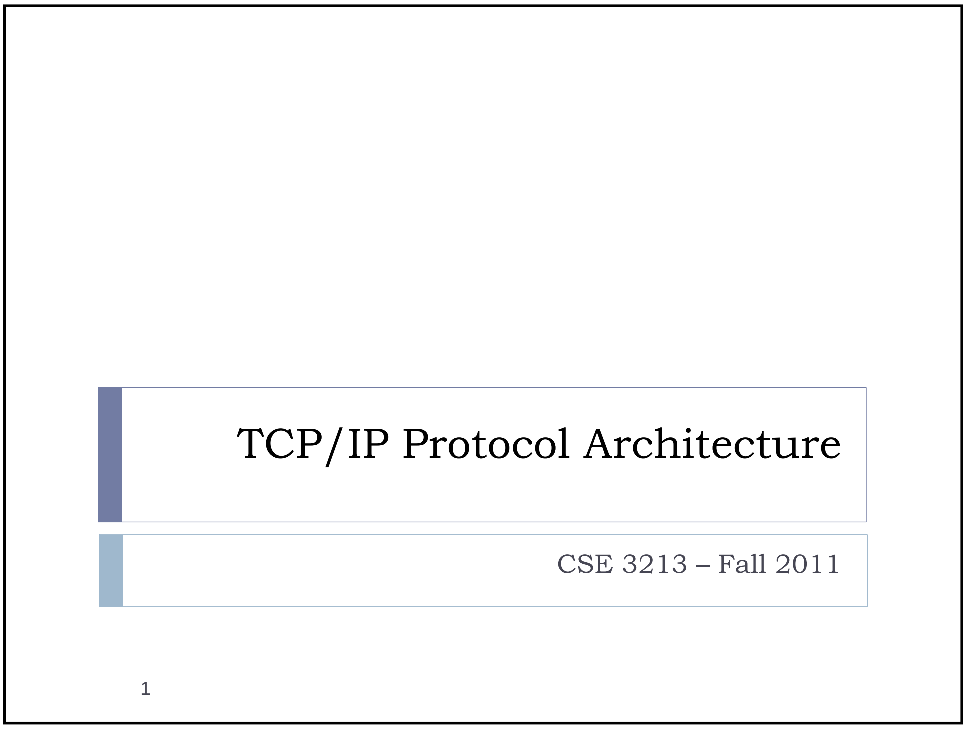
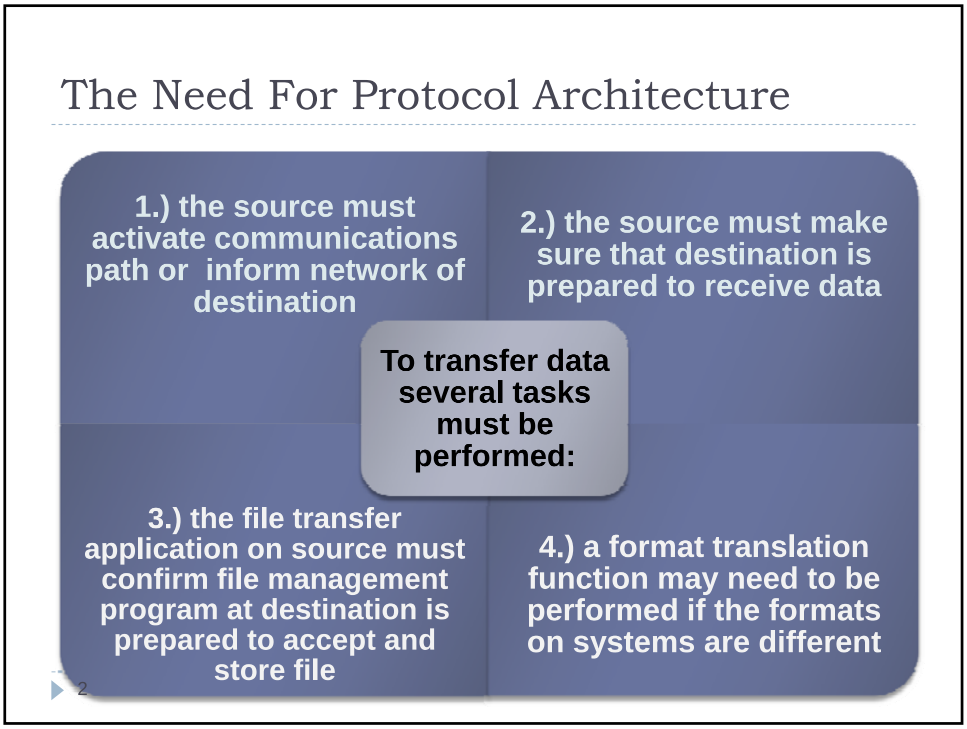


TCP/IP Protocol Architecture

CSE 3213 – Fall 2011

1



The Need For Protocol Architecture

To transfer data several tasks must be performed:

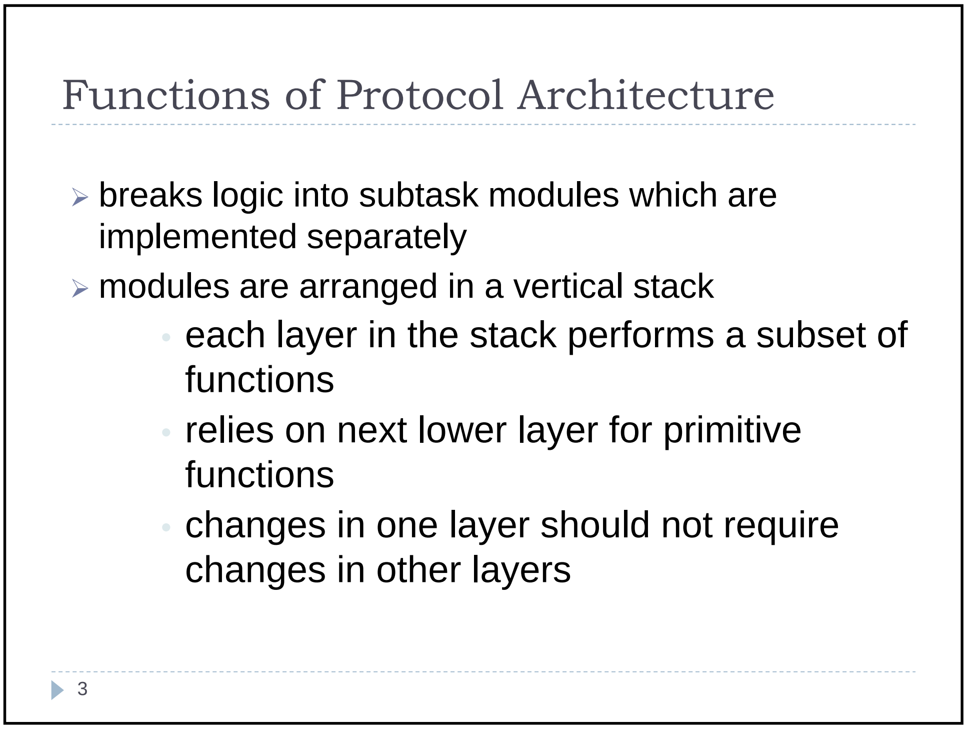
1.) the source must activate communications path or inform network of destination

