Summary Computer Networks I: complete - Notes

Computer Networks I (University of Queensland)

Lecture 1 - Network Models

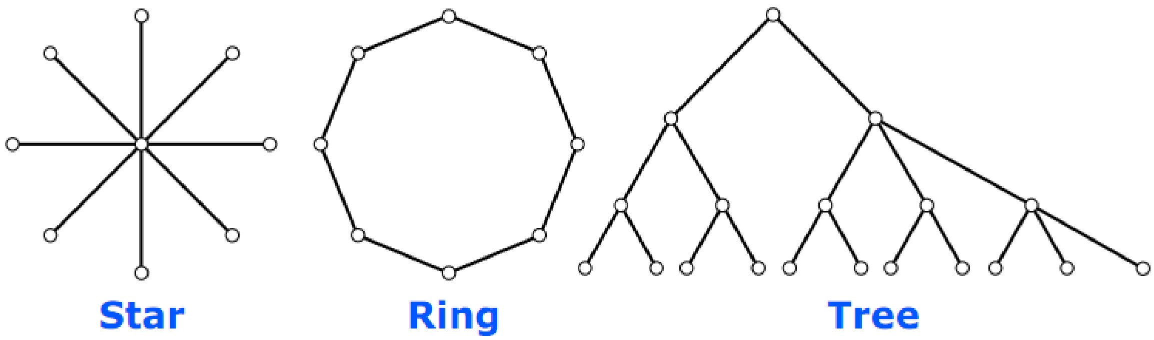
Networks provide connectivity between nodes over a link

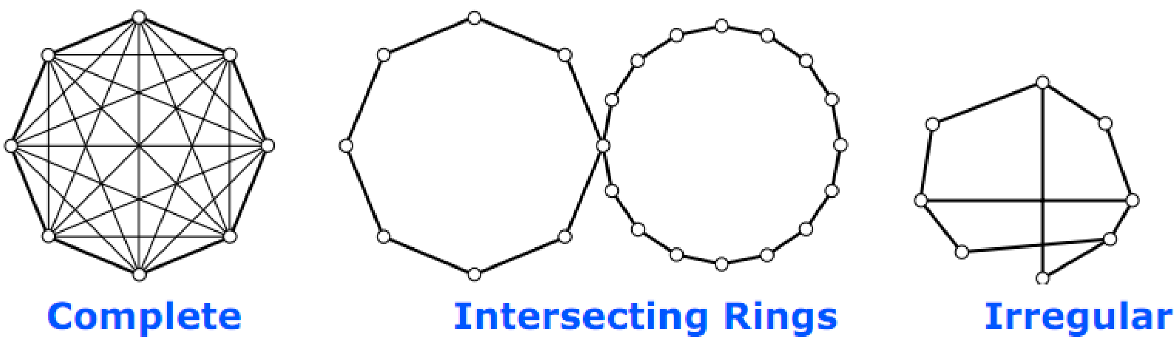
Node: hosts (computers and other devices)

Link: physical medium

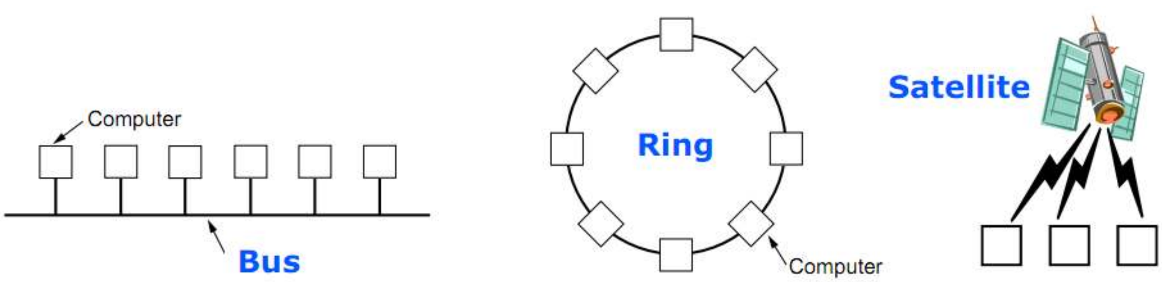
Point-to-Point Networks: pairs of nodes linked together (store-and-forward, packet-switched)

Packets sent from origin router to destination router via intermediate routers.





Broadcast Networks: Single channel shared by all hosts



Network: interconnected collection of computers
Distributed systems: Multiple computers not visible to users

Protocol: Procedures designed to achieve higher purpose
- *Syntax: Data format, signal levels*
- *Semantics: Meaning of data*
- *Timing: Speed matching, sequencing*

Protocol Hierarchies: Networks are organised as a series of layers, to offer services to higher layers, and to shield higher layers from implementation details.

