FIT1047 - Week 9

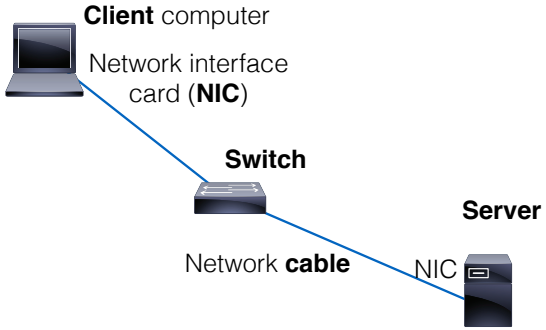
Networks: Physical and Data Link layers

MONASH University

Goals for this week

- Understand how messages can be transmitted over physical media such as copper cables, optical fibres or radio waves
- Look at Media Access Control (Data Link layer): when is a device allowed to transmit?
- Study the basic structure of Ethernet and WiFi networks

Basic LAN components



The main components for building (wired) local area networks are Clients and servers, which are connected to a switch via a network cable. Each client and server needs at least one network interface card.

Network interface card (NIC)

Implements physical and data link layer

- includes unique data link layer address (MAC address)
- provides physical connection to the network (socket or antenna)
- implements protocols (error detection, construction of frames, modulation or encoding etc)

Connection to the computer

- often built into motherboards
- or connected via USB, PCI Express etc

Network interface card (NIC)

Network Cables

Physical connection between network devices

Different types:

- UTP (unshielded twisted pair, most common type for LAN)
- STP (shielded twisted pair)
- Optical fibre (not yet common in LANs)
- Coaxial (only old LANs)

Network Cables

Name	Data Rate	Cables
10BASE-T	10Mbps	UTP cat 3 / cat 5
100BASE-T	100Mbps	UTP cat 5
1000BASE-T	1Gbps	UTP cat 5, 5e, 6
1000BASE-X	1Gbps	optic fiber (single mode or multi-mode)
10GbE	10Gbps	UTP cat 5e, 6, 7 optic fibre
40GbE	40Gbps	optic fiber

This table is just for your information (you won't be assessed on the details). The main thing to remember is that the faster the network you want to build, the higher the category required for the cables (higher category = higher quality).

Physical layer

We'll now get a quick overview of how we can turn sequences of bits (the messages that we want to transmit) into *signals* that travel through a *medium*.

Physical media

- We transmit information using **physical signals**
- A signal travels through a **medium**:
  - **electrical** signals through e.g. copper wires
  - **radio waves** through "air" (or, really, space)
  - **light** signals through space or optical fibres

Digital vs Analog

- Digital **data**:
  - Discrete values (e.g. 0 and 1, or characters in the alphabet)
  - Discrete step from one symbol to the next
- Analog **data**:
  - Range of possible values (e.g. temperature, air pressure)
  - Continuous variation over time

We're only concerned with digital data here.

Digital vs Analog

- Digital **signal**:
  - Waveform with limited number of **discrete states**
- Analog **signal**:
  - Continuous, often **sinusoidal wave**
  - E.g. sound (pressure wave in air), light and radio (electromagnetic waves)

We can use both digital and analog signals to transmit digital data!

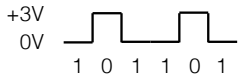
Transmission types

- analog signals for analog data:
  - e.g. analog FM radio
- digital signals for digital data:
  - e.g. old Ethernet, USB, the bus in a computer
- analog signals for digital data
  - e.g. modems, ADSL, Ethernet, WiFi, 4G, …

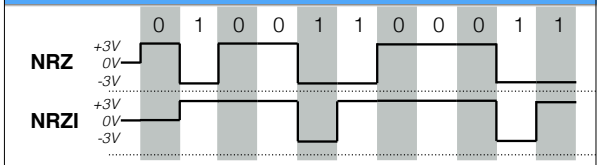
digital transmission

Digital transmission

- Digital signals are typically transmitted through copper cables
- A digital signal encodes 0s and 1s into different **voltage levels** on the cable
- This results in a **square wave**
- Simplest encoding: **unipolar**