2.) the source must make sure that destination is prepared to receive data

3.) the file transfer application on source must confirm file management program at destination is prepared to accept and store file

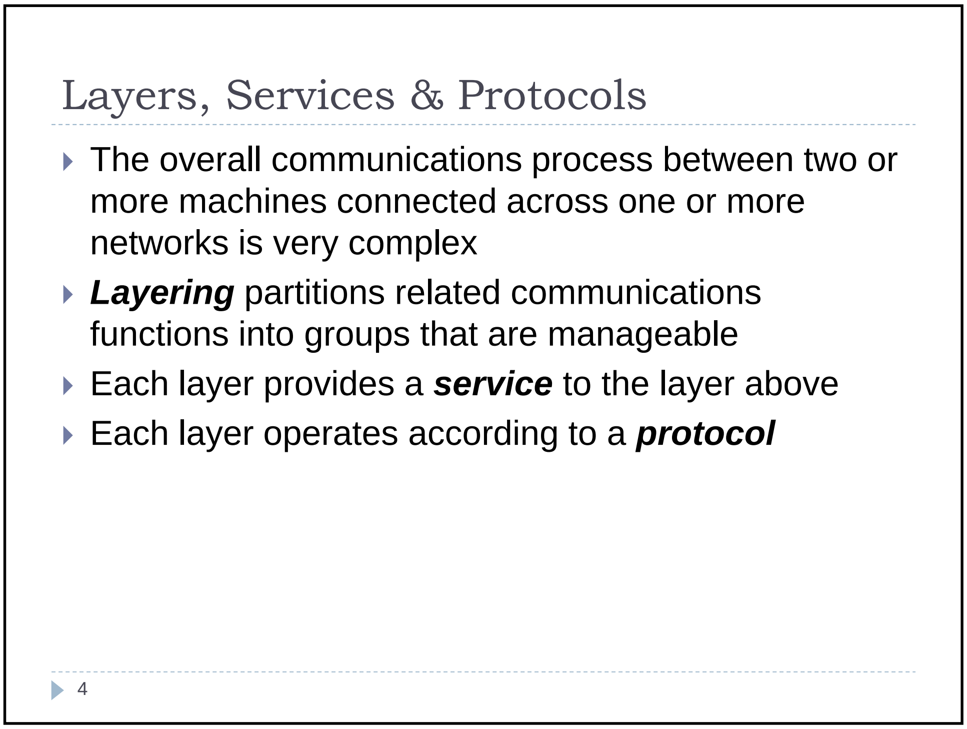
4.) a format translation function may need to be performed if the formats on systems are different

2



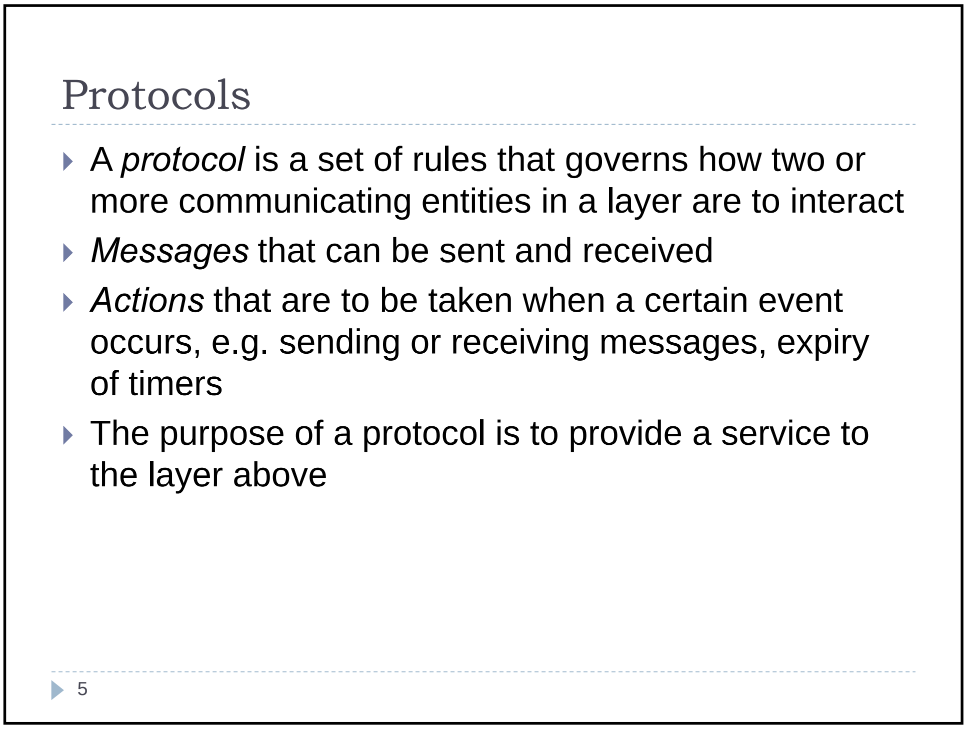
Functions of Protocol Architecture

- breaks logic into subtask modules which are implemented separately
- modules are arranged in a vertical stack
    - each layer in the stack performs a subset of functions
    - relies on next lower layer for primitive functions
    - changes in one layer should not require changes in other layers



