CSMA/CA

Why use collision avoidance rather than collision detection?

CSMA/CA

Why use collision avoidance rather than collision detection?

Clearly, the contention period means more latency in transmission

CSMA/CA

Why use collision avoidance rather than collision detection?

Clearly, the contention period means more latency in transmission

We do it because with wireless, collisions can be very hard to detect

CSMA/CA

Why use collision avoidance rather than collision detection?

Clearly, the contention period means more latency in transmission

We do it because with wireless, collisions can be very hard to detect

With Ethernet, detecting another host's signal on a wire is easy as the power of its signal is roughly the same as yours

CSMA/CA

In contrast, detecting another host's radio signal can be very difficult as it can be a tiny fraction of the power of yours, and your signal will drown out the colliding signal and make it undetectable

CSMA/CA

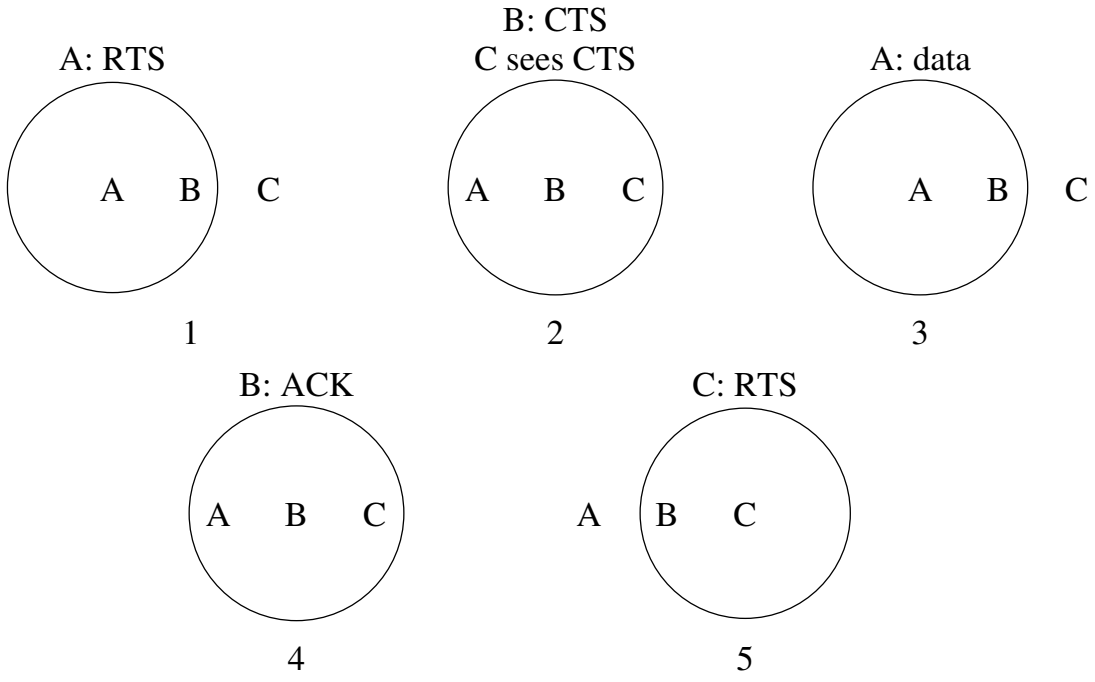
In contrast, detecting another host's radio signal can be very difficult as it can be a tiny fraction of the power of yours, and your signal will drown out the colliding signal and make it undetectable

Recall the wide range of power that Wi-Fi signals encompass: another destination might be transmitting quite powerfully, but its signal can be very small by the time it reaches you

Wi-Fi

To help further with the visibility problem, there is optional *RTS/CTS handshaking*, which can improve performance in certain circumstances

