CHAPTER 1
Network Foundation

H. Peyravi
Department of Computer Science
Kent State University
Kent, Ohio 44242
peyravi@mcs.kent.edu
http://mars.mcs.kent.edu/~peyravi

Fall 2001
Contents

- Perspective
- Network Classifications
- Elements of a network (subnetworks)
- Performance
- Network Architecture
- Types of Services
- Internet Architecture
- ISO Architecture
- Network Interconnections
Perspective

■ Network users: services that their applications need e.g., guarantee that each message it sends will be delivered without error within a certain amount of time

■ Network designers: cost-effective design e.g., that network resources are efficiently utilized and fairly allocated to different users

■ Network providers: system that is easy to administer and manage e.g., that faults can be easily isolated and it is easy to account for usage

History

■ We have migrated from industrial revolution (18th century) to age of steam engine (19th century), and to information gathering, processing and distribution (20th century).

■ In computer era, we have migrated from a single computer serving all organizations to computer networks.
Computer Networks vs. Distributed Systems

- In Distributed Systems, multiple computers are transparent.
  - Users are unaware of underlying structure
  - Mostly OS issue
  - Nodes are generally under one organization control
- In Computer Networks, autonomous computers are interconnected.
  - Users specify the location of resources
  - Nodes are autonomous
- Nevertheless, there are a lot of overlaps between them.

Network Goals

- Resource sharing: factory automation at different locations.
- High reliability: having alternative resources.
- Saving money: small computers have better price/performance.
- Flexibility: Adding more processors as load increases.
- Using network as communications medium.
## Network Classifications

<table>
<thead>
<tr>
<th>Processors</th>
<th>Location</th>
<th>Distance</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit-board</td>
<td>0.1m</td>
<td>Data flow machine</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>1m</td>
<td>multiprocessors</td>
<td></td>
</tr>
<tr>
<td>Desk</td>
<td>10m</td>
<td>DAN</td>
<td></td>
</tr>
<tr>
<td>Building</td>
<td>100m</td>
<td>LAN</td>
<td></td>
</tr>
<tr>
<td>Campus</td>
<td>1Km</td>
<td>LAN</td>
<td></td>
</tr>
<tr>
<td>City</td>
<td>10Km</td>
<td>MAN</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>10Km</td>
<td>WAN (long haul)</td>
<td></td>
</tr>
<tr>
<td>Continent</td>
<td>1000Km</td>
<td>Long Haul</td>
<td></td>
</tr>
<tr>
<td>Planet</td>
<td>10,000Km</td>
<td>Long Haul</td>
<td></td>
</tr>
</tbody>
</table>

- Network exists whenever two or more elements interact with each other.
- A network is a set of nodes and links.
- Why networks
  - sharing resources such as databases or CPUs
  - interprocesses or interprocessor communications.
  - providing reliability using backup or redundancy (routing?)
  - distributed processing
  - furnishing central control (defense, inventory, sales)
  - to provide compatibility of dissimilar equipment
  - maximum performance at minimum cost.
■ Topological classification

► Static networks
  • 1-D (bus)
  • 2-D (tree, stars, rings, mesh, etc.)
  • multidimensional (cube, hypercubes)

► Dynamic networks
  • one or more switches are used.

■ Technological Classification

► Circuit-switching networks
  • dedicated paths are used between source and destination.
  • no queuing
  • example: telephone systems.

► Packet Switching
  • The message is divided into a number of slices called packets of certain fixed size.
  • Each packet has its destination address.
  • Queuing involved
  • Routing is needed
  • errors involved

► Message Switching
  • The network receives the entire messages, stores them in a secondary storage and transmit them.
  • It provides long term storage even after the message has been delivered.
Network Classifications

- **Non-Switching Networks.**
  - Broadcast networks
  - Single node, data processing (800).
  - Single node, data base management (library).

- Voice transmission is still the most common mode of communications.

- All projections indicate that voice will continue to be the heaviest communications.

- Telephone is still analog although it is extensively used for data transmission.

- Data signals must normally be converted to voice (analog) signals using modems.

- AT&T in early 1960s introduced digital carrier system T1
  - Consists of 24 channels at 64 Kbps per channel.
  - 1.544 Mbps.
  - US, Canada and Japan.