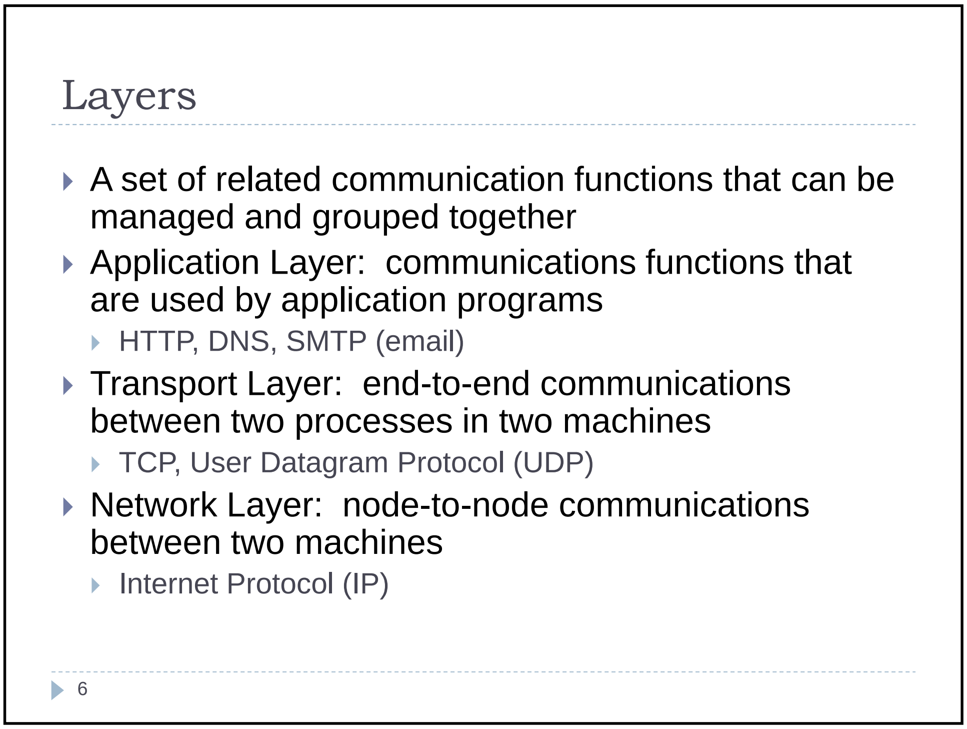
Layers, Services & Protocols

- The overall communications process between two or more machines connected across one or more networks is very complex
- ***Layering*** partitions related communications functions into groups that are manageable
- Each layer provides a ***service*** to the layer above
- Each layer operates according to a ***protocol***



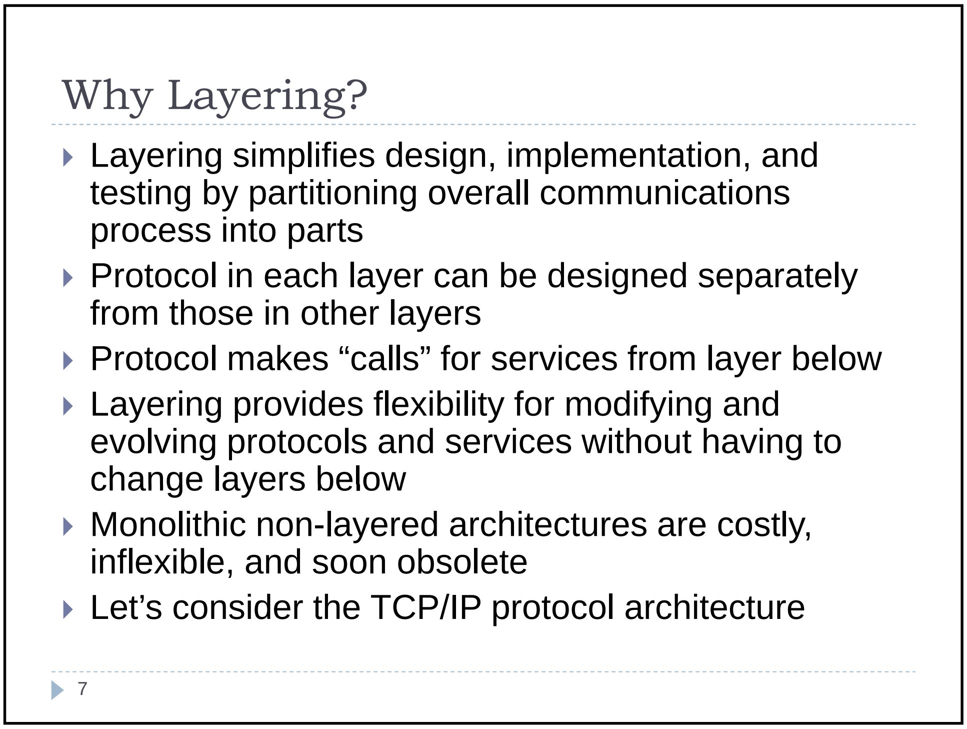
Protocols

- A *protocol* is a set of rules that governs how two or more communicating entities in a layer are to interact
- *Messages* that can be sent and received
- *Actions* that are to be taken when a certain event occurs, e.g. sending or receiving messages, expiry of timers
- The purpose of a protocol is to provide a service to the layer above