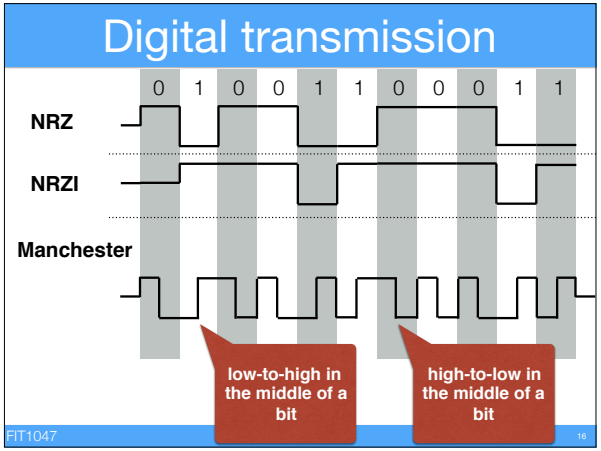
Digital transmission



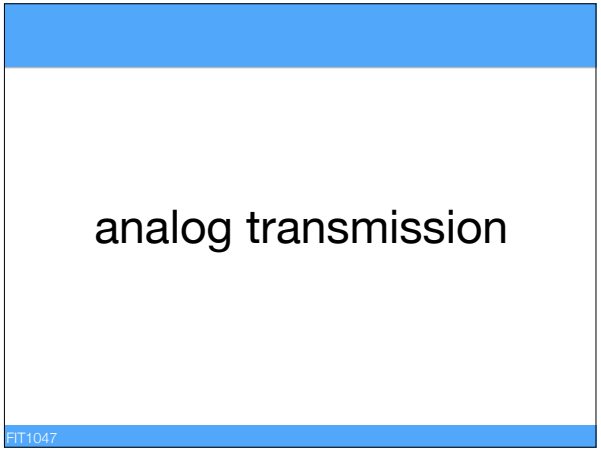
These are bipolar signals (switching between negative and positive polarity).

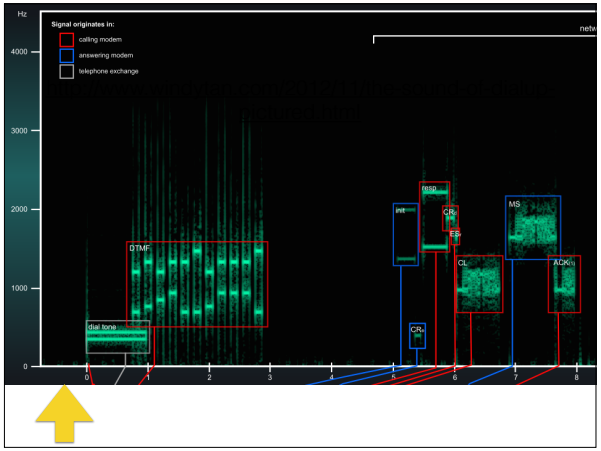
NRZ = "Non-return to zero". In this case 0 is transmitted as a positive voltage, and 1 as a negative voltage.

NRZI = "NRZ-Inverted". A 1 is transmitted as a change in polarity, a 0 as no change.

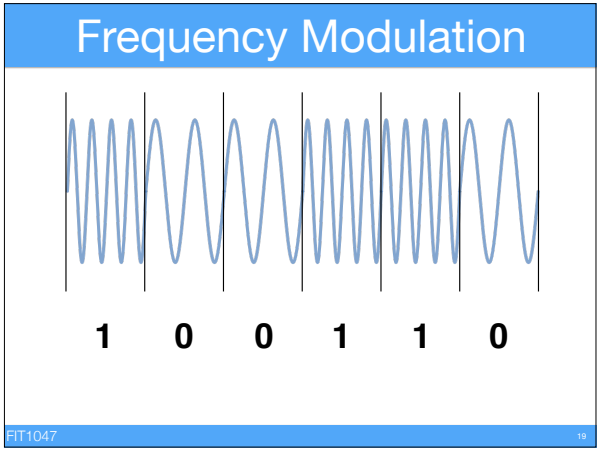


Manchester encoding: A 0 is represented as the voltage going from positive to negative, a 1 as negative to positive, but the transition happens in the middle of a bit. At the start of a bit, we may have to go to the opposite side so that the correct transition can happen.
Manchester encoding produces a "self-clocking" signal:
"Listening" on a cable immediately tells you whether transmission is happening!



