Cable TV

The cable TV system, where available, is also used to deliver Internet connectivity

Cable TV

The cable TV system, where available, is also used to deliver Internet connectivity

Newer installations are full fibre, but there is also a lot of another fibre/copper hybrid, with fibre to cabinets and then copper to the home

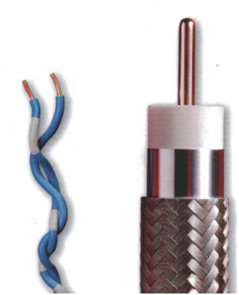
Cable TV

The cable TV system, where available, is also used to deliver Internet connectivity

Newer installations are full fibre, but there is also a lot of another fibre/copper hybrid, with fibre to cabinets and then copper to the home

However, the copper wires used is good(ish) quality coaxial cable that is well screened against interference and crosstalk, and so the data rates it supports are much higher

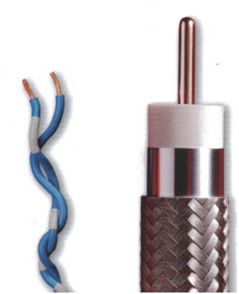
Cable TV



Telephone wire and coaxial cable

Picture from Virgin Media

Cable TV



Telephone wire and coaxial cable

Picture from Virgin Media

Exercise *Read up on Data Over Cable Service Interface Specification* (DOCSIS)

Wireless

The next physical medium we look at is wireless

Wireless

The next physical medium we look at is wireless

Wireless networks have been around for a long time: for example cellular telephone systems

Wireless

The next physical medium we look at is wireless

Wireless networks have been around for a long time: for example cellular telephone systems

Everything wireless is overseen by national and international bodies: we can’t have a free-for-all in a wide area shared resource

Wireless

The next physical medium we look at is wireless

Wireless networks have been around for a long time: for example cellular telephone systems

Everything wireless is overseen by national and international bodies: we can’t have a free-for-all in a wide area shared resource

One wireless system can affect another hundreds or thousands of miles away: there must be some sort of cooperation

Wireless

The next physical medium we look at is wireless

Wireless networks have been around for a long time: for example cellular telephone systems

Everything wireless is overseen by national and international bodies: we can’t have a free-for-all in a wide area shared resource

One wireless system can affect another hundreds or thousands of miles away: there must be some sort of cooperation

So some wireless systems are only allowed with very low power, e.g., Wi-Fi

Wireless

Europe has the *European Telecommunication Standards Institute* (ETSI)

Wireless

Europe has the *European Telecommunication Standards Institute* (ETSI)

USA has the *Federal Communication Commission* (FCC)

Wireless

Europe has the *European Telecommunication Standards Institute* (ETSI)

USA has the *Federal Communication Commission* (FCC)

Such bodies manage the radio spectrum, allocating various frequencies to various purposes, ensuring minimal interference between the competing concerns for parts of the spectrum

Wi-Fi

The IEEE 802.11 group of standards deal with “wireless Ethernet”, more commonly known as *Wi-Fi*

Wi-Fi

The IEEE 802.11 group of standards deal with “wireless Ethernet”, more commonly known as *Wi-Fi*

In principle, it is an analogue of CSMA/CD over wireless, but with some extra problems unique to wireless

Wi-Fi

The IEEE 802.11 group of standards deal with “wireless Ethernet”, more commonly known as *Wi-Fi*

In principle, it is an analogue of CSMA/CD over wireless, but with some extra problems unique to wireless

For example, the shared medium is now all around, not just within a wire

Wi-Fi

The IEEE 802.11 group of standards deal with “wireless Ethernet”, more commonly known as *Wi-Fi*

In principle, it is an analogue of CSMA/CD over wireless, but with some extra problems unique to wireless

For example, the shared medium is now all around, not just within a wire

So signals from *multiple* networks can interfere; not just the hosts *within* one network

Wi-Fi

Wireless networks generally have fairly high error rates due to interference from electrically noisy environments, signal reflections, other wireless networks, etc.

Wi-Fi

Wireless networks generally have fairly high error rates due to interference from electrically noisy environments, signal reflections, other wireless networks, etc.

So the bandwidth achievable is dependent on the circumstances of the environment

Wi-Fi

Wireless networks generally have fairly high error rates due to interference from electrically noisy environments, signal reflections, other wireless networks, etc.

