

Advanced Networks

Comp3010

1 Introductory Lecture

a) Structure

100% Examined

Directed reading on the course website

Past exams from 2007 onwards

Topics:

- Information theory and bandwidth
- Modulation and multiple access
- Error correcting codes
- Networking standards
- Applications

2 Information and Bandwidth

a) Bandwidth

Digital data measured in terms of bits

Bandwidth is the amount of data set in a given time

i.e. bits-per-second

Bandwidth has grown rapidly over the last few years

bit rate is similar to baud rate (symbols per second and there are only 2 symbols)

b) Compression

NEEDED!!!

Typical applications need vast amounts of bandwidth

Only way that mobile phones can receive calls, youtube can stream video etc...

c) Information Theory

Information theory developed by Claud Shannon

Information also measured in bits by Shannon (hence \log_2) but different symbol levels could be used (log base n)

different to data!

Information expresses meaning (semantics?) to the data received

d) Shannon Information

Degree of surprise

Considers a random discrete variable and asks how much information is received by observing the variable at a given value

$$h(x) = -\log_2(p(x))$$

$$h(x) = \log_2\left(\frac{1}{p(x)}\right)$$

i.e. if we expect a value (high $p(x)$) then less information is gained if we observe it

If we learn two independent facts then information is additive

$$p(x, y) = p(x)p(y)$$

$$h(x, y) = h(x) + h(y)$$

example:

Encoding numbers using the higher or lower game

choose a number between 0 and 63

play by asking the question *is n higher or lower than x*

the most efficient way of doing this is to divide the search space in half

$\text{ceil}(\log_2(63)) = 6$ so 6 questions needed to find the answer

Each question has a probability of $\frac{1}{2}$ of being true (as we divide search space in half)

This means that the answer for each question can be represented by 1 bit $1 = -\log_2(1/2)$

For the whole number to be encoded we needed 6 bits due to $h(x, y) = h(x) + h(y)$

e) Shannon Entropy

Suppose a sender wants to transmit the value of a random variable to a receiver

The average amount of information transmitted is given by:

$$H(X) = -\sum_{i=0}^n p(x_i) \log_2(p(x_i))$$

Points to the lower bound on the average number of bits to be transmitted which in non-uniform cases could point to where compression could be used

$$\text{AverageBits}(X) = \sum_{i=0}^n p(x_i) \times \text{CodeLength}(x_i)$$

example

Consider a random variable x which has 8 equally likely values

$$H(x) = -\sum_{i=0}^8 \frac{1}{8} \log_2 \frac{1}{8} = 3 \text{ bits}$$

This makes sense as 3 bits are used to encode 8 binary states

example2

if there are non-uniform probabilities for the states, compression can be brought into play

Consider that x can take the following values with probabilities

$$\{(a, \frac{1}{2}), (b, \frac{1}{4}), (c, \frac{1}{8}), (d, \frac{1}{16}), (e, \frac{1}{64}), (f, \frac{1}{64}), (g, \frac{1}{64}), (h, \frac{1}{64})\}$$

$$H(x) = \frac{-1}{2} \log_2 \frac{1}{2} - \frac{1}{4} \log_2 \frac{1}{4} - \frac{1}{8} \log_2 \frac{1}{8} \dots = 2 \text{ bits}$$

So despite having more states, compression is achieved

f) Noiseless Coding Theorem

Shannon 1948

States that Entropy is the lower bound on the number of bits needed to transmit the state of a random variable without losing any information

Uniform probability case is always an upper bound on this lower bound

3 Modulation and Multiple Access

a) Modulation

Transmitting a digital signal down a wire is in theory trivial

However, for radio signals it's not the same (or for long links)

One must take a signal (at a set frequency) and modulate it to add information

We can change:

- amplitude

- frequency

- phase

When applied to digital signals it's generally referred to as shift keying

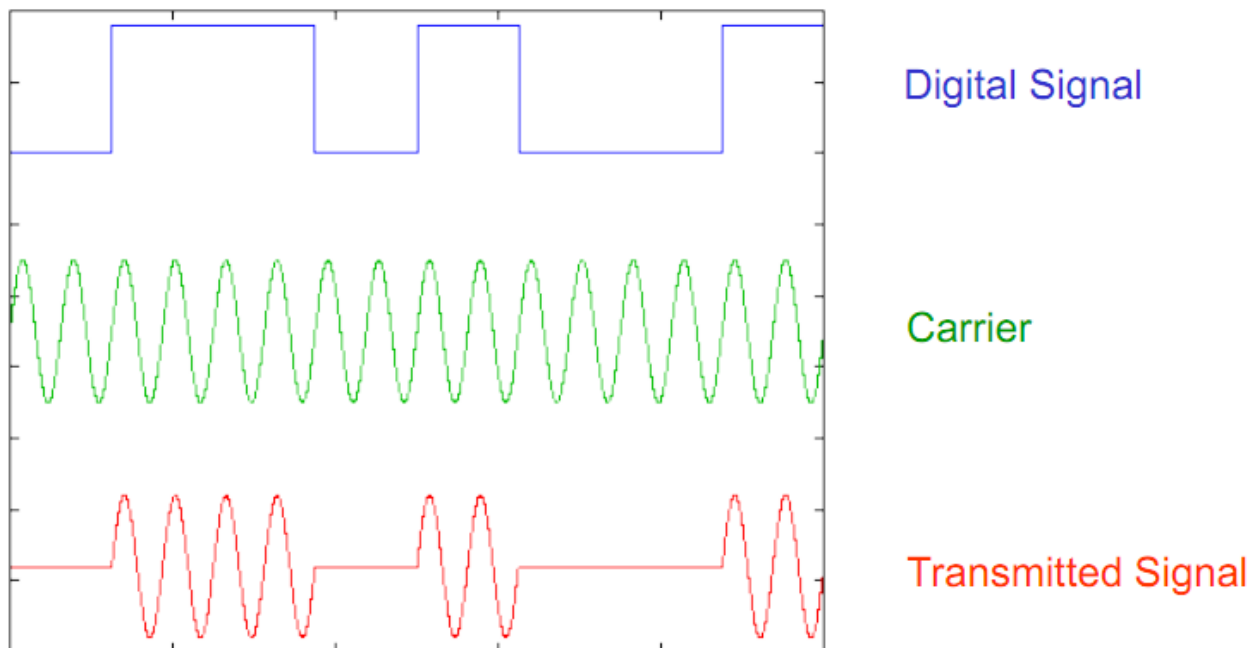
b) Amplitude Modulation

Modulate the amplitude of the output signal to represent digital levels

Encoding known as Amplitude Shift Keying (ASK)

Easy to do (simple electronics)

Very open to interference which could be disastrous for a digital system

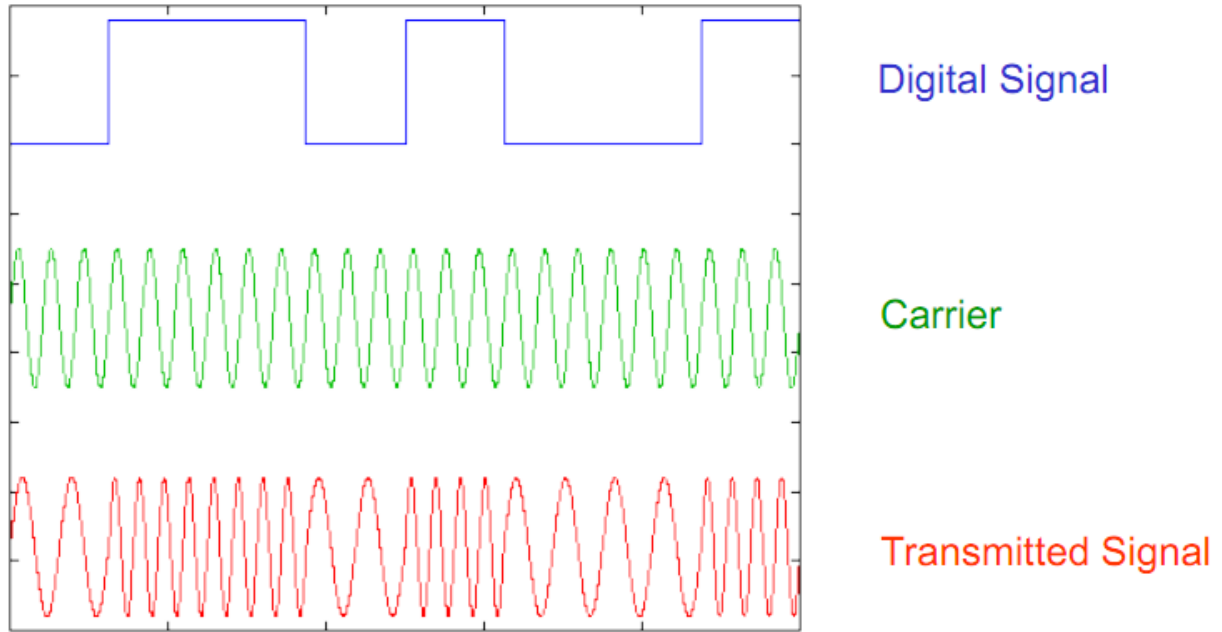


c) Frequency Modulation

Different frequencies for different digital levels

Encoding known as Frequency Shift Keying (FSK)

Used by Weather Fax



d) Phase-shift Modulation

Phase Shift Keying (PSK)

Different signal phases used to represent digital levels

For example:

0 – 0 degrees shift

1 – 180 degrees shift

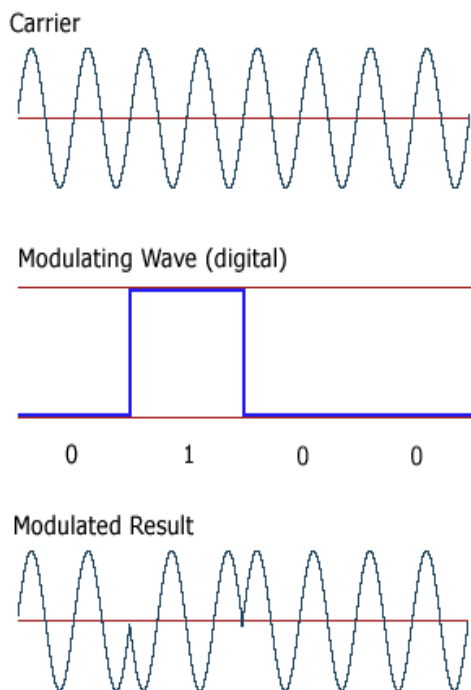


Illustration 1: Example showing PSK

Very hard for anything in the atmosphere (or environment) to interfere with the signal

so good for dealing with noise!!