Layers

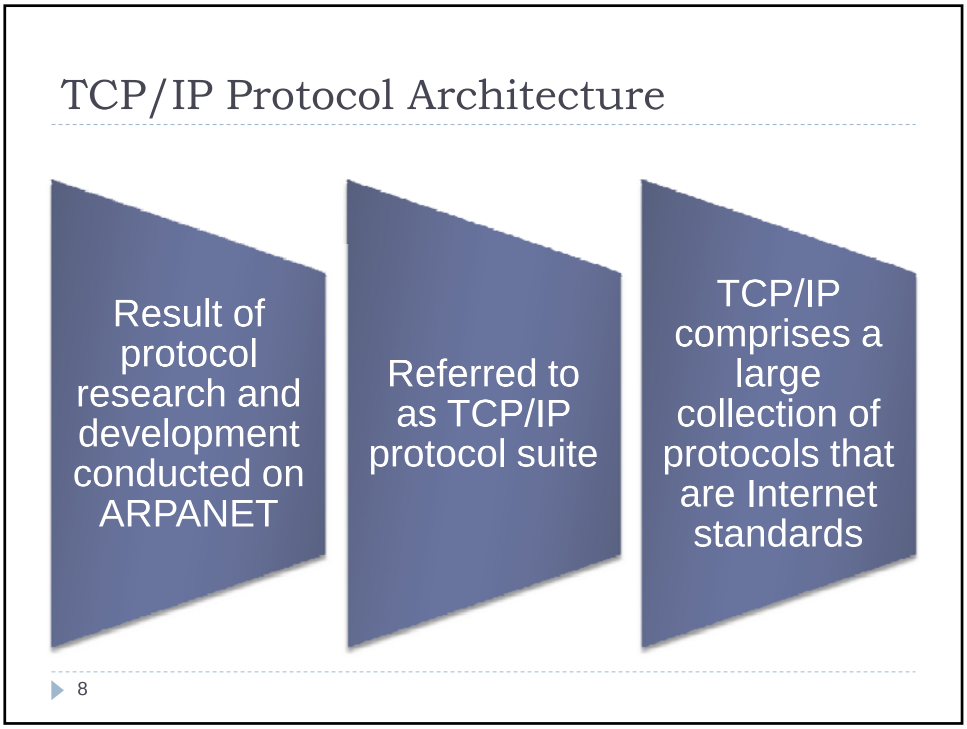
- A set of related communication functions that can be managed and grouped together
- Application Layer: communications functions that are used by application programs
  - HTTP, DNS, SMTP (email)
- Transport Layer: end-to-end communications between two processes in two machines
  - TCP, User Datagram Protocol (UDP)
- Network Layer: node-to-node communications between two machines
  - Internet Protocol (IP)



Why Layering?

- Layering simplifies design, implementation, and testing by partitioning overall communications process into parts
- Protocol in each layer can be designed separately from those in other layers
- Protocol makes “calls” for services from layer below
- Layering provides flexibility for modifying and evolving protocols and services without having to change layers below
- Monolithic non-layered architectures are costly, inflexible, and soon obsolete
- Let’s consider the TCP/IP protocol architecture

7



TCP/IP Protocol Architecture

Result of protocol research and development conducted on ARPANET

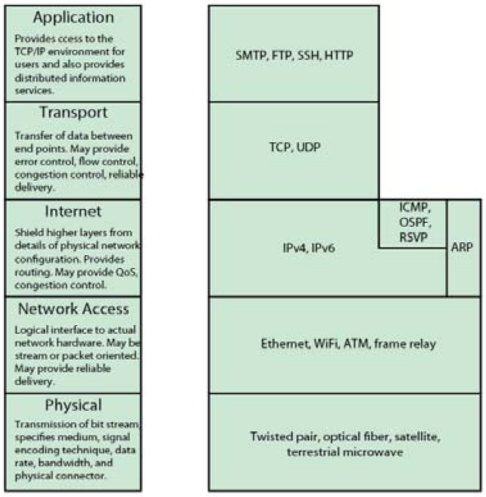
Referred to as TCP/IP protocol suite

TCP/IP comprises a large collection of protocols that are Internet standards

8

TCP/IP Layers and Example Protocols

also called
Data Link



Application
Provides ccess to the TCP/IP environment for users and also provides distributed information services.

Transport
Transfer of data between end points. May provide error control, flow control, congestion control, reliable delivery.

Internet
Shield higher layers from details of physical network configuration. Provides routing. May provide QoS, congestion control.

Network Access
Logical interface to actual network hardware. May be stream or packet oriented. May provide reliable delivery.

Physical
Transmission of bit stream; specifies medium, signal encoding technique, data rate, bandwidth, and physical connector.

SMTP, FTP, SSH, HTTP

TCP, UDP

IPv4, IPv6

ICMP, OSPF, RSVP

ARP

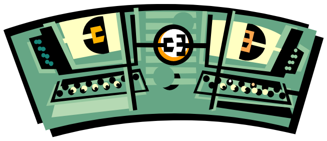
Ethernet, WiFi, ATM, frame relay

Twisted pair, optical fiber, satellite, terrestrial microwave

9

Physical Layer

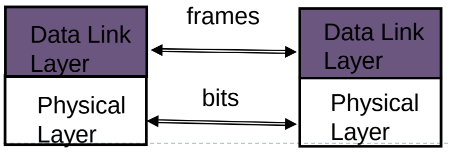
- Transfers *bits* across a link
- Concerned with issues like:
  - characteristics of transmission medium (optical fiber, twisted-pair cable, coaxial cable, wireless)
  - nature of the signals (modulation, signal strength, voltage levels, bit times)
  - data rates



10

Data Link (Network Access) Layer

- Transfers *frames* across *direct* connections
- Groups bits into frames
- Detection of <u>bit errors</u>; <u>retransmission</u> of frames
- Activation, maintenance and deactivation of data link connections
- <u>Medium access control</u> for LANs
- Flow control

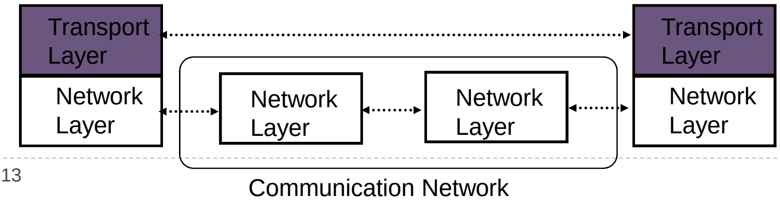


Network Layer

- Transfers *packets* across multiple links and/or multiple networks
- Addressing must scale to large networks
- Nodes *jointly* execute routing algorithm to determine paths across the network
- Forwarding transfers packet across a node
- Congestion control to deal with traffic surges
- Connection setup, maintenance, and teardown when connection-based

