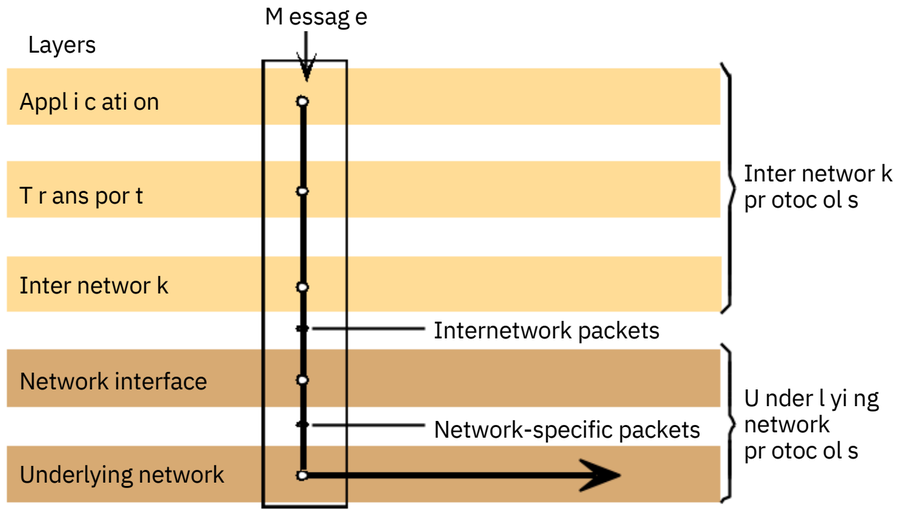
NETWORK PROGRAMMING

Lecture 2

What Exactly is a Protocol?

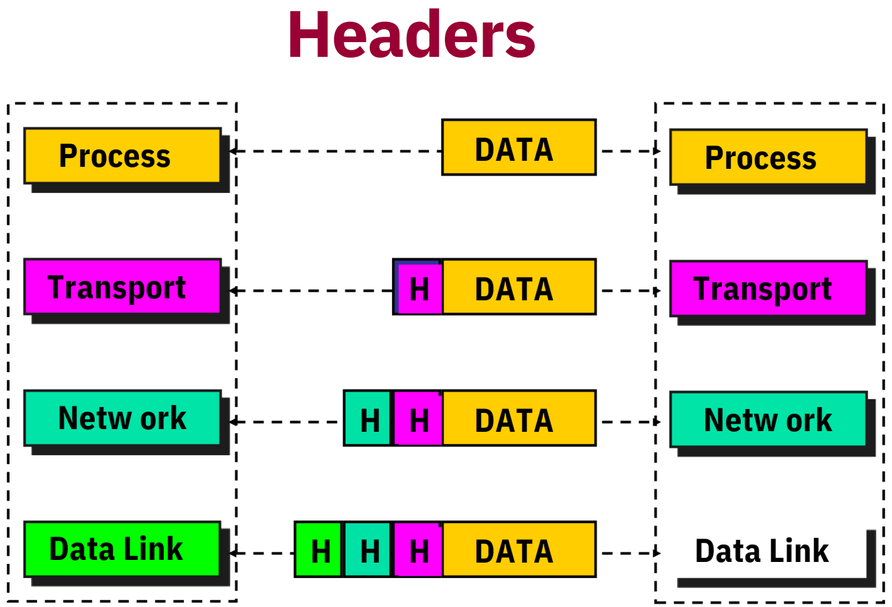
- An agreed upon convention for communication.
  - both endpoints need to understandthe protocol.
- Protocols must be formally definedand unambiguous!
- We will study several existing protocols and perhaps develop a few of our own.

Internetwork Layers



Layering & Headers

- Each layer needs to add some control information to the data in order to do it’s job.
- This information is typically prepended to the data before being given to the lower layer and therefore known as header.
- Once the lower layers deliver the data and control information -the peer layer uses the control information.



What are the headers?

Physical: no header -just a bunch of bits.

Data Link:

- address of the receiving endpoints
- address of the sending endpoint
- length of the data
- checksum.

Network layer header - examples

- protocol suite version
- type of service
- length of the data
- packet identifier
- fragment number
- time to live
- protocol
- header checksum
- source network address
- destination network address

Important Notes

- **Data-Link**: communication between machines on the same network.
- **Network**: communication between machineson possibly different networks.
- **Transport**: communication between processes(running on machines on possibly different networks).