So the bandwidth achievable is dependent on the circumstances of the environment

Conversely, wireless networks generate interference themselves which must be controlled so not to be to annoying to other people

Wireless Problems

In 802.11, the allowed power of transmission is generally kept quite low by the standards bodies to minimise interference

Wireless Problems

In 802.11, the allowed power of transmission is generally kept quite low by the standards bodies to minimise interference

E.g., a typical laptop will transmit at about 32mW; it can read a signal as low as 0.00000001mW

Wireless Problems

In 802.11, the allowed power of transmission is generally kept quite low by the standards bodies to minimise interference

E.g., a typical laptop will transmit at about 32mW; it can read a signal as low as 0.00000001mW

(A digital TV mast might transmit at 100kW)

Wireless Problems

In 802.11, the allowed power of transmission is generally kept quite low by the standards bodies to minimise interference

E.g., a typical laptop will transmit at about 32mW; it can read a signal as low as 0.00000001mW

(A digital TV mast might transmit at 100kW)

Thus the range achievable by Wi-Fi is often quite limited — deliberately

Wireless Problems

In 802.11, the allowed power of transmission is generally kept quite low by the standards bodies to minimise interference

E.g., a typical laptop will transmit at about 32mW; it can read a signal as low as 0.00000001mW

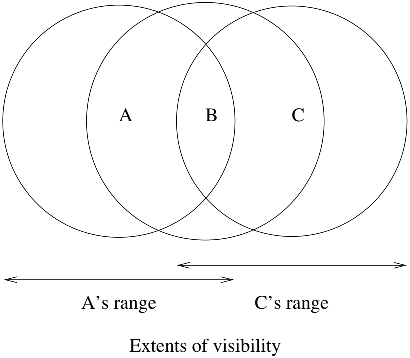
(A digital TV mast might transmit at 100kW)

Thus the range achievable by Wi-Fi is often quite limited — deliberately

But a limited range can cause complications

Wireless Problems

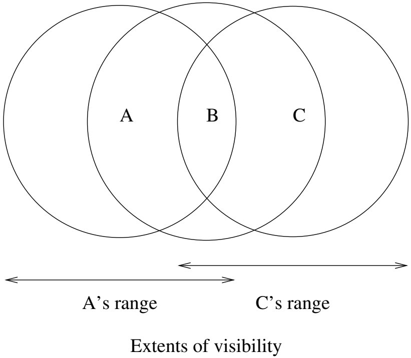
When we have wireless, we get the *hidden host* problem:



Hidden host

Wireless Problems

When we have wireless, we get the *hidden host* problem:



Hidden host

Hosts A can B can “see” each other; B and C can see each other, but A cannot see C, so A cannot tell if its packets to B are colliding with C’s to B

Wireless Problems

In reality, the ranges will not be circular, but something rather complicated dictated by the environment

Wireless Problems

In reality, the ranges will not be circular, but something rather complicated dictated by the environment

But the limited ranges mean that CSMA/CD will not work for wireless

Wireless Problems

In reality, the ranges will not be circular, but something rather complicated dictated by the environment

But the limited ranges mean that CSMA/CD will not work for wireless

CSMA/CD relies on everyone's signals being visible to everybody

Wireless Problems

Next difference: as packets are broadcast, wireless networks are intrinsically insecure, so extra effort must be taken over security and authentication

Wireless Problems

Next difference: as packets are broadcast, wireless networks are intrinsically insecure, so extra effort must be taken over security and authentication

War Driving is driving with your laptop around the neighbourhood until you find an unsecured wireless signal: then you have free access to the Internet!

Wireless Problems

Next difference: as packets are broadcast, wireless networks are intrinsically insecure, so extra effort must be taken over security and authentication

War Driving is driving with your laptop around the neighbourhood until you find an unsecured wireless signal: then you have free access to the Internet!

This is illegal in the UK and elsewhere

Wireless Problems

Next difference: as packets are broadcast, wireless networks are intrinsically insecure, so extra effort must be taken over security and authentication

War Driving is driving with your laptop around the neighbourhood until you find an unsecured wireless signal: then you have free access to the Internet!

This is illegal in the UK and elsewhere

These days, many fewer people forget to secure their networks than was common in the early days of Wi-Fi

Wireless Problems

Next difference: as packets are broadcast, wireless networks are intrinsically insecure, so extra effort must be taken over security and authentication

War Driving is driving with your laptop around the neighbourhood until you find an unsecured wireless signal: then you have free access to the Internet!

