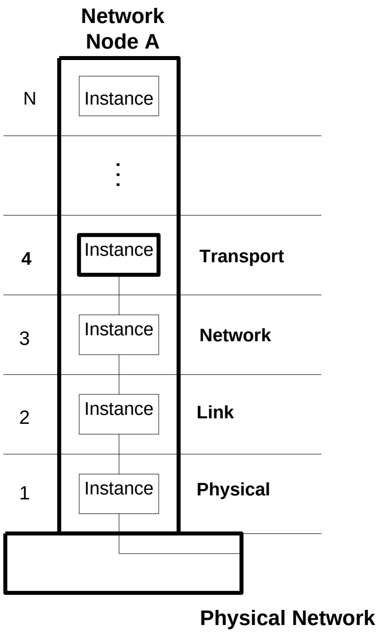
CS2005 Notes

Lecture 1a; Introduction to Networks

Networks are a collection of interconnected links and nodes

The network layer diagram;

- Standardise network protocols between nodes and instances;
- Standardise software interfaces between layers
- Standardise hardware
- Allow component (layer or sublayer) replacement

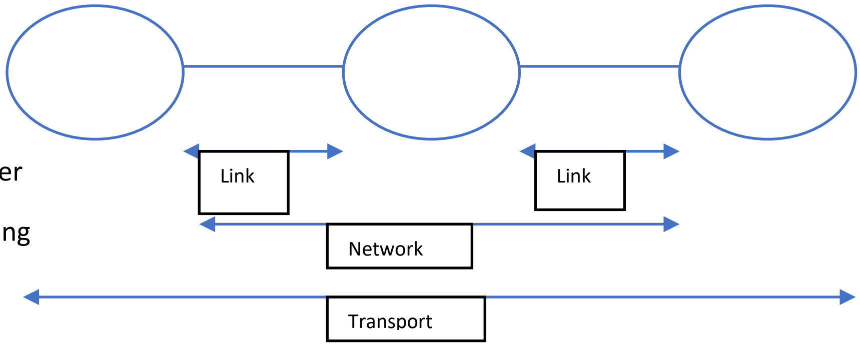


OSI 7 Layer Reference Model;

1) Application;
    a. Application Access, control and management, file transfer
       Protocols that fulfil certain tasks, transfer blocks of data from one thing to another
2) Presentation;
    a. Data transfer, syntax negotiation, data representation.
       Interpret data no matter what machine it is running on
       help understand data
3) Session;
    a. Dialogue and sync control
       Ensures longevity of a connection, picks up where it left of
4) Transport;
    a. End to End transfer
       (connection management, error control, Fragmentation, flow control)
       Ensure reliable, no errors, splits up big data, asks recipient if ready to receive data
5) Network;
    a. Network addressing, routing, call setup and clearing
       Sending a packet from node to node, hopping through network
6) Link;
    a. Data link control
       (framing, data transparency, error control, media access)
       send a bit, bits put together in link layer
7) Physical;
    a. Electrical and mechanical interface definitions
       Ethernet plug – put in socket, pin size, cable made in certain way

Purpose of the Layers;

Physical;	Bit level transfer
Link;	Node to Node transfer
Network;	Addressing and routing
Transport;	Reliable transfer



Physical Layer;

- Bit level transfer, node to node
- Specifications;
    - Mechanical – plugs sockets, cable
    - Electrical – voltage, impedance timing

Link Layer;

- Node to node transfer of frame
- Link addressing
- Topology
- Medium access

Network Layer;

- Routing End to End
- Network addressing
- Optimise routing

Transport Layer;

- Reliable transfer
- Error correction
- Flow control
- Fragmentation
- Multiplexing

Session Layer;

- Persistent transport layer connection
- Control intermittent connection
- Reliable data exchange

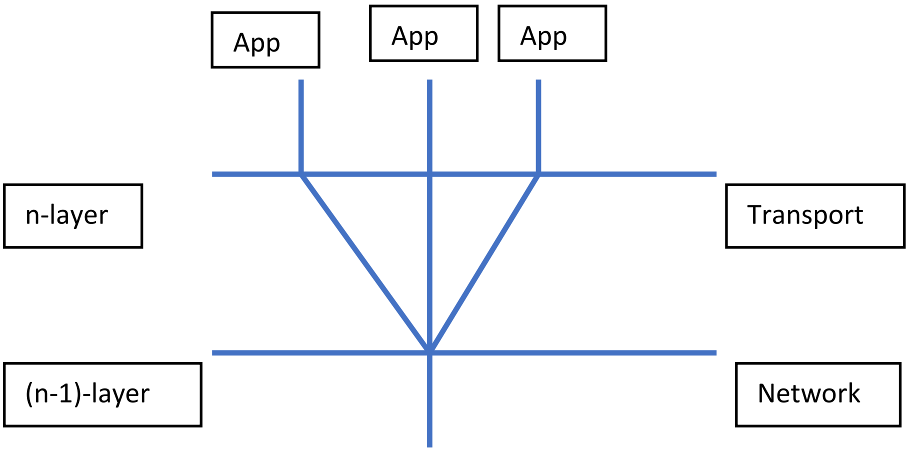
Presentation Layer;

- Negotiated Interpretation of incoming byte stream
- Network (machine) independent data transfer

Application Layer

- Application access
- Application data exchange
- Application control and management
- Application methods and data models

Multiplexing;

