Department of Computer Science and Software Engineering

The University of Melbourne

433-522 Internet Technologies

Course Notes

Contents

Lecture I
Network Fundamentals

Computer Networks

What is a Network? §1

- Network (Noun):
  - An intricately connected system of things or people.
  - An interconnected or intersecting configuration or system of components.
- Computer Network:
  - A data network with computers at one or more of the nodes. [Oxford Dictionary of Computing]
  - A collection of autonomous computers interconnected by a single technology.

What are the Internet and the World Wide Web? §1

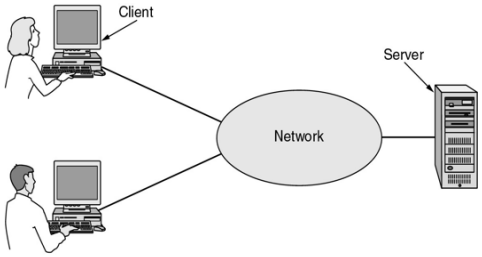
- Neither the internet nor the WWW is a computer network!
- Simple answers:
  - The internet is not a single network but a network of networks!
  - The WWW is a distributed system that runs on top of the internet

Uses of Computer Networks §1.1

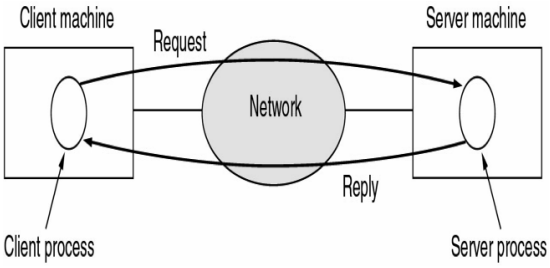
- Business Applications
- Home Applications
- Mobile Users
- Social Issues

How many different types of networks have you used?

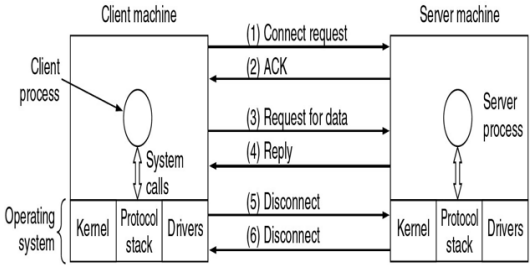
A Simple Client-Server Network §1.1.1



Requests/Replies in a Client-Server Model §1.1.1



Simple Client-Server Interaction §1.1.1

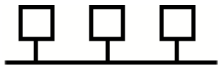


Network Types

Network Types §1.2

- Local Area Networks
- Metropolitan Area Networks
- Wide Area Networks
- Wireless Networks
- Internetworks

Differentiating Factors of Networks §1.2

- Transmission Type
  - Broadcast links 
    - Broadcast networks have a single communication channel shared by all machines on a network. Packets sent by any machine are received by all others, an address field in the packet specifies the intended recipient. Intended recipients process the packet contents, others simply ignore it.
    - Broadcasting is a mode of operation which allows a packet to be transmitted that every machine must process.
    - Multicasting is a mode of operation which allows a subset of machines to process a given packet.

Differentiating Factors of Networks §1.2

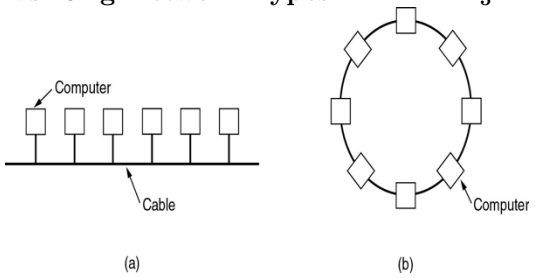
- Transmission Type cont
  - Point-to-point links 
    - Point to point networks consist of many connections between individual pairs of machines. Packets traveling from source to destination must visit intermediate machines to determine a route - often multiple routes of variant efficiencies are available and optimisation is an important principle.
  - Unicasting is the term used where point-to-point networks with a single sender and receiver pair can exchange data.
- Scale

Local Area Networks §1.2.1

Distinguished by 3 factors

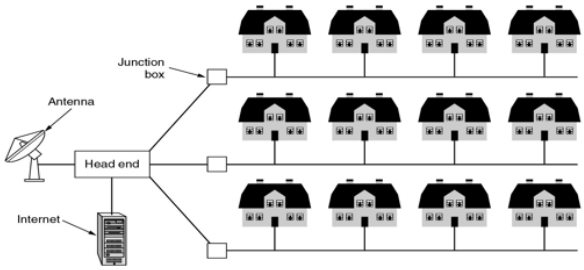
- Size
  - Worst-case transmission time can be predicted in advance
- Transmission Technology
  - Physically wired network
- Topology
  - Bus
    - only a single machine on the network can transmit at any point in time
    - requires a negotation mechanism to resolve transmission conflicts
    - Ethernet (IEEE 802.3) is the most common bus network
  - Ring
    - Each transmission bit is propagated individually
    - Requires access control to resolve propagation queuing
    - Token Ring (outdated), FDDI is the most common ring network type

Bus vs Ring Network Types §1.2.1



Metropolitan Area Networks (MAN) §1.2.2

- Coverage typically larger than a LAN
- Cable TV networks are a prime example

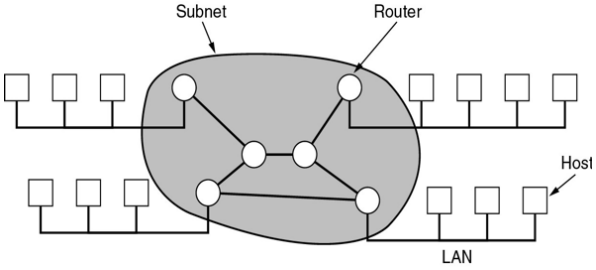


Wide Area Networks §1.2.3

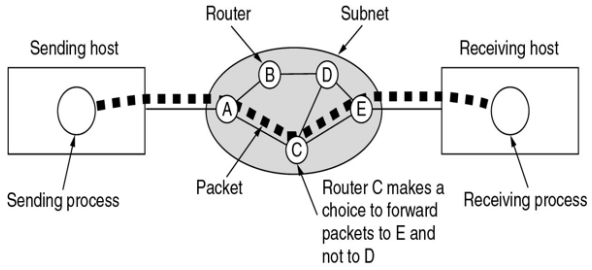
- Large scale geographical coverage - cities, states, countries
- Typically a single network provider is used across the WAN, although aggregation models are increasingly common
- WANs feature multiple hosts, typically owned by non-network providers

- WANs also feature multiple subnetworks, including different transmission types and a range of routing and switching infrastructure

LANs and Subnets on a WAN §1.2.3



Packet Switching on a WAN §1.2.3



Types of Wireless Networks §1.2.4

- System Interconnection
  - Short range radio (< 10m)
  - Low bandwidth (-100Kbps)
  - Numerous technologies including Infrared (IR), Bluetooth ...
- Wireless LAN
  - Longer range radio (typically 100-200m, but up to 3-4km with the right equipment)
  - Moderate bandwidth (1-54Mbps)
  - Requires transmission and reception devices
  - 802.11 family is the most common

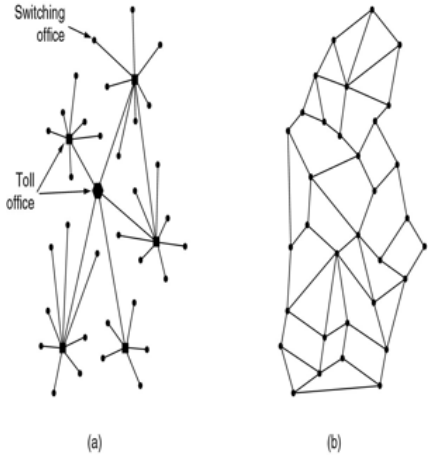
The Internet

The Internet §1.5.1

- The Internet is composed of the aggregation of many smaller networks - not a single network or under a single point of control
- Historically, the Internet developed in 3 distinct phases
  - ARPANET (1960's - early 1970's)
  - NSFNET (1970's - early 1980's)
  - Internet (1980's - present)

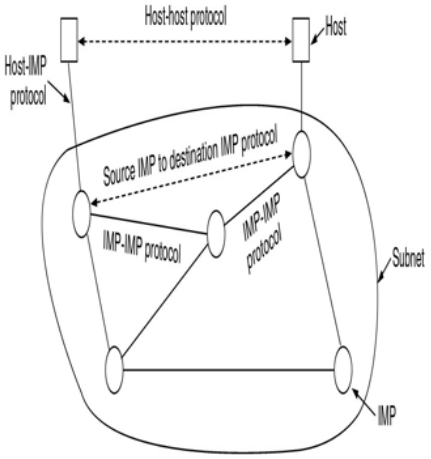
Network Topology Prior to ARPANET §1.5.1

- In (a), the traditional topology of a telephone network, primarily hierarchical with many single points of failure, characteristic of networks prior to the late 1960's
- For primarily military purposes, a high degree of fault tolerance was desirable, hence single points of failure need to be eliminated
- ARPANET design (b) included a distributed, redundant switching and routing infrastructure to address these weaknesses

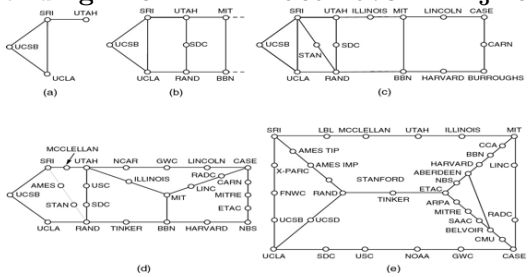


Layers in ARPANET's Network Design §1.5.1

- The basic unit of ARPANET was the IMP (Interface Message Processors) - each connected to at least 2 other IMPs
- At each node, an IMP and a single host were connected - the host generated or collected messages and passed them to the IMP for transmission
- IMP software was split into host and network components



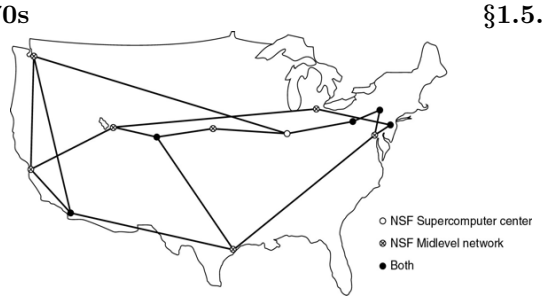
Expanding ARPANET 1969-1973 §1.5.1



Significant ARPANET Contributions §1.5.1

- In addition to geographical growth, ARPA funded transmission research to allow multiple transmission methods to be utilised to transfer packets eg radio waves in combination with copper wires.
- Protocols
  - Cerf and Kahn (1974) designed the TCP/IP model to allow communication using a single protocol stack over multiple interoperable network types. The TCP/IP model still underlies the Internet we use today.
- Software
  - Entities such as as BBN and UCB built protocol support into computer operating systems, notably Berkeley Unix. These basic protocol stacks are still used by modern operating systems.

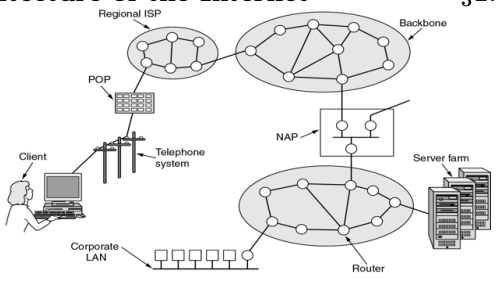
Strategic Network Backbones: NSFNet in the 1970s §1.5.1



Towards the Internet §1.5.1

- Privatisation of telecommunications infrastructures (particularly Network Access Points (NAPs) in the USA in the 1970s and 1980s allowed commercial providers to build internetworks
- The widespread adoption of the TCP/IP protocol stack ensured these networks and associated developments were interoperable regardless of who built them
- From 1970 until around 1990, there were only a small number of Internet applications - email, news, remote login, file transfer
- In the early 1990's the invention of the WWW, an application and protocol stack which built on TCP/IP, together with a GUI by which to navigate connected resources, massively promoted the use of the Internet by non-academic users.
- In the mid 1990's, growth fuelled by ISP's who offered individual users the ability to connect to their networks via a modem, and thus connect to the Internet.

Architecture of the Internet §1.5.1



Lecture II
Network Architecture Models

Protocols, Layers and Services

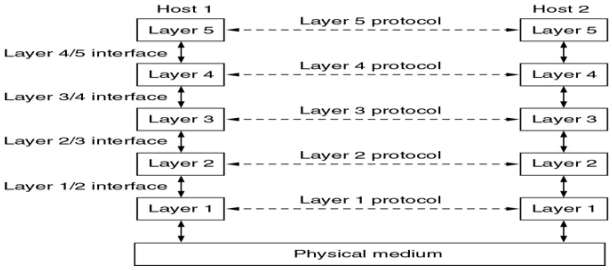
Protocol Hierarchies

Network Hierarchies §1.3.1

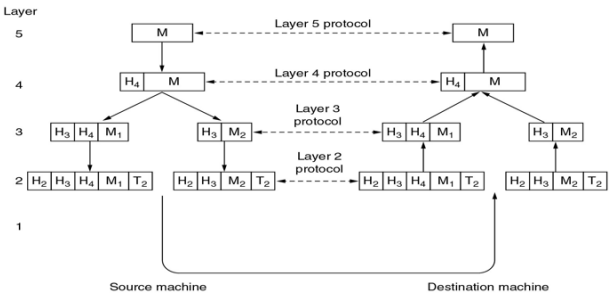
- Consider the network as a stack of layers
- Each layer offers services to layers above it
- Inter-layer exchanges are conducted according to a protocol

Design of Layer Models

Layers, Protocols and Interfaces §1.3.1



Protocol Hierarchies §1.3.1



Connection-Oriented and Connectionless Services

Connection-Oriented and Connectionless Services §1.3.3

- Connection Oriented: connect, use, disconnect (similar to telephone service)
  - Negotiation inherent in connection setup
- Connectionless: use (similar to postal service)
- Choice of service type has a corresponding impact on the reliability and quality of the service itself

Types of Service §1.3.3

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Services Primitives

Service Primitives §1.3.4

- Primitives are a formal set of operations for services
- The number and type of primitives in any particular context is dependent on nature of service itself - in general more complex services require more primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Services and Protocols

Relationship of Services and Protocols §1.3.5

- Service = set of primitives that a layer provides to a layer above it
  - interfaces between layers
- Protocol = rules which govern the format and meaning of packets that are exchanged by peers within a layer
  - Packets sent between peer entities

Network Reference Models

Reference Models §1.4

- OSI Reference Model
- TCP/IP Reference Model
- OSI and TCP/IP Compared
- OSI Model Critique
- TCP/IP Model Critique

Why do we need a network reference model? §1.4

- A reference model provides a common baseline for the development of many services and protocols by independent parties
- Since networks are multi-dimensional, a reference model can serve to simplify the design process
- It's engineering best practice to have an abstract reference model, and a reference model and corresponding implementations are always required for validation purposes

Open Systems Interconnect

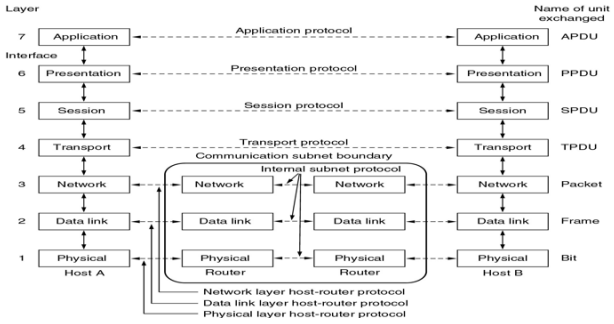
OSI Reference Model §1.4.1

- Open Systems Interconnection (OSI)
- ISO, Day (1995)
- 7 layers
- Layer divisions based on principled decisions

OSI Layer Division Principles §1.4.1

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well defined function
- The function of each layer should be chosen with a view toward defining internationally standardised protocols
- The layer boundaries should be chosen to minimise the information flow across the interfaces
- The number of layers should be large enough that distinct functions need not to be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

OSI Model Illustrated §1.4.1

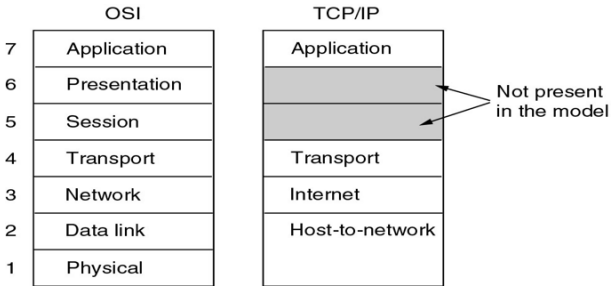


TCP/IP

TCP/IP Reference Model §1.4.2

- Transmission Control Protocol/Internet Protocol
- Cerf & Kahn (1974)
- Infrastructure independent
- 4 layers

TCP/IP Model Illustrated §1.4.2



Comparing OSI and TCP/IP §1.4.3

- Compare reference models, not the protocol stacks
- Differentiate Services, Interfaces, Protocols
- Attachment to protocols
- Number of layers
- Connectionless vs connection oriented

Criticisms of OSI Model #1 **§1.4.4**

- Timing
  - Juxtaposition research innovation and standards development.
    - Widespread adoption of the TCP/IP protocols preceded the formalisation of the OSI model
    - Vendors already begun offering TCP/IP based products.
    - OSI emerged about 5 years after industry had adopted TCP/IP
    - Vendors were reticent to add support for a second protocol stack until momentum had gathered behind OSI.
    - The combination of these factors meant that OSI was never adopted in practice

Criticisms of OSI Model #2 **§1.4.4**

- Technology
  - Some parts of the OSI model are fundamentally flawed.
  - Although there's 7 layers, 2 of these (session, presentation) are almost empty and 2 others (data link, network) are cramped.
  - Additionally some functions such as addressing, flow control and error control are recurring at each layer.
- Implementations
  - early implementations of OSI were inefficient, contrast with TCP/IP implementations which are easy to use, scalable and robust.
- Politics
  - OSI was widely perceived as the product of quasi-government standards processes rather than driven by good design processes

Criticisms of TCP/IP Model **§1.4.5**

- Lack of distinction between concepts
  - doesn't clearly distinguish between service, interface and protocol
- Not adaptable
  - not a general model, and hence poorly adapted to other protocol stacks
- Ambiguous layers
  - Host-to-network is not really a layer, but an interface between network and data link layers
- Omitted layers
  - Physical and data link layers are not present
- Early implementations were fragile

Network Standards

Network Standardization **§1.6**

- Standards provide an important common core, allowing a wide range of implementations which are interoperable
- Standardisation is a process of compromise between theortical desiderata and practical needs
  - The existence of a standard can be complemented or competed against by implementations - compare OSI and TCP/IP
- 3 types of standards which affect networking technologies
  - Telecommunications Standards
  - International Standards
  - Internet Standards

***Telecommunications Standards** **§1.6.1**

- International Telecommunications Union (ITU)
  - Radio communications (ITU-R)
  - Telecommunications (ITU-T)
  - Development (ITU-D)
  - ∼3000 recommendations
  - http://www.itu.int/

International Standards §1.6.2

- International Standards Organisation (ISO)
  - Highly formalised standards development process
  - 13,000 standards
  - ISO Workgroups (WG's) design the standard, Technical Committees (TC's) ratify it
  - http://www.iso.ch/
- National Standards Entities eg ANSI
- Professional Organisations eg IEEE

Internet Standards §1.6.3

- Internet Engineering Taskforce (IETF)
  - Open consortium
  - Mainly protocol level standards
  - RFC's
  - http://www.ietf.org/rfc
- World Wide Web Consortium (W3)
  - Membership based organisation
  - Mainly applications level standards
  - http://www.w3.org

Summary - Chapter 1

- Network fundamentals
  - Explain client-server model
  - Characterise differences between:
    - Point-to-point vs broadcast links
    - Bus vs ring network types
- Network Architecture Models
  - Explain differences between protocols, layers & services
  - Characterise features of connection-oriented vs connectionless services
  - Evaluate strengths & weaknesses of OSI & TCP/IP

Lecture III

Tutorial: Network Fundamentals

1. An alternative to a LAN is simply a big timesharing system with terminals for all users. Give two advantages of a client-server system using a LAN.

2. Besides bandwidth and latency, what other parameter is needed to give a good characterisation of the quality of service offered by a network used for digitised voice traffic.

3. A client-server system uses a satellite network, with the satellite at a height of $40,000$ km. What is the best case delay in respose to a request?

4. A collection of five routers is to be connected to a point-to-point subnet. Between each pair of routers, the designers may put a high speed line, a medium speed line, a low speed line, or no line. If it takes 100 ms of computer time to generate and inspect each topology, how long will it take to inspect all of them?

5. A disadvantage of a broadcast subnet is the capacity wasted when multiple hosts attempt to access the channel at the same time. As a simpistic example, suppose that time is divided into discrete slots with each of the n hosts attempting to use the channel with probability p during each slot. What fraction of slots are wasted due to collisions?

6. What are two reasons for using layered protocols?

7. The Internet is roughly doubling in size every 18 months. Although no one really knows for sure, one estimate put the number of hosts on it at 100 million in 2001. Use these data to compute the expected number of Internet hosts in the year 2010. Do you believe this? Explain why or why not.

8. List two advantages and two disadvatages of having international standards for network protocols.

9. Which of the OSI layers handles each of the following: a) Dividing the transmitted bit stream into frames. b) Determining which route through the subnet to use.

Lecture IV

The Physical Layer: Guided Transmission Media

What is the Physical Layer ? §2

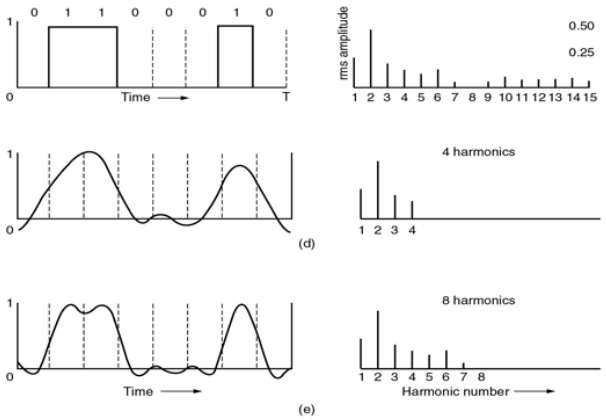
- Recall the layer hierarchy from network reference models
  - The physical layer is the lowest Layer in OSI model
  - The physical layer's properties in TCP/IP model are in the"host-to-network"division
- The physical layer is concerned with the mechanical, electrical and timing interfaces of the network
- Various physical media can be used to transmit data, but all of them are affected by a range of physical properties and hence have distinct differences
- How many different types of physical media can you think of?

Data Communications Theory

A Brief Introduction to Data Communications Theory §2.1

- Information on wire transmitted by variance of a physical property eg voltage, current.
  - A basic binary system - 0 or 1
- Value of this property as a single function of time f(t) allows modelling of signal behaviour
  - Fourier Analysis
    - A reasonably behaved periodic function can be constructed as the sum of a number of sines and cosines
    - Each sine/cosine enumerated is called a harmonic
  - Bandwidth Limited Signals
    - Available frequency range (bandwidth) is dependent on medium, distance etc

Bandwidth of a Signal §2.1.2



Maximum Data Rate of a Channel §2.1.3

- Even a perfect channel (media) has a finite transmission capacity governed by physical and chemical properties
- Nyquist (1924): if an arbitrary signal has been run through a low-pass filter of bandwidth H, the filtered signal can be reconstructed by making 2H samples per second
- Shannon (1948): random thermal noise impacts transmission -"signal to noise ratio"(dB)

Thinking about Networks for Data Transfer §2.2.1

- While networks are increasingly by default the means by which data is transferred , there are other options for data transfer - consider removable media such as tapes, CD ROMs, DVDs
  - Cost-wise, such removable media are often more efficient on a per Mb/Gb basis
  - However, using such media to transfer data introduces a significant delay"never underestimate the bandwidth of a car boot full of DVD's":

    - 1000 DVD's x 4300Mb at 100km/h over distance of 100 kms = 4.3Tb / hr or 1.2 Gbps
    - At $5/DVD, plus say $20,000 for the car, that's $25,000 for a 1.2 Gbps data transfer over 100kms - to build a 1 Gbps network over 100km costs in the order of $1 million
- Data transfer over a network is not always the most efficient method to use

The Bandwidth Revolution? §2.2.1

- Evolutionary steps in available bandwidth:
  - CPU speeds increase by a factor of ∼20 per decade
    - 1981: PC 4.77Mhz vs 2001: PC 2 Ghz
  - Bandwidth speeds increase by a factor of ∼125 per decade (1981: Modem 56kbps vs 2001: Net 1Gbps)
  - Current CPU speed now approaching physical limits - constrained by physical properties pertaining to granularity of engraving on silicon
  - Current bandwidth available up to 50Tbps - vastly exceeding the rate at which we can convert electrical impulses to optical pulses

Guided Transmission Media

Guided Transmission Media §2.2

- All guided transmission media simply transmit a raw bit stream from one location to another
- Guided transmission media has a range of forms, we'll consider several including:
- Portable Media
  - Twisted Pair
  - Coaxial Cable
  - Fibre Optics

Twisted Pair

Twisted Pair §2.2.2

- Two insulated copper wires, twisted in helical (DNA) form.
- Twisting reduces radiance of waves from effectively parallel antennae
- Distance up to <5km, repeaters can extend this distance (large buildings often have km's of cabling)
- Bundling in shielded sheaths
  - twisting reduces interference

Properties and Types of Twisted Pair §2.2.2

- Carry either analogue or digital signals
- Bandwidth dependent on distance, wire quality/density
- Cat 3 - 2 wires, 4 pairs in sheath, 16Mhz
- Cat 5 - 2 wires, 4 pair in sheath, more twists = less interference, higher quality over longer distance, 100 Mhz
- Cat 6 - 250 Mhz
- Cat 7 - 600Mhz + ?

Cat 3 and Cat 5 §2.2.2

(a)

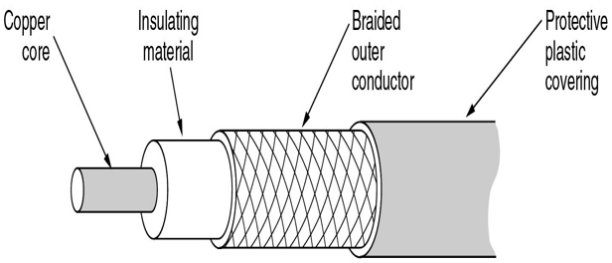
(b)

Coax

Coaxial Cable §2.2.3

- Better shielding than twisted pair = higher speeds over greater distances
- Copper core with insulation, mesh, and sheath
- Bandwidth approaches 1Ghz
- Still widely used for cable TV/Internet

Coaxial Cable §2.2.3



Fiber Optics

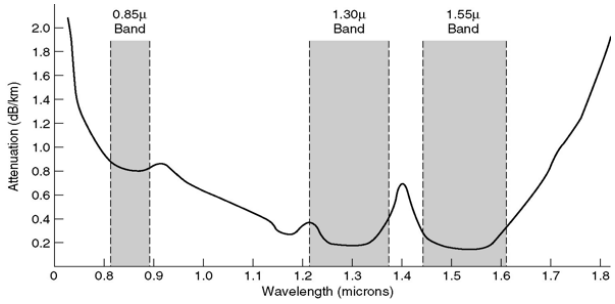
Fibre Optics §2.2.4

- Optical transmission has 3 components: light source, transmission medium, detector
- Semantics: light = 1, no light = 0 (basic binary system)
- Data transmission over a fibre of glass
- A detector generates electrical pulse when light hits it
- Refraction between air/silica boundary is compensated for by design - total internal reflection

Transmission of Light Through Fibre §2.2.4

- Attennuation (loss per km) of light through glass depends on wavelength of light
- Optical communications at 0.85, 1.30, 1.55 microns
  - 1.30 and 1.55 have low loss (<5%/km)
  - 0.85 physical property sharing between laser and electronics
- Chromatic Dispersion alleviated by solitons (a technique to make light pulses in a shape reciprocal to the hyperbolic cosine of a frequency)

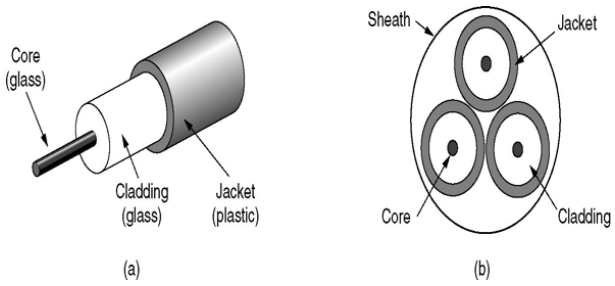
Attenuation of Light §2.2.4



Fiber Optic Cables #1 §2.2.4

- Glass core around 50 microns
- Cladding with lower refractive index
- Jacket
- Bundled in sheath
- Terrestrial - in ground close to surface
- Transoceanic - on sea bed (loose or anchored)

Fiber Optic Cables #2 §2.2.4



Fiber Optic Connections §2.2.4

- Connectors and Fiber Sockets (10-20% loss, but easy to configure)
- Mechanical Splice (10% loss but labour intensive)
- Fusion (<1% loss, but specialised)
- Signalling using LED's or semiconductor lasers

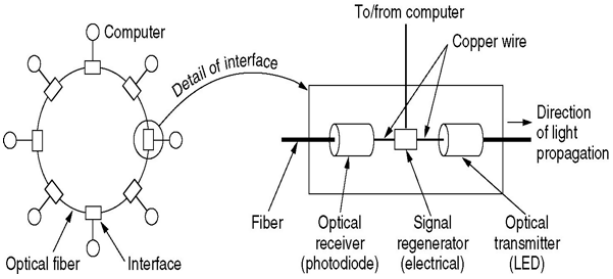
Semiconductors vs LEDs in Fiber Optics §2.2.4

Item	LED	Semiconductor laser
Data rate	Low	High
Fiber type	Multimode	Multimode or single mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

Fiber Optic Networks **§2.2.4**

- Fiber optic cable is a scalable network media - LAN, WAN, long haul
- Fibre optic cable can be considered either as a ring or as a bus network type (series of point to point connections)

Fiber Optic Ring Overview **§2.2.4**



Fiber Optics vs Copper Wire **§2.2.4**

- Advantages of fiber:
  - higher bandwidths
  - greater distance between repeaters (5km vs. 50km)
  - not physically influenced by interference or surges
  - thin/lightweight
  - no leakage
  - difficult to tap
- Advantages of copper:
  - cheaper
  - no specialist skills required
- Since network providers have already widely deployed copper infrastructure, fiber optics is seen largely as a strategic backbone technology which complements copper
- However, as the price of fiber optics is reduced, it is becoming more prevalent (fiber to the desktop)

Lecture V

The Physical Layer: Telephony Networks and Wireless Networks

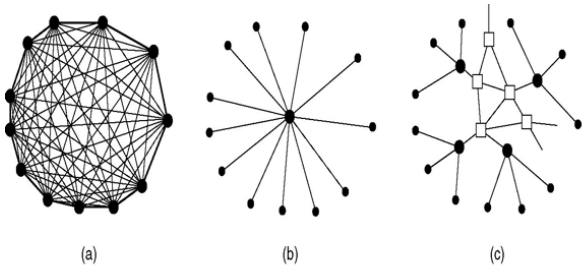
Telephony Based Data Transmission

PSTN

PSTN **§2.5**

- The"Public Switched Telephone Network"
- Structure
  - Loops - analogue twisted pairs to properties
  - Trunks - digital fibre optics connecting switching offices
  - Switching offices - call routing services
- The PSTN is fraught with regulatory requirements

Structure of PSTN **§2.5.1**



(a) Fully-interconnected network;
(b) Centralized switch;
(c) Two-level hierarchy.

Telephony Regulation §2.5.2

- US nomenclature:
  - LATA: local access and transport area
  - LEC: local exchange carrier
  - IXC: interexchange carrier
  - POP: point of presence
- Australian context:
  - Telstra acted as a LATA, LEC and IXC
  - Later arrivals - Optus, Hutchison, Vodafone - act mainly as LEC and IXC's

Local Loop §2.5.3

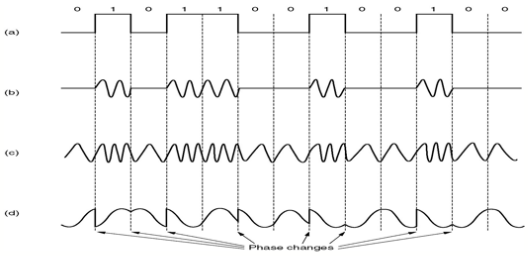
- The"last mile"
- Analogue technologies dominant but innovation due to high cost of digital conversion
- AD and DA conversion typically via modems
- Transmission problems: attenuation, distortion, noise

Modems

Modems §2.5.3

- AC signaling using:
  - Amplitude Modulation
  - Frequency Modulation
  - Phase Modulation

Modulation Types §2.5.3



(a) A binary signal; (b) Amplitude modulation;
(c) Frequency modulation; (d) Phase modulation

Modems Terminology §2.5.3

- Modem = Modulator / Demodulator
- Bandwidth = physical property (range of frequencies)
- Baud = symbols per second
- Modulation type = number of bits / symbol

Modems Types §2.5.3

- Combinations of bandwidth, baud and modulation
  - V.32 = 9.6Kbps
  - V.32bis = 14.4Kbps
  - V.34 = 28.8Kbps
  - V34.bis = 33.6Kbps
  - V.90 = 56Kbps/33.6Kbps
  - V.92 = 56Kbps/48Kbps (??)
- Functions based on mode of transmission
  - Full Duplex = traffic both directions simultaneously
  - Half Duplex = traffic one way at a time
  - Simplex = traffic one way

Wireless Data Transmission

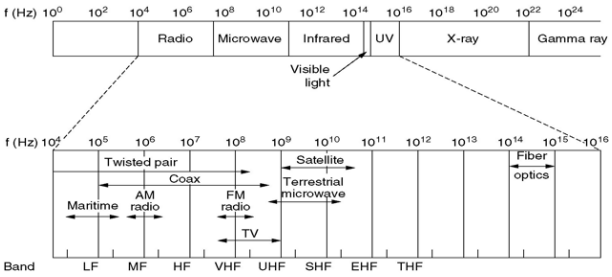
Wireless Transmission §2.3

- Mobile users requires a mobility enabled network - contrast with the wired networks seen earlier
- Wireless networks can provide advantages even in fixed location environments
- There are many types of wireless data transmission networks, but they all have a common basis - radio wave propagation

ElectroMagnetic Spectrum §2.3.1

- Number of oscillations per second of a wave is called frequency, measured in Hertz (Hz).
- Distance between two consecutive minima or maxima is called wavelength.
- All EM waves travel at same speed (speed of light)
- Fundamental relationship:
  - Wavelength x Frequency = Speed of Light

Spectrum Divisions §2.3.1



Regulation of EM Spectrum §2.3.3

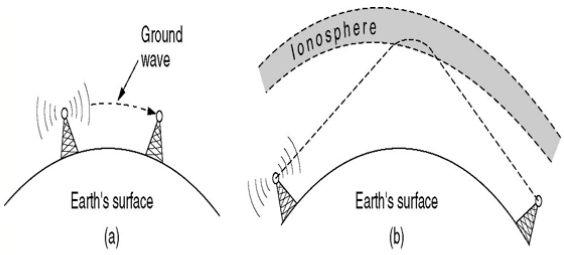
- Everyone wants a higher data rate therefore wants more spectrum ...
- National and international allocations are required
- Still require frequency allocation -"beauty contest", lottery, auction
- Unregulated spectrum - consumer applications

Radio

Radio Transmission §2.3.2

- Radio waves are easy to generate, propagate over long distances, penetrate solid objects, omni-directional and therefore used widely
- Properties of RW are frequency dependent - relationship of frequency to power
- Interference is a factor, regulation can assist

RW Reception §2.3.2



a) VLF, LF, MF follow ground – affects distance for reception; b) HF VHF refract from ionosphere and sent back

Microwave Transmission §2.3.3

- >100Mhz = waves travel in straight lines, narrow focus
- Higher signal to noise ratio, but requires accurate transmit/receive alignment (eg satellite TV dish)
- General principle of higher the tower, the further apart towers can be (roughly relational)
- Microwaves to not pass through objects very well, and are subject to multipath fading when refracted
- Bands up to 10Ghz used, but above 4Ghz are absorbed by water (eg rain)
- Main advantage is that no right of way is needed, but line of sight is required. Also cheap to install.

Infrared and Millimeter Waves §2.3.4

- Widely used for short range communication - e.g. remote controls
- Positives: cheap, easy to build, directional
- Negatives: obstructions

Lightwave Transmission §2.3.5

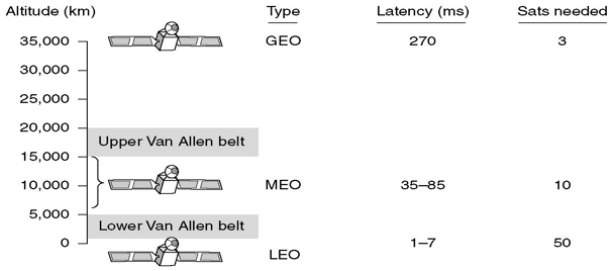
- "laser"
- High bandwidth, low cost, not regulated
- Requires careful alignment because of narrow beam
- Condition dependent e.g. fog, rain

Satellite

Communication Satellites §2.4

- Transponders receive in one spectrum portion and rebroadcasts in another -"bent pipe"
- The higher the satellite, the longer the period of visibility ("window")
  - At low orbits, the window is small, thus more a needed to provide continuous coverage
  - Cost increases with orbit height
- "Footprint"indicates coverage area

Some Properties of Communications Satellites §2.4



Geostationary Satellites §2.4.1

- $\sim$ 35,800km
- Latency $\sim$270ms
- Theory: only 3 needed for global coverage
- ITU allocates orbit slots and frequencies
- Roundtrip delay because of large distances
- Excellent broadcast media

Principal Satellite Bands §2.4.1

Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

Medium Earth Orbit Satellites §2.4.2

- $\sim$5,000-15,000 km
- Latency 35-85ms
- Theory: only 10 needed for global coverage
- Shorter windows ($\sim$6 hours)
- Smaller footprint, lower power required
- GPS Satellites

Low Earth Orbit Satellites §2.4.3

- $\sim$1000-5000km
- Latency: 1-7ms
- Theory: 50 needed for global coverage
- Low power, cheaper (!)
- Example Satellite Networks
  - Iridium
    - 66 satellites - built mid to late 1990's. Business plan did not assume growth of mobile phone network and related standards (eg GSM). Voice, data, paging, fax. 750km altitude, one satellite every 32 degrees of latitude. Each satellite has 48 beams, for total of 1628 beams covering earth's surface. Communication is in orbit - relay between satellites.
  - Globalstar
    - 48 satellites using bent pipe relay. Large ground stations mean lower power telephones can be used. Focus on voice only.

Advantages of Satellite §2.4.4

- Bandwidth accessible
- Mobile communication
- Broadcast mode
- Bad terrestrial infrastructure
- Local condition independent
- Rapid deployment

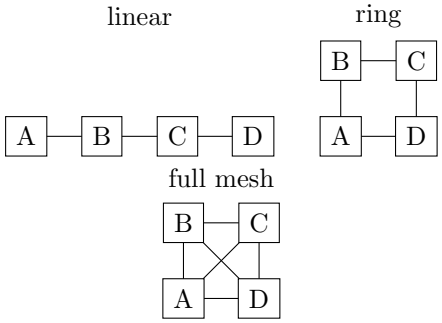
Summary - Chapter 2

- Data Communications Theory
  - Calculate the maximum data rate of a noiseless channel
  - Characterise different guided media
    - Twised pair vs coaxial cable vs fibre optics
- Telephony Networks
  - Explain structure of the PSTN
  - Recognise different modulation types
- Wireless Data Transmission
  - Explain differences between wireless transmission types
    - Radio, EM, microwave, infrared
  - Choose the appropriate type of satellite for an application

Lecture VI

Tutorial: Physical Layer

1. Consider the following 3 network topologies for connecting N nodes:



   In the general case of an N node network: (a) How many links are there in each network? (b) What is the maximum delay between any pair of nodes, assuming each link has a delay of 10ms, and the shortest path is used between nodes? (c) What is the minimum number of links that need to be cut in order to isolate one or more nodes? (d) Which topology would you use to connect military command centres?

2. Consider a telephone signal that is bandwidth limited to 4 kHz. (a) At what rate should you sample the signal so that you can completely reconstruct the signal? (b) If each sample of the signal is to be encoded at 256 levels, how many bits/symbol are required for each sample? (c) What is the minimum bit rate required to transmit this signal?

3. Identify 2 ways in which the OSI reference model and the TCP/IP reference model are the same. Identify 2 ways in which these models differ.

4. A noiseless 4 kHz channel is sampled every 1 msec. What is the maximum data rate?

5. Television channels are 6 MHz wide. How many bits/sec can be sent if four-level digital signals are used? Assume a noiseless channel.

6. Is the Nyquist theorem true for optical fibre or only for copper wire?

7. Radio antennas often work best when the diameter of the antenna is equal to the wavelength of the radio wave. Reasonable antennas range from 1 cm to 5 meters in diameter. What frequency range does this cover?

8. A laser beam 1 mm wide is aimed at a detector 1 mm wide 100 m away on the roof of a building. How much of an angular diversion (in

degrees) does the laser have to have before it misses the detector?

9. Consider a satellite at the altitude of geostationary satellites, but whose orbital plane is inclined to the equatorial plane by an angle ϕ. To a stationary user of the earth's surface at north latitude ϕ, does this satellite appear motionless in the sky? If not, describe its motion.

10. Is an oil pipe a simplex system, a half-duplex system, or a full duplex system, or none of the above?

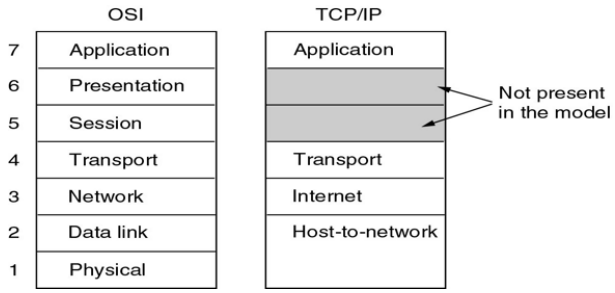
11. In a constellation diagram, all points lie on a circle centered on the origin. What kind of modulation is being used?

12. Ten signals, each requiring 4000 Hz, are multiplexed onto a single channel using FDM. How much minimum bandwidth is required for the multiplexed channel? Assume that the guard bands are 400 Hz wide.

Lecture VII
Data Layer Design

Data Link Layer Design Issues

The Data Link Layer in OSI and TCP/IP §3

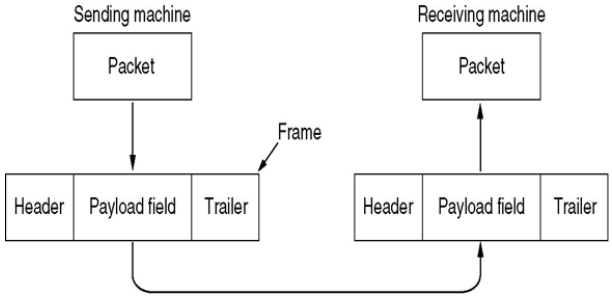


Functions & Methods of the Data Layer §3.1

- Functions of the data link layer:
  - Provide a well-defined service interface to network layer
  - Handling transmission errors
  - Data flow regulation
- Primary method:
  - Take packets from network layer, and encapsulate them into frames (containing a header, a payload, a trailer)

Units

Packets and Frames Illustrated §3.1



Services

Services Provided to Network Layer §3.1.1

- Principal concern is transferring data from network layer on source host to network layer on destination host
- Services provided:
  - Unacknowledged connectionless service
  - Acknowledged connectionless service
  - Acknowledged connection-oriented service

Unacknowledged Connectionless Service §3.1.1

- Source host transmits independent frames to recipient host with no acknowledgement
- No logical connection establishment or release
- No lost frame recovery mechanism (or left to higher levels)
- Eg LANs

Acknowledged Connectionless Service §3.1.1

- Source host transmits independent frames to recipient host with acknowledgement
- No logical connection establishment or release
- Each frame individually acknowledged (retransmission)
- Eg Wireless

Acknowledged Connection-Oriented Service §3.1.1

- Source host transmits independent frames to recipient host after connection establishment and with acknowledgement
- Connection established and released
- Frames numbered, counted, acknowledged with logical order enforced
- Eg WANs, VPNs

Framing

Framing §3.1.2

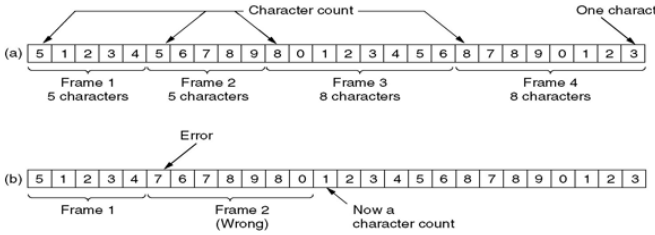
- Physical layer provides no guarantee a raw stream of bits is error free
- Framing is the method used by data link layer to break raw bit stream into discrete units and generate a checksum for the unit
- Checksums can be computed and embedded at the source, then computed and compared at the destination *checksum = f(payload)*
- The primary purpose therefore, of framing, is to provide some level of redundancy over the unreliable physical layer

Framing Methods §3.1.2

- Framing methods:
  - Character count
  - Flag bytes with byte stuffing
  - Start and end flags with bit stuffing
  - Physical layer coding violations
- Most data link protocols use a combination of character count and one other method

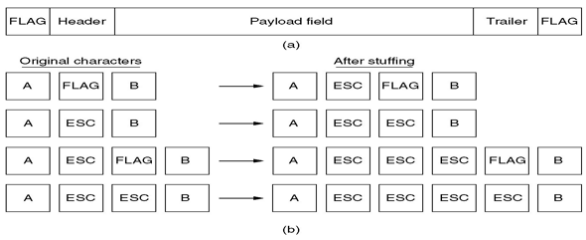
Character Counts §3.1.2

- Uses a field in the frame header to specify the number of characters in a frame



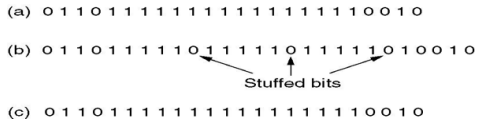
Flag Bytes with Byte Stuffing §3.1.2

- Each frame starts and ends with a special byte -"flag byte"



Start and End flags with Bit stuffing §3.1.2

- Frames contain an arbitrary number of bits and allow character codes with an arbitrary number of bits per character
- Each frame begins and ends with a special bit pattern *e.g. 01111110*



Physical layer coding violations §3.1.2

- If physical medium contains some redundancy, then we can use physical properties (eg electrical impluses) to delimit frames
  - eg 1 bit of data encoded using 2 physical bits → each data bit has a transition and so boundaries can be determined easily
  - The 2nd physical bit could be a standard impulse at a different voltage to data

Error Detection & Correction

Error Control §3.1.3

- How can we ensure all frames are delivered to the network layer and delivered in canonical order ?
  - Control frames
    - Positive and negative *acknowledgements* sent by receiver
  - Timers
    - *Timeout* values independent of acknowledgements
  - Sequencing
    - *Sequence numbers* help to resolve sort orders in the case of multiple retransmissions

Flow Control §3.1.4

- The *fast senders* vs slow receivers problem requires a solution
- Principles to control when sender can send next frame
  - Feedback based flow control
  - Rate based flow control

Error Detection and Correction §3.2

- Physical media may be subject to errors
- Errors may occur *randomly* or in *bursts*
- Bursts of errors are easier to detect but harder to resolve
- Resolution needs to occur before handing data to network layer

Methods of Error Detection and Correction §3.2

- 2 methods for error handling:
  - Include enough information in frames to allow reconstruction/deduction of original content (*error-correcting*)
  - Include enough redundancy to allow receiver to determine an error occurred and request retransmission (*error-detecting*)
- Different transmission methods may use different error detection and correction methods

Error Correcting Codes §3.2.1

- More efficient in noisy transmission media eg wireless
- Frame consists of *data bits* and *check bits*
- Codeword is the unit containing both data and check bits
- Codewords can be compared to determine how many bits differ
  - "Hamming distance": the degree of similarity between two codewords i.e. number of single-bit errors needed to convert one codeword to another

Error Detecting Codes §3.2.2

- More efficient in some transmission media - eg where low error rates occur (copper wires)
- *Cyclical Redundancy Check* - polynomial code used to compute a checksum for a block and attached to block in transmission
- Some polynomials are adopted as standards eg IEEE 802

Lecture VIII
Data Link Protocols

Elementary Data Link Protocols

Elementary Data Link Protocols §3.3

- Data links can be simulated
- Simulations may expose weaknesses in the design of data link protocols, or their relative strengths
- All simulations include assumptions - integration of layers, direction and timing of transmission, data supply, no host/router crashes

Elementary Data Link Protocol Functional Primitives §3.3

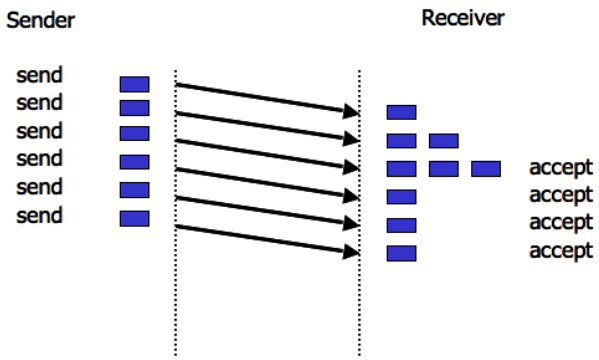
- These core functions are necessary for all different types of data protocols.
  - wait_for_event
  - to_network_layer
  - from_network_layer
  - from_physical_layer
  - to_physical_layer
  - start_timer
  - stop_timer

  - start_ack_timer
  - stop_ack_timer
  - void

A Very Simple Protocol §3.3.1

- Data transmitted one direction
- Physical and network layers always ready
- Infinite time and buffer space available
- Communication channel never loses frames

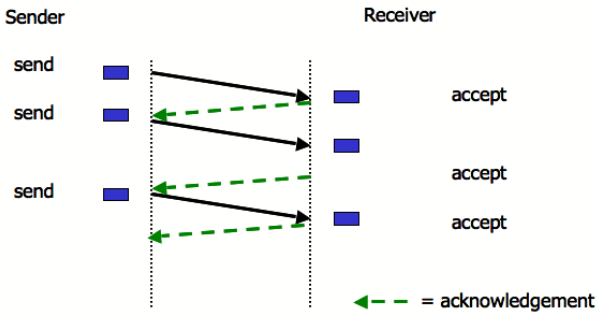
A Very Simple Protocol §3.3.1



Stop and Wait Protocol §3.3.2

- (think: fast sender / slow receiver)
- Data transmitted in one direction
- Physical and network layers not always ready
- Time is relatively important, buffer space constrained

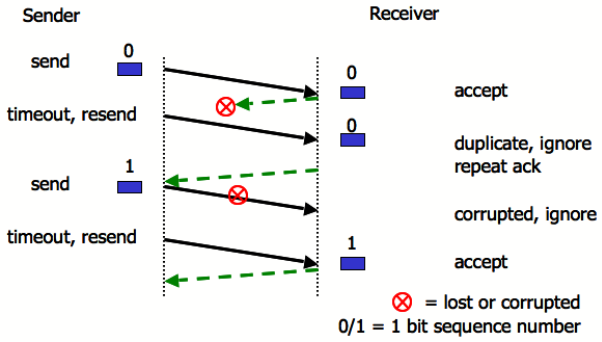
Stop and Wait Protocol §3.3.2



Noisy Channel Protocol §3.3.3

- Frames can be lost either entirely or partially
- Requires distinction between frames already sent/received and those being re-transmitted
- Requires timeout function to determine arrival or non-arrival of complete frames

Noisy Channel Protocol §3.3.3



Sliding Window Protocols §3.4

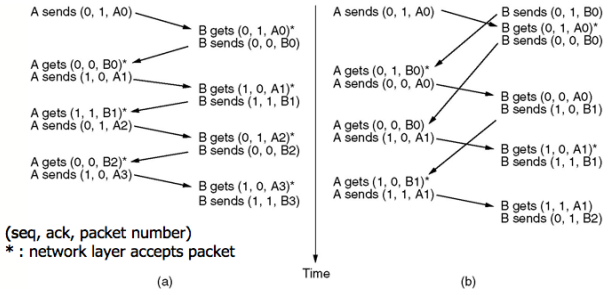
- Data is commonly transmitted in *both directions* simultaneously
- Sender maintains a set of *sequence numbers* corresponding to frames it is allowed to send (within the"sending window")
- Receiver maintains a set of *sequence numbers* corresponding to frames it is allowed to accept (within the"receiving window")

Sliding Window Protocols

One Bit Sliding Window Protocol §3.4.1

- Similar to stop and wait
- Problems can arise if both sides send an initial packet - synchronization issues

One Bit Sliding Window Protocol Illustrated §3.4.1



Protocol Using Go-Back-N §3.4.2

- Long transmission times need to be taken into account when programming timeouts eg low bandwidth or long distance
- Senders *don't need to wait* for acknowledgement for each frame before sending next frame

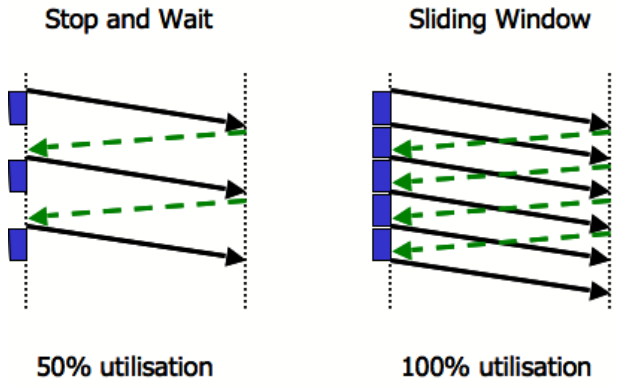
Go-Back-N vs Selective Repeat §3.4.2

- Go-Back-N: receiver discards all subsequent frames from error point, sending no acknowledgement, until the next frame in sequence
- Selective Repeat: receiver buffers good frames after an error point, and relies on sender to resend oldest unacknowledged frames
- Tradeoff between *bandwidth* and *buffer space*

Pipelining §3.4.2

- Principle of efficiency in communication channel usage
- Line utilisation $= \frac{\text{frame size (bits)}}{\text{frame size (bits)} + \text{capacity} \times \text{round-trip-time}}$

Pipelining §3.4.2



Protocol Using Selective Repeat §3.4.3

- An alternative error handling strategy is to allow receiver to *accept and buffer frames* following any damaged or lost frames
- Both sender and receiver have a window of acceptable sequence numbers
- On frame arrival, the sequence number is checked to see if it falls within the window and whether it has already been accepted
- In this model frames can be non-sequential

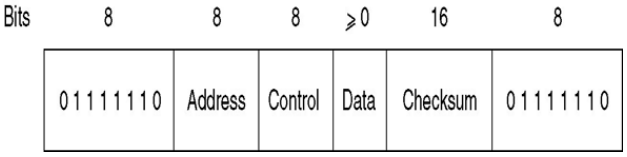
Example Data Link Protocols

Example Data Link Protocols §3.6.1

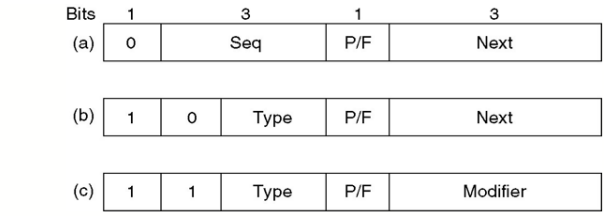
- HDLC: a bit oriented protocol with numerous variants used since 1960's
- Lineage from IBM mainframe communications
  - SDLC: IBM
  - ADCCP: ANSI
  - HDLC: ISO
  - LAP: CCITT
  - LAPB: CCITT
- PPP: data link protocol used widely in the internet domain
  - Data layer protocols on internet are common at both hosts-router and router-router level
  - Typically Point-to-Point connections

Characteristics of HDLC §3.6.1

- Bit oriented
- Uses bit stuffing
- 32 bit frame, sliding window (3 bit sequence)
- Frame structure:



Control Fields in HDLC §3.6.1



a) Information frame; b) Supervisory frame; c) Unnumbered frame

HDLC Primitives §3.6.1

- Disconnect (DISC)
  - going offline
- Set Normal Response Mode (SRMN)
  - back online
- Frame Reject (FRMR)
  - frame rejected, correct checksum but bad syntax or semantics
- Unnumbered Acknowledgement (UA)
  - loss or damage of a control frame

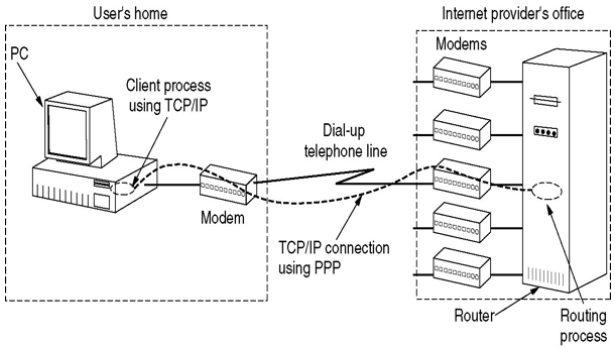
Point to Point Protocol (PPP) §3.6.2

- IETF RFC 1661 (extended in RFC's 1662, 1663)
- Handles
  - error detection
  - Multiple protocols
  - IP address negotiation
  - authentication

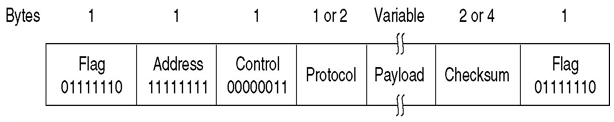
Main Features of PPP §3.6.2

- Framing method that unambiguously delineates frame start and end and handles error detection
- Link protocol (LCP) controls line connection/disconnection - supports both sync/async circuits, bit and byte encodings
- Network protocol (NCP) negotiates network layer options independently of network layer protocol used

A Typical PPP Scenario §3.6.2

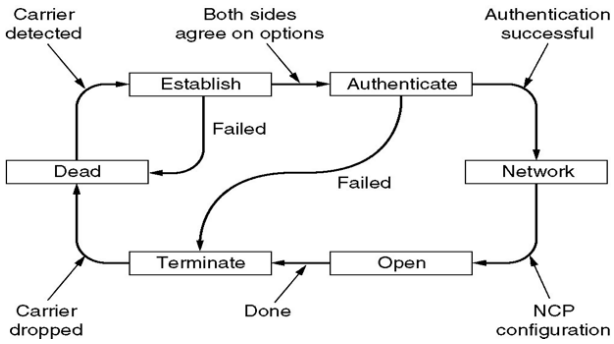


PPP Frames §3.6.2



Flag: standard HDLC flag byte
Address: standard HDLC address
Control: standard HDLC control
Protocol: which protocol ? LCP/NCP/IP/IPX/AppleTalk
starts with 0: network layer protocols
starts with 1: negotiation
Payload: actual data, negotiated length to a maximum
Checksum: standard checksum
Flag: standard HDLC flag byte

PPP Link State Control §3.6.2



LCP Frame Types §3.6.2

Name	Direction	Description
Configure-request	I → R	List of proposed options and values
Configure-ack	I ← R	All options are accepted
Configure-nak	I ← R	Some options are not accepted
Configure-reject	I ← R	Some options are not negotiable
Terminate-request	I → R	Request to shut the line down
Terminate-ack	I ← R	OK, line shut down
Code-reject	I ← R	Unknown request received
Protocol-reject	I ← R	Unknown protocol requested
Echo-request	I → R	Please send this frame back
Echo-reply	I ← R	Here is the frame back
Discard-request	I → R	Just discard this frame (for testing)

PPP and HDLC Compared §3.6.2

- PPP and HDLC are similar, but major differences are:
  - PPP is *character* oriented, HDLC is *bit* oriented
  - PPP uses byte stuffing so all frames are an integral number of bytes
  - PPP and HDLC both have optional reliable transmission
  - PPP is usable over a wider variety of physical media / connection types

Summary - Chapter 3

- Data Link Layer
  - Contrast types of services provided
  - Apply different framing methods
    - Character count, bit and byte stuffing
  - Explain methods for error detection / correction
- Data Link Layer Protocols
  - Characterise different protocols
    - stop-&-wait, sliding window, go-back-N, selective repeat
  - Calculate efficiency of stop-and-wait
  - Compare HDLC and PPP protocols

Lecture IX

Tutorial: Data Link Layer

1. The following character encoding is used in a data link protocol:

   A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000

   Show the bit sequence transmitted (in binary) for the four-character frame: A B ESC FLAG when each of the following framing method is used: 1. Character count. 2. Flag bytes with byte stuffing. 3. Starting and ending flag bytes, with bit stuffing.

2. The following data fragment occurs in the middle of a data stream for which the byte-stuffing algorithm described in the lecture is used: A B ESC C ESC FLAG FLAG D. What is the output after stuffing?

3. One of your classmates, Scrooge, has pointed out that it is wasteful to end each frame with a flag byte and then begin the next one with a second flag byte. One flag byte could do the job as well, and a byte saved is a byte earned. Do you agree?

4. When bit stuffing is used, is it possible for the loss, insertion, or modification of a single bit to cause an error not detected by the checksum? If not, why not? If so, how? Does the check sum length play a role here?

5. A bit string, 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

6. Data link protocols almost always put the CRC in a trailer rather than in a header. Why?

7. A channel has a bit rate of 4 kbps and a propagation delay of 20 msec. For what range of frame sizes does stop-and-wait give an efficiency of at least 50 percent?

8. A 100 km long cable runs at the T1 data rate. The propagation speed in the cable is 2/3 the speed of light in a vacuum. How many bits fit in the cable?

Lecture X

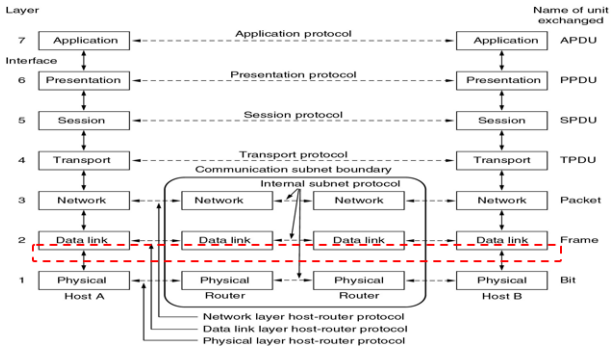
Channel Allocation and Multiple Access Protocols in the MAC Sub-layer

The MAC Sub-layer

Introduction §4

- On *point to point* networks, there are only singular sender and receiver pairs, eliminating transmission contention
- On *broadcast networks*, determining right to transmit is a complex problem
- *Medium Access Control* (MAC) sub-layer is used to assist in resolving transmission conflicts

The MAC Sub-layer §4



Channel Allocation Problems

Types of Channel Allocation Mechanisms §4.1

- Various methods exist for allocating a single broadcast channel amongst competing users
  - Static Channel Allocation
  - Dynamic Channel Allocation

Static Channel Allocation §4.1.1

- Arbitrary division of a channel into segments and each user allocated a dedicated segment for transmission
- *Frequency Division Multiplexing* (FDM) is typically used
- Significant inefficiencies arise when:
  - Number of senders > allocated segments
  - Number of senders is not static
  - Traffic is bursty

Dynamic Channel Allocation §4.1.2

- Channel segmentation is dynamic, segment allocation is dynamic
- Assumptions for dynamic channel allocation:
  - Independent transmission stations
  - Single channel for all communication
  - Simultaneous transmission results in damaged frames
  - Time
    - Transmission can begin at any time
    - Transmission can begin only within discrete intervals
  - Carrier Sense
    - Detection of channel use prior to transmission
    - No detection of channel use prior to transmission

Multiple Access Protocols

Multiple Access Protocols §4.2

- Carrier Sense Multiple Access
- Collision Free
- Limited Contention
- Wavelength Division Multiple Access
- MACA/MACAW (for Wireless LANs)

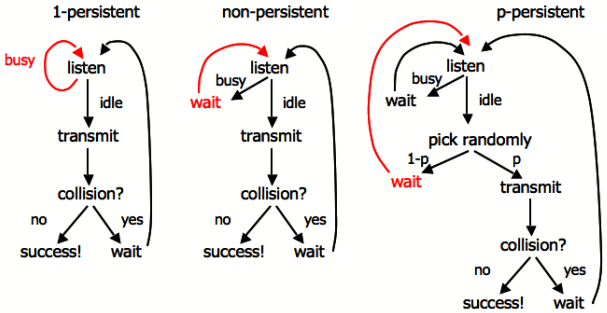
Carrier Sense Multiple Access (CSMA) Protocols §4.2.2

- In networks which require transmission state detection to determine transmission rights dynamically, there are specific protocols which are used
  - *Persistent and Non-Persistent CSMA*
  - *CSMA* with *Collision Detection*

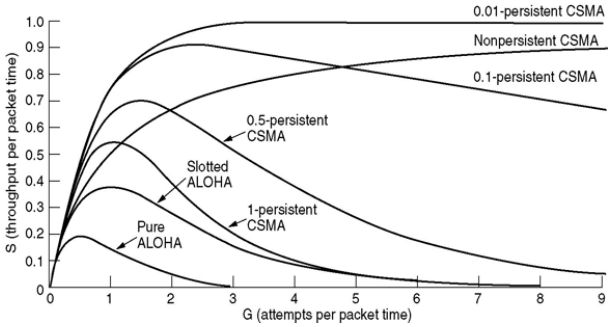
Persistent and Non-Persistent CSMA §4.2.2

- When a sender has data to transmit, *first check channel* to detect other active transmission
- 1-persistent CSMA
  - Wait until channel idle; transmit one frame and check collisions; if collision, wait for a random time and repeat
- Non-persistent CSMA
  - If channel busy, *wait random period* and check again; if not, start transmitting
- p-persistent CSMA
  - If channel idle, *transmit with probability p*, or *wait with probability (1-p)* and check again

Persistent and Non-Persistent CSMA §4.2.2



CSMA Variants §4.2.2



CSMA with Collision Detection §4.2.2

- Principle that *transmission aborted* when collision detected
- After collision detected, abort, wait random period, try again
- Channel must be continually monitored, implies only *half-duplex* system

Collision Free Protocols §4.2.3

- Bit Map Protocol
  - 1 bit per station overhead
  - Division of transmission right, and transmission event - no collisions as this is a *reservation based* protocol
- Binary Countdown Protocol
  - Avoid the 1 bit per station scalability problem by using binary station addressing
  - No collisions as higher-order bit positions are used to arbitrate between stations wanting to transmit
  - Higher numbered stations have a higher priority

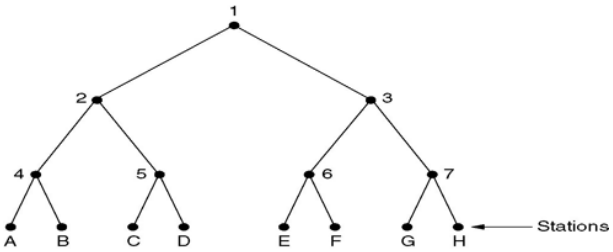
Limited Contention Protocols §4.2.4

- 2 strategies - *contention* and *collision free* - both become inefficient at different points
  - Under *higher loads*, contention is less attractive because overhead associated with channel arbitration becomes greater
  - Under *low loads*, collision free is less attractive because of a higher delay between transmissions.

- *Limited Content Protocols* increase the probability of stations acquiring transmission rights by arbitrarily dividing stations and using a binary algorithm to determine rights allocation

Adaptive Tree Walk Protocol §4.2.4

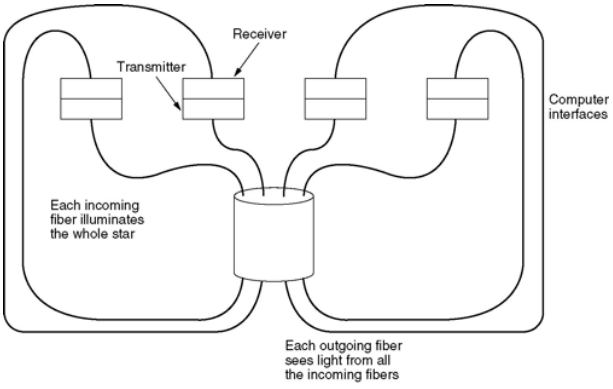
- All stations compete for right to transmit, if a collision occurs, binary division is used to resolve contention



Wavelength Division Multiple Access (WDMA) Protocols §4.2.5

- On optical fibre networks, differentiating wavelengths for light transmission allows multiple transmissions occur simultaneously
- Topology is typically *hub and spoke*
- Stations are assigned an *input* and *output* wavelength in addition to a *control channel*

Wavelength Division Multiple Access (WDMA) Protocols §4.2.5



WDMA Traffic Classes §4.2.5

- *Constant data rate* connection oriented traffic eg video
- *Variable data rate* connection oriented traffic eg file transfers
- *Datagram* traffic eg UDP packets

WDMA Send/Receive Architecture §4.2.5

- Each station has two transmitters and two receivers
- Transmitters
  - *Tunable* transmitter for sending *control signals*
  - *Fixed* transmitter for sending *data*
- Receivers
  - *Fixed* receiver for listening to *control signals*
  - *Tunable* receiver for receiving *data*

Wireless LAN Protocols §4.2.6

- When a station is in the range of two transmitters or relays, interference affects signal reception
- Require detection of *transmissions to receiver*, not just carrier sensing
- Transmission Protocols for Wireless LANs (802.11)
  - Multiple Access with Collision Avoidance (MACA)
  - Multiple Access with Collision Avoidance for Wireless (MACAW)

Multiple Access with Collision Avoidance (MACA) §4.2.6

- Sender asks receiver to transmit short control frame
- Stations near receiver hear control frame
- Sender can then transmit data to receiver

Multiple Access with Collision Avoidance for Wireless (MACAW) §4.2.6

- Improvement on MACA
- ACK after each successful data frame
- Carrier Sense
- Each sender/receiver pair has a separate random backoff interval
- Congestion information can be exchanged separately

Lecture XI

A MAC Sub-Layer Case Study: Ethernet

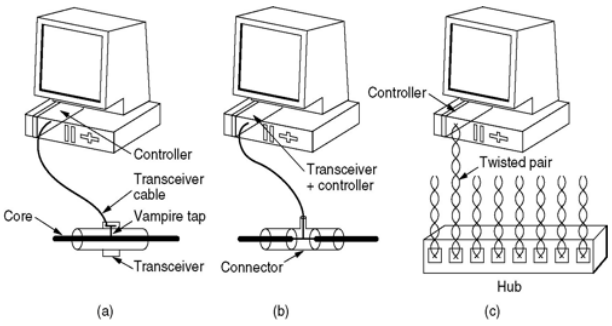
Ethernet Cabling Types

Ethernet Cabling Types: Constraints §4.3.1

- Each type of Ethernet has a *maximum cable length* per segment.
- Multiple cable lengths can be connected by *repeaters* - a physical device which receives, amplifies and retransmits signals in both directions.
- Notation: Bandwidth+Signal Type+Segment Length

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

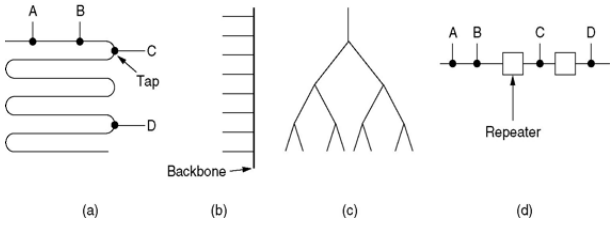
Ethernet Cabling Types Physical Interfaces §4.3.1



(a) 10Base5, (b) 10Base2, (c) 10Base-T.

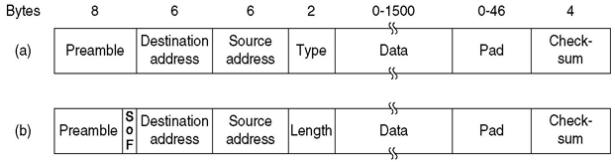
Ethernet Topologies §4.3.1

- Ethernet Cable Topologies: a) Linear, b) Spine, c) Tree, d) Segmented



Ethernet Frame Format

Ethernet Frame Format §4.3.3



- a) earlier Ethernet frames
- b) 802.3 frames

MAC Addressing

MAC Addressing §4.3.3

- Source and Destination Addressing can be done at a local or global levels
- The *MAC Address* provides the unique identifier for a physical interface
- MAC Address is a 48-bit number encoded in the frame
  - eg 00:02:2D:66:7C:2C

Binary Exponential Backoff Algorithm

Binary Exponential Backoff Algorithm §4.3.4

- CSMA/CD: *Collision detection* is a feature of Ethernet
- *Minimum frame length* means transmission cannot finish before collision from far end of cable detected

- Resolving this contention uses a particular algorithm, BEBA
- BEBA dynamically adjusts the retransmission delay based on the number of stations attempting to send

Ethernet Performance

Ethernet Performance **§4.3.5**

Definition 1.

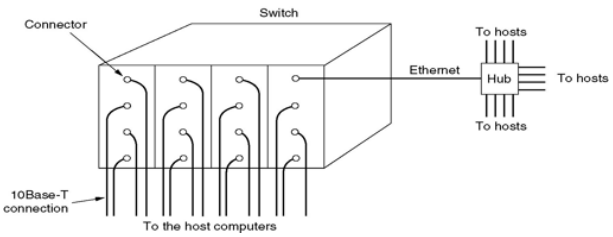
$$\text{Channel Efficiency} = \frac{1}{1 + 2BLe/cF}$$

- F : frame length
- B : bandwidth
- L : cable length
- c : speed of light
- optimal case of e contention slots per frame
- When cF is large, the channel efficiency will be high.
- Increasing network bandwidth or distance (BL) reduces the efficiency for a given frame size

Switched Ethernet

Switched Ethernet **§4.3.6**

- Switching allows the handling of *increased traffic loads* on a network
- When a station wants to transmit an Ethernet frame, it sends a standard frame to the switch.
- The switch determines if the frame is destined for another station connected to the same switch, and if so, the frame is copied there. If not, the switch transmits the frame across a high speed backbone to the station (possibly via another switch)



Fast Ethernet

Fast Ethernet **§4.3.7**

- IEEE 802.3u
  - Designed to be backward compatible with existing Ethernet LANs
  - Hesitancy to adopt a new protocol
  - Fast to implement
- Essentially a reduction in bit time from 100nsec to 10nsec - allows higher rate of transmission
- Requires hubs and switching

Fast Ethernet Cabling Types **§4.3.7**

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabit Ethernet

Gigabit Ethernet **§4.3.8**

- IEEE 802.3z
  - Goal to increase speed by factor of 10, whilst remaining backwards compatible with 802.3e and 802.3u
- Fundamentally *point to point* rather than multidrop
- Both copper and fibre cabling can be used

Gigabit Ethernet Cabling Types **§4.3.8**

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 µ) or multimode (50, 62.5 µ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Ethernet in Retrospect

Ethernet in Retrospect **§4.3.10**

- Why has Ethernet become so pervasive?
  - Reliable
  - Cheap - no specialised skills required
  - Easy to maintain
  - Good internetworking with dominant TCP/IP stack

Summary (Chapter 4)

- MAC Sub-layer
  - Compare different CSMA schemes
  - Summarise collision free protocols
  - Explain for WDMA and Wireless protocols
- Ethernet
  - Explain key features of Ethernet
  - Evaluate factors affecting Ethernet performance

Lecture XII
Tutorial: MAC Sub-Layer

1. Consider the delay of pure ALOHA versus slotted ALOHA at low load. Which one is less? Explain your answer.

2. The wireless LANs that we studied used protocols such as MACA instead of using CSMA/CD. Under what conditions, if any, would it be possible to use CSMA/CD instead?

3. Sixteen stations, numbered 1 through 16, are contending for the use of a shared channel by using the adaptive tree walk protocol. If all the stations whose adresses are prime numbers suddenly became ready at once, how many bit slots are needed to resolve the contension.

4. Six stations, A through F, communicate using the MACA protocol. Is it possible that two transmissions take place simultaneously? Explain your answer.

5. Ethernet frames must be at least 64 bytes long to ensure that the transmitter is still going in the event of a collision at the far end of the cable. Fast Ehternet has the same 64 byte minimum frame size but can get the bits out ten times faster. How is it possible to maintain the same minimum frame size?

6. A switch designed for use with fast Ethernet has a backplane that can move 10 Gbps. How many frames/sec can it handle in the worse case?

7. Give two reasons why networks might use an error-correcting code instead of error detection and retransmission.

Lecture XIII

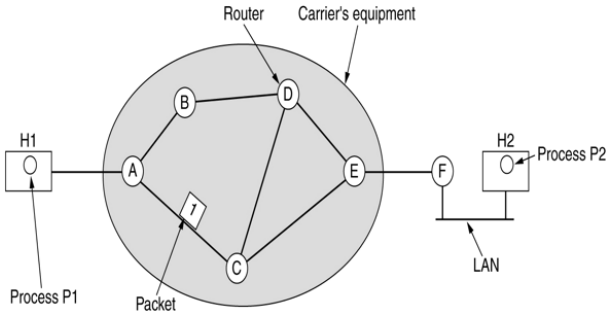
The Network Layer : Design and Implementation

Network Layer Design Issues

Network Layer Design Issues §5.1

- Which *services* are provided to the transport layer ?
- How do design issues affect *performance* ?

Store and Forward Packet Switching §5.1.1



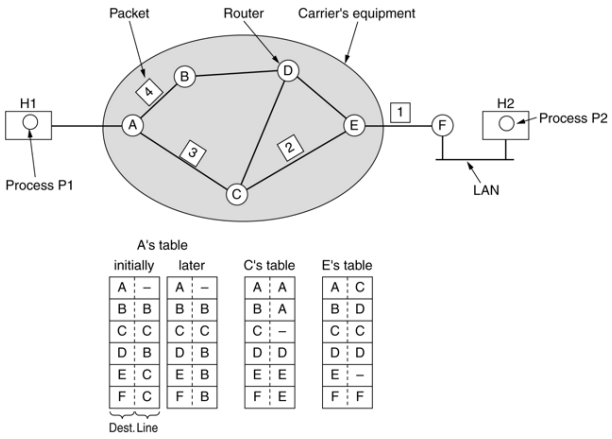
Services Provided to the Transport Layer §5.1.2

- Design goals:
  - Services should be independent of router technologies
  - Transport layer should be shielded from number, type and topology of routers
  - Network addressing should use a uniform numbering plan

Types of Services §5.1.2

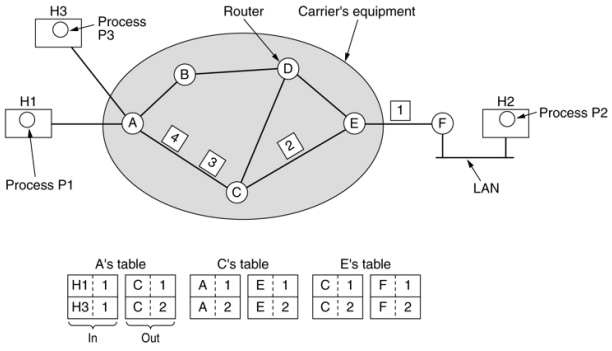
- *Connectionless*: Packets (datagrams) injected into subnet independently and packets individually routed to destination
  - Internet: move packets in a potentially unreliable subnet - QoS is not easily implemented
- *Connection-oriented*: Packets travelling between destinations all use the same route
  - Telco: guarantee reliability of subnet - QoS is important

Routing within a datagram subnet §5.1.3



Internetworking

Routing within a virtual-circuit subnet §5.1.4



Differences in Virtual Circuit and Datagram Subnets §5.1.5

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Compromises in VC and Datagram Subnets §5.1.5

- Compromises:
  - Memory vs bandwidth
    - VC's require more space in router memory, and save potential overhead in full addressing of each packet
  - Setup time vs address parsing time
    - VC's require setup time and resources, but packet transmission is very fast
  - Amount of memory
    - datagram subnets require large tables of every possible destination routes, whereas VC does not
  - QoS and congestion avoidance
    - VC's can use a tighter QoS - able to reserve CPU, bandwidth and buffer in advance
  - Longevity
    - VC's can exist for a long time eg PVC's
  - Vulnerability
    - VC's particularly vulnerable to hardware/software crashes - all VC's aborted and no traffic until they are rebuilt; datagram uses an alternative route

Routing Algorithms

Routing Algorithms §5.2

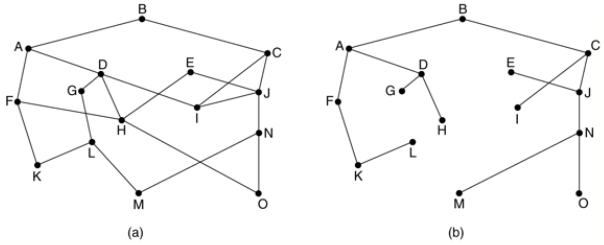
- The *routing algorithm* is responsible for deciding on which output line an incoming packet should be transmitted
- *Non-Adaptive Algorithms*
  - Static decision making process
- *Adaptive Algorithms*
  - Dynamic decision making process

Optimality Principle §5.2.1

"If router B is on the optimal path from router A to router C, then the optimal path for B to C also falls along the same route"

- The set of optimal routes from all sources to a given destination form a tree rooted at the destination -"*sink tree*"
- The goal of a routing algorithm is to discover and utilise the sink trees for all routers

Sink tree §5.2.1

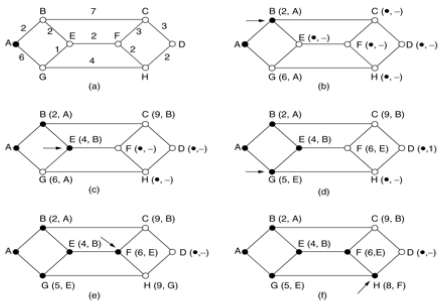


(a) A subnet. (b) A sink tree for router B.

Shortest Path Routing §5.2.2

- A *non-adaptive* algorithm
- Shortest path can be determined by building a graph with each *node* representing a router, and each *arc* representing a communication link.
- To choose a path between 2 routers, the algorithm finds the shortest path between them on the graph

Shortest path (Dijkstra's Algorithm) §5.2.2



The first 5 steps used in computing the shortest path from A to D. The arrows indicate the working node.

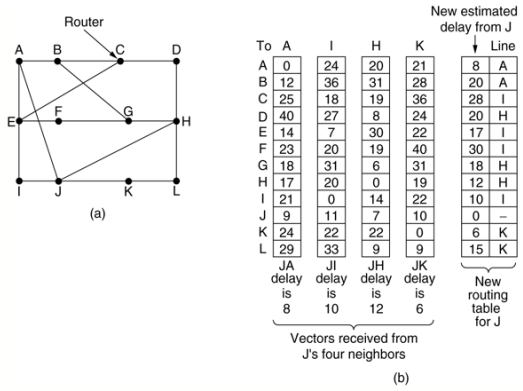
Flooding §5.2.3

- A *non-adaptive* algorithm
- Every incoming packet is sent out on *every outgoing line* except the one on which it arrived
- Generates a large number of duplicate packets - *inefficient*
- *Selective flooding* (where routers send packets only on links which are in approximately the right direction) is an improved variation

Distance Vector Routing §5.2.4

- A *dynamic* algorithm
- Each router maintains a table which includes the *best known distance* to each destination (a metric) and which line to use to get there.
- Tables are exchanged with *neighbouring routers*
- "*Global information shared locally*"

Distance Vector Routing §5.2.4

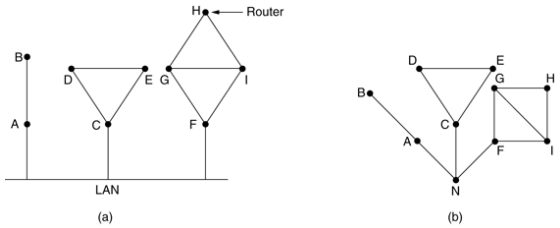


(a) A subnet (b) Input from A, I, H, K, and the new routing table for J.

Link State Routing §5.2.5

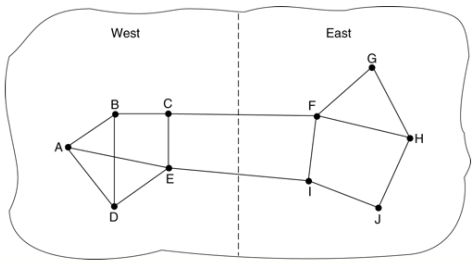
- A dynamic algorithm
- Routers:
  1. Discover neighbours and learn network addresses
  2. Measure delay or cost to each neighbour
  3. Construct packet resulting from previous steps
  4. Send this packet to all other routers
  5. Compute the shortest path to every other router
- "*Local information shared globally*"

Learning about the neighbours §5.2.5



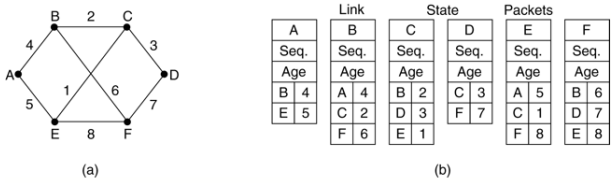
(a) Nine routers and a LAN. (b) A graph model of (a).

Measuring line cost §5.2.5



A subnet in which the East and West parts are connected by two lines.

Building link state packets §5.2.5

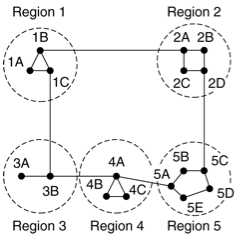


(a) A subnet. (b) The link state packets for this subnet.

Hierarchical Routing §5.2.6

- As networks grow in size, routing tables expand but this impacts CPU and memory requirements
- Dividing all routers into *regions* allows efficiencies
  - Each router knows everything about other routers in its region but nothing about routers in other regions
  - Routers which connect to two regions act as exchange points for routing decisions

Hierarchical Routing §5.2.6



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Broadcast Routing §5.2.7

- Broadcast routing allows hosts to send messages to *many or all* other hosts
  - Single distinct packet
  - Flooding
  - Multi-destination routing
    - a router receives a single packet which encapsulates the list of destinations, and then constructs a specific packet for each one (acts as a relay)
  - Reverse path forwarding
    - when a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line normally used for sending packets to the source of the broadcast. If so there is a high probability that the route used to transmit the received packet is the best route. The router then forwards the packet onto all other lines.

Multicast Routing §5.2.8

- A routing algorithm used to send a message to a well-defined group within the whole network
- Each router computes a spanning tree covering all other routers - the first router to receive the packet prunes the spanning tree to eliminate all lines which do not lead to members of the group

Lecture XIV
The Network Layer in the Internet

Internet Protocol Addressing & Numbering

Internetworking §5.5

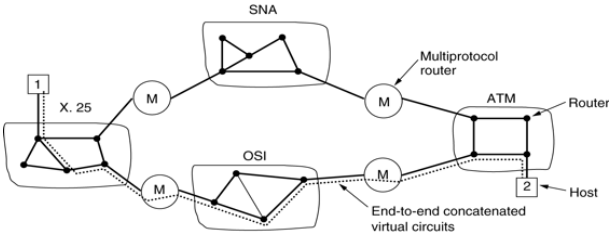
- Issues when connecting networks:
  - Different network types and protocols
  - Different motivations for network choices
  - Different technologies at both hardware and software levels

Differences at the Network Layer §5.5.1

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

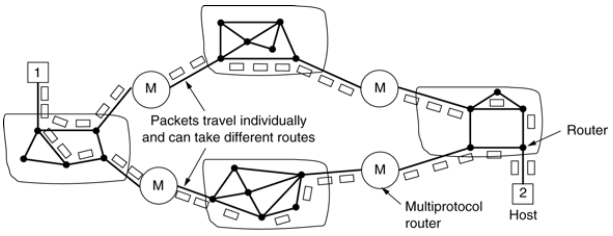
Concatenated Virtual Circuits §5.5.3

- Connection-oriented networks can be connected using concatenated virtual circuits



Connectionless Internetworking §5.5.4

- Connectionless networks can be connected using datagrams



Fragmentation §5.5.7

- All networks have a *maximum size* for packets, could be motivated by:
  - Hardware
  - Operating system
  - Protocols
  - Standards compliance
  - Desire to reduce transmissions due to errors
  - Desire for efficiency in communication channel
- *Fragmentation* (division of packets into fragments) allows network gateways to meet size constraints

Internetwork Routing §5.5.6

- Need to route:
  - *Within* a network using an *interior gateway protocol* (eg OSPF)
  - *Between* networks using an *exterior gateway protocol* (eg BGP)

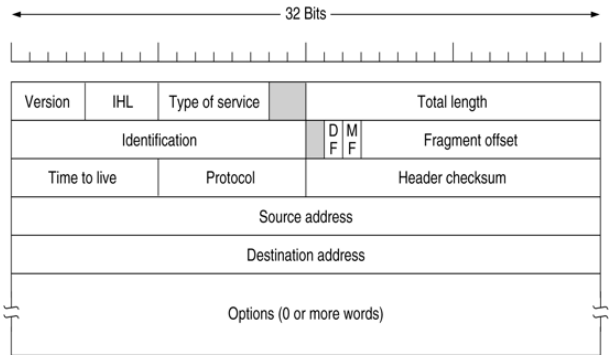
Principles of Internet Design §5.6

- RFC 1958"Architectural Principles of the Internet"(supplementary reading)
  - Core Principles
    * Make sure it works
    * Keep it simple
    * Make clear choices
    * Exploit modularity
    * Expect heterogeneity
    * Avoid static options and parameters
    * Choose a good, but not necessarily perfect design
    * Be strict in sending and tolerant in receiving
    * Consider scalability
    * Consider performance vs costs

Internet Protocol (IP) §5.6.1

- Provides a"*best-effort*"service to *route datagrams* from source host to destination host
- These hosts may be
  - On *same* network
  - On *different* networks
- Each network is called an *Autonomous System* (AS)

IPv4 Frame Structure Illustrated §5.6.1



IPv4 Frame Structure in Detail §5.6.1

- IPv4 Frame consists of a header and some text
- header is 20 byte fixed part + variable length optional part
- Version: IPv4 or IPv6
- IHL: Header Length - variable so this indicates actual
- Type: differentiates different classes of service
- Total Length: header and payload, maximum length 65535 bytes
- Identification: allows host to determine which datagram the new fragment belongs to - all fragments of same datagram have same ID
- DF: Don't Fragment byte

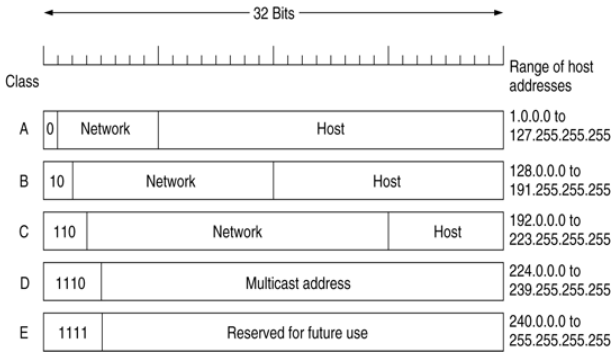
IPv4 Frame Structure in Detail (continued) §5.6.1

- MF: More Fragment byte - are there more or is this the last one ?
- Fragment offset: where in the datagram the current fragment belongs
- TTL: limits packet lifetimes - hops or seconds
- Protocol: TCP, UDP, others ...
- Header Checksum: verifies the header only
- Source Address: IP - host/network
- Destination Address: IP - host/network
- Options: eg security, strict vs loose source routing, record route, timestamp

IP Addresses §5.6.2

- IP Address is a 32 bit number that encodes network and host number eg: 128.250.32.103 (dotted decimal notation)
- 0.0.0.0 is lowest, 255.255.255.255 is highest
- Overall IP allocation responsibility of Internet Corporation for Assigned Names and Numbers (ICANN) by delegation to IANA and Regional Internet Registries (RIR's)

IP Address Formats §5.6.2



IP Numbering Schemes §5.6.1

- Class A: 128 networks, 16m hosts each
- Class B: 16,384 networks, 64k hosts each
- Class C: 2m networks, 256 hosts each
- Class D: multicast

Subnets §5.6.1

- Subnetting allows networks to be split into several parts for internal uses whilst acting like a single network for external use
- Subnet masks can be written using:
  - "dotted decimal"(eg 255.255.255.128 indicates 2 internal networks) or
  - "slash"notation (eg /25)

Common Subnet Masks §5.6.1

Number of Subnets	Subnet Mask	Slash Notation
1	255.255.255.0	/24
2	255.255.255.128	/25
4	255.255.255.192	/26
8	255.255.255.224	/27

Classful Addressing vs Classless Interdomain Routing §5.6.1

- Historically, classful addressing required allocation of complete classes (became very inefficient)
- Currently CIDR (RFC1519) allows allocation of variable sized blocks of IP address space regardless of classes

IP Addressing and Routing Tables §5.6.1

- Routing tables are typically based around a triple:
  - IP Address
  - Subnet Mask
  - Outgoing Line (physical or virtual)
- Eg: 203.32.8.0 255.255.255.0 Eth 0
- Longest mask always used when choosing a route

Control Protocols for Internetworking

Internet Control Protocols §5.6.3

- Control protocols in the network layer on the Internet
  - ICMP
  - ARP
  - RARP

ICMP §5.6.3

- *Internet Control Message Protocol*
- Used for testing and monitoring ambient conditions between hosts and routers

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ARP §5.6.3

- *Address Resolution Protocol*
- RFC 826
- Used resolve IP allocation to MAC address by broadcasting IP address to all machines on network
- *Proxy ARP* - determination of IP allocation by a third party
- *ARP Cache* - temporary storage of ARP results

RARP §5.6.3

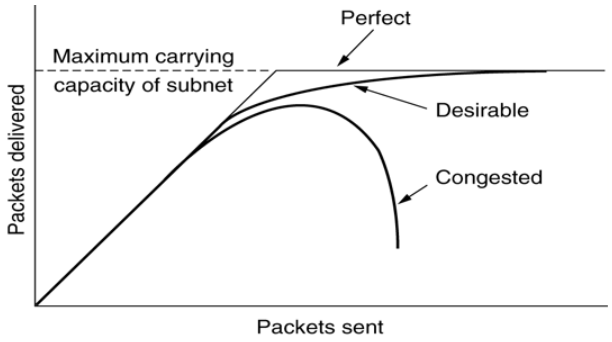
- *Reverse Address Resolution Protocol*
- RFC 903
- Used to resolve MAC addressing into IP allocation by broadcasting MAC to all machines on network

Routing and Routing Control

Routing and Routing Control

- Congestion Control Algorithms
- Quality of Service (QoS)

Congestion Control §5.3



Congestion Control vs Flow Control §5.3

- *Flow control* is an issue for point to point traffic, primarily concerned with preventing sender transmitting data faster than receiver can receive it
- *Congestion control* is an issue affecting the ability of the subnet to actually carry the available traffic, in a global context

General Network Policies Affecting Congestion §5.3.2

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Load Shedding §5.3.5

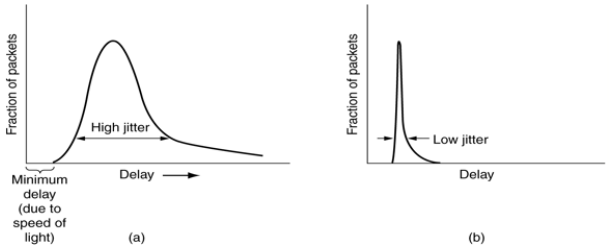
- When congestion control mechanisms fail, load shedding is the only remaining possibility - drop packets
- In order to ameliorate impact, applications can mark certain packets as priority to avoid discard policy (some applications have more stringent requirements than others)

Quality of Service §5.4

- Expected network performance is an important criterion for a wide range of network applications
- Some engineering techniques are available to guarantee Quality of Service (QoS)
- 4 parameters: reliability, delay, jitter, bandwidth

Jitter Control §5.3.6

- Jitter is the variation in packet arrival times
  - a) high jitter
  - b) low jitter



Mechanisms for Jitter Control §5.3.6

- Jitter can be contained by determining the expected transit time of a packet
- Packets can be "shuffled" at each hop in order to minimise jitter - slower packets sent first, faster packets wait in a queue
- For certain applications jitter control is extremely important (eg Voice Over IP), as it directly affects the quality perceived by the application user

QoS Requirements §5.4.1

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Techniques for Good QoS #1 §5.4.2

- Over-provisioning
  - more than adequate buffer, router CPU, and bandwidth (expensive and not scalable ... yet)
- Buffering
  - buffer received flows before delivery - increases delay, but smoothes out jitter, no effect in reliability or bandwidth
- Traffic Shaping
  - regulate the average rate of transmission and burstiness of transmission
- "Buckets"
  - leaky bucket: finite internal queue (in a buffer), regulates outbound flow as well as inbound flow
  - token bucket: finite internal queue (in buffer), variable to maximum outbound flow

Techniques for Good QoS #2 §5.4.2

- Resource Reservation
  - reserve bandwidth, buffer space, CPU in advance
- Admission Control
  - routers can decide based on traffic patterns whether to accept new flows, or reject/reroute them
- Proportional Routing

  - different traffic types for same destination split across multiple routes
- Packet Scheduling
  - fair queuing, weighted fair queueing

Summary (Chapter 5)

- Routing
  - Summarise differences between VC and Datagram subnetworks
  - Demonstrate and contrast Distance Vector and Link State Routing
- Internet Protocol
  - Explain principles of Internet design
  - Analyse structure of IP addresses
  - Explain roles of different Internet Control Protocols
- Quality of Service
  - Summarise effects on congestion of policies at different layers
  - Characterise QoS requirements of different applications

Lecture XV
Tutorial: Network Layer

1. If there are n independent paths between two nodes in a network, and the probability that an individual path is working is p, what is the probability of these two nodes being connected? Assume path failures are independent. (Hint: first try to calculate what is the probability that all paths have failed)

2. Give two example computer applications for which connection-oriented service is appropriate. Now give two examples for which connectionless service is best.

3. Assuming that all routers and hosts are working properly and that all software in both is free of all errors, is there any chance, however small, that a packet will be delivered to the wrong destination?

4. Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is.

5. Is fragmentation needed in concatenated virtual-circuit internets or only in datagram systems?

6. A router blasting out IP packets whose total length (header plus data) is 1024 bytes. Assuming that packets live for 10 sec, what is the maximum line speed the router can operate at without danger of cycling through the IP datagram ID number space?

7. Suppose that instead of using 16 bits for the network part of a class B address originally, 20 bits had been used. How many class B networks would there have been?

8. A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts that it can handle?

9. A router has just received the following IP addresses: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21 and 57.6.120.0/21. If all of them use the same outgoing line, can they be aggregated? If so, to what? If not, why not?

10. A router has the following (CIDR) entries in its routing table:

Address/mask	Next hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
default	Router 2

For each of the following IP adresses, what does the router do if a packet with that address arrives? a) 135.46.63.10, b) 135.46.57.14, c) 135.46.52.2, d) 192.53.40.7, e) 192.53.56.7

11. You have just explained the ARP protocol to a friend. When you are all done, he says "I've got it. ARP provides a service to the network layer, so it is a part of the data link layer." What do you say to him?

12. IPv6 uses 16 bytes addresses. If a block of 1 million addresses is allocated every picosecond, how long will the addresses last?

13. The *Protocol* field used in the IPv4 header is not present in the fixed IPv6 header. Why not?

Lecture XVI

Transport Layer Fundamentals: Services, Primitives and Connecting

The Transport Service §6.1

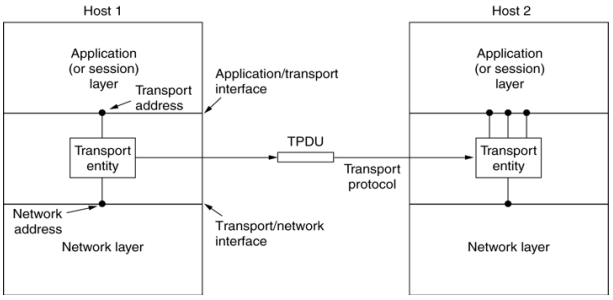
- Primary function
  - provide reliable cost-effective data transport from source to destination, independent of physical or data networks

Transport Layer Services

Transport Layer Services §6.1.1

- Transport Layer *Services* provide interfaces between the Application Layer and the Network Layer
- Transport *Entities* (the hardware or software which actually does the work) can exist in multiple locations:
  - OS kernel
  - User process
  - System library
  - NIC

The Transport Entity Illustrated §6.1.1



Types of Transport Layer Services §6.1.1

- We revisit 2 fundamental service types we have seen in the Data, MAC and Network layers:
  - *Connection-oriented*: connection establishment, data transfer, connection release
  - *Connectionless*: data transfer

Transport Layer and Network Layer Services Compared §6.1.1

- If *transport* and *network* layers are so similar, why are there two layers?
  - Transport layer code runs entirely on *hosts*
  - Network layer code runs almost entirely on *routers*
  - Transport layer can fix *reliability problems* caused by the Network layer eg delayed, lost or duplicated packets

Role of the Transport Layer §6.1.1

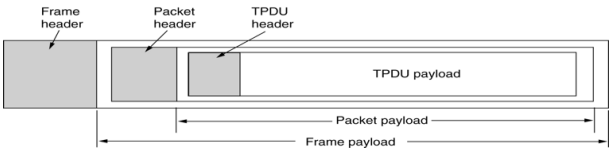
- The Transport Layer occupies a key position in the layer hierarchy because it clearly delineates
  - *providers* of reliable data transmission services
    - at the network, data and physical layers
  - *users* of reliable data transmission services
    - at the application and session layers
- In particular, connection-oriented transport services provide a *reliable service* on top of an *unreliable network*

Features of Transport Layer §6.1.1

- Mechanism for improved QoS for users
  - Reliability at application level through interface with network layer
  - Abstraction and primitives provide a *simpler API* for application developers independent of network layer

Transport Layer Encapsulation §6.1.2

- Abstract representation of messages sent to and from transport entities
  - Transport Protocol Data Unit (TPDU)
- Encapsulation of *TPDUs* (transport layer units) in *packets* (network layer units) in *frames* (data layer units)



Transport Layer Primitives

Transport Service Primitives §6.1.2

- Primitives: core functions which allow interface with transport services

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

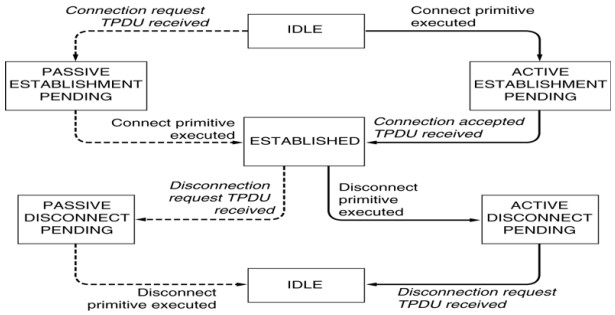
Simple Connections and Primitives §6.1.2

- Server executes *LISTEN*
- Client executes *CONNECT*
  - Sends CONNECTION REQUEST TPDU to Server
  - Receives CONNECTION ACCEPTED TPDU to Client
- Data exchanged using *SEND* and *RECEIVE*
- Either party executes *DISCONNECT*

Disconnection Primitives §6.1.2

- *Asymmetric* Disconnection
  - Either party can issue a DISCONNECT, which results in DISCONNECT TPDU and transmission ends in both directions
- *Symmetric* Disconnection
  - Both parties issue DISCONNECT, closing only one direction at a time - allows flexibility to remain in receive mode

Simple Connections Illustrated §6.1.2



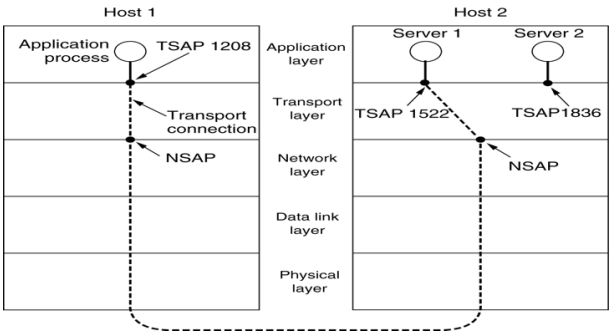
Transport vs Data Link Protocols §6.2

- Transport services are implemented as protocols used between transport entities
- Transport services have some *similarities* with *data link* protocols
  - error control
  - Sequencing
  - flow control
- Transport services have some *differences* with *data link* protocols
  - physical network vs physical/data/network
  - addressing
  - connection establishment
  - storage

Addressing §6.2.1

- Specification of remote process to connect to is required at application and transport layers
- Addressing in transport layer is typically done using *Transport Service Access Points* (TSAPs)
  - on the internet, a TSAP is commonly referred to as a *port* (eg port 80)
- Addressing in the network later is typically done using *Network Service Access Points* (NSAPs)
  - on the internet, the concept of an NSAP is commonly interpreted as simply an *IP address*

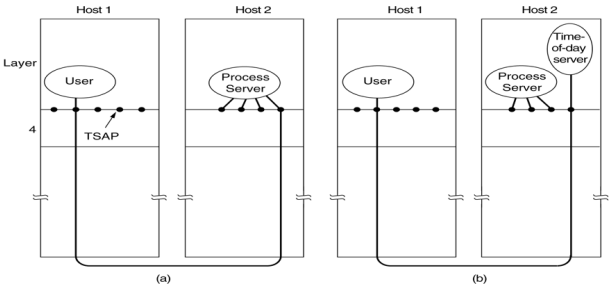
TSAPs, NSAPs and Transport Layer Connections Illustrated §6.2.1



Two Types of TSAP Allocation §6.2.1

- Static
  - Well known services have standard allocated TSAPs/ports, which are embedded in OS
  - cf. Unix /etc/services, www.iana.org
- Mediated
  - A process server intercepts inbound connections and spawns requested server and attaches inbound connection
    - cf. Unix /etc/(x)inetd

TSAP Allocation Illustrated §6.2.1



- (a) Process Server intercepts inbound connection
- (b) Process Server attaches inbound connection to spawned server process

Connection Establishment in the Real World §6.2.2

- When networks can *lose, store and duplicate* packets, connection establishment can be complicated
  - congested networks may delay acknowledgements
  - incurring repeated multiple transmissions
  - any of which may not arrive at all or out of sequence - *delayed duplicates*
- Applications degenerate with such congestion (eg. imagine duplication of bank withdrawals)

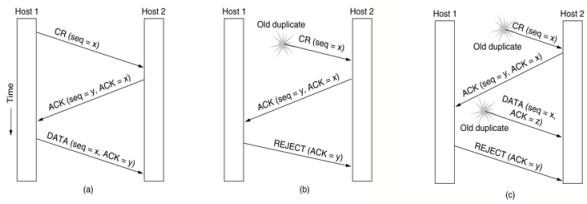
Reliable Connection Establishment §6.2.2

- Ensure *packet lifetimes* are bounded
- Assign *sequence numbers* that will not be reused within a packet lifetime
- Ensure initial send and receive sequence numbers are *agreed* at start of connection: *three way handshake*

Three Way Handshake §6.2.2

- Tomlinson (1975): Devised solution which avoids problems which can occur when both sides allocate same sequence numbers by accident (eg after host /router crash)
- Sender and receivers exchange information about which sequencing strategy each will use, and agree on it before transmitting TPDU's

Three Way Handshake §6.2.2



- (a) Normal operation,
- (b) Old CONNECTION REQUEST appearing out of nowhere.
- (c) Duplicate CONNECTION REQUEST and duplicate ACK.

Connection Release §6.2.3

- Asymmetric vs Symmetric connection release types
- *Asymmetric* release may result in data loss hence symmetric release is more attractive
- *Symmetric* release works well where each process has a set amount of data to transmit and knows when it has been sent
- What happens in other cases?

Resolving the Connection Release Problem §6.2.3

- How to we decide the importance of the last message? Is it essential or not?
- No protocol exists which can resolve this ambiguity
- Strategies to allow connection release
  - 3 way handshake
  - Finite retry
  - Timeouts

Sockets

Sockets §6.1.3

- Sockets widely used for interconnections
  - "Berkeley"sockets are predominant in internet applications
- Socket model does not include the TPDU concept

Socket Primitives for TCP §6.1.3

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Lecture XVII
Transport Layer Protocols for the Internet

Internet Transport Protocols

UDP (connectionless)

User Datagram Protocol (UDP) §6.4.1

- RFC 768
- Provides a protocol whereby applications can transmit encapsulated IP datagrams without a connection establishment
- UDP transmits in segments consisting of an 8-byte header followed by the payload
- UDP headers contain source and destination ports, payload is handed to the process which is attached to the particular port at destination (using BIND primitive or similar)

User Datagram Protocol (UDP) §6.4.1

- Main *advantage* of using UDP over raw IP is the ability to specify ports for source and destination pairs
- Both source and destination ports are required - destination allows initial routing for incoming segments, source allows reply routing for outgoing segments

Strengths and Weaknesses of UDP §6.4.1

- *Strengths*: provides an IP interface with multiplexing/de-multiplexing capabilities and consequently, transmission efficiencies
- *Weaknesses*: UDP does not include support for flow control, error control or retransmission of bad segments
- *Conclusion*: where applications require a precise level of control over packet flow/error/timing, UDP is a good choice

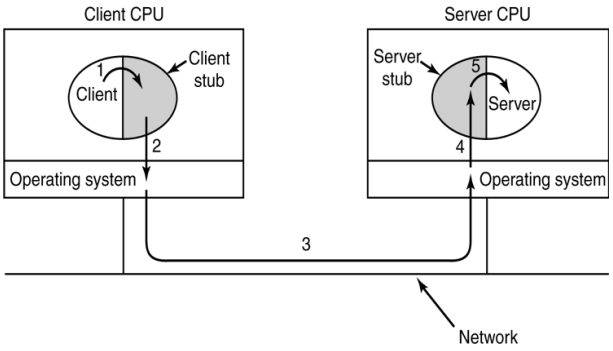
Using UDP: Remote Procedure Call (RPC) §6.4.2

- Sending a message and getting a reply back is analogous to making a *function call* in programming languages
- Birrell and Nelson (1984) modified this approach to allow local programs to call procedures on remote hosts using UDP as the transport protocol
  - *Remote Procedure Call (RPC)*

Using UDP: Remote Procedure Call (RPC) §6.4.2

- To call a remote procedure, the client is bound to a small library (the *client stub*) that represents the server procedure in the client's address space.
- Similarly the server is bound with a procedure called the *server stub*. These stubs hide the fact that the procedure itself is not local.

RPC Illustrated §6.4.2



TCP (connection-oriented)

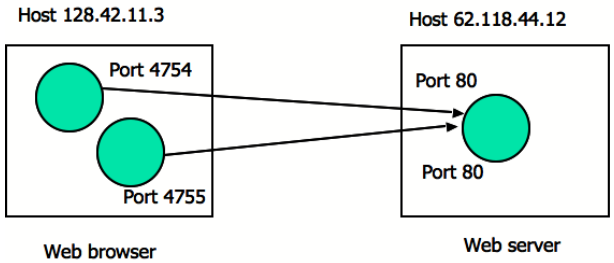
Transmission Control Protocol (TCP) §6.5.1

- RFC 793, 1122, 1323
- Provides a protocol by which applications can transmit IP datagrams within a *connection-oriented* framework, thus increasing reliability
- TCP transport entity manages TCP streams and interfaces to the IP layer - can exist in numerous locations (kernel, library, user process)
- TCP entity accepts user data streams, and segments them into pieces <64Kb (often 1460b in order to fit the IP and TCP headers into a single Ethernet frame), and sends each piece as a separate IP datagram
- Recipient TCP entities reconstruct the original byte streams from the encapsulation

The TCP Service Model §6.5.2

- Sender and receiver both create"*sockets*", consisting of the IP address of the host and a port number
- For TCP Service to be activated, connections must be explicitly established between a socket at a sending host *(src-host, src-port)* and a socket at a receiving host *(dest-host, dest-port)*
- A socket may be used for multiple connections simultaneously

Example §6.5.1



Port Allocations §6.5.2

- Recall TSAPs from earlier lecture
- Port numbers can range from 0-65535
- Port numbers are regulated by IANA (http://www.iana.org/assignments/port-numbers)
- Ports are classified into 3 segments:
  - Well Known Ports (0-1023)
    - 21 FTP
    - 22 SSH
    - 23 Telnet
    - 25 SMTP
    - 80 HTTP
    - 110 POP3

    * 119 NNTP
  - Registered Ports (1024-49151)
  - Dynamic Ports (49152-65535)

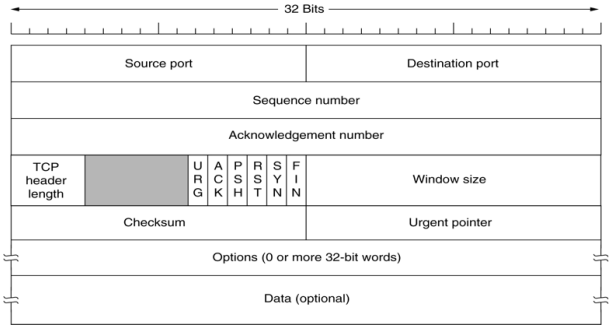
Features of TCP Connections §6.5.2

- TCP connections are:
  - *Full duplex* - data in both directions simultaneously
  - *Point to point* - exact pairs of senders and receivers
  - *Byte streams*, not message streams - message boundaries are not preserved
  - *Buffer capable* - TCP entity can choose to buffer prior to sending or not depending on the context
    * PUSH flag - indicates a transmission not to be delayed
    * URGENT flag - indicates that transmission should be sent immediately (priority above in process data)

TCP Protocol §6.5.3

- Data exchanged between TCP entities in segments - each segment has a fixed 20 byte header plus zero or more data bytes
- TCP entities decide how large segments should be within 2 constraints, namely:
  - 65,515 byte IP payload
  - Maximum Transfer Unit (MTU) - generally 1500 bytes
- *Sliding window protocol* - sender transmits and starts a timer, receiver sends back an acknowledgement which is the next sequence number expected - if sender's timer expires before acknowledgement, then the sender transmits the original segment again

The TCP Segment Header §6.5.4



TCP Connection Establishment and Release §6.5.5,6

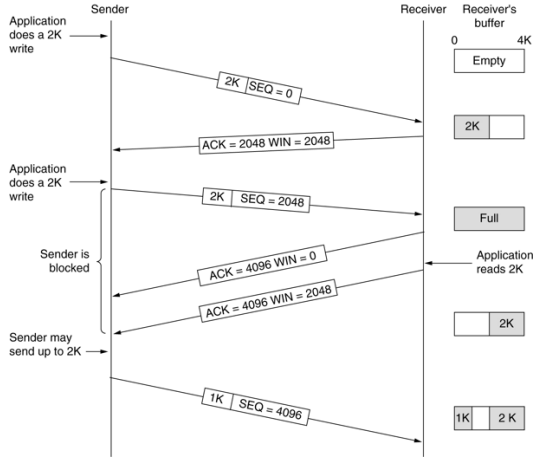
- Connections established using *three-way handshake*
- Two simultaneous connection attempts results in only one connection (uniquely identified by end points)
- Connections released asynchronously (2 x asymmetric releases, one for each transmission direction)
- Timers used to lost connection releases (three army problem)

Modelling TCP Connection Management - States §6.5.7

State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

TCP Transmission Policy §6.5.8

- TCP acknowledges bytes, not packets
- Receiver advertises window based on available buffer space



TCP and Congestion Control §6.5.9

- When networks are overloaded, congestion occurs, potentially affecting all layers
- Although lower layers (data and network) attempt to ameliorate congestion, in reality TCP impacts congestion most significantly because TCP offers methods to transparently reduce the data rate, and hence reduce congestion itself

The TCP Approach to Congestion Control §6.5.9

- TCP adopts a defensive stance - open loop solution
  - At connection establishment, a suitable window size is chosen by the receiver based on its buffer size
  - If the sender is constrained to this size, then congestion problems will not occur due to buffer overflow at the receiver itself, but may still occur due to congestion within the network

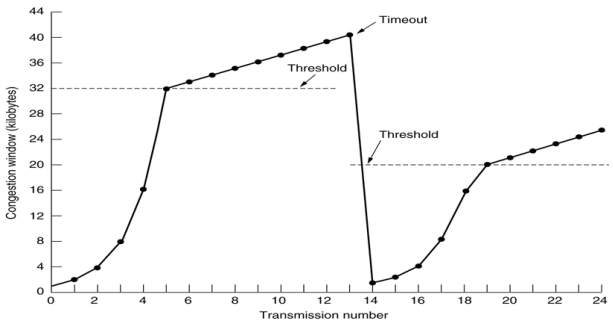
Incremental Congestion Control: Design §6.5.9

- Two different problems exist
  - *network capacity* and *receiver capacity*
  - these should be dealt with separately, but compatibly
- The sender maintains two windows
  - *Window* described by the *receiver*
  - *Congestion window*
- Each regulates the number of bytes the sender can transmit - the maximum transmission rate is the minimum of the two windows

Incremental Congestion Control: Implementation §6.5.9

- On connection establishment, the sender initializes the congestion window to the size of the maximum segment in use on the connection, and transmits one segment
- If this segment is acknowledged before the timer expires, the sender adds another segment's worth of bytes to the congestion window, making it two maximum size segments, and transmits two segments
- As each new segment is acknowledged, the congestion window is increased by one maximum segment size
- In effect, each acknowledgement doubles the congestion window - which grows until either a timeout occurs or the receiver's specified window is reached

Internet Congestion Control Illustrated §6.5.9



Summary (Chapter 6)

- Transport Layer Services
  - Discuss challenges in providing reliable services over unreliable network layer
  - Explain solutions for connection establishment and release
- Internet Transport Protocols
  - Characterise differences between TCP and UDP
  - Explain TCP congestion control

Lecture XVIII

Tutorial: Transport Layer

1. Why does the maximum packet lifetime, T, have to be large enough to ensure that not only the packet but also its acknowledgements have vanished?

2. Imagine that a two-way handshake, rather than a three-way handshake were used to set up connections. In other words, the third message was not required. Are deadlocks now possible? Give an example or show that none exist.

3. Why does UDP exist? Would it not have been enough to just let the user processes send raw IP packets?

4. A client sends a 128 byte request to a server located 100 km away over a 1 gigabit optical fibre. What is the efficiency of the line during the remote proceedure call?

5. Both UDP and TCP use port numbers to identify the destination entity when delivering a message. Given two reasons for why these protocols invented a new abstract ID (port numbers), instead of using process IDs, which already existed when these protocols were designed?

6. Datagram fragmentation and reassembly are handled by IP and are invisible to TCP. Does this mean the TCP does not have to worry about data arriving in the wrong order?

7. A process on host 1 has been assigned port p, and a process on host 2 has been assigned port q. Is is possible for there to be two or more TCP connections between these two ports at the same time?

8. The maximum payload of a TCP segment is $65,495$ bytes. Why was such a strange number chosen?

9. Suppose that the TCP congestion windown is set to 18 KB and a timeout occurs. How big will the window be if the next four trasmission bursts are successful? Assume that the maximum segment size is 1 KB.

10. To get around the problem of sequence numbers wrapping around while old packets still exist, one could use 64 bit sequence numbers. However, theoretically, an optical fibre can run at 75 Tbps. What maximum packet lifetime is required to make sure that future 75 Tbps networks do not have wraparound problems even with 64 bit sequence numbers? Assume that each byte has its own sequence number, as TCP does.

Lecture XIX

Core Internet Applications: Domain Name System

Domain Name System

DNS §7.1

- DNS = Domain Name System
- Essentially, the technology behind mapping *host.domain.com* to an *IP address*
- A hierarchical, domain-based naming scheme and distributed database for implementing the naming scheme
- Integrates network addressing and human-readable addressing conventions
- The primary function of DNS is to map domain names to *resource records* (in both forward and reverse directions - somewhat analogous to ARP/RARP for IP/MAC mappings)

DNS Codified §7.1

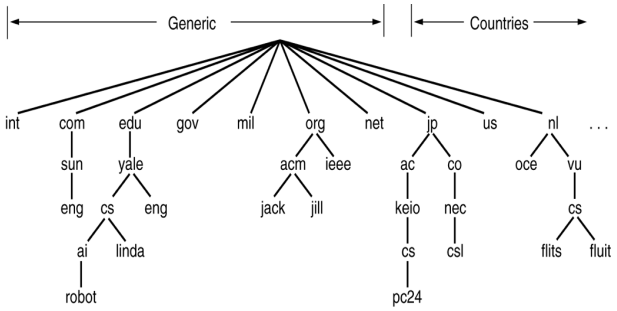
- Number of RFC's is directly related to importance of DNS as a foundation to many other services
  - RFC 1034: Domain Names - Concepts and Facilities
  - RFC 1035: Domain Names: Implementation and Specification
  - RFC 1519: Domain Name System Structure and Delegation
  - RFC 2219: Use of DNS Aliases for Network Services
  - RFC 2606: Reserved Top Level DNS Names
  - RFC 3647: Role of the Domain Name System

Domain Name Characteristics §7.1

- Domain names:
  - Are case insensitive
  - Can have up to 63 characters per constituent
  - Can have up to 255 chars per path
  - Can be internationalised (since 1999)
- Naming conventions usually follow either organisational or physical boundaries eg.
  - au.ibm.com / uk.ibm.com (for email)
  - ibm.com.au / ibm.co.uk (for web)
- Absolute domain names ends in a .
- Relative domain names end in a constituent eg .com

Division of Name Spaces

Conceptual Divisions of DNS Namespace §7.1.1



Domain Name Properties and Units

Resource Records §7.1.2

- The Resource Record (RR) is the main object in the Domain Name System
- A RR consists of a domain name, TTL, class, type, value
  - Domain Name: which domain this record applies to
  - TTL: indicates stability or temporal extent of the record
  - Class: IN for internet (others exist, but deprecated)
  - Type: a closed vocabulary of the following:

    - A : The Internet address of the host
    - CNAME : The canonical name for an alias
    - MX : The mail exchanger
    - NS : The name server
    - PTR : The host name if the query is in the form of an Internet address; otherwise the pointer to other information
    - SOA : The domain's start-of-authority information
  - Value: data (semantics depend on record type)

Resolving Domain Names

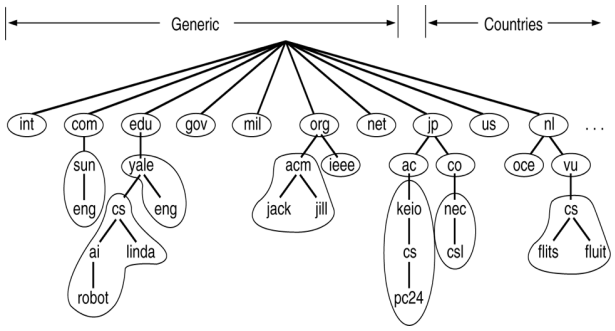
A Typical DNS Query: nslookup §7.1.2

```
[badenh@mundroo] badenh [1:52] nslookup
Default Server:  muruke.cs.mu.OZ.AU
Address:  128.250.37.78

> www.cs.mu.oz.au
Server:  muruke.cs.mu.OZ.AU
Address:  128.250.37.78

Name:    muckleshoot.cs.mu.oz.au
Address:  128.250.37.80
Aliases:  www.cs.mu.oz.au

> www.unimelb.edu.au
Server:  muruke.cs.mu.OZ.AU
Address:  128.250.37.78

Non-authoritative answer:
Name:    www.unimelb.edu.au
Address:  128.250.6.182
```

A Typical DNS Query: dig §7.1.2

```
[badenh@isogawa badenh]$ dig @203.32.8.111 www.cs.mu.oz.au

; <<>> DiG 9.2.1 <<>> @203.32.8.111 www.cs.mu.oz.au
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38114
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; QUESTION SECTION:
;www.cs.mu.oz.au.               IN      A

;; ANSWER SECTION:
www.cs.mu.oz.au.        14382   IN      CNAME   muckleshoot.cs.mu.oz.au.
muckleshoot.cs.mu.oz.au. 14382  IN      A       128.250.37.80

;; AUTHORITY SECTION:
cs.mu.oz.au.            14382   IN      NS      munnari.oz.au.
cs.mu.oz.au.            14382   IN      NS      rip.psg.COM.
cs.mu.oz.au.            14382   IN      NS      mulga.cs.mu.oz.au.

;; ADDITIONAL SECTION:
mulga.cs.mu.oz.au.      12993   IN      A       128.250.1.22

;; Query time: 35 msec
;; SERVER: 203.32.8.111#53(203.32.8.111)
;; WHEN: Mon Oct  6 08:59:58 2003
;; MSG SIZE  rcvd: 158
```

Zones in DNS Namespace §7.1.3



DNS Zone Files §7.1.3

- A *zone file* contains the DNS information
- DNS zone files have two types:
  - Forward zone files
    - Allow queries to resolve host and domain names to IP addresses
  - Reverse zone files
    - Allow queries to resolve IP addresses to host and domain names
- Some internet services depend on being able to perform *reverse lookups*, and in general for IP address space, the Regional Internet Registry holds a default reverse zone file (in-addr.arpa)

Name Servers

Zone Name Servers §7.1.3

- DNS namespace divided into overlapping zones
- Each zone contains a part of the DNS tree and also name servers authoritative for that zone -
  - usually 2 nameservers for a zone (called the primary and secondary nameservers),
  - sometimes secondary is actually outside the zone (for reliability)
- Name servers are arranged in a hierarchical manner extending from a set of root servers

Root Name Servers §7.1.3

- The root servers form the authoritative cluster for enquiry in the event of locally-unresolvable name queries
- There are 12 root servers globally
  - In some cases, a root server is a cluster of servers that are in the anycast IP space
    - F-ROOT 13 servers
    - J-ROOT 8 servers

DNS In Action §7.1.3

- A *resolver client* asks *local NS* for the domain to IP mapping, if answer is known by the local NS, then it sends the answer
- If answer is not known then the *local NS* queries the *top level (root) NS* for domain and then relays the answer to the resolver client
- Essentially this is a recursive query mode
- Queries are subject to timers to avoid longer than necessary response times

DNS Software

- DNS Server Software
  - BIND
  - djbdns
  - Microsoft Domain Name Server
- DNS Query Tools
  - nslookup
  - dig

Lecture XX
Core Internet Applications: Email

Email

Email Services §7.2

- Email has a long heritage (since 1960's), in this time evolutionary steps in infrastructure and standards have been taken
- Standards for Internet-enabled email are based on 2 RFC's
  - RFC 821 (transmission)
  - RFC 822 (message format)
  - RFC 2821 and RFC 2822 (revised versions of earlier RFCs)
- Alternative schemas were based on the X.400 series of standards (now largely defunct)

Email Architecture and Services §7.2.1

- *User agents* (UA's/ MUA's)
  - Allow user to read and send email
- *Message transfer agents* (MTA's)
  - Transport messages from source - destination

The User Agent

The User Agent §7.2.2

- Basic functions: compose, report, display, dispose
- *Envelope* and *contents*: encapsulation of transport related information
- *Header* and *body*: header - user agent control info; body for human recipient
- User must provide message, destination, optional other parameters
- Addressing scheme *user@dns-address*

Message Formats and Components

Message Formats §7.2.3

- Message =
  - RFC821 envelope
  - Header fields (line of ASCII text with fieldname:value syntax)
  - Blank line delimiter
  - Message body

Email Headers §7.2.3

```
Return-Path: <sb@cs.mu.oz.au>
Received: from unagi.cis.upenn.edu (UNAGI.CIS.UPENN.E-
        DU [158.130.8.153]) by mulga.cs.mu.OZ.AU with
        ESMTP id JAA10247; Mon, 6 Oct 2003 09:05:02
        +1000 (EST)
Received: from sb.wlan.cs.mu.OZ.AU (sb.wlan.cs.mu.OZ.-
        AU [128.250.23.34]) (authenticated bits=0) by
        unagi.cis.upenn.edu (8.12.10/8.12.9) with ESMTP
        id h95N4w2r005541; Sun, 5 Oct 2003 19:05:00
        -0400 (EDT)
Subject: Dafydd Gibbon's Office Allocation
From: Steven Bird <sb@cs.mu.OZ.AU>
To: Baden Hughes <badenh@cs.mu.OZ.AU>
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
X-Mailer: Ximian Evolution 1.0.8
Date: 06 Oct 2003 09:02:33 +1000
Message-Id: <1065394956.2989.2.camel@aviary>
Mime-Version: 1.0
X-UIDL: 6c802a08612557283e1b8c10adc367b7
```

RFC 822: Message Transport §7.2.3

- RFC 822 doesn't distinguish header and envelope fields
- RFC 822 headers related to message transport
  - To:
  - Cc:
  - Bcc:
  - From:
  - Sender:
  - Received:
  - Return-Path:

RFC 822: Message Header §7.2.3

- RFC 822 headers related to message header
  - Date:
  - Reply-To:
  - Message-Id:
  - In-Reply-To:
  - References
  - Keywords:
  - Subject:
- RFC 822 allows users to invent new headers for private use but they must start with X-

Multipurpose Internet Mail Extentsions (MIME) #1 §7.2.3

- In the early days of email, messages were in English and used only ASCII - RFC 822 reflects these simple constraints.
- In time the inadequacy of RFC822 became apparent
  - Languages with accents (French, Spanish)
  - Non-Latin alphabets (eg Cyrillic)
  - Non-alphabetic language (eg Chinese, Japanese)
  - Messages with content other than text (audio, images)
- As a result, MIME (RFC 1341) was written (later updated in RFCs 2045-2049)

Multipurpose Internet Mail Extentsions (MIME) #2 §7.2.3

- MIME retains RFC822 format but adds structural elements to the message body and defines encoding rules for non-ASCII messages - thus leverage existing infrastructure for RFC822 services, and leaving MIME functionality changes to the user agent
- MIME has 5 additional message headers:
  - MIME-Version: identifies the MIME version
  - Content-Description: human readable describing contents
  - Content-Id: unique identifier
  - Content-Transfer-Encoding: how body is wrapped for transmission
  - Content-Type: type and format of content

MIME Types and Subtypes §7.2.3

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

Message Transfer Protocols

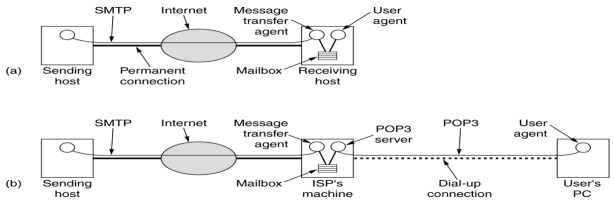
Message Transfer §7.2.4

- Transfer
  - SMTP
- Delivery
  - Local
  - POP3
  - IMAP

SMTP §7.2.4

- Simple Message Transfer Protocol
- Simple ASCII protocol, operating on TCP port 25
- RFC 821: Simple Mail Transfer Protocol
- RFC 2821: Extended Simple Mail Transfer Protocol
- RFC 2821 delineated by HELO vs EHLO, new features of 2821

Receiving Local vs Remote Mail §7.2.5



- (a) Sending and reading mail when the receiver has a permanent Internet connection and the user agent runs on the same machine as the message transfer agent.
- (b) Reading e-mail when the receiver has a dial-up connection to an ISP.

POP3 §7.2.5

- Post Office Protocol
- RFC 1939: Post Office Protocol - Version 3
- 3 states of a POP3 transaction
  - Authorisation
  - Transactions
  - Update
- POP3 Syntax
  - USER / PASS
  - LIST
  - RETR / DELE
  - QUIT (update)

IMAP §7.2.5

- Internet Message Access Protocol
- Retain mailbox contents online and allow manipulation of online and offline messages and mailbox folders
- Implications of server infrastructure to support high volume of IMAP users (implies storage projections by the provider, and hence limitations)
- RFC 2060 & RFC 3051: Internet Message Access Protocol

POP3 and IMAP Compared §7.2.5

Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

Email Software

- UA's
  - Outlook (+Express), Eudora, Pine, Mutt, mh, Evolution, Thunderbird
- Agent Middleware (User -> Server)
  - Pop3d, qpopper, fetchmail
- MTA's
  - sendmail, Qmail, PostFix, Exchange, MDaemon, IMail

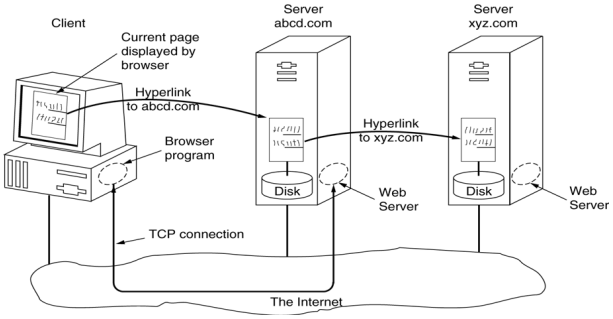
Lecture XXI
Core Internet Applications: WWW

World Wide Web

World Wide Web §7.3

- History: CERN 1989, Hypertext 1991 Conf - Tim Berners-Lee
- Marc Andreessen @ UIUC Mosaic 1993, then Netscape
- Browser wars MS and Netscape 1994-1998
- W3C 1994 (CERN, MIT) internet standards body

Component Model of WWW Technologies §7.3.1



Architectural Overview §7.3.1

- Client - Server Model
  - Client - Browser based access to pages
  - Server - daemon based content delivery of pages
  - URL
    - *Protocol + DNS Name + file name*
    - Extensions of URL - URN (location independent)

HTTP

HTTP §7.3.4

- Hypertext Transfer Protocol
- RFC 2616: Hypertext Transfer Protocol 1.1
- Connections:
  - HTTP 1.0 - single connect for each transaction for each client-server pair,
  - HTTP 1.1 persistent connections per server-client pair
- Methods: GET / PUT

HTTP Request Methods §7.3.4

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

HTTP Error Codes §7.3.4

Code	Meaning	Examples
1xx	Information	100 = server agrees to handle client's request
2xx	Success	200 = request succeeded; 204 = no content present
3xx	Redirection	301 = page moved; 304 = cached page still valid
4xx	Client error	403 = forbidden page; 404 = page not found
5xx	Server error	500 = internal server error; 503 = try again later

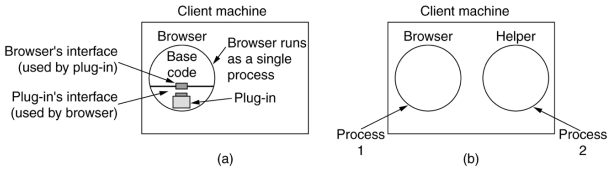
Client Side Process §7.3.1

- 9 Step process
  - Browser determines URL
  - Browser conducts DNS lookup to determine IP Address
  - DNS replies
  - Browser connects to IP Address on TCP port 80
  - Browser requests the specified file
  - Server sends the specified file
  - Server releases the TCP connection
  - Browser displays specified file
  - Browser fetches and displays all associated content (images etc)

Client Side Content §7.3.1

- HTML + other types
- Plugins - integrated software module which executes inside the browser, direct access to online context
- Helper - separate program which can be instantiated by the browser, but can only access local cache of file content
  - application/pdf
  - application/msword
- Integration of browser and OS based MIME dependencies
- Risks eg exe's

Plugins vs Helpers §7.3.1



- a) a plugin
- b) a helper application

Server Side WWW §7.3.1

- 5 step process
  - Accept TCP Connection from client (browser)
  - Identify the file requested
  - Get the specified file from the local disk storage
  - Send the file to the client
  - Release the TCP connection

Cookies §7.3.1

- The Web is basically stateless
- Cookies to place small amount (<4Kb) of info on users computer and re-use deterministically (RFC 2109)
- Cookies have 5 fields - domain, path, content, expiry, security
- Questionable mechanism for tracking users (invisibly perhaps) and learning about user behaviour eg competitor snooping, undesirable content etc

Web markup languages

Static Web Documents §7.3.2

- HTML - Hypertext Markup Language
  - a simple language designed to encode both content and presentational information
  - Plain text encoding, with browser based rendering
  - Restricted to ISO-8859 Latin-1 character set (internationalisation not introduced until XHTML with UTF encodings)
- Web Page Components
  - Structural divisions:
    - Head <head> ... </head>
    - Body <body> ... </body>
  - Syntactically Restricted Tag Sets
  - Attributes & Values <img src="pic1.gif"alt="pic1.gif">

Evolution of Functions in HTML §7.3.2

- HTML 1.0 (CERN 1991)
  - hyperlinking, images, lists
- HTML 2.0 (IETF 1996)
  - added image maps, forms
- HTML 3.2 (W3C 1996)
  - equations, toolbars, tables
- HTML 4.0 (W3C 1998)
  - accessibility, object embedding, scripting

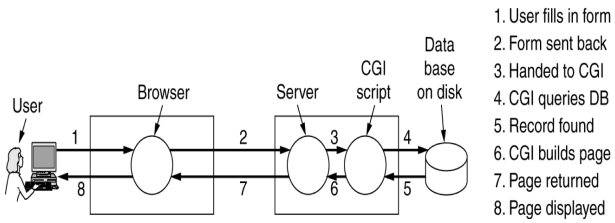
Beyond HTML ... **§7.3.2**

- XML (Extensible Markup Language) & XSL (Extensible Stylesheet Language)
  - Primary feature of these technologies is the separation of content and presentational markup
  - Stringent validation requirements
- XHTML -
  - Essentially an expression of HTML 4.0 as valid XML
  - Major differences to HTML 4.0 are the requirements for conformance, case folding, well-formedness, attribute specification, nesting and embedding, and inclusion of a document type identifier

Web scripting languages

Dynamic Web Documents **§7.3.3**

- The need for dynamism in the web document environment has been motivated both by interactivity (user) requirements as well as functionality and scalability (infrastructural) requirements.



Server Side Dynamic Documents **§7.3.3**

- Processing requires communication by the client with the web server, the execution of some action, and formulation of a response
- Technologies
  - CGI - Common Gateway Interface
  - PHP - PHP Hypertext Preprocessor
  - ASP - Active Server Pages
  - JSP - Java Server Pages

Client Side Dynamic Documents **§7.3.3**

- All processing is entirely done on the client side (directly and by in the browser)
- Technologies
  - JavaScript
  - Java Applets - compiled Java code (platform independent)
  - ActiveX - compiled code for Windows

Client and server software

Common WWW Software

- Browsers
  - Netscape
  - Internet Explorer
  - Mozilla
  - Opera
  - Amaya
- Web Servers
  - Apache
  - Internet Information Server
  - Zope (PHP Embedded Portal)
- Others
  - Squid - Web Caching
  - OpenSSL - Security (HTTPS)

Summary - Multimedia

- DNS
  - Describe operation of DNS lookup
- Email
  - Explain which functions should be performed in Message Transfer Agent or User Agent
  - Compare POP3 and IMAP
- World Wide Web
  - Choose between server-side vs client side technologies for dynamic content
  - Explain difference between plug-ins and helpers
  - Describe the role of cookies

Lecture XXII

Tutorial: Application Layer

1. The IP address of the domain name www.cs.mu.oz.au is 128.250.37.78. Is this address on a Class A, B or C subnetwork?

2. There has been huge growth in the number of websites in the .com domain. This creates an enormous load on the root DNS server for the .com domain. What solutions can you propose to solve this load problem, without requiring changes to names in the .com domain?

3. My mail system gives me the option of setting a "vacation message", so that if someone sends me an e-mail while I'm away, they will receive an automatic reply to let them know that I am not reading my mail. Explain whether this agent should be implemented in the user agent or the message transfer agent?

4. The Dodgy Bank wants to provide easy authentication for its on-line banking service. It is proposing that once a user is authenticated using a password, the bank automatically stores a cookie containing the customer's ID on the customer's computer. This means the customer does not need to enter their ID or password when they next access the on-line banking service. Why is this a bad idea?

5. Many businesses have three distinct and worldwide unique identifiers. What are they?

6. According to the information given Fig. 7-3, is *little-sister.cs.vu.nl* on a class A, B or C network?

7. In Fig. 7-3, there is no period after *rowboat*? Why not?

8. DNS uses UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. Does this cause a problem, and if so, how is it resolved?

9. Can a machine with a single DNS name have multiple IP adresses? How could this occur?

10. Some e-mail systems support a header field *Content Return:*. It specifies whether the body of the message is to be returned in the event of nondelivery. Does this field belong to the envelope or the header?

11. Suppose that someone sets up a vacation daemon and then sends a message just before logging out. Unfortunately, the recipient has been on vacation for a week and also has a vacation daemon in place. What happens next? Will canned replies go back and forth until someone returns?

12. POP3 allows users to fetch and download e-mail from a remote mailbox. Does this mean the the format of remote mailboxes has to standarised so that any POP3 program on the client side can read the mailbox on any mail server? Discuss your answer.

13. The standard *http* URL assumes that the Web server is listening on port 80. However, it is possible for a Web server to listen on some other port. Devise a reasonable syntax for a URL accessing a file on a nonstandard port.

14. Although it was not mentioned in the text, an alternative form for a URL is to use the IP

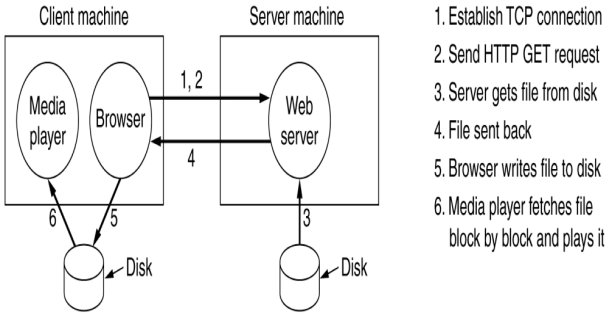
address instead of its DNS name. An example of using an IP address is *http://192.31.231.66/index.html*. How does the browser know whether the name following the scheme is a DNS name or an IP address?

15. For each of the following applications, tell whether it would be 1) possible and 2) better to use PHP script or JavaScript and why. a) Displaying a calendar for any requested month since September 1752. b) Displaying the schedule of flights from Amsterdam to New York. c) Graphing a polynomial from user supplied co-efficients.

Lecture XXIII
The Application Layer: Multimedia Networks

Multimedia Networks

A Basic Model for Multimedia on the Web §7.4.3



Problems with the Basic Model §7.4.3

- The entire media file must be transmitted over the network before playback starts, causing delay in user experience (eg to transmit a 5Mb file over a 56Kbps link takes about 5 minutes)
- Basic model assumes mainly point-to-point media distribution rather than a point-to-multipoint (broadcast) distribution model
- QoS is not considered
- Basic model assumes the browser/plugin/helper integration and traditional service types

Characteristics of Multimedia Networks §7.4.3

- Higher bandwidth requirements
- Higher QoS requirement
- New infrastructure models
- New service providers

Streaming Media Protocols §7.4.3

- Transport Protocols
  - TCP
- Open Protocols
  - HTTP
  - RTP - Real-time Transport Protocol (RFC 1889)
  - RTSP - Real Time Streaming Protocol (RFC 2326)
  - MPEG-4 (ISO)
- Closed Protocols
  - Real Networks' RealAudio
  - Microsoft's Windows Media
  - Apple's QuickTime

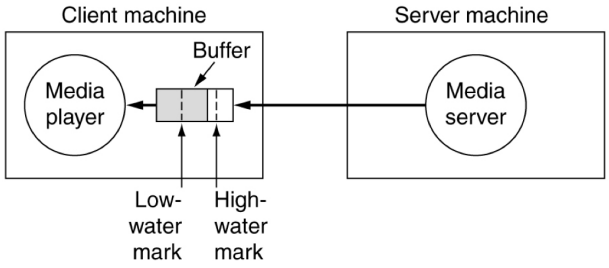
The Role of Multimedia Playback Software §7.4.3

- 4 main tasks of the multimedia playback software
  - Manage the user interface
  - Handle transmission errors in conjunction with transport protocols
  - Decompress the multimedia files (codecs)
  - Eliminate jitter

Jitter Management §7.4.3

- Similarly to router buffering, multimedia software buffers streamed media sources prior to transmission
- Buffering is a defensive mechanism to reduce jitter (variance in average packet arrival times)
- Ideally the stream buffer will continue to be filled at the same rate the stream is played back to the user

Jitter Management §7.4.3



Jitter Management §7.4.3

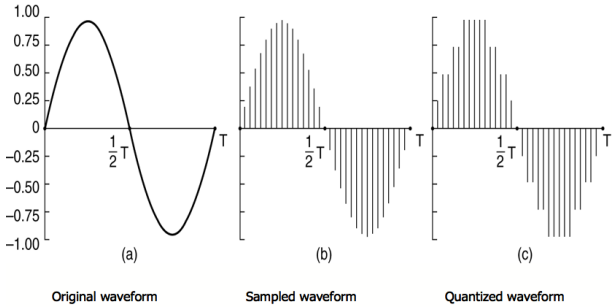
- Two different buffering modes
  - *Pull server*: as long as there is room in the buffer to another block, the media player continues to request additional blocks from the server (goal to keep the buffer as full as possible)
  - *Push server*: media player sends a play request, and the server continuously pushes data to the player, media player uses a FIFO scheme to draw from the buffer, and uses a compensation mechanism when the buffer is not filled to capacity - high and low watermarks trigger starts or stops in the playback

Audio

Audio Compression §7.4.2

- To transmit CD quality audio over a network requires 705.6Kbps for mono or 1.411Mbps for stereo
- Obviously compression is required to make the transmission of audio viable from a bandwidth perspective, but compression must also ensure that maximum quality is retained
- Different approaches to compression
  - *Waveform coding* - Fourier transformation of signal into frequency components
  - *Perceptual coding* - exploits flaws in human auditory system so that a signal sounds the same even if it looks significantly different on an oscilloscope - the popular MP3 format is based on perceptual coding

Audio Compression §7.4.1



Compressed Audio Formats §7.4.2

- In audio compression, the main concern is the loss of aural quality In all audio compression, a variant degree of information is lost owing to resampling intervals and quantization
- MIME: audio/mpeg
- Others: wav, mp3, cda, ogg, wma, ram

An Example Format: MP3 §7.4.2

- MP3 is really MPEG Audio Layer 3
- MP3's compression is based on perceptual coding (resampling and quantization)
- MP3 audio compression results in significant file size savings without a perceived loss of audio quality
- Typical MP3 audio compression rates for CD quality audio reduce the need for bandwidth from ∼1.4Mbps for stereo down to 96-128Kbps

Video

Digital Video Systems §7.4.6

- Digital video is essentially a sequence of frames, each frame consists of a rectangular grid of pixels
  - 1-bit pixels = black and white
  - 8-bit pixels = 256 gray
  - 24-bit pixels = RGB (16 million colour)
- To produce smooth motion, digital video must play at least 25 frames per second
- Two metrics of interest

  - *Smoothness* - number of different images per second
  - *Flicker* - number of times screen is painted per second

Video Compression #1 §7.4.7

- Using a 1024x768 pixel monitor, and showing colour video (24bits per pixel) at 25 frames per second requires a data feed rate of 472Mbps
- The bandwidth factor again means transmitting uncompressed video over a network is very inefficient, and requires compression approaches similar to audio
- All compression systems require 2 algorithms - one for encoding and one for decoding - but these need not be symmetrical in usage (encode once, decode numerous times - think movie)
- For real time applications, eg video conferencing, encoding speeds need to be very fast to give acceptable performance

Video Compression #2 §7.4.7

- Encoding and decoding does not necessarily need to be invertable - loss of some data may be acceptable in order to achieve other goals (eg size reduction)
- If decoded output is not identical to encoded input, then compression schemes are said to be *lossy*
- If decoded output is identical to encoded input, then compression schemes are said to be *lossless*

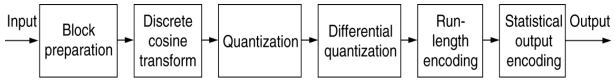
Compressed Video Formats §7.4.7

- Similarly to audio compression, in all video compression, a variant degree of information is lost owing to resampling intervals and quantization
- In video compression, the main concern is the loss of visual quality
- MIME: video/quicktime, video/mpeg, video/jpeg
- Others: dvix ...

JPEG Standard §7.4.7

- If a video can be considered as a series of images (plus sound) then image compression standards and audio compression standards could be sufficient to conduct compression
- JPEG - Joint Photographic Experts Group - standard for compressing images
- JPEG has 4 modes, although only the lossy sequential mode is of interest in this context

Compression with JPEG §7.4.7



JPEG compression in lossy sequential mode

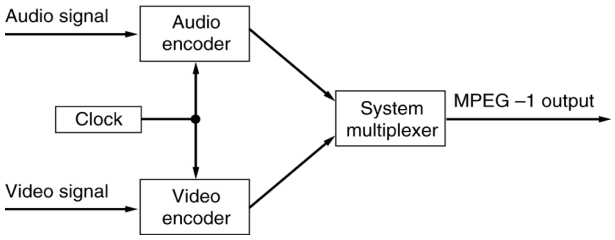
- JPEG often provides compression ratios of 20:1
- JPEG compression is symetric, decoding takes as long as encoding

MPEG Standard §7.4.7

- MPEG - Motion Picture Experts Group
- MPEG can compress both audio and video together (using synchronised streams)
- The evolution of MPEG
  - MPEG-1: VCR quality at 1.2 Mbps (40:1)
  - MPEG-2: Broadcast quality at 4-6Mbps (200:1)
  - MPEG-4: DVD quality at 10Mbps (1200:1)

MPEG Components §7.4.7

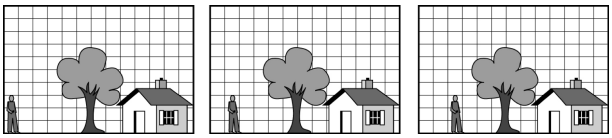
- MPEG-1 has 3 parts: audio, video and system
- The two media streams are synchronised using a system clock which provides timing information to both encoders/decoders



Compression with MPEG-1 §7.4.7

- MPEG-1
  - Uses both spatial and temporal redundancy to reduce media file size
    - Spatial - each frame separately encoded with JPEG
    - Temporal - highly similar frames are phased out of the frame sequence
  - 4 frame types
    - Intracoded - self contained JPEG encoded still pictures
    - Predictive - block by block difference with last frame
    - Bidirectional - differences between last and next frames
    - DC-Coded - block averages used for fast forward
  - Uses an 8x8 pixel frame of reference for computation
  - Supports a single level of resolution (320x240pixels)

Compression with MPEG-1 §7.4.7



Three consecutive frames

Compression with MPEG-2 §7.4.7

- MPEG-2 supports Intracoded, Predictive and Bidirectional frames, but not DC-Coded frames
- Uses larger frame of reference (10x10 pixel block), which allows for better quality and compression
- Supports multiple levels of resolution (up to 1024x768)

Video over the Web §7.4.8

- Embedded with web content
  - Streaming servers required to deliver content over ordinary connection
- Integrated with other consumer services eg cable television (video on demand)
  - Content stored on central video servers
  - Delivered via a shared network to consumers

Lecture XXIV

The Application Layer: Voice Over IP

Voice over IP (VOIP)

Pre-VOIP

Pre-VOIP: Voice over ATM (VoATM)

- 2 specific traffic classes have potential for passing real time traffic with a given QoS
  - Constant Bit Rate (CBR)
  - Variable Bit Rate (VBR)
- Signalling
  - VoATM doesn't include signalling support other than that provided at the ATM (AAL) level
- Addressing
  - VoATM has both private and public addressing schemes
    - Authority and Format Identifier (AFI) consisting of data country code, international code designator, and local desigator
- Routing
  - VoATM uses a Private Network to Network Interface (PNNI), a hierarchical link-state routing protocol
  - Virtual Circuit switching constrains possible routes

Pre-VOIP: Voice over Frame Relay (VoFR)

- Frame Relay networks which are common in telecommunications infrastructure have long been used to carry voice traffic in addition to data
- VoFR Signalling
  - FRF.11 standard for call setup, coding types, packet formats between vendor implementations
- VoFR Addressing
  - Static address tables mapped to Permanent Virtual Circuits
  - Routing based on maximising bandwidth utilisation
  - FRF.12 standard to minimise delay on multiplexed voice and data VCs

The Emergence of VOIP §7.4.5

- Voice services becoming applications on top of data networks are being driven by a number of factors:
  - Data has overtaken voice as the primary traffic on many networks originally built for voice
  - PSTN infrastructure is not flexible enough for the rapid deployment of new features
  - PSTN technologies are largely incompatible with the convergence of data/voice/video
  - The architecture built primarily for voice is not flexible enough to carry data
  - Network providers are increasingly looking to leverage investment in network infrastructure by bring new services to data networks
- Where suitable data networks are already in existence, the evolution of audio encoding technologies has allowed voice to be transmitted over data links - hence VOIP

VOIP Benefits

Benefits of VOIP §7.4.5

- Financial savings
- Consolidated infrastructure
- Flexible infrastructure
- Standards based voice and data

VOIP Technologies

VOIP Technologies §7.4.5

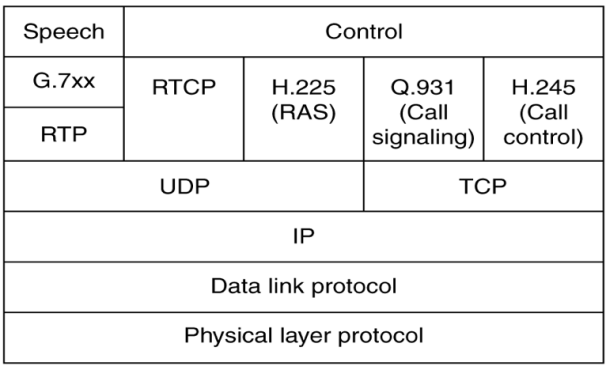
- Within the VOIP domain, there are 3 distinct models for service provision
  - infrastructural - PSTN/PABX integration
  - virtual - media gateways, virtual directories
  - value-added - voice mail
- Alternative VOIP Technologies
  - H.323
  - SGCP and MGCP
  - SIP

H.323 §7.4.5

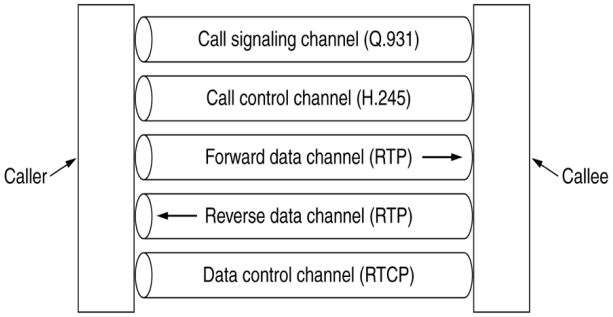
- H.323 is an international standard that specifies how multimedia traffic is carried over packet networks
- H.323 integrates existing standards to provide a layered protocol stack
- H.323 was originally developed to enable multimedia applications to run over *unreliable data networks* - includes support for audio (including VOIP), video and data sharing services within a single protocol stack

Protocols

The H.323 Protocol Stack §7.4.5



Logical Channels in H.323 VOIP §7.4.5



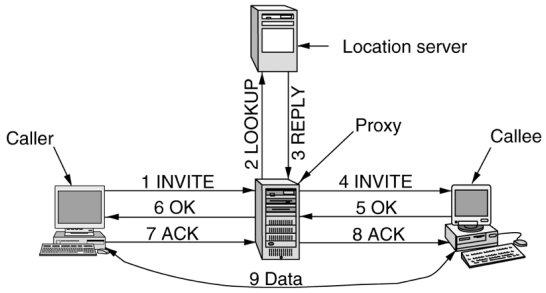
Session Initiation Protocol (SIP) §7.4.5

- SIP codified in RFC 3261
- Modelled on HTTP, simple ASCII based protocol, method + parameters, similar headers to MIME
- SIP Architecture
  - A single network module rather than a complete protocol suite
  - SIP only handles the setup, management and termination of sessions - requires other protocols such as RTP/RTCP for data transport. SIP is an application layer protocol and can run over UDP or TCP
- SIP Functionality
  - Two party, multiparty and multicast
  - Callee location, callee capabilities, call setup, call termination
- SIP Addressing: addressing based on a URL type schema
  - sip:badenh@estragon.cs.mu.oz.au
  - SIP URLs can contain IPv4 or IPv6 addresses or actual telephone numbers

SIP Methods §7.4.5

Method	Description
INVITE	Request initiation of a session
ACK	Confirm that a session has been initiated
BYE	Request termination of a session
OPTIONS	Query a host about its capabilities
CANCEL	Cancel a pending request
REGISTER	Inform a redirection server about the user's current location

SIP Methods §7.4.5



H.323 and SIP Compared §7.4.5

Item	H.323	SIP
Designed by	ITU	IETF
Compatibility with PSTN	Yes	Largely
Compatibility with Internet	No	Yes
Architecture	Monolithic	Modular
Completeness	Full protocol stack	SIP just handles setup
Parameter negotiation	Yes	Yes
Call signaling	Q.931 over TCP	SIP over TCP or UDP
Message format	Binary	ASCII
Media transport	RTP/RTCP	RTP/RTCP
Multiparty calls	Yes	Yes
Multimedia conferences	Yes	No
Addressing	Host or telephone number	URL
Call termination	Explicit or TCP release	Explicit or timeout
Instant messaging	No	Yes
Encryption	Yes	Yes
Size of standards	1400 pages	250 pages
Implementation	Large and complex	Moderate
Status	Widely deployed	Up and coming

Evolving Voice over Data Solutions

- First voice-data integration technologies were designed to eliminate long distance phone toll charges by providing tie lines between PABXs over a WAN infrastructure
- Later support for analogue telephony devices was introduced to allow off-premises extensions to PABX
- As data networks expanded, enterprise wide call handling began to migrate towards the data network - shorter call forwarding distances between PABX and WAN gateways
- With increased voice traffic, connection admission control became a more significant issue
- With larger networks, dial plans and directory services became essential
- Centralised call control through the use of H.323 gatekeeper functions allowed voice and data transmissions to be regulated at a single point

Future of Network-Centric Telephony Applications

- As integration increases, new solutions are emerging - typically allowing for packetised voice technologies to replace PABX with end to end solutions
- Generally 2 categories of technologies and application architectures
  - *UnPABX*: Server based call routing, with direct connections to data network, trunk telephony network and analogue telephony networks
  - *LAN-PABX*: Telephony on the desktop - rather than actual telephone handsets, the telephony function is in software on a workstation - Layer 3 base

Incentives for Packet Based Telephony

- Un-PABX systems typically cost less than systems they replace
- LAN-PABX systems bring much greater flexibility to end users
- Both leverage existing infrastructure - either the convergence of communications infrastructure or wired/wireless connections to the workstation
- Fully integrated applications, which allow manipulation of complex software services via telephony interfaces will likely drive the convergence of voice and data even further

Summary - Multimedia

- Multimedia networks
  - Describe techniques for jitter management
  - Explain techniques for audio compression
  - Compare JPEG and MPEG standards
- VoIP
  - Contrast H.323 and SIP
  - Explain steps in SIP call establishment

Lecture XXV
Tutorial: Application Layer

1. A compact disk holds 650 MB of data. Is compression used for audio CDs? Explain you reasoning.

2. Could a psychoacoustic model be used to reduce the bandwidth needed for Internet telephony? If so, what conditions, if any, would have to be met to make it work? If not, why not?

3. An audio streaming server has a one way distance of 50 msec with a media player. It outputs at 1 Mbps. If the media player has a 1 MB buffer, what can you say about the position of the low water mark and the high water mark?

4. Does voice over IP have the same problems with firewalls that streaming audio does? Discuss your answer.

5. What is the bit rate for transmitting uncompressed 800×600 pixel colour frames with 8 bits/pixel at 40 frames/sec?

6. Can a 1 bit error in an MPEG frame affect more than the frame in which the error occurs? Explain your answer.

Lecture XXVI
Network Management: The Basics

What is Network Management?

What is Network Management ?

- Network management means different things to different people
  - single network consultant monitoring network activity with a protocol analyzer
  - a distributed database, automated polling of network devices
  - high-end workstations generating real-time graphical views of network topology changes and traffic.
- In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

Benefits of Network Management

- The development of Network Management methodologies allowed network owners to
  - Control strategic assets
  - Control complexity
  - Improve service
  - Balance various needs:
    - Performance
    - Availability
    - Security
    - Cost
  - Reduce downtime
  - Control costs

Network Management Processes

Management Processes: Design and Optimisation

- Data collection definition
- Baseline creation
- Trend analysis
- Response time analysis
- Capacity planning
- Procurement and provisioning
- Topology design

Management Processes: Implement and Change

- Installation
- Configuration
- Address management
- Adds, moves, changes
- Security management
- Accounting and billing
- Assets and inventory management
- User management
- Data management

Management Processes: Monitor and Diagnose

- Defining thresholds
- Monitoring exceptions
- Isolating problems
- Validating problems
- Troubleshooting problems
- Bypassing and resolving problems

Network Management Architectures

Network Management Architectures and Components

- Most network management architectures use the same basic structure and set of relationships.
  - End stations (*managed devices*), such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems (for example, when one or more user-determined thresholds are exceeded).
  - Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.

Network Management Architectures and Components (cont.)

- Management entities also can poll end stations to check the values of certain variables.
  - Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls.
- *Agents* are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it (proactively or reactively) to management entities within *network management systems* (NMSs) via a network management protocol.
- Well-known network management protocols include the *Simple Network Management Protocol* (SNMP) and *Common Management Information Protocol* (CMIP)

ISO Network Management Model

ISO Network Management Model

- 5 aspects:
  - Performance Management
  - Configuration Management
  - Accounting Management
  - Fault Management
  - Security Management

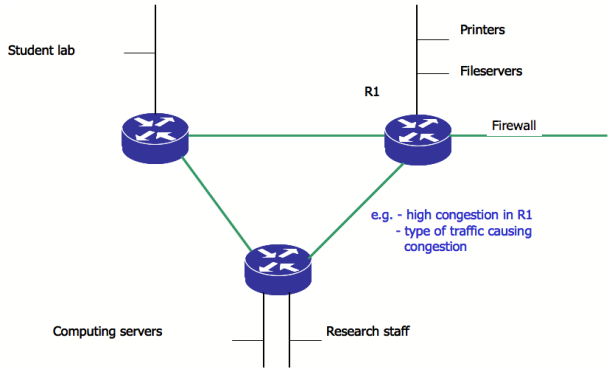
ISO Performance Management

- The goal of *performance management* is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level.
- Performance management involves three main steps.
  - First, performance data is gathered on variables of interest to network administrators.
  - Second, the data is analyzed to determine normal (baseline) levels.
  - Finally, appropriate performance thresholds are determined for each important variable so that exceeding these thresholds indicates a network problem worthy of attention.
- Management entities continually monitor performance variables. When a performance threshold is exceeded, an alert is generated and sent to the network management system.
- Each of the steps just described is part of the process to set up a reactive system. When performance becomes unacceptable because of an exceeded user-defined threshold, the system reacts by sending a message.

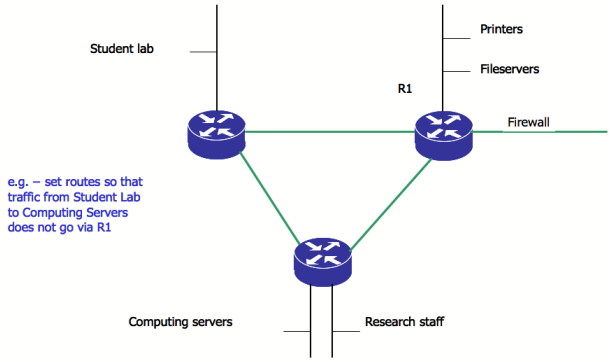
Performance Management in Practice

- Performance management allows considerations of questions like:
  - What is the level of capacity utilization?
  - Is there excessive traffic?
  - Has throughput been reduced to unacceptable levels?
  - Are there bottlenecks?
  - Is response time increasing?
- Performance management indicators include metrics for availability, response time, accuracy throughput, utilization

Example - Performance



Example - Configuration



ISO Configuration Management

- The goal of *configuration management* is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.
- Each network device has a variety of version information associated with it. A typical computer may have a number components:
  - Operating system
  - Ethernet interface
  - TCP/IP software
  - Network client software
  - Network application software
- A configuration management subsystem stores this information in a database for easy access. When a problem occurs, this database can be searched for clues that may help solve the problem.

Configuration Management in Practice

- Configuration management allows consideration of actions such as:
  - Installation of new hardware/software
  - Tracking changes in control configuration
  - Who, what and why? - network topology
  - Revert/undo changes
  - Change management
  - Configuration auditing and compliance
  - Does it do what was intended ?

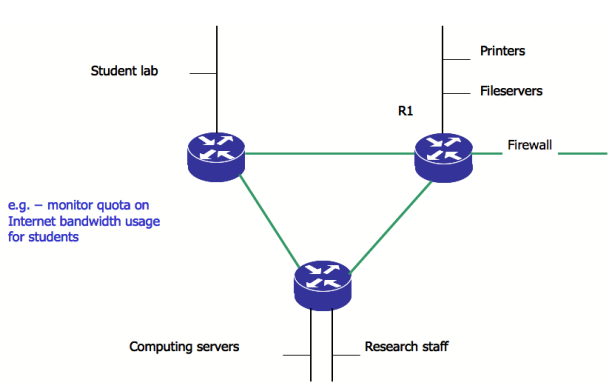
ISO Accounting Management

- The goal of *accounting management* is to measure network utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of network access across all users.
- As with performance management, the first step toward appropriate accounting management is to measure utilization of all important network resources. Analysis of the results provides insight into current usage patterns, and usage quotas can be set at this point. Some correction, of course, will be required to reach optimal access practices. From this point, ongoing measurement of resource use can yield billing information as well as information used to assess continued fair and optimal resource utilization.

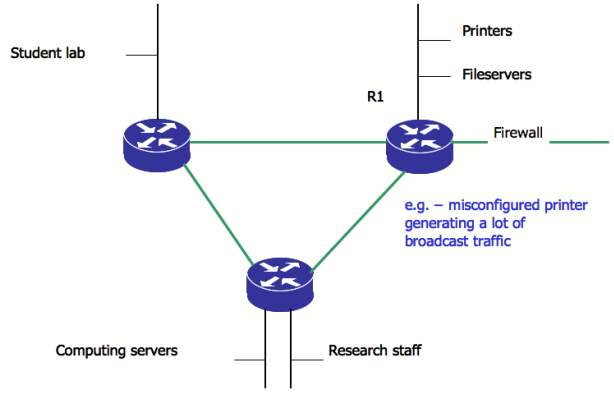
Accounting Management in Practice

- Accounting management allows functions like:
  - Identifying consumers and suppliers of network resources - users and groups
  - Mapping network resources consumption to customer identity
  - Billing for network resource consumption

Example - Accounting



Example - Fault



ISO Fault Management

- The goal of *fault management* is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively.
- Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.
- Fault management involves first determining symptoms and isolating the problem.
- Then the problem is fixed and the solution is tested on all-important subsystems.
- Finally, the detection and resolution of the problem is recorded

Fault Management in Practice

- Fault management methods allow
  - Detection of the fault
  - Determination of exactly where the fault is
  - Isolating the rest of the network from the failure so that it can continue to function
  - Reconfigure or modify the network in such a way as to minimize the impact
  - Repair or replace the failed components

ISO Security Management

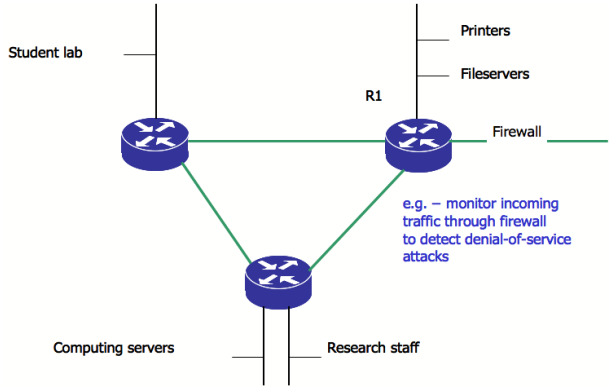
- The goal of *security management* is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization.
- Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to any network resource is inappropriate, mostly because such users are usually company outsiders. For other (internal) network users, access to information originating from a particular department is inappropriate.
- Security management subsystems perform several functions.
  - They identify sensitive network resources (including systems, files, and other entities) and determine mappings between sensitive network resources and user sets.
  - They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources.

Security Management in Practice

- Security management concerns a number of different areas:
  - Security services: generating, distributing, storing of encryption keys for services
  - Exception alarm generation, detection of problems

- Uniform access control to resources
- Backups, data security
- Security logging

Example - Security



Proactive Management

- Monitoring networks even when problems do not occur
  - Determine network service goals
  - Define metrics for measuring whether goals have been met
  - Define processes for data collection and reporting
  - Implement network management systems
  - Collect performance data and record trends
  - Analyse results and write reports
  - Locate irregularities and bottlenecks
  - Plan and implement network improvements
  - Review and adjust metrics and processes if necessary
  - Document changes

Lecture XXVII
Simple Network Management Protocol

The SNMP Environment and Basic Operations

SNMP Background

- The *Simple Network Management Protocol* (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices.
- It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.
- SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP Versions

SNMP Versions

- Two versions of SNMP exist:
  - *SNMP version 1* (SNMPv1)
  - *SNMP version 2* (SNMPv2)
- Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations.
- Standardization of yet another version of SNMP-SNMP Version 3 (SNMPv3)-is pending.

The SNMP Environment

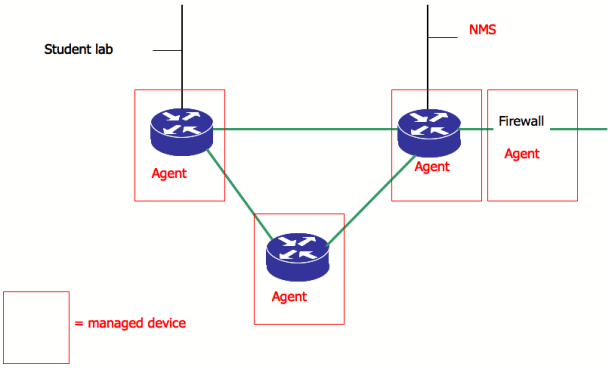
- An SNMP-managed network consists of three key components:
  - managed devices
  - Agents
  - network-management systems (NMSs).
- A *managed device* is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers,

switches and bridges, hubs, computer hosts, or printers.

The SNMP Environment (cont.)

- An *agent* is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
- An *NMS* executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

Example



SNMP Operations

Basic SNMP Operations

- Managed devices are monitored and controlled using four basic SNMP commands: *read*, *write*, *trap*, and traversal operations.
- The *read* command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.
- The *write* command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
- The *trap* command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.
- Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

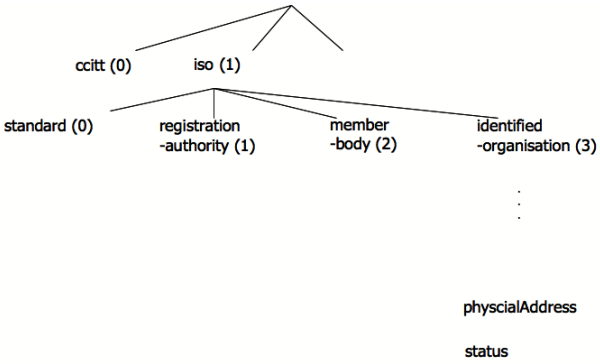
SNMP Management Information Base (MIB)

- A *Management Information Base* (MIB) is a collection of information that is organized hierarchically. MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers.
- A managed object (sometimes called a MIB object, an object, or a MIB) is one of any number of specific characteristics of a managed device. Managed objects are comprised of one or more object instances, which are essentially variables.
- Two types of managed objects exist: scalar and tabular. *Scalar objects* define a single object instance. *Tabular objects* define multiple related object instances that are grouped in MIB tables.
- An example of a managed object is atInput, which is a scalar object that contains a single object instance, the integer value that indicates the total number of input AppleTalk packets on a router interface.

SNMP MIBS Cont.

- An *object identifier* (or object ID) uniquely identifies a managed object in the MIB hierarchy. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations.
- The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations.
- Vendors can define private branches that include managed objects for their own products. MIBs that have not been standardized typically are positioned in the experimental branch.
- The managed object atInput can be uniquely identified either by the object name - *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput* -or by the equivalent object descriptor, *1.3.6.1.4.1.9.3.3.1.*

SNMP MIBS



SNMP Version 1

- *SNMP version 1 (SNMPv1)* is the initial implementation of the SNMP protocol. It is described in Request For Comments (RFC) 1157 and functions within the specifications of the Structure of Management Information (SMI).
- SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX).
- SNMPv1 is widely used and is the de facto network-management protocol in the Internet community.
- The *Structure of Management Information* (SMI) defines the rules for describing management information, using Abstract Syntax Notation One (ASN.1). The SNMPv1 SMI is defined in RFC 1155. The SMI makes three key specifications: ASN.1 data types, SMI-specific data types, and SNMP MIB tables.

SNMP v1 Data Types and Tables

- Three simple data types are defined in the SNMPv1 SMI, all of which are unique values:
  - *Integer* data type is a signed integer in the range of -2,147,483,648 to 2,147,483,647.
  - *Octet strings* are ordered sequences of 0 to 65,535 octets.
  - *Object IDs* come from the set of all object identifiers allocated according to the rules specified in ASN.1.
- Seven application-wide data types exist in the SNMPv1 SMI:
  - *Network addresses* represent an address from a particular protocol family. SNMPv1 supports only 32-bit IP addresses.
  - *Counters* are non-negative integers that increase until they reach a maximum value and then return to zero. In SNMPv1, a 32-bit counter size is specified.
  - *Gauges* are non-negative integers that can increase or decrease but that retain the maximum value reached.
  - A *time tick* represents a hundredth of a second since some event.

SNMP v1 Data Types and Tables (cont.)

- Seven application-wide data types exist in the SNMPv1 SMI (cont.):
  - An *opaque* represents an arbitrary encoding that is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.
  - An *integer* represents signed integer-valued information. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.
  - An *unsigned integer* represents unsigned integer-valued information and is useful when values are always non-negative. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.
- The SNMPv1 SMI defines highly structured tables that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables are composed of zero or more rows, which are indexed in a way that allows SNMP to retrieve or alter an entire row with a single *Get*, *GetNext*, or *Set* command.

SNMP v1 Protocol Operations

- SNMP is a simple request/response protocol.
  - The network-management system issues a request, and managed devices return responses.
  - This behavior is implemented by using one of four protocol operations:

  - The *Get* operation is used by the NMS to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, it does not provide any values.
  - The *GetNext* operation is used by the NMS to retrieve the value of the next object instance in a table or a list within an agent.
  - The *Set* operation is used by the NMS to set the values of object instances within an agent.
  - The *Trap* operation is used by agents to asynchronously inform the NMS of a significant event.

Performance Management

Overview

- What is Performance Management ?
- Why do we want Performance Management ?
- Issues for Performance Management
- Performance Management Techniques

Network Performance Management

- Why do we want to manage network performance ?
  - Connectivity
  - Security
  - Cost optimisation
  - Manageable growth

Performance Issues

- Structural imbalances in network infrastructure
  - fast communication lines connected to slow routers or CPU's or vv
- Synchronous overloading
  - broadcast storms, massively parallel rebooting and network initialisation eg DHCP
- System and network tuning
  - compromises between CPU, memory, buffer, network infrastructure metrics
- Faster networks = old problems thresholds are reached faster, new problems emerge

Design Options for Better Performance

- CPU Speed is more important than network speed
  - OS and protocol overheads dominate time on the wire. If you double the CPU speed, you can almost double the throughput - doubling bandwidth has almost no impact as bottlenecks are almost always at the host
- Reduced packet counts result in reduced software overheads
  - Per TPDU processing overhead can be significant. It is better to send fewer large TPDU's than a greater number of smaller TPDUs
- Minimize context switches
  - Switching from user mode to kernel mode in order to transmit and receive have a significant performance impact - use libraries to do buffering and transfer

Design Options for Better Performance Cont.

- Minimize copying
  - Copies of data exist simultaneously in multiple places - NIC, kernel, network layer, transport layer, application. CPU constraints mean that processing many copies can drastically affect performance
- You can buy more bandwidth, but not lower delay
  - Parallel long haul fibres increase bandwidth but not delay. Delay improvements mean adjusting protocol, OS or network software.
- Avoiding congestion is better than recovering from it
  - Recovering from congestion takes time and resources. Avoiding the occurrence of congestion in the first place is actually a better solution.

- Avoid timeouts
  - Timers should be used sparingly, and set according to well evaluated parameters. Every time a timer expires, some action is generally repeated - if this is really necessary, then it should be repeated, if not then the repetition is introducing inefficiency.

New Networks, New Problems

- Consider the move from megabit to gigabit:
  - Protocol sequences are now smaller than optimal (sequence wrapping can occur)
  - Communication speeds improved exponentially, computation speeds improved linearly
  - As distances increase, and bandwidth over distance increases, strategies for repeating lost or damaged transmissions become less efficient
  - Over long distances, network infrastructure is delay limited rather than bandwidth limited
  - On higher capacity networks, increased regulation is required to assure quality of service owing to greater bandwidth and longer distances

Principles for Next Generation Networks

- Design for speed, not for bandwidth optimisation
  - Avoid feedback loops over long distances
  - Reduce packet header sizes
  - Checksum header and payloads separately
  - Increase the maximum data size
  - Minimise processing time in software
  - Minimise copying time in software

Summary - Management

- ISO Network Management Model
  - Explain the goals of each aspect of network management
  - Give examples of practical tasks in each aspect
- SNMP
  - Summarise the basic SNMP operations
- Performance Management Issues
  - Explain different design options for improving network performance
  - Contrast the differences in optimising performance between older generation and new generation networks

Lecture XXVIII
Network Security: Cryptography

Network Security in General

What is Security? §8

- Network security is a factor of 4 related concepts
  - Secrecy
  - Authentication
  - Non-repudiation
  - Integrity control
- All of these are equally valid for traditional systems, but have different implications in a networked environment
- Aspects of security can be found at all layers of a protocol stack
- Apart from the physical layer, almost all security implementations are based on common cryptographic principles

Cryptography

Cryptography §8.1

- Cryptographic Constituents and Relations
- Symmetric Key Algorithms
- Assymetric Key Algorithms
- Digital Signatures
- Public Key Management

Cryptography Concepts §8.1.1

- Three foundational concepts
  - Plaintext
  - Keys
  - Ciphertext
- *Plaintext* messages to be encrypted can be transformed (encrypted/decrypted) by a function that is parameterized by a *key*, the output of the transformation process is *ciphertext*

Basic Constituents and Relations

Relation of Cryptographic Constituents §8.1.1

- $C = E_K(P)$
- $P = D_K(C)$
- $D_K(E_K(P)) = P$
- Where: C = ciphertext, P = plaintext, E = encryption, D = decryption, K = key

Keys §8.1.1

- A key is a short string that allows the selection of one of many potential encryptions
- The key can be changed as often as required
- Kerckhoff's Principle: *all algorithms must be public, only the keys are secret* (ensures cryptographic algorithms are robust)
- How many possible keys are available when using numerical strings of length:
  - 2 digits?
  - 3 digits?
  - 6 digits?
- The size of the overall key space is determined by the number of bits in the key string
- The longer the key, the more effort is required to break a given encryption

Fundamental Machinery: XOR §8.1.1

- An XOR is an "exclusive or".
- A XOR B means A or B, but not both
- XOR is commonly used in cryptography as a comparison mechanism in multiphase encryption and decryption

A	B	A XOR B
F	F	F
F	T	T
T	F	T
T	T	F

Ciphers

Types of Ciphers §8.1.2,3,4

- Substitution cipher
  - Each letter of group of letters is replaced systematically by other letters or groups of letters (breakable with knowledge of the replacement system)
- Transposition cipher
  - All letters are re-ordered without disguising them (breakable with knowledge of re-ordering system)
- One-time pad
  - Uses a random bit string as the key, convert the plaintext into a bit string, then XOR the two strings bit by bit (unbreakable because given a sufficiently large sample of each letter, digram, and trigram will occur with equal distribution)

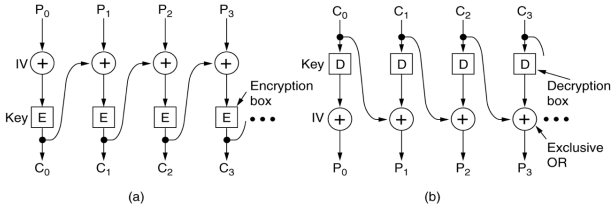
Algorithms

Symmetric Key Algorithms §8.2

- A symmetric key algorithm uses the *same key* for both encryption and decryption
- Symmetric key algorithms can use permutation, substitution and a combination of both to encrypt and decrypt
- 2 Symmetric Key Algorithms
  - Data Encryption Standard (DES)
    - Uses 64 bit blocks and 56 bit keys
    - 2^{56} key space
    - Triple DES has a 3×2^{56} key space
  - Advanced Encryption Standard (AES)
    - uses 128 bit blocks and 128 bit keys (others available)
    - 2^{128} key space

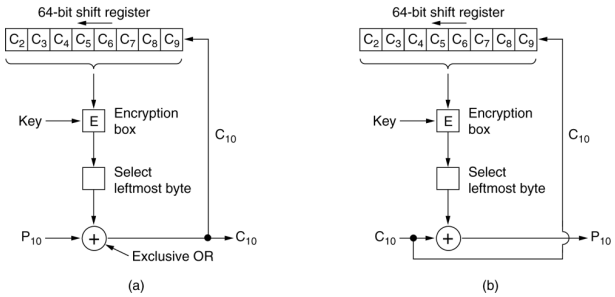
Cipher Modes: Block Chaining §8.2.3

- In block chaining mode, each plaintext block is XOR'ed with the previous ciphertext block before being encrypted
- (a) encryption, (b) decryption



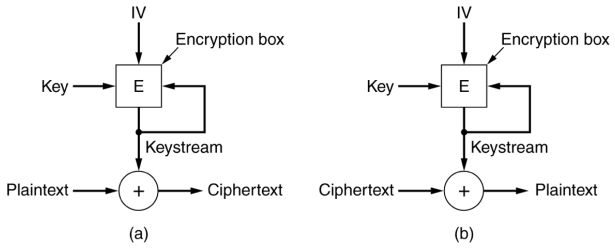
Cipher Modes: Feedback Mode §8.2.3

- In cipher feedback mode, byte-by-byte encryption is used rather than block-by-block encryption, together with a shift register
- (a) encryption, (b) decryption



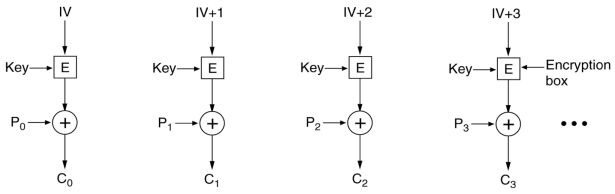
Cipher Modes: Stream Ciphers §8.2.3

- In stream cipher mode, recursive sequential block encryption is used as a one-time pad, and XOR'ed with plaintext to generate ciphertext
- (a) encryption, (b) decryption



Cipher Modes: Counter Mode §8.2.3

- In counter mode, plaintext is not directly encrypted, but an initialisation parameter plus an arbitrary constant is encrypted, and the resulting ciphertext is XOR'ed with plaintext to generate new ciphertext



Other Symmetric Key Algorithms §8.2.4

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Public Key Algorithms §8.3

- Diffie & Hellman (1976) proposed a radically different model to symmetric key algorithms - *asymmetric key algorithms*, where the key used to encrypt and the key used to decrypt are different, and not derivable from each other
- Diffie-Hellman 2 key system
  - Key 1: *public key*, useable by anyone to encrypt messages to the owner of the key
  - Key 2: *private key*, required to decrypt the message (and held only by the owner of the key)

RSA, An Asymetric Key Algorithm §8.3.1

- RSA - Rivest, Shamir, Adleman (1978)
- Very robust algorithm, but requires keys of length 1024 bits
- Simplified RSA method
  - Choose 2 large prime numbers, p and q (both 1024 bits)
  - Compute $n = p \times q$, and $z = (p-1) \times (q-1)$
  - Choose a number relatively prime to z and call it d
  - Find e such that $e \times d = 1 \mod z$
  - Use this number as the key to encrypt and decrypt
- RSA's security is based on the difficulty involved in factoring *large numbers* - approx 10^{25} years to factor a 500 digit number using a brute force approach
- RSA is too slow for encrypting/decrypting large volumes of data, but is widely used for *secure key distribution*

Using Cryptography: Digital Signatures §8.4

- Cryptographic approaches can be used to ensure *authenticity* and allow for *non-repudiation*
- Requirements
  - Receiver can verify the claimed identity of the sender
  - Sender cannot repudiate contents of the message
  - Receiver cannot have derived the message themselves
- Three approaches
  - Using symmetric keys via an intermediary to ensure non-repudiation
  - Using public keys as individuals
  - Using message digests

Message Digests §8.4.3

- Basic concept of a message digest is to use a *one-way hash function* to take an arbitrary length of plaintext and compute a fixed-length bit string
- A message digest (MD) has four important properties:
  1. Given P, it is easy to compute $MD(P)$
  2. Given $MD(P)$ it is effectively impossible to find P
  3. Given P, no one can find P' such that $MD(P') = MD(P)$
  4. A change in even a single bit of input produces a very different output
- Given 3), the hashing function should be at least 128 bits long
- Given 4), the hashing function should scramble the bits very thoroughly
- Computing a message digest from plaintext is much faster than encrypting plaintext - so digests can be used to speedup the derivation of a digital signature

Message Digest Algorithms §8.4.3

- MD5
- SHA-1
- Comparative output
  - File contents:"this is a test"
  - MD5: e19c1283c925b3206685ff522acfe3e6
  - SHA-1: 6476df3aac780622368173fe6e768a2edc3932c8

Birthday Attack §8.4.4

- Despite the apparent complexity of message digests, perhaps actual complexity is less than perhaps earlier thought
  - Does it take 2^m operations to subvert an m-bit message?
  - In fact, $2^{m/2}$ may be sufficient to break a message digest algorithm
    - Using probability, it can be determined that less than the maximum number of operations may be required to find the answer
    - For a 64-bit message digest, the hashing function can probably be found by generating 2^{32} messages, and looking for two with the same message digest

Public Key Management §8.5

- There is a need for specific PK infrastructure primarily to avoid compromising the security of PK's during the distribution process
- Certification Authority (CA)
  - A trusted intermediary who uses non-electronic identification to identify users prior to certifying keys and certificates
- X.509
  - An international standard for certificate expression
- PKI
  - Hierarchically structured certificate authorities allow for the establishment of a chain of trust or certification path

Lecture XXIX

Network Security: Communication Security

Communication Network Security §8.6

- Cryptography provides the foundation on which network and application security operates

Authentication

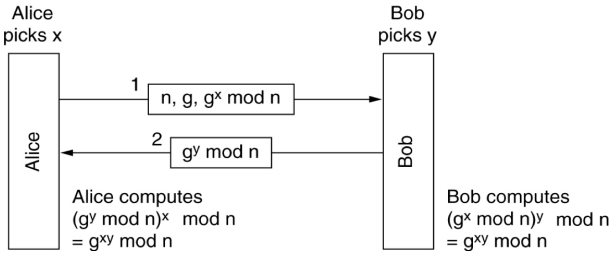
Authentication Protocols §8.7

- Authentication is a primary tenet of network security
- However, authentication itself needs to be secure also
- There are a number of common methods for secure authentication, but all subscribe to a single principle: *minimise the use of permanent/private keys* in establishment of secure connections (the less packets are exchanged using permanent/private keys, the less exposure to potential attackers)
- Four methods in common use:
  - Shared keys
  - Key distribution
  - Kerberos
  - Public keys

Authentication Based on a Shared Secret Key §8.7.2

- In this method, one party sends a random number to the other party, who transforms it and sends the result back - essentially a challenge and response protocol

- Establishing a shared key directly between the two parties requires a mechanism to ensure identity of both parties is confirmed - a mechanism such as Diffie-Hellman key exchange is used



Authentication Using a Key Distribution Center §8.7.3

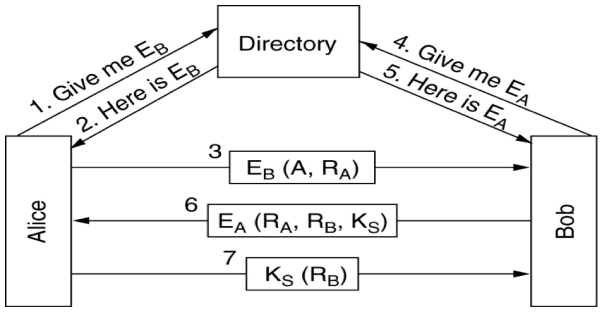
- In this method, a trusted intermediary is used to facilitate the authentication
- Users each share a key with a central key distribution centre, and authenticate to the KDC directly
- The KDC then acts as a relay between the two parties
- Two different algorithms for using a KDC
  - Needham Schroeder
  - Otway-Rees

Authentication Using Kerberos §8.7.4

- In this method, a multi-component system is required
  - Authentication Server
  - Ticket Granting Server
  - Recipient
- Authentication is managed centrally, and then party to party communication is facilitated by single use cryptographic tickets
- Uses Needham-Schroeder algorithm to minimise insecure connection setup packet exchange

Authentication Using Public Key Cryptography §8.7.5

- Public key cryptographic models can be used to assist with the authentication process



Firewalls

Firewalls §8.6.2

- While IPSec ensures security in transit, a firewall ensures security at the network perimeter
- Firewalls are positioned at the network boundary, and provide a controlled series of route between the internal and external networks
- Three characteristics of firewalls
  - All *inbound and outbound traffic* must transit the firewall
  - Only *authorised traffic* must pass through the firewall
  - Firewalls should be *immune to penetration* themselves

Firewall Scope §8.6.2

- Single choke point for range of functions
  - Deny access to unauthorised users either inbound or outbound
- Monitoring location for security related events
- Platform for non-security functions
  - NAT
  - Usage logging and auditing
- Platform for extended security functions
  - IPSEC
  - VPNs
  - Anti-Virus

Firewall Constraints §8.6.2

- No protection against threats originating via bypass networks
  - Direct dialin systems
  - Direct dialout systems
- No protection against internal threats
  - Network segmentation and access control may alleviate internal risks
- No protection against application payload threats
  - Viruses, trojans etc spread as application payloads eg email attachments

Firewall Types and Techniques §8.6.2

- Four firewall techniques
  - Service control
  - Direction control
  - User control
  - Behaviour control
- Types of firewalls
  - Packet filter
  - Application gateway
  - Circuit gateway
  - Bastion host

IPSec

IPSec §8.6.1

- IPSec represents one view of how to embed security in the protocol stack - at the network level
- In the IPSec model, encryption is compulsory, but for graceful failover, a null encryption algorithm can be used between points which are not cryptographically inclined
- The major IPSec framework features are *secrecy*, *data integrity*, and *replay attack protection*
- The IPSec framework allows multiple algorithms and multiple levels of granularity
- IPSec is connection-oriented, with connections being called SA's (security associations)

IPSec Implementation §8.6.1

- IPSec has two main implementation components
  - New headers being added to packets in transit
  - ISAKMP key management
- IPSec has 2 modes
  - *Transport mode* - uses header insertion
    - Authentication Header (AH) - provides no encryption but provides integrity checking using Hashed Message Authentication Code (HMAC)
  - *Tunnel mode* - uses packet encapsulation
    - Encapsulating Security Payload (ESP) - provides an encryption layer as well as HMAC based integrity checking

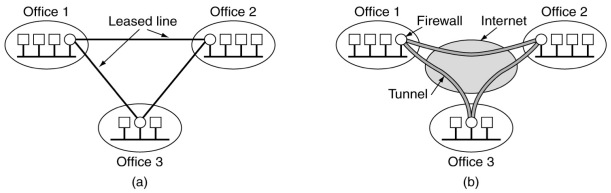
Virtual Private Networks

Virtual Private Networks §8.6.3

- Unlike a physical network based on leased lines between locations for which secure transit is required, a Virtual Private Network (VPN) is a virtual layer on top of an IP network which provides a secure end-to-end connection over public infrastructure
- A common VPN implementation model is to use a firewall at each end of a connection, use the firewalls to setup a SA to create an IPSec tunnel between the two end points, and then selectively route traffic for the specific destination via the encrypted connection
- Using such models, the security infrastructure is transparent to end users as the firewalls are responsible for the maintenance of the VPN

VPNs Illustrated §8.6.3

- (a) a leased line network
- (b) a virtual private network



IPSec VPNs **§8.6.3**

- Components of an IPSec VPN
  - Content encryption algorithm eg DES, 3DEs, AES
  - Collision-free hashing algorithm eg MD5, SHA-1
  - Diffie-Hellman key exchange protocol
  - Public Key Infrastructure for Certification
- IPSec VPN Architecture
  - *Authentication Header* (AH) added to an IP Packet to provide data origin authentication and data integrity checking
  - An *Encapsulating Security Payload* (ESP) for IP provides encryption, data origin authentication and data integrity checking
  - *Internet Security Assocation and Key Management Protocol* (ISAKMP) and Internet Key Exchange (IKE) allow VPN devices to
    - securely negotiate and manage IPSec security associations (SAs)
    - to generate, exchange and manage the keys that are used by the cryptographic algorithms employed by IPSec

Wireless Security

Wireless Security Context **§8.6.4**

- Wired networks are relatively easy to secure because they require physical access to intercept traffic
- Wireless networks are more difficult to secure because of omnidirectional signal propagation
- Additionally by default most wireless network equipment operates in an insecure and promiscuous manner
- 802.11 has a native secure protocol, *Wired Equivalency Protocol* (WEP), which is a 40-bit encryption based on RC4 algorithm

Wireless Security Issues **§8.6.4**

- WEP suffers from two inherent insecurities
  - 40 bit encryption is breakable with low-moderate computational resources
  - RC4 re-uses keys, so capturing a sufficient volume of encrypted traffic will guarantee key identification
    - An inherent weakness in WEP is that it uses only a 24 bit range to populate initialisation values for RC4, so after 2^{24} packets, the sequence cycles being to repeat
    - A number of attacks against RC4 have demonstrated that the key can be derived from the encrypted stream given sufficient sample data
- Given these constraints, how can wireless networks be secured ?

Securing Wireless **§8.6.4**

- MAC Address Filtering
  - Only allow specified MAC interfaces to establish connections
- Non-Broadcast SSID
  - Prevent discovery of Community String by eavesdroppers
- Additional encryption (128bit WEP)
  - Increased security through longer key lengths
- Multilayered security
  - All of the above plus a VPN over wireless and regimented user authentication

Summary - Security

- Cryptography
  - Contrast the strengths and weaknesses of different cipher modes
  - Explain the use of message digests
- Authentication
  - Describe the basic operation of authentication using public key cryptography
- Network Security
  - Describe the key functions that need to be provided by a firewall
  - Summarise some of the challenges for wireless network security

Lecture XXX

Tutorial: Network Security

1. Design an attack on the DES cipher by using the knowledge that the plaintext to be sent contains only upper case ASCII letters and the space character.

2. Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of the ciphertext in block C_i has been corrupted during transmission. How much of the plaintext will be corrupted as a result?

3. Give reasons why a firewall might be configured to (a) inspect incoming traffic, and (b) inspect outgoing packets. How likely is it that these inspections will be successful?

4. An organization uses a VPN to securely connect its sites over the Internet. Is there any reason why Alice, an employee of the organization, might need to use additional security to communicate with Bob, another employee of the organization, if they communicate via the VPN?

5. Find a 77 bit one-time pad that generates the text "Donald Duck" from the ciphertext of Fig. 8-4.

6. Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block C_i is accidently transformed from a 0 to a 1 during transmission. How much plaintext will be garbled as a result?

7. Now consider ciphertext block chaining again. Instead of a single 0 bit being transformed into a 1 bit, an extra 0 bit is inserted into the ciphertext stream after block C_i. How much plaintext will be garbled as a result?

8. Compare cipher block chaining with cipher feedback mode in terms of the number of encryption operations needed to transmit a large file. Which one is more efficient and by how much?

9. Suppose a user, Maria, discovers that her private RSA key $(d1, n1)$ is the same as the public RSA key $(e2, n2)$ of another user, Frances. In other words, $d1 = e1$ and $n1 = n2$. Should Maria consider changing her public and private keys? Explain your answer.

10. Consider the use of counter mode, as shown in Fig. 8-15, but with $IV = 0$. Does the use of 0 threaten the security of the cipher in general?

11. The Diffie-Hellman key exchange is being used to establish a secret key between Alice and Bob. Alice sends Bob (719, 3, 191). Bob responds with (543). Alice's secret number, x, is 16. What is the secret key?

12. Assuming that everyone on the Internet used PGP, could a PGP message be sent to an arbitrary Internet address and be decoded correctly by all concerned? Discuss your answer.

Lecture XXXI
Course Review

Course Review

- "The objective for this subject is for students to develop an understanding of foundational network technologies and applications, and be able to demonstrate proficiency in internetworking and its management" (from the Handbook Entry for 433-522)
- Major Goals
  - Develop an understanding
  - Foundational network technologies and applications
  - Proficiency in internetworking and its management

Week 1: Introduction

- Computer networks can be used for a wide range of services and by a wide range of users, and are becoming increasingly prevalent
- Networks can be classified based on coverage and bandwidth eg LAN, MAN, WAN, wireless
- Network software consists of protocols, the syntax that governs network communication - protocols are collected into a stack
- Different models for the various layers of a network exist (OSI, TCP/IP)

Week 1: Introduction

- Networks can provide connection-oriented or connectionless services
- The Internet is the most widely known network, but its precursor, ARPANET provided the context for the development of many operational technologies
- Standardisation of both hardware and software is important to ensure interoperability between different implementations

Week 1: Introduction

- Network fundamentals
  - Explain client-server model
  - Characterise differences between
    - Point-to-point vs broadcast links
    - Bus vs ring network types
- Network Architecture Models
  - Explain differences between protocols, layers & services
  - Characterise features of connection-oriented vs connectionless services
  - Evaluate strengths & weaknesses of OSI & TCP/IP

Week 2: Physical Layer

- Physical layer is the basis of all network technologies - natural limits on different types of channels and thus affect their bandwidth
- Transmission media can be guided (twisted pair, coaxial cable, fibre optics) or unguided (radio, infrared, lasers, microwaves)
- The PSTN network is a key element in many networks as it provides the local loop between the consumer and the network service provider - can be used by telephony, data and integrated services
- On PSTN networks, both packet and circuit switching are important

Week 2: Physical Layer

- Data Communications Theory
  - Calculate the maximum data rate of a noiseless channel
  - Characterise different guided media
    - Twised pair vs coaxial cable vs fibre optics
- Telephony Networks
  - Explain structure of the PSTN
  - Recognise different modulation types

- Wireless Data Transmission
  - Explain differences between wireless transmission types
    - Radio, EM, microwave, infrared
  - Choose the appropriate type of satellite for an application

Week 3: Data Layer

- The data link layer converts a raw bit stream into a series of frames
- Various framing methods are used
- Protocols at the data link layer can provide error detection and control, as well as flow control - the sliding window mechanism is used to integrate these two concepts
- Sliding window protocols can be categorised based on the function which determines the size of the sender's and receiver's windows
- Sample protocols which demonstrate the increased complexity of protocol design
- Many networks use a bit oriented protocol at the data link level - all use flag bytes to delimit frames and bit stuffing to prevent flag bytes occurring in the data
- The Internet uses PPP as the major protocol over point to point lines

Week 3: Data Layer

- Data Link Layer
  - Contrast types of services provided
  - Apply different framing methods
    - Character count, bit and byte stuffing
  - Explain methods for error detection / correction
- Data Link Layer Protocols
  - Characterise different protocols
    - stop-&-wait, sliding window, go-back-N, selective repeat
  - Calculate efficiency of stop-and-wait
  - Compare HDLC and PPP protocols

Week 4: Medium Access Control Sublayer

- In networks which have a single communication channel available, the design of the allocation mechanism for this channel is important, and many methods have been developed to achieve this
- The simplest allocation schemes are FDM and TDM - both best when traffic is continuous and number of nodes is small
- In larger systems, protocols derived from ALOHA are better choices
- Carrier sensing can be used by nodes to determine the state of the channel in advance of transmission
- Some protocols reduce or eliminate contention - binary countdown, tree walk
- Wireless LANs have unique problems and solutions for transmission management - MACA, MACAW
- Ethernet (dominant form of local area networking) is available in speeds from 10Mbps to 1Gbps using mostly twisted pair media
- Wireless LANs are becoming common, mostly using 802.11

Week 4: Medium Access Control Sublayer

- MAC Sub-layer
  - Compare different CSMA schemes
  - Summarise collision free protocols
  - Explain for WDMA and Wireless protocols
- Ethernet
  - Explain key features of Ethernet
  - Evaluate factors affecting Ethernet performance

Week 5: Network Layer

- The network layer provides services to the transport layer in either virtual circuit or datagram modes
- Main purpose of network layer is to route packets from source to destination
- Many routing algorithms are used in modern networks - static vs dynamic algorithms,
- Other routing variants - broadcast, multicast, hierarchical routing
- Congestion can occur in the network layer, necessitating mechanisms to resolve congestion including retransmission policies, flow control, load shedding, choke packets
- The Internet has a variety of protocols available at the network layer - IP as the primary data transport protocol, but also ICMP, ARP, RARP

Week 5: Network Layer

- Routing
  - Summarise differences between VC and Datagram subnetworks
  - Demonstrate and contrast Distance Vector and Link State Routing
- Internet Protocol
  - Explain principles of Internet design
  - Analyse structure of IP addresses
  - Explain roles of different Internet Control Protocols
- Quality of Service
  - Summarise effects on congestion of policies at different layers
  - Characterise QoS requirements of different applications

Week 6: Transport Layer

- The transport layer provides reliable, end to end connection oriented byte streams
- Primitives allow the establishment, use and release of connections
- Berkeley sockets are a common method for utilising the transport layer interface
- Transport protocols must also perform connection management over unreliable networks - mechanisms for handling lost or duplicate packets are important
- Three way handshakes are a common connection establishment mechanism
- The Internet has 2 main transport protocols - TCP and UDP

Week 6: Transport Layer

- UDP is a connectionless protocol that mainly wraps IP packets with additional features of multiplexing using ports in addition to an IP address
- TCP is a reliable byte stream protocol, which allows segments to be disassembled and reassembled during transit
- Network performance is dominated by the need to reduce protocol and TPDU overhead - increasing problems at higher speeds - protocols should be designed to minimise the impact of increased traffic

Week 6: Transport Layer

- Transport Layer Services
  - Discuss challenges in providing reliable services over unreliable network layer
  - Explain solutions for connection establishment and release
- Internet Transport Protocols
  - Characterise differences between TCP and UDP
  - Explain TCP congestion control

Week 7: Application Layer: Core Internet Applications

- Foundational to the Internet architecture is the hierarchical naming scheme DNS
- DNS is implemented as a distributed database system which can be queried by clients to determine mappings between IP addresses, host names, and various other types of records

- Email is a dominant Internet application consisting of two components - the user agent and the mail transfer agent
- Email sent by SMTP, and alternatively received by POP3 or IMAP

Week 7: Application Layer: Core Internet Applications

- Email has been extended to allow the transmission of non-text objects through the use of MIME
- The WWW is actually an application that uses the Internet as a foundation
- Browsers are used to navigate the WWW, with the assistance of browser plugins and helper applications for rich content handling
- Information sources on the WWW can include both static and dynamic document types
- Web standards are continuously evolving

Week 7: Application Layer: Core Internet Applications

- DNS
  - Describe operation of DNS lookup
- Email
  - Explain which functions should be performed in Message Transfer Agent or User Agent
  - Explain techniques for audio compression
  - Compare POP3 and IMAP
- World Wide Web
  - Choose between server-side vs client side technologies for dynamic content
  - Explain difference between plug-ins and helpers
  - Describe the role of cookies

Week 8: Application Layer: Emerging Internet Applications

- Multimedia on the web has become a feature of the Internet in the last 5 years
- Multimedia networks are characterised by higher bandwidth requirements and the need for Quality of Service in order to be accepted by end users
- Online audio requires compression in order to achieve efficient transmission
- Data networks are increasingly being used to carry voice traffic and this new traffic brings different perspectives to network design
- The dominant VOIP technologies are H.323 and SIP, which provide a number of core functions, with specialisation in different areas, both derive from different traditions of standards development
- Online video also requires compression in order to achieve efficient transmission

Week 8: Application Layer: Emerging Internet Applications

- Multimedia networks
  - Describe techniques for jitter management
  - Explain techniques for audio compression
  - Compare JPEG and MPEG standards
- VoIP
  - Contrast H.323 and SIP
  - Explain steps in SIP call establishment

Week 10: Network Security

- Network security is an important issue to consider given our increased dependence on network transmission of data
- Cryptography is a method that can be used to protect confidential data
- Ciphers are used to convert plaintext into ciphertext - many different types are available
- Cryptographic algorithms can be divided into symmetric and assymetric types

- Public key algorithms are architecturally distinguished by the use of a widely distributed key for encryption, and a private key for decryption
- Digital signatures can be constructed to ensure the reliability and non-repudiation of data - message digests, digital certificates

Week 10: Network Security

- Cryptographic tools can be used to secure network traffic - IPSec is the dominant model and is widely used to constructed encrypted streams between sources and destinations
- Firewalls are an important component of network security architectures, serving not only as a border between public and private networks but also as the termination points for virtual private networks
- Network security is a pervasive issue - existing at all layers of a network architecture

Week 10: Network Security

- Cryptography
  - Contrast the strengths and weaknesses of different cipher modes
  - Explain the use of message digests
- Authentication
  - Describe the basic operation of authentication using public key cryptography
- Network Security
  - Describe the key functions that need to be provided by a firewall
  - Summarise some of the challenges for wireless network security

Week 11: Student Presentations

- What was important about the presentations and written reports ?
  - Experience in conducting research
  - Integrative writing - bringing together multiple aspects of a technology
  - Critical evaluation of technologies

Week 12: Review

- "Generic skills" to take away from this course:
  - be able to analyse the relationship between different components of computer networks;
  - be able to conceptually and practically differentiate the various layers in internetwork architectures;
  - be able to conduct research into emerging networking technologies;
  - be able to apply network security and network management concepts in today's networked environments.

Lecture XXXII

Exam Discussion

Practice Exam

Practice Exam

- Practice Exam will be available on website
- Questions are indicative of the types of questions on this year's exam
- Suggest students take the practice exam, and then attend consultation sessions to review answers and problems

Examinable Content

Examinable Content

- Exam will test your understanding of the course topics and ability to meet the course objectives
- Focus will be on understanding of concepts rather than recall of specific items from readings and lectures

- Questions are "topical" - typically a topic and scenario is given and brief discussion is requested.
- Examinable Content - reflects material covered in lectures, tutorials and assignements

Exam Details

Exam Details

- Length: 3 hours in length, with 15 minutes reading time
- The exam will *not* be an open book exam
- I will be in attendance at the exam itself during reading time to answer any questions that may arise

Exam Structure

- Exam consists of 20 *short* answer questions. You should attempt to answer all questions.
- Each question will be worth a maximum of 3 marks.
- Questions should be able to be answered in a *maximum of 2 paragraphs* (usually less).

Exam Revision

Exam Revision

- Identify the key concepts from each week's readings, lectures, tutorials and assignments
- Don't ignore any of the lectures, tutorials, assignments and relevant sections from the textbook - examinable content may originate in any of them
- Look for recurring themes
- Consider how key concepts from different topics could be related eg.
  - jitter management for streamed media
- Try some questions from the end of chapter question sets, but don't spend all your time on them

Exam Consultations

Exam Consultations

- I will be available for consultation regarding the examination on the following dates/times/locations:
  - Please see COMP90007 (433-522)LMS for more details;
- Unless you can demonstrate a *legitimate* reason why you cannot attend one of these consultation sessions, I will not be conducting individual consultations regarding the exam at other times.

Lecture XXXIII
Where to from here?

Now you've done 522, what next?
If you are interested in internet technologies in general, there are other MIT/MSSE/MIS subjects you may want to consider in future semesters:

- SWEN90002 Engineering for Internet Applications
- COMP90017 Sensor Networks and Applications
- COMP90024 Cluster and Grid Computing