William Stallings
Data and Computer Communications

Chapter 2

Protocols and Architecture

Characteristics of Protocols

- Direct or indirect
- Monolithic or structured
- Symmetric or asymmetric
- Standard or nonstandard

Direct or Indirect

- Direct
  - Systems share a point to point link or
  - Systems share a multi-point link
  - Data can pass without intervening active agent
- Indirect
  - Switched networks or
  - Internetworks or internets
  - Data transfer depend on other entities

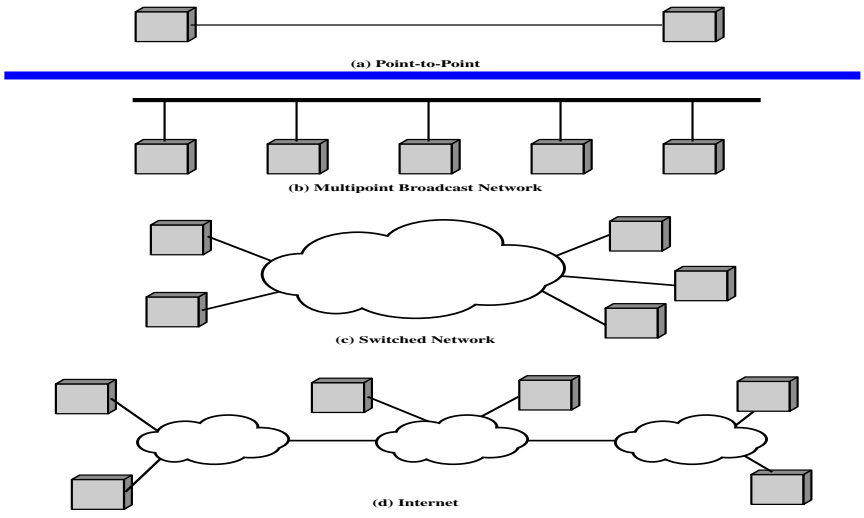


Figure 2.1 Means of Connection of Communicating Systems

Monolithic or Structured

- Communication is a complex task
- Too complex for single unit
- Structured design breaks down problem into smaller units
- A set of protocols with hierarchical or layered structure
- Higher-level entities rely on lower-level entities to exchange data

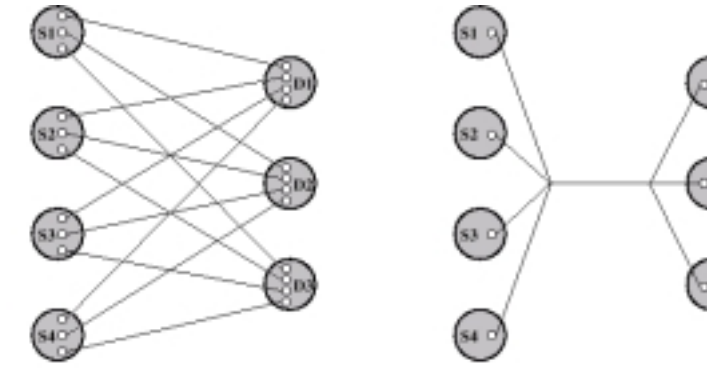
Symmetric or Asymmetric

- Symmetric
  - Communication between peer entities
- Asymmetric
  - May be dictated by the logic of an exchange e.g. client/server
  - Desire to keep one of the entities or systems simple
  - A computer that polls and selects a number of terminals

Standard or Nonstandard

- Nonstandard protocols built for specific computers and tasks
- K sources and L receivers leads to K*L protocols and 2*K*L implementations
- If common protocol used, K + L implementations needed

Use of Standard Protocols



(a) Without standards: 12 different protocols; 24 protocol implementations

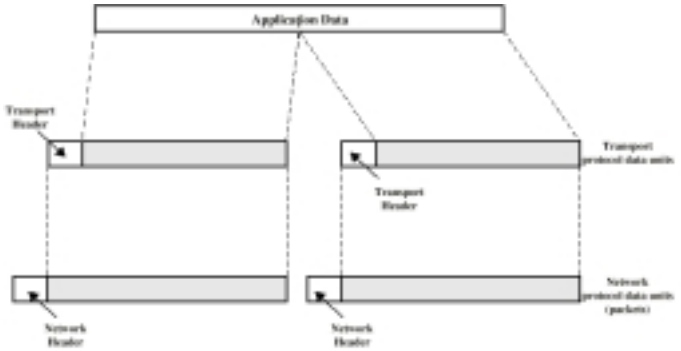
(a) With standards: 1 protocol; 7 implementations