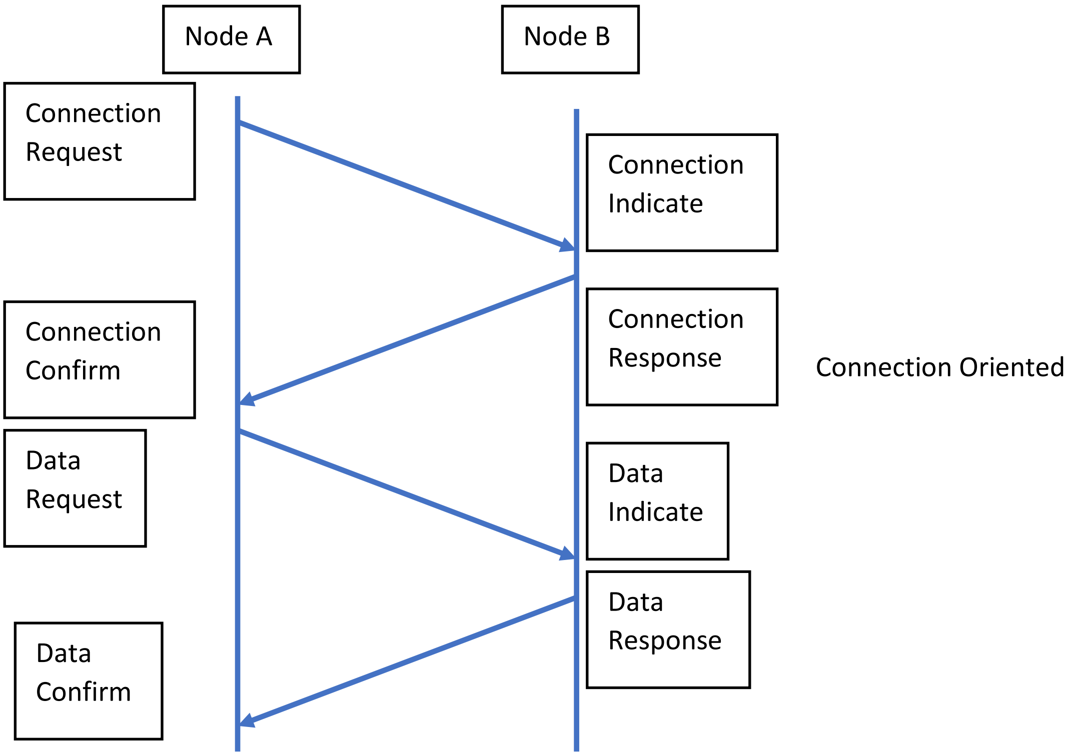


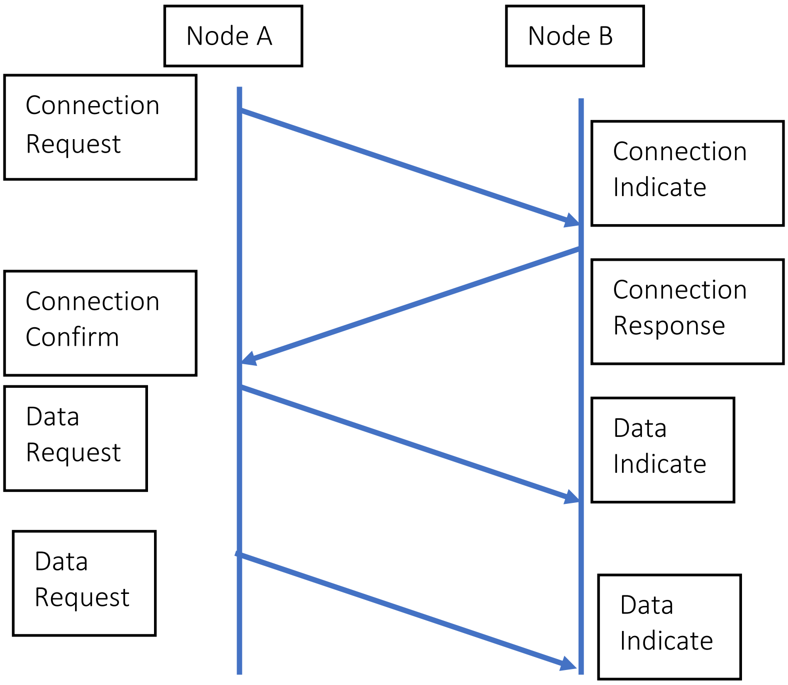
Connection-oriented;

(between 2 peers)

Like a phone call;

- Must establish connection
- Both parties must be available
- Address used only to set up
- Data arrives in order sent
- Error control possible
- Flow control possible
- Must hang up



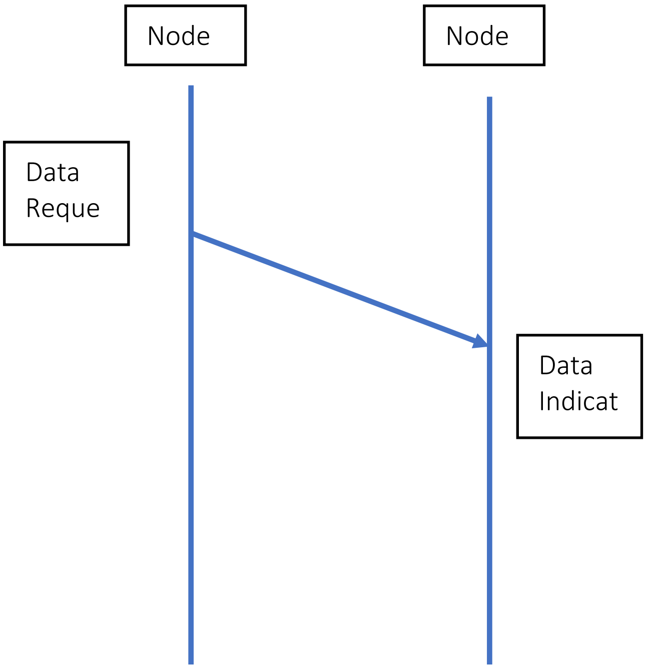


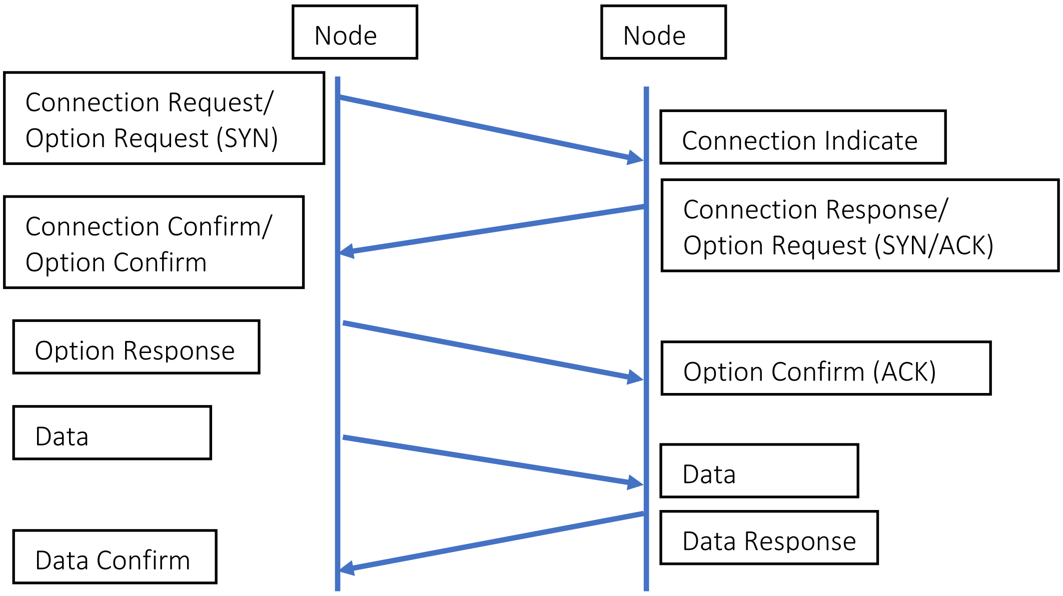
Connection Oriented – unacknowledged

Connectionless;

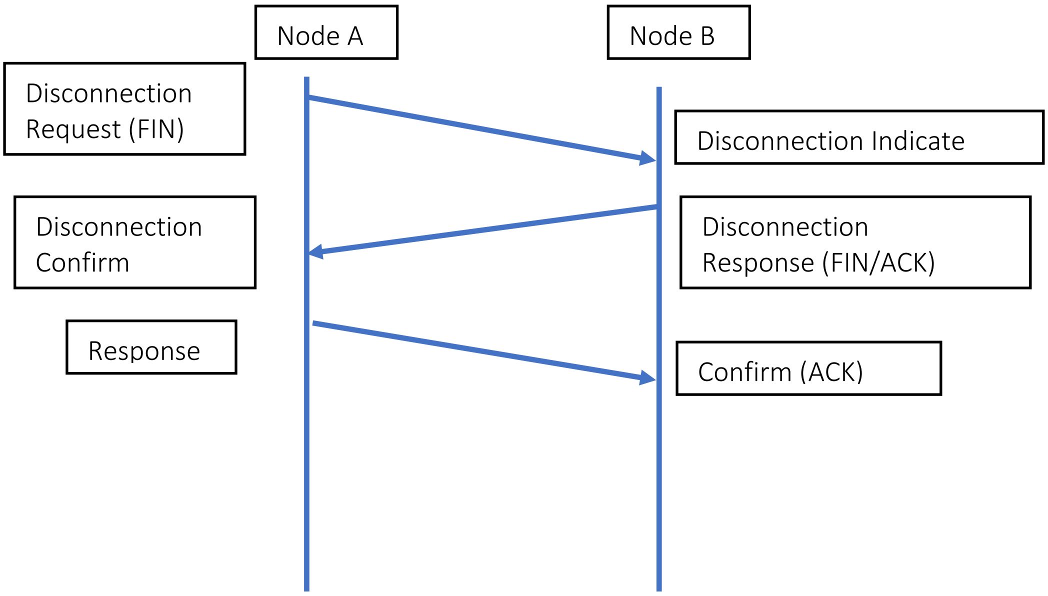
Like a letter

- No connection required
- Received does not need to be present
- Every packet needs an address
- Data may arrive in any order
- No error control
- No flow control
- Data may be lost




Node
Node
Connection Request/ Option Request (SYN)
Connection Indicate
Connection Response/ Option Request (SYN/ACK)
Connection Confirm/ Option Confirm
Option Response
Option Confirm (ACK)
Data
Data
Data Response
Data Confirm

TCP connection-oriented; 3 way handshake connection
this shows a connection establishment, single frame of data being sent



TCP connection-oriented; 3 way handshake Disconnect

Lecture 3; Physical and Link Layers;

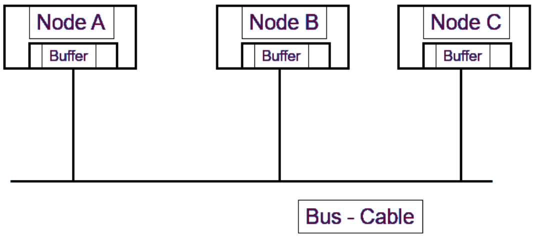
Network Topology;