Connection-Orientated: Establishes conn, uses conn, releases conn

Connectionless: contains full destination, no connection

Reliability: can be reliable or unreliable
- *Reliable: receiver acknowledges receipt*
- *Unreliable: no acknowledgement required*

OSI Reference Model: Open systems interconnection
1. *Physical Layer: Bit transmission*
2. *Data-Link Layer: Reliable transmission of frames*
3. *Network Layer: Routing of packets*
4. *Transport Layer: End-to-end communication*
5. *Session Layer: Allows users to establish connection*
6. *Presentation Layer: Data representation*
7. *Application Layer: Providing services to end-user*

Provide issues with each

TCP/IP Reference Model: from ARPANET, named after two primary protocols.
- *Layers: Only has layers 2, 3, 4 and 7 from OSI model*

We use layers 1, 2, 3, 4 and 5 for our representation.

Lecture 2 - Interprocess Communication

Interprocess Communication (IPC): four different ways

Shared memory

Message passing

Remote Procedure Calls (RPC)

Transactions

Message Passing: Two primitives, send or receive

Can be blocking(synchronous) or non-blocking (asynchronous)

Lecture 3 - TCP/UDP

Transport options

UDP – User Datagram Protocol (Unreliable)
TCP – Transmission Control Protocol (Reliable)

IP and data link are not reliable.

Socket = IP and port

UDP – Connectionless

Eight byte header
Source port, destination port, UDP length, UDP checksum

UDP Main Points

Don't care about packet loss (streaming)
Small messages and reliable networks
No flow control
Simple implementation

TCP Main Points

Connection orientated
Reliable
Byte stream
Full Duplex
Point to point

Port Number

16 bits (0 – 65535)
Below 1024 are well known ports (eg. 80 – HTTP)

TCP Protocol

Exchanges segments
20 byte header plus data
Size limited by IP packet size (max 65535) and MTU (Max Transfer Unit) (1500 bytes for Ethernet)

TCP Segment header

Source port (16 bits)
Destination port (16 bits)
Sequence Number (32 bit)
ACK number (32 bit)

TCP header length (4 bits, number of 32 b it words in header, usually 5)
6 unused bits
TCP header flags (each on bit)
Urgent pointer
ACK
PSH – pushed data, do not buffer
RST – reset connection, aborted or refused
SYN – synchronise sequence numbers
FIN – finished sending data
Advertised windows – available buffer size for receiving data
Urgent pointer – byte offset to where urgent data is found

TCP and UDP Checksum Header
Calculated on partial header and data
Compulsory for TCP, optional for UDP

Connection Establishment
-> SYN (SEQ = X)
<- SYN/ACK (SEQ = Y, ACK = X + 1)
-> ACK (SEQ = X + 1, ACK Y + 1)

Sliding Window Protocol
Flow control
Transport and data link layer
Transport layer – dynamic window
Data link layer – static window
Can have multiple unACK'ed messages
Upper bound is the window
Blocks when full, receives when not full

Flow control
Regulates flow of messages

Congestion Control
Fixes congestion (lost packets)

TCP Bad for new Technologies
High bandwidth, long distance, long delay
Range of sequence numbers too small
Wireless packet loss treated as congestion

Sequence Number Wrap Around

Bandwidth	*Time Until Wrap Around*

T1 (1.5 Mbps)	*6.4 hours*
Ethernet (10 Mbps)	*57 minutes*
T3 (45 Mbps)	*13 minutes*
FDDI (100 Mbps)	*6 minutes*
STS-3 (155 Mbps)	*4 minutes*
STS-12 (622 Mbps)	*55 seconds*
STS-24 (1.2 Gbps)	*28 seconds*

Maximum segment life (MSL) is assumed to be 120 seconds

Lecture 4 - Physical Layer

Physical Layer

Responsible for transmission of raw bit streams

Guided – fiber optical cables
Unguided – Radio

Channel Sharing

Simplex (one way)
Half duplex (two way, one at a time)
Full duplex

Time Varying Signals

Discrete (digital)
Continuous (analog)

Spectrum

Range of frequencies

Bandwidth

Width of spectrum (absolute)
Effective bandwidth (where most of the energy is contained)

Data Rate

Measured in bits per second (bps)