But requires very complex electronics to make it work

Can encode multiple bit levels by shifting by different quantities

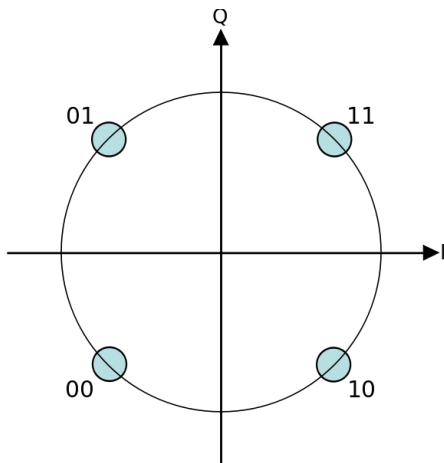
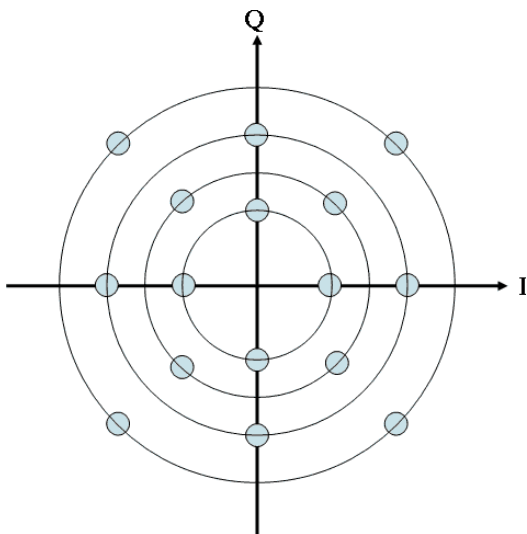


Illustration 2: QPSK - i.e. 4 levels implying 2 bits can be transmitted at once

e) Quadrature Amplitude Modulation

Can combine QPSK with Amplitude Modulation over short distances to transmit 4 bits at once



f) Radio Spectrum

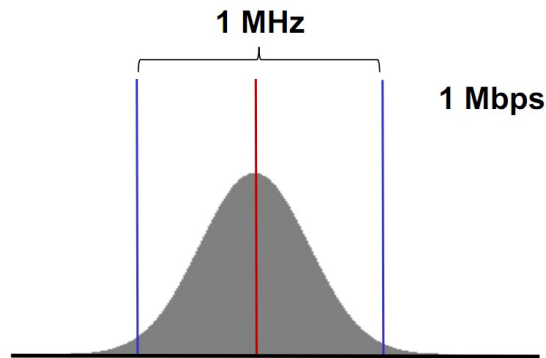
Range of frequencies for radio signals

Divided up into bands which have been given different uses

This is because energy from signals can overlap each other when they are modulated so they need a given bandwidth from the radio spectrum

The more a given signal is modulated the more energy is dissipated over neighbouring frequencies

If you wish to transmit 1Mbps then a 1Mhz wide part of the spectrum is needed to be used



g) Multiple Access

Now that users are tuned into the right frequency and not interfering with other devices...

Have to work out how multiple users can communicate together

3 different schemes which in theory give the same data rate each but in practice only 1 is good

h) FDMA

Frequency division

Take the allocated spectrum and divide into channels

Assign different uses for different channels and perhaps for different users

i.e.:

- channel 1 : outbound from base station
- channel 2 : inbound from r1
- channel 3 : inbound from r2
- ...

Limiting number of channels and requires space around channels so bandwidth not fully used

Bandwidth wasted when channels not used

i) TDMA

Time-based multiplexing

Each user takes it in turn to send data over the radio

Each user gets a set amount of time to send their data

Requires very accurate clocks and gaps between transmission times to allow for overlap

Used in early mobile phones GSM

j) CDMA

Uses codes for each user and each bit level from each user

Codes are orthogonal

Each user sends their code (1bit x number of users) all at the same time

Decode by multiplying the received summed code by each users code to get their message

Used in 3G mobile phone communications

(see slides)

Codes represent a Walsh matrix with an $N \times N$ matrix encoding N different users

4 Forward Error Correction

a) What and Why

Sending data over wireless links is prone to error

This can often be detected via cyclic redundancy checks (CRC) and retransmission requested

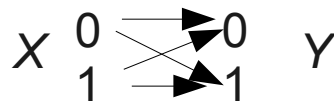
This can be rather inefficient though

In many cases it is better to try and reduce the errors in the first place (especially in larger systems)

b) Bit Error Ratio

BER

Gives the probability that a bit will be received in correctly



$$P(y=0|x=0)=P(y=1|x=1)=1-f$$

$$P(y=1|x=0)=P(y=0|x=1)=f$$

Where f is the BEF rate

This can be generalised over a word by considering different output combinations and their probability. K is length of the word and n is the number of correct bits

$$P(n \text{ correct bits}) = \binom{K}{n} f^{k-n} (1-f)^n$$

$$P(n \text{ error bits}) = \binom{K}{n} f^n (1-f)^{k-n}$$

where $\binom{K}{n}$ is the combinational operator

c) Repetition Codes

Simplest way to reduce errors though adding redundancy through repetition

Concept:

- take each bit and send it n times
- at the receiving end take the majority vote between the received bits to get the value

The thinking is that the probability of extra bits flipping is less than the probability of 1 bit flipping

Because it takes the majority vote, up to $\lfloor \frac{n}{2} \rfloor$ errors can occur but bandwidth reduced by a factor of n

$$P(\text{Success}) = P(0 \text{ err}) + P(1 \text{ err}) + \dots + P(\lfloor \frac{n}{2} \rfloor \text{ err})$$

d) Block Codes

Take a block of K bits and transmit N bits with $N > K$ to add redundancy

In a linear block code the extra bits are a linear function of the original K bits

Called parity check bits

This can be used to recover data from small errors

e) Hamming Code

For every 4 bits transmit 7 bits (7, 4) coding

Hamming codes specified usually in a lookup table but have mathematical background

Can correctly decode if there are 0 or 1 errors without having to ask for the data again (2 errors will cause the correction code to appear correct most of the time)

Bandwidth only reduced to $\frac{4}{7}$ of what it was (better than Repetition Codes)

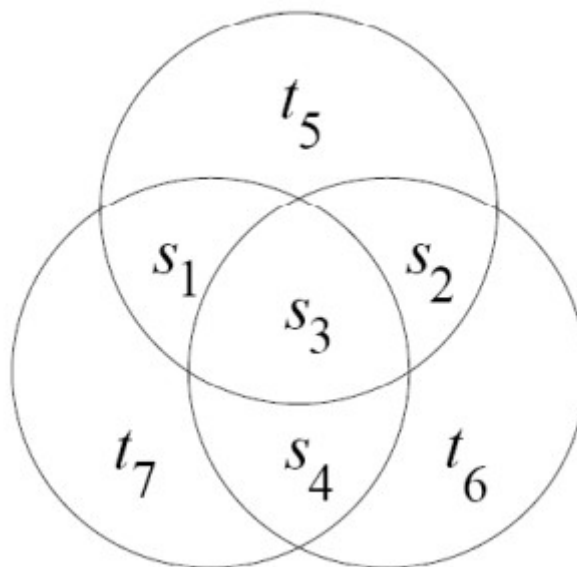
Whole family of BCH coding working on this principle, some allow for more errors by having a bigger code

f) Encoding

initial block is s_1, s_2, s_3, s_4

sent block is $s_1, s_2, s_3, s_4, t_5, t_6, t_7$

t 's act as parity checks for combinations of 3 input bits and themselves



if t_5 is high then (s_1, s_2, s_3, t_5) has 0 or 2 high bits in it i.e. 2 of s_1, s_2 and s_3 are 0

Decode through using logic

g) Noisy-Channel Coding Theorem

The capacity of a channel is the maximum rate at which communication is possible with an arbitrarily small probability of error

$$C(f) = 1 - H(f) = 1 - \left[f \log_2 \frac{1}{f} + (1-f) \log_2 \frac{1}{1-f} \right] \quad \text{where } f \text{ is the BER}$$

5 Bluetooth

a) Introduction

Short range radio method for wireless communications

Low power

Can cope with data transfer (which requires a lot of error correction) and faster data transfer (i.e. voice communication)

Multiple Access

Open specification aimed as a replacement for cables between small mobile devices

Agreed standard between large mobile phone manufacturers

Royalty free

Available anywhere in the world it uses an unlicensed (though regulated) part of the EM spectrum

The 2.4Ghz band

Low data rates (~1Mbps)

Designed to replace cables between small mobile devices

b) 2.4 Ghz Band

Unlicensed as its not really wanted

is regulated though

Same frequency as water vibrates at so a lot of interference will be received if this is done over a long range

this band suffers from lots of interference which must be anticipated and appropriately handled

Lots of short range devices uses this frequency which can cause a lot of interference:

- bluetooth
- wifi

And also gets interference from microwave ovens

c) Bluetooth Radio

Divides the 2.4GHz band into 79 channels each with 1Mhz width allowing for 1Mps transfer rate

Uses Phase Shift Keying as its modulation technique

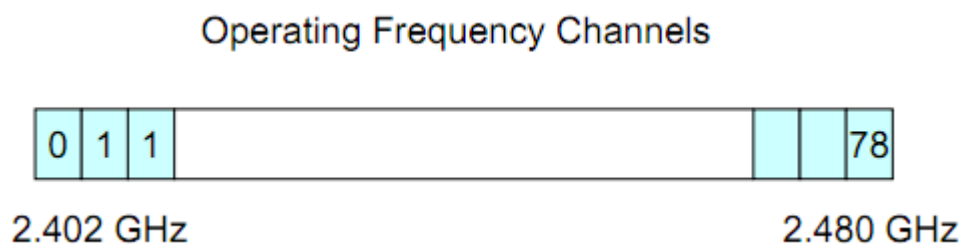


Illustration 3: Bluetooth band

d) Frequency Hopping

To reduce interference transmissions frequently hop between channels (1600 times per second)

Spreads out power dissipation more evenly over the band in order to reduce interference with other devices

Increased security (as hijacking devices will have to know the hopping pattern to get all the data)

Pseudo random sequence of channels is used and devices must agree on where to start in this

sequence in order to stay in sync. It appears random to outside observers but isn't random
the agreement is done in a setup linking phase

e) Master and Slave

One device is chosen to be the master and controls the frequency hopping pattern and packet timing between different devices it is talking to

These devices are known as slaves

Master can communicate with 7 slaves but can 'park' 255 more

No Slaves can directly communicate with other slaves

forming a star network with master at the center

Slaves can (in the protocol) connect to multiple masters although this isn't used much

No difference in the hardware between slaves and masters

f) Time Division Multiple Access

The master can setup the timing in order to communicate with multiple devices by sending/receiving multiple packets in a frame (1, 3 or 5 at a time) and setting when (in time) the next burst takes place