This is illegal in the UK and elsewhere

These days, many fewer people forget to secure their networks than was common in the early days of Wi-Fi

Only use a Wi-Fi network if you have permission to do so

Wireless 802.11

There are several parts to the 802.11 standard, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax and more

Wireless 802.11

There are several parts to the 802.11 standard, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax and more

You may now see them under the brandings:

Wi-Fi 1	802.11b
Wi-Fi 2	802.11a
Wi-Fi 3	802.11g
Wi-Fi 4	802.11n
Wi-Fi 5	802.11ac
Wi-Fi 6	802.11ax

Wireless 802.11

There are several parts to the 802.11 standard, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax and more

You may now see them under the brandings:

Wi-Fi 1	802.11b
Wi-Fi 2	802.11a
Wi-Fi 3	802.11g
Wi-Fi 4	802.11n
Wi-Fi 5	802.11ac
Wi-Fi 6	802.11ax

And the recently announced (2020) Wi-Fi 6E (using the recently freed 6GHz band)

Wireless 802.11

Other parts of 802.11, like 11c, 11d, 11e, 11f, 11h, 11i deal with things like power management, quality of service, security and authentication and so on

Wireless 802.11

The original standard specified signalling rates of up to 2Mb/s

Wireless 802.11

The original standard specified signalling rates of up to 2Mb/s

Up to 100m (300 feet) indoors and 300m (1000 feet) outdoors

Wireless 802.11

The original standard specified signalling rates of up to 2Mb/s

Up to 100m (300 feet) indoors and 300m (1000 feet) outdoors

There was an infra-red mode as well as a radio mode, but this was not widely implemented

Wireless 802.11

The original standard specified signalling rates of up to 2Mb/s

Up to 100m (300 feet) indoors and 300m (1000 feet) outdoors

There was an infra-red mode as well as a radio mode, but this was not widely implemented

802.11b extended this to rates of 5.5Mb/s and 11Mb/s

Wireless 802.11

They use the unlicensed 2.4GHz waveband

Wireless 802.11

They use the unlicensed 2.4GHz waveband

That means you do not need to get a licence to use that frequency at low power

Wireless 802.11

They use the unlicensed 2.4GHz waveband

That means you do not need to get a licence to use that frequency at low power

This was a frequency that was otherwise unusable commercially and is subject to interference from microwave ovens and other things

Wireless 802.11

They use the unlicensed 2.4GHz waveband

That means you do not need to get a licence to use that frequency at low power

This was a frequency that was otherwise unusable commercially and is subject to interference from microwave ovens and other things

And the frequency fell within the capabilities of low-power chips that were buildable at the time

Wireless 802.11

		channel bandwidth	rate
WiFi 1	11b	20MHz	11Mb/s
WiFi 2	11a	20MHz	54Mb/s
WiFi 3	11g	20MHz	54Mb/s
WiFi 4	11n	40MHz	top 150Mb/s, typical 72Mb/s
WiFi 5	11ac	80MHz	160MHz optional, top 6.9Gb/s, typical 433Mb/s
WiFi 6*	11ax	160MHz	top 9.6Gb/s, typical 600Mb/s
WiFi 7	11be	320MHz	ratified 2024?

*WiFi 6E uses the newly released 6GHz waveband (lots of new spectrum)

Wireless 802.11

Wider channels give more bandwidth, but are more likely to be interfered with by environmental noise

Wireless 802.11

Wider channels give more bandwidth, but are more likely to be interfered with by environmental noise

Improvements are achieved through more sophisticated encodings and using more wireless channels simultaneously

Wireless 802.11

Each will fall back to previous standards to maintain compatability with earlier devices

Wireless 802.11

Each will fall back to previous standards to maintain compatability with earlier devices

For example, a 5GHz signal has problems going through walls, so 11a can fall back to 11b if you move to the next room

Wireless 802.11

Each will fall back to previous standards to maintain compatability with earlier devices

For example, a 5GHz signal has problems going through walls, so 11a can fall back to 11b if you move to the next room

Exercise Look these up. Particularly the use of multiple aerials for *beamforming* and *spacial multiplexing*

Wireless 802.11

802.11 hardware is branded “Wi-Fi”, which is actually a certificate of interopability given to manufacturers whose equipment demonstrably works with other manufacturers’

Wireless 802.11

802.11 hardware is branded “Wi-Fi”, which is actually a certificate of interopability given to manufacturers whose equipment demonstrably works with other manufacturers’

Administered by the Wi-Fi Alliance, a consortium of interested companies

Wireless 802.11

The bits in 802.11 are not simply transmitted directly: there is a lot of environmental interference to overcome