Bandwidth

Measured in Hertz (Hz)
Higher data rate implies larger bandwidth

Signal Strength

Signal is attenuated during transmission
Signal strength is measured in Decibels (dB)

$$Power \in dB = 10\log_{10}(P_1/P_2)$$

Voice Grade Telephone

Frequency band - 200 to 3200Hz
Bandwidth – 3kHz

Maximum Data rate of channel (Nyquist Theorem)

$$C = 2W\log_2 M$$

$W = bandwidth$
$M = Levels\ per\ signal$

Shannon's Theorem

SNR – Signal to Noise Ratio

$C = W \log_2(1 + S/N)$

S/N *must not be in dB*

Modulation

AM (Amplitude Modulation)
FM (Frequency Modulation)
PM (Phase Modulation)
Can have different combinations

Baud Rate

Symbol rate (Symbols per second)

Bit Rate

Bit rate does not equal baud rate
Bit rate = baud rate × bits per symbol
Bits per symbol = log2(number of symbols)

QPSK – Quadrature Phase Shift Keying

Constellation pattern
Angle represents phase of signal
Distance from (0,0) represents amplitude
QPSK – only phase is varied

Multiplexing

TDM – Time Division Multiplexing
  Users allocated bandwidth
FDM – Frequency Division Multiplexing
  Each channel gets a different frequency
WDM – Wavelength Division Multiplexing
  Each channel gets a different wavelength (fiber optics)
CDMA – Code Division Multiple Access
  Codes used to separate signals (mobile phone networks)

End to End Delay

Circuit switching
  Time = call time + propagation delay + transmission time
Message Switching
  Time = k × (propagation delay per hop + transmission delay)

k is the number of hops

Analogue to Digital Conversion

- *Sampling*
  - *Measure signal amplitude at regular times (PAM)*
- *Quantisation*
  - *Convert measured amplitude into discrete levels*
- *Encoding*
  - *Pulse Code Modulation*
  - *Encode the levels as a n-bit signal using binary signaling*

Lecture 5 - Data Link Layer

Link Layer

Send data between adjacent nodes

Overcomes deficiencies of physical layer

Framing

Breaks sequence of bits into frames

Sentinel based

Byte stuffing, bit stuffing

Counter Based

Clock Based

Coding violation

Character stuffing

For each accidental DLE in payload, another DLE is inserted

Escape at front and end as well

Bit Stuffing

Insert 0 after five consecutive 1's (vice versa)

Remove from data when received

Counter based

Include length in header

Clock based

Equal time for frames

Coding violation

Every bit is encoded as a pair of bits

Parity Error Checking

Even parity – Parity bit set so that the total number of 1's is even.

Odd parity – Parity bit is set so the total number of 1's is odd.

Can detect single bit errors and any odd number of bit errors.

Error detection codes

R – redundant checksum data

M – message size

N – length of message M + R

M/N – Code Rate

The lower the mn/ the higher the overhead of the code

We want r << m

Hamming Distance

The number of bits two words differ by

The hamming distance of a code is the minimum difference between any two code words

A code with hamming distance d can detect up to d – 1 single bit errors.

CRC Check

Represent m message as m – 1 degree polynomial

Append m – 1 bits to the end of the data

If MSB is 1 then subtract polynomial from data

If 0 then subtract 0

Reliable Delivery

ARQ – Automatic Repeat Request

Stop and Wait

Send than wait for ACK

Sender adds sequence number to every frame

Each ACK contains sequence number of the frame it acknowledges

Uses ACK NAK

Only needs 0 and 1's for sequence numbers

Performance of Stop and Wait

f: frame size in bits

b: data rate of channel [bps]

d: propagation delay [s] (d≈5ms per 1000km)

u: line utilization

Total time to send a frame = d + f/b + d

*Line Utilisation = u = f/b / (2d + f/b) = f / (2d*b + f)*

Sliding Window

Allows multiple outstanding unpacked frames

Go-Back-N

Out of order packets are discarded

Selective Repeat

Repeats sending or individual NAKed packets

Requires larger receiver buffer

Sequence Numbers

Must not run out of then

Comparison

Go-Back-N	*Selective Repeat*

Used in standard TCP *Requires small buffer* *Wastes bandwidth*	*More efficient* *Requires larger buffer*

Lecture 6 - Medium Access Layer

MAC Sub layer

CD – Collision Detect

CA – Collision Advoidance

CS – Carrier Sense

Slotted – Only start transmitting at certain times

Poisson Process

Probability of k frame transmission attempts within time interval t is

Formula

Persistent CSMA

Persistent carrier sense multiple access

Will transmit at first quiet period

Non-Persistent CSMA

Will wait a random time before CS

Long delay at light loads

CSMA/CD

Only senses well when propagation between furthest stations are far

Collision Free Protocols – Bit Map Method

Contention period between each transmission period

MACA (Multiple Access with Collision Avoidance)

