CS2005 Notes

Ashwin Notes Write Up

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

## Purpose of the Layers;

Link

Link

Network

Transport

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;

Network

App 1

App 2

App 3

Transport

n-layer

(n-1)-layer

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 Response

Node A

Node B

Connection Indicate

Connection Request

Connection Confirm

Data Request

Data Confirm

Data Indicate

Data Response

Connection Oriented

Connection

Response

Node A

Node B

Connection

Indicate

Connection Request

Connection

Confirm

Data

Request

Data

Indicate

Data

Request

Data

Indicate

Connection Oriented – unacknowledged

## Connectionless;

Node A

Node B

Data

Request

Data

Indicate

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

Connection Response/

Option Request (SYN/ACK)

Node A

Node B

Connection Indicate

Connection Request/

Option Request (SYN)

Connection Confirm/

Option Confirm

Data Request

Data Confirm

Data Indicate

Data Response

Option Confirm (ACK)

Option Response

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

Disconnection

Response (FIN/ACK)

Node A

Node B

Disconnection Indicate

Disconnection

Request (FIN)

Disconnection

Confirm

Confirm (ACK)

Response

TCP connection-oriented; 3 way handshake Disconnect

## 

Lecture 3 – Physical and Link Layers;

## Network Topology;

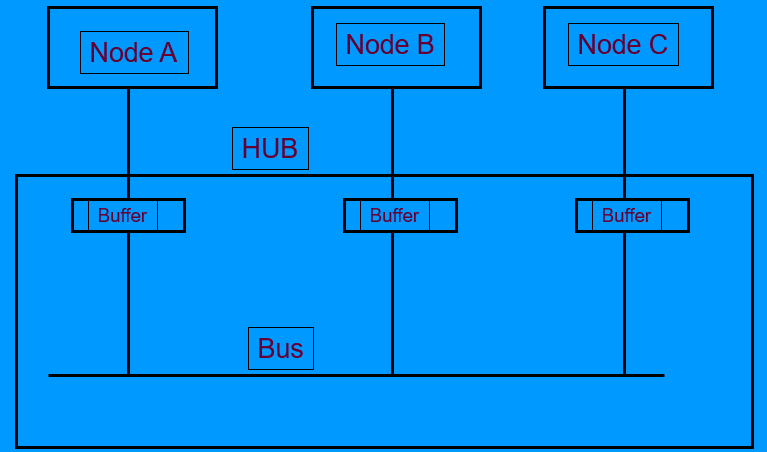
The way in which constituent parts are interrelated or arranged

* Bus
* Star ring
* P2P
* Wireless

## Bus – cable;

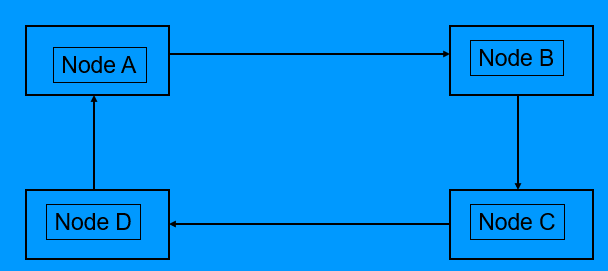
* Unreliable
* Error control is a long process – time consuming
* Only one node can transmit data at an given time – bandwidth restrictions

## 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



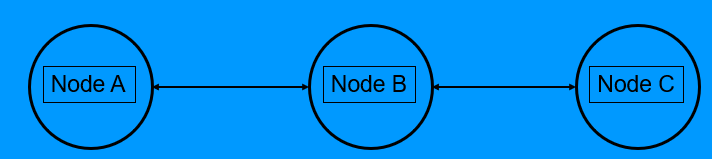
## Ring – Physical;

* 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;

