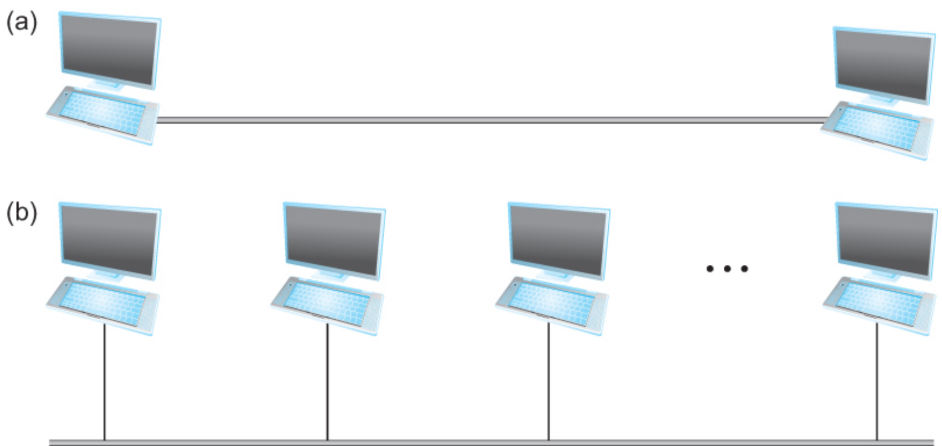
Computer Network Midterm Exam

- A total of 43 questions
  - 37 multiple-choice questions
    - 5 points each (185 points)
  - 6 short essay questions
    - 5 questions of 10 points and 1 of 15 points (65 points)
- For a total of 250 points (100%)
- Thursday February 9th
  - You have 1 hour and 30 minutes
  - No bathroom breaks
  - No questions during the midterm exam
    - If in doubt, make and state an assumption and answer the question based on the assumption
- Closed books, notes, phones, etc.

Computer Network

Midterm Study Guide Slides

Connectivity



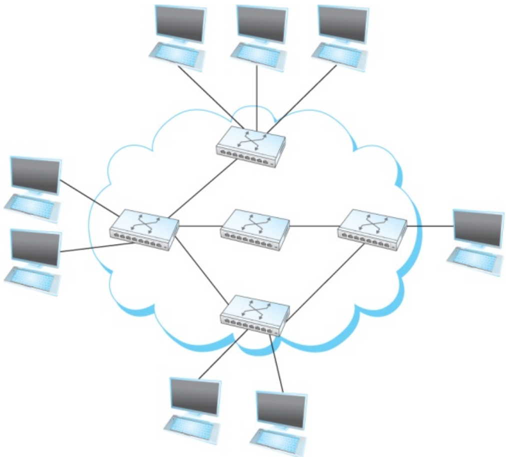
(a) Point-to-point

(b) Multiple access

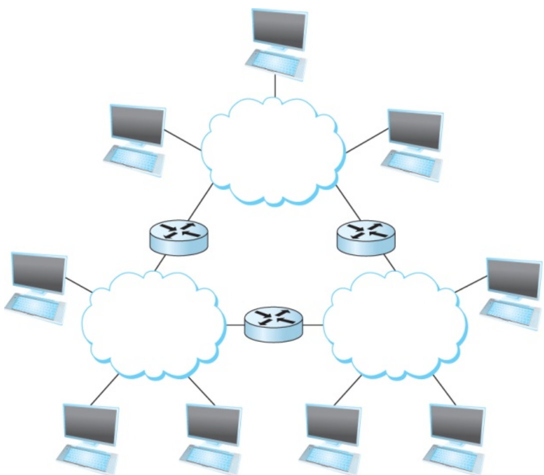
- Need to understand the following terminologies
  - Scale
  - Link
  - Nodes
  - Point-to-point
  - Multiple access
  - Switched Network
    - Circuit Switched
    - Packet Switched
  - Packet, message
  - Store-and-forward

Connectivity

(a)



(b)

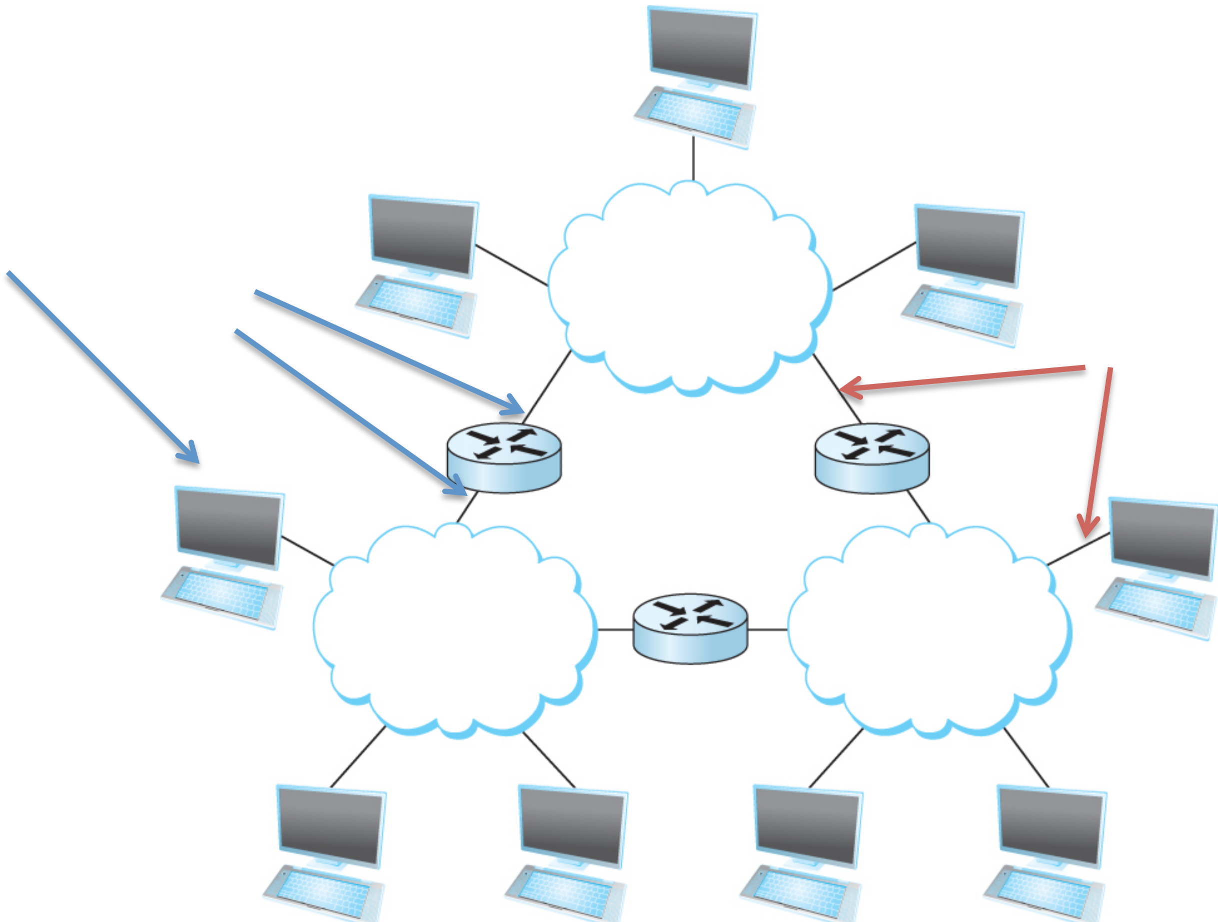


(a) A switched network

(b) Interconnection of networks

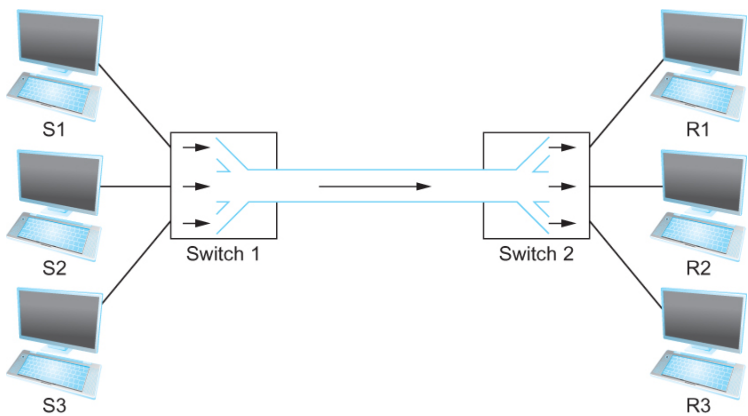
- Terminologies (contd.)
  - Hosts
  - Switches
  - Internetwork
  - Host-to-host connectivity
  - Address
  - Unicast/broadcast/multicast

Interconnection of Networks



In communication **networks**, a **node** (Latin nodus, 'knot') is either a connection point, a redistribution point (e.g. data communications equipment), or a communication endpoint (e.g. data terminal equipment).

Sharing Resources: Links & Nodes



Multiplexing multiple logical flows over a single physical link

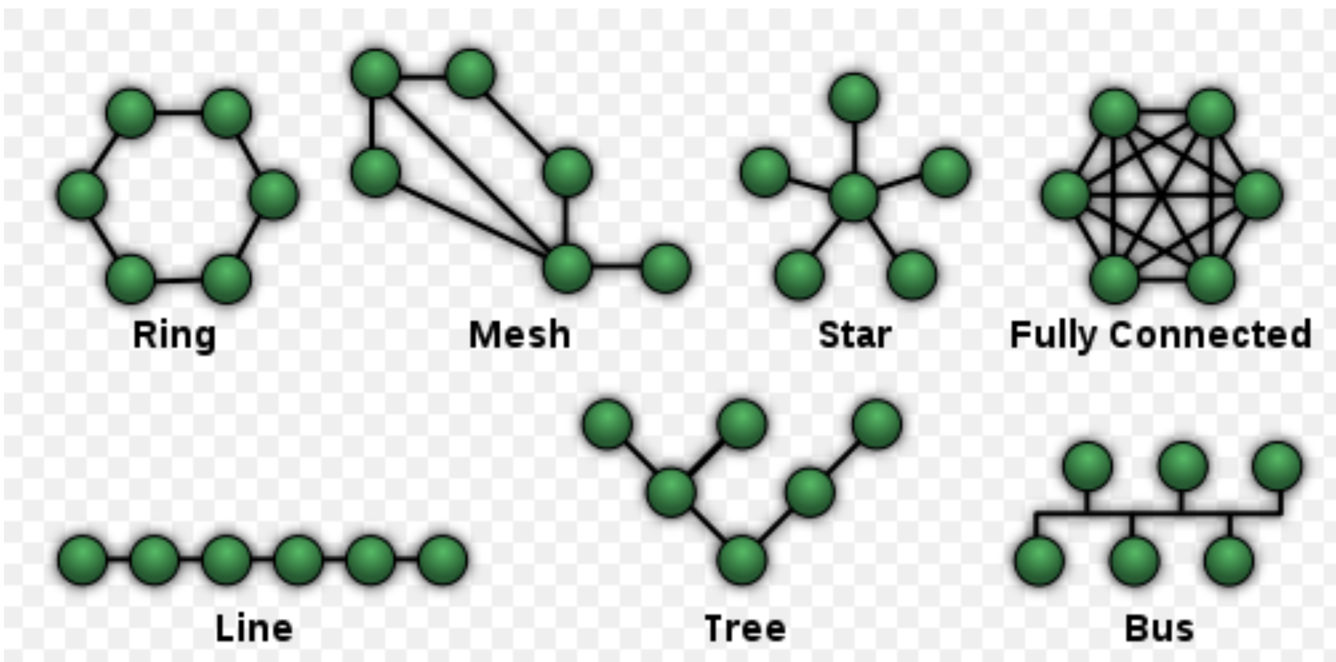
- How to share these resources?
  - Multiplexing
  - De-multiplexing
  - Time-division Multiplexing (TDM)
    - Time slots/data transmitted in predetermined slots
  - FDM: Frequency Division Multiplexing
  - Statistical Multiplexing
    - Modified TDM
    - Data is transmitted based on demand of each flow.

