History of Ethernet

• In 1971, the University of Hawaii, ALOHANET, a radio system, was the first Multiple Access network.

• In 1976, carrier sense was introduced.

• In the late 1970s, 2.94 Mbps Ethernet was implemented by Dr. Robert M. Metcalfe at the Xerox Palo Alto Research Center.
  – over 100 personal workstations on a 1-km cable.

• In 1980, a consortium of DEC, Intel, and Xerox (DIX) build a 10 Mbps Ethernet.
  – Published the first Ethernet specifications.
  – The basis for the IEEE standard 802.3.
  – *This standard used a MAC protocol called CSMA/CD within a standard Ethernet frame, across a common physical medium bus with channel attached MAC addressed stations.*

• First products for Ethernet appeared in 1981.
802.3 CSMA/CD (Ethernet)

• CSMA/CD allows at rates theoretically reaching 10 Mbps
  – Increasingly inefficient under heavier traffic loads
  – Actual throughput may only be 3.5 Mbps

• Best effort delivery
  – No complete guarantee of successful sending a message

• Specific data link functions of Ethernet include
  – Encapsulation and de encapsulation of user data
  – Media access management (such as physical layer and buffer management)
  – Collision detection and handling
  – Data encoding and decoding
  – Channel access to the LAN medium.
CSMA/CD Routine

- **States of the Ethernet**
  - Idle
  - Transmission
  - Collision

- **Key features of the CSMA/CD**
  - Listening to the channel
  - Transmitting only if an "idle" channel is detected
  - Waiting a random amount of time if it is busy

---

Data ready

Listen

Busy Idle

Wait

Transmit/ Listen

Collision Success
History of Token Ring

- Developed by IBM development labs in Zurich, Switzerland, in the late 1960s

- In 1985, IBM chose 4Mbps Token Ring as its LAN protocol

- First products appearing in 1986
  - Wiring concentrator (Multistation Access Unit),
  - Cabling with type 3 telephone cable

- IEEE has adopted Token Ring as IEEE Standard 802.5
  - 802.5 MAC Token Passing Protocol working on the IEEE 802.2 Logical Link Control sublayer

- Later, IEEE 802.4 defined a Token Bus standard
  - A token passing MAC protocol for operating on a bus topology

- In 1988, the 16 Mbit/s standard was introduced.
  - Response to Ethernet's speed advantage
802.5 Token Ring

- Most often implemented as a Physical star topology with hub/concentrator and forming a Logical Ring

- Token are data packets with multiple fields
  - Token moves counter-clockwise around ring
  - Token status is marked “Free” or “Busy”

- Any station may seize a free token
  - Modify its status
  - Load data into token
  - Send token to the destination station

- If the token is busy (the token contains data destined for a different station)
  - Non-addressee station regenerates it and passes it on to the next station without modification

- Only one station on the ring can transmit data over the common medium at a given time
Token Ring

- Multistation Access Units (MAUs) used as Token Ring hubs
  - Automatically bypass non-operational spokes
  - May be passive or active (integral repeater)

- Token Ring types
  - Type 1: Shielded Twisted Pair
    - Up to 260 notes
  - Type 3: Unshielding Twisted Pair (Category 3,4,5 UTP)
    - Up to 72 nodes

- Under uniformly high traffic loading, the Token Ring protocol is much more bandwidth efficient than other LAN protocols
  - Because there are fewer idle tokens
  - Opposed to Ethernet, where heavy load causes many collisions
  - Un-even traffic loading may cause “starvation”

- Tokens may be assigned priorities for specific stations on the ring
Token Ring Passing Routine

1. Free token

2. Token with C destination

3. Token passed through node D on to node C

4. Token received by node C and new free token passed to B
Fiber Data Distribution Interface (FDDI)

- LAN and MAN standard defined by ANSI and CBEMA as X3T12
  - Also recognized as an ISO standard

- Token Ring is the basis for FDDI
  - Similar protocol logic except
    - Free token seizing
    - Release of token after transmission

- Physical star topology with hub/concentrator and forming a Logical Ring

- Requires a master station
  - Listens for the presence of a good token
  - If a good token is not heard after a specified time, it regenerate ones