Wireless 802.11

The bits in 802.11 are not simply transmitted directly: there is a lot of environmental interference to overcome

Instead the signal is spread over many frequencies using variety of techniques collectively called *spread spectrum*

Wireless 802.11

The bits in 802.11 are not simply transmitted directly: there is a lot of environmental interference to overcome

Instead the signal is spread over many frequencies using variety of techniques collectively called *spread spectrum*

Exercise Read about *Direct Sequence Spread Spectrum* (DSSS)

Wireless 802.11

The bits in 802.11 are not simply transmitted directly: there is a lot of environmental interference to overcome

Instead the signal is spread over many frequencies using variety of techniques collectively called *spread spectrum*

Exercise Read about *Direct Sequence Spread Spectrum* (DSSS)

Exercise And read about film actress Hedy Lamarr

Wireless 802.11

For Wi-Fi, the allocated frequency band (2.4–2.5GHz) is split into 14 overlapping 22MHz channels each centred on specified frequencies

Wireless 802.11

For Wi-Fi, the allocated frequency band (2.4–2.5GHz) is split into 14 overlapping 22MHz channels each centred on specified frequencies

The number of channels available depends on the country

- Most of Europe: 13
- North America: 11
- Japan: 14

Wireless 802.11

Channel	GHz
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Wireless 802.11

These channels are 5MHz apart, so neighbouring channels overlap (as they are 22MHz wide) and interfere. Therefore you need to take care which channels you use

Wireless 802.11

These channels are 5MHz apart, so neighbouring channels overlap (as they are 22MHz wide) and interfere. Therefore you need to take care which channels you use

There are recommendations on using channels

Wireless 802.11

- Separate channels by at least 2 (e.g., use 1 and 4) to reduce interference

Wireless 802.11

- Separate channels by at least 2 (e.g., use 1 and 4) to reduce interference
- Separate by 4 (e.g., use 1 and 6) to have no interference at all

Wireless 802.11

- Separate channels by at least 2 (e.g., use 1 and 4) to reduce interference
- Separate by 4 (e.g., use 1 and 6) to have no interference at all
- This means we can have three non-interfering co-located networks on channels 1, 6 and 11

Wireless 802.11

Separating networks physically gives more leeway:

Wireless 802.11

Separating networks physically gives more leeway:

- Separate by 1 (e.g., use 1 and 3) if the networks are more than 40m apart

Wireless 802.11

Separating networks physically gives more leeway:

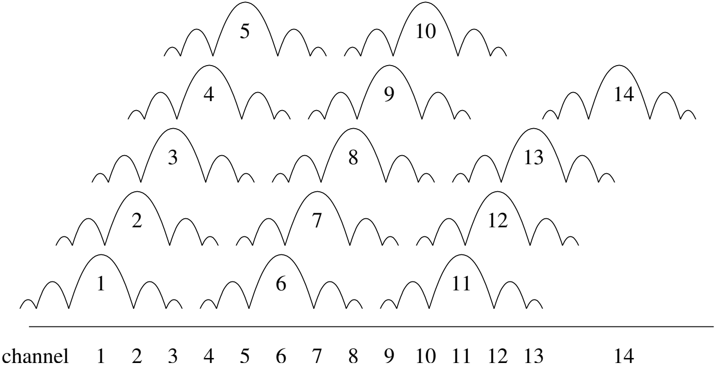
- Separate by 1 (e.g., use 1 and 3) if the networks are more than 40m apart
- Adjacent channels (e.g., use 1 and 2) are OK over 100m

Wireless 802.11

Separating networks physically gives more leeway:

- Separate by 1 (e.g., use 1 and 3) if the networks are more than 40m apart
- Adjacent channels (e.g., use 1 and 2) are OK over 100m
- Channels can be reused when the networks are sufficiently separated

Wireless 802.11



Overlapping WiFi channels at 2.4GHz

Wireless 802.11

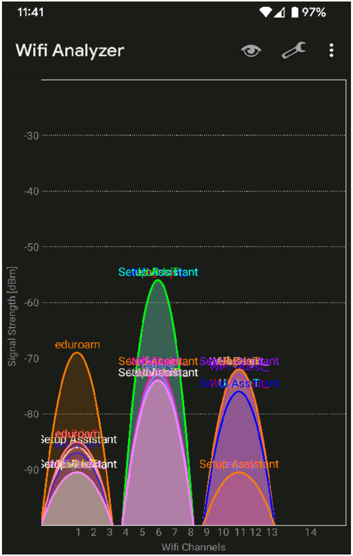
More subtle channel allocations allow a little overlap (e.g., using channels 1 and 3) that have a little interference, but a greater overall aggregate bandwidth