Categorizing Networks Based on Size

- LAN
  - Local area network (extends less than 1 km)
  - School, home, office buildding
- MAN
  - Metropolitan area network (spans tens of kilometers), somewhere between LAN and WAN
  - University campus, a network of a few LAN networks
- WAN
  - Wide area network (can be worldwide)
  - Across metropolitan, regional, national or international boundaries, using leased telecommunication lines
- SAN
  - Storage area network (formerly known as system area network)
    - Confined to a single room
    - Fiber channel is a common SAN technology used to connect high-performance computing systems to storage servers and data vaults
- DAN

Network Topology

- Is the arrangement of the various elements (links, nodes, etc.) of a computer network.
  - Point to point
  - Star (shared)
  - Token ring (shared)
  - Bus (shared)

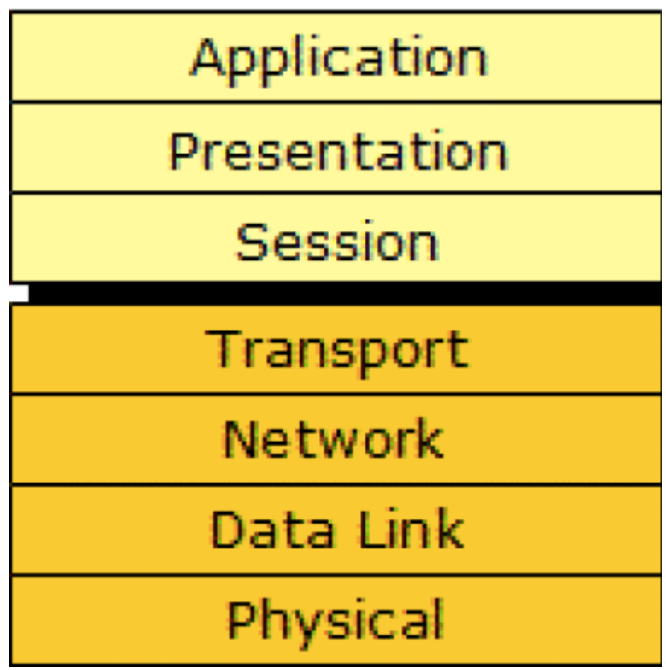


Network Architecture

- Abstraction – hiding of details behind a well-defined interface
- Use layering to provide abstraction
- Layering also provides nice features;
  1. Decomposes the problem of building a network into more manageable components
     - Each component solves one part of the problem
  2. Provides a more modular design

Network Architecture

- Not an easy task
- Network architectures can help
  - The OSI architecture (7 layers)
    - Open System Interconnection
  - The Internet architecture (5 layers)
    - TCP/IP



OSI Reference Model

- Open Systems Interconnect reference model provides general design guidance for data communication systems
  - to make sure all functions needed for communications are addressed
- Designed by International Standards Organization (ISO)
- 7 layer model of networking
- Each layer must be independent and only communicates to one above and below

OSI Reference Model

7 Application Network APIs (end hosts)

- Application/user wants to use network, either receive or send to network

6 Presentation Formatting (end hosts)

- What format is this data in?

5 Session Synchronization (end hosts)

- Sending and receiving nodes must be in synch, timing is important

4 Transport Packet (end hosts)

- Packet management (how many are they, did they all get there?)

3 Network Addressing/Routing (routers, gateways)

- IP addressing and routing packets all the way to the destination

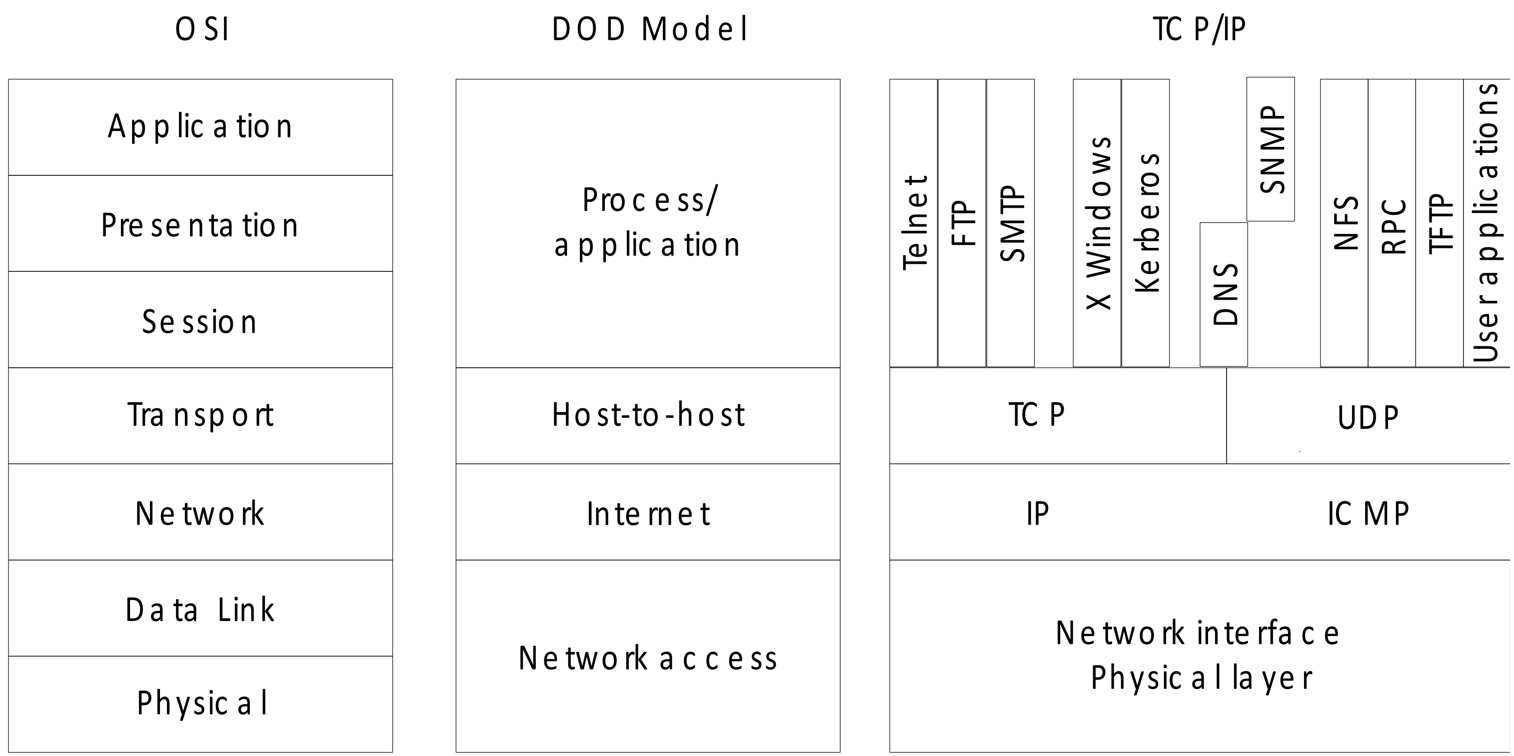
2 Data Link Data Frames (Bridges, switches)

- Data frame management (putting it into the appropriate envelope, Ethernet or token ring frame?)

1 Physical Hardware (hubs & repeaters, no brains))

- How is the network card (NIC) is connected to the cable, how are we physically connected to the network? Puts the data on the network wire

How TCP/IP Corresponds to OSI



What is a protocol as it relates to a communications network?

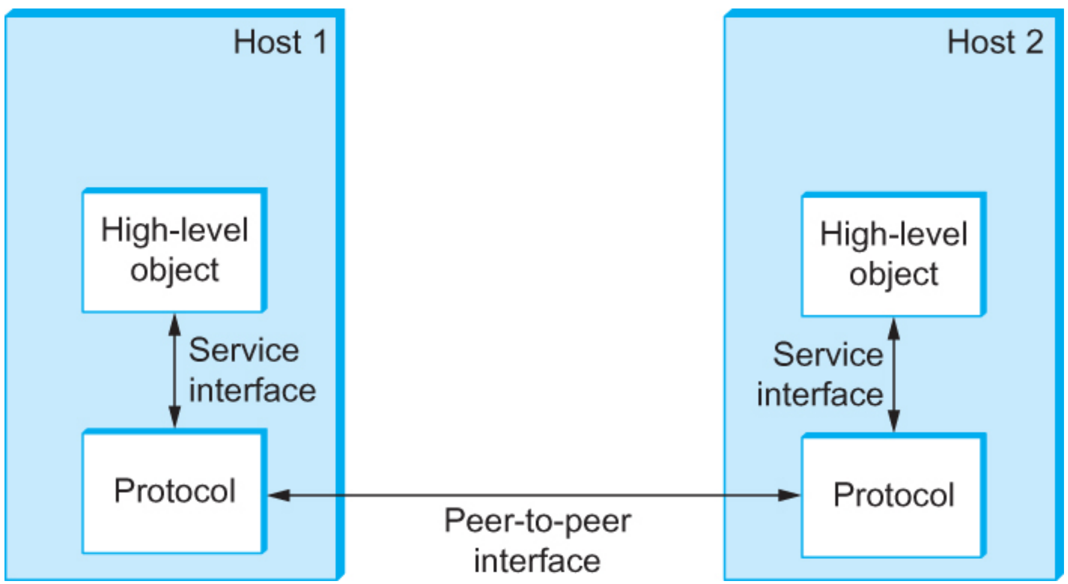
Protocol

- A set of rules and procedures used for communication
- Say you want to use USPS to send a letter to a friend:
  - Use an envelop
  - Write the destination address
    - Put it in a specific location on the envelop
    - Use a specific format
  - Put a return address
  - Put a stamp
  - Get it on to the USPS network
    - Post office
    - Mail man