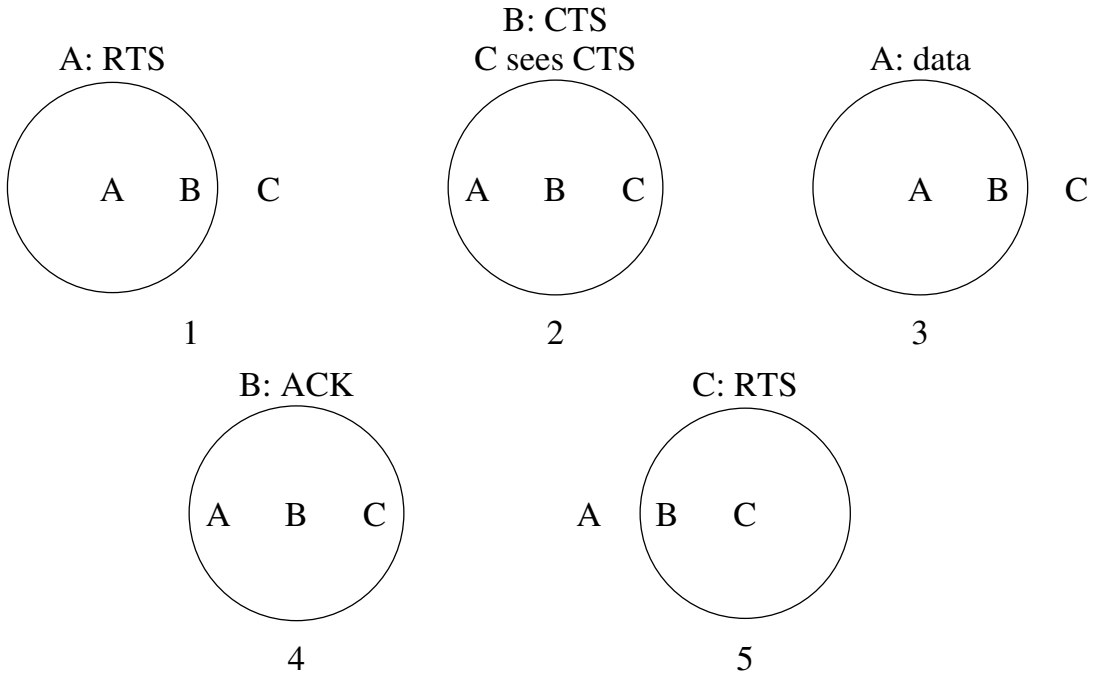
RTS/CTS



RTS/CTS handshaking

1. Before sending a data packet the source A can send a *request to send* (RTS) packet to B;

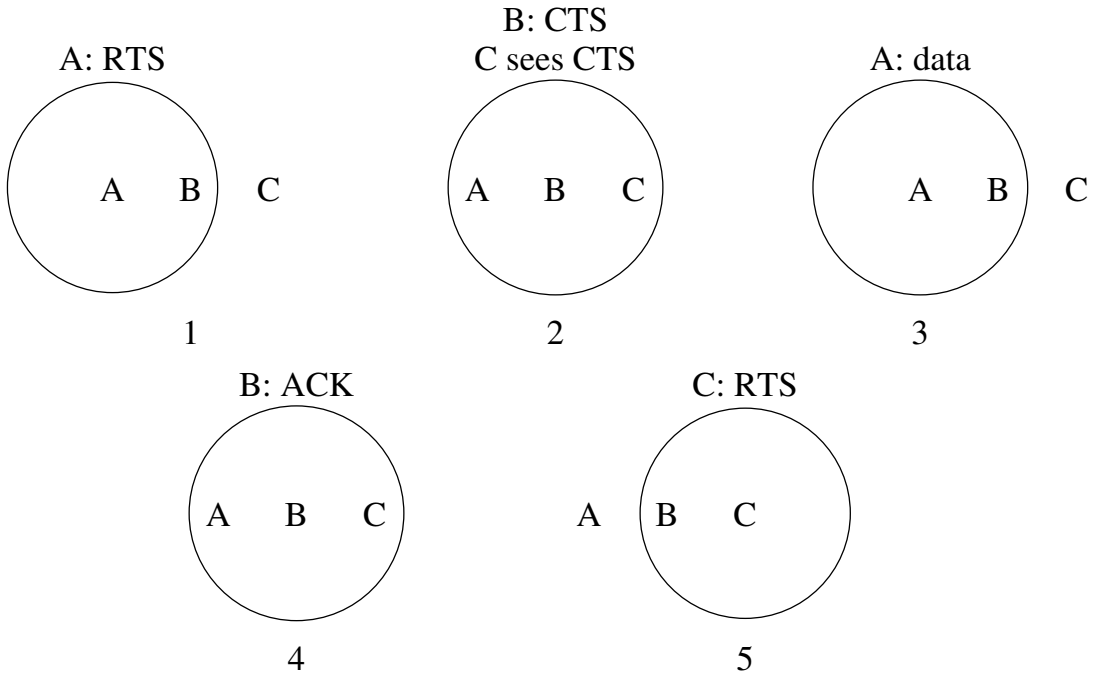
RTS/CTS



RTS/CTS handshaking

2. If the destination B is happy (it is not already receiving from another host that A cannot see) it responds with a *clear to send* (CTS) packet;