Wireless 802.11

More subtle channel allocations allow a little overlap (e.g., using channels 1 and 3) that have a little interference, but a greater overall aggregate bandwidth

Exercise Mobile phones have wireless apps that display the wireless environment. Walk around and see what it is like

Wireless 802.11



WiFi Analyzer app

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

This is similar to CSMA/CD, but with a big difference

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

This is similar to CSMA/CD, but with a big difference

- Carrier sense: to deal with the common case of non-hidden hosts, first listen for a signal

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

This is similar to CSMA/CD, but with a big difference

- Carrier sense: to deal with the common case of non-hidden hosts, first listen for a signal
- If free, send a packet

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

This is similar to CSMA/CD, but with a big difference

- Carrier sense: to deal with the common case of non-hidden hosts, first listen for a signal
- If free, send a packet
- If busy, wait until the end of the transmission and then enter a *contention period*: wait a random period

CSMA/CA

So 802.11 can’t use CSMA/CD, like wired Ethernet

Instead, it uses carrier sense, multiple access, *collision avoidance* (CSMA/CA)

This is similar to CSMA/CD, but with a big difference

- Carrier sense: to deal with the common case of non-hidden hosts, first listen for a signal
- If free, send a packet
- If busy, wait until the end of the transmission and then enter a *contention period*: wait a random period
- Go back to carrier sense

CSMA/CA

Waiting for the contention period is the collision avoidance

CSMA/CA

Waiting for the contention period is the collision avoidance

A random wait mean that several hosts wanting to transmit are unlikely to all start transmitting simultaneously

CSMA/CA

Waiting for the contention period is the collision avoidance

A random wait mean that several hosts wanting to transmit are unlikely to all start transmitting simultaneously

We are trying to avoid a collision in advance rather than detect one after the fact: we know that signal detection is problematic

CSMA/CA

Waiting for the contention period is the collision avoidance

A random wait mean that several hosts wanting to transmit are unlikely to all start transmitting simultaneously

We are trying to avoid a collision in advance rather than detect one after the fact: we know that signal detection is problematic

But collision avoidance does not *guarantee* no collisions, particularly with hidden hosts, so we need more

CSMA/CA

Thus, on successful receipt of a packet, a host will broadcast an acknowledgement (ACK) packet

CSMA/CA

Thus, on successful receipt of a packet, a host will broadcast an acknowledgement (ACK) packet

This is just a packet to inform the sender that everything worked well and there was, in fact, no collision or other loss

CSMA/CA

Thus, on successful receipt of a packet, a host will broadcast an acknowledgement (ACK) packet

This is just a packet to inform the sender that everything worked well and there was, in fact, no collision or other loss

If the sender never gets the ACK, it will resend, starting from the CS again

CSMA/CA

Thus, on successful receipt of a packet, a host will broadcast an acknowledgement (ACK) packet

This is just a packet to inform the sender that everything worked well and there was, in fact, no collision or other loss

If the sender never gets the ACK, it will resend, starting from the CS again

This ACK is important, as measurements have found loss rates on the order of 30%

CSMA/CA

Thus, on successful receipt of a packet, a host will broadcast an acknowledgement (ACK) packet

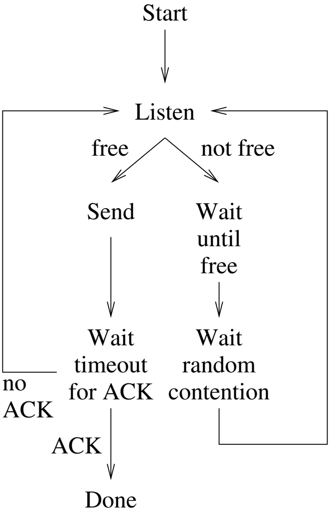
This is just a packet to inform the sender that everything worked well and there was, in fact, no collision or other loss

If the sender never gets the ACK, it will resend, starting from the CS again

This ACK is important, as measurements have found loss rates on the order of 30%

Note the ACK is also visible to everyone in range of the destination, giving extra indication to others when a transmission has finished

CSMA/CA



CSMA/CA flowchart

CSMA/CA

Exercise Compare and contrast the CSMA/CA flowchart with the CSMA/CD flowchart