Ports

- Modern computers do many different things at once. Email, FTP, Web, … all need to be separated.
- This is accomplished through ports.
- Each host with an IP address has 65,535 logical ports which are purely abstractions.
- Each port is identified by a number (1 ~ 65535).
- Each port can be allocated to a particular service.
- Data for a particular service is sent to the selected port. The receiver checks each packet for both the address and the port.
- 1 ~ 1023 are reserved for well-known services.

Important Internet Services & Protocols

- Ping (Packet Inter-Network Grouper)
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- NNTP (Network News Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol 3)
- SNMP (Simple Network Management Protocol)
- Telnet (Network Virtual Terminal Protocol)

Well-Known Port Assignments

Protocol	Port	Purpose
ftp-data 20	21	FTP file transfer FTP
ftp telnet	23	commands Telnet connection
smtp	25	Simple Mail Transfer Protocol
finger	79	Get information about users
http	80	HyperText Transfer Protocol
pop3	110	Post Office Protocol V3
nntp	119	Network News Transfer Protocol

Sockets

- A server can server many clients at the same time and needs some way of distinguishing between clients.
- A socket is an abstract concept (not a hardware element) used to indicate one end-point of a link between two processes.
- A client creates a socket and send a request to the server.
- On receiving the request, the server create a new socket which is dedicated to the communication with that client.

IPv4 Addressing

- Every computer on an IP network is identified by a unique four-byte address(such as 203.64.88.11).
- Each number is in the range of 0to 255.
- A packet header includes the destination address and the source address.
- Human aren’t very good at numeric address. The Domain Name System(DNS)was developed to do the translation between symbolic hostnames (csie.ndhu.edu.tw) and numeric IP address.
- For network programming, we may need to process both hostnames and IP addresses.

Internet Address Classes

- Internet addresses are assigned by the Internet Network Information Center(**InterNIC**).
- IP addresses are allocated in blocks of two sizes called **Class B**and **Class C**.
- A **Class C**specifies the first three bytes of the address (eg. 203.64.88) which allows room for 254 addresses.
- .0 and .255 addresses are reserved and should never be assigned to hosts.
- A **Class B**address block only specifies the first two bytes which has room for roughly 65,000 hosts.
- Several address blocks and patterns are special. All 10. And 192. Address are deliberately unassigned. These **non-routable**addresses are useful for building private networks.

Internet Address Classes (Cont.)

- Addresses beginning with 127 (most commonly 127.0.0.1) always mean the **local loopback address**. Theses address always point to the local computer. The hostname for this address is generally **localhost**.
- The address 0.0.0.0 always refers to the originating host, but may only be used as a source address.
- Any address that begins with 0.0 is assumed to refer to a host on the same local network.