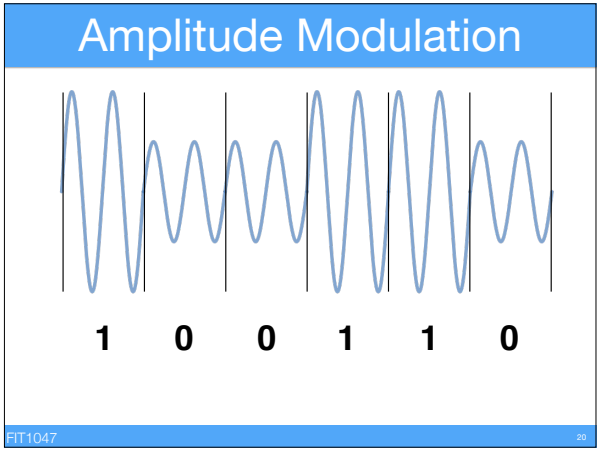


This shows you the *spectrum* of a dial-up modem "handshake" (i.e., where two modems establish a connection with each other). A modem (modulator/demodulator) turns digital data into sounds that can be transmitted over a normal telephone line. This is one way of turning digital data into analog signals. But we can also produce analog electrical signals directly, i.e., without producing sounds first.

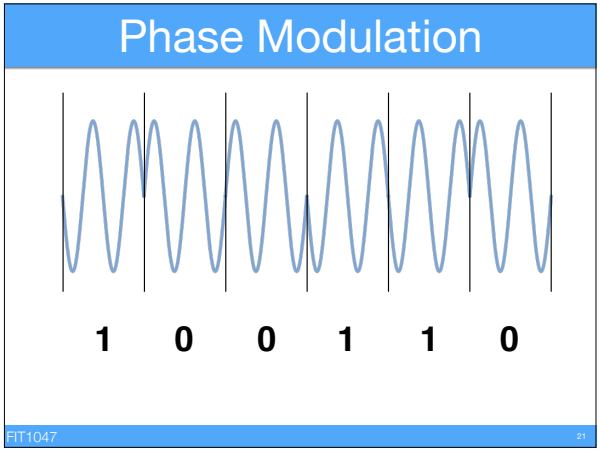


Frequency: how many cycles per second. Corresponds to the pitch of a sound wave, or the colour of a light wave.

In Frequency Modulation (FM), we represent 0s and 1s by different frequencies. Each bit is transmitted for the same amount of time (the vertical bars in the picture).



Amplitude: corresponds to the loudness of a sound wave. In Amplitude Modulation, the frequency is kept constant, but we change the amplitude of the signal to encode our message.



Phase: the initial angle at which the wave begins (e.g. the first wave starts by going downwards, whereas the wave in the second time unit starts by going upwards).
As for FM and AM, we can use the phase angle to encode our message.
In practice, most modulation schemes (e.g. for modems, ADSL, or modern Ethernet) modulate both the amplitude and the phase at the same time.

Data Link layer

Data Link Layer

- Now we've seen how we can convert digital data into a signal and back
- The data link layer
  - **controls** access to the physical layer (MAC = Media Access Control)
  - **encodes/decodes** between frames and signals
  - implements **error detection**
  - **interfaces** to the network layer

Contention-based MAC

Any device can transmit at any time

- "first come first served"

Collisions: two devices transmitting at the same time

- packets in a collision are damaged
- **avoid** collisions by carrier sensing (listening on the network for transmission)
- **detect** collisions and re-transmit

Used in Ethernet

MAC = Media Access Control. This is the part of the Data Link layer protocol that is concerned with the interface to the physical medium. There are other forms of MAC, but we will only look at this one.