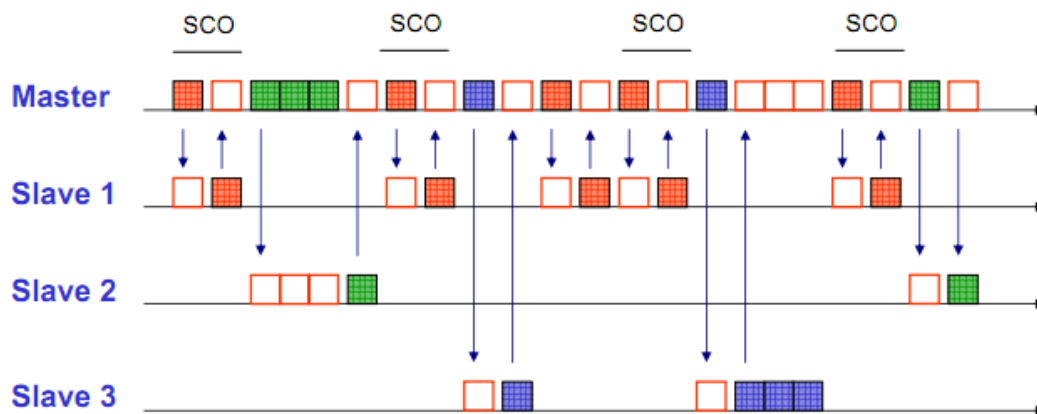


Illustration 4: example of multiple access on bluetooth

Each packet takes $625 \mu s$ to transmit

g) Frametypes and protocols

Bluetooth supports many different 'protocols' but the two main ones are SCO and ACL

SCO: Synchronous Connection Orientated

Real time data

Fixed slot duration

Slots reserved

No retransmission

Uses for things such as voice communication which interference isn't an issue. Like UDP in internet protocols

ACL : Asynchronous Connectionless Link

A bit like TCP in internet protocols

Packet switched data

Error correction using (15,10) hamming codes

can detect and fix 1 error

can detect 2 errors

Retransmission of failed frames

Used for data transfer and situations which require the correct information to be received

Adds extra overhead though

h) Future

Bluetooth 2.0 and 2.1

- data rates up to 2.1 Mbps

- lower power consumption

- improved pairing for greater security

Bluetooth 3.0

- ultra wide band technology

- claims 480 Mbps

- uses wifi to do the main data send

6 Wifi

a) Standard

IEEE 802.11 standards group

Typically 802.11g used now though 802.11n is the latest standard

Uses the 2.4Ghz band although 'n' uses 5Ghz aswell

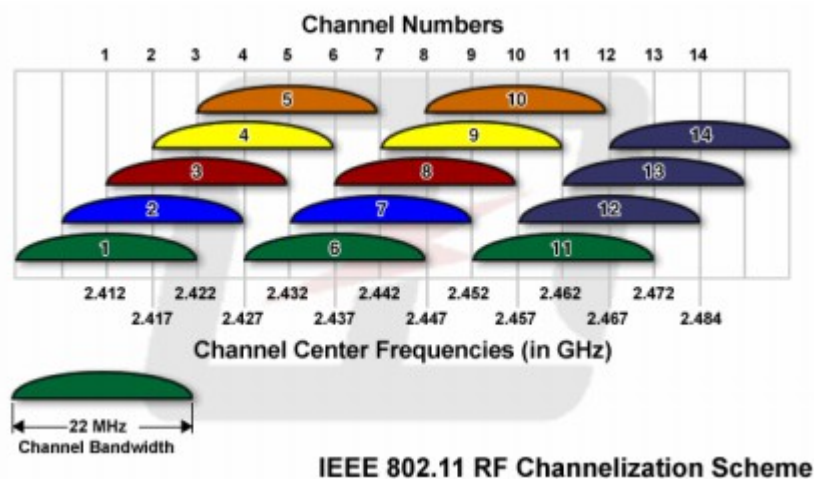
b) Band

Spectrum divided into 14 22Mhz channels

Only one used at a time by each router

They all overlap a bit (see diagram)

Some channels are blocked in some countries



c) Multiple Access

Uses collision avoidance

Essentially a reproduction of ethernet over wireless where the channel replaces the wire

Can get quite congested (just like ethernet again)

d) Connection Modes

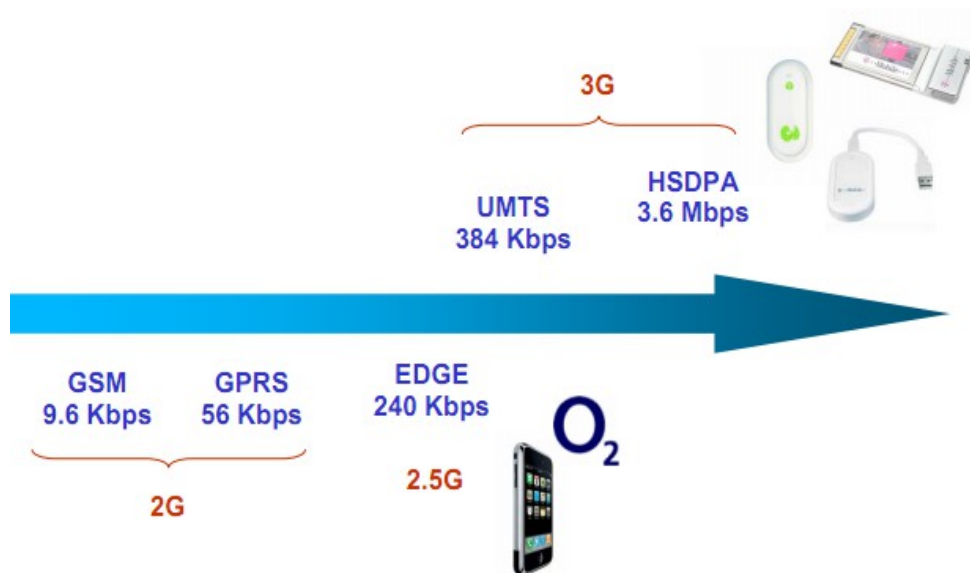
More adhoc than bluetooth

Client-server architecture

Allows for roaming between access points

7 WWAN

a) Mobile Phone Spectrum



Doesn't use 2.4Ghz range as its a long range protocol but this requires licensing

Use of mobile phone spectrum regulated and licensed

Government decided to auction off 3G licences in 2000 for £22.5Billion

HSDPA is the other 3G Protocol

UMTS : Universal Mobile Telecommunications Systems

HSDPA : High-Speed Downlink Packet Access

b) UMTS

Use QPSK for modulation

CDMA to allow for multiple access

requires every phone to have a unique chip code to identify it

High Power and long range

10-50km range

1 Watt power usage

~250min continuous talk time on a typical battery

8 Wireless Sensor Networks

a) Multi-Hop routing

Wireless Sensors are typically small and have a low battery power

Efforts need to be made to reduce power consumption

Transmission of data uses power

- more data more power used
- higher frequency more power used
- longer distances more power used

So for sensor to get its data back to the basestation it might be better to use other sensors along the way

This is known as multi-hop routing

A node requires E_{elec} to transmit 1 bit (the power to send and receive bits is the power needed by the circuits) and E_{amp} which is the power of the amplifier per m^2 distance

Power to transmit k bits over d meters in one hop

$$E_{single}(k, d) = kE_{elec} + kd^2 E_{amp}$$

Power to transmit k bits over d meters in n hops

$$E_{multi}(k, d) = n(kE_{elec} + k(\frac{d}{n})^2 E_{amp}) + (n-1)kE_{elec}$$

If $E_{multi} < E_{single}$ then its better to use multi-hop routing.

9 Mobile IPv6

a) Host Mobility

Host moves from one WLAN hotspot to another with a different IP subnet

address valid in previous subnet is no longer valid/reachable

likely to break persistent connection applications i.e. SSH

Other hosts can not reach the nomadic device by its original address

b) Mobile IPv6

Is standards for Ipv4 but work has stopped on them

2 Key functions:

to keep a persistent connection when moving between different wireless subnets i.e. when someone is walking across a campus

to be addressable via a single globally reachable IP address when away from “home” network

Implementation: mipl for linux

c) Dynamic DNS

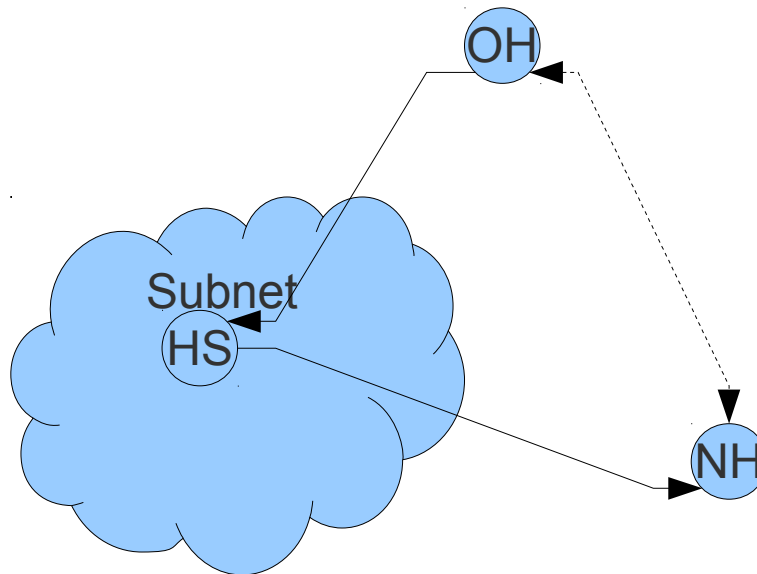
An alternative where a name is constant by the IP it points to is updated

Requires authentication

Fairly commonly used

Can be slow to update DNS registries

d) Schema



HS – a forwarding device typically a router which handles mobility

NH – the nomadic/moving host

OH – outside host trying to communicate with NH

HS a record of the location of NH globally. If they are in the same subnet then everything is fine and the router forwards the request as a normal router would. However, if NH moves to a different subnet it sends a message to HS with its new IP. From then on HS forwards all requests for NH to its new IP (proxy?). This is only the send path as NH can reply directly to OH although care must be taken around IP spoofing. If OH is an MIPv6 enabled device it can learn the 'real' IP of NH and then use this to communicate directly with it as this will be faster than routing through another node which might be sub optimal.