- CCITT has 30-voice channel at 2.048 Mbps (rest of the world).

- Many telephone carriers provide all digital transmission over selected portion of the network.

- the great interest is transmitting packetized voice in real time.

- Protocols are the building blocks (not buzzwords) of a complex system developed based on engineering principles.

- How these building blocks are glued together to construct a network?
They are constantly being redefined, extended, and replaced.

Why networks are designed the way they are?

Protocols

Exponential growth of Internet in recent years

- Software run on general purpose computers
- Easy to develop new software
- WWW is the popular application

Massive computational power of the hosts.

- A requirement to play back voice codes
Elements of a network (subnet networks)

- Sources: terminals, information processors, or network processors.
- Switches: relaying nodes, terminal controlling nodes, or Interface Message Processor (IMPs).
- Destinations: remote terminals, computers, or network processors.

Applications

- FTP
- WWW
  - Synonymous with the Internet
  - Set of clients and servers using the same language: Hyper Text Transfer Protocol (HTTP).
  - Graphic client programs (Web browser) such as Mosaic and Netscape
  - URL (uniform resource locator) is function of a Web browser that opens a location on the Web
  - URL displays index.html
- Network Video
  - Synonymous with the Internet
  - Require a special hardware (frame grabber) to decode images for standard TV, 352 \times 240 \textit{pixels} \times 24 \textit{bits}
Connectivity

- **Building Blocks**
  - links: coax cable, optical fiber...
  - nodes: general-purpose workstations...

- **Direct Links**
  - point-to-point
    - point-to-point network
  - multiple access
    - multiple access network
- Indirect Connectivity
  - switched networks

- internetworks
A network can be defined recursively as two or more nodes connected by a physical link, or by two or more networks connected by one or more nodes.

- **Switching Strategies**
  - circuit switching: dedicated circuit; send/receive a bit stream
  - packet switching: store-and-forward; send/receive messages (packets)

- **Addressing and Routing**
  - address: byte-string that identifies a node; usually unique
  - routing: process of determining how to forward messages towards the destination node based on its address
  - types of addresses
    - unicast: node-specific
    - broadcast: all nodes on the network
    - multicast: some subset of nodes on the network
Cost-Effective Resource Sharing

Must share (*multiplex*) network resources (nodes and links) among multiple users.

Common Multiplexing Strategies

- Time-Division Multiplexing (TDM) $\Rightarrow$ TDMA
- Frequency-Division Multiplexing (FDM) $\Rightarrow$ FDMA
- Code-Division Multiplexing (CDM) $\Rightarrow$ CDMA
- Wave-Division Multiplexing (WDM) $\Rightarrow$ WDMA
Statistical Multiplexing

- Time-division, but on demand rather than fixed
- Reschedule link on a per-packet basis
- Packets from different sources interleaved on the link
- Buffer packets that are *contending* for the link
- Packet queue may be processed FIFO, but not necessarily
- Buffer overflow is called *congestion*
The application programs running on the hosts connected to the network must be able to communicate in a meaningful way.

Network supports common process-to-process channels; e.g.,

- Request/Reply: for file access and digital libraries
- Message Stream: for video applications
  - video: sequence of frames
  - resolution: 1/4 TV-size image = 352x240 pixels;
  - 24-bit color: frame = (352 x 240 x 24)/8 = 247.5KB;
  - frame rate: 30 fps = 7500KBps = 60Mbps
  - video on-demand versus video-conferencing
What Could Go Wrong in a Network?

- Bit-level errors (electrical interference)
- Packet-level errors (congestion)
- Link and node failures
- Messages are delayed
- Messages are deliver out-of-order
- Third parties eavesdrop

The key problem is to fill in the gap between what applications expect and what the underlying technology provides.
Performance

- Bandwidth (throughput)
  - Amount of data that can be transmitted per time unit
  - Example: 10Mbps
  - link versus end-to-end
  - Notation
    - KB = $2^{10}$ bytes
    - Mbps = $10^6$ bits per second
  - Bandwidth related to “bit width”

\[
\begin{align*}
1 \text{Mbps} & \quad \text{(each bit 1 microseconds wide)} \\
2 \text{Mbps} & \quad \text{(each bit 0.5 microseconds wide)}
\end{align*}
\]
Latency (delay)