Ethernet

Dominant LAN technology

- Standardised as IEEE 802.3
- used by almost all LANs
- developed in 1973, standardised in 1980

Physical layer

- Originally 10Mbps over shared media coaxial cable
- Now mostly switched 100Mbps or 1Gbps over UTP
- Standards exist for optic fiber up to 100Gbps

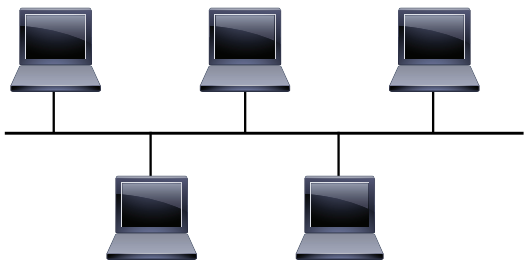
Ethernet MAC

Media Access Control: CSMA/CD

- Carrier Sense (**CS**):
  listen on bus, only transmit if no other signal is "sensed"
- Multiple Access (**MA**):
  several devices access the same medium
- Collision Detection (**CD**):
  when signal other than own is detected:
  - transmit jam signal (so all other devices detect collision)
  - both wait random time before re-transmitting

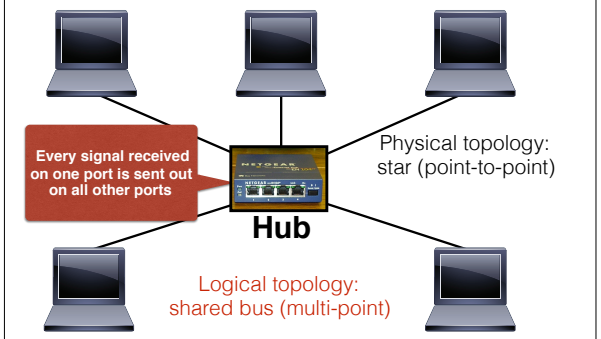
Ethernet

Topology:
shared bus (multi-point)



One cable, but only one device is allowed to send at a time. This was the design of the first Ethernet (late 1970s, early 1980s). The advantage of this setup is that it's easy to add new devices to the network: a single cable runs through the entire building (or floor of a building), and a new device simply needs to be attached to that cable.

Ethernet



The **physical** topology describes the layout of the cables: each device has its own connection to the hub, so the physical topology is a **star.**
The **logical** topology describes how the network looks from the device's point of view: since all signals are just redistributed by the hub on all of its ports, it still looks like a single long cable (a shared bus or multi-point topology).

Problems with Shared Ethernet

Half-duplex

- only one device can send at a time

Broadcasting

- all frames are delivered to all devices, not just destination

Limited network size

- CSMA/CD limits size of **collision domain**

Solution: implement logical star topology!

A **collision domain** is a set of devices that are connected to the same shared Ethernet, so that if two of those devices send simultaneously, the frames "collide" (destroying the useful data and requiring the frames to be resent).

Switched Ethernet

Switched Ethernet

Network switch

- looks like hub
- 16 to 24 ports for UTP cables
- **but**: circuit no longer shared!

A switch is a layer 2 device

- reads MAC address of frame
- transmits **only** to destination port

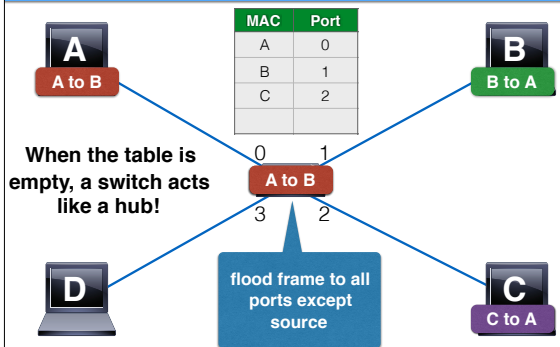
How does the switch know the destination port?

FIT1047 - Week 9

Networks: Physical and Data Link layers

MONASH University

Switch Forwarding Table



When the switch is started, it doesn't know anything about which devices it is connected to. So when a frame arrives (like the one from A to B), it must send that frame to all ports (just like a hub would). But it can remember that A is connected to port 0, so from now on, when a packet arrives for A, it can send it there directly. So remember: the forwarding table is built by looking at the **source** that a packet came from!

Switches and MAC

Full-duplex circuits

- point-to-point connection between computer and switch
- no collisions possible

But frames may still be sent at the same time

- e.g. A sends to B while C sends to D
- or A and B both send to C simultaneously
- switch has **memory**: stores second frame until transmission of first frame is finished, then forwards the second - **store and forward**

Switched Ethernet runs at up to 95% capacity, compared to 50% for shared Ethernet!