The way in which constituent parts are interrelated or arranged

- Bus
- Star ring
- P2P
- Wireless

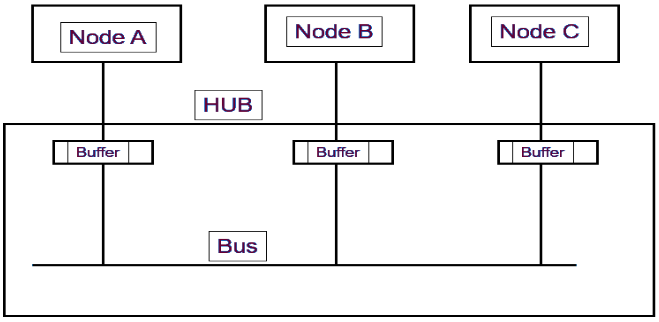
Bus – cable;

- Unreliable
- Error control is a long process – time consuming
- Only one node can transmit data at an given time – bandwidth restrictions



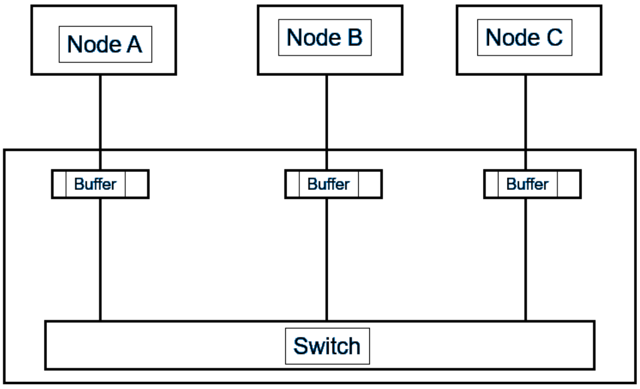
Bus – Hub;

- Instead of node to node connections, bus is *within* the hub
- Cables connect from buffer to each node
- Bus cannot be disconnected or roken – network works when notes are inserted and removed from network



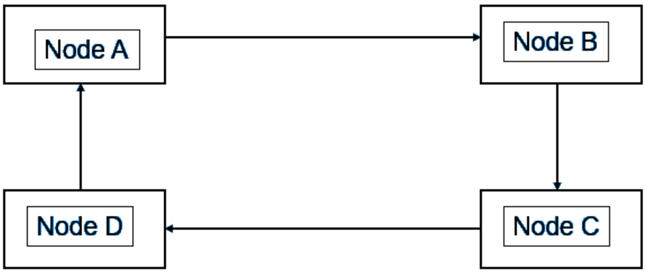
Star – Switch;

- Switching unit can take care of multiple packets at the same time
- The links are bi-directional
- Reliable – can plug and unplug without disrupting the rest of the network



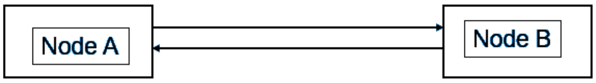
Ring – Physical;

- It takes time to pass packets around the ring
- Can take care of multiple packets at the same time
- Any node can send data to any other node



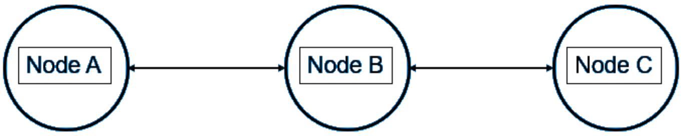
P2P;

- Bi-directional connection



Wireless;

- How does Node A know about the existence of Node C? vice versa
- Node A cannot transmit at the same time as Node C, otherwise Node C will get garbled message.

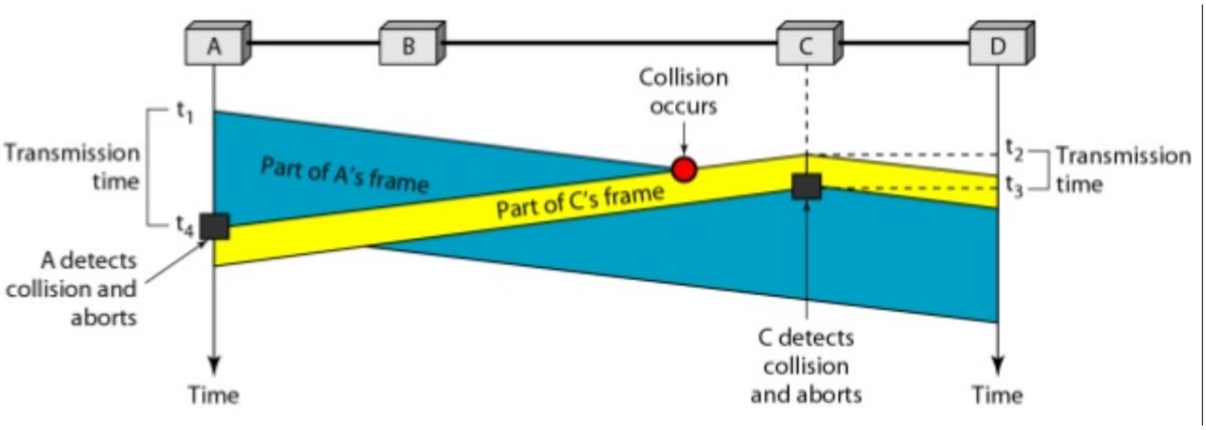


(not strictly a topology, but physical characteristics to be considered)

MAC protocol – Human Example;

	HUMAN	MAC	
BUS OR PEER	Coffee room	CSMA/CD	Carrier Sense Multiple access/Collision Detection
MASTER/SLAVE	Committee	Polling	Master in control – hand over control and back
TOKEN PASSING	Greek Democracy	Token Ring	Speak with token
RADIO	All for one	Aloha	Anyone can speak at any time

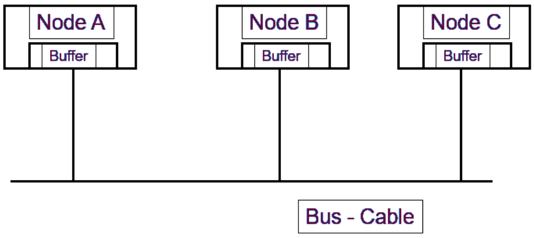
CSMA/CD protocol;



- Any of these nodes can transmit at any time
- Need to implement a turn taking protocol on these nodes for fair turn taking

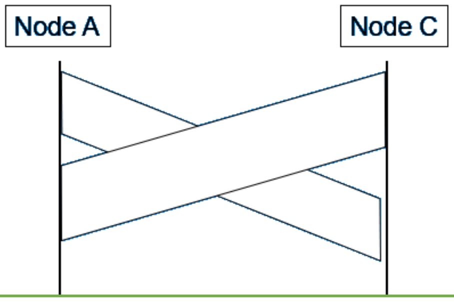
Biggest Problem of CSMA/CD protocol;

- When a node at each end determines to transmit
- It takes time to pass a packet down the cable, Node C doesn't know what Node A is transmitting, Packets could get corrupted due to this



Collision Detection;

- Minimum packet length (header and footer of packet)
- Jamming signal sent to make aware of corruption
- Length of frame
- If Node A must transmit continuously to detect collision, what is the minimum frame size?



Length of Frame;

$$Td = 2 * Tp$$

Where Td is the duration
Where Tp is the propagation delay

Propagation time;

$$Td = 2 * \frac{L}{V}$$

Where Td is the propagation time
Where L is the length
Where V is the velocity

Duration of the Frame size/transmit rate;

$$Td = \frac{Bits}{Tx}$$

Where Td is the duration
Where $Bits$ is the frame size
Where Tx is the transmission rate

Frame Size;

$$Bits = 2 * L * \frac{Tx}{V}$$

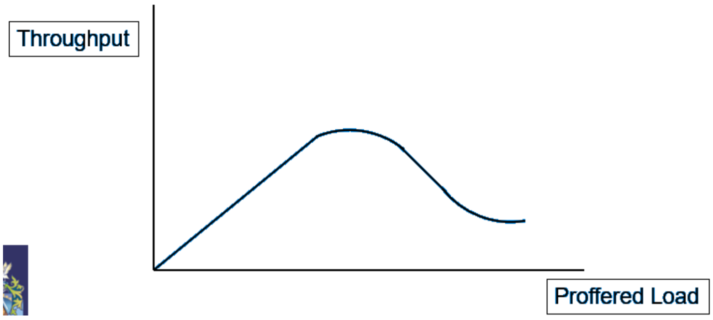
Where $Bits$ is the frame size
Where L is the length
Where Tx is the transmission rate
Where V is the velocity

Example; Suppose

$$V = \frac{c}{3} = 10^8 \, m/s$$
$$Tx = 10Mbps$$
$$L = 2500m$$
$$Bits = 500 \equiv 62.5 \; bytes$$

What Happens after a collision?