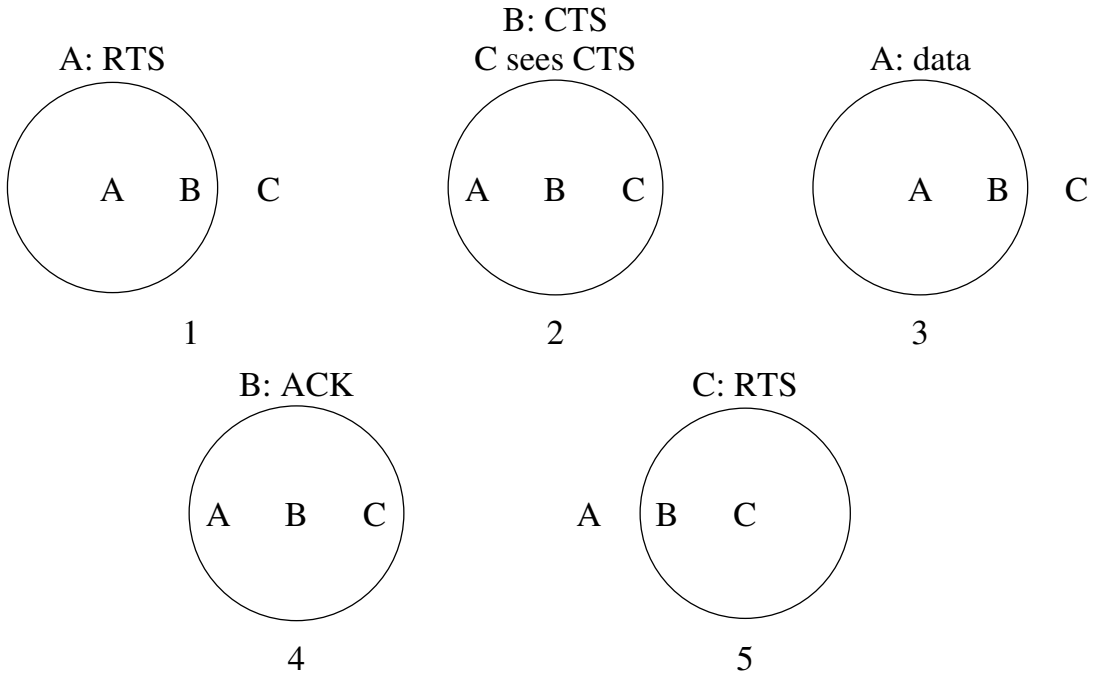
RTS/CTS



RTS/CTS handshaking

2. Every other host within the range of the destination will see the CTS and so know not to send themselves;

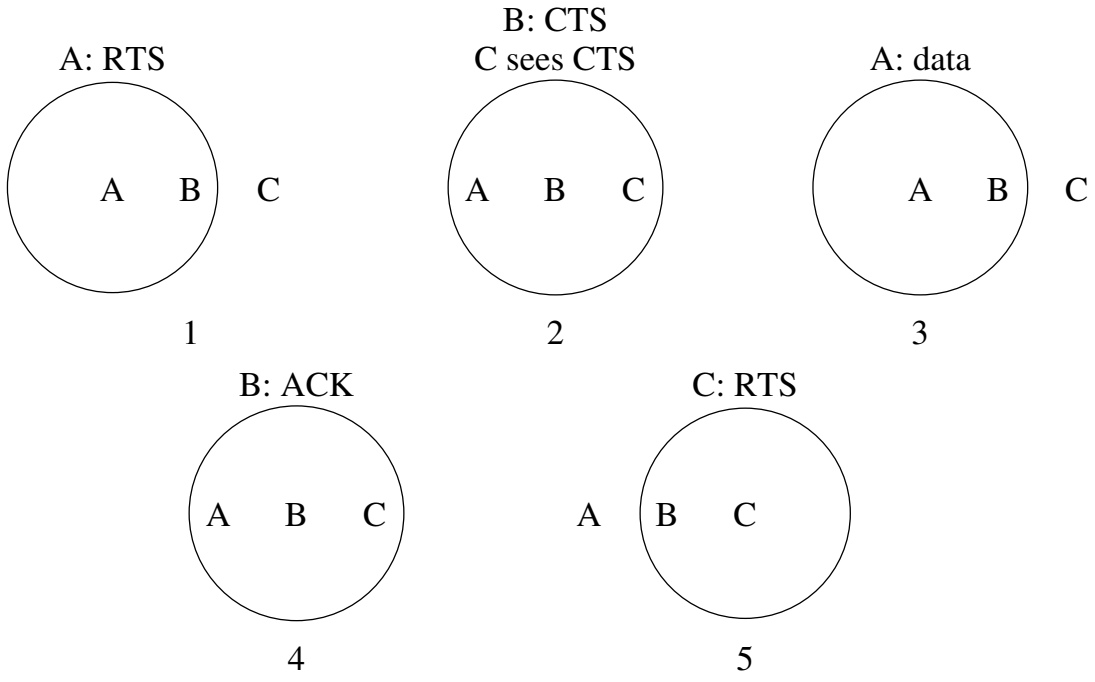
RTS/CTS



RTS/CTS handshaking

3. The RTS and CTS contain the length of the desired transmission so other hosts know how long they will have to wait;

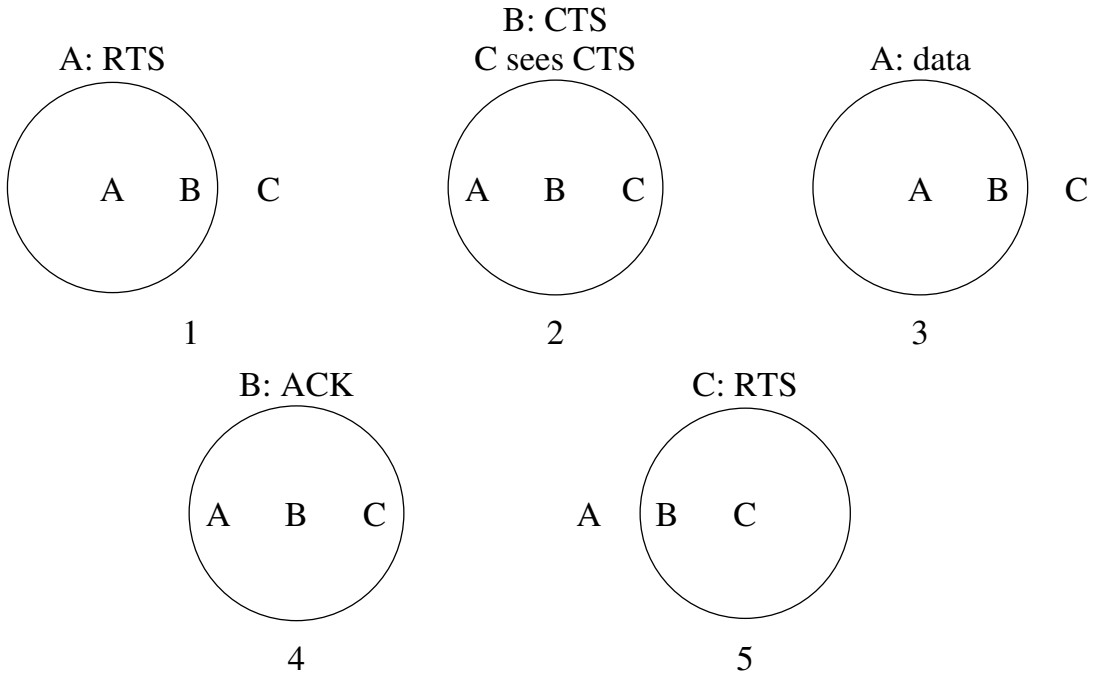
RTS/CTS



RTS/CTS handshaking

4. Similarly, the final ACK is visible to everyone;

RTS/CTS



RTS/CTS handshaking

5. Then C can start with its own RTS

RTS/CTS

This means there is even more latency overhead before data starts to be transmitted, so RTS/CTS can be switched off or on as required:

RTS/CTS

This means there is even more latency overhead before data starts to be transmitted, so RTS/CTS can be switched off or on as required:

RTS/CTS always on: good for large or busy networks

RTS/CTS

This means there is even more latency overhead before data starts to be transmitted, so RTS/CTS can be switched off or on as required:

RTS/CTS always on: good for large or busy networks