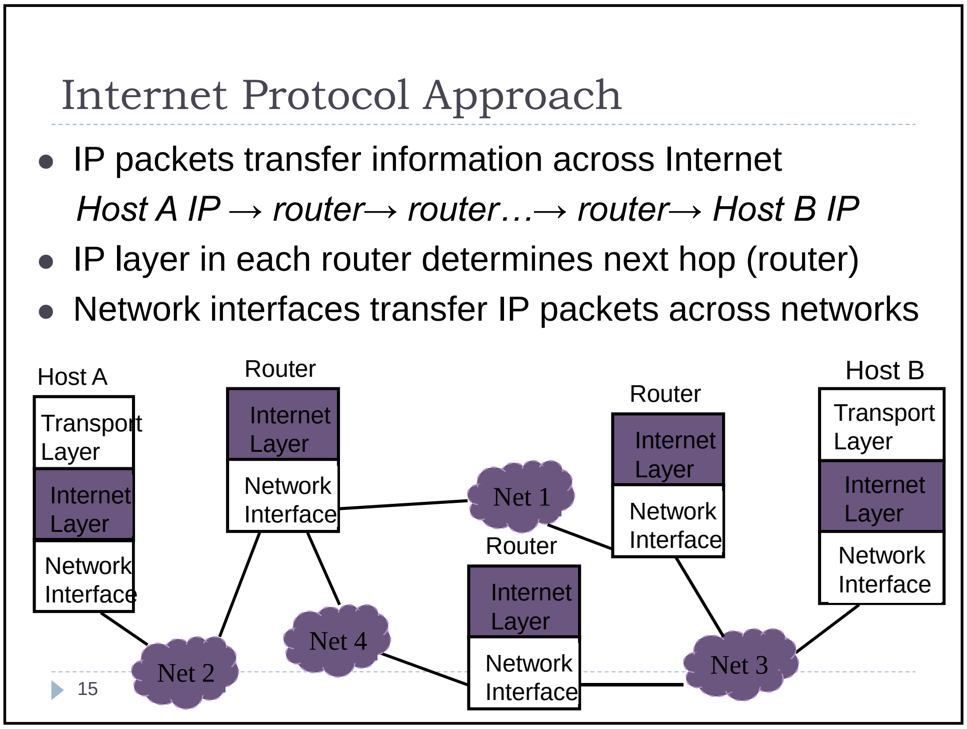
Transport Layer

- Transfers data end-to-end from process in a machine to process in another machine
- Reliable stream transfer or quick-and-simple single-block transfer
- Port numbers enable multiplexing
- Message segmentation and reassembly
- Connection setup, maintenance, and release



Application Layer

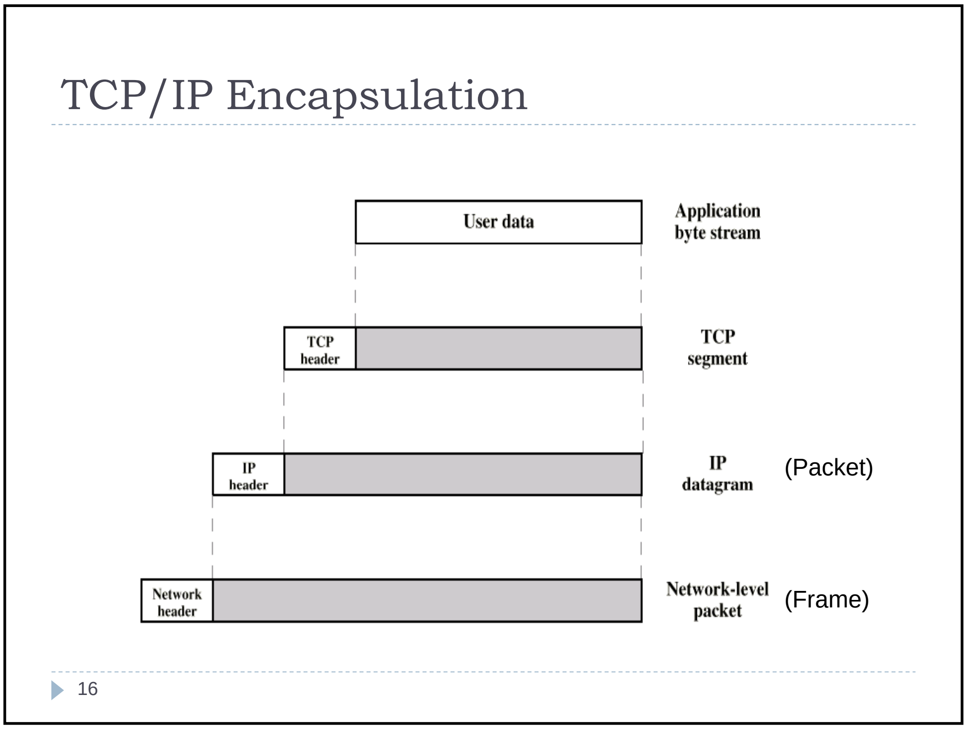
- Contains the logic needed to support various user applications (HTTP, FTP, SSH)
- A separate module is needed for each type of application.



