 5 classes



1.0.0.0 - 127.255.255.255

128.0.0.0 - 191.255.255.255

192.0.0.0 - 223.255.255.255

224.0.0.0 - 239.255.255.255

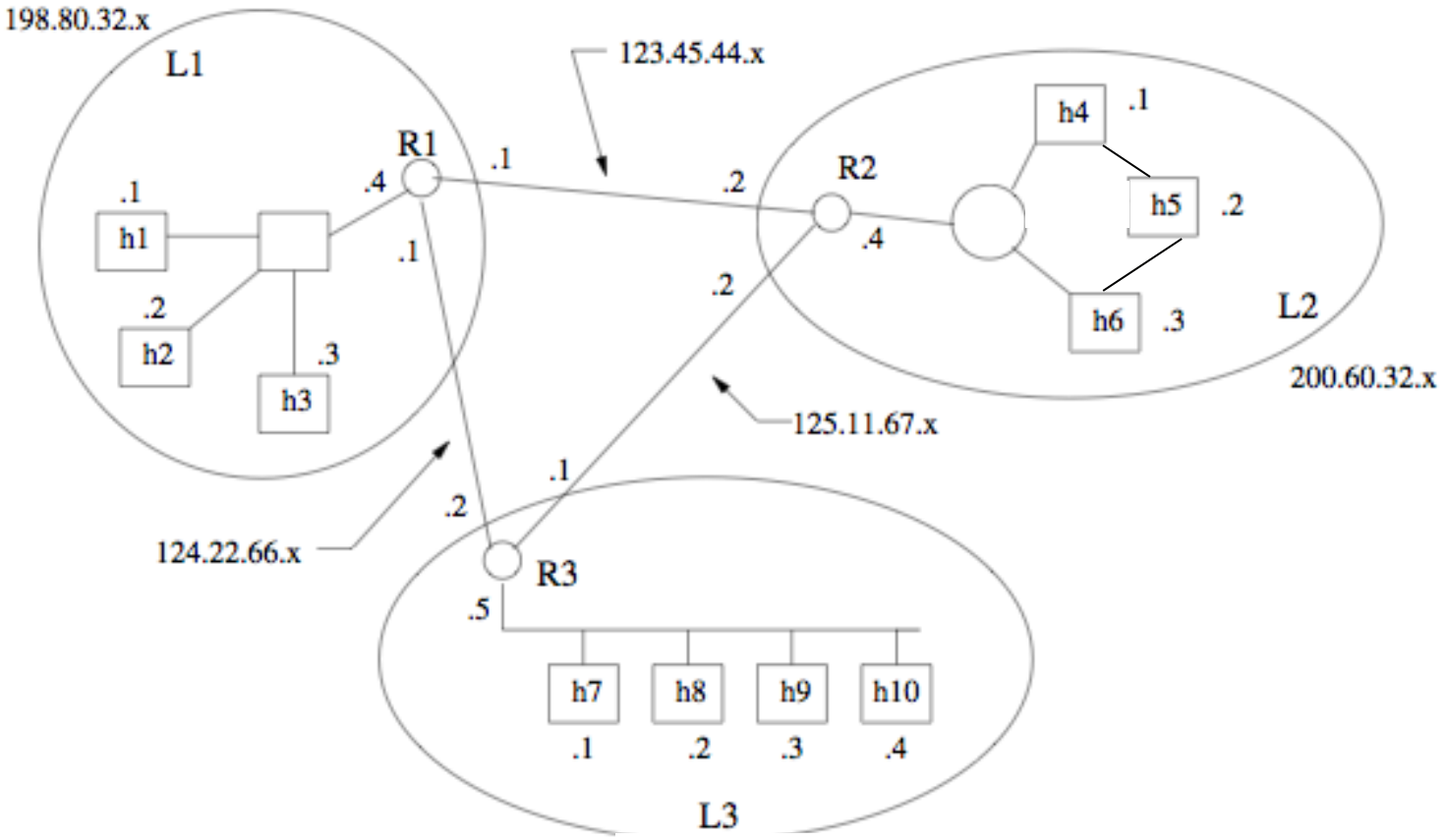
240.0.0.0 - 247.255.255.255

IP Address Classes (cont.)