Basic Functions of Protocols

- Encapsulation
- Segmentation and reassembly
- Connection control
- Ordered delivery
- Flow control
- Error control
- Addressing
- Multiplexing
- Transmission services

Encapsulation

- Addition of control information to data
  - Address information
  - Error-detecting code
  - Protocol control



Segmentation (Fragmentation)

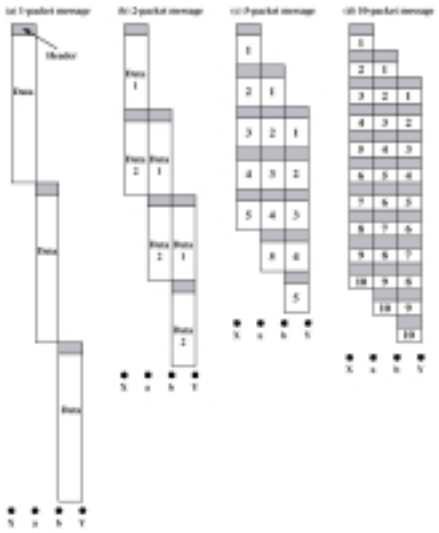
- Data blocks are of bounded size
- Application layer messages may be large
- Network packets may be smaller
- Splitting larger blocks into smaller ones is segmentation (or fragmentation in TCP/IP)
  - ATM blocks (cells) are 53 octets (bytes) long
  - Ethernet blocks (frames) are up to 1526 octets long

Advantages & Disadvantages of Segmentation

- Advantages
  - More efficient error control
  - More equitable access to network facilities with shorter delays
  - Smaller buffers needed
  - More efficient for checkpoints and restart/recovery
- Disadvantages
  - Overheads
  - Increased interrupts at receiver
  - More processing time

Effect of Packet Size on Transmission Time

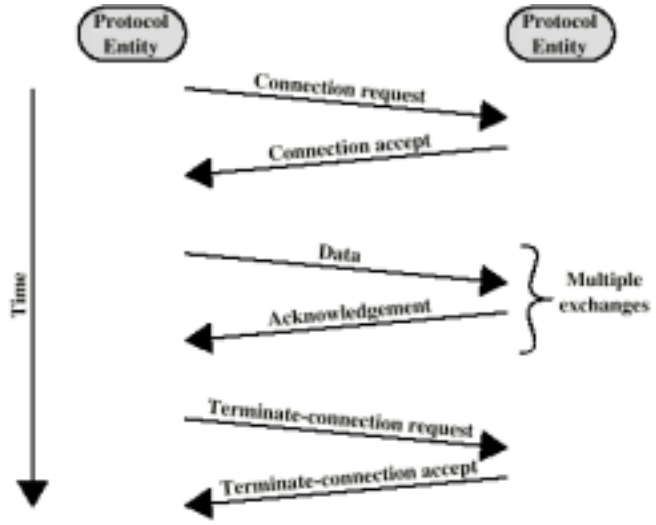
- Message has 40 bytes
- Packet header is 3 bytes
- If packet size is 43 bytes
  - one packet
  - 3*43=192 bytes
- If packet size is 23 bytes
  - two packets
  - 4*23=92 bytes
- If packet size is 11 bytes
  - five packets
  - 7*11=77 bytes
- If packet size is 7 bytes
  - ten packets
  - 12*7=84 bytes



Connection Control

- Data transfer is either connectionless or connection-oriented
- Connectionless: each PDU is treated independently of other PDUs, e.g. use of Datagram
- Connection-oriented (e.g. virtual circuit)
  - Connection Establishment
  - Data transfer
  - Connection termination
- Connection interruption and recovery
- In connection establishment, protocols negotiate syntax, semantics, and timing
- Protocols may allow certain optional features that must be agreed upon by negotiation

Connection Oriented Data Transfer



Datagram

- Each packet treated independently
- Packets can take any practical route
- Packets may arrive out of order
- Packets may go missing
- Up to receiver to re-order packets and recover from missing packets

Virtual Circuit

- Preplanned route established before any packets sent
- Call request and call accept packets establish connection (handshake)
- Each packet contains a virtual circuit identifier instead of destination address
- No routing decisions required for each packet
- Clear request to drop circuit
- Not a dedicated path

