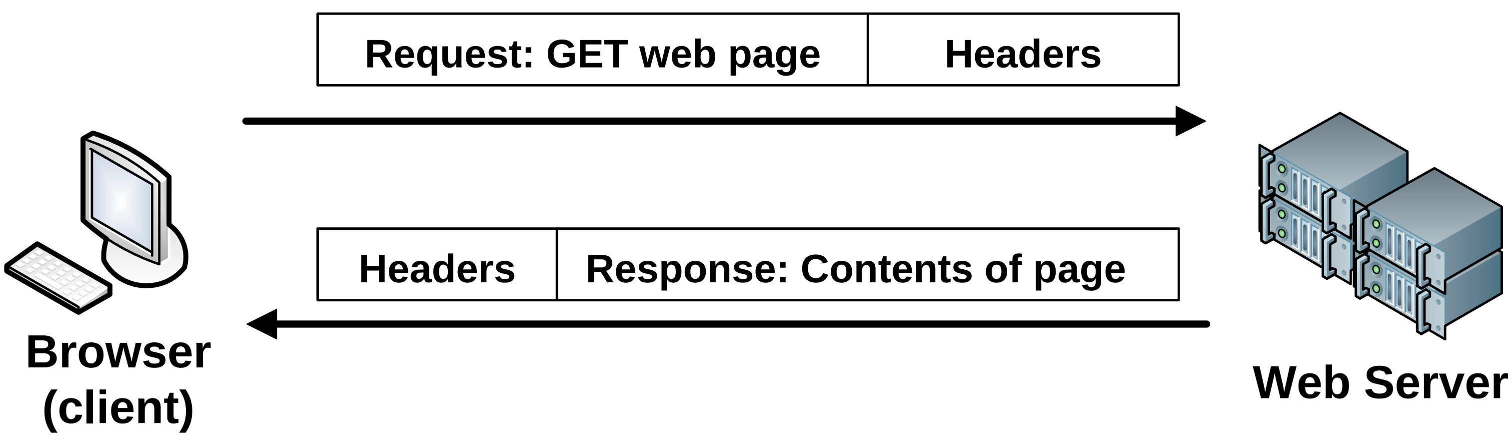
NET 363
Introduction to LANs

Data Packets: Protocols and Addresses

Greg Brewster
DePaul University

Packets?

- All network communications is done using data packets. A packet is a sequence of bits sent over a link containing:
  - An initial set of bytes called the **packet headers**, which contain control information about how and where to transmit the packet across the network
  - The **application data** (either Request or Response)
  - Possibly, **packet trailer** bytes at the end.

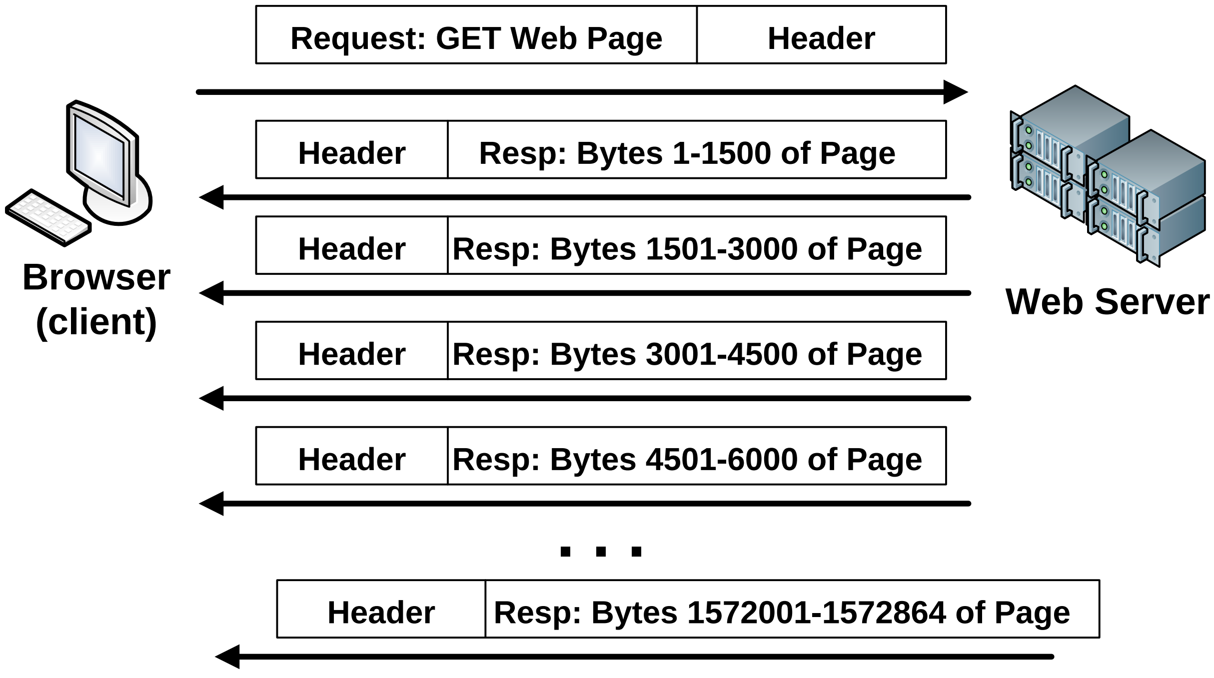


Maximum Packet Size

- Packets can't be too large. There is a maximum packet size (or maximum transmission unit – **MTU**).
- For example: maximum Ethernet packet size is 1500 bytes of user data (more or less). We will assume MTU = 1500 bytes unless otherwise stated.
- Clients typically send single-packet Requests. Servers typically send multi-packet Responses.
  - Because Requests are small enough to fit in 1 packet, but Responses are often too large to fit in 1 packet.

Multi-packet Response

- For example, a server Response for downloading a 1.5 Mbyte web page requires over 1000 packets to send.