Rack-mounted switches

Monash communications cabinet, Caulfield, Bldg. H level 6

The cables from all the network sockets in the offices and labs on one floor of the building arrive at the back of the rack-mounted patch boards (on the left of the picture). Each network socket is connected to one socket on the patch panel. We can then connect the patch panel socket to a switch (on the right) to connect that office to the Monash network.

Rack-mounted switches

These are the switches. The blue cables connect the switches to the patch panel, and from there to the offices and labs on this floor.

The red cables connect the switches to the rest of the Monash network.

Rack-mounted switches

What you can't see easily here, is that there are many empty sockets on the patch board. The idea is that you fit out each office and meeting room with several network sockets, in case you need them later (because it is expensive to put in new cables later). But you only connect those that are actually in use to a switch.

Wireless Local Area Networks

Why WiFi?

Wireless LANs

- eliminate cables (heritage buildings, rented apartments, …)
- allow for more flexible network access
- facilitate mobile workers (e.g. hospital)

Basic setup

- WLAN NICs connect to Access Points (APs) using radio frequencies
- APs are connected to wired LANs (or backbones)

WLAN Technology

Wi-Fi (or "Wireless Ethernet")

- IEEE 802.11 family of standards
- Original standard from 1997-1999 (802.11a, 802.11b)
- Widely used: 802.11g (2003), 802.11n (2009)
- Latest: 802.11ac

Other wireless LAN technologies

- WiMAX (802.16)
- Bluetooth (802.15), also called WPAN (Wireless Personal Area Network)

We'll only talk about 802.11 in this unit. Bluetooth has become very popular, especially since version 4.0, but is typically used to create small networks of personal devices (e.g. computer-to-smartphone or smartphone-to-fitness-tracker)

WLAN Radio Frequencies

Most WLANs use the 2.4GHz and/or 5GHz range

- high frequencies allow for large bandwidth
- but higher frequencies have stronger attenuation

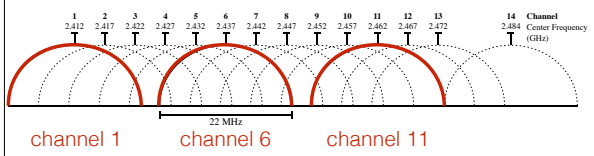
WLAN channels

- Networks in the same area should not use the same frequencies
- WLAN spectrum is divided into **channels**, each network is set to a different channel

Attenuation: signal getting weaker with distance.

Compromise between bandwidth and attenuation. WLAN is only used for relatively short range connections (up to 50m or so).

WLAN channels (802.11n)



2.4GHZ band

- 2.4000-2.4835 GHz
- 13 channels, each 22 MHz wide
- But channels overlap! Only 5 MHz apart

Only 3 non-overlapping channels. Other channels should not be used.

Channel 14 is only used in Japan.

CSMA/CA Media Access Control

All devices in a WLAN share the medium

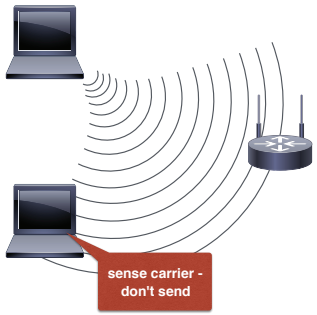
- use the same channel (frequency band)
- need to deal with collisions

CSMA/CA

- Carrier Sense, Multiple Access
- **C**ollision **A**voidance
- Compare to 802.3: **C**ollision **D**etection
- Devices try to **actively avoid** collisions

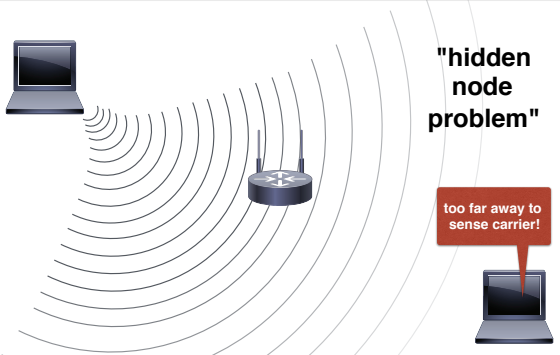
Why do we need a different strategy than in wired Ethernet? Because devices may be too far apart from each other to do carrier sense!