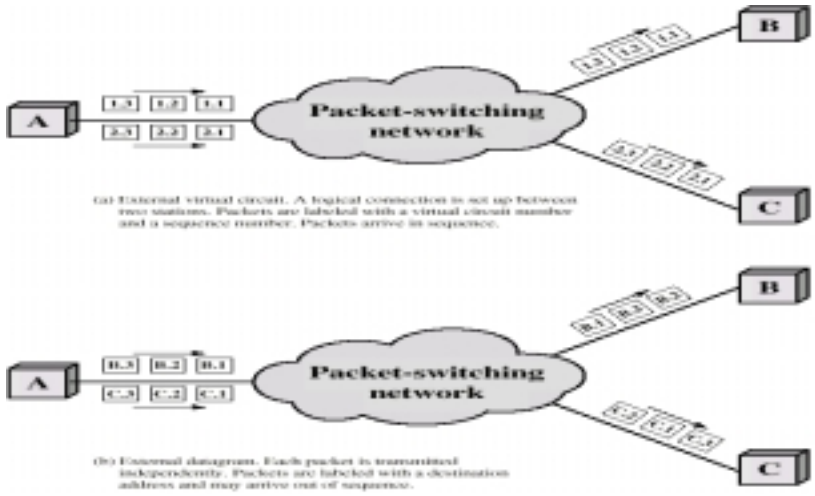
Virtual Circuits vs. Datagram

- Virtual circuits
  - Network can provide sequencing and error control
  - Packets are forwarded more quickly
    - No routing decisions to make
  - Less reliable
    - Loss of a node looses all circuits through that node
- Datagram
  - No call setup phase
    - Better if few packets
  - More flexible
    - Routing can be used to avoid congested parts of the network

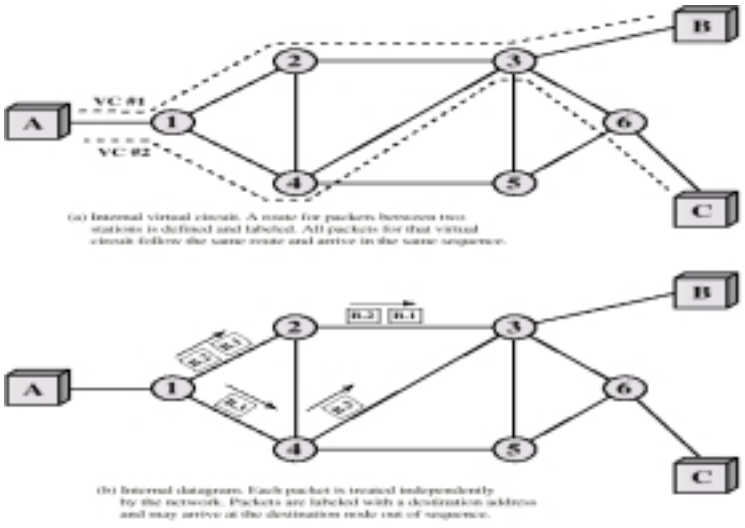
Packet Switching External and Internal Operation

- Packet switching - datagrams or virtual circuits
- Interface between station and network node
  - Connection oriented
    - Station requests logical connection (virtual circuit)
    - All packets identified as belonging to that connection & sequentially numbered
    - Network delivers packets in sequence
    - External virtual circuit service
    - e.g. X.25
    - Different from internal virtual circuit operation
  - Connectionless
    - Packets handled independently
    - External datagram service
    - Different from internal datagram operation

External Virtual Circuit and Datagram Operation



Internal Virtual Circuit and Datagram Operation



(a) Internal virtual circuit. A route for packets between two stations is defined and labelled. All packets for that virtual circuit follow the same route and arrive in the same sequence.

(b) Internal datagram. Each packet is treated independently by the network. Packets are labeled with a destination address and may arrive at the destination node out of sequence.

Connection Control

- Data transfer uses sequencing
- Both entities number PDUs and keep track of both incoming and outgoing numbers
- Sequence numbers used for
  - Ordered delivery
  - Flow control
  - Error control

Ordered Delivery

- PDUs may traverse different paths through network
- PDUs may arrive out of order
- Sequentially number PDUs to allow for ordering
- Problem if sequence numbers repeat after overflow
- Have maximum sequence number to be twice maximum number of outstanding PDUs

Flow Control

- Done by receiving entity
- Limit amount or rate of data
- Stop and wait: each PDU must be acknowledged before the next can be sent
- Credit systems: allow a number of PDUs to be sent without acknowledgment
  - Sliding window
- Flow control is implemented in several protocols

Error Control

- Guard against data loss or damage
- Error detection
  - Sender inserts error detecting code
  - Receiver checks this code
  - If OK, acknowledge
  - If error, discard packet
- Retransmission
  - If no acknowledge in given time, re-transmit
- Performed at various levels