RTS/CTS never on: good for small or lightly loaded networks where every host can see all other hosts

RTS/CTS

This means there is even more latency overhead before data starts to be transmitted, so RTS/CTS can be switched off or on as required:

RTS/CTS always on: good for large or busy networks

RTS/CTS never on: good for small or lightly loaded networks where every host can see all other hosts

RTS/CTS for large packets only: a compromise that reduces the relatively large overhead for small packets

Wireless Rates

Although 802.11b is nominally 11Mb/s and 802.11g is nominally 54Mb/s remember these are the signalling rates, not the data rates

Wireless Rates

Although 802.11b is nominally 11Mb/s and 802.11g is nominally 54Mb/s remember these are the signalling rates, not the data rates

The signalling rate is the raw bit rate over the airwaves: a lot of that is consumed in overheads

Wireless Rates

Although 802.11b is nominally 11Mb/s and 802.11g is nominally 54Mb/s remember these are the signalling rates, not the data rates

The signalling rate is the raw bit rate over the airwaves: a lot of that is consumed in overheads

Realistically, 802.11b gives about 3 to 4Mb/s and 802.11g about 20Mb/s

Wireless Rates

Although 802.11b is nominally 11Mb/s and 802.11g is nominally 54Mb/s remember these are the signalling rates, not the data rates

The signalling rate is the raw bit rate over the airwaves: a lot of that is consumed in overheads

Realistically, 802.11b gives about 3 to 4Mb/s and 802.11g about 20Mb/s

Some of the later 802.11 standard improve speeds by reducing overheads (as well as using better encodings)

802.11

Exercise 802.11ac (branded “Wi-Fi 5”) is common and 11ax (“Wi-Fi 6”) hardware becoming more common. Read up on what they promise and what they deliver

Wireless Networks

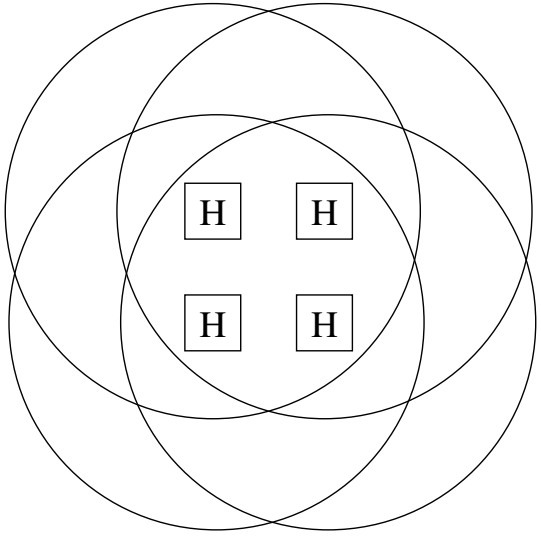
While the use of access points is common, this is not the only way to set up a wireless network

Wireless Networks

While the use of access points is common, this is not the only way to set up a wireless network

802.11 can be arranged in point-to-point networks called *Ad-Hoc* or *Independent Basic Service Set* (IBSS)