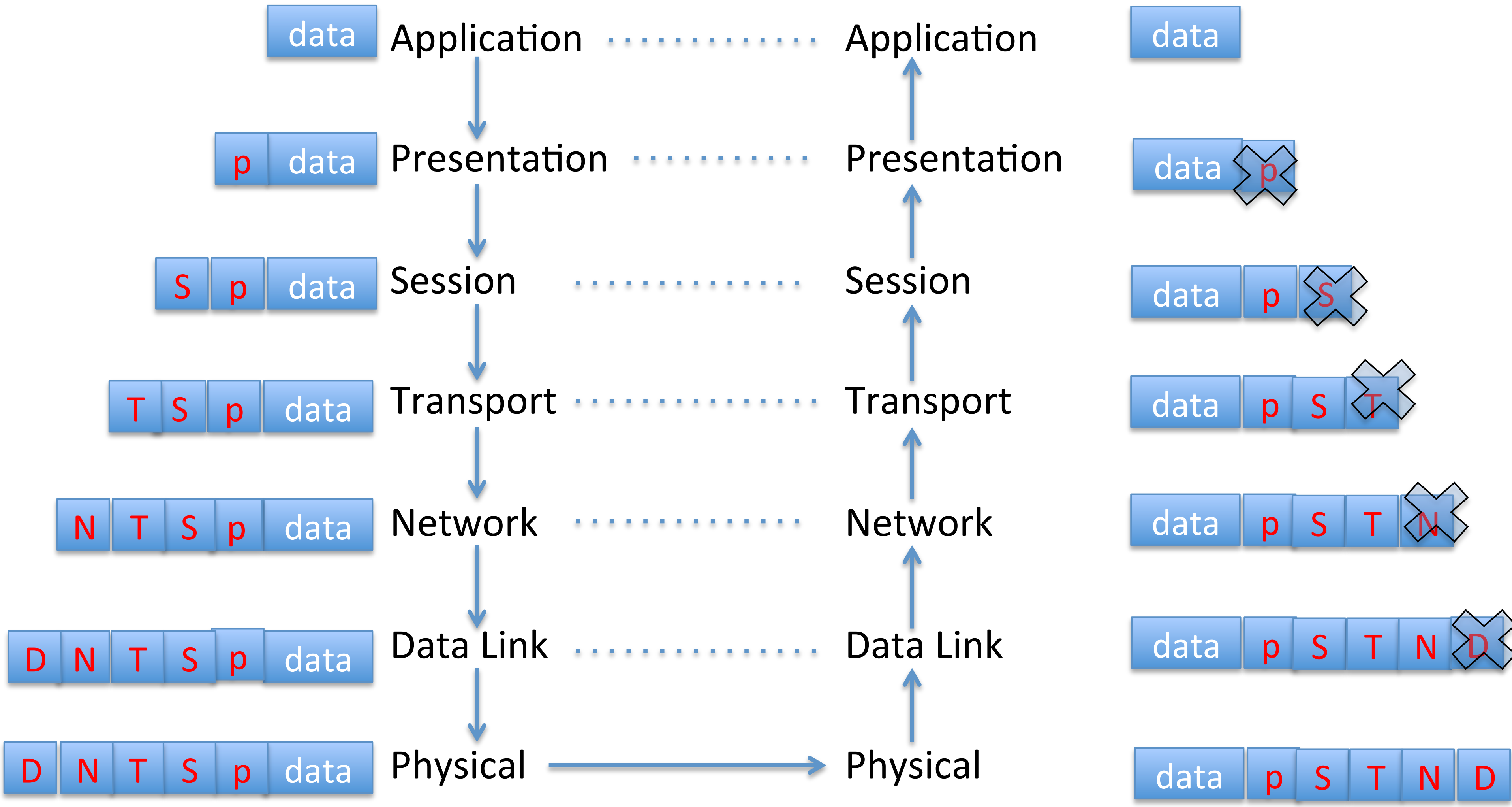
A formal set of conventions governing the format and relative timing of message exchange in the network.

Protocol

- A protocol in a layered architecture provides two interfaces:
  1. Between modules/layers on the same machine
  2. Between same modules/layers on peer machines



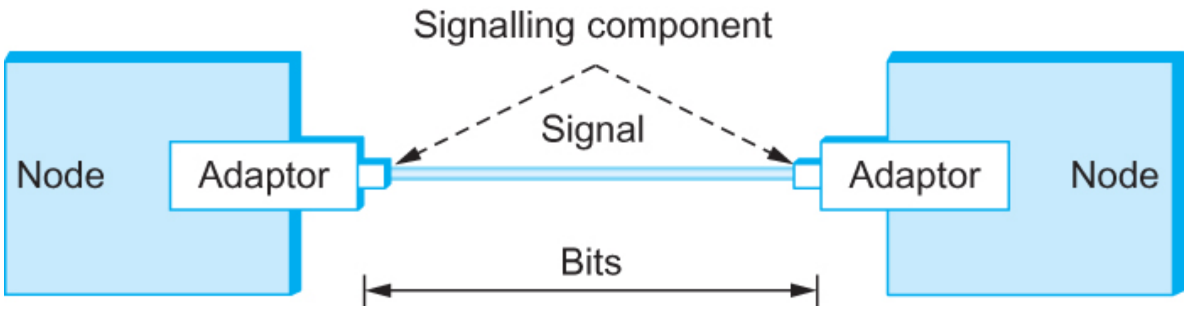
Encapsulation in OSI Model



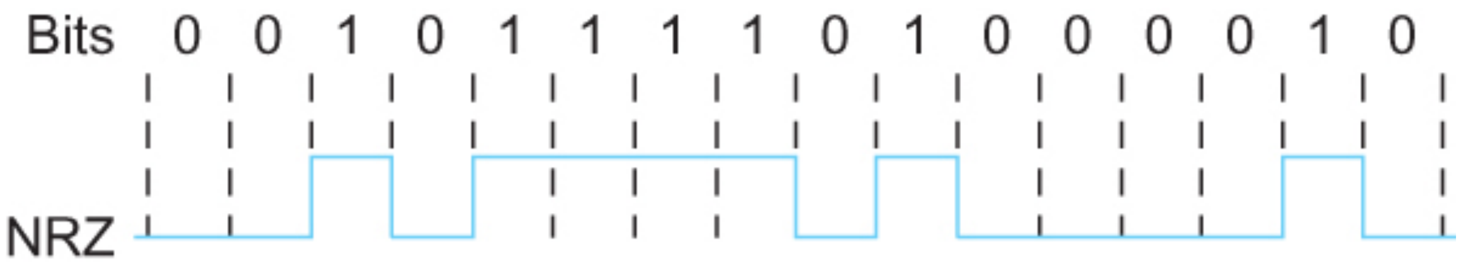
OSI Reference Model

OSI Layer	Function
Application	User interface, communication apps
Presentation	Character sets, encryption, compression
Session	Maintain connection, login, upper layer errors
Transport	Other (guaranteed delivery)
Network	Network ID, routing
Data Link	Access control, data flow, framing, device ID, error detection
Physical	Electrical & physical interface, topology, encoding

Encoding and Transmitting the Signal

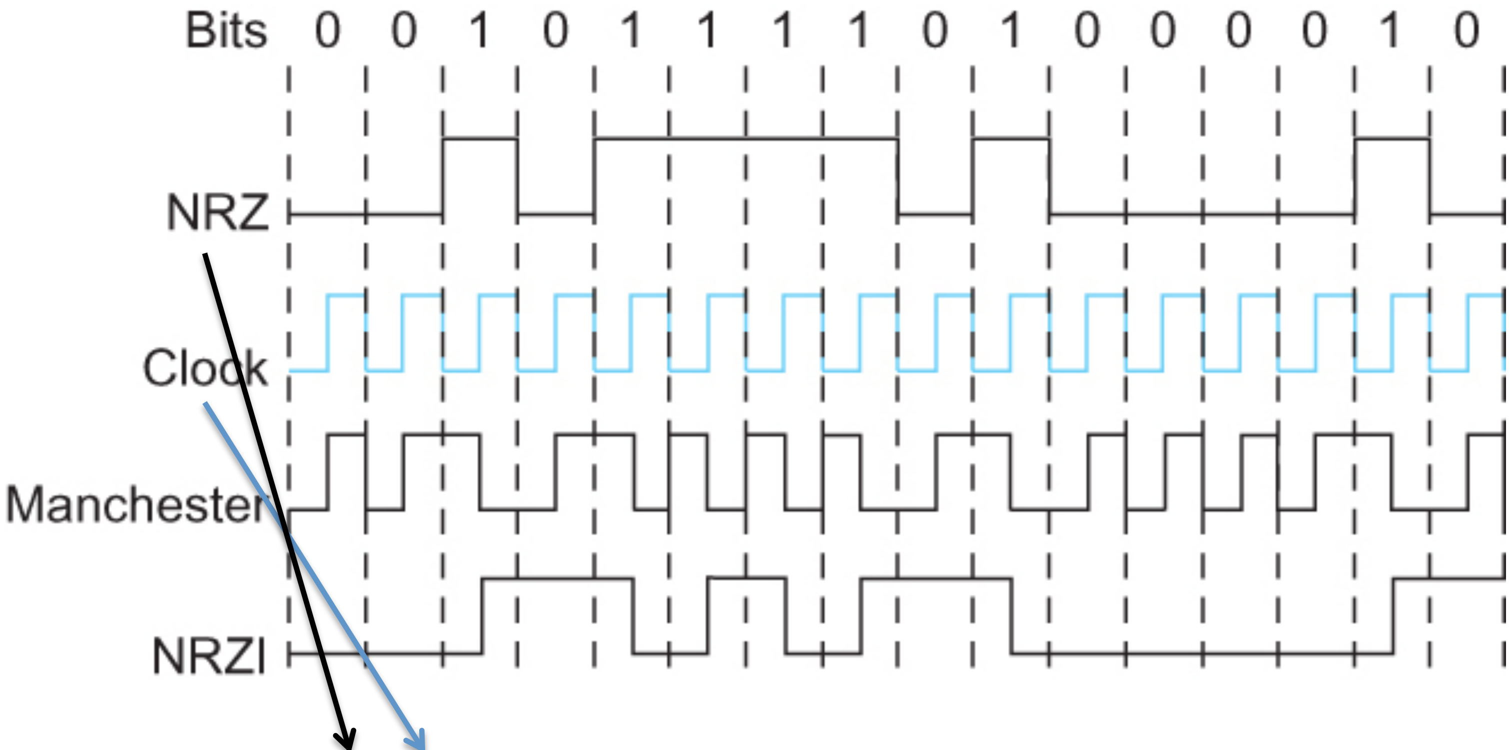


Signals travel between signaling components; bits flow between adaptors



NRZ encoding of a bit stream

Encoding



x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0

OSI Reference Model

OSI Layer	Function
Application	User interface, communication apps
Presentation	Character sets, encryption, compression
Session	Maintain connection, login, upper layer errors
Transport	Other (guaranteed delivery)
Network	Network ID, routing
Data Link	Access control, data flow, framing, device ID, error detection
Physical	Electrical & physical interface, topology, encoding