Where is the duration  
Where is the propagation delay

### Propagation time;

Where is the propagation time  
Where is the length   
Where is the velocity

### Duration of the Frame size/transmit rate;

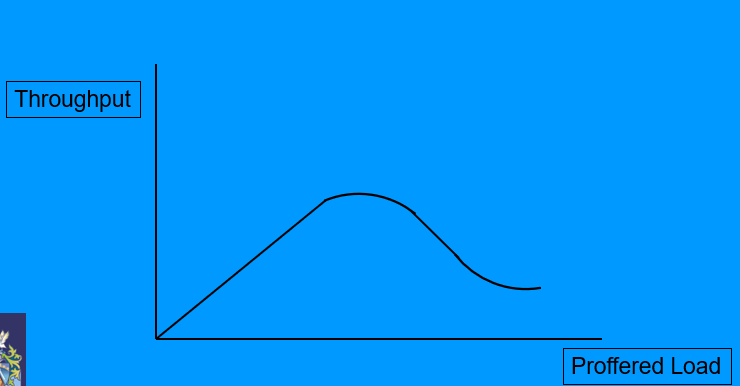
Where is the duration   
Where is the frame size  
Where is the transmission rate

### Frame Size;

Where is the frame size  
Where is the length   
Where is the transmission rate  
Where is the velocity

Example; Suppose

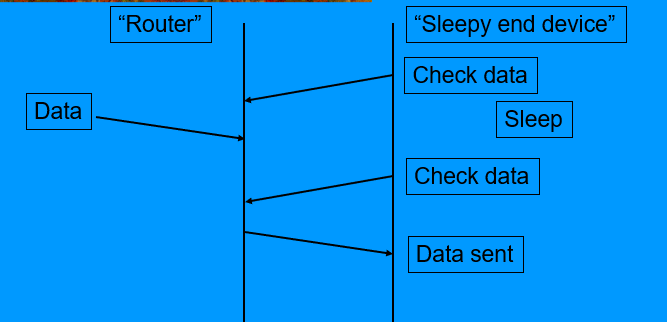
What Happens after a collision?

* 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
  + Repeat
  + Report error if fail after 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

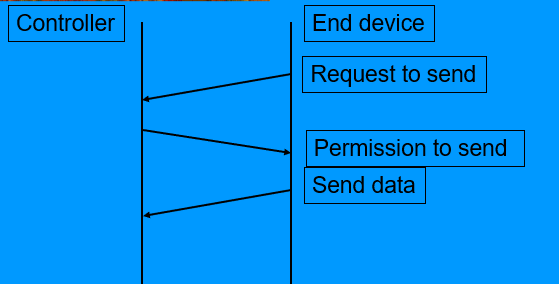
## “sleepy end device” protocol;



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 bits with bits added by generatior polynomial of
  + 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)

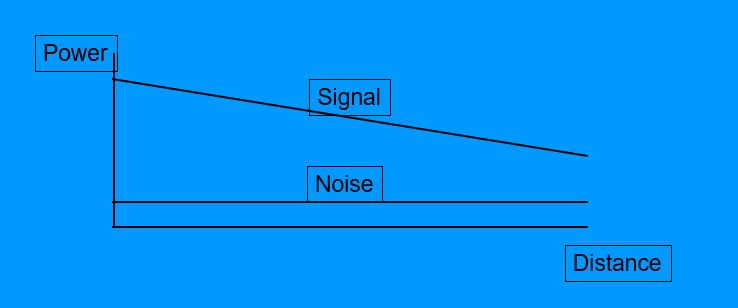
## Technology for Network connections;

* 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?