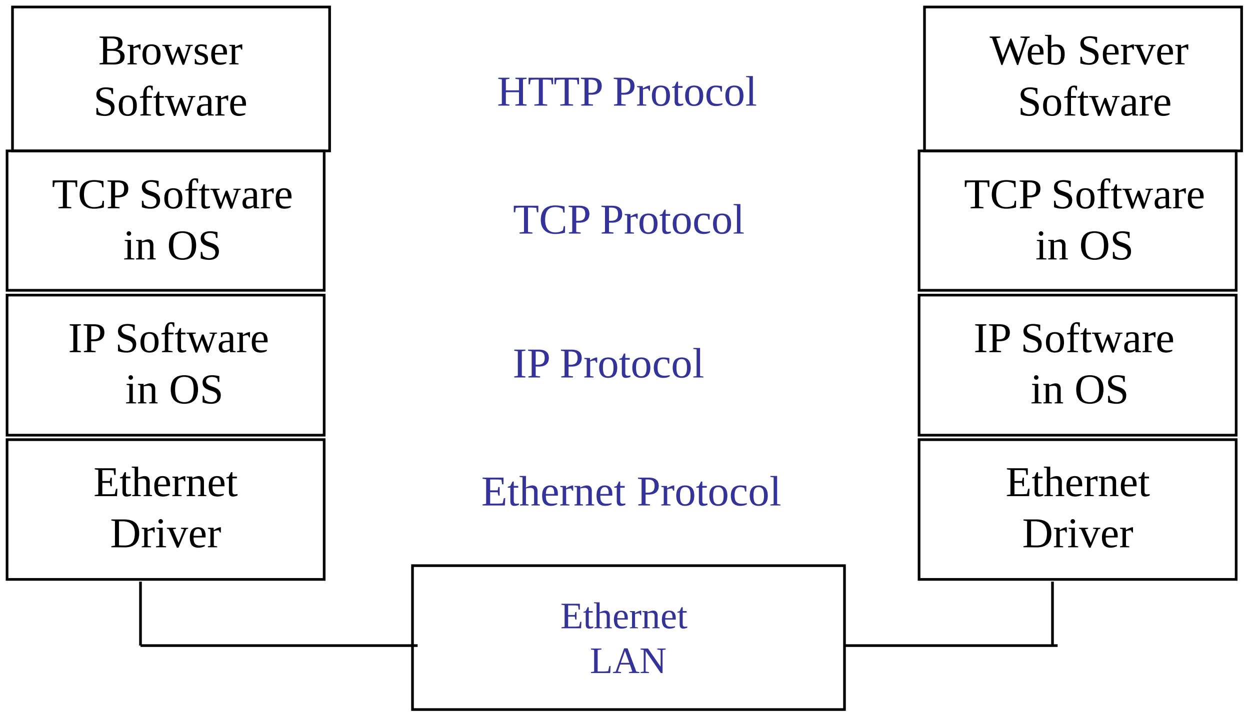
Protocols

- Clients and servers must follow a set of rules called a protocol which determines
  - Packet format
    - Permissible requests and responses
    - Format of header information and data
  - Packet ordering and timing
- Protocol standards are documents that define protocols.
  - For Internet applications, protocol standards are called Request for Comments (RFCs).
    - http://www.rfc-editor.org/rfcsearch.html

TCP/IP Model Layers

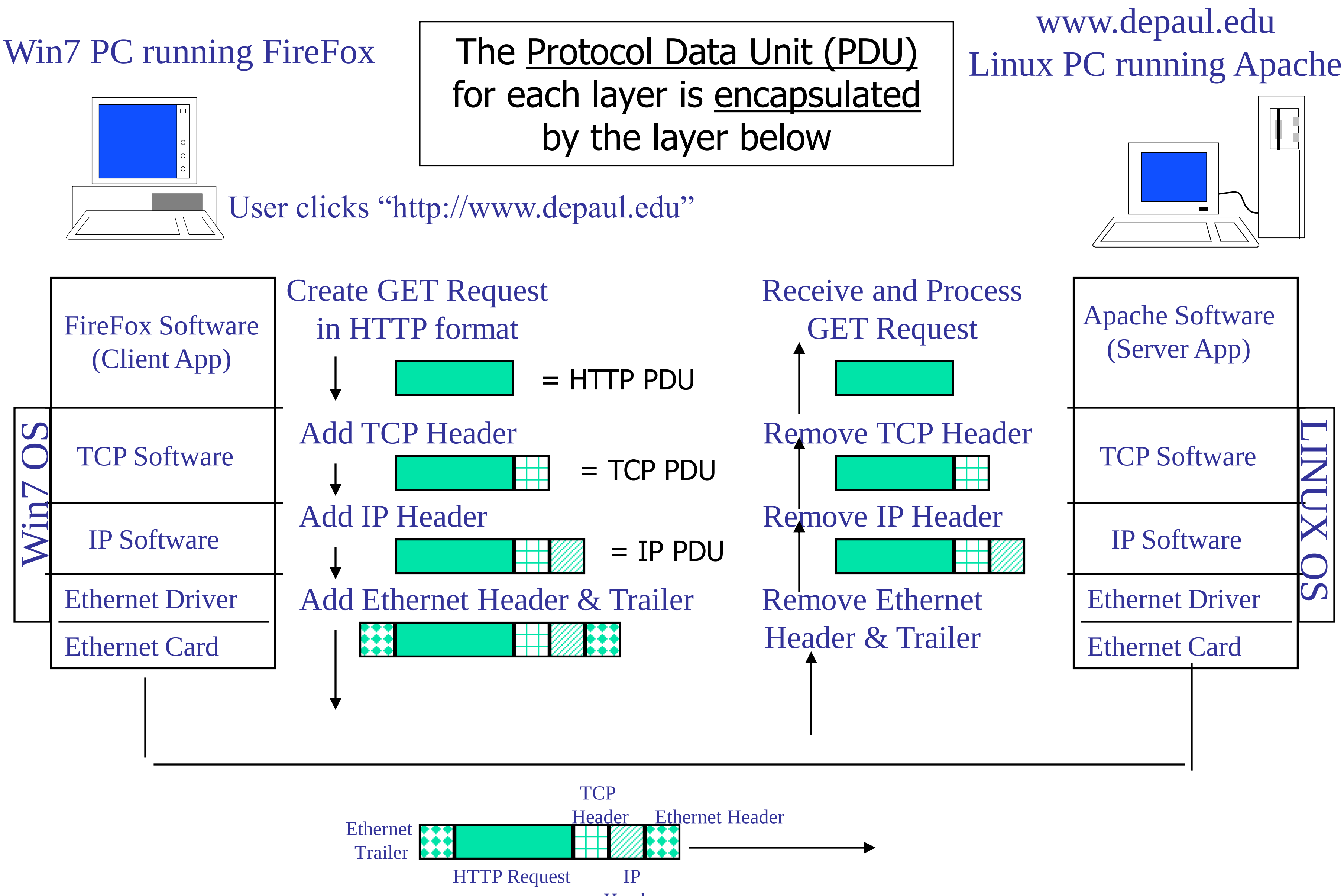
- **Application Protocol**
  - Controls the exchange of Requests and Responses between the client process and the server process.
  - Examples: Hypertext Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP), etc.
- **Transport Protocol**
  - Implements Flow Control and Error Control, if needed. Includes Port Numbers identifying the application process.
  - Examples: Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- **Internet Protocol**
  - Controls the routing of the packet across the Internet.
  - Examples: IPv4, IPv6, IPSec (secure IP)
- **Data Link Protocol**
  - Controls the sending of a packet across a single subnet.
  - Examples: Ethernet, Point to Point Protocol (PPP), etc.

Example: Web (HTTP)



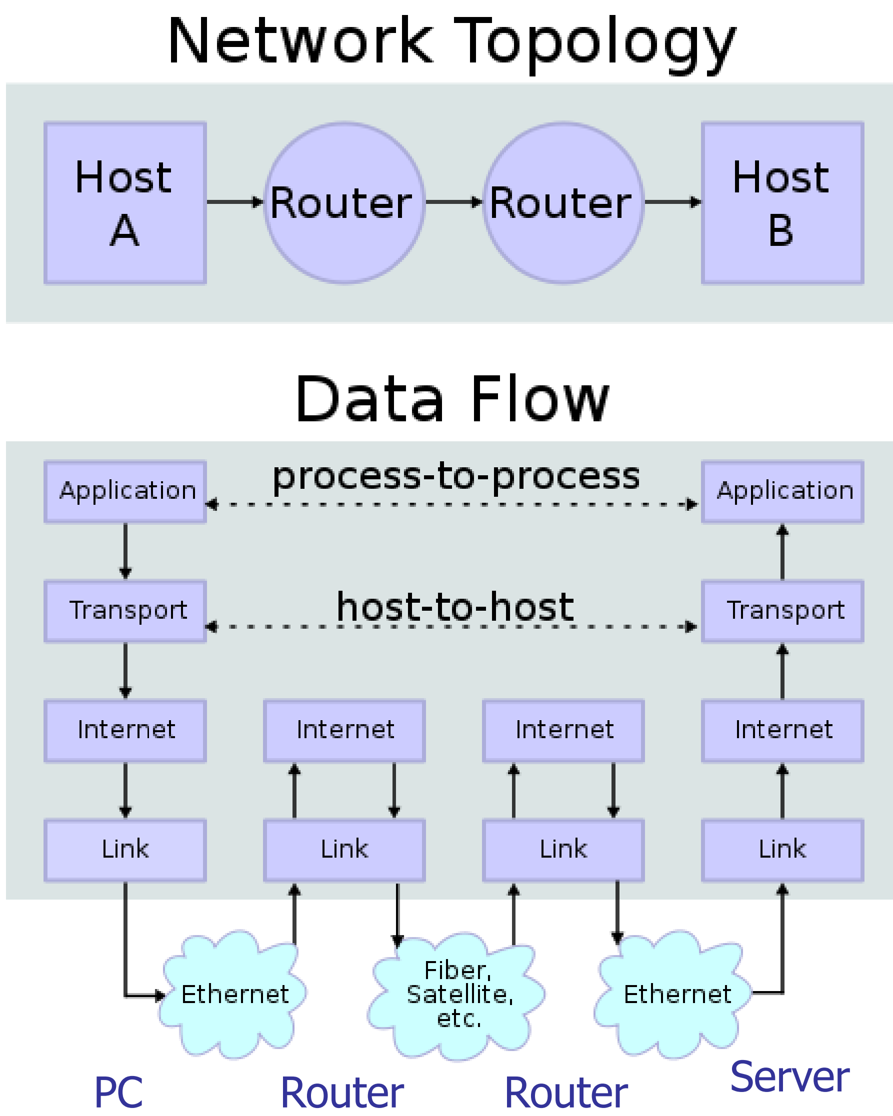
Each Layer Adds a Header

The Protocol Data Unit (PDU) for each layer is encapsulated by the layer below



Why All The Layers?

- **Why** do we need multiple layers?
- Each header is only viewed and used by certain devices.
  - The <u>Ethernet header</u> is used by Ethernet hubs and switches.
  - The <u>IP header</u> is used by IP routers
  - The <u>TCP header</u> is used by PCs and servers for error detection/correction.
  - The <u>application header</u> (i.e. HTTP) is used by the application (i.e. browser)



Source: Wikipedia

Addresses

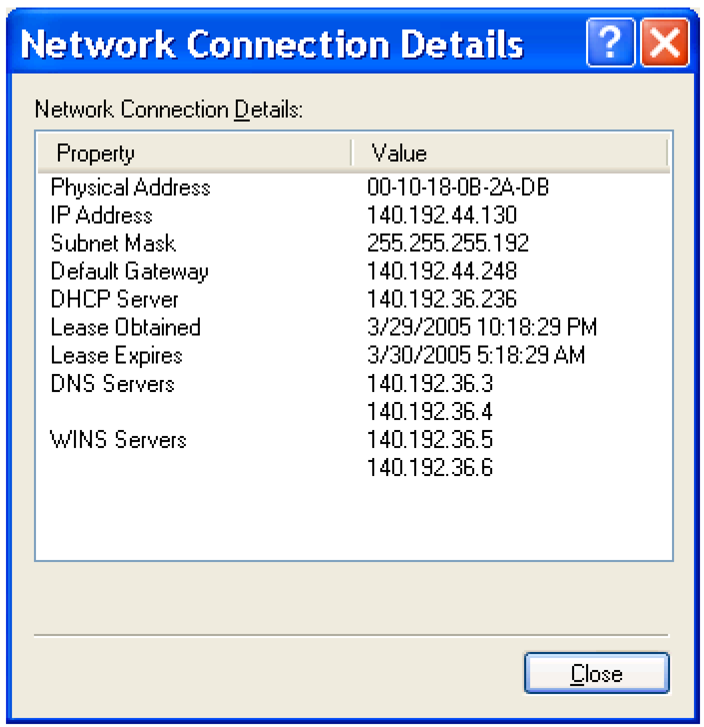
- Addresses identify systems at each layer
- Data Link level address
  - Local physical address (like serial number)
  - Example: Ethernet 6-byte MAC: 00:1a:23:43:22:0d
- Network level address
  - Global logical address (assigned by net admin)
  - Example: IPv4 address (140.192.33.2)
- Transport level address
  - Identifies software process on a machine
  - Example: TCP/UDP Port number (port 80 for web server)

Ethernet MAC addresses

- Every Ethernet interface has a 6-byte **physical address** or **MAC (medium access control) address** assigned and burned into the interface hardware when it is manufactured.
- MAC address is like a serial number.
- MAC address of every Ethernet device is guaranteed to be globally unique.

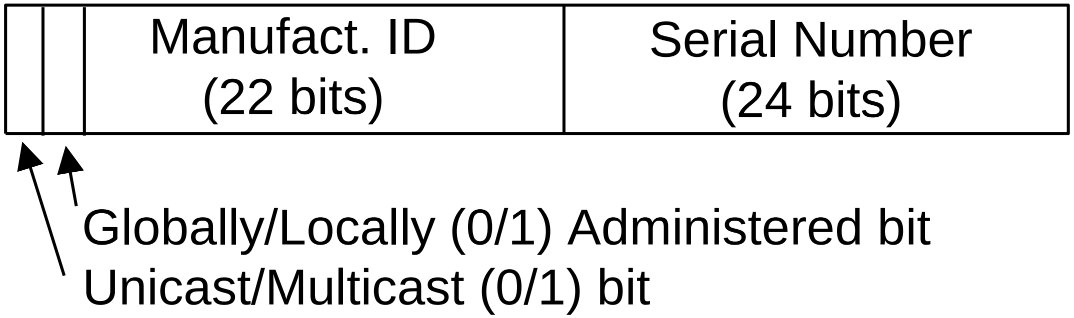
Device addresses

- Address information (both MAC and IP) for a network connection can be found in Connection Details or by running "ipconfig /all" on Windows. (For Mac: "ifconfig" in Terminal or "About this Mac").



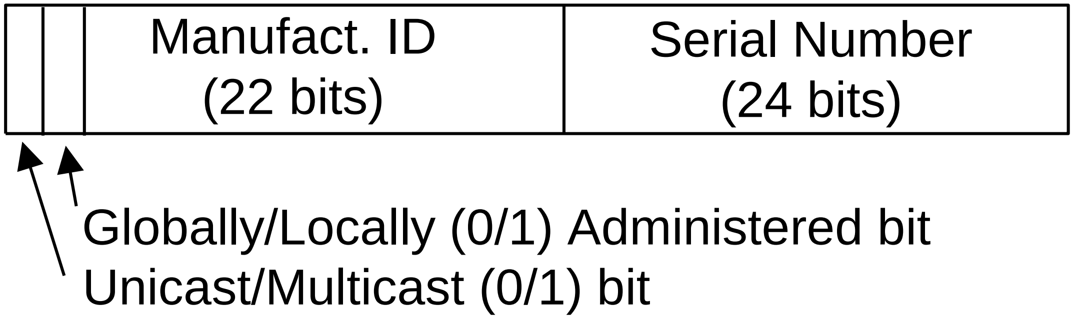
Ethernet MAC Address format

(length = 6 bytes = 48 bits)



- Manufacturer IDs are uniquely assigned to Ethernet equipment manufacturers by IEEE (Institute for Electrical and Electronics Engineers).
- Each manufacturer ensures that each Ethernet interface on every device they make has a unique Serial Number.
- Result: every Ethernet interface has unique address.

Ethernet MAC Address format
(length = 6 bytes = 48 bits)



- Special address bits:
  - Globally/Locally Administered bit – determines if this address was allocated by IEEE (0) or locally generated (1).
  - Unicast/Multicast bit – determines if this address corresponds to a single device (0) or a group of devices (1).
- If all 48 bits are set to 1 (FF:FF:FF:FF:FF:FF) this is the broadcast address which causes data packet to be copied to every device on the LAN.

IPv4 Addresses

- Each **IP address** is **4 bytes** long
- Dotted decimal notation
  - Each byte (8 bits) is written in decimal separated by dots, like
  - Each of the 4 values is in range 0 - 255.
  - Example: 150.21.39.52

IP Addresses

- IP addressing is **hierarchical.**
- In "**Classful Addressing**" an IP address contains 3 parts:
  - An **IP Network** part that is used by Internet backbone routers to deliver packets to a particular IP Network. IP Network values are assigned by Internet Assigned Numbers Authority (www.iana.org) to guarantee global uniqueness.
  - An **IP Subnet** part that is used by internal routers within an IP Network to deliver packets to a particular Subnet. Subnet address values are assigned by local network administration.
  - An **IP Host** part that identifies a particular individual device on the subnet. Chosen by network admin or randomly assigned from subnet address pool by DHCP server.

Address Example

Network		Subnet	Host
130	**88**	**55**	**12**

Network = 130.88.0.0/16

Subnet Mask = 255.255.255.0

Subnet = 130.88.55.0/24

Host = 12

DePaul IP Addressing (140.192.0.0/16 block)

- DePaul University was assigned IP Network prefix **<u>140.192.0.0/16</u>** by the IANA back in the 1980s. This is a **Class B** address. So, DePaul controls all IP addresses that start with 140.192 in 1st 2 bytes (140.192.0.0 – 140.192.255.255).
- DePaul Information Services (IS) assigns <u>Subnet IDs</u> to various departments and groups at the university. For example:
  - IP subnet 140.192.32.0/24 – CTI servers
  - IP subnet 140.192.34.0/24 – 6th and 7th floor CTI office PCs
  - IP subnet 140.192.35.0/24 – 8th and 9th floor CTI office PCs
- Individual devices in each subnet are then each assigned a unique <u>Host ID</u>, either manually or automatically (using Dynamic Host Configuration Protocol (DHCP)).

DHCP

- How does a device get assigned an IP address?
  - Network admin could do <u>static configuration</u>.
  - <u>OR</u> device can broadcast to DHCP server (Dynamic Host Configuration Protocol) to obtain the **<u>4 IP Host Configuration Values</u>** required to send IP data**:**
    - IP Address
    - Subnet Mask
    - Default Gateway IP (router interface on subnet)
    - DNS Server IP address
- DHCP server maintains pool of free IP addresses for each subnet and allocates with a *lease time*.

TCP/UDP Ports

- TCP and UDP headers contain two 2-byte **Port Numbers**:
  - Source Port
  - Destination Port
- A Port Number identifies a particular software process running on a computer
  - When a client process (such as a browser window) starts up, the operating system assigns it an unused Private Port Number.
  - When a server process (such as a Web server) executes, the operating system binds it to a Well-Known or Registered Port number based on its function.

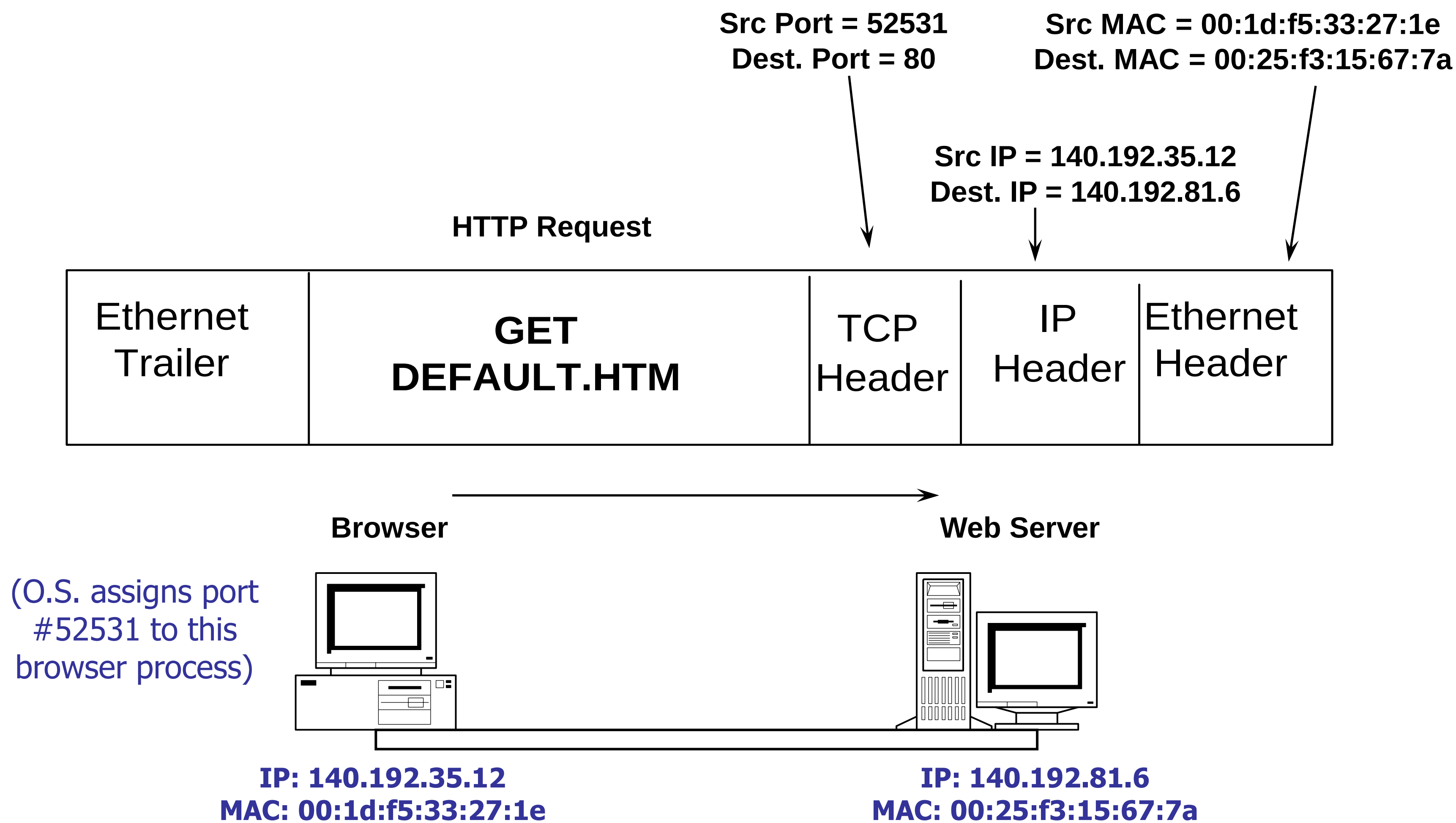
Port Number Ranges

- 3 defined ranges of port numbers:
  - Well Known Ports (0-1023)
    - These port numbers are specified by IANA to identify globally recognized server applications. They never change.
  - Registered Ports (1024-49151)
    - These port numbers are assigned by software vendors for new server processes. IANA may register these port numbers, but global use of registered numbers is not required.
  - Dynamic/Private Ports (49151-65535)
    - These port numbers are locally assigned to client processes.
- See http://www.iana.org/assignments/port-numbers

Some Well-Known Port Numbers
(memorize for CCNA)

- Echo (ping) = UDP port 7
- File Transfer (FTP) = TCP port 21
- Secure Shell (SSH) = TCP port 22
- Remote login (Telnet) = TCP port 23
- E-mail (SMTP) = TCP port 25
- DNS = UDP port 53
- HTTP (Web) = TCP port 80
- Post Office Protocol (POP3) = TCP port 110
- … and many, many more!!

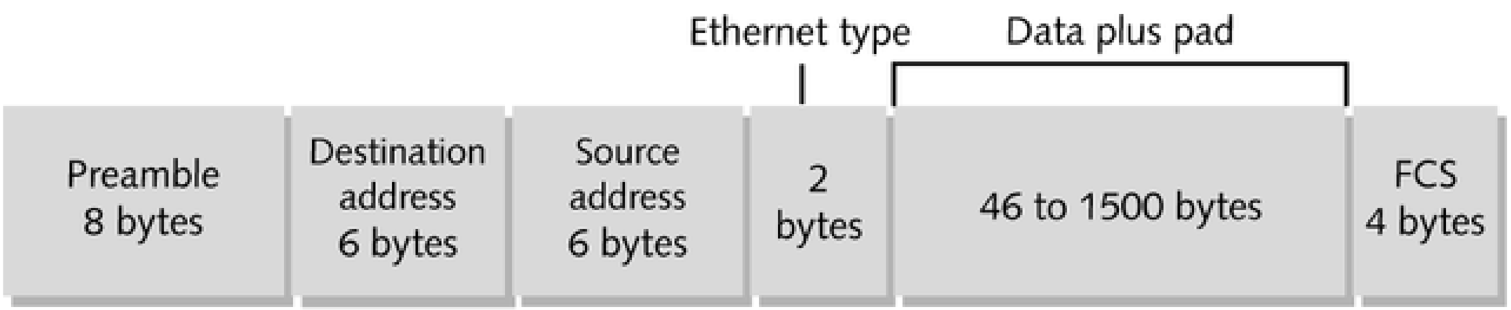
Addressing Example: Web Request
(assuming src/dest on same subnet)



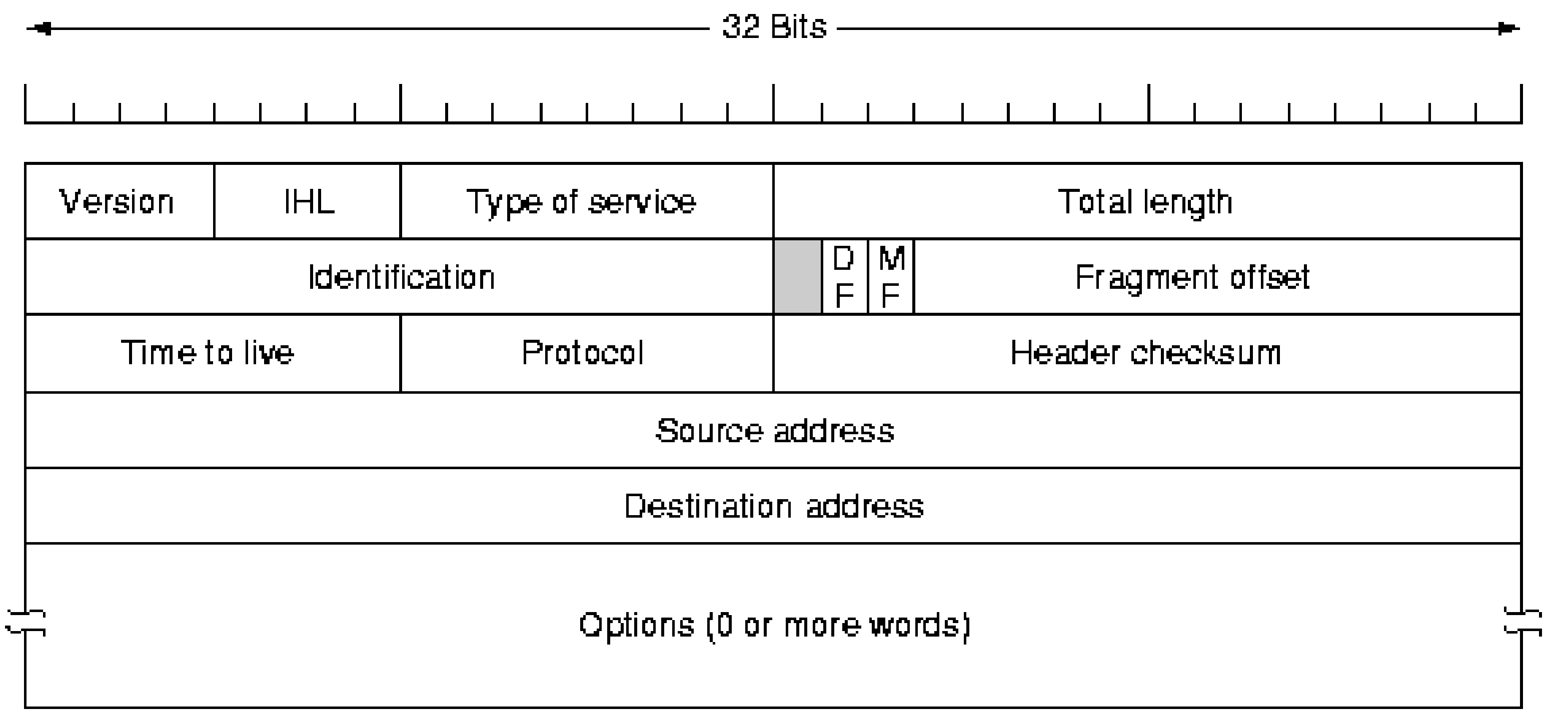
In Response packet, Src and Dest values will be swapped in all headers