- 100 Mbps maximum datarate
  - Actual throughput much lower

- Physical media-dependent
  - Single or multi-mode fiber
  - Copper Data Distribution Interface (CDDI) with STP or UTP
FDDI Ring

- Dual counter-rotating rings
  - Primary ring
  - Secondary ring

- Two types of nodes
  - *Class A* or *Primary Stations* are attached to both rings
  - *Class B* or *Secondary Stations* are attached to both rings

- Dual-attached stations use an internal by-pass switch to automatically “self heal” the network
  - Both physical ports share a single MAC Layer and MAC addresses
FDDI Applications

- Link high-performance desktop machines in a workgroup

- High speed backbone to link routers & concentrators
  - MAN and WAN applications

- FDDI standard for max distance between end-stations and concentrators
  - 100m with Cat. 5 UTP
  - 2 km with multi-mode fiber
  - 60km with single-mode fiber

- Total size
  - 500 dual attached nodes
  - Total circumference of 200 km for dual-attached fiber rings
FDDI Self Healing

- Dual-attached FDDI nodes may bypass breaks in the network lines
- Automatically causes a “ring wrap” (loop back)
  - Traffic is diverted to the secondary ring
  - The point of failure is removed from the network
- FDDI nodes may connect to multiple concentrators
FDDI Operations

- A node with traffic to send may seize a free token
  - Takes original token off the ring
  - Transmits full frame with destination address

- A new token is released onto the ring
  - Even though the destination station has not received the full frame

**Major difference from Token Ring**
- Allows high speed transmissions can be without waiting for the transmitting station to clear the original token

- Addressee only reads the frame & copies the message

- Non-addressees read the frame & do nothing

- Original frame eventually returns to the transmitting node
  - Transmitting node purges frame from the ring
FDDI Token Passing Routine

1. A absorbs the token

2. A transmits frame to C & appends new token (D ignores frame)

3. C reads in frame & frame continues back to A (D has chance to transmit if it has traffic to send)

4. A takes the frame off the network (C has a chance to transmit if it has traffic to send)
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1960</td>
<td>RAND Corp. published paper on survivable computer communications in the event of a nuclear exchange using packet switching</td>
</tr>
<tr>
<td>1960s</td>
<td>ARPA (Advanced Research Projects Agency) was working on a way to share technical information among university, military, and defense contractors</td>
</tr>
</tbody>
</table>
| 1972 | ARPANET connects 4 universities with the first packet switching network  
  - Uses Network Control Protocol (NCP) and Interface Message Processor (IMP) protocol  
  - ARPA Internetting Project begins to study how to link various packet networks  
  * Basis for development of TCP/IP |
| 1975 | Management of the Internet is transferred to the Defense Communications Agency (DCA)  
  - BBN opens TELNET, first commercial packet switched network  
  - TCP defined |
History of TCP/IP

- **1982** - TCP/IP becomes the standard for network communications on ARPANET
- **1983** - ARPANET began using TCP/IP
  - MILNET and DDN (Defense Data Network) split off from ARPANET
  - ARPANET was the nonmilitary research network and the origin of the Internet
- **1989** - ARPANET ceases and joins to NSFNET
- **1991** - NSF lifts the restrictions against commercial use of the Internet
- Now many Network Operating Systems (NOS) have integral TCP/IP
  - Novell NetWare, Banyan Vines, and Windows 95/98
Transmission Control protocol (TCP) / Internet Protocol (IP)

- Many network and transport protocols work closely together
- User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and TCP interface directly with IP
  - Allow the host to distinguish among multiple applications through port numbers
  - TCP provides adaptive flow control, segmentation, and reassembly, and prioritized data flows
  - TCP provides a reliable sequenced delivery of data to applications
  - UDP only provides unacknowledged datagram capability
TCP/IP Functions

• TCP and IP assumes that the underlying network is a connectionless datagram network
  – Packets may be delivered out of order or have duplicates delivered

• IP provides a connectionless datagram delivery service to the transport layer
  – Does not provide:
    • End to end reliable delivery
    • Error or flow control
    • Retransmission
  – Relies on TCP to provide these functions.