Framing

- Two Categories (approaches) of Framing Protocols

  1. Byte-oriented approach
     - Looking for a specific byte (character) or byte count to determine where the frames starts or ends

  2. Bit-oriented approach
     - Looking for a series (or combination) of bits to synchronize

Framing

- Byte-oriented Protocols
  - Views each frame as a collection (group) of bytes (characters)
  - Two approaches
    - Flag-based
      - BISYNC (Binary Synchronous Communication Protocol)
        - » Developed by IBM (late 1960)
      - Point-to-Point Protocol (PPP)
    - Byte-counting
      - DDCMP (Digital Data Communication Protocol)
        - » Developed by Digital Equipment Corporation (1974)

DDCMP count how many bytes are contained in the frame
– If count is corrupted => Framing error

Framing

- Bit-oriented Protocol
  - They were developed to overcome the limitations of character oriented protocols
  - It does not rely on a specific code or character flag for interpretation of line control.
    - To allow independence of codes (code transparency).
  - Transparency is achieved by means of *bit stuffing.*

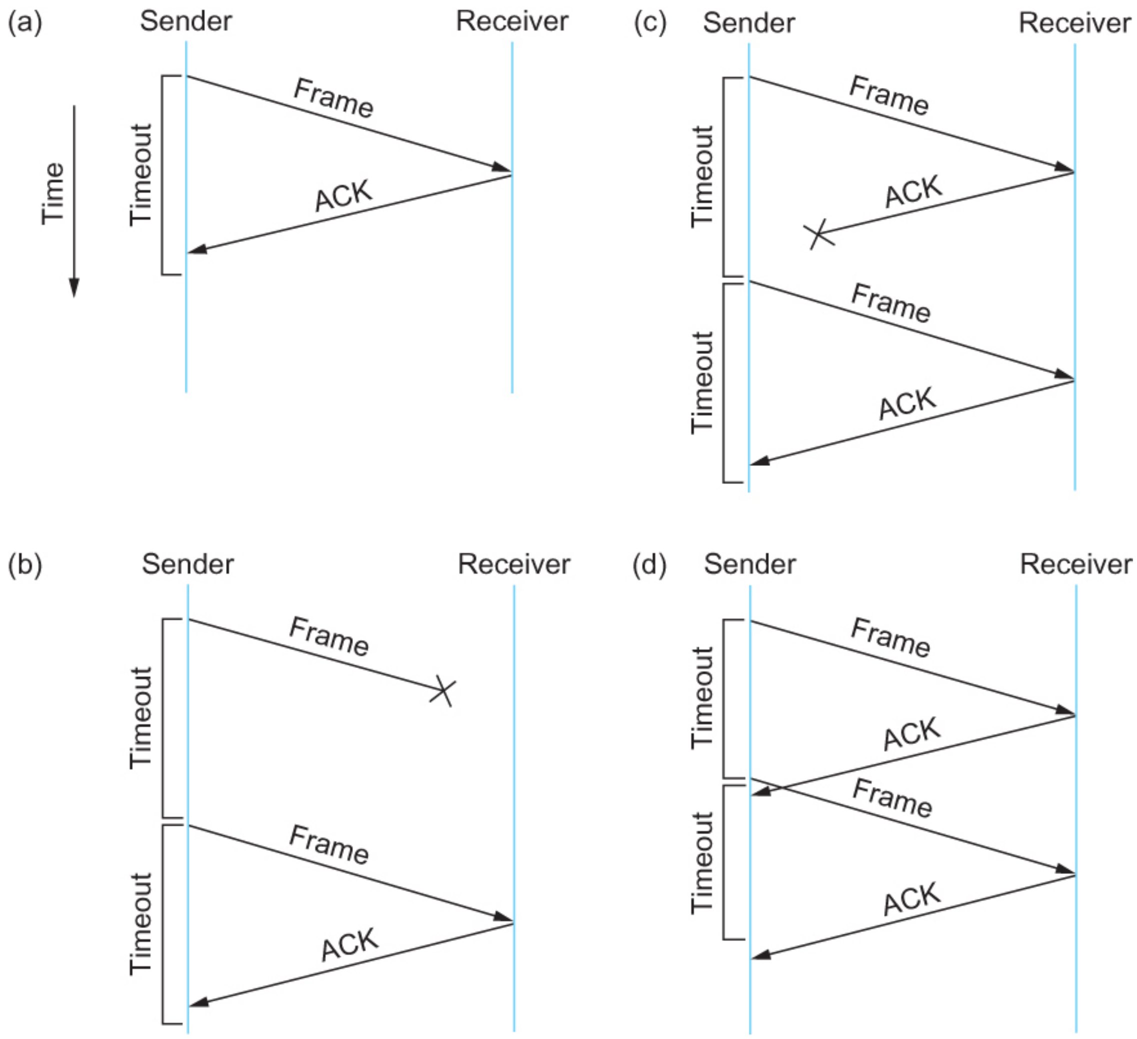
Error-Detection Algorithms

- At data link layer
  - Two-dimensional Parity
  - Cyclic Redundancy Check (CRC)
- At higher layers (TCP/IP)
  - Checksum

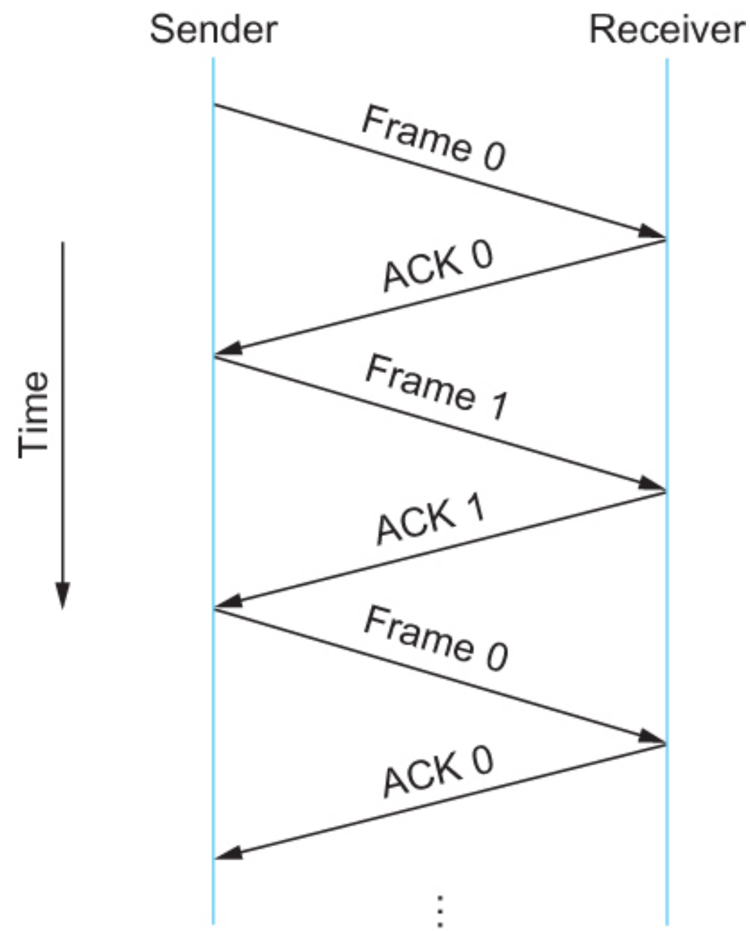
Stop and Wait Protocol

- Idea of stop-and-wait protocol is straightforward
  - Over a single link/hop, after transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
  - If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame

Stop and Wait Protocol



Stop and Wait Protocol



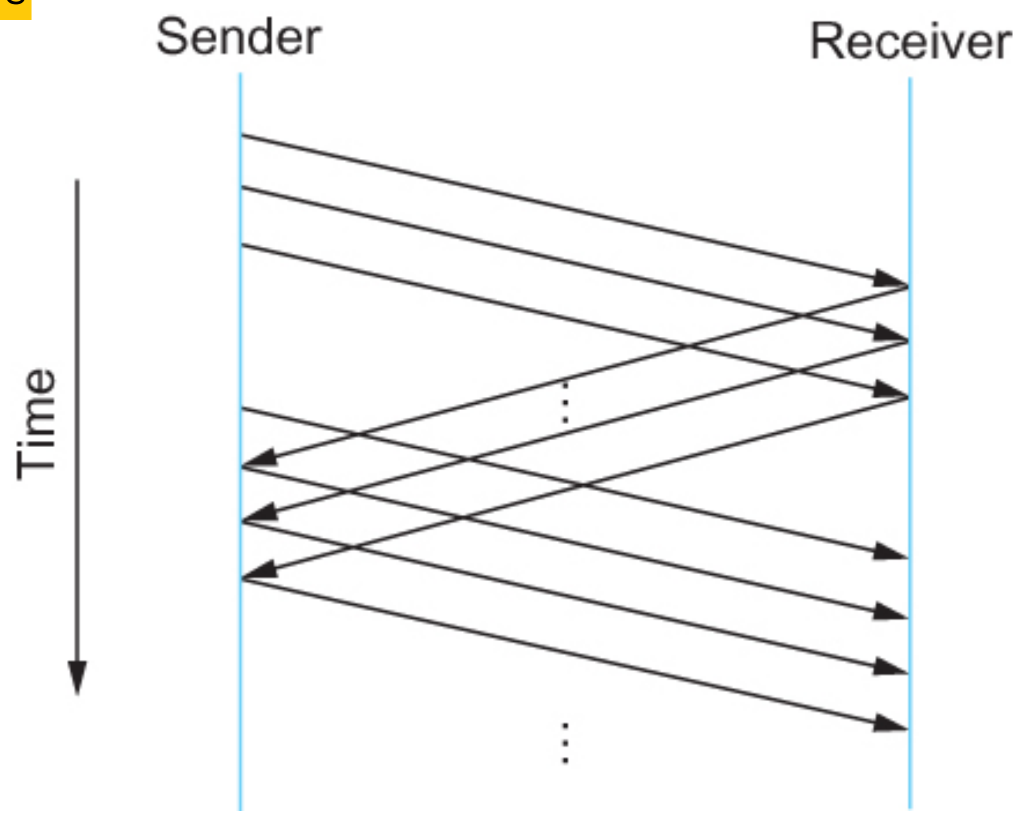
Stop and Wait Protocol

- The sender has only one outstanding frame on the link at any time
  - This may be far below the link's capacity
- Consider a 1.5 Mbps link with a 45 ms RTT
  - The link capacity can be calculated as delay $\times$ bandwidth product = 67.5 Kb or approximately 8 KB
  - (8KB)/(~1250 Bytes/frame) = 6 frames
    - 6 times more frames can be supported by the link
  - To use the link fully, then sender should transmit up to six frames before having to wait for an acknowledgement

Sliding Window Protocol

LFS-LAR <= SWS

LFR< SeqNum <= LAF



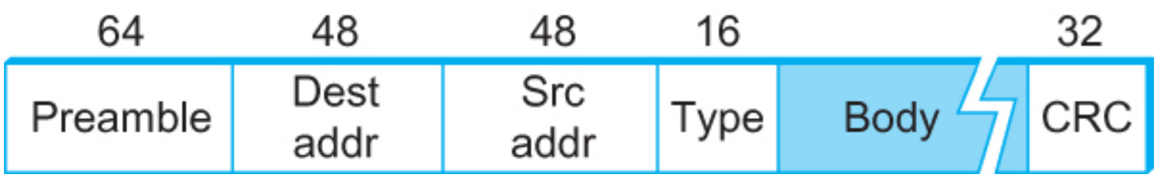
Timeline for Sliding Window Protocol

Ethernet - Based on CSMA/CD Technology

- Most successful local area networking (as well as MAN) technology of last 20 years.
- Uses CSMA/CD technology
  - Carrier Sense Multiple Access with Collision Detection.
  - Multiple access means that a set of nodes send and receive frames over a shared link.
  - Carrier sense means that all nodes can distinguish between an idle and a busy link.
  - Collision detection means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

Access Protocol for Ethernet

- The algorithm is commonly called Ethernet's Media Access Control (MAC).
  - It is implemented in Hardware on the network adaptor.
  - The MAC address belongs to the network adapter and not the host
  - A host may have more than one network adapter each with a unique MAC address
- Frame format
  - Preamble
  - Host and Destination Address
  - Packet type
  - Data
  - CRC



Ethernet Addresses

- The address belongs to the adaptor, not the host.
  - It is usually burnt into ROM.
- Ethernet addresses are typically printed in a human readable format
  - As a sequence of six numbers separated by colons.
  - Each number corresponds to 1 byte of the 6 byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte
  - Leading 0s are dropped.
  - For example, 8:0:2b:e4:b1:2 is

    00001000 00000000 00101011 11100100 10110001 00000010

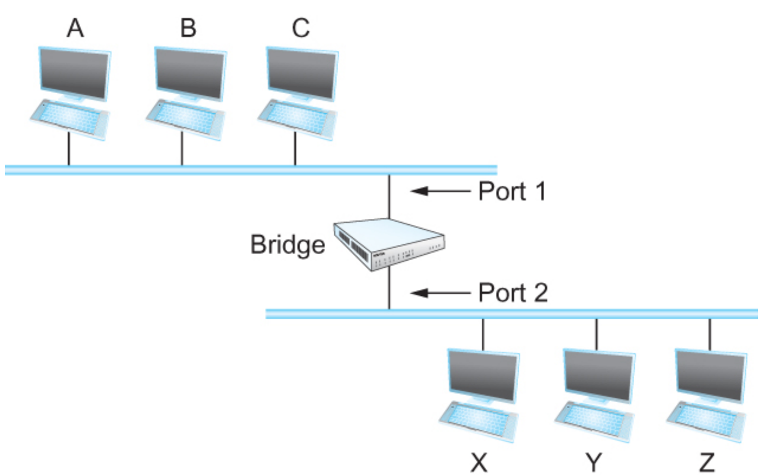
    8 : 0 : 2 b : e 4 : b 1 : 2

Bridges (LAN Switches)

- Bridges (LAN Switches)
  - Class of switches that is used to forward packets between shared-media LANs such as Ethernets (or token ring)
  - Suppose you have a pair of Ethernets that you want to interconnect
    1. One approach is put a repeater in between them
       - It might exceed the physical limitation of the Ethernet
         - » No more than four repeaters between any pair of hosts
         - » No more than a total of 2500 m in length is allowed
    2. An alternative would be to put a bridge between the two Ethernets and have it forward frames from one Ethernet to the other
       - A collection of LANs connected by one or more bridges is usually said to form an Extended LAN

Bridges (LAN Switches)

- If the bridge receives a frame that is addressed to host not currently in the table (say right after first boot, or deleted after timeout)
  - Forward the frame out on all other ports
  - The table only optimizes performance, without it, bridge acts as a hub

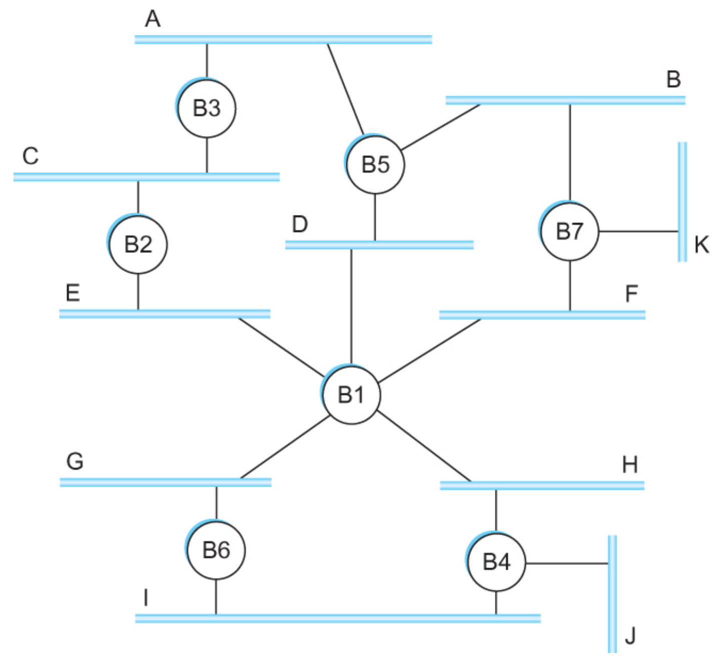


Host	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

Bridges (LAN Switches)

- Strategy works fine if the extended LAN does not have a loop in it

- Why?
  - Frames potentially loop through the extended LAN forever

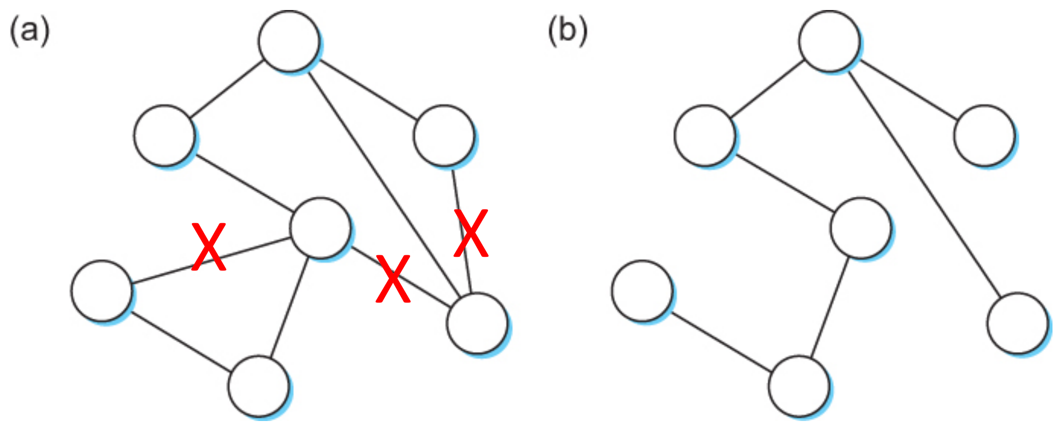


  - Bridges B1, B4, and B6 form a loop

Spanning Tree Algorithm

- Think of the extended LAN as being represented by a graph that possibly has loops (cycles)

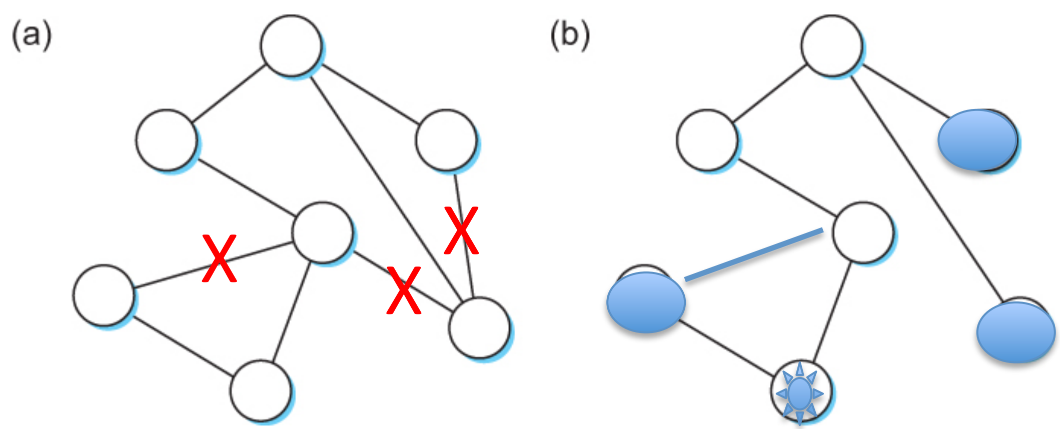
- A spanning tree is a sub-graph of this graph that covers all the vertices but contains no cycles
  - Spanning tree keeps all the vertices (nodes) of the original graph but throws out some of the edges