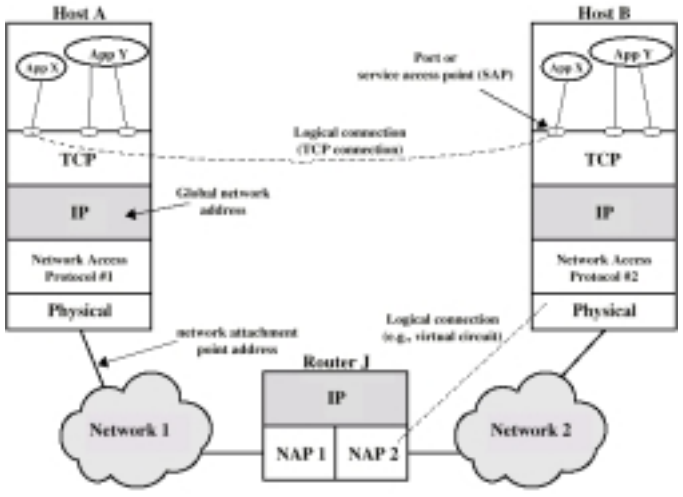
Addressing Issues

- Addressing level
- Addressing scope
- Connection identifiers
- Addressing mode

Addressing level

- Level in architecture at which entity is named
- Unique address for each end system (computer) and intermediate system (router)
- Network level address
  - IP or internet address (TCP/IP)
  - Network service access point or NSAP (OSI)
- Process within the system
  - Port number (TCP/IP)
  - Service access point or SAP (OSI)

Address Concepts



Addressing Scope

- Characteristics of a global address
  - Global nonambiguity
    - Global address identifies unique system
    - There is only one system with address X
  - Global applicability
    - It is possible at any system (any address) to identify any other system (address) by the global address of the other system
    - Address X identifies that system from anywhere on the network
- Each network must maintain a unique address for each device in the network (network attachment pint address)
  - MAC address on IEEE 802 networks
  - X.25 host address

Connection Identifiers

- Connection oriented data transfer (virtual circuits)
- Allocate a connection identifier during the transfer phase
  - Reduced overhead as connection identifiers are shorter than global addresses
    - In X.25 protocol, connection identifier is a 12-bit virtual circuit number
  - Routing is defined and identified by connection identifier eliminating routing for each PDU
  - Entities may want multiple connections - multiplexing
  - State information
    - Enables flow control and error control using sequence numbers

Addressing Mode

- Usually an address refers to a single system
  - Unicast address
  - Sent to one machine or person
- May address all entities within a domain
  - Broadcast
  - Sent to all machines or users
- May address a subset of the entities in a domain
  - Multicast
  - Sent to some machines or a group of users

IP Addresses - Class A

- 32 bit global internet address
- Network part and host part
- Class A
  - Start with binary 0
  - Network address 7 bits
  - Host address 24 bits
  - 2^7 = 128 class A addresses
  - Range 1.x.x.x to 126.x.x.x
  - All 0 reserved
  - 01111111 (127) reserved for loopback
  - All allocated

IP Addresses - Class B

- Start 10
- Network address 14 bits
- Host address 16 bits
- 2^{14} = 16,384 class B addresses
- Range 128.x.x.x to 191.x.x.x
- All allocated

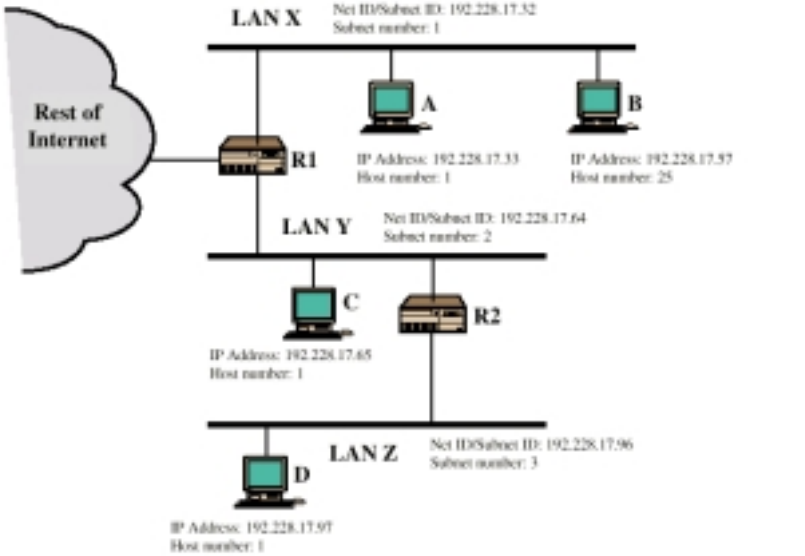
IP Addresses - Class C

- Start 110
- Network address 21 bits
- Host address 8 bits
- 2^{21} = 2,097,152 class C addresses
- Range 192.x.x.x to 223.x.x.x
- Nearly all allocated
  - See IPv6