- Time it takes to send message from point A to point B
- Example: 24 milliseconds (ms)
- Sometimes interested in round-trip time (RTT)

Components of latency

\[
\text{Latency} = \text{Propagation} + \text{Transmit} + \text{Queue}
\]

- Propagation = Distance / SpeedOfLight
- Transmit = Size / Bandwidth

Speed of light

- \(3.0 \times 10^8\) meters/second in a vacuum
- \(2.3 \times 10^8\) meters/second in a cable
- \(2.0 \times 10^8\) meters/second in a fiber

Notes

- no queuing delays in direct link
- bandwidth not relevant if Size = 1 bit
- process-to-process latency includes software overhead
- software overhead can dominate when Distance is small

Relative importance of bandwidth and latency

- small message (e.g., 1 byte): 1ms vs 100ms dominates 1Mbps vs 100Mbps
- large message (e.g., 25 MB): 1Mbps vs 100Mbps dominates 1ms vs 100ms
Example: 100ms RTT and 45Mbps Bandwidth = 560 KB of data

Application Needs

- bandwidth requirements: burst versus peak rate
- jitter: variance in latency (inter-packet gap)
When two humans engage in a dialog, communication takes place at three levels:

- Cognitive level: some level of understanding
- Language level: no longer concerned with the subject.
- Transmission level: neither the concept nor the language is important (physical means).

A network consists of a series of levels called layers.

A protocol is the rule of conversation; each layer has its own protocol.

An example in human speech is: don’t interrupt when somebody speaks.

Another example is return address on regular mail.

Each computer and/or each application program in the computer may require a different communication access method and protocol.

- Setup a session through the network.
- They must agree on the format.
- Terminals must be able to regulate data rates.
- Packets may arrive out of order.
Layered Architecture

- IBM SNA was one of first layered architecture, and ISO is rapidly becoming and International standard.
- Protocols must appear in every network node.
- The bottom 3 layers of ISO provide network services and the upper 4 layers provide services to the end users.

ISO/OSI Reference Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>ftp, e-mail rlogin</td>
</tr>
<tr>
<td>Presentation</td>
<td>ASCII text, sound</td>
</tr>
<tr>
<td>Session</td>
<td>Establish/manage connection</td>
</tr>
<tr>
<td>Transport</td>
<td>End-to-end communication: TCP</td>
</tr>
<tr>
<td>Network</td>
<td>Routing, Addressing: IP</td>
</tr>
<tr>
<td>Datalink</td>
<td>Two part communication: Ethernet</td>
</tr>
<tr>
<td>Physical</td>
<td>How to transmit signal: Coding</td>
</tr>
</tbody>
</table>
1. Physical Layer
   - performs direct transmission of logical information into physical phenomena (electronic pulses).
   - modulators/demodulators are used at this layer.

2. Data Link Layer
   - makes sure that the message indeed reach the other end without corruption (signal distortion and noise).
   - acknowledgments
   - detect duplications.
   - timers for retransmission.

3. Network Layer
   - controls routes for individual message through the actual topology.
   - finds the best route.
   - finds alternate routes.
   - buffering and deadlock handling.

4. Transport Layer
   - locates the other party
   - creates a transport pipe between both end-users.
   - breaking the message into packets and reassembling them at the destination.
   - applies flow control to the packet stream.
5. Session Layer

- is responsible for the relation between two end-users.
- maintains the integrity and controls the data exchanged between the end-users.
- the end-users are aware of each other when the relation is established (synchronization).
- it uses naming and addressing to identify a particular user.
- makes sure that the lower layer guarantees delivering the message (flow control).

6. Presentation Layer

- it translates the language used by the application layer.
- it makes the users as independent as possible, then they can concentrate on conversation.

7. Application Layer (end users)

- where they process information that is being exchanged.
- the users don’t want to be aware of the mechanism of the network.
- The users shouldn’t be bothered by each other’s language.
Advantages of Layered Architecture

- Any given layer can be modified or upgraded without effecting the other layers.
- Modulazition by means of layering simplifies the overall design.
- Different layers can be assigned to different standards, committees, and design teams.
- Different mechanisms (packet-switching, circuit-switching) may be used without effecting more than one layer.
- Different machines may be plugged in at different layers.
- The relation between different control functions can be better understood.
- Common lower levels may be shared by different higher levels.
- Functions (especially at lower levels) may be removed from software to hardware and microcodes.
- Increases the compatibility of different machines.