Sender broadcasts RTS (request to send)

Receiver replies with CTS (Clear to send)

Lecture 7 - Medium Access Sublayer, Internetworking

Manchester Encoding

1 - high to low transition
0 - low to high transition
Every bit has a transition in the middle

802.3 MAC Sublayer Protocol

7 bytes preamble 10101010
Start of frame delimiter (1 byte) 10101011
6 bytes for destination address
6 bytes for source address
2 bytes for number of bytes in data field (length 0 - 1500)
Data (0 - 1500)
Padding
4 Byte CRC checksum

Stuff about various standards goes here

Interconnection devices

Layer	*Device*
Application Layer	*Application gateway*
Transport Layer	*Transport gateway*
Network Layer	*Router*
Data Link Layer	*Bridge, switch*
Physical Layer	*Repeater, Hub*

Stuff in devices goes here

Virtual LANs

more goes here

Datagram VS Virual-Circuit Network

Internet *Data exchange between computers* *No strict timing* *Delivery order/timing not guaranteed* *Complexity on edges of network*	*ATM* *Evolved for telephony* *Human conversation* *Strict requirements* *Complexity inside network*

Lecture 8 - Network Layer: IP, routing

Tier 1

Backbone
International coverage
Treat each other as equals
622Mbps - 10Gbps
connected to all other T1's

Tier 2

Smaller regional ISP's
Connects to at least one T1 and possibly other T2's

Tier 3

Last hop network

IETF

Governing body for internet standards
Standards published as Request for Comments (RFC)
RFC's numbered in order of publication

Internet

Collection of Subnetworks
BGP - Border gateway protocol used to exchange routing information
Quasi-hierarchical
Governed by Internet Engineering Task Force (IETF)
  Publishes standards as request for comments

IP Header Fields

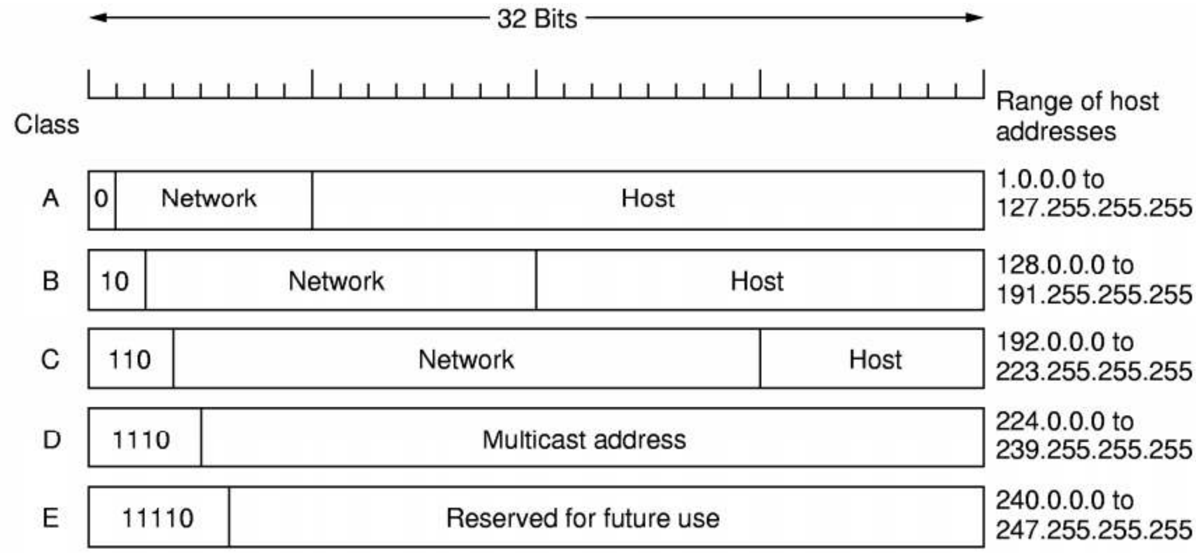
IP Datagram

IP Version
Header length
Type
Total datagram length
16-bit identifier - for fragmentation
flag - for fragmentation
fragmentation offset - for fragmentation
Time to live
Upper layer protocol to deliver payload to
Source IP
Destination IP
Options
Data
Size of fragments should be a multiple of 8, except for the last fragment

IP Addressing

32-bit identifier

IP Address Classes



All zeroes means this host
All ones means broadcast
A - up to 126 (2^7 - 2) networks
16 million hosts each
B has up to 16382 networks with 64000 hosts each
C has up to 2 million networks with 254 hosts each

Hierarchical Address Space
With a flat address space, each router would need to know about everything.
Routing algorithms would be too complex
Subnets are just another level of hierarchy added inside algorithms

DHCP
Assigns IP on receiving a "DHCP DISCOVER" form a host
Assigned for certain amount of time before it expires, then needs to request renewal

ICANN
Internet Corporation for Assigned Names and Numbers
Allocates IP addresses.
Manages DNS
Assigns domain names and resolves disputes

NAT - Network Address Translation
Only one public address is used while hosts use a private IP
Uses a Network address translation table

ICMP - Internet Control Message Protocol

Used by hosts and routers to communicate network-level information

Encapsulated in IP datagrams

Typically 56 bytes

Lecture 9 - Network Layer: Routing, Multicast

Routing

Should be distributed and dynamic

Intra-domain Routing

Within a domain where all routers are under the same administrative control

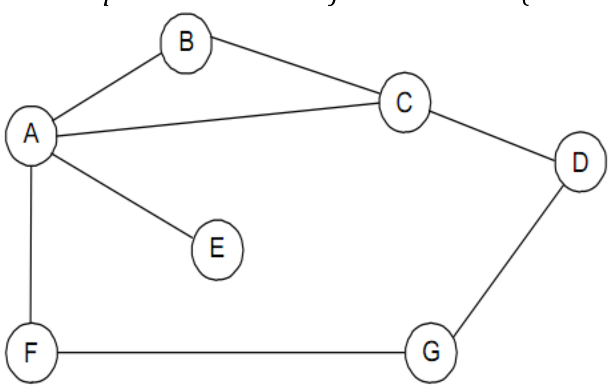
Uses Interior Gateway Protocols (IGPs)

Distance Vector Routing

Each node contains a triple of (Destination, Cost, NextHop)

Updates are exchanged with directly connected neighbours periodically, or when changes occur.

Updates local table if a better route (smaller cost and came from nexthop) is received



Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Can cause convert to infinity problems

Don't send back to neighbours what they told you

Interior Gateway Routing Protocol (IGRP)

Link State Routing

Link state packet is generated by each node

Contains:

ID of the node that created it

Cost of link to each directly connected neighbour

Sequence number

Time to live for this packet

Dijkstra's Algorithm

Start with node S

Permanently label S with [0,S]

Tentatively label others (infinity, -)

Make node S the working node n_w

Repeat until all nodes are permanently labelled

For Each tentatively labelled node (n) next to n_w calculate

d = cost to n_w + distance from n to n_w

if d < n's tentative distance then tentatively relabe to (d, n_w)

Of all the tentatively labelled nodes select the one with the least cost make its label permanent and make it the working node

Lecture 10 - Multimedia Protocols

QOS

Network provides application woith leveks of performance needed for application to function

QOS Parameters

- *Data Rate*
- *Delay*
- *Jitter*
- *Reliability*
  - *Bit error rate*
  - *Packet error rate*

Streaming Multimedia Applications

- *Delays sensitive*
- *Loss tolerant (opposite of normal data)*

RTSP - Real Time Streaming Protocol

Protocol used to stream interactive media (flow control)

Lecture 11 - Quality of Service

QOS Considerations (Internet Evolution)

- *Laissez -Faire*
  - *No major changes, more bandwidth when required*
- *Integrated Service Philosophy*
  - *Fundamental changes so that apps can reserver end-to-end bandwidth*
- *Differential Services Philosophy*
  - *Create classes for data service*

RTP - Real-Time Protocol

- *Specifies a packet structure for packets carrying audio and video data*
- *Encapsulated in UDP segments*
- *Contains*
  - *Payload type*
  - *Packet sequence number*
  - *Timestamp*
  - *Streams Source*

RTCP - Real Time Control Protocol

- *Evaluates peformance and control performance*

Approches to QOS

- *Overprovisioning*
- *Resource reservation*
- *Service classes*
- *Traffic engineering*

Techniques for achieving QOS

- *Buffering*
- *Traffic shpaing*
- *Traffic Policing*
- *Packet scheduling*
- *Admission control*

Lecture 12 - Network Security

Phishing

Fraudulently collecting data by pretending to be someone else

Social Engineering

A method to trick people into revealing passwords or other information

Confidentiality

Only sender and receiver should be able to understand message contents

Authenication

Sender and receiver want to confirm identity of each other

Message Integrity

Insuring the message hasn't been tampered with

Non-repudiation

Ensuring that users cannot deny the occurrence of particular events