Wireless Networks

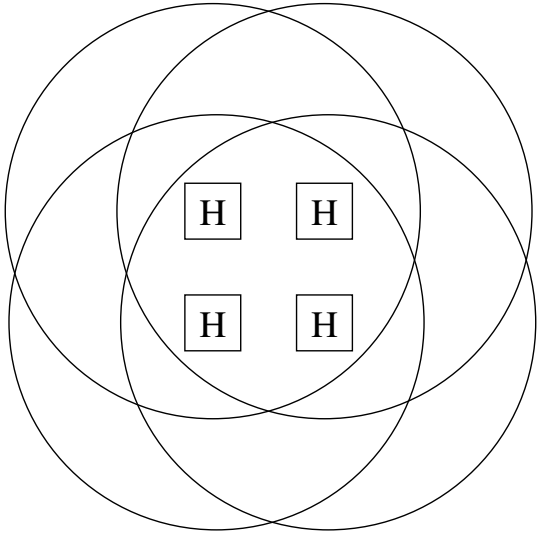


Point−to−point connections

IBSS

Ad-Hoc network

Wireless Networks



Point–to–point connections

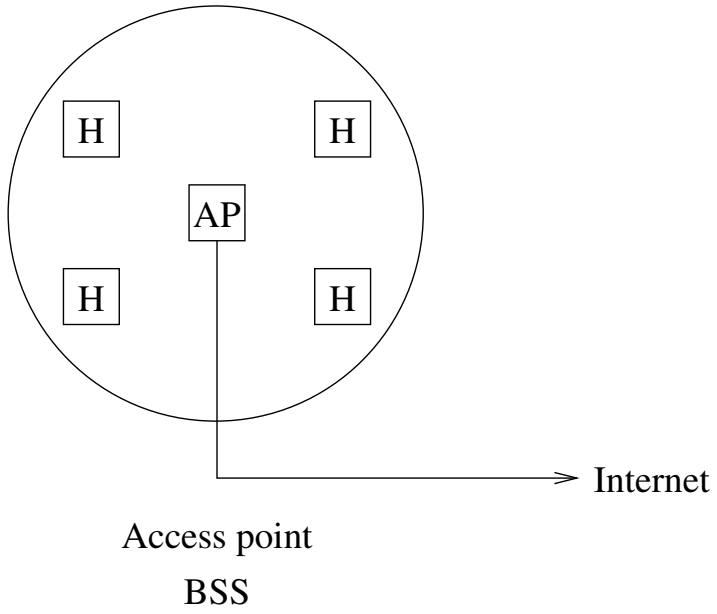
IBSS

Ad-Hoc network

Each host communicates directly with each other without an access point

Wireless Networks

But the usual Wi-Fi network is a *Infrastructure* or *Basic Service Set* (BSS), where a central hub (*access point*) relays traffic between hosts



Usual access point setup

Wireless Networks

This is more expensive to set up (as you have to buy an AP), but covers a larger area

Wireless Networks

This is more expensive to set up (as you have to buy an AP), but covers a larger area

And is easier to manage by non-technical users

Wireless Networks

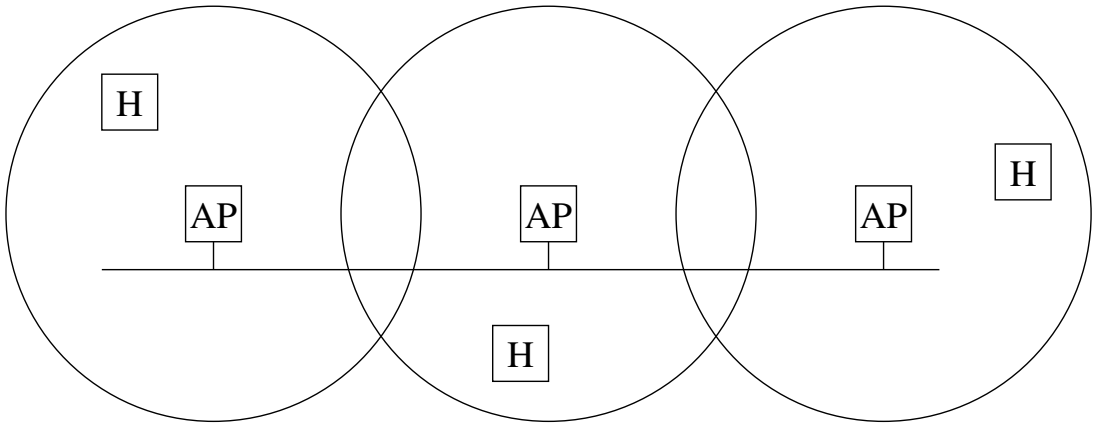
This is more expensive to set up (as you have to buy an AP), but covers a larger area