Disadvantages of Layered Architecture

- Total overhead is higher.
- Two communicating machines may have to use certain functions which they could do without layers.
- As technology changes, the functions may not be in the most cost-effective layer.
**OSI Terminology**

- **Entities**: active elements in each layer is called entities:
  - software: such as a process
  - software: such as I/O chips
- **Peer Entities**: entities in the same layer on different machines.
- Entities in layer \( N \) implement a service used by layer \( N + 1 \). Layer \( N \) is called service provider, and layer \( N + 1 \) is called service user.
- Services are available at Service Access Points (SAPs)
  - SAPs in telephone systems are sockets
  - SAP addresses are the telephone numbers of these sockets.
  - SAP addresses in postal service are P.O. box numbers.
  - In Berkeley UNIX, SAPs are sockets, and SAP addresses are socket numbers.
- At a typical interface (SAP point) between layer \( N \) and layer \( N + 1 \)
  - layer \( N + 1 \) passes an *IDU* (Interface Data Unit) to layer \( N \) entity through the SAP
  - *IDU* consists of *ICI* (Interface Control Information) and *SDU* (Service Data Unit).
  - In order to transfer the *SDU*, layer \( N \) may have to fragment it to several pieces, each with a header called *PDU* (protocol Data Unit).
Types of Services

- **Connection-oriented**
  - Reliable
  - Message Sequence
  - Unreliable

- **Datagram**
  - Reliable
  - Acknowledged
  - Request-Reply
  - Unreliable

- **Byte stream**: User message boundaries are not preserved
- **Request-reply**: The reply serves as an acknowledgement as well
- **Message oriented or byte oriented approach** can be used for unreliable connection-oriented communication
Service Orientations

- Connection-oriented services
  - the sender pushes objects in at one end and the receiver collects them in the same order at the other end.
  - it was modeled after the telephone system.

- Connectionless-oriented services
  - it was modeled after the postal service
  - packet could take independent routes
  - packet could be received out of order collects them in the same order at the other end.
  - datagrams

- Request-Reply services
  - sender transmits a single datagram containing a request, the reply contains the answer.
Quality of Services

- Some reliable services use acknowledgments and hence overheads.
- File Transfer is a reliable connection oriented service.
- Reliable connection-oriented service has two variations:
  - message sequence: message boundaries are preserved.
  - byte streams: no message boundary are preserved.
- In some connection-oriented services the delay introduced by the ACKs are unacceptable (digitized voice traffic). Some level of noise is tolerable.
Service Primitives (operations)

- The primitives tell to perform some action or report on an action taken by a peer entity.

- OSI primitives can be divided into four classes
  1. **request**: An entity wants the service to do some work.
  2. **indication**: An entity is to be informed about an event.
  3. **response**: An entity wants to respond to an event.
  4. **confirm**: An entity is to be informed about its request.

- Services and protocols are distinct concepts:
  - services are set of primitives that a layer provide to the layer above it.
  - services relate to an interface between two layers.
  - services are abstract data types.
  - protocols are set of rules governing the format and meaning of the frames, packets or messages.
  - protocols are implementations of the services data types.
  - entities use protocols in order to implement services.

- Unfortunately, OSI does not distinguish between these two.
Network Standardization

- In the early days, different vendors had different networks.
- Standards fall into two categories:
  - De facto standard
    - have just happened without formal plan.
    - IBM PC, UNIX, DOS.
  - De Jure standard (by law)
    - formal legal standards
- De Jure standards are two classes.
  - those established by treaty among national governments,
  - voluntary non-treaty organizations.
Internet Architecture

- Defined by Internet Engineering Task Force (IETF)

- Another view
**TCP vs. OSI**

TCP/IP Ref. Model
- Application
- Transport
- Internetwork
- Host to Network

TCP/IP Protocols
- FTP
- HTTP
- NV
- TFTP
- TCP
- UDP
- IP
- Ethernet
- Token
- FDDI

OSI Ref. Model
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

**Internetworking**

Application A
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Application B
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical