Cat 5e and Cat 6/6a is what you will find most widely used today

Cat 5e and Cat 6/6a is what you will find most widely used today

Cat 6a is roughly the same price as Cat 5e and gives some future-proofing

Cat 5e and Cat 6/6a is what you will find most widely used today

Cat 6a is roughly the same price as Cat 5e and gives some future-proofing

In particular, Cat 5e is at the edge of supporting 1Gb and bad installs can easily cause problems, dropping the speed to 100Mb. Cat6 has more "headroom"

There is no testing body to ensure the Category standards are met, so anyone can call any cable anything they like

There is no testing body to ensure the Category standards are met, so anyone can call any cable anything they like

Reports say that 80% of Cat 6 (and higher) cables (even expensive ones) on sale do not meet the relevant standard; many even fail the Cat 5e test

The NBASE-T Alliance claims "an estimated 70 billion meters of cabling, which is more than 10 trips to Pluto" has been installed

The NBASE-T Alliance claims "an estimated 70 billion meters of cabling, which is more than 10 trips to Pluto" has been installed

So people are trying hard to make new Ethernet standards that don't require ripping out the old cabling and installing new

The NBASE-T Alliance claims "an estimated 70 billion meters of cabling, which is more than 10 trips to Pluto" has been installed

So people are trying hard to make new Ethernet standards that don't require ripping out the old cabling and installing new

Thus we have intermediate curiosities like 2.5GBaseT and 5GBaseT (standards developed *after* 10GBaseT), that run on lower-spec cables

The NBASE-T Alliance claims "an estimated 70 billion meters of cabling, which is more than 10 trips to Pluto" has been installed

So people are trying hard to make new Ethernet standards that don't require ripping out the old cabling and installing new

Thus we have intermediate curiosities like 2.5GBaseT and 5GBaseT (standards developed *after* 10GBaseT), that run on lower-spec cables

The higher speeds and more expensive cabling is usually found only in specialist installations like data centres, HPC and Internet exchanges
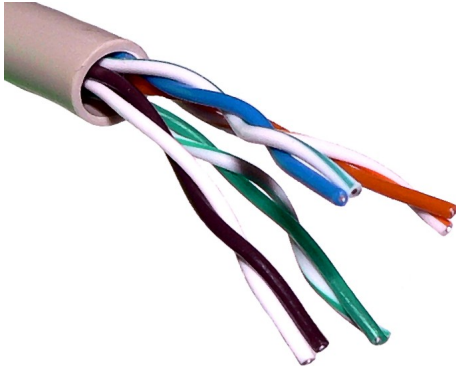
Networks
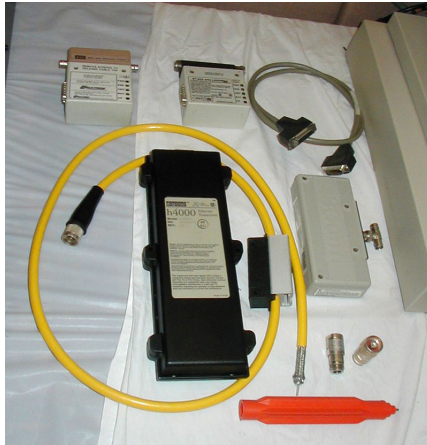
10Base5 Transceivers

By Robert.Harker at English Wikipedia, CC BY-SA 2.5, `https://commons.wikimedia.org/w/index.php?curid=9891521`

Networks
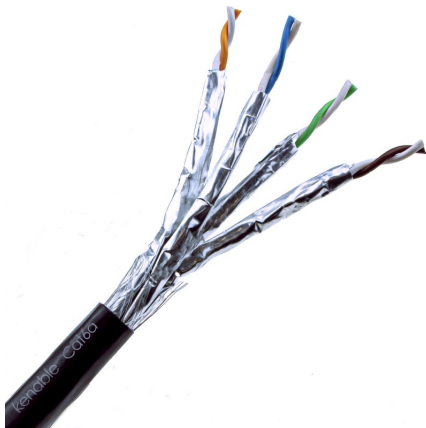## Ethernet

UTP cable (Wikipedia)

Screened Shielded Cat 6a (Kenable)

Networks
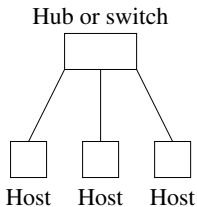
Ethernet

Twisted pair differs from coaxial Ethernet in that it uses *hubs* or (these days) *switches* to connect multiple hosts together

Twisted pair differs from coaxial Ethernet in that it uses *hubs* or (these days) *switches* to connect multiple hosts together

Hosts connected using a hub or switch

Hubs were simple electrical repeaters. An incoming signal is sent out on all outputs

Networks
Ethernet

Hubs were simple electrical repeaters. An incoming signal is sent out on all outputs

There is a single *collision domain* as all hosts see all signals: any pair of signals between any hosts will collide

Networks
Ethernet

Hubs were simple electrical repeaters. An incoming signal is sent out on all outputs

There is a single *collision domain* as all hosts see all signals: any pair of signals between any hosts will collide

The available bandwidth is shared amongst all the hosts

A switch understands the link layer and can track where a destination host is. It only sends the signal out on the single output that has the destination host

A switch understands the link layer and can track where a destination host is. It only sends the signal out on the single output that has the destination host

Hub vs Switch

This requires the switch to read and understand the MAC addresses in the frames and to track the socket where each host is plugged in

This requires the switch to read and understand the MAC addresses in the frames and to track the socket where each host is plugged in

This is extra complexity in the switch hardware, but reduces the number of possible collisions, increasing throughput

This requires the switch to read and understand the MAC addresses in the frames and to track the socket where each host is plugged in

This is extra complexity in the switch hardware, but reduces the number of possible collisions, increasing throughput

Each output cable is now a separate collision domain
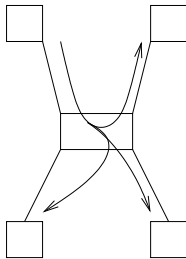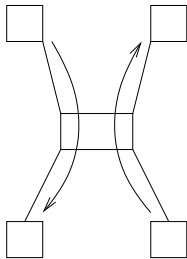
Networks
Ethernet

This requires the switch to read and understand the MAC addresses in the frames and to track the socket where each host is plugged in

This is extra complexity in the switch hardware, but reduces the number of possible collisions, increasing throughput

Each output cable is now a separate collision domain

The full bandwidth is available on *each* output, simultaneously

This requires the switch to read and understand the MAC addresses in the frames and to track the socket where each host is plugged in

This is extra complexity in the switch hardware, but reduces the number of possible collisions, increasing throughput

Each output cable is now a separate collision domain

The full bandwidth is available on *each* output, simultaneously

Collisions only if two hosts send to the same destination simultaneously
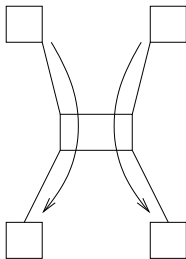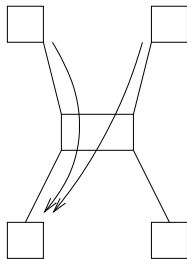
No collision   Collision

Collisions in switches

If an output is busy, rather than have a collision, a switch may choose to *store and forward* a packet later when that output is free

If an output is busy, rather than have a collision, a switch may choose to *store and forward* a packet later when that output is free

Now there can be no collisions and we might think we can do away with CSMA/CD

If an output is busy, rather than have a collision, a switch may choose to *store and forward* a packet later when that output is free

Now there can be no collisions and we might think we can do away with CSMA/CD

But buffers in the switch can fill up and then packets would have to be dropped by the switch

If an output is busy, rather than have a collision, a switch may choose to *store and forward* a packet later when that output is free

Now there can be no collisions and we might think we can do away with CSMA/CD

But buffers in the switch can fill up and then packets would have to be dropped by the switch

Instead the switch can send a jamming signal on an input to get it to back off and resend later: thus still using CSMA/CD

Some switches can *cut through*, sending the start of the packet onwards before the tail has arrived: more complex, but less latency through the switch

Some switches can *cut through*, sending the start of the packet onwards before the tail has arrived: more complex, but less latency through the switch

Switches can run *full duplex*, with independent inward and outward traffic to each host

Some switches can *cut through*, sending the start of the packet onwards before the tail has arrived: more complex, but less latency through the switch

Switches can run *full duplex*, with independent inward and outward traffic to each host

This gives *twice* the total bandwidth of previously

Some switches can *cut through*, sending the start of the packet onwards before the tail has arrived: more complex, but less latency through the switch

Switches can run *full duplex*, with independent inward and outward traffic to each host

This gives *twice* the total bandwidth of previously

No collisions are possible between opposing traffic as inward and outward traffic runs over different twisted pairs (below 1Gb)

Ethernet is moving faster: 10Mb/s to 1Gb/s and more, all using the same basic CSMA/CD protocol, but using differing electrical signalling

Ethernet is moving faster: 10Mb/s to 1Gb/s and more, all using the same basic CSMA/CD protocol, but using differing electrical signalling

Ethernet cards can autonegotiate to select optimum speed

Ethernet is moving faster: 10Mb/s to 1Gb/s and more, all using the same basic CSMA/CD protocol, but using differing electrical signalling

Ethernet cards can autonegotiate to select optimum speed

But it's not just a case of increasing the frequency of the signal, there are other complications to get around the electrical limitations of the cables (discussed later, if we have time)

Ethernet with speeds above 100Gb/s are called *Terabit Ethernet*

Ethernet with speeds above 100Gb/s are called *Terabit Ethernet*

200Gb/s and 400Gb/s Ethernet are available, while 800Gb/s and 1.6Tb/s are under development

Ethernet with speeds above 100Gb/s are called *Terabit Ethernet*

200Gb/s and 400Gb/s Ethernet are available, while 800Gb/s and 1.6Tb/s are under development

Mostly optical fibre rather than copper twisted pair, but some support for very short (e.g., 2m) copper connections

Ethernet with speeds above 100Gb/s are called *Terabit Ethernet*

200Gb/s and 400Gb/s Ethernet are available, while 800Gb/s and 1.6Tb/s are under development

Mostly optical fibre rather than copper twisted pair, but some support for very short (e.g., 2m) copper connections

Not likely to be seen in the home for many years!

Networks
Ethernet

Addendum: October 2023

Some ISPs have just announced they will sell $> 1Gb/s$ FTTH products, namely 1.6Gb/s (EE) and 2.2Gb/s (Vodafone in 2024), so providing a "True Gigabit" to the home

To take advantage of this your home network will need a 2.5Gb/s switch: these are available at a moderate price premium over 1Gb/s switches

Your PC or laptop will need a 2.5Gb/s port: you can get USB-C to 2.5Gb/s adaptors reasonably cheaply

Cat 6a will be fine (Cat 5e *should* work, too)

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)

Collaborating with the International Telecommunication Union (ITU)

Wireless

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

USA has the *Federal Communication Commission* (FCC)

Collaborating with the International Telecommunication Union (ITU)

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 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:

A's range   C's range
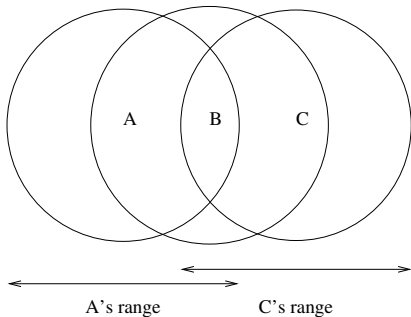
Extents of visibility

Hidden host

Wireless Problems

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

A's range   C's range

Extents of visibility

Hidden host
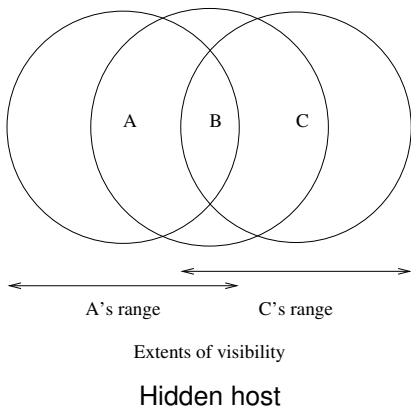
Hosts A can B can "see" each other; B and C can see each other, but A cannot see C, so A cannot tell if its packets to B are colliding with C's to B

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 for CD to work

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

Wi-Fi 7 (802.11be) is due in 2024

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

		Freqs GHz	Signalling rate
WiFi 1	11	2.4	2Mb/s
WiFi 2	11b	2.4	11Mb/s
WiFi 3	11g	2.4	54Mb/s
WiFi 3	11a	5	54Mb/s
WiFi 4	11n	2.4,5	600Mb/s
WiFi 5	11ac	5	6.9Gb/s
WiFi 6	11ax	2.4,5	9.6Gb/s
WiFi 6E	11ax	6	9.6Gb/s
(WiFi 7	11be	2.4,5,6	46Gb/s)

Wireless 802.11

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

Wireless 802.11

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

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

Wireless 802.11

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

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

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

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

Those are central frequencies, with each channel being 22MHz wide

Wireless 802.11

Those are central frequencies, with each channel being 22MHz wide

So, for example, channel 1 is 2.401–2.423GHz and channel 2 is 2.406–2.428GHz

Wireless 802.11

Those are central frequencies, with each channel being 22MHz wide

So, for example, channel 1 is 2.401–2.423GHz and channel 2 is 2.406–2.428GHz

The 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

Those are central frequencies, with each channel being 22MHz wide

So, for example, channel 1 is 2.401–2.423GHz and channel 2 is 2.406–2.428GHz

The 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

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
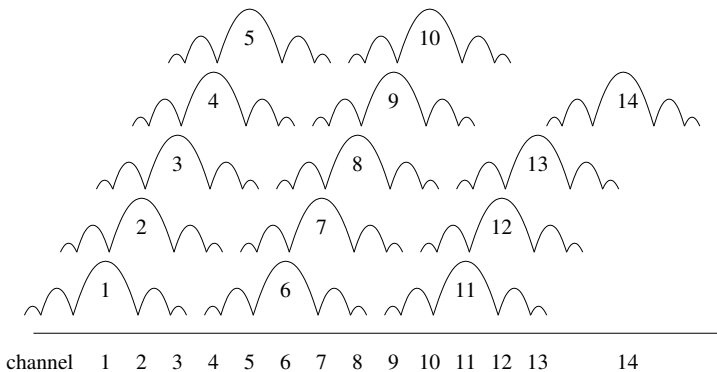
Overlapping WiFi channels at 2.4GHz
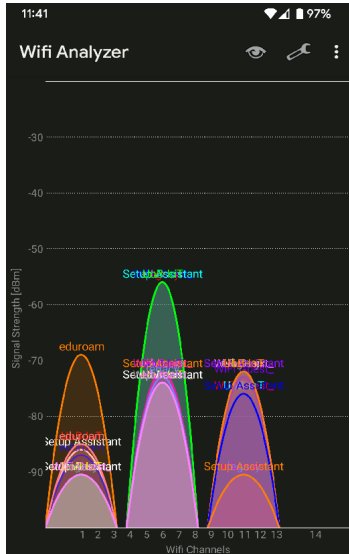
Wireless 802.11

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