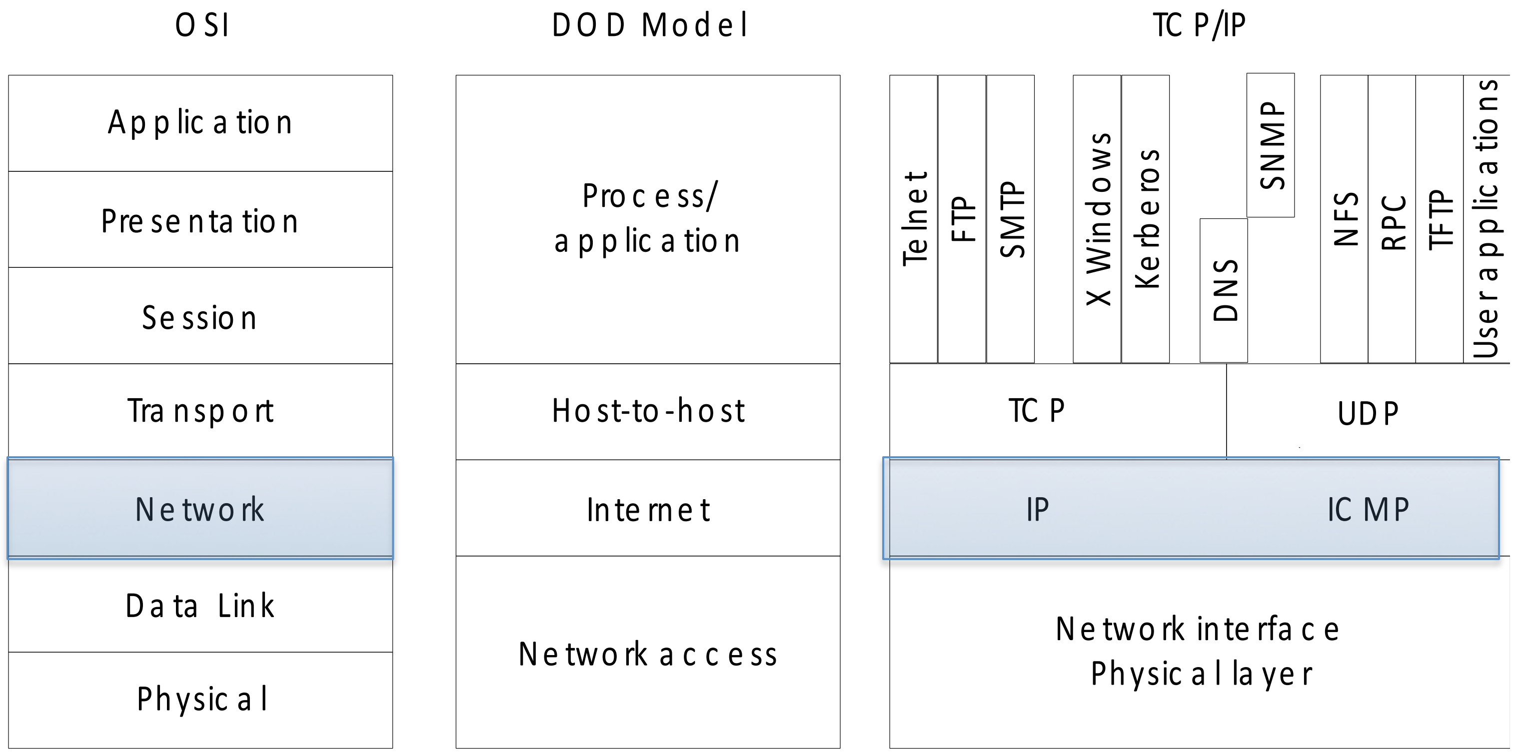
Example of (a) a cyclic graph; (b) a corresponding spanning tree.

Spanning Tree Algorithm

- How does it eliminate loops?
  - Each bridge decides the ports over which it is and is not willing to forward frames
    - In a sense, it is by removing ports from the topology that the extended LAN is reduced to an acyclic tree
    - It is even possible that an entire bridge will not participate in forwarding frames
- Algorithm is dynamic
  - The bridges are always prepared to reconfigure themselves into a new spanning tree if some bridges fail

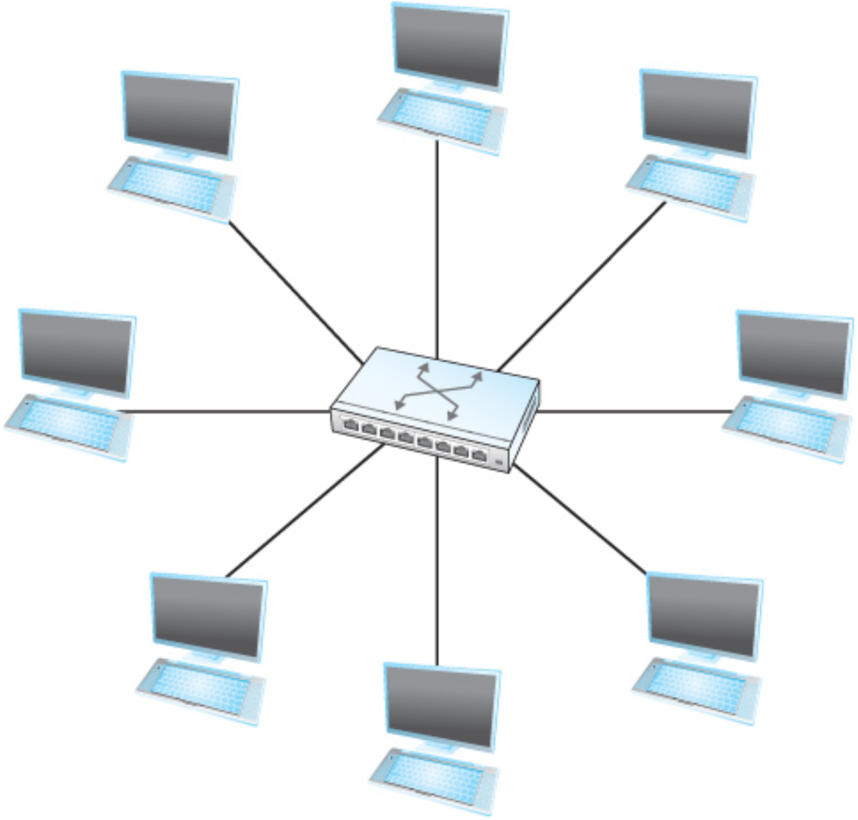


How TCP/IP Corresponds to OSI



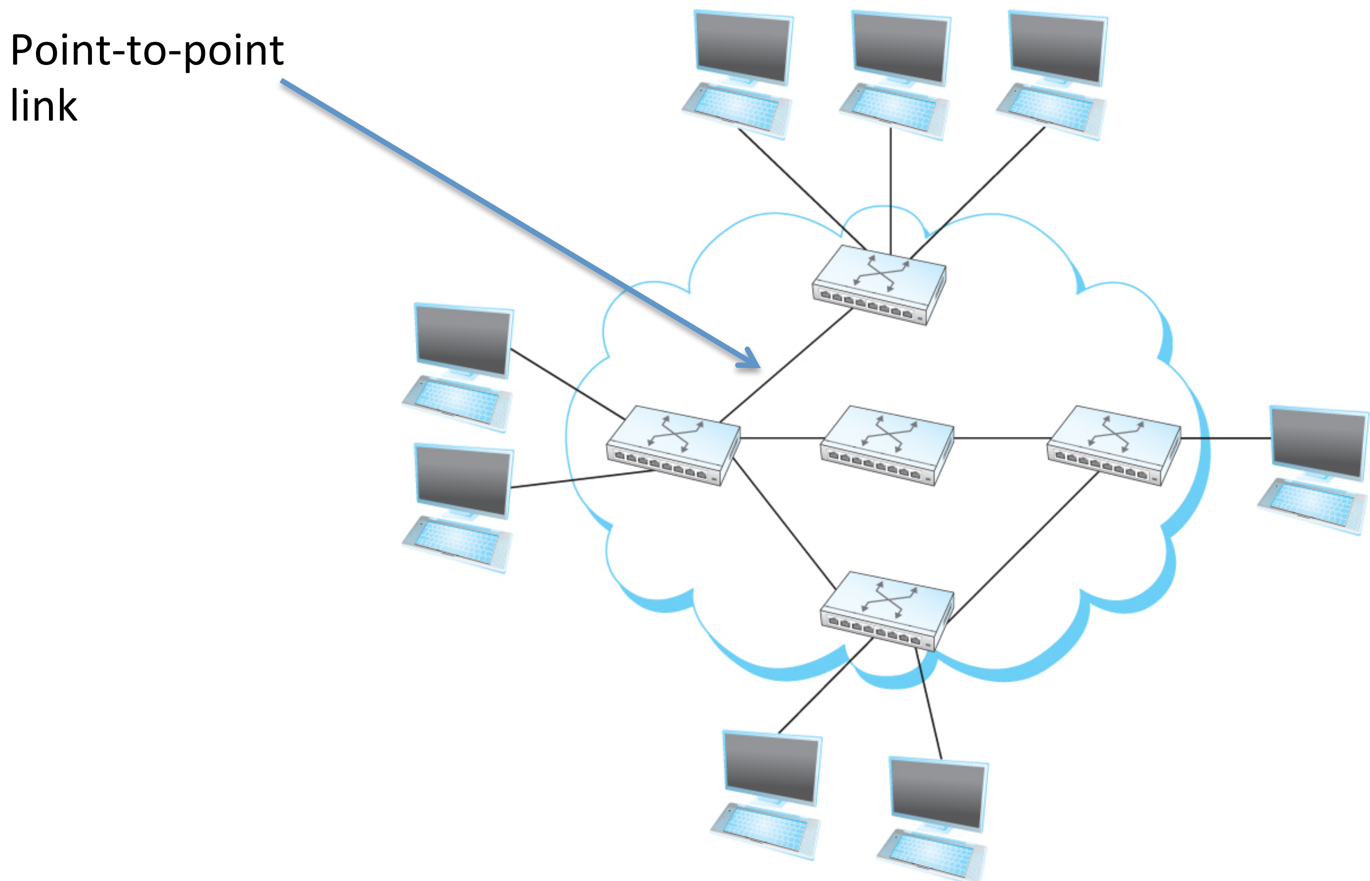
Switching and Forwarding

- Switch
  – A multi-input, multi-output device



Switching and Forwarding

- Switching and forwarding
  - Interconnect links to form a large network



Switching and Forwarding

- How does the switch decide which output port to place each packet on?
- Two common approaches
    1. *Datagram or Connectionless approach*
    2. *Virtual circuit or Connection-oriented approach*
- A third approach *source routing* is less common

Switching and Forwarding (Virtual Circuit Switching)

- Characteristics of VC
  - There is at least one RTT of delay before data is sent
  - Per-packet overhead caused by the header is reduced relative to the datagram model (higher transmission speed)
  - If a switch or a link in a connection fails, the connection is broken and a new one will need to be established.
    - Also the old one needs to be torn down to free up table storage space in the switches.
  - The link selection decision to forward the connection request has similarities with the function of a routing algorithm.

Switching and Forwarding (Virtual Circuit Switching)

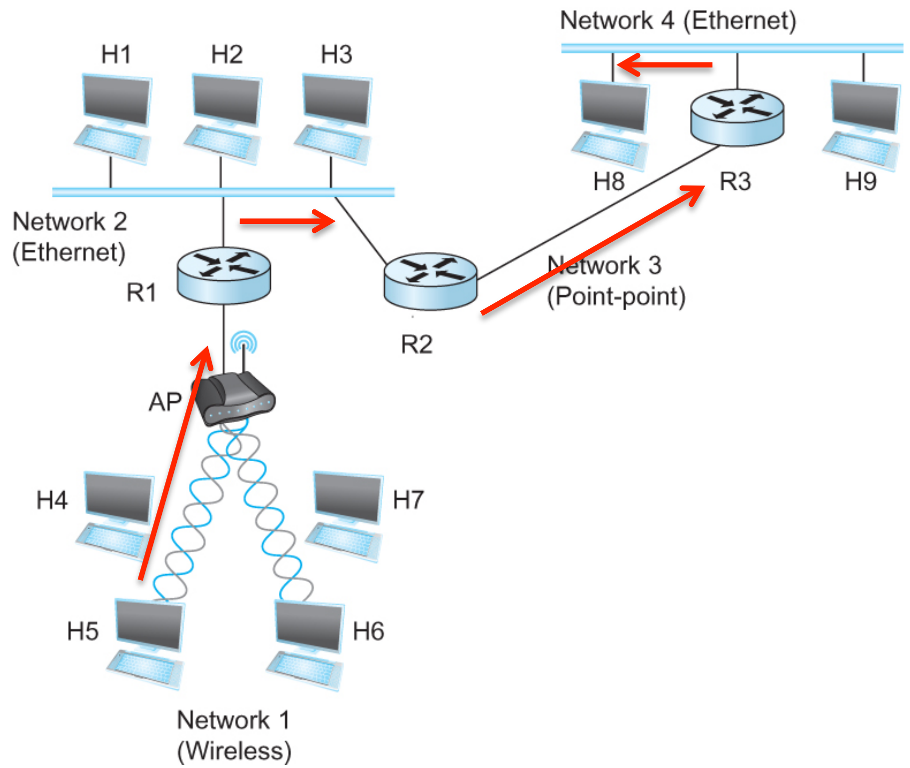
- Good Properties of VC
  - By the time the host gets the go-ahead to send data, it knows quite a lot about the network
  - It is also possible to allocate resources to the virtual circuit at the time it is established

Switching and Forwarding (Virtual Circuit Switching)

- Comparison with the Datagram Model
  - Datagram network has no connection establishment phase and each switch processes each packet independently
  - Each arriving packet competes with all other packets for buffer space
  - If there are no buffers, the incoming packet must be dropped
- In VC, we could imagine providing each circuit with a different quality of service (QoS)
  - The network gives the user some kind of <u>performance related guarantee</u>
    - Switches set aside the resources they need to meet this guarantee
- Most popular examples of VC technologies are Frame Relay and ATM
  - One of the applications of Frame Relay is the construction of VPN

Internetworking

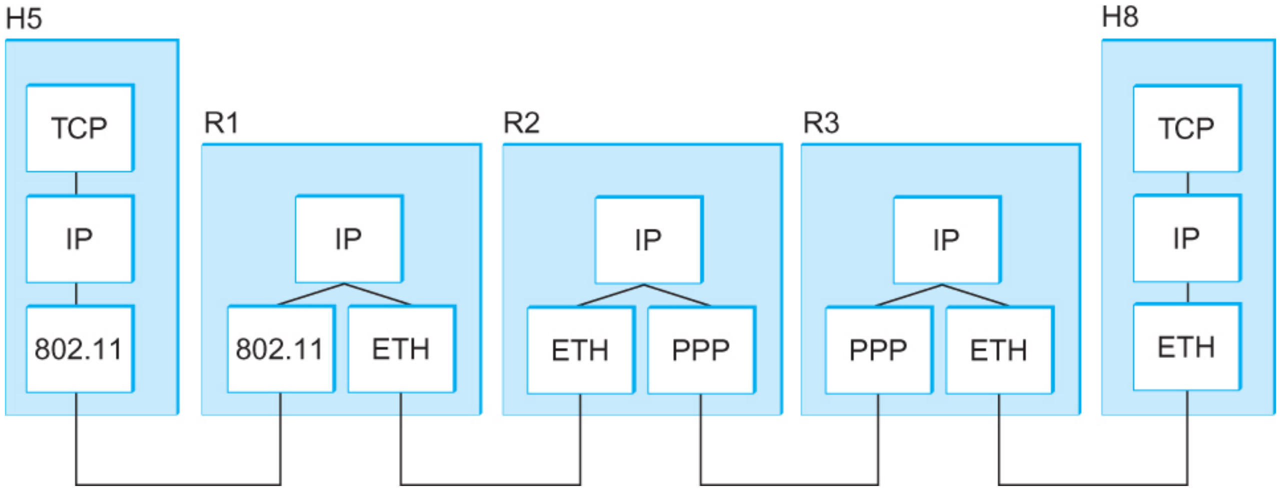
- What is an internetwork?
  - A network of networks
  - An arbitrary collection of networks interconnected to provide some sort of host-to-host packet delivery service (say, H5 to H8)



A simple internetwork where H represents hosts and R represents routers

Internetworking

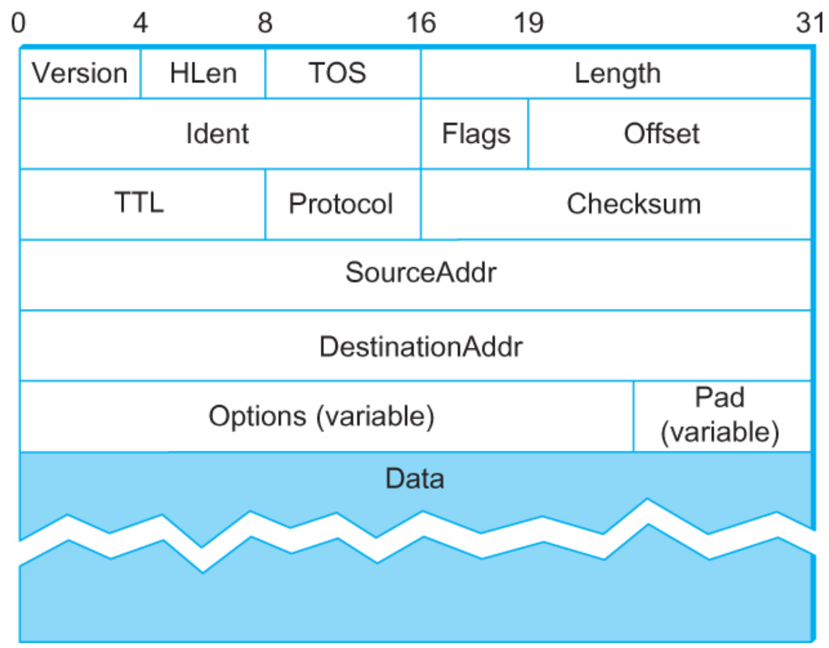
- What is IP?
  - IP stands for Internet Protocol
  - Key tool used today to build scalable, heterogeneous internetworks
  - It runs on all the nodes in a collection of networks and defines the infrastructure that allows these nodes and networks to function as a single logical internetwork



A simple internetwork showing the protocol layers

IPv4 Packet Format

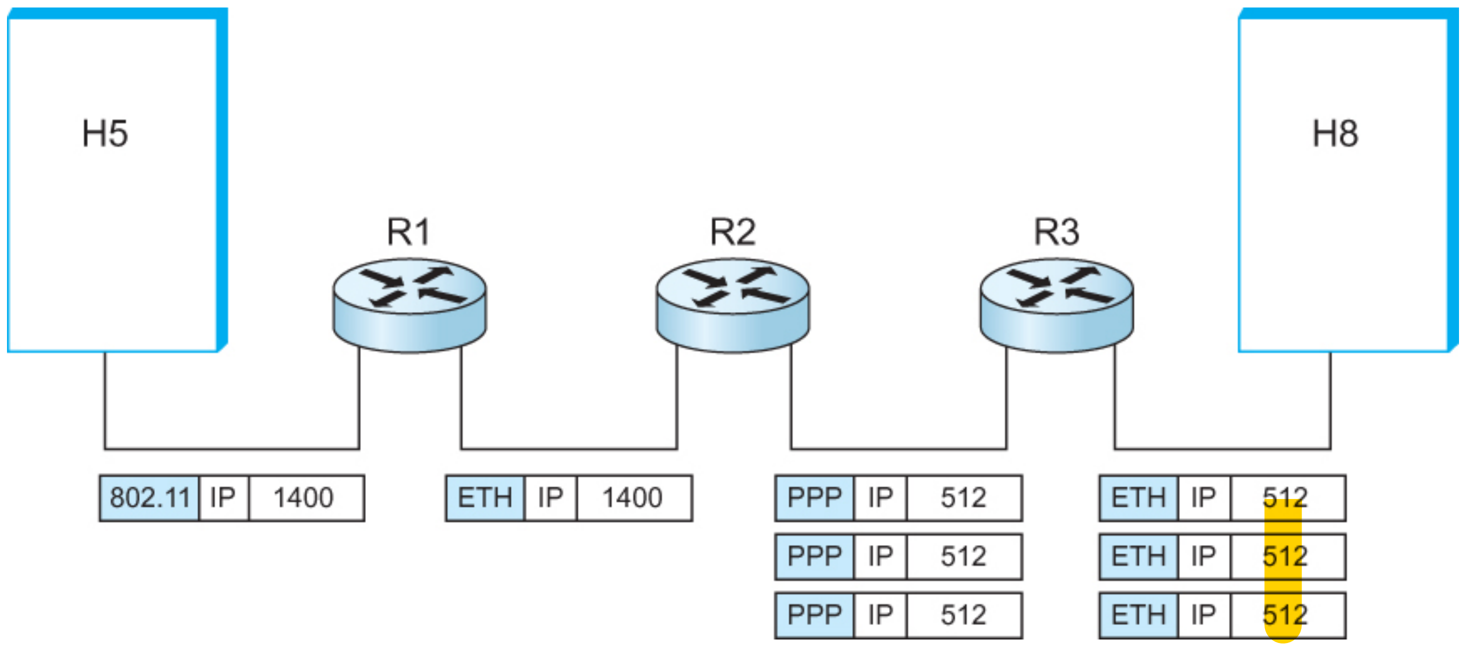
- Version (4): currently 4
- Hlen (4): header length (number of 32-bit words in header, min 20 bytes + options)
- TOS (8): type of service (to allow packets to be treated differently based on the application needs)
- Length (16): number of bytes in this datagram including the header (max 2^{16} = 65,535 bytes)
- Ident (16): used by fragmentation
- Flags & Offset (16): used by fragmentation
- TTL (8): number of hops this datagram has traveled
- Protocol (8): demux key (TCP=6, UDP=17) for higher-layer protocol
- Checksum (16): of the header only
- DestAddr & SrcAddr (32)