• IP operates of over a number of network, data link, and physical layer services
  – Network layer: IP operates over X.25 and SMDS
  – At the data link layer, IP operates over frame relay, Ethernet, Token Ring, FDDI, and ATM
  – At the physical layer: IP operates over circuit switched and dedicated lines

• TCP is a connection oriented protocol
  – Has specific messages for an application to request a distant connection
  – Has messages for a destination to identify that it is ready to receive incoming connection requests
TCP/IP Operation

- TCP works over IP to achieve end to end reliable transmission of data across network

- TCP handles packet segmentation and reassembly using the sequence number in the TCP header
  - IP does this using the fragment control fields in the IP header
  - Either method, or both, may be used

- TCP/IP of acceptance of datagrams out of order and ability to operate over an unreliable underlying network
  - Makes it quite robust
  - None of the other standard modern data communication protocols has this attribute
  - IPX/SPX approximates it
Traffic and Congestion Control

- TCP flow control uses a sliding window flow control protocol
  - Like X.25, but with a variable size window

- The sender starts with a window size equal to that of one TCP segment
  - The IP datagrams are delivered to the destination workstation
  - The delivered TCP segment is acknowledged.

- The sender then increments the window size and transmits more segments
  - Until the network has become congested and the third segment is lost (not acknowledged)
  - The sender detects this by starting a timer whenever a segment is sent
  - If the timer expires, then
    - The segment is resent
    - The sender reduces window size to one segment
    - The process is repeated

- Specific implementations will vary
  - Fine tuning of the algorithms
  - The TCP/IP architecture permits the sender and receiver to use different algorithms
TCP Dynamic Windowing Flow Control

Window

1  S(0) ——— S(0)
2  S(1) ——— ACK(0) ——— S(1)
     S(2) ——— ACK(1) ——— S(2)
     S(3) ——— ACK(2) ——— S(3)
3  S(4) ——— ACK(3) ——— S(4)
     S(5) ——— ACK(4) ——— S(5)
     Timeout
1  S(5) ——— X ——— S(5)

S = TCP Segment
ACK = Acknowledgement
(N) = Segment Number
Internet Addresses

• Computers
  – host.institution.domain
    e.g. lucia.lib.lawrence.edu

• Users
  – username@host.institution.domain
    e.g. wnekr@bah.com

• Uniform Resource Locator (URL)
  – protocol://host.institution.domain[/directory/filename]
    e.g. http://cwis.lawrence.edu/www/lib/learn/5.htm
Domain Naming Service 1

- The Internet Network Information Center (InterNIC) is the government-sponsored activity that assigns all US domain names
  - charges $100 for the first two years of domain name service, plus $50 every subsequent year
  - currently, the domain name registrar is Network Solutions Inc. but 4 other companies are being transitioned into this role

- Sites outside the US use different organizations to assign domain names using their own standards
  - E.g. domain names .co.uk or .ac.uk, indicate a company or academic institution in the United Kingdom

- Domain Naming Service (DNS) is an Internet protocol and distributed database
  - Used to translate between domain names and IP addresses
    - pointing a browser at www.asite.com is far easier than remembering the site's numeric IP address
  - Used to control Internet email delivery
Domain Naming Service 2

- At the top of the DNS database tree are Root Name Servers, which contain pointers to master name servers for each of the top-level domains (e.g. .com).
  - E.g. to find the IP address of www.asite.com, a DNS server would ask the root name server for the address of the master name server for the .com domain.

- The Master Name Servers for each of the top-level domains contain a record and name-server address of each domain name.

- The individual name servers for each domain name contain detailed address information for the hosts in that domain.