10 Ipv4 to Ipv6 Transition

a) Why Ipv6

No more Ipv4 space

To enable end-to-end global addressing and to reduce the need for NAT

Securing Ipv6 in your own network so you can manage it

To enable new research and products

b) Image of address exhaustion

Pressure on organisations to return address space which they do not use

Trading and leasing on Ipv4 address space

More complex network management

Routing tables becoming larger as address blocks become disjoint

ISPs using Carrier Grade NAT so users have a NAT within a NAT

c) Ipv6 deployments

Academic networks have support

ISP take up is low

Uptake by end users is low

Google and Facebook moving to support Ipv6 access of their services

Ipv6 used more on internal networking than for global access

d) Deployment approaches

If there is no existing infrastructure or need for Ipv4 then its trivial

Initially enable Ipv6 capacity on existing Ipv4 infrastructure

- run both protocols in dual stack mode giving users the choice of what to use

- can enable infrastructure before hosts/apps need to upgrade

initially may create ipv6 clouds which need to be connected

- requires tunnelling through Ipv4 networks

- ipv6 packets encapsulated in ipv4 packets

requires routers which know how to unpack these packets correctly in order to interface between ipv4 and ipv6 traffic

- may require ipv4 packets to be encapsulated in ipv6 packets aswell

e) Dual Stack

Gives host the choice of what to use as both methods are accepted

i.e. DNS returns Ipv4 and Ipv6 address then user can choose what to use

Must be confident that Ipv6 connectivity is good otherwise things won't work

f) Tunnelling

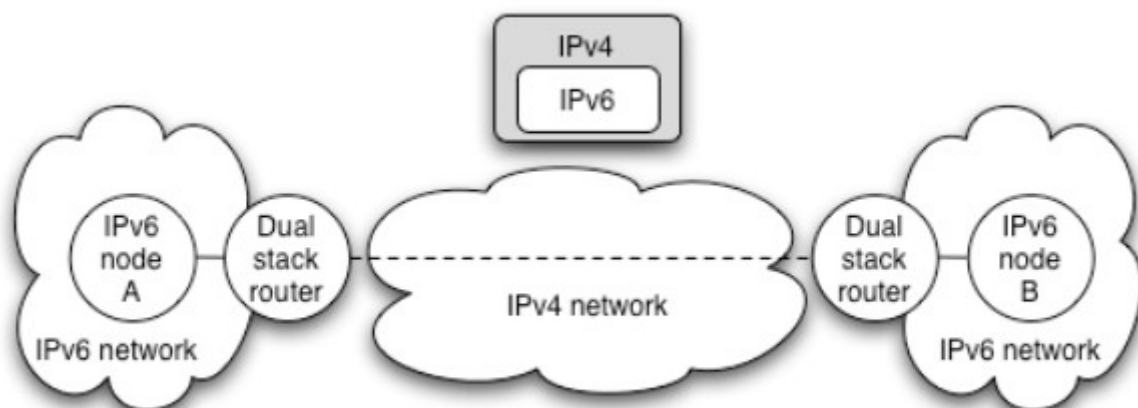
Want to connect Ipv6 islands in an Ipv4 sea

Use tunnelling to achieve this

Tunnels might need to be router to router (site to site) or host to router (host to site)

Can be setup manually or automatically

May at latency



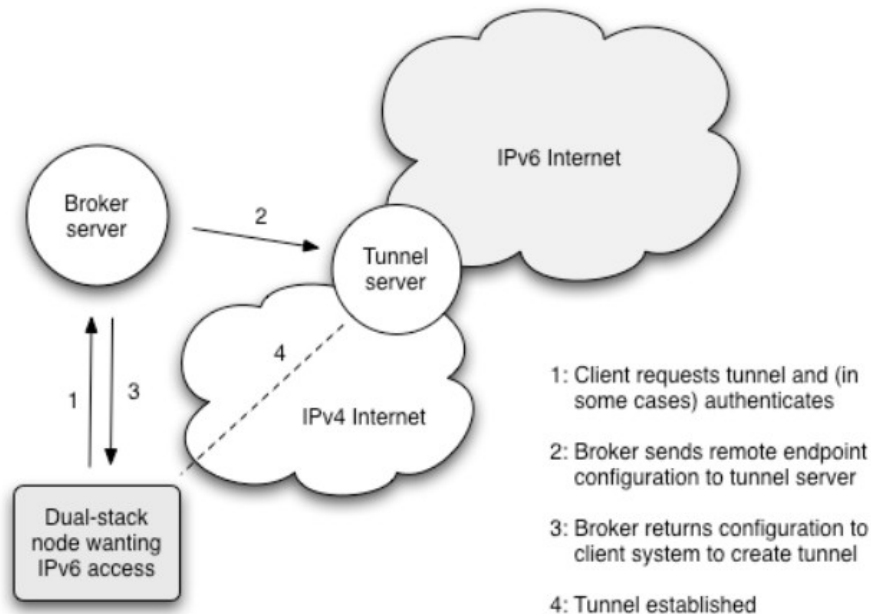
g) Tunnel Setup

Done with a Tunnel broker system

Users register and authenticate to request a tunnel with a central broker

Broker then sends details of the tunnel server to the user and registers their settings on the tunnel server

User then access Ipv6 services in dual stack mode by using the tunnel server as their Ipv6 router through tunnelling to it over the Ipv4 network



Alternatively this can be provided by an ISP directly

Broker issues:

- ISPs can't track Ipv6 usage levels

- round trip times may suffer if topology is bad

- traffic concentrated through tunnel servers → overloading

- may not be suited if ipv4 address is dynamic

h) Automatic Tunnelling

Goal is to avoid requiring support staff to setup and maintain tunnels

Can make tunnels on demand

Simpler for end users

The most common method used is 6to4

- router-to-router

- well supported commercially

i) 6to4

In its simplest mode its used to connect 2 Ipv6 islands over an Ipv4 network

Trick is to use a special 2002::/16 Ipv6 prefix that is reserved for 6to4 use only

the next 32 bits of the 6to4 address are the 32 bits if the Ipv4 router at the edge of the network

When a 6to4 router sees a packet with destination prefix 2002::/16 which isn't in its network it knows to tunnel is over Ipv4 to the address indicated by the next 32 bits

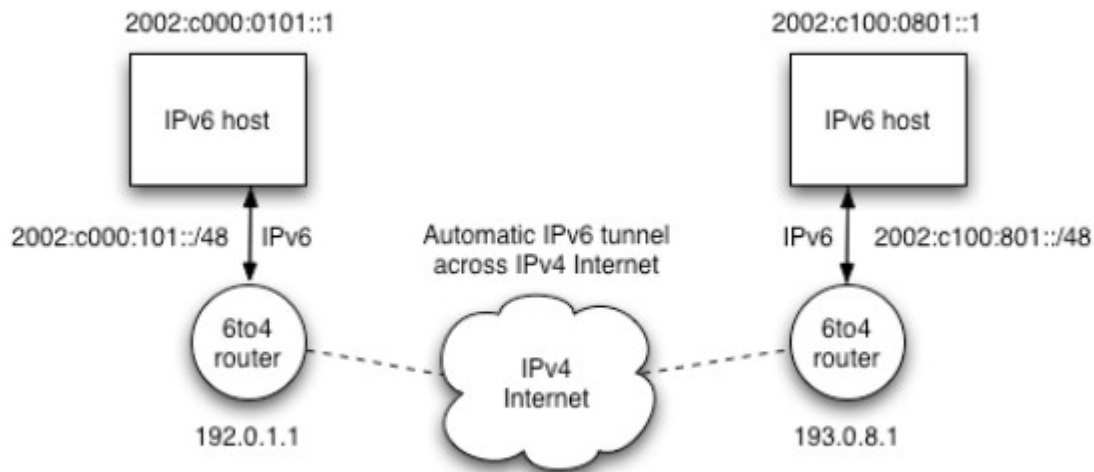


Illustration 5: 6to4 schema

Advantages

- simple to deploy and use
- automatic with no admin effort to put in
- tunnelled packets automatically route efficiently over Ipv4 to correct destination

Disadvantages

How does a node on a 6to4 site communicate with an Ipv6 node on a regular real Ipv6 site?

j) 6to4 Relay

A 6to4 Relay solves the problem of 6to4 networks communicating with non-sixto4 networks

Its a dual-stack router with a 6to4 interface to a real Ipv6 interface

Ipv6 packets which are non 6to4 are tunnelled to the relay, decapusulated and then forwarded using the relays real Ipv6 interface

Ipv6 packets send from a real Ipv6 site towards an address in the 2002::/16 prefix are routed to the relay and then tunnelled to the destination site on 6to4

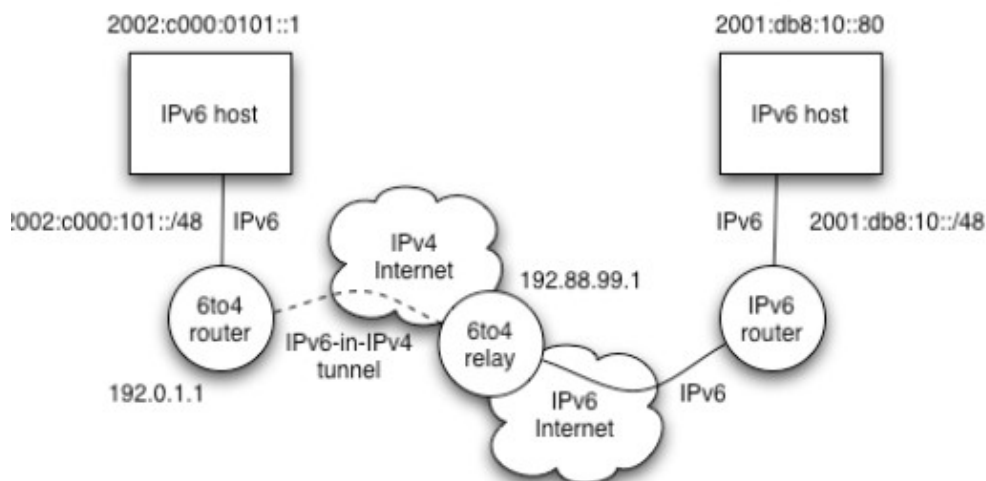
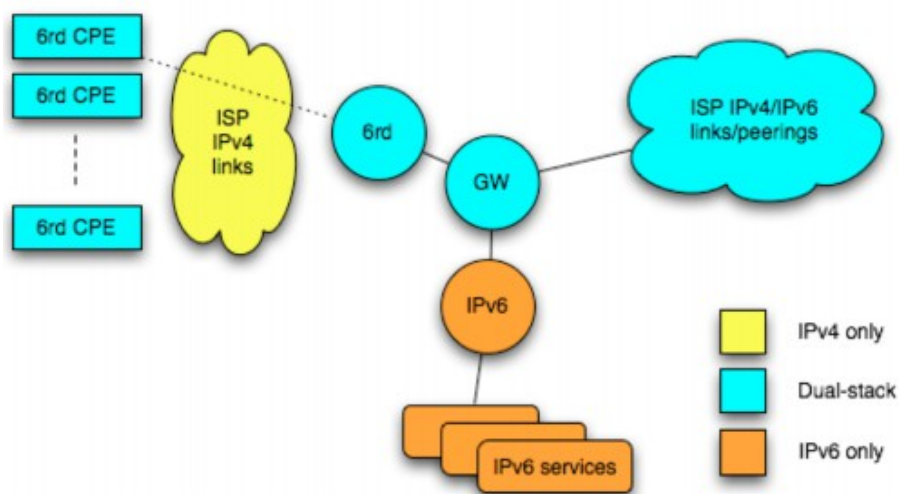