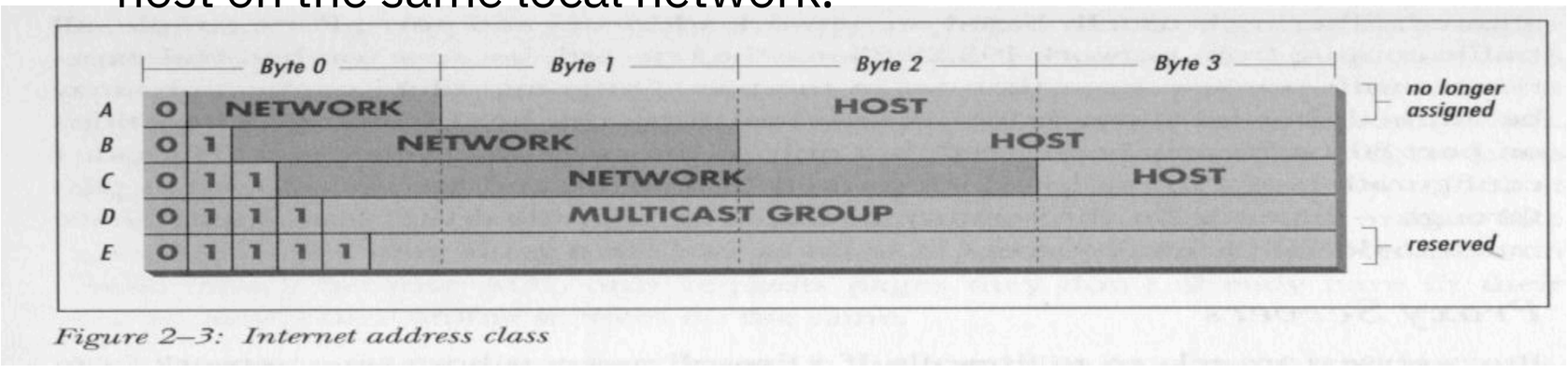


Figure 2–3: Internet address class

IPv6 Addressing

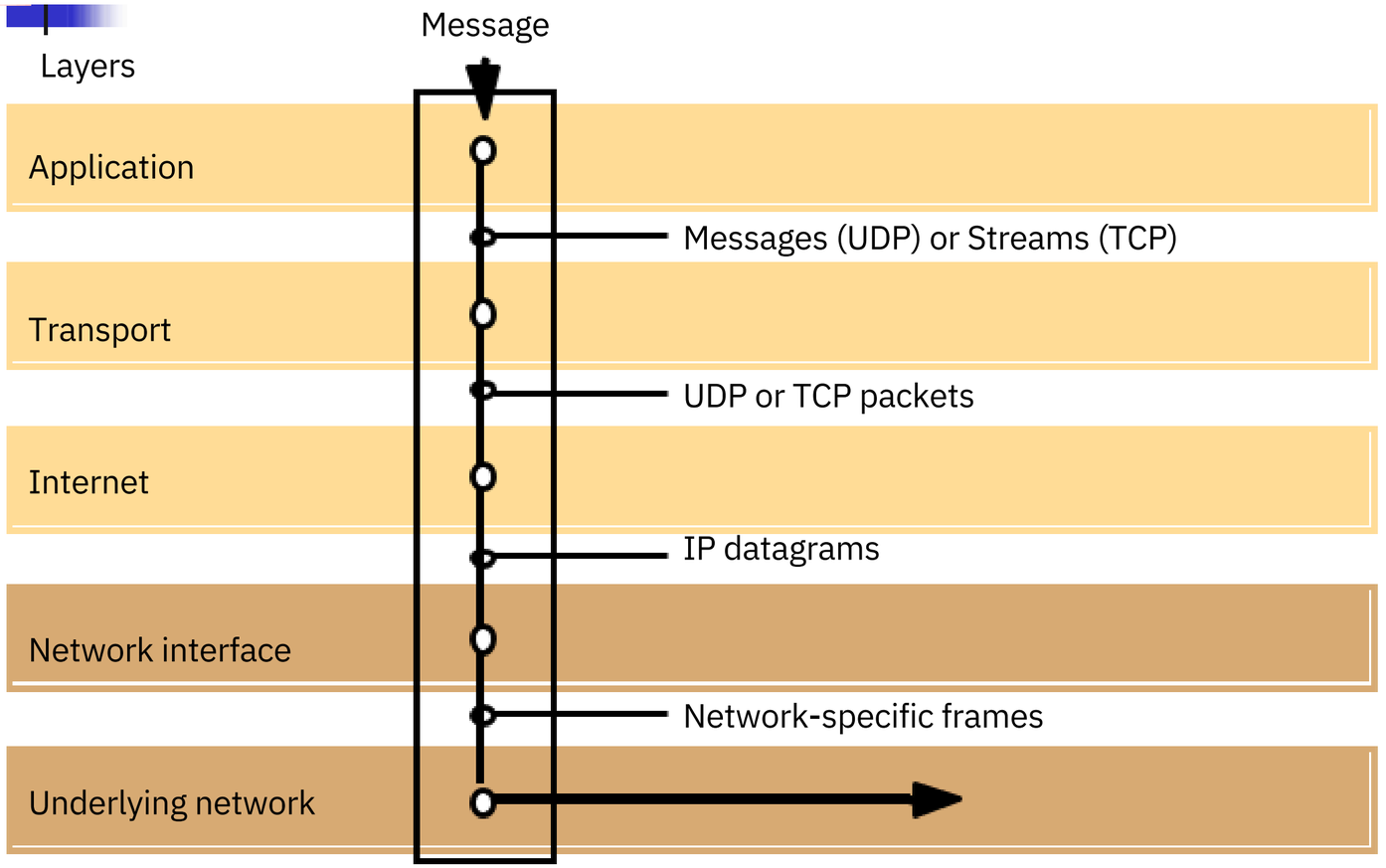
- World IPv6 Launch began on 6 June 2012.
- Uses 128-bitaddresses, which provide massively more addresses, written as colon-separated hexadecimal numbers, eg.

- Most common Internet applications already work with IPv6.
- IPv6 will gradually replace IPv4, with the two coexisting for a number of years during a transition period.