Link

Link

Network

Transport

* 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

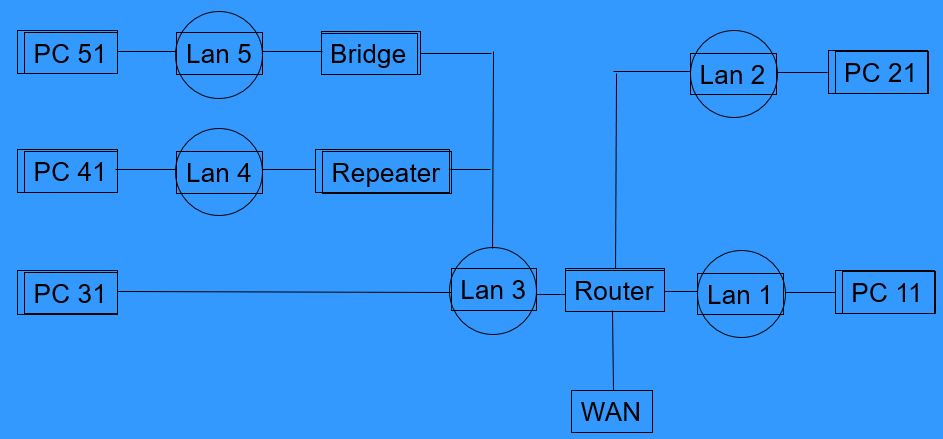
## Segmentation of physical networks;

* 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

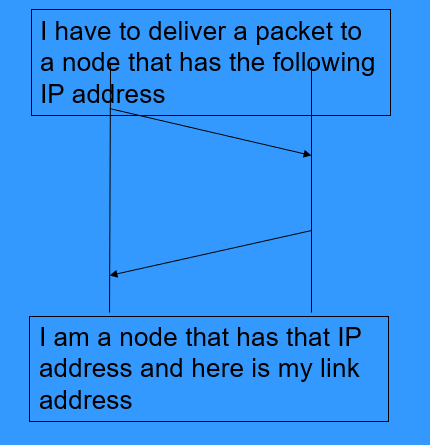
This indicates subnet masking

## 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

## 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](http://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

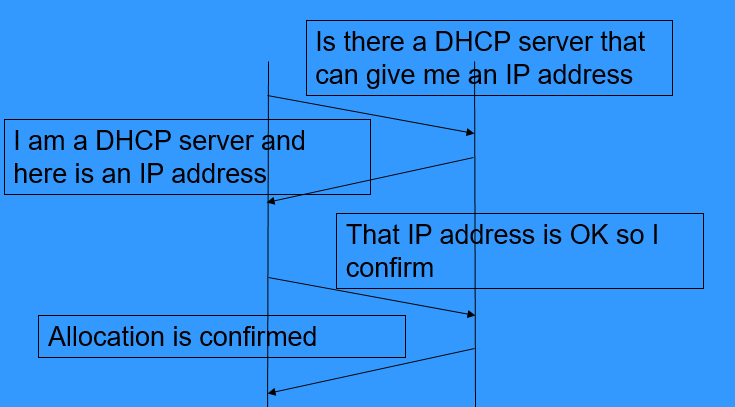
## ICMP;

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.

## 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?

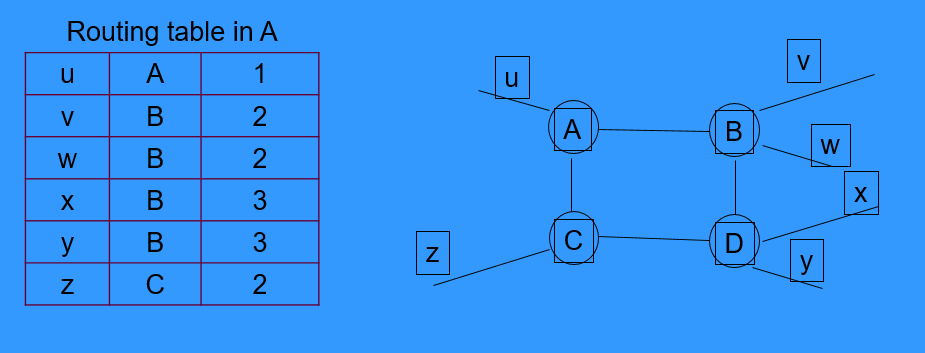
* Routing split into 2 domains
  + Interior gateway protocol (IGP)
  + Exterior gateway protocol (EGP)

## 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.)
* 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 infortiona, in-order to deliver any other organisation, there is a large number of class C