Subnets and Subnet Masks

- Allow arbitrary complexity of internetworked LANs within organization
- Insulate overall internet from growth of network numbers and routing complexity
- To rest of internet site looks like a single network
- Each LAN assigned subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- Subnet mask indicates which bits are subnet number and which are host number

Routing Using Subnets



Multiplexing

- Combining several signals for transmission on shared medium
- Supporting multiple connections on one machine
- Mapping of multiple connections at one level to a single connection at another
  - Carrying a number of connections on one fiber optic cable
  - Aggregating or bonding ISDN lines to gain bandwidth

Multiplexing

- Upward Multiplexing
  - Multiple higher-level connections are multiplexed on a single lower-level connection
  - Connecting your PC to ISP for multiple applications, including web, email, ftp, telnet
- Downward Multiplexing
  - Split a single higher-level connection over a number of lower-level connections
  - Useful for reliability, performance, or efficiency

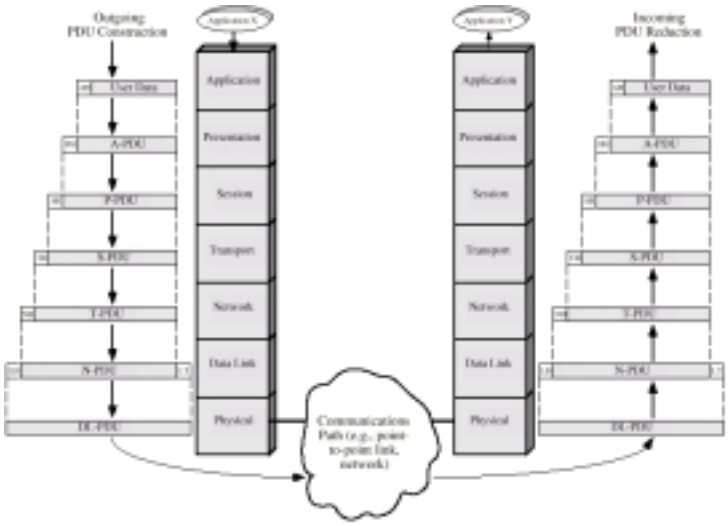
Transmission Services

- Priority
  - e.g. control messages
  - Assigned on a message basis on connection basis
- Quality of service
  - Minimum acceptable throughput
  - Maximum acceptable delay
- Security
  - Access restrictions

OSI - The Model

- A seven layer model
- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers

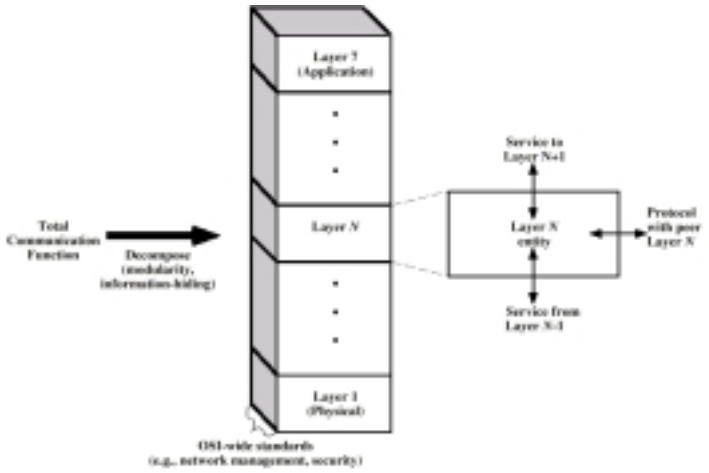
The OSI Environment



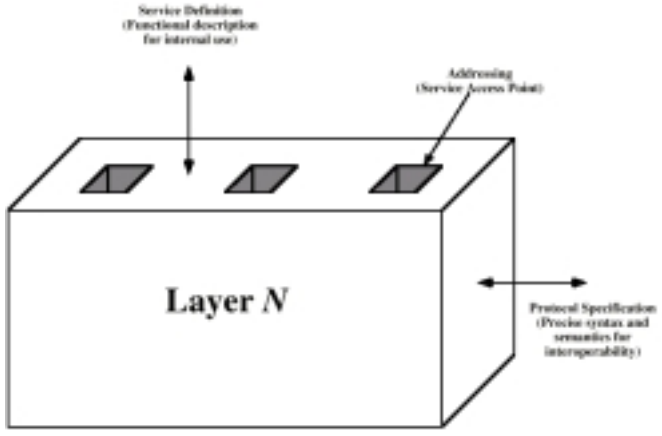
OSI as Framework for Standardization

- Defines functions at each layer and facilitates standards-making process.
- Standards at each layer can be developed independently and simultaneously.
- Changes in standards in one layer need not affect other layers
  - Well defined boundaries (interface) between layers