- Class A
  - 8-bit network address, 24-bit node ID address, 126 networks of 16 million hosts
- Class B
  - 16-bit network address, 16-bit node ID address, 16,384 networks of 64K hosts
- Class C
  - 24-bit network address, 8-bit node ID address, 2 million networks of 254 hosts
- Class D is multicast address
- Class E is reserved for future use

IP Routing

- An IP router keeps track of other networks and all local hosts by using routing tables.



Router's Actions to IP Packets

- Checksum
  - Verify checksum
  - Decrement time-to-live field
  - Recompute checksum
- Extract the IP address of the packet.
- If the packet's source route option is marked, route the packet according to the route indicated. Skip the remaining steps.
- Determine the network ID contained in the IP address. Does the network ID match any network to which the router is connected?
  - If yes, determine the MAC address of the destination and send the IP packet to that destination.
  - If not, find the network ID in the routing table and forward the packet to the specified router.
  - If, for some reason, the network is not in the routing table, forward the packet to a default router.

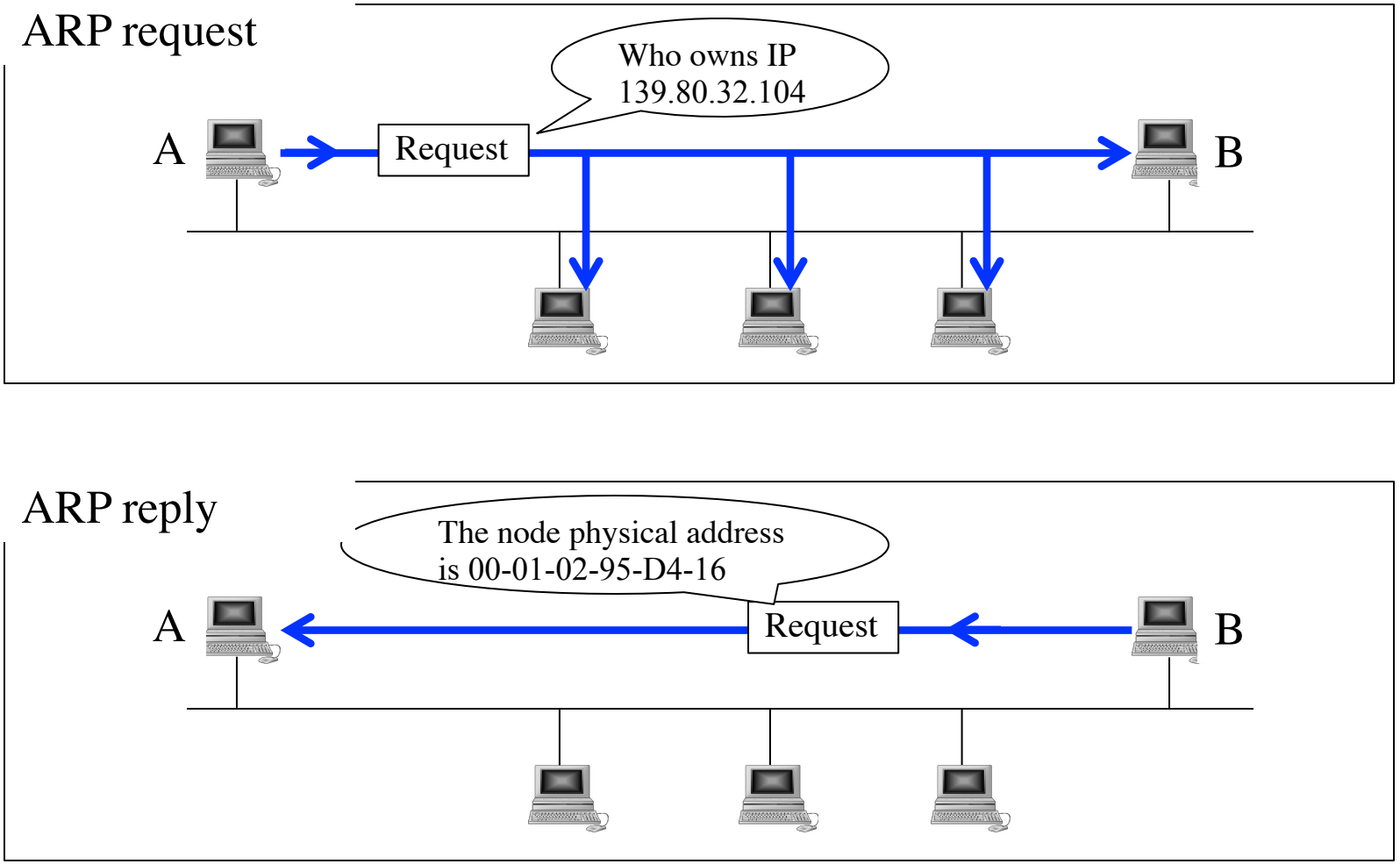
Mapping IP Addresses to Hardware Addresses