IP, TCP and UDP

- Since IP was developed with military sponsorship :
  - designed to be **robust**(allow multiple routes between any two points), **open**and **platform-independent**.
- Since IP packets of the same data stream may not take the same route, TCP was added to:
  - acknowledge receiptof IP packets
  - request retransmissionof lost packets
  - put back together the packet order
- TCP carries high overhead. UDP is used when the packet order isn’t that important, and when packet lost won’t completely corrupt the data stream.
- Error correction codescan be built into UDP.

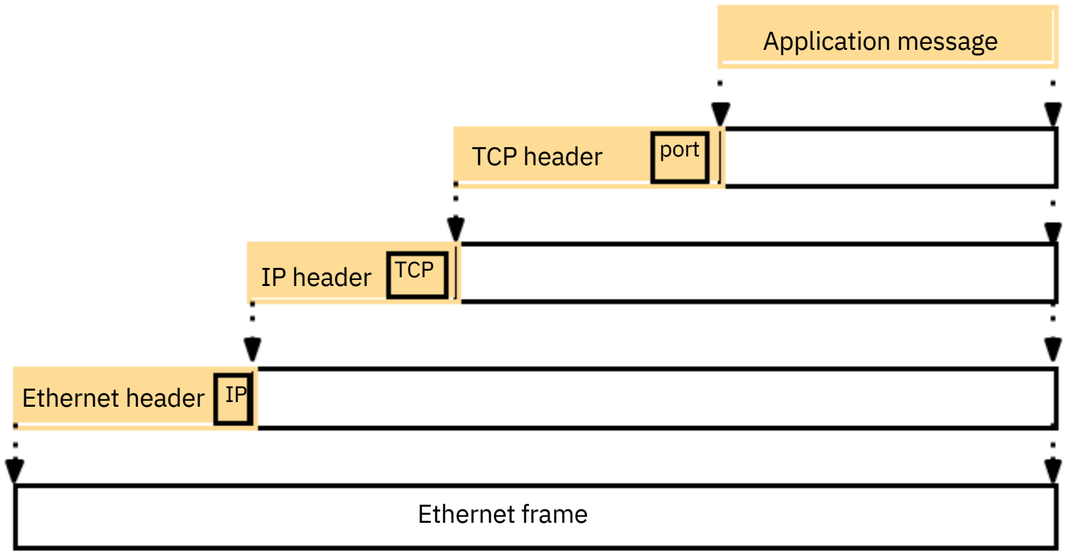
TCP/IP Layers



TCP/IP Features

- Encapsulation
- IP Addressing
  - IPv4 address structure
  - Address resolution
- IP Routing
- IPv6 addressing
- MobileIP
- DNS
- Firewall security

TCP/IP Encapsulation (Ethernet)



UDP Overview

- A one-shotnetwork service
- Also uses sockets, but destroyed after a UDP datagram is sent or received
- No error correction or retransmission
- Works best with small, independentpackets of information
- Good for application scenarios such as:
  - Multimedia streaming
  - Network discovery services
  - Control services

    Basic information services

What is Network Programming?

- Network programs: Programs that use network **in some way** to do their work.
  - Send/receive data across a network
  - Provide/invoke services over a network
  - Mobile computing through wireless networks
  - Cloud/edge computing
- Network programmingis the discipline of designing and implementing network programs.

The Key Players

- Server (Service provider)
  - a program that provides data and/or services to other programs
  - a computer that manages a network resource
    - file server, Web server, database server, mail server, …
- Client (Service consumer)
  - a program that relies on another program for some of its data or services
    - Web browser, email client, ...
- Protocols
  - an agreed-upon way of exchanging info and service requests between clients and servers

Why Network Programming?

- Sharing of information
  - stock quote, airline schedule, Lotto numbers, ...
- Parallel and distributed computing
  - SETI@HomeProject (Search for Extraterrestrial Intelligence at Home) (http://setiathome.ssl.berkeley.edu)
- Application services
  - client-server applications, ECommerce, chat room, multiplayer network games, ...
- Collaborative computing
  - desktop conferencing, webcast, group workflow, ...
  - peer-to-peer applications

Python Networking

- Python supports network programmingat two levels.
- With **low-level networking**, we can access sockets of underlying OS for both connection-orientedand connectionless communication.
- Python **networking libraries** provide higher-level access to specific application-level network protocols, such as FTP, HTTP, and so on.