Why is WLAN different?



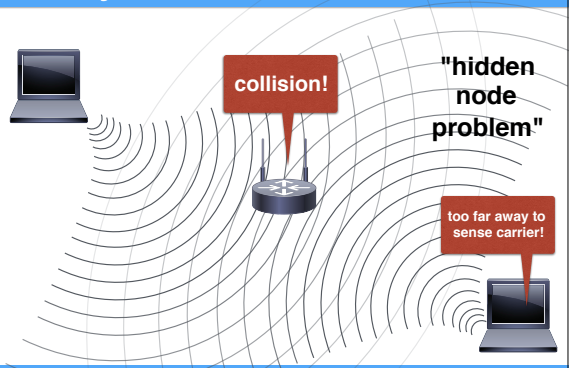
If devices are close enough, they can sense the other's transmissions (their "carrier").

Why is WLAN different?



But if we're too far away, then the access point may still get a connection to the other device, but the transmission is too weak for us to detect.
The hidden node problem means that a device cannot reliably detect collisions. The radio waves may collide at the access point (so both packets are destroyed) but both senders won't notice that.

Why is WLAN different?



We therefore need additional mechanisms for Media Access Control.

Two solutions: ARQ + Controlled Access

802.11 uses stop-and-wait ARQ

- ARQ = Automatic Repeat ReQuest
- AP sends ACK (acknowledgement) after receiving a frame
- devices only send next frame after receiving ACK for previous frame, otherwise re-send original

802.11 *may* use *controlled* access

- device can send "Request To Send" (RTS)
- only transmit frame if AP sends "Clear To Send" (CTS)

ARQ is a very common technique for error correction (we'll see it again in the next lecture on TCP). It simply means that the receiver acknowledges the successful reception of a message - and if a sender doesn't get an acknowledgement, it sends the message again.

ARQ deals with the hidden node problem: even if a device does not detect a collision, it knows something went wrong when it doesn't get an ACK.

RTS/CTS is implemented e.g. in Monash WLAN.

802.11 ARQ

Hidden node problem

- collision detection not reliable
- instead, receiver needs to ACK every frame

What if no ACK?

- we may not sense a carrier (too far away)
- re-sending immediately therefore might be bad idea

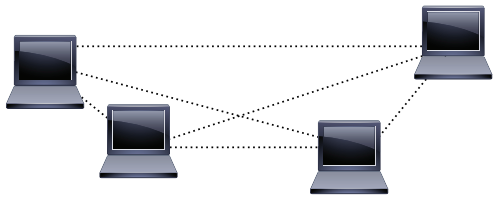
Solution: exponential back-off

- 1st collision: everybody waits 0 or 1 time unit
- 2nd: everybody waits between 0 and 3 time units
- 3rd: everybody waits between 0 and 7 time units…

Same as random back-off after waiting: when a collision happens, we have to make sure only 1 device starts the re-transmission.

WLAN Topology

Basic Service Set (BSS)

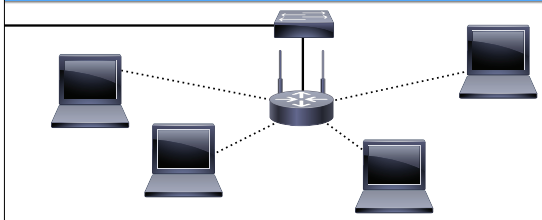


Independent BSS

- **ad-hoc** network
- devices communicate directly with each other

This is the type of WLAN that you can create e.g. between your phone and your laptop, or between computers directly. All devices in such a network can send messages to each other directly (like in a shared Ethernet LAN).