- The data link layer does not understand IP addresses.
- IP addresses cannot be used by the data link layer to send frames.
- How does an IP address get mapped to a MAC address?
  - Hardware address
  - Ethernet address
- Consider
  - 139.80.32.104
  - 00-01-02-95-D4-16

Address Resolution Protocol (ARP)

- When the IP layer gets frame with an IP address and determines it is on its own LAN, it needs to determine the hardware address of the destination.
- ARP algorithm:
  - The router broadcasts a frame onto the network asking "who owns the IP address specified?"
  - The host specified by the IP address responds with its hardware address.
  - The router uses the hardware address to send the packet to the destination.

Address Resolution Protocol (cont.)



A Routing Example

- Consider the network of slide 15.
  - L1 is a star LAN using IEEE 802.3.
  - L2 is a ring LAN using IEEE 802.5.
  - L3 is a bus LAN using IEEE 802.3.
  - The interconnecting network uses leased telephone lines as the physical layer and PPP as the data link layer.
  - R1, R2, and R3 are routers which connect between the LANs and the interconnecting network.
  - Each host (non-router) has an IP address (unique in the IP network).
    - h1-h3 have IP addresses: 198.80.32.1 - 198.80.32.3 (class C)
    - h4-h6 have IP addresses: 200.60.32.1 - 200.60.32.3 (class C)
    - h7-h10 have IP addresses: 132.80.32.1 - 132.80.32.4 (class B)
  - Each host has a MAC address, hi_mac, local to its LAN.

Routing Example (cont.)

- Each router is connected to both a LAN and the interconnecting network.
- Each router has an IP address for each of its LAN connections.
  - R1 has a LAN IP address 198.80.32.4
  - R2 has a LAN IP address 200.60.32.4
  - R3 has a LAN IP address 132.80.32.5
- Each router also has IP addresses for each of its interconnecting network connections.
  - R1 has IP addresses: 123.45.44.1 and 124.22.66.1
  - R2 has IP addresses: 123.45.44.2 and 125.11.67.2
  - R3 has IP addresses: 124.22.66.2 and 125.11.67.1
- Each router has multiple MAC addresses: one for its LAN, one for each of its interconnecting networks.
  - Will use *Ri_mac* to represent them.

A Routing Example (cont.)

- The routing tables are as follows

	R1	R2	R3
Destination	Next hop		
198.80.32	local	123.45.44.1	124.22.66.1
200.60.32	123.45.44.2	local	125.11.67.2
132.80.32	124.22.66.2	125.11.67.1	local

A Routing Example (cont.)

- IP layer at each host:
  - It can receive packets from the TCP layer.
  - If a packet is destined to a host in its LAN, it uses ARP to find the host's MAC address, *hi_mac*, and sends the packet using *hi_mac*.
  - If a packet is destined to a host outside its LAN, it finds the router's MAC address using ARP and sends the packet to the router using *Ri_mac*.

A Specific Routing Example

- Assume h1 wants to send an IP packet to h9.
- *h1* sets the destination field of the packet as 132.80.32.3.
- Because the packet has a destination outside L1, *h1* finds the MAC address of *R1* using ARP and sends the packet using *R1_mac.*
- When *R1* receives the packet, it checks the destination of the packet and finds it is 132.80.32.3.
- *R1* checks its routing table and finds the next hop for network 132.80 is 124.22.66.2 (*R3*). *R1* uses ARP to find the MAC address of 124.22.66.2, *R3_mac*, and sends the packet using *R3_mac.*
- When *R3* receives the packet, it checks the destination of the packet and finds it is 132.80.32.3.
- *R3* knows 132.80.32.3 is in its LAN. So *R3* uses ARP to find the MAC address of 132.80.32.3 (*h9_mac). R3* sends the packet using *h9_mac.*
- Finally the IP network layer in *h9* receives the packet.

Summary

- Concepts
  - TCP/IP protocol suite
  - TCP/IP reference model
  - IP protocol
  - IP packet
  - IP address, IP domain, and IP name
  - Address Resolution Protocol (ARP)
- How an IP packet is sent through Internet?