And is easier to manage by non-technical users

Also the AP can connect into a wired network and so the rest of the Internet

Wireless Networks

Extended Service Set (ESS) connects several APs by a wired network

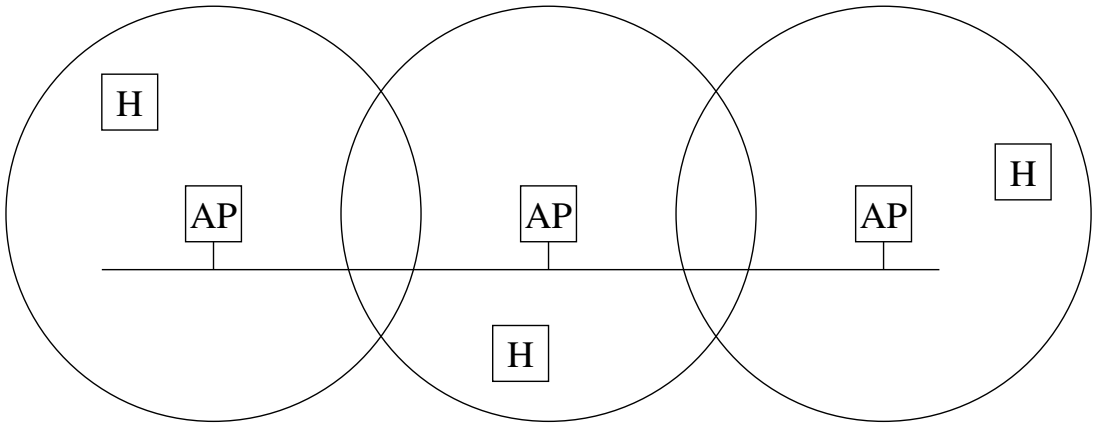


ESS

Extended network

Wireless Networks

Extended Service Set (ESS) connects several APs by a wired network



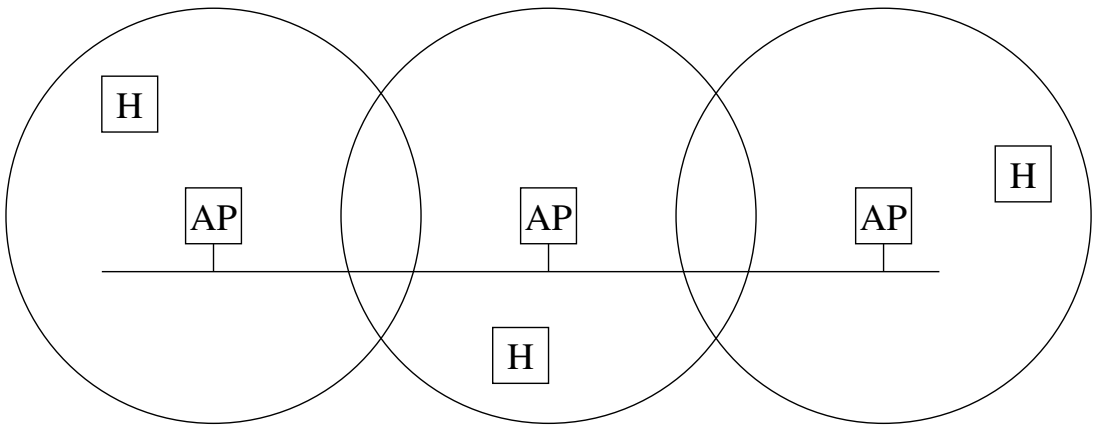
ESS

Extended network

This allows hosts to roam and things can be configured to handoff automatically between APs if the required authentication infrastructure is set up in the APs

Wireless Networks

Extended Service Set (ESS) connects several APs by a wired network



ESS

Extended network

This allows hosts to roam and things can be configured to handoff automatically between APs if the required authentication infrastructure is set up in the APs

An ESS can cover an area as large as you like

Wireless Networks

Exercise Read about *Wi-Fi Direct*, another peer-to-peer wireless connection between hosts, often used as a device setup mechanism. Compare with Ad-Hoc mode

Exercise Read about Mesh networks

Wireless Security

While we are talking about authentication. . .