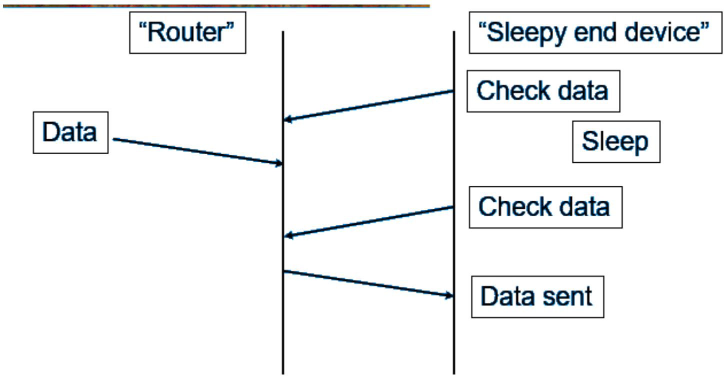
- Exponential back-off protocol – 802.3
  - Introduce notion of random delays
  - All waiting nodes choose a transmission window
  - If further collision, increase number of transmission windows $(x2)$
  - Repeat
  - Report error if fail after n tries
- Effect of Load



As low loads throughput will increase in line with increasing proffered load

As proffered load increases, more time is expended on resolving collisions and throughput decreases

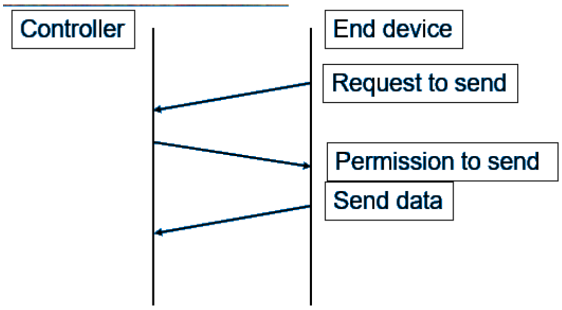
"sleepy end device" protocol;



Sleeps for 10 seconds then wakes up to send data

Puts the device to sleep for a period, then wakes up, checks for new data – results in latency of response

"Reservation" protocol;



Instead of transmitting the entire packet of data, use a short message "I would like to transmit"

Controller chooses one of the requests to have permission to send its data

Basic Frame Format;

What do we need?

Where is the frame going?	Destination
Who has sent the frame?	Source
Start and end of frame	length of delimiters
Wake up receivers	Sync of clocks
Error check	collision or interface
Error correction if possible	
Address multiple receivers	
Options	
Technology dependent aspects	

MAC Frame Format;

BYTE LENGTH	NAME	USES
7	Preamble	Sync receiver
1	SD	Indicate start of frame
6	DA	Address of destination node
6	SA	Address of sending node
2	Length	No. of bytes in data field
0-1500	Data	-any up to max size-
AS REQUIRED	Padding	Extra bytes to meet min frame size
4	FCS	Check bit errors in frame

Addressing multiple receivers;

- Broadcast address used to cause all listening receivers to accept fame (FFFFFFFF)
- Multicast address used to cause configured receiver to accept frame

IEEE address format;

OUI –	Organisation Unique Identifier e.g. Brunel == 0x801687
Unique ID –	maintained by organisation to ensure globally unique identifier

Why use padding?

- Frame format of min fixed size, given by the headers when 0 data
- CSMA/CD requires min frame size to detect collisions
- Have to pad to meet min frame size

What is Frame Check Sequence?

- Detect corruption on the wire or collision
- Bytes added at the end to check for corruption upon reception

Types of FCS;

- Parity;
  - The total number of 1's that are transmitted are the same as the type that you have chosen
  - Even parity; even no. of 1's (binary string ends with 0)
  - Odd parity; odd no. of 1's (binary string ends with a 1)
- Checksum;
  - Treat the frame as an array, go through and add up all contents
  - Receiver calculates checksum and compares
- Cyclic Redundancy Check (CRC);
  - Powerful technique to detect errors
  - If no error remainder = 0
  - If remainder of non-zero this indicates an error
  - Repeated modulo 2 division of data sequence of n bits with $r0$ bits added by generatior polynomial of $length\ r + 1\ bits$
  - Calculate in exam long division 1001 / -sequence-

Advantages of CRC;

- Can be calculated bit by bit "on the fly"
- Easily implemented in hardware – fast
- Detects all R(remainder) bit errors

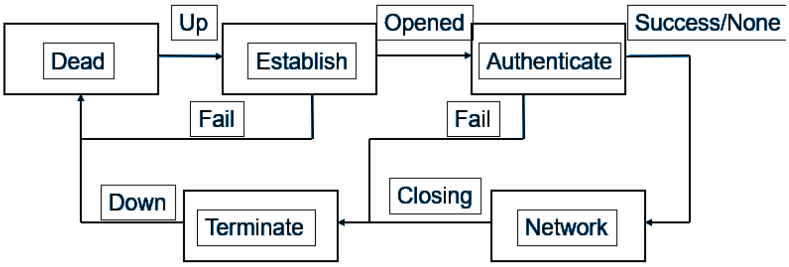
P2P protocol;

- Used on serial link (e.g. modems)
- Transparent transfer of any network protocol
- Uses link control protocol (LCP)
- Use state model (automaton)
- Can include authentication

P2P Frame Format;

BYTE LENGTH	NAME	USES
2	Protocol	Tells type of packet (e.g. IP, LCP)
0-1500	Information	Network packet
-AS REQUIRED-	Padding	To ensure min size is met

P2P state model;



Network systems are event driven.

Events drive the state model between states

Substituting Sub-Layers;

- Sub layers in the link layer
- Allows different tech to be contained within the sub layer (and substitution of layers)

Transmission Characteristics;

Transmission rate - bandwidth	Higher bandwidth, faster data
Transmission Delay	T for source to destination
Transmission Time	T for transmit a complete frame (size + rate)
Error rate	Retransmission of data
Transmission protocol	Implementation of error checking and ack
Asymmetric bandwidth	Download high, upload low
Latency time	Satellite's higher ping than fibre optic

Circuit vs Packet Switched;

- Circuit Switched;
    - Connection required
    - Connection throughout data exchange
    - Cost based on connection time
    - Generally single connection only allowed
        - Telephone systems
- Packet switched;
    - No connection required
    - Virtual connection by application
    - Cost based on data transferred
    - Many virtual connections
        - Good for real time applications where there is a constant throughput of data

Division of Resource;

How can we share the resources between number of users?

- Total available bandwidth is shared as a sub band
- Frequency division multiplexing – frequency divided between channels
- Time division multiplexing – time divided between channels

Synchronous

- Equal slots are allocated on a rotating basis

Asynchronous

- Random allocation where channels come in and use it on an as-need basis

Physical Limitations;

A signal is not received as a perfect shape (digital signal – often received in analogue wave form)

- Rounded due to bandwidth
- Noise is added (value detected incorrectly, signal exceeds decision) – logarithmic

Extended LANs;

- Bridge can be used to extend length of a single LAN doman
- Brdge will separate traffic and keep traffic local to the LAN segment
- Remote bridge will join 2 separate LANs

- Switches may be connected to increase no. of ports
- Switches can be interconnected to increase network resilience (down time)
- Can cause frames to circulate endlessly
- Create a spanning tree and cut this point of circulation (spanning tree protocol)

Technology for Network connections;

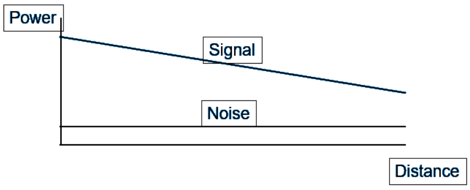
- ATM used for broadband
- Asynchronous transfer mode

How to transfer data and video at same time (multi user etc)

- Split data and video packets into smaller selves
- Max efficiency = big frames sent fast (high speed bursts) so ratio of data to header is large
- Types of ATM traffic;
    - Helps decide which traffic to drop when network becomes congested
- Constant bit rate
- Real time variable bit rate
- Non-real time variable bit rate
- Available bit rate
- Unspecified bit rate

Broadband characteristics;

- More capacity =/= more throughput – more bandwidth
- Vectoring

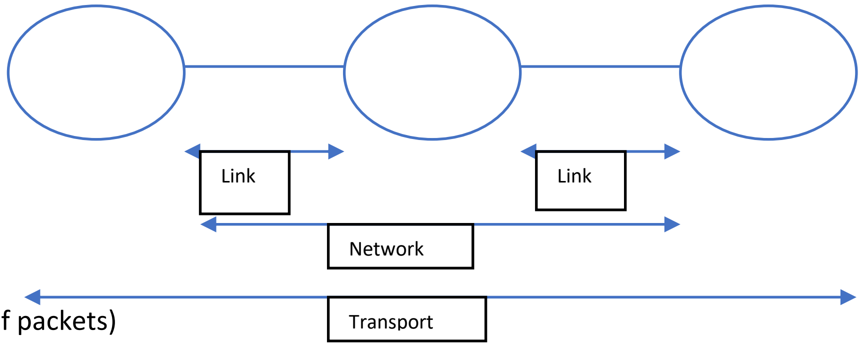


Lecture 4; Network Layers;

- End to end routing
- Network addressing
- Optimised routing - find best route
- Integrate link techs

Network Layer addressing;

what to include in the header of the packer?