IP Fragmentation and Reassembly

- Each network has some MTU (Maximum Transmission Unit)
  - Ethernet (1500 bytes), FDDI (4500 bytes)
- Strategy
  - Fragmentation occurs in a router when it receives a datagram that it wants to forward over a network link which has (MTU < datagram)
  - Reassembly is done at the receiving host
  - All the fragments carry the same identifier in the *Ident* field
  - Fragments are self-contained IP datagrams

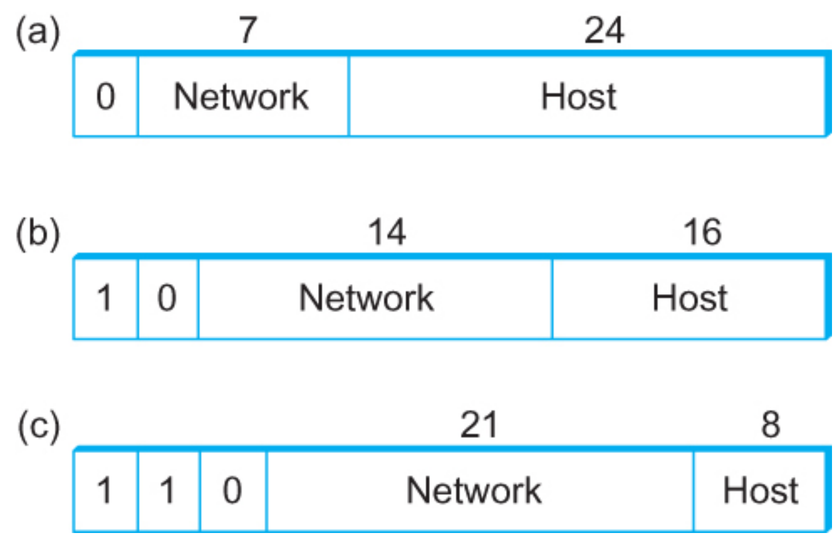
IP Fragmentation and Reassembly



IP datagrams traversing the sequence of physical networks

Global Addresses

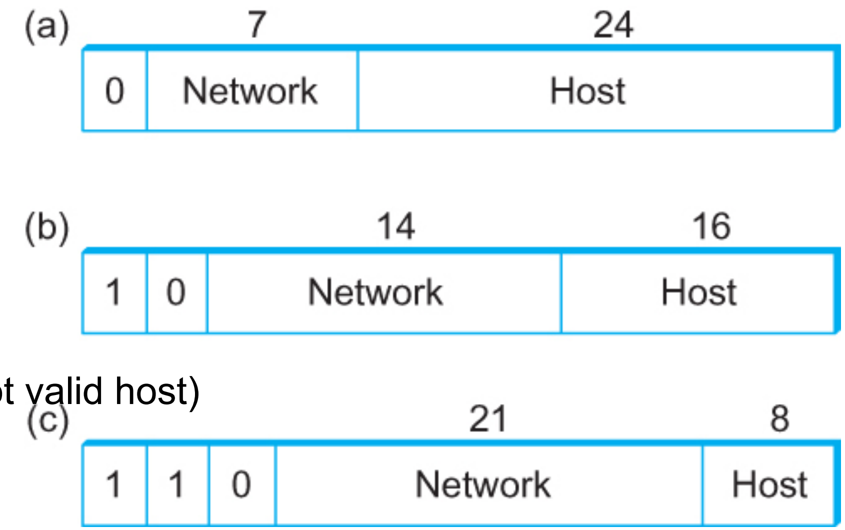
- Properties
  - globally unique
  - hierarchical: network + host
  - 4 Billion IP address (2^{32}), half are A type, ¼ is B type, and 1/8 is C type
- Format (all 32 bits)
  - Class D (multicasting)
    - Leading bits are 1110
  - Class E (research)
    - Leading bits 1111



- Dot notation
  - 10.3.2.4
  - 128.96.33.81
  - 192.168.1.1 (11000000 10101000 00000001 00000001)

Octet 1 Octet 2 Octet 3 Octet 4

Global Addresses



2^21 class C networks
(255 broadcast, 0 is not valid host)

Class	1st Octet	Mask	Format
A	1 – 127	255.0.0.0	n.h.h.h
B	128 - 191	255.255.0.0	n.n.h.h
C	192 - 223	255.255.255.0	n.n.n.h
D	224 - 239	Multicast	Multicast
E	240 - 255	Experimental	Experimental

Classless Addressing

CIDR Notation

- Traditionally, subnet masks were determined by the IP address class, so there were only really three subnet masks you would see – For the class A, B and C networks
- To preserve IP address space, use them more efficiently, and help decrease burdon on global routing tables classless interdomain routing was born (CIDR).
- CIDR is used for IP address aggregation and specifies the subnet mask in a different notation
- The CIDR notation lists the network followed by a "/" followed by the number of subnet mask bits
  - Example: 192.168.0.0/16 ← dotted decimal mask 255.255.0.0
  - Example: 220.140.100.0/25 ← dotted decimal mask 255.255.255.128
  - Example: 8.8.8.8/30 ← dotted decimal mask 255.255.255.252

IP Layer Protocols

- ARP (Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- ICMP (Internet Control Message Protocol)

Address Translation

- ARP (Address Resolution Protocol)
  – Table of IP to physical (MAC) address bindings
  – Broadcast request if IP address not in table
    - Target machine responds with its physical address
  – Table entries are discarded if not refreshed

Host Configurations

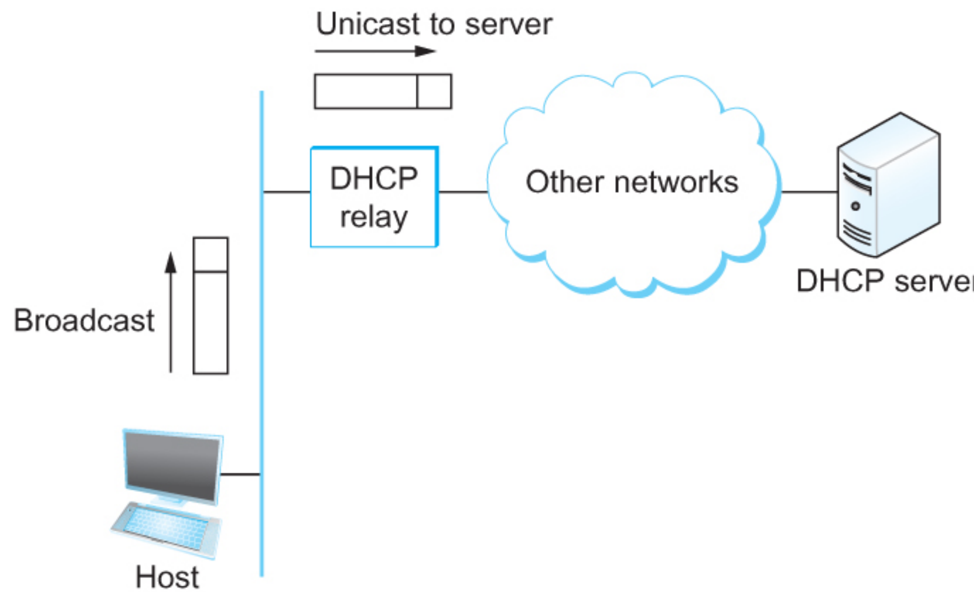
- Ethernet addresses are configured into network by manufacturer and they are unique
- IP addresses must be unique on a given internetwork but also must reflect the structure of the internetwork
- Most host Operating Systems provide a way to manually configure the IP information for the host
- Drawbacks of manual configuration
  - A lot of work to configure all the hosts in a large network
  - Configuration process is error-prone
- Automated Configuration Process is required

Dynamic Host Configuration Protocol (DHCP)

- DHCP server is responsible for providing configuration information to hosts
- There is at least one DHCP server for an administrative domain
- DHCP server maintains a pool of available addresses

DHCP

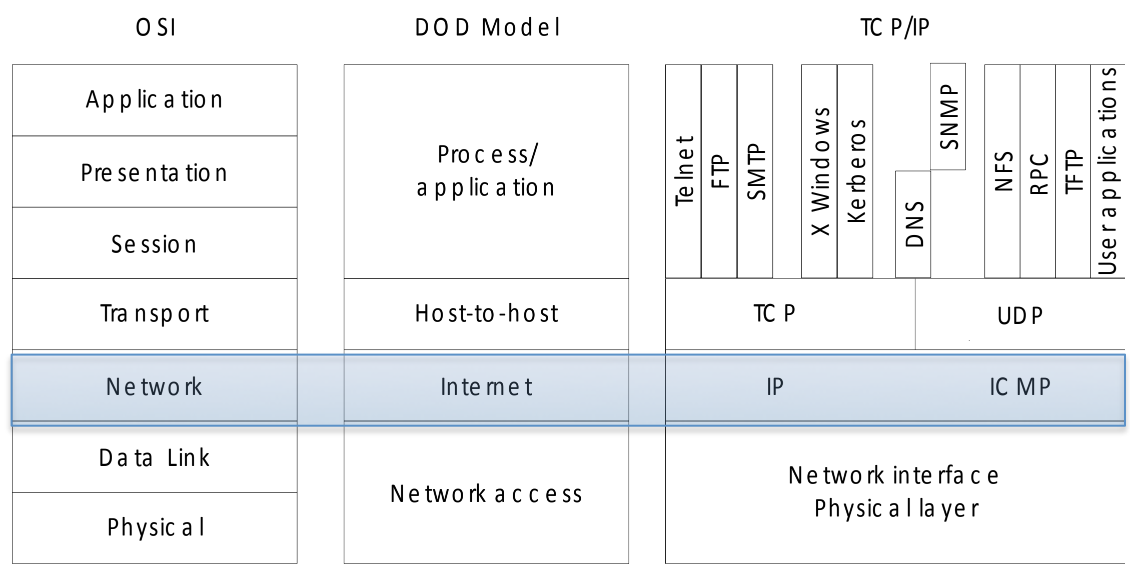
- Newly booted or attached host sends DHCPDISCOVER message to a special IP address (255.255.255.255)
  - Broadcast
- DHCP relay agent unicasts the message to DHCP server and waits for the response



https://www.youtube.com/watch?v=RUZohsAxPxQ

Internet Control Message Protocol (ICMP)

- Defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully
  - Destination host unreachable due to link /node failure
  - Reassembly process failed
  - TTL had reached 0 (so datagrams don't cycle forever)
  - IP header checksum failed



Internet Control Message Protocol (ICMP)

- ICMP-Redirect (a useful ICMP control message)
  - From router to a source host
  - With a better route information (for the consequent packets)