(Wired) Ethernet Frame Header

- **Ethernet frame header:**
  - **<u>Preamble</u> field contains fixed bit values for synchronizing sender and receiver clocks.**
  - **<u>Destination</u> and <u>Source</u> MAC addresses (6 bytes each).**
  - **<u>Ethernet Type</u> field used to identify the protocol carried in the next header (IP, ARP, AppleTalk, etc.)**
- **Ethernet frame trailer**
  - **<u>FCS</u> used for error checking.**



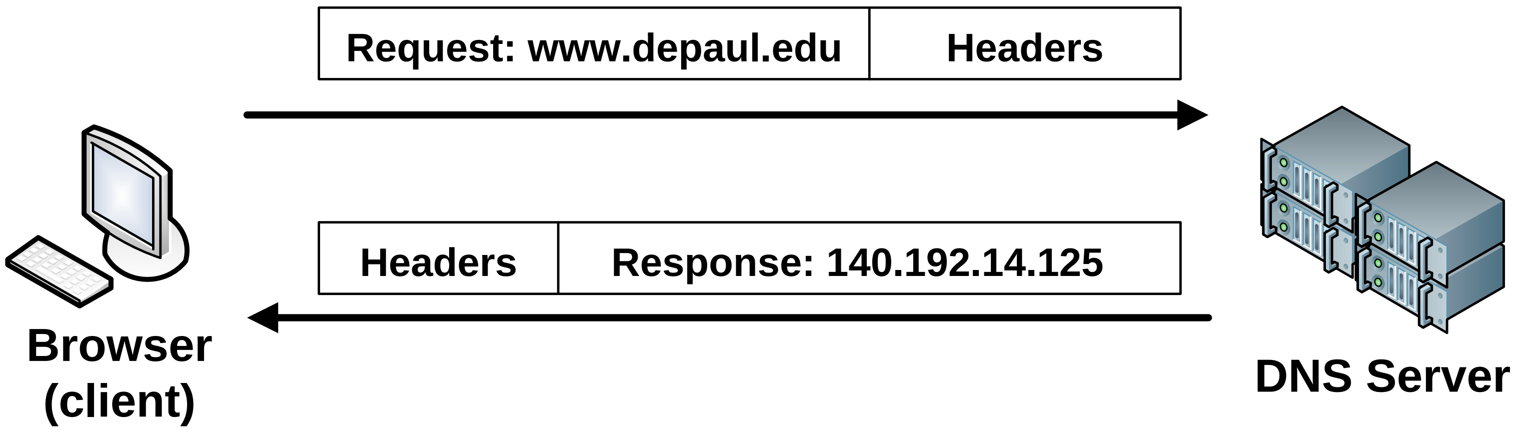
IPv4 Header



32 Bits
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
Options (0 or more words)

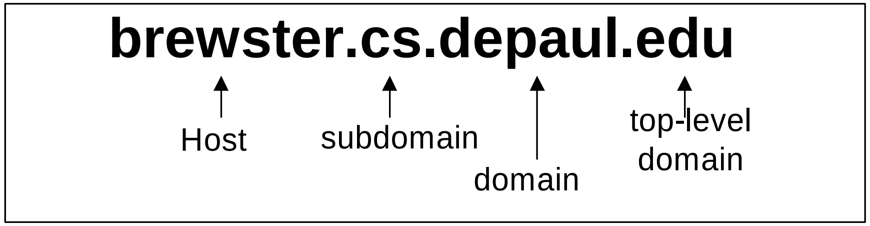
DNS Names

- There are **Domain Name System (DNS)** servers on the Internet that translate from a DNS Name to an IP address.
- Client sends **DNS Request** with DNS name to DNS Server
- DNS Server sends **DNS Response** with corresponding IP Address.

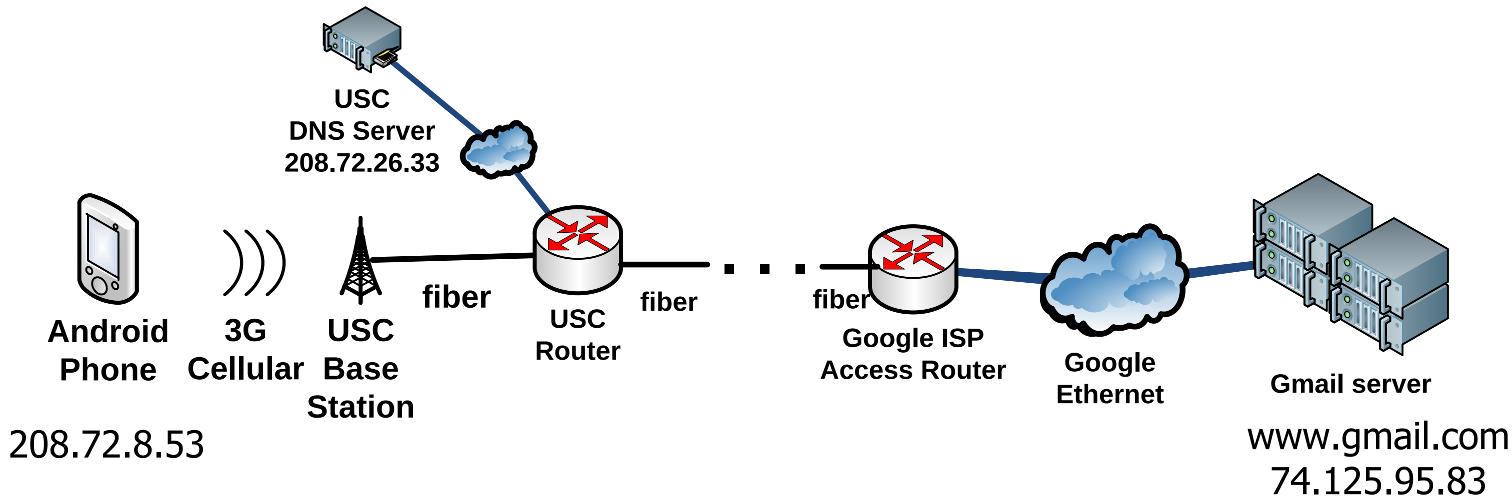


Domain Name System

- A system of **Domain Name System (DNS)** servers allows users to refer to any device by **DNS Name** (i.e. brewster.cs.depaul.edu) rather than by **IP address** (i.e. 140.192.32.9)



DNS Lookup to get to Gmail



IP address of local DNS Server (208.72.26.33 in this example) must be configured into device.

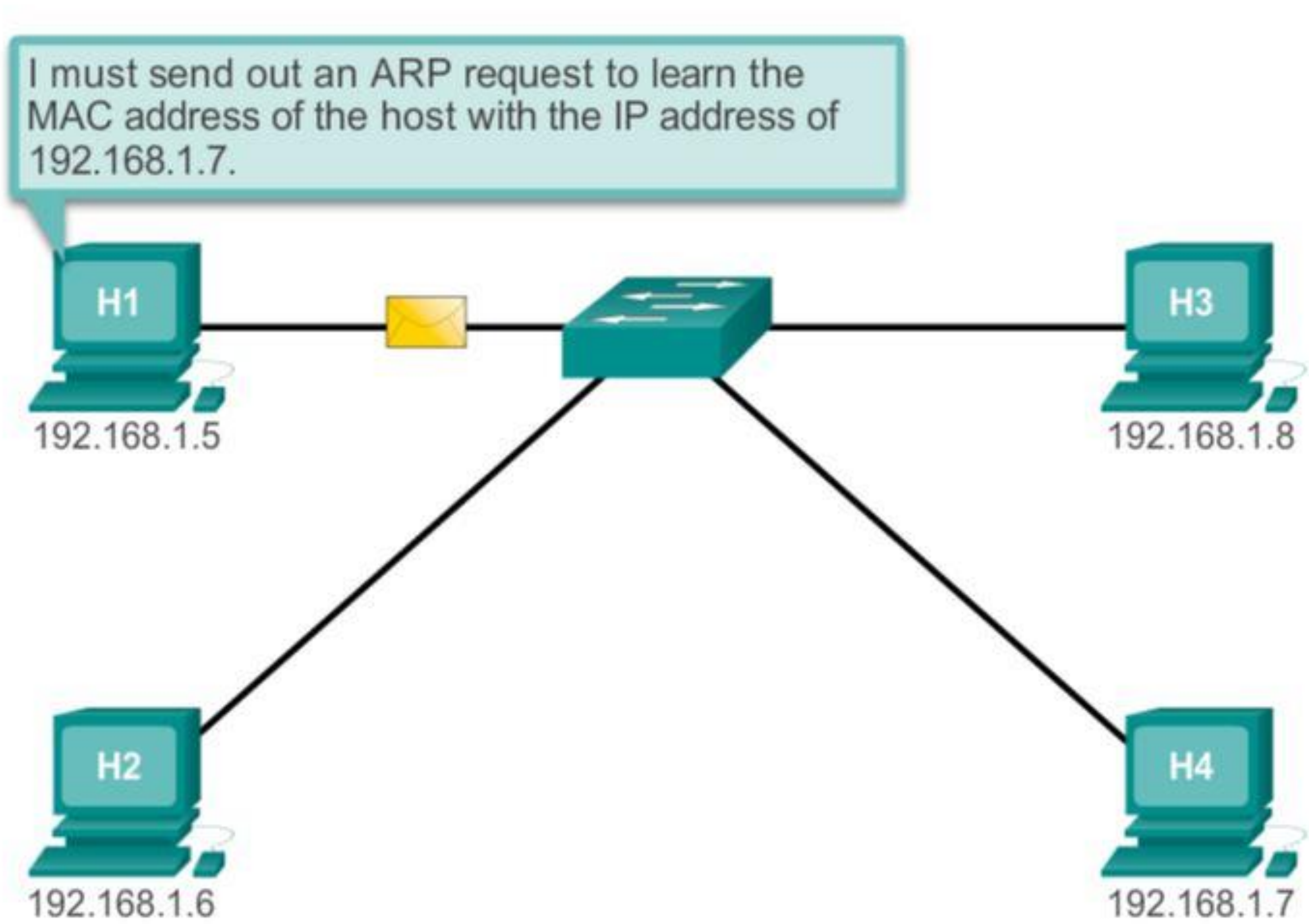
How does a PC find IP/MAC address of DNS name?

- User types a DNS name: i.e. "www.depaul.edu"
- PC sends DNS Request packet to DNS server and gets back the IP address of destination.
- Then PC can use ARP to find the Physical / MAC / Ethernet Address associated with the IP address:
  - PC checks in local ARP Cache – might already be there.
  - If not and if destination is on local subnet, PC broadcasts an ARP Request packet and gets back the Physical address of destination, and sends packet directly to destination.
  - If destination is on a remote subnet, then PC forwards the packet to the local router (called the *default gateway*).

Address Resolution Protocol (ARP)

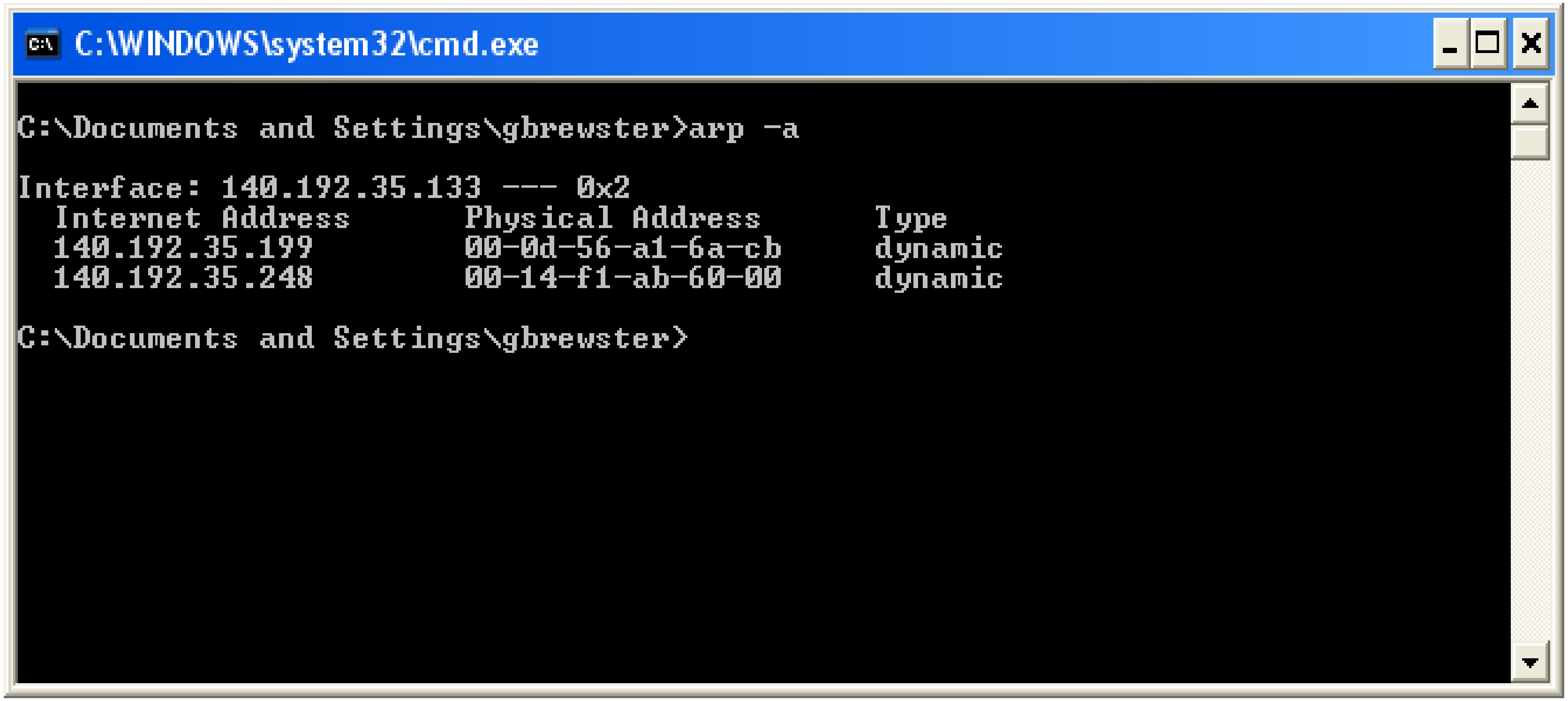
- ARP is a broadcast protocol used to determine <u>the MAC address corresponding to a known IP address</u>
  - *ARP Request* packet containing an IP address is <u>broadcast</u> on a subnet.
  - *ARP Reply* is sent by device that recognizes its IP address in the ARP Request.
  - IP Address/MAC Address pairs are stored in **ARP Table** (also called **ARP cache**) by the sender so ARP Request does not need to be re-sent for the same destination.

ARP Process


I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
H1
192.168.1.5
H3
192.168.1.8
H2
192.168.1.6
H4
192.168.1.7

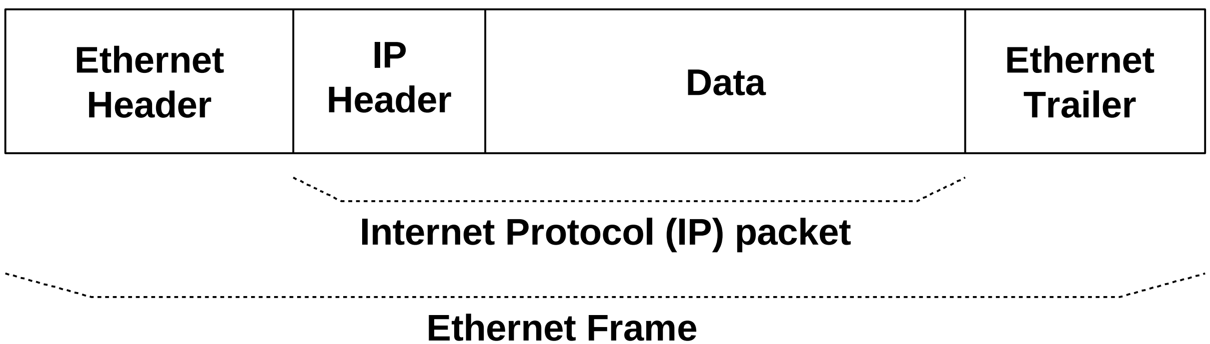
Viewing your ARP Cache

- You can view the contents of your computer's ARP Cache using the 'arp –a' command (PC or Mac)



Packets inside Frames

- Terminology: **IP packet** is carried inside **Ethernet frame**. IP is encapsulated by Ethernet.



It used to be worse: the OSI 7-layer model

- The original layered protocol model was the 7-layer Open Systems Interconnect model (1977)
  - Theoretical model used to describe 7 separate layers of functionality required for end-to-end data communications
  - Useful to understand for historical context

The 7 OSI Layers
with WWW examples

- Layer 7: Application Layer (ex: HTTP)
- Layer 6: Presentation Layer (ex: SSL encryption)
- Layer 5: Session Layer (ex: SSL authentication/login)
- Layer 4: Transport Layer (ex: TCP)
- Layer 3: Network Layer (ex: IP)
- Layer 2: Data Link Layer (ex: Ethernet Framing)
- Layer 1: Physical Layer (ex: Ethernet Hardware)

Figure 2.6 *Summary of OSI Layers*

Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

Cisco Network Design Model

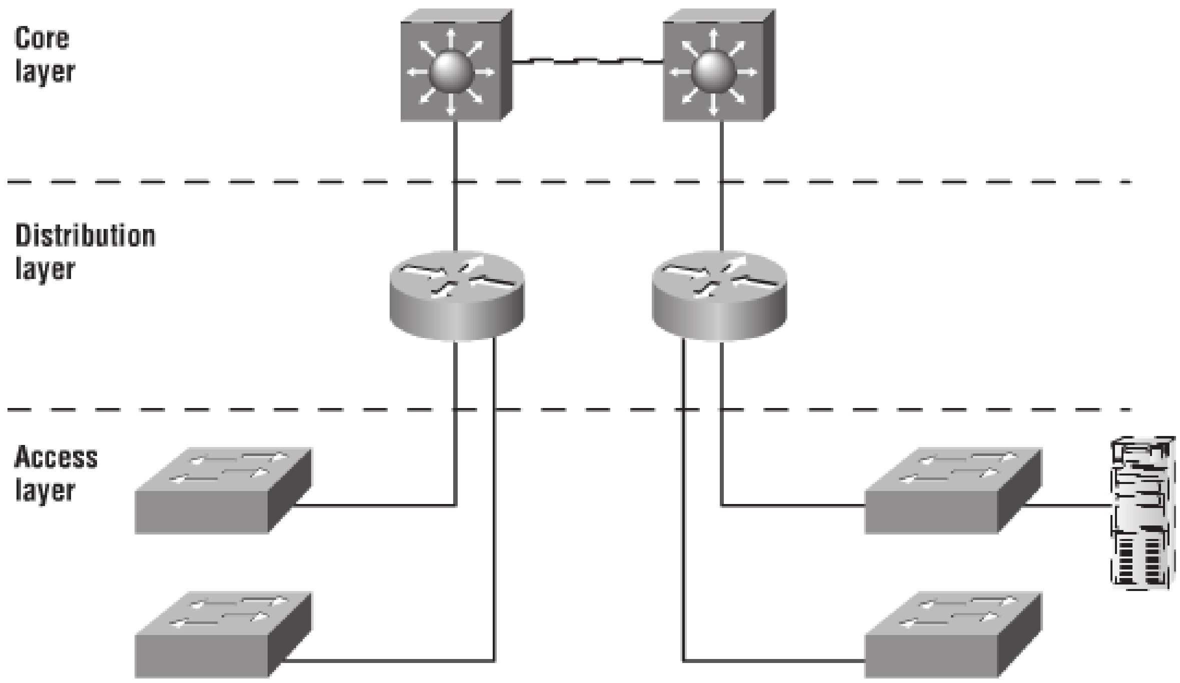


FIGURE 2.14 The Cisco hierarchical model

Used to categorize network device types and functions in a large enterprise network

3-Layer Network Design Model

- Access Layer
  - Contains hubs and switches that connect directly to user desktops and servers.
  - Key features: switch port security, virtual LANs, multicast
- Distribution Layer
  - Contains layer 3 switches and/or routers that interconnect access layer switches and core backbone.
  - Key features: redundancy, virtual LANs, access control lists, address translation (NAT), DHCP, multicast, RIP, EIGRP, OSPF.
- Core Layer
  - Contains high-end routers that form the backbone of the organizational network and connect to ISP or other AS.
  - Key features: redundancy, highest reliability, highest data rates, minimize router features (for performance), EIGRP, OSPF, BGP.