- Source address
- Destination address
- Length
- Version
- Protocol type
- Fragmentation
- Identification of the packet
- Time to live (to stop circulation of packets)
- Type of packet

Standards Organisation;

Why use standards?

- Interoperability between systems
- Include expertise in developing standards
- Market support and adoption

What options?

- Proprietary
- De facto standards
- Industry consortium
- Profile

Regulatory bodies;

Ensure appropriate standards are enforced

- Safety
- Enacted through laws
- Regulate sales and distribution within a country or region

Network layer options;

Several uses – can record info on the route of a packet

What do we need from the network layer to support the delivery of packets and management of the network and devices on the network?

Name	Definition	Use
DNS	Domain name system	Resolves names to IP addresses
ARP	Address resolution protocol	Resolves IP address to link addresses
RIP	Routing Information Protocol	Exchange info on routing
ICMP	Internet Control Message Protocol	Diagnostics
DHCP	Dynamic Host Configuration Protocol	Manage automatic allocation of IP addresses Provide another network's info to client

Internetworking;

Why an organisation would want to create sperate subnets within the organisation

- Extend physical network
- Increase capacity
- Management
- Fault tolerance
- Security

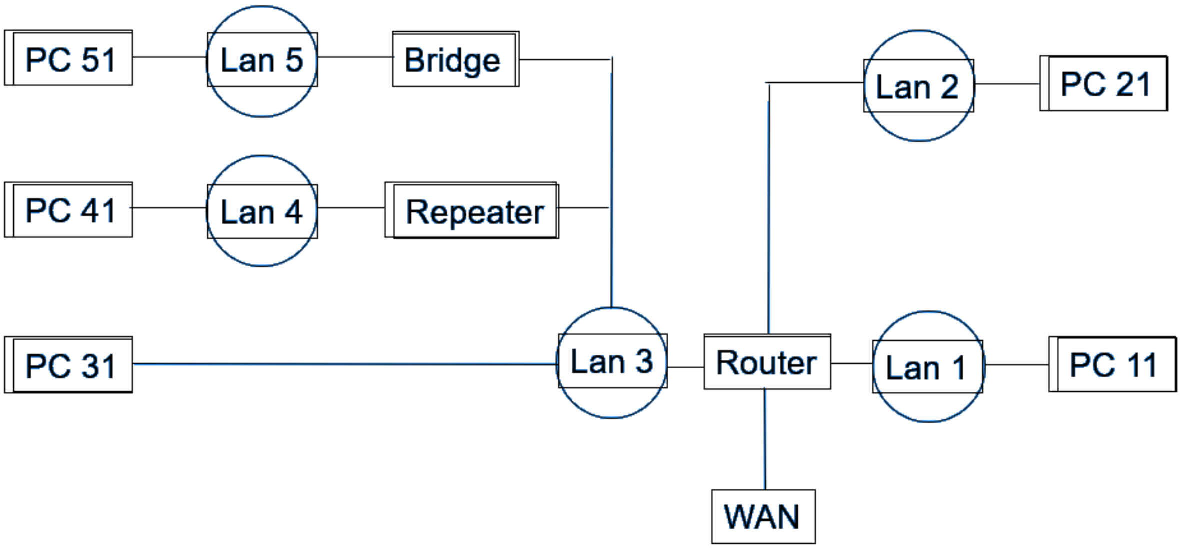
Segmentation of physical networks;

- More network segments
- Isolate faults
- Make segments secure
- Some segments can be publicly accessible

How to extend physical networks;

METHODS	LAYER TYPES
ADD REPEATERS	Physical Layer
ADD BRIDGES	Physical Layer
INTERCONNECT HUBS	Link Layer
INTERCONNECT SWITCHES	Link Layer
USE ROUTERS	Network Layer

Internetworking example;



- LAN1
  Isolated subnet
  - Used for publicly accessible servers
  - Screen incoming services
  - Router would isolate access by the servers on LAN1 to internal network LAN2
- LAN2
  Separate internal subnet
  - Used for internal servers
  - Isolate security and to prevent spread of viruses
  - Extend physical access by users
  - Extend physical size of network
- LAN3
  Acting as a backbone
  - Router
  - Isolate organisation from external access
  - Control external access by ysers
  - Extend physical size of network
- LAN4
  Internal extension
  - Joining floors of a building to create a single network
  - Connect hubs
- LAN5
  Extending using a bridge
  - Connect buildings as a single subnet
  - Use isolation tech such as fibre
  - Join switches – increase number of ports
  - Isolate traffic to separate segments

Network Addressing;

The larger the organisation, the more addresses you are allocated

- ARPA proposed the familiar A.B.C.D where teach part is 8 bits

Internal organisation;

How does an organisation use the address space it is allocated?

- Single subnet with large number of nodes
- Small number of subnets with many nodes
- Large number of subnets with few nodes

Free to choose;
Network nodes must understand which bits are;

- Subnet
- Node

e.g. suppose we are allocated a class B address and choose to have 256 switches each having 256 nodes;

- 134.83.0.0
- 134.83.1.0
- 134.83.2.0

This indicates subnet masking

Physical delivery of IP packets;

How does one node deliver an IP packet to another node using the IP address?

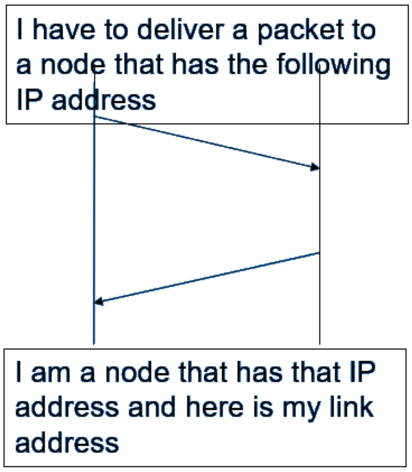
- Map a given IP address on a subnet to the link layer address on that subnet

ARP;

Address Resolution Protocol;

What are the IP and link layer addresses for the packet?

- The IP address will remain the same as it goes through the network
- Link later address will change each time


I have to deliver a packet to a node that has the following IP address
I am a node that has that IP address and here is my link address

Private Networks;

- No packet from these “private” networks should be routed into “public” networks
- “public” network could not deliver to a “private” network

Other Addresses;

The loopback 127.0.0.1

- A packet with this as the destination is delivered back into the same computer (host file)
    - Used for testing and development

Address space;

We have now ran out of address space if a unique address is allocaccted to every device

Solutions;

- Addresses may be re-used when not in use – DHCP
- Private network and NAT (tables)
    - Most networks comprimse many clients that access external servers
    - Most networks include few if any internal servers
    - NAT exploits the many unused ports of a client
    - Maps from internal private address to external private address
        - Outgoing packets will have address/port translated from internal to external
        - Incoming packets will have address/port translated from external to internal
    - Mapping table entries are created by TCP connection
    - Entry cleared by NAT router by TCP disconnect from mapping table
    - If there is no traffic using that mapping for a period, then the entry will be cleared (3 mins)
    - Mapping put in when UDP packet is transmitted – remains for short period of tie to allow returning packets to be delivered

Private network and NAT overview;

Advantages;

- Re-use address space
- Security – no incoming connections

Disadvantages;

- Limited number of incoming connections
- Routes may face time out if not used
- Client must initiate all outgoing connections

Private Network Issues;