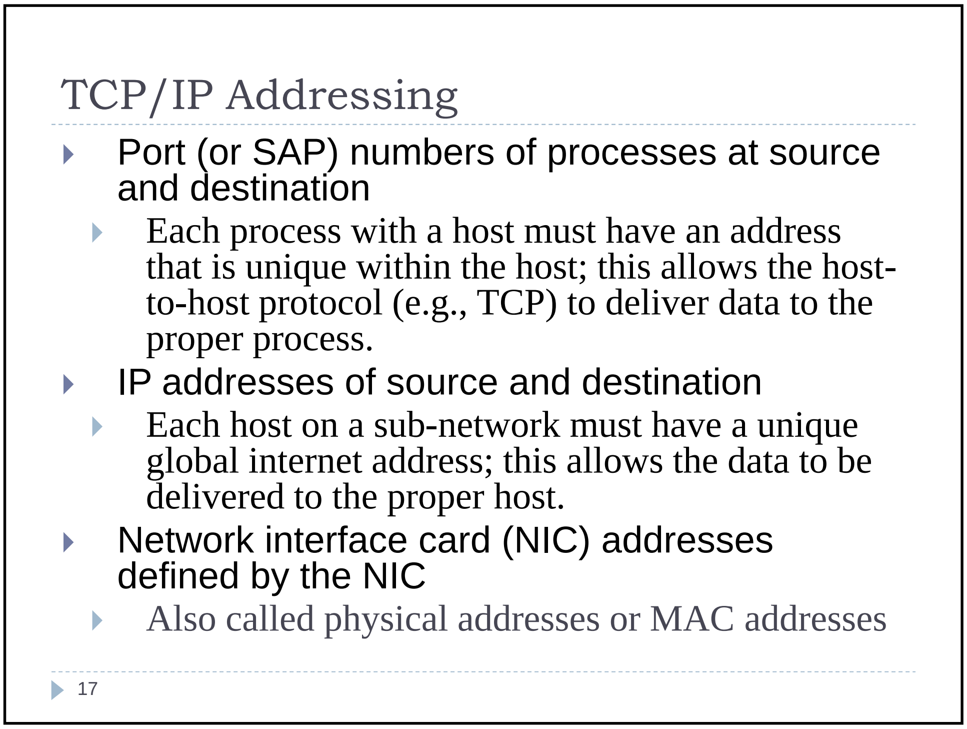
Internet Protocol Approach

- IP packets transfer information across Internet

  Host A IP → router→ router…→ router→ Host B IP
- IP layer in each router determines next hop (router)
- Network interfaces transfer IP packets across networks

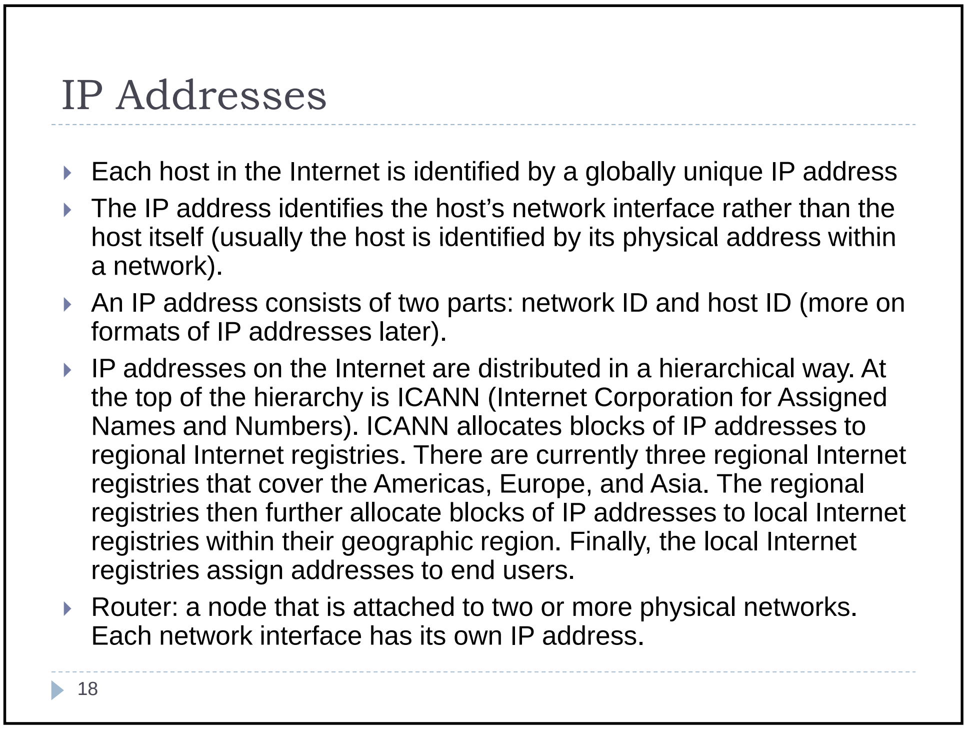


TCP/IP Encapsulation



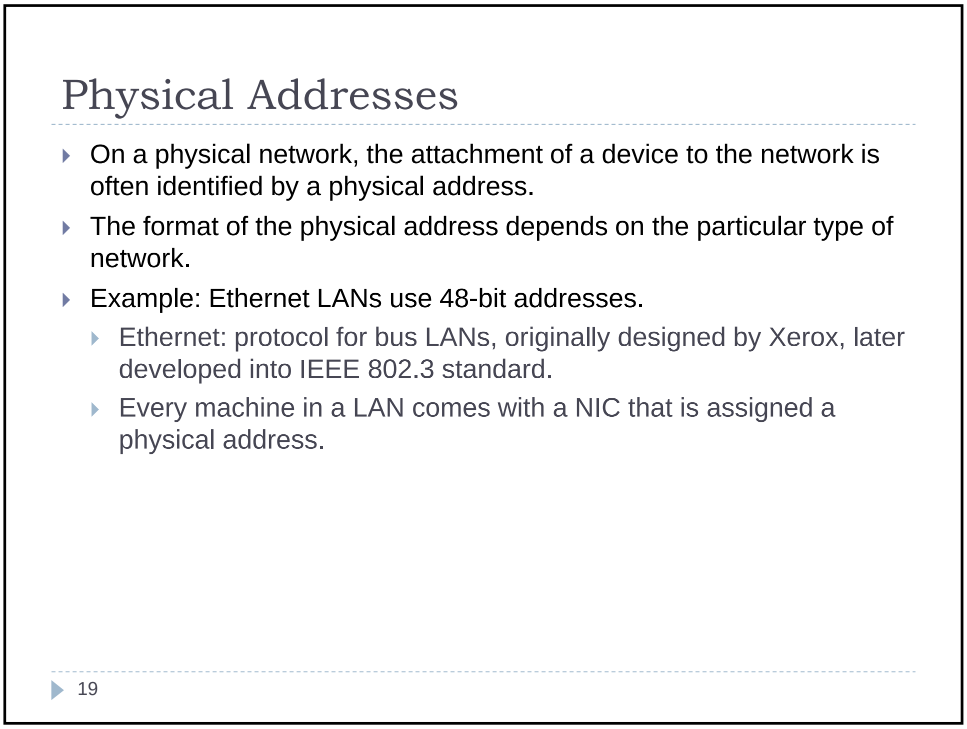
TCP/IP Addressing

- Port (or SAP) numbers of processes at source and destination
  - Each process with a host must have an address that is unique within the host; this allows the host-to-host protocol (e.g., TCP) to deliver data to the proper process.
- IP addresses of source and destination
  - Each host on a sub-network must have a unique global internet address; this allows the data to be delivered to the proper host.
- Network interface card (NIC) addresses defined by the NIC
  - Also called physical addresses or MAC addresses