OSI as Framework for Standardization



Layer Specific Standards



Elements of Standardization

- Protocol specification
  - Operates between two systems on same layer
  - May involve different operating systems
  - Protocol specification must be precise
    - Format of data units
    - Semantics of all fields
    - allowable sequence of PDUs
- Service definition
  - Functional description of what is provided, not how it is provided
- Addressing
  - Referenced by SAPs
  - Allows multiplexing from higher layer

Service Primitives and Parameters

- Services between adjacent layers expressed in terms of primitives and parameters
- Primitive specifies the function to be performed
- Parameters used to pass data and control information
- Four types of primitives
  - Request
  - Indication
  - Response
  - Confirm

Service Primitives

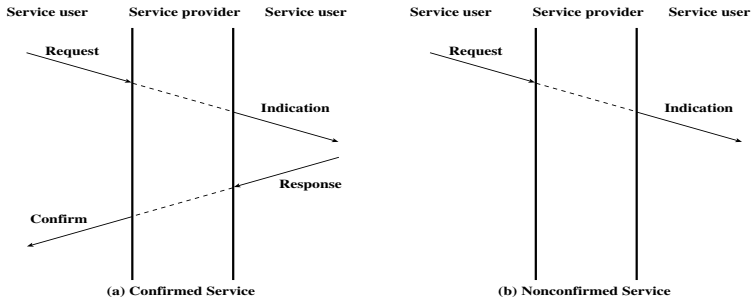


Figure 2.9 Time Sequence Diagrams for Service Primitives

OSI Layers - Physical

- Physical interface between devices
  - Mechanical
    - Physical properties of interface to transmission medium
    - Specifications of pluggable connector
  - Electrical
    - Representation of bits in terms of voltage levels
    - Data transmission rates
  - Functional
    - Functions of individual circuits of physical interface
  - Procedural
    - Sequence of events by which bit streams are exchanged
- Examples: EIA-232-F, portions of ISDN and LAN standards

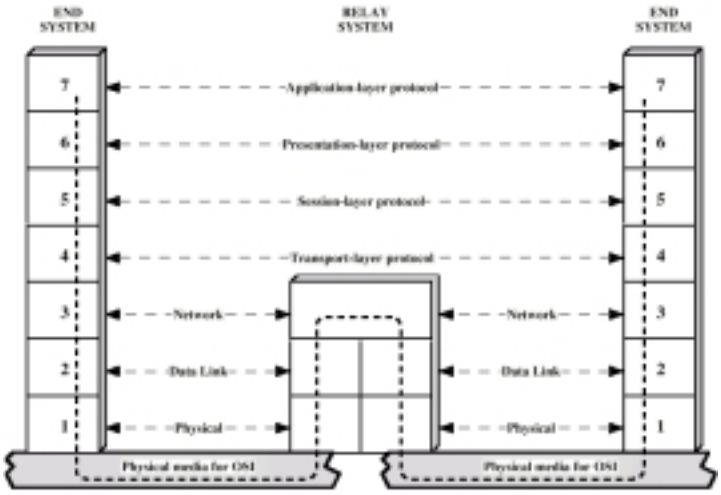
OSI Layers – Data Link

- Makes physical link reliable through error detection and control
- Activates, maintains and deactivates link
- Higher layers may assume error free transmission
- Communication through a number of data links require higher layers to perform some error control
- Examples: High-level Data link control (HDLC)

OSI Layers - Network

- Transfers information across communications network performing switching & routing
- Hides data transmission and switching technologies
- Not needed on direct links
- Highest layer in a network node
- System interacts with network
  - Specification of destination address
  - Request for network services like priority
- Examples: packet level of X.25 standard

Use of a Relay



OSI Layers - Transport

- Mechanisms for exchange of data between end systems
- Ensures data delivered error free, in sequence, no losses, no duplicates
- May optimize the use of network services
- Provides quality of service based on acceptable error rates, maximum delay, priority, security
- Size and complexity depend on reliability of underlying layers
- Examples: connection-oriented TCP (transmission control protocol), connectionless UDP (user datagram protocol)