- Some protocols need to set up an incoming connection (FTP, P2P, NAT)
- Need to monitor protocol and fulfil request
- Need to obtain external IP address for application

Domain Naming Service – DNS;

As a distributed database that stores all the names that I use and prvides a mapping of the IP address of that name

- Domain name is hierarchical
  e.g. www.brunel.ac.uk
  www – local administered
  brunel.ac.uk global administered
- DHCP will allocate different addresses on each connection
- Connecting to different network will allocate different address

Dynamic DNS

- Provides protocol for IP addresses of a domain name to be updated
- On each change of IP, the node updates its DDNS entry

VPN – Virtual Private Network;

Appears to be part of another network

Diagnostics and Management;

Overcome the mobility problem within different networks and how to maintain consistent presence

ICMP;

Developed in order to support doing diagnostics within a network (why no connectivity)

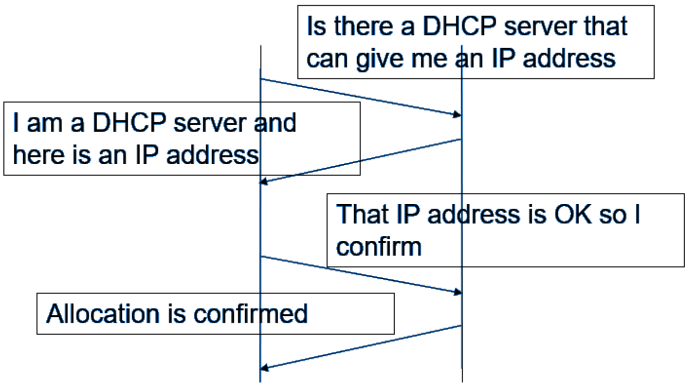
Services include;

- Error messages returned from network nodes to sources (e.g. network unreachable)
- Information messages (TTL exceeded)
- Source quench (sent it buffer overflow)
- Echo message (pin, traceroute)

Example of tools;

- Get IP address (DHCP_
- Get MAC address for IP address (ARP)
- Get IP addresses for name (DNS)
- Wireshark trace

DHCP is used to allocate an IP address to an end device - that will either be an address from the pool or you can reserve an IP address for a given MAC address.

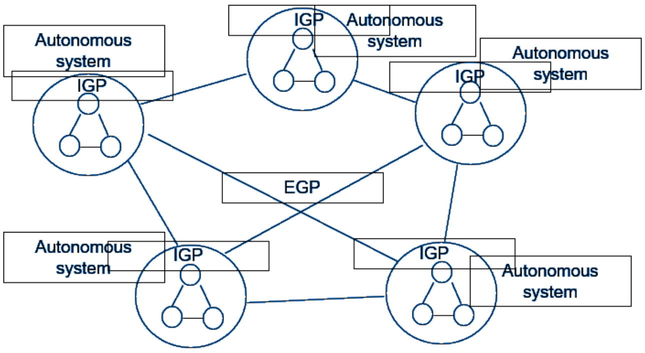

Is there a DHCP server that can give me an IP address
I am a DHCP server and here is an IP address
That IP address is OK so I confirm
Allocation is confirmed

IPv6 Motivations (why not just stick with IPv4)

- Lack of address space
- Improved efficiency in routing
- Enhanced performance – fixed header size, no ARP
- Enhanced functionality
- Better QoS
- Supports mobile home (IP roaming – therefor also supports 4G networking too)

Network layer Routing;

How are packets routed around the network?



- Routing split into 2 domains
  - Interior gateway protocol (IGP)
  - Exterior gateway protocol (EGP)

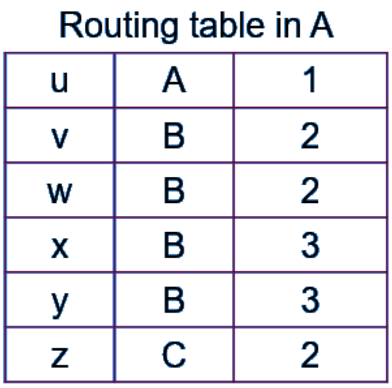
Autonomous Systems – AS

A network that is managed by a single organisation

- All routes aware of all subnets
- Common IGP – RIP (distance vector – Routing Information Protocol), OSPF (link state – Open Shortest Path First)
- Frequent routing messages exchanged between routers to ensure resilient to network changes such as link or node failure.

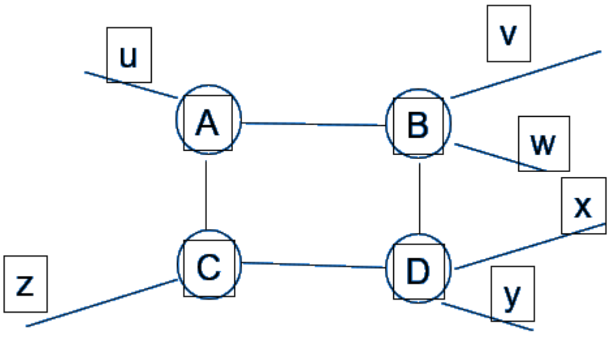
RIP (distance Vector);

- Each node only has information to determine the next node in the route (e.g.)



Routing table in A

u	A	1
v	B	2
w	B	2
x	B	3
y	B	3
z	C	2



- Assumes next node has information to forward to destination
- Choose route on lowest metric
- Each node builds up a table which is then forwarded onto the next router
- Each node will advertise its routing table to adjacent node on frequent intervals
- Vulnerable to loops

OSFP (Open Shortest Path First);

- Each node collects information on state of each link and builds up its own map of topology
- Network flooded with packets to understand the topology
- Each node constructs a map of routes for AS using Dijkstra’s Algorithm
- This reduces the chance of loops

BGP (Border Gateway Protocol);

- How to get through the Autonomous System from one end to another
- Does not pass any information on routing within AS
- Provides information to route packet to destination through separate AS
- Other routes then deliver to border gateway based on prefix
- BGP works out OSPF to determine optimum route to deliver packet

Issues;

- If you are trying to prove the information, in-order to deliver any other organisation, there is a large number of class C
- An ISP may disaggregate its Class C or advertise disaggregated Class A and Class B
- Currently global rating table exceeds 512k entries

MPLS (Multi-Protocol Label Switching Architecture);

- Multi-cast routing
- Multi-media application, several clients connected at once
- Eliminate duplicates at each of the routing nodes

Lecture 5; Transport Layer

- Reliable transfer of packets
- Error correction
- Flow control
- Fragmentation
- Multiplexing

TCP Multiplexing;

- Header of a frame a 4-tuple
    - Source port/address
    - Destination port/address
- All 4 pieces of information is required to uniquely deliver
- Can identify multiple processes on one node with connections to a single application in a destination by using the source port
- Processes on separate nodes using the same source port with connection to a single application in a destination by source address

Connection oriented;

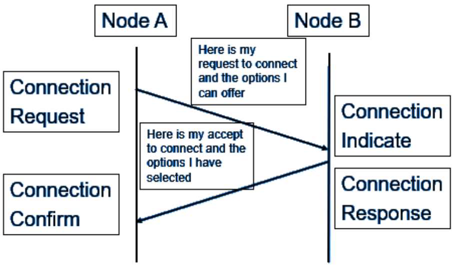
Like a phone call (see lect1a for more info)

- Flow control possible (e.g. "hold on one second, let me write that down")

2-way connect handshake;

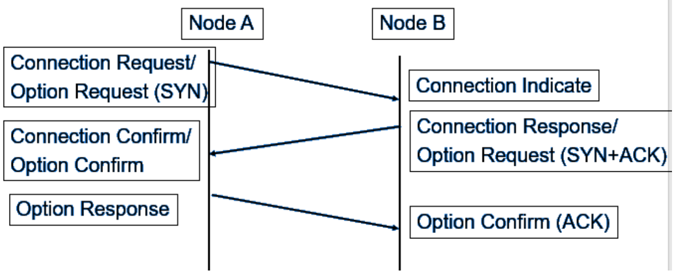
- Connection oriented

  Weaknesses;
- When 2 requests are sent, and Node A will not know which response corresponds to which request/timing problem


Node A
Node B
Here is my request to connect and the options I can offer
Connection Request
Connection Indicate
Here is my accept to connect and the options I have selected
Connection Confirm
Connection Response

TCP connection oriented 3-way handshake connect;

- If there is a time out it will not send the ACK in response
- Eliminates the timing problem


Node A
Node B
Connection Request/ Option Request (SYN)
Connection Indicate
Connection Confirm/ Option Confirm
Connection Response/ Option Request (SYN+ACK)
Option Response
Option Confirm (ACK)

TCP oriented, Simultaneous Disconnect;

- At the end of transmission(hang up), each one tells the other to "hang up"
- Node A tells Node B to disconnect and vice versa
- Disconnect request (FIN)
- Disconnect response (ACK)
- Half close – only 1 node disconnects

Finite state machines, state level programming;

- Connectionless, like a letter (Lect1a)
- No error control – don't know if it arrived or arrived with an error

Connection Oriented, Reliable data transfer;

- For every packet of data sent there will be an acknowledgement of that the data has been received
- Error protocol (NACK) – Negative ACKnowledgement
- When data is sent garbled
- The acknowledgement could become garbled
- Data therefor needs to be sent again

Error and loss;

- I expected an ACK within a certain time there was NO ACK so assume data was lost. Data sent again.