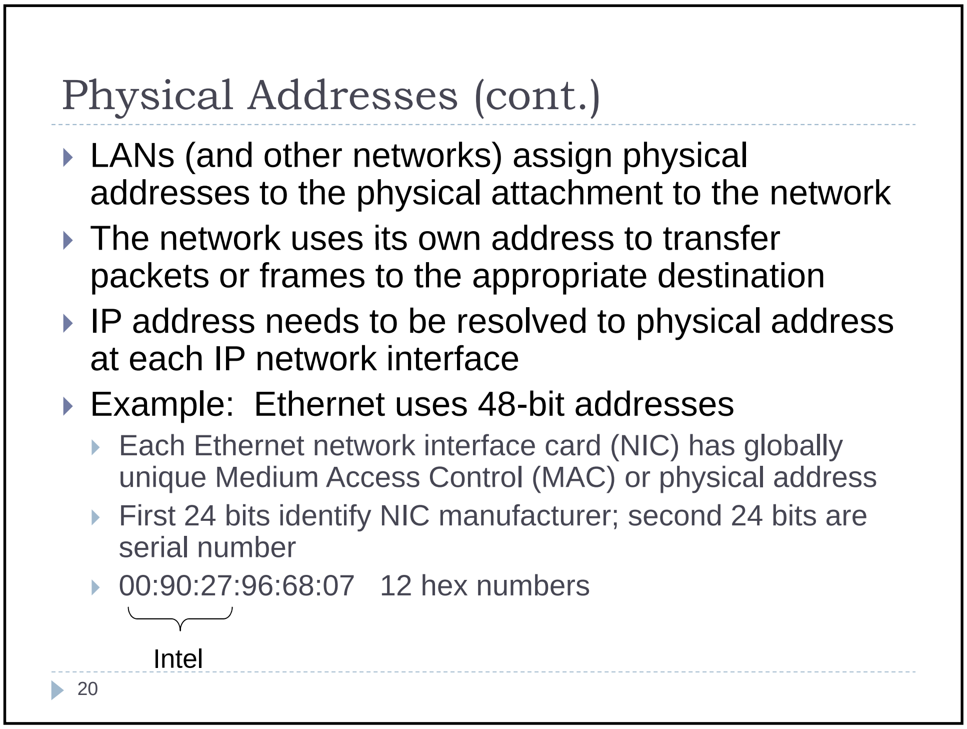
IP Addresses

- Each host in the Internet is identified by a globally unique IP address
- The IP address identifies the host's network interface rather than the host itself (usually the host is identified by its physical address within a network).
- An IP address consists of two parts: network ID and host ID (more on formats of IP addresses later).
- IP addresses on the Internet are distributed in a hierarchical way. At the top of the hierarchy is ICANN (Internet Corporation for Assigned Names and Numbers). ICANN allocates blocks of IP addresses to regional Internet registries. There are currently three regional Internet registries that cover the Americas, Europe, and Asia. The regional registries then further allocate blocks of IP addresses to local Internet registries within their geographic region. Finally, the local Internet registries assign addresses to end users.
- Router: a node that is attached to two or more physical networks. Each network interface has its own IP address.



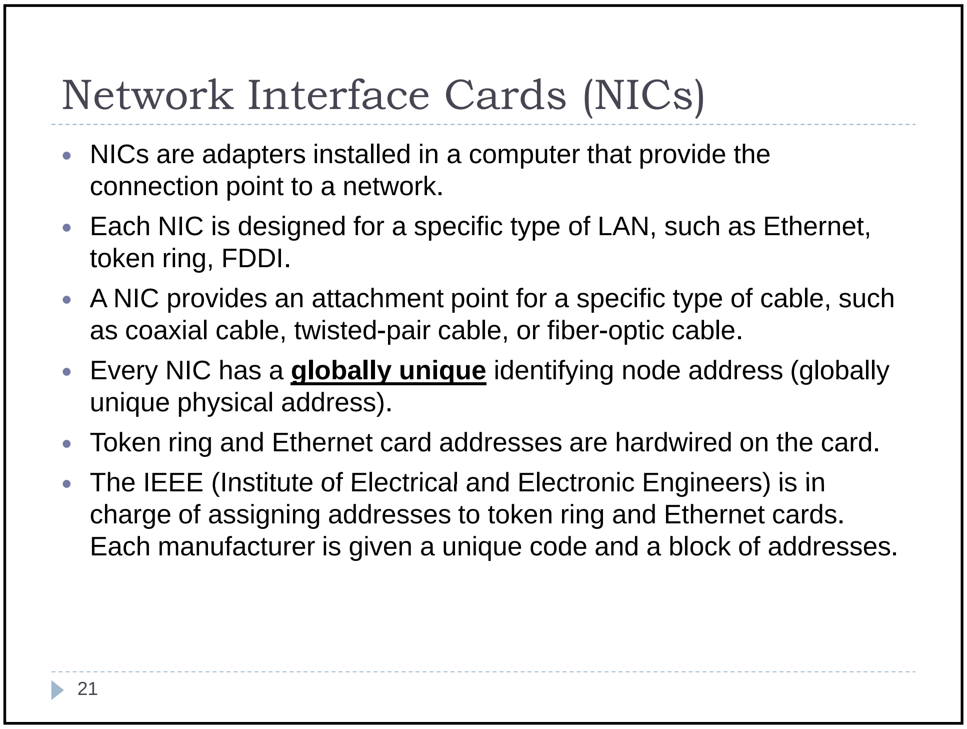
Physical Addresses

- On a physical network, the attachment of a device to the network is often identified by a physical address.
- The format of the physical address depends on the particular type of network.
- Example: Ethernet LANs use 48-bit addresses.
  - Ethernet: protocol for bus LANs, originally designed by Xerox, later developed into IEEE 802.3 standard.
  - Every machine in a LAN comes with a NIC that is assigned a physical address.