![Diagram of DNS structure]
IP Addressing

- IP addressing is based on hosts and networks
  - Hosts or nodes are any device capable of receiving and transmitting IP packets e.g. workstations and routers
  - Hosts are connected together by one or more networks

- Host IP addresses are composed of two parts: a network address and a host address within the network
  - Unlike IPX addresses
  - An IP address is 32 bits wide
  - The portion of the address is used to specify the network and the portion used to specify the host varies from network to network

- IP addresses are, by convention, expressed as four decimal numbers separated by periods e.g. "200.1.2.3"
IP Address Classes

• Valid IP addresses thus range from 0.0.0.0 to 255.255.255.255,
  – A total of about 4.3 billion addresses

• The first few bits of the address indicate the Class that the address belongs to:

<table>
<thead>
<tr>
<th>Class</th>
<th>Prefix</th>
<th>Network Number</th>
<th>Host Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>Bits 1-7</td>
<td>Bits 8-31</td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td>Bits 2-15</td>
<td>Bits 16-31</td>
</tr>
<tr>
<td>C</td>
<td>110</td>
<td>Bits 3-24</td>
<td>Bits 25-31</td>
</tr>
<tr>
<td>D</td>
<td>1110</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>1111</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

– Class D addresses are multicast, and Class E are reserved

• The range of network numbers and host numbers may then be derived:

<table>
<thead>
<tr>
<th>Class</th>
<th>Range of Net Numbers</th>
<th>Range of Host Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0 to 126</td>
<td>0.0.1 to 255.255.254</td>
</tr>
<tr>
<td>B</td>
<td>128.0 to 191.255</td>
<td>0.1 to 255.254</td>
</tr>
<tr>
<td>C</td>
<td>192.0.0 to 254.255.255</td>
<td>1 to 254</td>
</tr>
</tbody>
</table>
Classed IP Addressing and the ARP

• Reserved addresses
  – Addresses starting with 127 is a loopback address
    • Never be used for addressing outside the host
  – A host number of all binary 1's indicates a directed broadcast over the specific network
    • E.g. 200.1.2.255 = a broadcast over network 200.1.2
  – A host number of 0 indicates "this host"
  – A network number of 0 indicates "this network"

• Reserved addresses severely reduce the available IP addresses from the theoretical maximum of 4.3 billion

• Most Internet users will be assigned addresses within Class C
  – Many networks with relatively fewer nodes
  – Address space is becoming very limited
  – Primary motivation for IPv6, which will have 128 bits of address space
Internal Network Addressing

- A small internal TCP/IP network consisting of one Ethernet segment and three nodes
  - The IP network number is 200.1.2.
  - The host numbers are 1, 2, and 3
  - These are Class C addresses (max of 254 nodes on this network segment)

Each node has a corresponding six byte Ethernet address
- Normally written in hexadecimal form separated by dashes, e.g. 02-FE-87-4A-8C-A9
Address Resolution Protocol (ARP)

• Node A needs to send a packet to node C
  – A knows C's IP address
  – The Address Resolution Protocol (ARP) is used for the dynamic discovery of C's Ethernet address

• ARP keeps an internal table of IP address and corresponding Ethernet address
  – The ARP module at node A does a lookup in its table on C's IP address
  – If this is the first transmission, the ARP will discover no entry
    • ARP will then broadcast a special request packet over the Ethernet segment
    • If the receiving node (node C) has the specified IP address, it will return its Ethernet address in a reply packet back to node A
    • Once node A receives this reply packet, the ARP module updates its table
    • Node A uses the Ethernet address to direct the packet to node C
    • ARP table entries
      – Stored statically
      – Stored with a time stamp so that old table entries are periodically flushed
Two Connected Ethernets

- Separate Ethernet networks that are joined by node C
  - Device C acts as an IP router between these two networks
  - A router chooses different paths for packets, based on IP addressing
  - The router will have more than one address as it is part of different network.
Two Connected Ethernets

- Each Ethernet segment has its own Class C network number
  - The router must know which network interface to use to reach a specific node
  - Each interface is assigned a network number.

- If A wants to send a packet to E, it must first send it to C who can then forward the packet to E
  - Accomplished by having A use C's Ethernet address, but E's IP address
  - C will receive a packet destined to E and will then forward it using E's Ethernet address

- If E was assigned the same network number as A
  - A would try to reach E by sending an ARP request and hoping for a reply
  - However, because E is on a different segment, it will never see the ARP request and never reply

- By specifying that E is on a different network
  - The IP module in A will know that E cannot be reached directly
  - Requires forwarding by some node on the same network