Stop-Start protocol;

- Send a packet
- Wait for ack

Window Protocol;

- Cannot wait for the ACK of each packet
- Send several packets and wait for ACK

TCP end to End flow control;

- Transmitter sends data
- When data arrives, it will be pushed to application

TCP persistence Timer;

- If I don't get information to update my status at Node A then send a message out to ask for an update

TCP End To End flow control – window protocol;

- E.g. a very chatty person who does not stop talking
- Route may become congested,
- No other nodes will get in
- Router gets overloaded

TCP congestion control;

- Want the system to support fair sharing of the bandwidth

Transmission Characteristics;

Ass the preferred load grows, the throughput drops.

- Slow start up to stop build-up of traffic
- If we send one packet and we wait for its ACK and we time how long that takes, we can get an estimate of the likely roundtrip delay that we are experiencing at that moment in time
- Will eventually become congested, so drop back down to number of packets before congestion

TCP congestion – choke packets;

- If a router determines a packet source is sending too many packets and its causing the buffer to become overloaded, it can send a choke packet to say "please slow down"

TCP frame requirements;

FRAME REQUIREMENTS	USES
SOURCE AND DESTINATION PORT NUMBERS	Multiplexing
SEQUENCE NUMBER FOR ACK	Outgoing data
ACK NUMBER	Incoming data
CURRENT RECEIVE WINDOW SIZE	Flow control
FLAGS FOR SYN, FIN AND ACK PACKETS	Connect and Disconnect
OTHER FLAGS?	Push complete frame
OPTIONS	Max segment size
HEADER LENGTH	Checksum – check for no errors

-

Application Characteristics;

- Reliable delivery – no packet loss
- Delay – can be tolerated, as long as reliability is not lost
- Timely delivery – Smooth playback

Data e.g. file transfer

Service e.g. Real time media

Session initiation protocol;

- Your name + email address – provides mechanisms for call setup (e.g.)

Real time media;

- Requires TCP type characteristics
- Needs UDP type behaviour
- New behaviours – timing of packet
- New type required – real time protocol

Multi-media types;

- Streaming, stored
    - Can overcome sove of the ups and downs in the traffic
- Conversation two-way
    - Cant have delay – leads to congestion issues
- Streaming live
    - Can tolerate some delay to allow buffering

Lecture 6; Presentation and Application layer and Session Layer

Application Layer;

- Closest to the user – where the user interacts with the network
- Interface between the applications and the underlying network
- The protocols enable us to exchange data between sources and destination hosts
- TCP/IP application layer includes the functions of the three upper layers of the OSI model

Presentation layer;

- Format data – in a way that they can be understood by different OS'
- Compress data
- Encrypt data – to have secure transport of data and files

Session Layer;

- Maintains dialogs between source and destination hosts – helps us to get back to where we left off in the conversation
- Initiate dialogs
- Keep them active
- Restart session when there is a disruption

TCP/IP application layer protocols;

- Specify the format and control information necessary for common internet functions
- Must be implemented in both source and destination hosts
- The source and destination implementation must be compatible

Application architectures;

- Client server
- P2P

Client server architecture;

- Server;
    - Always-on host
    - Permanent IP address
    - Data centres for scaling
- Clients;
    - Communicate with server
    - May be intermittently connected
    - May change IP addresses
    - Do not communicate with each other – only with the server

P2P architecture;

- Servers are not always on
- Systems communicate randomly
- Peers request service from other peers
- Hosts are both clients and servers
- Any time connection is made, you can have different IP addresses
- Complex management

Creating network applications;

- Write program that;
  - Runs on different end systems
  - Communicates over the network
  - No need to write software for the network – core devices
  - Network-core devices do not run user applications

Processes/application communicating;

- The same host can run more than one application
- When applications run on the same host, the OS takes care of the communication
- When they are on different hosts there is an exchange of messages

Sockets;

- Process sends/receives messages to/from socket
- Application layer communicates to underlying layers through sockets
- Socket is a door to send data
- Client process; process that initiates communication
- Server process' process that waits to be contacted

Addressing processes;

- Identify hosts
  - IP address
  - Port Number

Transport Services for apps;

- Data integrity;
  - some apps require 100% data, some can tolerate losses
- Timing;
  - Some applications can be delayed while others would not tolerate any sort of delay
- Throughput;
  - Bandwidth that we use
  - Some require min throughput to function – some more flexible
- Security;
  - Encrypt data to ensure secure data transfer

Internet Transport protocol Services;

- TCP service;
  - Reliable transport
  - Connection oriented
  - Flow control
  - Congestion control

  Does not provide;

  - Timing
  - Min throughput guarantee
  - Security

- UDP service;
  - Unreliable data transfer

  does not provide;

  - Reliability
  - Flow control
  - Congestion control
  - Timing
  - Throughput
  - Security
  - Connection setup

HTTP;

Uses TCP protocol

Non-persistent HTTP;

- One object sent over TCP connection

Persistent HTTP;

- Multiple object sent over TCP

Round trip time;

- Time for a small packet to travel from client to server and back

HTTP message;

- Request
- Response

GET	Requesting data
POST	Send data
HEAD	Ask server to not send requested data
PUT	Upload files
Delete	Delete files specified

Cookies;

Can be used for;

- Authorisation
- Shopping carts (holding personalised data)
- Recommendations
- State of session

FTP;

- Transfer file to/from remote host
- Client – initiates transfer
- Server: remote host

Email;

Three major components;

- User agents
- Mail servers
- Simple mail transfer protocol (SMTP)

User agent;

- Writing emails or receiving emails

Mail servers;

- Store all information/emails in mail-box
- Message queue – of outgoing mail messages
- SMTP
    - Client – sending mail server
    - Server – receive mail from other servers
- SMTP is built on TCP – must be reliable
- Generally on port 25

Phases of transfer;

1) Handshaking
2) Transfer of message
3) Closure

Scenario;

User agent -> personal server -> recipient server -> recipient agent

POP – post office protocol;

- Pulling all the mail out from your own mail server

IMAP – internet mail access protocol

Distributed Hashing – Hash Table;

- A data structure where you have key value pairs – use hash keys to perform operations
- Any peer can query database with a key
- Database returns value for the key
- Peer churn – peers can leave and join the network
- Circular DHT – Distributed Hash Table
    - Each peer is only aware of immediate successor and predecessor
- Handling peer churn;
    - Each peer constantly checks its two successors to check ‘aliveness’
    - If successor leaves then peer automatically selects next in line

Resolving a Query;

What is the min number of hops (if a node goes out and subsequent nodes simultaneously)?

- Each node stores a global index table – keep track of entire network
    - (this is expensive to maintain and inefficient in terms of space)
- Each node stores neighbour’s indexes
    - Minimum maintenance cost takes time and many hops

Patsy algorithm;

- Routing table will be much smaller
- Tries to match the first element then the next etc etc

Lecture 7; Security

What is network security?

- Confidentiality
    - only sender and intended receiver should “understand” message contents
- Authentication
    - Sender and receiver want to confirm identity of each other
- Message integrity
    - Sender and receiver want to make sure message is not altered
- Access and availability
    - Services must be accessible and available to users

What bad things can an intruder do?

- Eavesdrop – intercept messages
- Insert messages
- Impersonation
- Hijacking
- Denial of service

Cryptography;

‘languages’;

- Plain text – un-ecrypted messages that anyone can see
- Cipher text – scrambled up and unreadable
- Substitution cipher – substituting one thing for another
- Permutation cipher – change the order of the input text

How strong are these encryption methods?