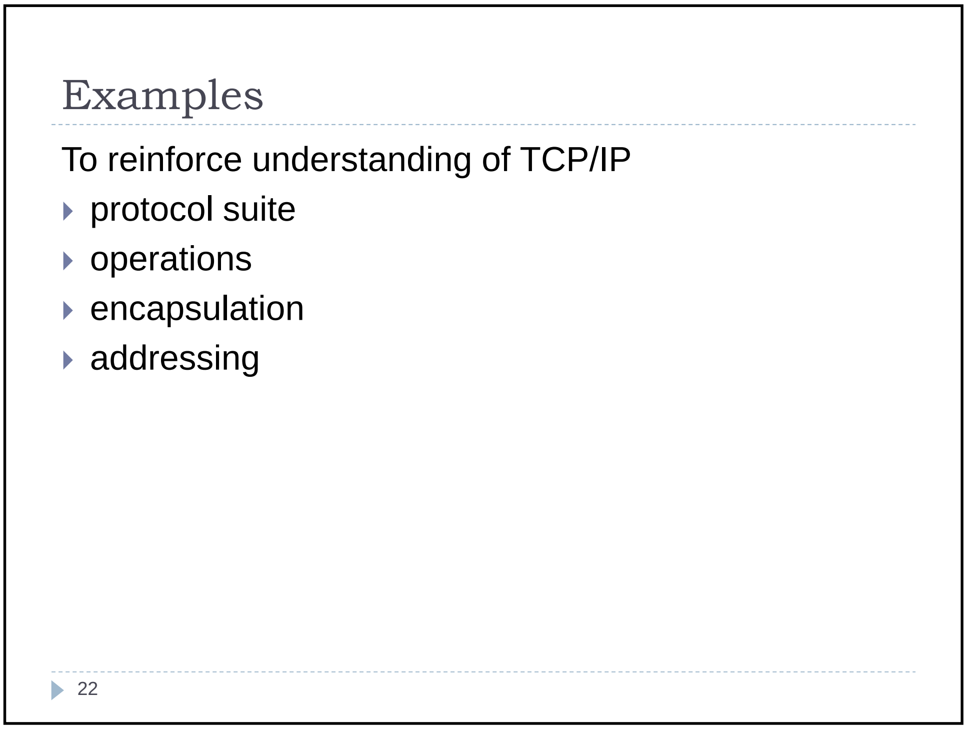
Physical Addresses (cont.)

- LANs (and other networks) assign physical addresses to the physical attachment to the network
- The network uses its own address to transfer packets or frames to the appropriate destination
- IP address needs to be resolved to physical address at each IP network interface
- Example: Ethernet uses 48-bit addresses
  - Each Ethernet network interface card (NIC) has globally unique Medium Access Control (MAC) or physical address
  - First 24 bits identify NIC manufacturer; second 24 bits are serial number
  - $\underbrace{00:90:27}_{\text{Intel}}:96:68:07$ 12 hex numbers



Network Interface Cards (NICs)

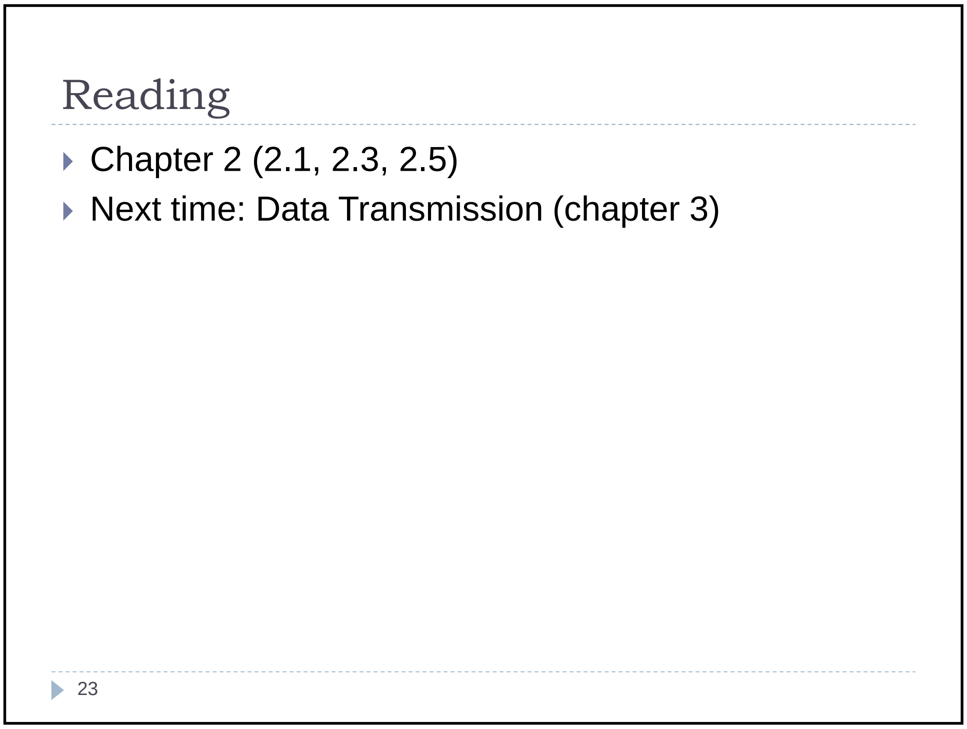
- NICs are adapters installed in a computer that provide the connection point to a network.
- Each NIC is designed for a specific type of LAN, such as Ethernet, token ring, FDDI.
- A NIC provides an attachment point for a specific type of cable, such as coaxial cable, twisted-pair cable, or fiber-optic cable.
- Every NIC has a **globally unique** identifying node address (globally unique physical address).
- Token ring and Ethernet card addresses are hardwired on the card.
- The IEEE (Institute of Electrical and Electronic Engineers) is in charge of assigning addresses to token ring and Ethernet cards. Each manufacturer is given a unique code and a block of addresses.



Examples

To reinforce understanding of TCP/IP

- protocol suite
- operations
- encapsulation
- addressing



Reading

- Chapter 2 (2.1, 2.3, 2.5)
- Next time: Data Transmission (chapter 3)