OSI Layers - Session

- Control of dialogues between applications
- Dialogue discipline
  - Full duplex or half duplex
- Grouping
  - Mark data to define groups of data
- Recovery
  - Checkpoint to allow retransmission of all data since last checkpoint due to failure

OSI Layers – Presentation & Application

- Presentation
  - Data formats and coding
  - Defines syntax used between application entities
  - Provides for selection and modification of representation used
  - Data compression and encryption
- Application
  - Interface between application programs and OSI environment

TCP/IP Protocol Suite

- Dominant commercial protocol architecture
- Specified and extensively used before OSI
- Developed by research funded US Department of Defense
- Used by the Internet

TCP/IP Approach

- Modular and hierarchical like the OSI model
- Descriptive in nature compared to prescriptive nature of OSI
  - OSI dictates that protocols in a layer perform certain functions
  - In TCP/IP, it is possible to have two protocols in same layer with different functionality
- Does not require strict use of all layers
  - Application level protocols may directly run on top of IP

TCP/IP Protocol Architecture

- Application Layer
  - Communication between processes or applications
- End to end or transport layer (TCP/UDP/...)
  - End to end transfer of data
  - May include reliability mechanism (TCP)
  - Hides detail of underlying network
  - Implemented in end systems only
- Internet Layer (IP)
  - Routing of data
  - Implemented in all end systems and routers

TCP/IP Protocol Architecture

- Network Layer
  - Logical interface between end system and network
- Physical Layer
  - Transmission medium
  - Signal rate and encoding

PDUs in TCP/IP

Operation of TCP and IP

- Two levels of addressing
  - Unique host address over global internet, used by IP
  - Unique process (port) address within host, used by TCP
- TCP header
  - Destination port: address to whom data to be delivered
  - Sequence number: used by destination TCP to reorder segments
  - Checksum: code to check error during transmission

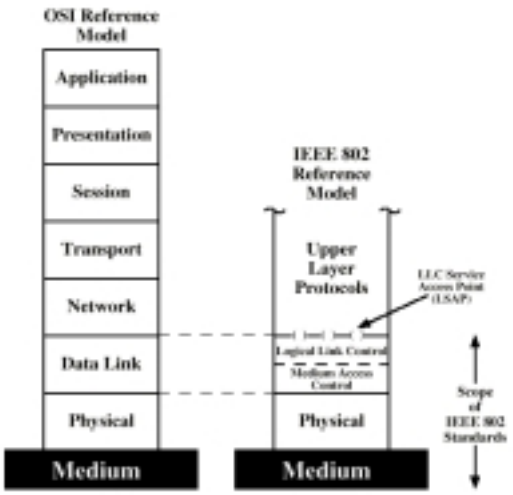
Operation of TCP and IP

- IP datagram
  - Created by adding IP header to each segment
  - Header includes destination host address
  - Presented to network access layer for transmission
- Packet or frame
  - Created by network access layer by adding its header
  - Header contains information for network to transfer data across it
    - Destination network address
    - Facilities request

LAN Protocol Architecture

- Lower layers of OSI model
- IEEE 802 reference model
- Physical
- Logical link control (LLC)
- Media access control (MAC)

IEEE 802 v OSI



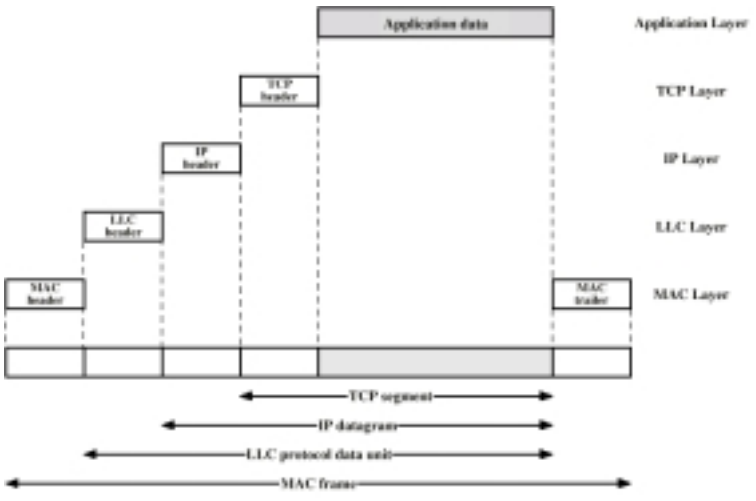
IEEE 802 Layers

- Physical
  - Encoding/decoding
  - Preamble generation/removal
  - Bit transmission/reception
  - Transmission medium and topology
- Logical Link Control
  - Interface to higher levels
  - Flow and error control