- Cipher-text only attack
    - Brute force
    - Statistical analysis
- Known-plaintext attack
    - Know what original message was
- Chosen plain text attack
    - Can request ciphertext for chosen plain text

Symmetric key cryptography;

- The idea that you have one key that you would use to encrypt and decrypt your data
- You need to decide on a key beforehand

DES – Data encryption standard

- Builds on substitution and permutation cipher that we have already seen
- 56-bit symmetric key
- 64-bit plaintext input
- Block cipher with block chaining

How secure?

- Some people can discover the key in 25 seconds
- No good analytic attack yet known

Making DES more secure;

- Use 2 DES keys – K1 and K2
- In order to gain backwards compatibility $E(K_1, D(K_2, E(K_1, m)))$

AES – Advanced Encryption Standard

- Symmetric key algorithm

Public Key Crypto;

- Symmetric key – need to know key before hand
- Public key -2 keys private (only known to receiver) and public

Requirements;

- ○ Need K_B and L_B such that;

$$D(Lb, E(Kb, m)) = m$$

- ○ Given the public key $K_{b,}$ it should be impossible to compute private key L_b

Prerequisite: modular arithmetic;

$$(x\ mod\ n)^d\ modn = x^d mod\ n$$

Nonce-number used only once in a lifetime;

- To prove Alice is "alive", bob sends alice nonce, alice must return R, encrypted with a shared secret key

Security hole;

- Man in the middle attack – Trudy poses as alice to bob
- Difficult to detect

Digital signatures;

- Sender digitally sings particular document, establishes them as the owner
  - ○ Alice verifies that bob signed message m
  - ○ No one else signed m
  - ○ Bob signed m and not a modified message of m ('m')

Message digest;

- Apply the private key to the abstract of a message (much faster)
- Apply hash function to make this happen (many to 1)

Check sum is a poor crypto hash function

MD5 and SHA-1 - good hash function

Public key certification;

- Certification authorities – bob provides "proof of identity" to trusted third party

Secure email;

Must satisfy;

- Message has to be secret

- Message has to be signed by sender to receiver
- Message has to be addressed to right destination without it being tampered with

Public key encryption is slow, best way to encrypt message is private key (symmetric key encryption)

MITM attack;

- Change our messages
- Pretend they are part of the communication
- Stop the communication

SSL – secure socket layer – extra layer added in TCP/IP

- Industry standard

Provides;

- Confidentiality
- Integrity
- Authentication

PGP (pretty good privacy);

- Send emails
- Handshake is encrypted to confirm identity

SSL, 4 stages of communication;

1) Handshake – certify and exchange keys to encrypt data to be shared
2) Key derivation – derive more keys – don't use only 1 key
3) Data transfer – don't send all the data at once, it is broke up into a series of records
4) Connection closure – special message sent to securely close the connection

Handshake SSL;

- TCP handshake
- SSL handshake

MS (Master Secret)

- Used to generate symmetric keys for remainder of session

EMS – encrypted master secret

Key derivation; bad to use same key for more than one crypto operation

- Generate 4 keys using MS and some other data
  - K_c = encryption for data sent from client to server
  - M_C = MAC for data sent from client to server
  - K_S = encryption key for data sent from server to client
  - M_S = MAC key for data sent from server to client

Data records;

- Ssl breaks data into smaller records
- Each record carries a mac
- Receiver can act on each record as it arrive s

Close transaction;

- MTM can close transaction before it has ended

Solution;

- MAC (Mx, sequence type data)

SSL record protocol;

- Record header
  - Content type
  - Version
  - Length
- MAC
  - Sequence number
  - MAC key Mk
- Fragment
  - Each SSL fragment 2^14 bytes (^16k bytes)

WPA (wifi protected access)

- Improved security

CIA – confidentiality, integrity and authentication

what is network layer confidentiality?

- All data sent from one entity to another would be hidden
- Provides “blanket” coverage over the layer

VPN

- Orgs and institutes often want private networks for security
- VPNs help with;
  - Data integrity
  - Origin auth
  - Replay attack prevention
  - Confidentiality

Two IPsec Protocols;

- Authentication header (AH) protocol;
  - Provides source auth and data integrity but not confidentiality
- Encapsulation security protocol (ESP)
  - Provides CIA and is more widely used than AH

Security association;

- Database internally stored and it tells you who is who

IP sequence numbers;

- Goal – prevent attacker from sniffing and replaying a packet

Internet Key Exchange;

- Manual keying is impractical for VPN with many end points
- Internet key exchange is more dynamic
- Exchange for algos, secret keys, SPI numbers

IPsec peers can be 2 end systems, 2 routers/firewalls or a router/firewall and an end system

Firewalls;

- Let some packets in while blocking others
- Some packets could contain malware, sniffers etc
- Prevents DDOS attacks
- Prevents access of internal data
- Prevents illegal mods
- Only allows authorised access

3 types of firewalls;

1) Stateless packet filters
2) Stateful packet filters
3) Application gateways

Stateless packet filtering;

- We don't let every packet that exists enter network
- Accepts packets based on;
  - Source/destination IP
  - TCP/UDP source/destination port numbers
  - ICMP message types
  - TCP SYN and ACK bits

Access control list;

- Table of rules which packets must meet otherwise denial
- Stateless packet filtering
  - Heavy handed
  - More than what is required
- Stateful packet filter
  - (later)
- Look at packet to see if TCP connection has been set-up first before it accepts messages

Application gateway;

- Application program that runs on a firewall system for 2 nodes

Limitations of firewalls;

- Might block too much

Intrusion detection systems;

- Looks at packet contents and examines correlation among multiple packets
  - Port scanning
  - Network mapping
  - DOS attack

Lecture 8; Mobile Wireless

QOS – quality of service;

- There is not enough bandwidth to cope with all types of data
- Cannot give all data the same privileges
- Various applications will expect certain quality (video calls etc)

Issues;

- Sharing the same space but varying priorities

How to measure quality?

- Bandwidth
- Delay
- Jitter – difference in delays
- Acks
- Error rate
- Loss rate

Parameters for QOS;

- Peak cell rate – max rate of transmission
- Sustainable cell rate – average cell transmission rate
- Max burst size – max no of cells transmitted
- Min cell rate – min cells needed for functionality
- Cell-delay variation tolerance – error margin

QOS in networks

RSVP

- Reservation protocol
- If unused, others use it (bandwidth)

Lecture 9; Wireless Networks

Wireless hosts;

- Laptops
- Smartphones

Base station;

- Cell towers
- Access points

Wireless links;

- “wireless port”

Infrastructure mode;

- Base station connects moviles into wired network
- Hand off
    - Connection maintained when passing across 2 towers

Characteristics of wireless links

- Signal strength can decrease
- Interference
- Multipath propagation
    - Signals could bounce off other things which could alter its arrival time
- SNR – signal to noise ratio
- Hidden terminal problem (A cannot head C, means they are unaware of their interference at B – A and C both transmit to B, B has interference from the simultaneous comms)

Signal attenuation;

- Signal is being lost as you go further away

CDMA (code division multiple access)

- Unique code assigned to each user
- Orthogonal – codes that do not interfere with each other

Wi-Fi;

- Access point = router – this accesses the wider internet
- Host must associate itself with at access point
- Scans for beacon frames which are sent out by router
- Selects an AP

Passive scanning;

- Listen out for beacon frames
- Listen passively

Active scanning;

- Send out a request frame asking if there are any AP’s to connect to
- Probing “can I connect”

Avoiding collisions;

- Small requests to send packets sent in order to detect collision so that resources are not wasted within the packet being sent
- A clear to send (CTS) is sent in response to RTS (similar to reservations)

RTS and CTS are used to sync

Frame;

- Contains address
  - Like envelope to a letter
- Collision avoidance is built into the frame

802.11 – power management

Types of frames;

- Data frames (01)
- Control frames (10) – solve problems, clearing operations
- Management frames (00) – authentication between access points

Mobility within same subnet;

- As it moves, disassociates with one AP and associates with another AP which is stronger

Network security;

- Link layer – WEP/802.11 (WPA)
- Network layer – Ipsec
- Transport layer – SSL
- Application layer – PGP

WEP – wire equivalent privacy;

- Very weak
- Can be cracked by collecting initialisation vectors

WPA;

Security mechanisms which eliminate issues such as;

- Access control
- Authentication
- Authorisation
- Confidentiality
- Data integrity
- Key management
- Protection against known attacks