Basic Service Set (BSS)

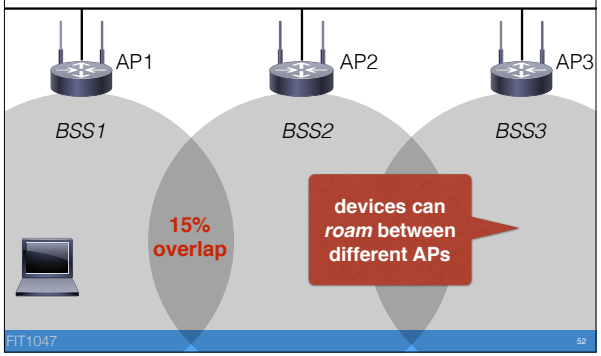


Infrastructure BSS

- all devices communicate with one Access Point (AP)
- AP connects to LAN
- all devices communicate **via** the AP

This is the much more common type of WLAN: all devices connect to a central *Access Point* (e.g. your WiFi router at home, or the access points at Monash). The difference is that devices can now only communicate *via* the AP, i.e., it has to relay all messages. The AP is usually connected to a wired (Ethernet) network to provide the connection to the rest of the network (and e.g. the Internet).

Extended Service Set (ESS)



FIT1047 52

An Extended Service Set uses *multiple* APs to cover a larger area. A device can automatically switch from one AP to the next when it detects that one signal becomes weaker while another one becomes stronger. All APs transmit the same SSID (Service Set Identifier, e.g. "eduroam") so that devices know they can "roam" from one to the next. The APs need to be set to different channels.

Extended Service Set (ESS)

Extends range of mobility

- set of infrastructure BSSs
- APs communicate to forward traffic between BSSs
- APs communicate via **distribution system (LAN)**
- devices see a **single layer 2** connection

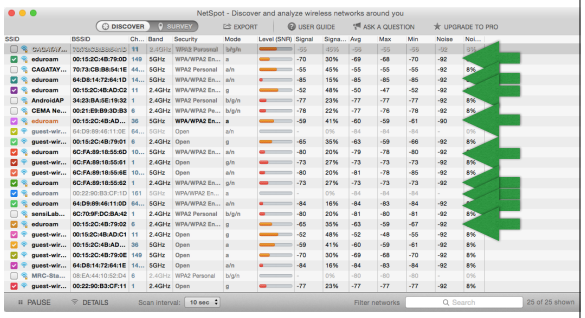
Roaming between different ESSs

- not possible in 802.11 protocol
- requires higher-level protocol, e.g. Mobile IP

FIT1047 53

Important: higher layers (network, transport, application) don’t see any change when roaming inside an ESS. I.e. all TCP connections stay alive (e.g. if you're on a Skype call it won't disconnect, or a download won't be interrupted).

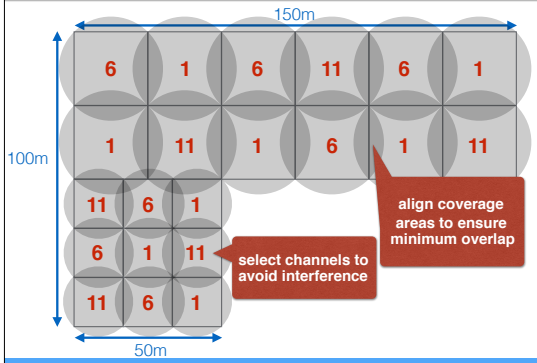
Extended Service Set (ESS)



FIT1047 54

Several APs for eduroam, device connects to the one with the strongest signal.

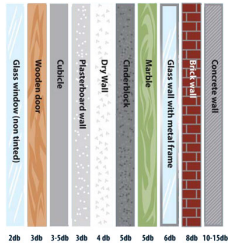
Planning Example



Attenuation

Walls can introduce significant attenuation.

- 3db means signal strength halves
- 6db means 1/4
- these values are for 2.4GHz, attenuation is even higher in 5GHz



Source: http://www.liveport.com/wifi-signal-attenuation

Attenuation simply means that a signal gets weaker. One source of attenuation is simple distance: Just think of sound waves, the volume at which you hear a sound goes down significantly the further away you are from the source. Similarly, certain materials can weaken a signal. The table shows you how different materials affect the signal strength of WiFi.

Summary

Physical layer:

- Media: copper cables, optical fibres or radio waves
- modulate digital data onto digital or analog signals

Data link layer:

- Media access control (CSMA/CD and CSMA/CA)
- Ethernet as the dominant LAN technology
- Wireless LANs