Illustration 6: 6to4 Relay schema

Relay needs to be discovered by the 6to4 router and by the Ipv6 router
 typically the any-cast address 192.88.99.1 address is reserved for relays on Ipv4
 Since Ipv6 only sites will use their nearest Relay to reply, it might become an asymmetric path
 Other problems:
 possible relay abuse for DoS attacks
 asymmetric model is hard to debug

k) 6rd

Variant of 6to4 used by free.fr ISP in France
 Works like 6to4 but ISP running 6rd uses its own regular prefix instead of 2002::/16
 Change ensures traffic from regular native Ipv6 sites is routed to the ISP's own networking
 Requires ISP support though



11 Ipv6 Trainisition and Coexistence with Ipv4

a) Ipv6 only scenarios

Large scale sensor networks : ipv4 space isn't available
 New application areas
 Ipv4 network changing to Ipv6 only : unlikely as this is a sudden change
 An existing dual-stack network may consider to drop Ipv4 support
 Some Ipv6 only devices may be introduced into a dual-stack network

b) Other scenarios

Ipv6 only network but with elements that might not be able to run Ipv6 for various reasons
 applications that can't be ported to ipv6 : old applications, source code not available etc..
 ipv4 only operating systems : i.e. win98
 ipv4 only hardware : some printers and internet TVs though might change

c) Translation

For an only Ipv4 only system to communicate with an Ipv6 only system some form of translation is required

Can be done at various layers:

- network : translation/mapping of fields in the IP headers
 - some headers don't have equivalents

- Transport layer

 - using a TCP dual stack relay to make intermediate requests

- application layer

 - use a dual-stack application layer gateway

d) Network Layer

Network Address Translation – Protocol Translation

- like Ipv4 NAT but for a change in protocol

Uses stateless IP/ICMP translation (SIIT)

- SIIT defines algorithms to translate between ipv4 and ipv6 where-ever possible

More for Ipv6 to Ipv4 translations rather than the other way around

- due to complexity

NAT-PT is dual stack on your network edge

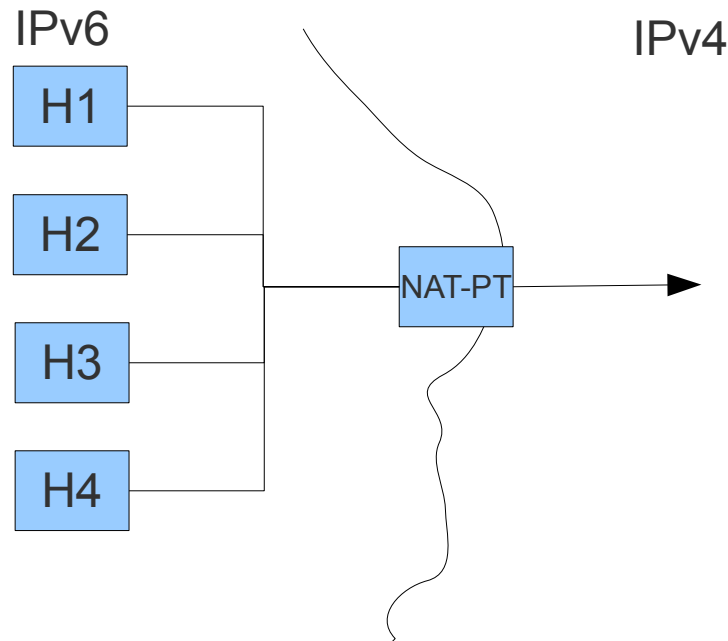


Illustration 7: IPv6 to IPv4 via NAT-PT

e) NAT-PT Downsides

Has all the short comings of Ipv4 NAT

- needs to hold state on the nat-pt box

Considered as a last resort mechanism

- deprecated

- new work on NAT64 and DNS64 with focus on Ipv6 only clients accessing ipv4 only services

f) Application Layer Gateways

ALGs

aka proxies

Simpler solution to NAT

Many applications support ALG already

- Web cache

- SMTP gateway

- DNS resolver

- irc service

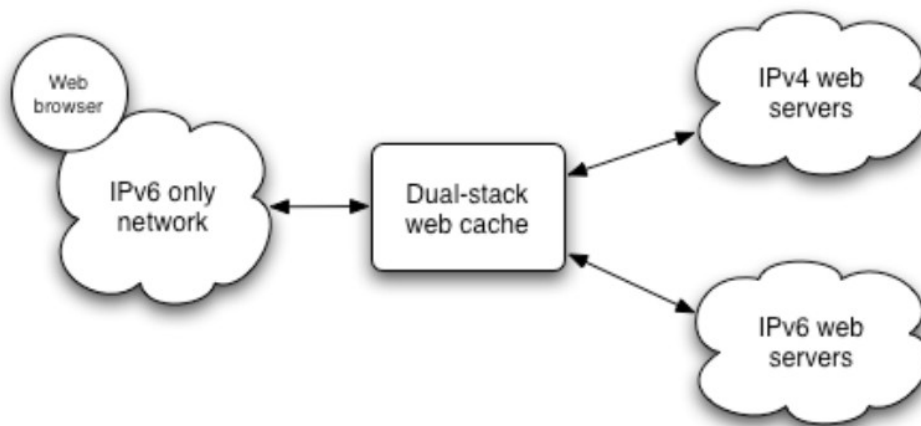


Illustration 8: ALG example

Simple and already in use

But requires client to use ALG configuration (but can already be set up) and only works for ALG supported applications

g) Conclusions

Lots of Ipv6 transition tools available but must be deployed on a site specific basis

Current best practice is for dual stacking

- incremental deployment

Ipv6 networks can be deployed but the key issue is how to link them to a mainly ipv4 internet

- i.e. NAT64

Needs to be done more readily now that ipv4 space is exhausted but space is still needed to assist with transition

12 Dynamic Host Autoconfiguration

a) What needs configuring

Addressing information:

- host address

- netmask (what's local)

- gateway (how to go further)

Naming system (DNS)

Other services like email, printers and proxies

b) Principles

Anything can be configured or misconfigured

Want to make things as simple and re-usable as possible

Keep simple and standardised to allow a full range of devices to use the network

Encourage interoperability, redundancy, low latency, conflict resolution and independence from lower layers

Limit the amount of traffic required

Auto-configuration *is not* access control : link and network access are different

c) Manual Configuration

Local configuration files store protocol bootstrap parameters

```
/etc/sysconfig/network
NETWORKING=yes
FORWARD_IPV4=false
HOSTNAME=orgs.ecs.soton.ac.uk
DOMAINNAME=ecs.soton.ac.uk
GATEWAY=152.78.191.254
GATEWAYDEV=eth0

/etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=152.78.191.129
NETMASK=255.255.255.128

/etc/resolv.conf
search ecs.soton.ac.uk
nameserver 152.78.70.1
```

Illustration 9: Example manuconfiguration settings from linux

This can work well for very small networks where the topology is static and understandable

Doesn't scale well to:

- large number of hosts
- nomadic hosts
- mobile hosts
- frequently changing network configurations
- service provider prone to change and thus require network renumbering
- home networks with white goods

Also not user friendly

d) Stateful Autoconfiguration

Requires somewhere to hold the state of the network

Administratively, centralising protocol configuration makes sense

- single point of administration
- site/enterprise-wide changes become trivial to deploy
- incidental benefits such as simplicity of adding a new node
- gives extra control

e) Hierarchy of Addresses

In a layered protocol stack (i.e. link-layer, IP, TCP) layers are configured starting from the lowest non-configured layer up through the stack

i.e. in Ethernet the MAC address is typically hard-coded into the device

A broadcast-enabled lower layer (i.e. Ethernet) removes the need to know the location of the

configuration service

but may have to deal with many replies if there are many configuration services

f) RARP

Reverse ARP

ARP is used for finding the MAC address for an IP address

It tries to find the IP address for a MAC address

Client broadcasts the RARP request to obtain an IP address

Waits (with timeouts and retries) for a response

Can then issue ICMP messages to acquire further configuration

subnet mask

default router location

This is basically obsolete now though

g) BOOTP

Bootstrap Protocol

Designed to be lightweight and to configure networking before loading a network-based operating system

Originally for diskless operating systems in the 1980s

Configures IP address and default router

BOOTP server has a list of these values for a set of MAC addresses that can join the network

Uses UDP-based protocol

Using IP to configure IP

Broadcast BOOTP Request

- Source IP address = 0.0.0.0 (unspecified)
- Target IP address = 255.255.255.255 (broadcast)
- Target UDP port = 67 (BOOTP server)
- MAC address used in source frame is the local NIC's, which the BOOTP server can look up in its database

BOOTP Response from server

- Send to UDP port 68 (BOOTP client), to one of the following:
 - Either: requester's intended IP address and actual MAC address
 - Or: broadcast IP address (all 1s on IP and MAC), relying on requestor's ability to detect unique transaction number

Illustration 10: Example BOOTP startup. NICs = network interface controllers

h) DHCP

Dynamic Host Configuration Protocol

An evolution of BOOTP to cater for more dynamic networks

Enables plug and play networking

DHCP Servers offer:

manually configured addresses for known NICs

Pool of address to be allocated as and when unknown NICs connect (dynamic)

Dynamic addresses may be given out once and then remain static or may be timed out to return to the pool after use

A client may request its old addresses again if it knows it

Allows for address leasing

DHCP-assigned addresses are not permanent but are given a validity or lease time

Short leases may not persist across reboots or may even need to be renewed whilst live

Could be competition for addresses and its up to the server to manage this

DHCP can also be used to configure more than just networking

Basically BOOTP packets are used with options on the end
subnet mask, gateway, time-server, DNS server etc...