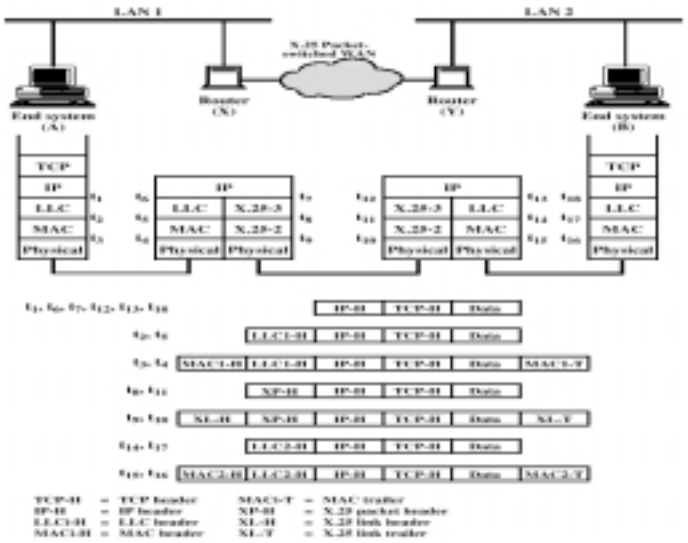
IEEE 802 Layers

- Media Access Control
  - Assembly of data into frame with address and error detection fields
  - Disassembly of frame
    - Address recognition
    - Error detection
  - Govern access to transmission medium
  - Not found in traditional layer 2 data link control
  - For the same LLC, several MAC options may be available

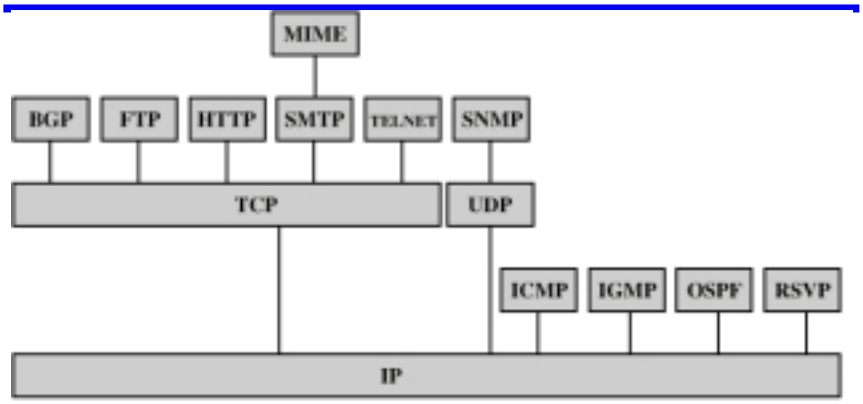
LAN Protocols in Context



IP Operation



Some Protocols in TCP/IP Suite



BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

Simple Mail Transfer Protocol (SMTP)

- Basic email utility
- Mechanism to transfer messages across hosts
- Features include mailing lists, return receipts, and forwarding
- Does not specify message creation; just transfer of message using TCP

File Transfer Protocol (FTP)

- Transfer files across systems under user commands
- Accommodate both text and binary files
- Upon request, sets up connection for exchange of control messages
- Upon approval, a second TCP opened for actual data transfer
  - Avoids overhead of control information
- After file transfer complete, control connection signals completion and accepts new commands

Telnet

- Remote login capability
- Designed to work with simple scroll-mode terminals
- Implemented in two modules
  - User telnet
    - Interacts with terminal I/O module to communicate with local terminal
    - Converts between characteristics of real terminals and network standards
  - Server telnet
    - Interacts with an application acting as a terminal handler
    - Makes remote terminal appear as local to application
- Traffic between user and server telnet carried on TCP

Internetworking Terms (1)

- Communications Network
  - Facility that provides data transfer service
- An internet
  - Collection of communications networks interconnected by bridges and/or routers
- The Internet - note upper case I
  - The global collection of thousands of individual machines and networks
- Intranet
  - Corporate internet operating within the organization
  - Uses Internet (TCP/IP and http)technology to deliver documents and resources

Internetworking Terms (2)

- End System (ES)
  - Device attached to one of the networks of an internet
  - Supports end-user applications or services
- Intermediate System (IS)
  - Device used to connect two networks
  - Permits communication between end systems attached to different networks

Internetworking Terms (3)

- Bridge
  - IS used to connect two LANs using similar LAN protocols
  - Address filter passing on packets to the required network only
  - OSI layer 2 (Data Link)
- Router
  - Connects two (possibly dissimilar) networks
  - Uses internet protocol present in each router and end system
  - OSI Layer 3 (Network)