DHCP Example Interaction

- Client looks for a server: *DHCP DISCOVER*
 - Source = 0.0.0.0 port 68
 - Destination = 255.255.255.255 port 67
 - May request an address (option 50)
- Server responds from own IP address: *DHCP OFFER*
 - Destination is proposed client IP + MAC address, port 68
 - Contains offered IP address (BOOTP compatible), plus *DHCP Options* for netmask, gateway, DNS server, and potentially others
- Client confirms it wants it, sending *DHCP REQUEST*
 - Destination is broadcast port 67, in case of multiple responses
- Server acknowledges this with *DHCP ACK* to client.
 - Any relevant state has been installed, configuration is ready to use

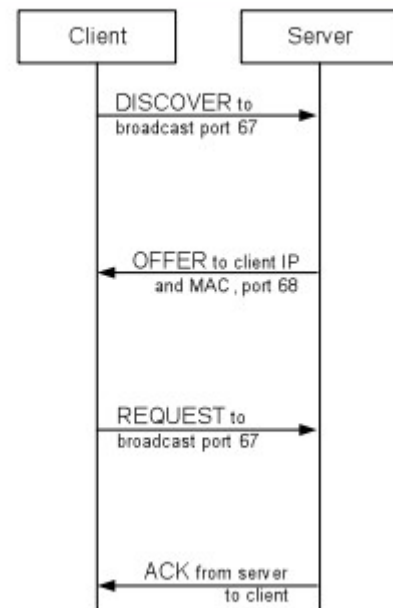


Illustration 11: Example DHCP interaction

i) Multicast in Ipv6

There is no broadcast in Ipv6 only multicast

Nearest to broadcast is all-hosts link-local

When auto-configuring only small scales are relevant else configuration would become irrelevant/insecure

j) Stateless Auto-configuration

Router advertisements can inform the network participants of an existing router for a prefix and clients can also generate global-scope addresses by appending their EUI-64 address to the advertised /64 network prefixes

EUI-64 : 64 bit global identifiers

Router advertisements have lifelines

This is known as stateless address auto configuration since it requires no state information to be stored about the clients on the auto configuration server (gateway)

Client requires more information than just their address though

k) DHCPv6

Redesign of DHCP(v4)

Can coexist with stateless address auto configuration or operate on its own

- Uses link-local interface identifiers to communicate with clients
- Uses multicast for service discovery
- Permits hierarchical network address management
- Uses relay
- Can be stateful or stateless

l) Anycast

Routing mechanism that permits sending data to one of many potential hosts providing the same service

i.e. one to one of many

Most suited to connectionless UDP protocols such as DNS

Used in 6to4

Could be used for well-known addresses for DNS servers etc..

Not secure unless it is known to be on a local network but then a local multicast may be more appropriate

13 Advanced Multicast

a) Requirements for Multicast

Addressing

need to obtain/acquire an IP multicast group address to use, whether globally or locally scoped

Protocol requirements

Hosts need to be able to signal an interest in a group to routers

IGMP ipv4

Routers need to negotiate reception of multicast group traffic

PIM-SM

Service or multi-cast group discovery by clients

b) Multicast tree

Set of paths between sender and receivers

Trees exist per multicast group

Each router maintaining forwarding state for each group

Leaf routers use IGMP to determine Ipv4 listeners

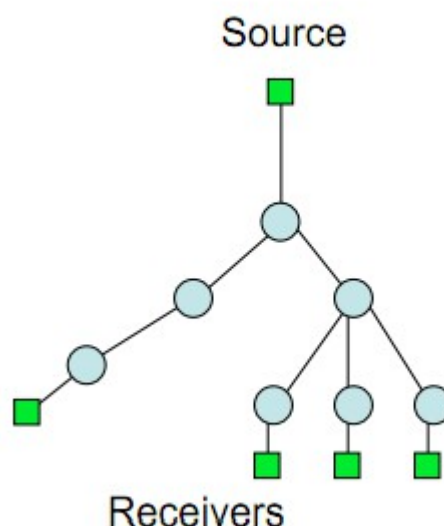


Illustration 12: Multicast tree example

c) Address Assignment and GLOP

Content providers need to know which (global) multi-cast group to use for their application
there's no allocation hierarchy like in Ipv4

GLOP is an allocation method

Multicast address assignment based on BGP AS numbers

233.x.x.0/24 where x.x is an officially assigned AS number

RFC 6034

Unicast prefix-based multicast groups addresses created under 234.0.0.0/8

Soton campus has 152.78.0.0/16 so can use 234.152.78.0/24

Reduces the number of multicast addresses available to sites

i.e. a /24 site only gets 1 address (/32 ?)

d) SAP

Session Announcement Protocol

announce multi-cast content (group addresses) to a well known multi-cast group

service discovery mechanism

Can take a while to receive advertisements

Not reliable

dead services can still be on the SAP list

e) PIM Sparse and Dense Mode

Protocol Independent Multi-cast

Independent of unicast routing protocol

PIM-DM

Flood and prune algorithm

Taught in COMP2008

PIM-SM

Doesn't flood like SM

Scales much better

More widely used today

f) ASM

Any Source Multicast

Use an agreed multicast group address

Any host can send to the group

commonly used in video conference

Receivers don't know the sources at the start (hidden sources?)

Receiver's router joins with (*,G)

g) SSM

Uses group addresses under 232.0.0.0/8

Usually one sender for the group

i.e. IPTV

Receiver know sender's IP in advance

Router joins with (S,G)

Lacks support in operating systems like OSX so isn't widely used

h) PIM-SM operational components

PIM messages between nodes

join and prune

used to create the forwarding tree

IGMP between Ipv4 nodes and routers

A rendezvous point (RP) as a means for sources and receiver's to discover each other

All routers in a PIM domain (site?) use a common RP

Initially sender sends multicast packets towards RP and receiver's send a join message to it

i) IGMP Operation

Host sends an IGMP Report when an application wants to join a multicast group

This is registered at the first router (gateway?) and send upstream?

Hosts leave a group by informing their router or when they do not respond to an IGMP Query

A prune message is then sent upstream

Router queries host every ~125seconds asking for a report of which multicast groups It wants to listen to

j) PIM-SM Phases

Initially sender's don't know about receivers only the group number

2 phases in the PIM-SM process

Initial:

Rendezvous Point (RP) learns about senders and receivers

uses this to create a Rendezvous Point Tree (RPT)

Optimisation

Shortest Path Tree (SPT) is worked out

k) RP learns sender

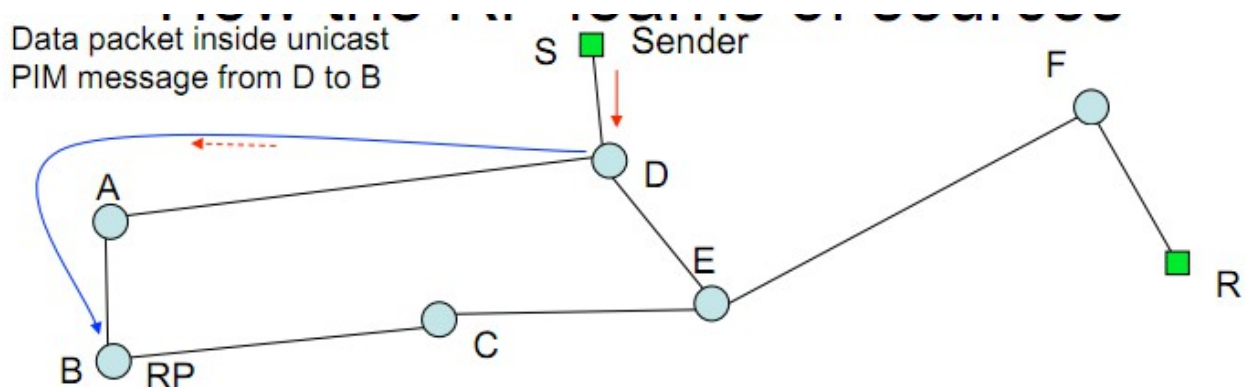


Illustration 13: RP learning about the sender point

Routers A->F set up with B as their Rendezvous Point

On each link (i.e. F-R and D-S) router elected to be the designated router which allows communication with the RP (this is abstracted from the sender S)
D sends the multicast traffic encapsulated in unicast PIM-Register messages to B
B then learns about the sender S broadcasting to the group

l) RP learns receiver

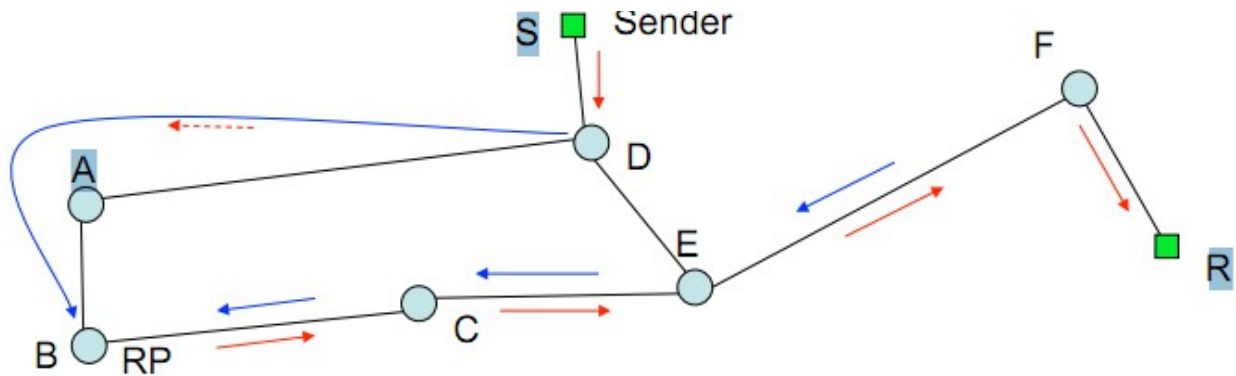


Illustration 14: RP learning about a receiver

Receiver R sends a PIM join message to F
This is forwarded onto the known RP router by F (not known to R)
RP can then send data down the reverse path to R

m) Avoiding encapsulation

In the current scenario multi-cast from S is encapsulated into unicast traffic at D and sent to RP
PIM-SM allows for receiver's to get traffic directly IF they know the sender

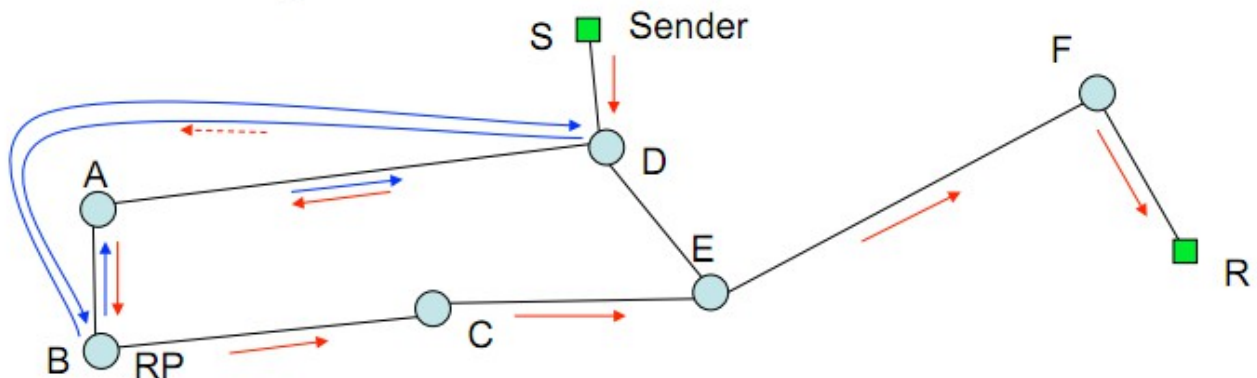


Illustration 15: Removing encapsulation

B wants to stop receiving PIM-Register unicast messages from D&S
B sends a JOIN message to D for the group
D then sends native multicast traffic to B
B then sends a Register Stop message to D so that it stops receiving the encapsulated traffic
Thus only multicast traffic is flowing in the system

n) Multicast route optimisation

Router F is now receiving packets from S via the RP
Wants to receive directly from S (well the router D)
Since it now knows the location of S it can send a join towards it

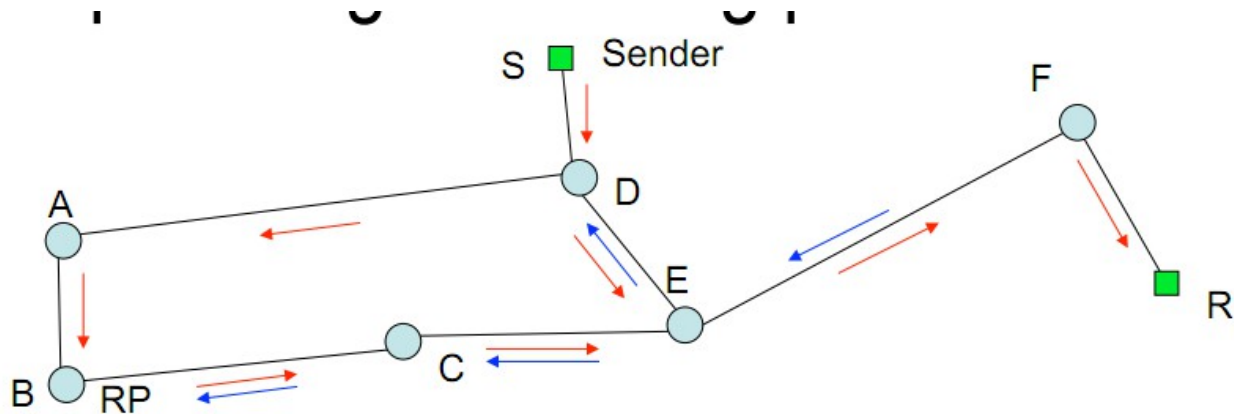


Illustration 16: Shortening the path

F sends join towards S

E forwards this on and starts receiving S traffic directly from D

It now works out which path is optimal : the RP route coming in via C, or the direct route from D

It sends a PRUNE message to C which breaks the route

o) Inter-Domain Multicast

Typically a small ISP or campus will have a PIM domain

Each PIM(-SM) domain will have 1 RP for all groups

Multi-cast Service Discover Protocol used (MSDP)

RP s are pre-configured in a mesh

When an RP learns of a new sender it sends a Source Active announcement to the mesh

this is flooded around the mesh

The sender IP is included in the SA message so any new receivers joining a group the sender is sending on can automatically construct the shortest path forwarding tree

14 IP Routing

a) Site requirements

Change from site to site

SOHO Networks

Unmanaged, usually a single subnet i.e. a small campus

Enterprises

Managed, multiple (sub)-networks with internal routing
i.e. A large campus like Southampton

Distributed Enterprises:

Linking lots of sites with dedicated interconnects

Mobile Networks

May change point of attachment over time

Emerging method

b) Site ISP relationship

Sites want simple, robust and cheap ways for ISPs to deliver their services

Not concerned with global impact

wants to be abstracted from this

But they can cause them by impacting on global routing tables

i.e. multi-homing

c) Challenge

To evolve the existing internet architecture to enjoy better scalability and growth

Want to reduce 'pain' for ISPs whilst still providing easy service for sites

Typical requirements:

- provider independence : i.e. easy to change ISP

- multi-homing

- traffic engineering

- mobile network support

- scalability (for ISPs)

d) Provider Independence

Applies to larger sites more than smaller ones

Want to avoid dependence on any ISP

- Sites get Provider Aggregatable address space PA

Make it easier for sites to change provider

Avoid renumbering when changing ISP

- a problem with Ipv6

Currently facilitated in various ways

- Provider Independent address space PI

 - Assigned from regional registries

 - /48 in Ipv6

 - /24 in Ipv4

- Using NAT at the site border (but that only helps with internal routing?)

- Using historically assigned address blocks from the early internet era

 - i.e. /8 s assigned to companies like IBM and Ford

Provider Independent address space provides extra routes which will be a problem in Ipv6

e) Multi-homing

Using multiple ISPs at a site to increase reliability or load balancing

Uses up address space and more prefixes are advertised

Could use a PI but that might cause confusion in the deeper parts of the internet

f) Traffic Engineering

Might want to send different traffic on different routes to normal based on certain criteria

- i.e. sending time-critical traffic on the shortest time route and non-critical traffic on a longer route

- i.e. using a high-speed link for certain hosts and then a slower link for less important hosts

Requires more specific routes to be advertised creating more work for routers to do and more state for them to hold

Reduces aggregation

g) Mobile Networks

An emerging area

Mobile Ipv6 for nomadic hosts

What if the router or whole network moves?

Can have PI for the mobile site but that would cause more de-aggregation
Renumbering the site at new location
 would cause a lot of work and hassle
Use a home prefix and tunnelling
 Mobile Ipv6 for sites – seems to be the preferred direction
What if mobile networks multi-home?

h) Scalability

A design consideration for ISPs and standards setters rather than user sites
Need to encourage user sites to use what's best rather than what's cheapest
Want changes to be transparent for sites as much as possible
Want as much aggregation as possible to reduce the number of routes routers have to deal with

i) Pressures on the routing system

BGP requires an ASN per site/ISP
 16 bit number originally but this is exhausted
 32 bit numbers being introduced
Continual growth in the total number of routes
 affects the memory usage of routers
 includes many 'more-specific' routes
Churn of routes
 how much routes change
 affects the processing power of routers needed to keep routes up to date
IP global pool exhaustion
 causes sites to have disjointed subnets
 de-aggregation of blocks
Trust
 how to decide whether to trust routing updates
 can be abused to create blackholes in the internet to block traffic to certain hosts

j) Route growth

Exponential growth in routes
BGP registration tailing off due to new ISPs finding it harder to get space
Most noticeable in the USA
Lots of churn/updates coming from a small part of the internet
 small number of ISPs providing lots of churn

k) Ipv6

Makes things harder from a routing perspective
Routers now need tables for both Ipv4 and Ipv6
v6 addresses are bigger → more memory needed
Ipv6 PI now in use at /48 level
Slow uptake of ipv6 still

15 Network Security and Monitoring

Hacking – being taught to show us how to protect networks

a) What is security

A PROCESS!

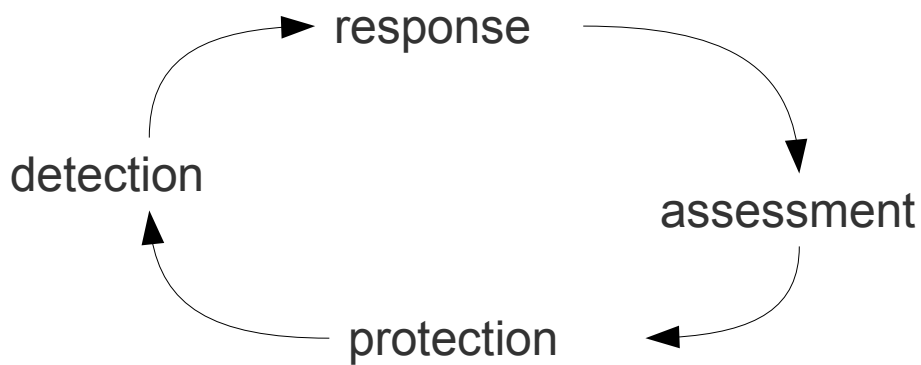


Illustration 17: Security process

Can only find something is secure by testing and monitoring it

Very few impenetrable systems ← almost everything is hackable

NSM is concerned with the collection and escalation of incidents but WON'T protect your network!

b) The basics

OSI 7 level model referenced not the 4 level TCP/IP model

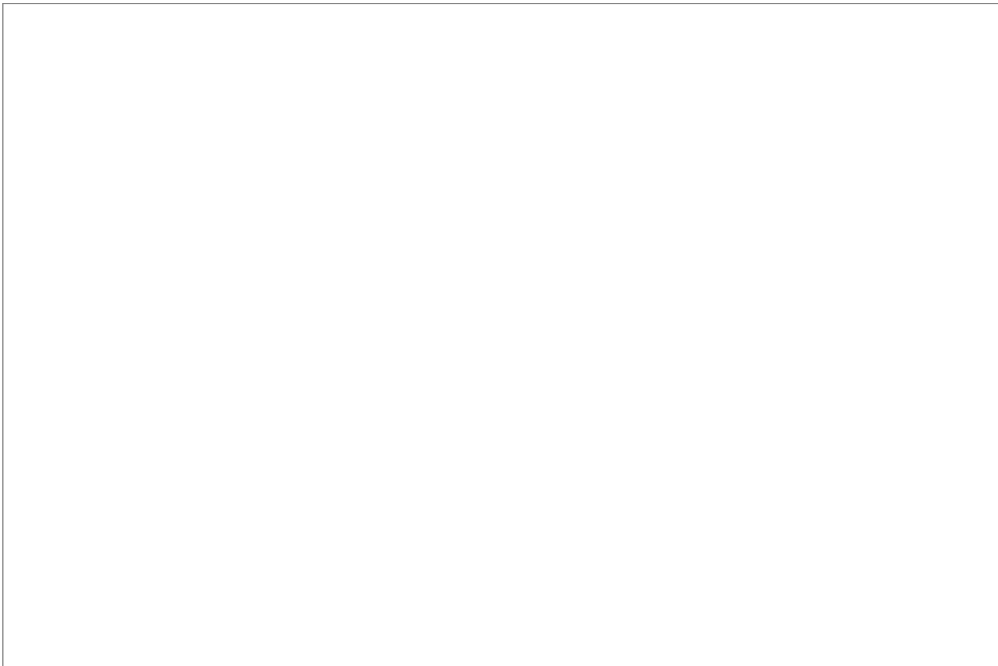


Illustration 18: Network stack

What happens we request google.com

1. Check host for or local cache for IP address of Google.com

2. If its not found send a DNS request
UDP or TCP used (TCP when query is large)
Port 53 for request
Ipv6 → AAAA record
Ipv4 → A record

..

Server for DNS set in DHCP or other setup stage

Source Port chosen at random from a range set by the Operation System

Can use this to identify a hosts OS by monitoring their DNS traffic

c) HTTP

Uses TCP in lots of short sessions

GET and POST

Layer 7 protocol (Application level)

d) TCP

Synchronous and reliable

3 way handshake for establishing a connection

Really quite secure – hard to spoof TCP

e) Default Gateway

Traffic sent to the default gateway when destination IP isn't on the same subnet

DG must be on the same segment as the host

DG's MAC address stays in the host's ARP cache

f) NAT

Prevents private addresses (192.168.1.1 etc... defined in RFC1918) being used on the internet

NAT translates private addresses to real addresses

Can break things as hides hosts but can be useful for security

g) Protocols

Netflow session data

useful in security

says what packets are flowing on the network, where they are going

Full content packet capture

wireshark and tcpdump

takes packets and stores a copy of the whole them

Signature based Intruder detection

detect hackers?

16 Server Hacking

a) 5 Phases

Typically 5 distinct phases of compromise

Reconnaissance

Exploitation

Reinforcement

Consolidation

Pillage

Advanced attackers will launch the different phases from different source Ips over a long period of time

Not all attacks will use all 5 phases

b) Reconnaissance

An attacker will scope out a network/host to discover services, vulnerabilities and connectivity prior to an attack

Port Scan : find TCP ports being used

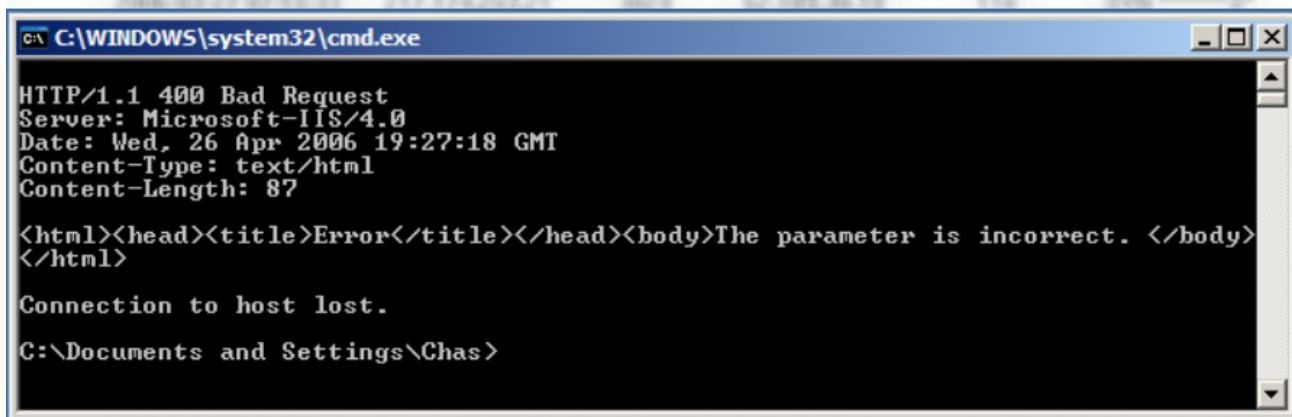
Banner Grabbing : Sending commands to get information

DNS Brute Forcing and Google : Getting more info

Google is a powerful tool

Want to discover services and use their weakness and exploits

Quite hard to detect



```
C:\WINDOWS\system32\cmd.exe
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Wed, 26 Apr 2006 19:27:18 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.
C:\Documents and Settings\Chas>
```

Illustration 19: Example banner grab

c) Port Scan

One attacker to One host : can be hard or easy to detect depending on the speed of the scan

One to Many Ports : again can be hard to detect depending on the speed of the scan

connect to every IP in v4 and test a particular port

Can sometimes be obvious in logs that someone is doing this (case at ECS?)

Many to One : difficult to spot

Uses botnets to control lots of external hosts in order to find open ports

d) Exploitation

Done by various means:

remote command execution

buffer overflow

SQL injection

running arbitrary SQL commands and trying to view the results somehow

Brute Force

pushing through lots of commands/data

Vulnerability is normally the result of bad coding of web services

i.e. in PHP not escaping mysql commands

Network tools like nessus can be used to help identify weaknesses

e) Reinforcement

Retrieve tools, Escalate privileges, install root-kit

Attackers often make the host download tools and programs to assist the attack

This is easy to detect:

- web-server making outbound requests is unlikely

Escalate privileges

- normally to get to super-user level to take control of the computer

- although not necessary for all attacks to take place

Install root kit

- attempts to hide the fact the machine has been hacked from other users/admins

Can use deep file system forensics to find malicious files, but hard to do if the root kit is good

f) Consolidation

Using a secure back door to run commands on the system

The attacker returns to the scene

Can be encrypted

Often IRC used to talk to multiple remote hosts

Encryption can often be reverse engineered as source code for rootkits is available

Monitoring of traffic can help in detecting attacks

g) Pillage

Steal information or data

Damage or destroy data or systems

Attack other systems from that machine

DoS or DdoS

High amounts of data being generated in DoS attacks may over write logs so it might be hard to detect

h) Summary

Security Analyst must know what type of traffic to expect in each phase

Must be able to cope with losing data sources and make assumptions based on past experience

17 Client Hacking

a) Introduction

The most commonly attacked device is the client

Attacks can be classified by their distribution:

- Universal

- Targeted

But all attacks share similarities

- code is unwittingly run on clients

- Most install themselves so they restart after boot

- Control channel to send data back to a command server

 - Irc, HTTP, P2P etc..

b) Universal Infection Vectors

How the attack spreads

Drive By Download

- Web based

- XSS Attacks

- Popular sites which have extra code inserted

Binding

- Seed popular files on file sharing sites

- Attach some extra (hidden) code

- Drops silently in install

c) Drive By Download

Silently install malware by exploiting a vulnerability

Often use hidden elements to do the dirty work

- hidden iframes

- obfuscated javascript (hidden)

Exploit kits target a range of vulnerabilities to infect as many machines as possible

d) Zbot, zeus and wsnpoem

Most popular universal malware in use today

Steals your data

- even if you're using SSL and Anti Virus

- gets it from web forms etc.. and sends to a controller

Most malware today uses HTTP as its control channel

- so it blends with normal traffic and is harder to spot

Defend by blocking bad domains

- DNS sinkhole

- IP based blocking

- Transparent proxy

But need that list of bad domains first

e) Anti Virus Software

Have a difficult task

- A system to detect millions of files

- Must be fast

- Must be able to detect and fix problems

Often signature based

- Byte patterns from sections of a malicious file

- Can be evaded by using obfuscation techniques

BUT

- AV software does help

- will pick up some viruses

- modern software helps defend against bad URLs etc..

- can block hidden activity the user doesn't spot

f) Malware Obfuscation

Compiled exe has imports for DLLs

These are set out in the PE header of the exe file

However, DLLs and functions can be loaded dynamically at runtime

This can be used to hide imports and make it hard for AV to spot it

g) Targeted Malware

Not spread universally

code might not be unique though

delivery method unique though

usually aimed at certain individuals or companies

Exploit trust

Can be embedded in Office files and PDFs

macros

Usually target a certain exploit based on prior knowledge of systems

i.e. MS Word exploit for a company using MS Office

Low AV detection

Control channel (HTTP based) used to steal documents or data

May want to take control of the host

use it to take over other computers in a company

spy on an internal network

Network traffic might change

lots of outbound HTTP traffic sending data rather than requesting it

this might be detectable

h) Reverse Engineering

A skill in need

Static Analysis – reading the assembly code

Debugging

these can be time consuming

Sandboxing

run time analysis in a controlled environment

Real systems or atleast emulations

can study what the malware does

Can try to monitor programs and see where they hook other APIs using run time analysis tools

18 Wireless Security

a) Why bother

Obligations to make sure resources are used by authorised people

i.e. in a business we don't want anyone else using our network

Limit liabilities through misuse

i.e. a business is liable for copyright abuse done through its network

Security

b) Simple Schemes

These aren't very good and can be abused

MAC-Based

- what ECS uses

- users register their MAC address prior to connecting to the wireless

- only valid users can register MAC addresses

- But MAC addresses can be observed and spoofed

DHCP Control

- Only assign IP addresses to registered MAC addresses

- Devices can still set their IP manually

- MAC spoofing

- DHCP not secure

Hidden SSID/Network

- not as hidden as you would hope for

c) WEP

Wired Equivalent Privacy

Meant to be as secure as using a wired connection

40 or 104 bit key

Weaknesses found and quickly deprecated

d) IEEE 802.11i

Revision of 802.11 family to include more security features

Implemented Wi-Fi Protected Access standards (WPA)

WPA has 2 main modes:

- Personal Use using a given key

 - Only as strong as the key used

 - Can be abused due to a flaw in the encryption system used

- Enterprise mode

 - Stronger authentication mode

 - Port-based authentication

 - must authenticate before accessing the network

e) RADIUS

Remote Authentication Dial-In User Service

A standard for exchanging authentication requests

Originally used in old dial-up services

Uses UDP Messaging with optional shared secret based encryption

Client may provide extra authentication: passwords, certificates etc..

Server may ask for more authentication such as a PIN

Server includes accounting tools

f) Privileges

Might want to grant different privileges and levels to different users

These can be stored in Active Directory or LDAP back end servers

RADIUS supports the return of various options in its response

g) Web Redirection

Used by ISS and other commercial hotspot providers

Requires a log in every time

User Devices gets an IP via DHCP

User uses a web-client to access the internet but gets redirected to a login page by the gateway

User enters details and if successful then gateway gives them access based on their privileges

Advantages

- many ways to authenticate: username/password, PIN, SMS, scratch card

- Lots of systems available

- Only requires a web-browser on the client

- Easy to set privileges

Disadvantages

- challenge server (which controls authentication) could easily be spoofed

- clients which don't authenticate are still connected to the local WLAN and could cause problems

- have to authenticate every time

- not much Ipv6 support

h) Restricted VPN

Uses on campus sites more

User gains hotspot IP via DHCP

Can only communicate on the local network

Only VPN traffic is allowed to leave the network

Therefore clients must authorise with a VPN server to get access to the internet

This can be a set of VPN servers owned by the campus so only authorised users get access

advantages

- data security through vpn

- can use along side web-based authentication

- most devices have VPN software

disadvantages

- need VPN servers and this might not scale well

- VPN increases the bulk of traffic (because of encryption and tunnelling)

- clients can access local network without going through any other authentication

- can cause problems and vulnerabilities

i) 802.1X

Port-based access control

Run a 802.1X 'supplicant' on the user device

Supplicant communicates with authenticator

- does this at link layer using encryption and authentication

- can provide credentials to a RADIUS or similar server

Advantages

- Prevents abuse of the hotspot through layer 2 (link-layer) control

- Supports periodic re-authentication incase privileges change

- RADIUS to control access levels

- Can support Ipv6

- Credentials can be cached

Disadvantages

- Requires special supplicant software to communicate with authenticator
- short coming in mobile devices

- More complex solution for users to understand, use and deploy

j) **Roaming**

Want to have easy access no matter whose network you are a part of

Quite a challenge

Academic networks can use proxies to forward RADIUS requests

- RADIUS server on local network detects authentication is from a user from another network

- it then forwards the request on to an external proxy

- the proxy then resolves the request by querying the correct home RADIUS server

(abstracted from the RADIUS server in the network being connected to)