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

We have two issues:

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

We have two issues:

- is this machine allowed to connect to this network: authentication

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

We have two issues:

- is this machine allowed to connect to this network: authentication
- ensure data in transit is kept secret: privacy

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

We have two issues:

- is this machine allowed to connect to this network: authentication
- ensure data in transit is kept secret: privacy

On Ethernet, being plugged into the network is the “authentication”, while the physical security of the network is the “privacy”

Wireless Security

While we are talking about authentication. . .

Wireless packets are readable by anybody in the neighbourhood, so security is essential in a wireless network

We have two issues:

- is this machine allowed to connect to this network: authentication
- ensure data in transit is kept secret: privacy

On Ethernet, being plugged into the network is the “authentication”, while the physical security of the network is the “privacy”

But only private from people not on the network!

Wireless Security

Original 802.11 employed the *Wired Equivalent Privacy* (WEP) encryption scheme

Wireless Security

Original 802.11 employed the *Wired Equivalent Privacy* (WEP) encryption scheme

Both ends of a communication share a secret key that is used to encrypt the traffic between them

Wireless Security

Original 802.11 employed the *Wired Equivalent Privacy* (WEP) encryption scheme

Both ends of a communication share a secret key that is used to encrypt the traffic between them

WEP is now easily breakable: after collecting a modest amount of traffic the system can be broken

Wireless Security

Original 802.11 employed the *Wired Equivalent Privacy* (WEP) encryption scheme

Both ends of a communication share a secret key that is used to encrypt the traffic between them

WEP is now easily breakable: after collecting a modest amount of traffic the system can be broken

As can its successor, *Wi-Fi Protected Access* (WPA)

Wireless Security

Currently we use mostly WPA2, (IEEE 802.11i-2004)

Wireless Security

Currently we use mostly WPA2, (IEEE 802.11i-2004)

Exercise Read about the break of the WPA2 protocol (Oct 2017)

Wireless Security

Currently we use mostly WPA2, (IEEE 802.11i-2004)

Exercise Read about the break of the WPA2 protocol (Oct 2017)

Exercise Read about the new WPA3

Wireless Security

Two major ways to set up authentication are

Wireless Security

Two major ways to set up authentication are

- WPA-Personal: also called WPA-PSK (pre-shared key), where an access point has a secret key, and a host authenticates directly with the AP using the secret key

Wireless Security

Two major ways to set up authentication are

- WPA-Personal: also called WPA-PSK (pre-shared key), where an access point has a secret key, and a host authenticates directly with the AP using the secret key
- WPA-Enterprise (802.11X): requires a separate authentication server (typically a RADIUS server) that the AP will contact. Much more fiddly to manage, but allows roaming across an ESS. Also roaming across institutions using hierarchical RADIUS servers

Wireless Security

Two major ways to set up authentication are

- WPA-Personal: also called WPA-PSK (pre-shared key), where an access point has a secret key, and a host authenticates directly with the AP using the secret key
- WPA-Enterprise (802.11X): requires a separate authentication server (typically a RADIUS server) that the AP will contact. Much more fiddly to manage, but allows roaming across an ESS. Also roaming across institutions using hierarchical RADIUS servers

We usually find BSS using WPA-PSK and ESS using WPA-Enterprise, but either can use either

Wireless Security

For WPA-PSK the secret key is usually derived from a password for ease of use

Wireless Security

For WPA-PSK the secret key is usually derived from a password for ease of use

The password is communicated off-line, e.g., written down somewhere

Wireless Security

For WPA-PSK the secret key is usually derived from a password for ease of use

The password is communicated off-line, e.g., written down somewhere

Everybody on the network shares the same key/password; authentication is done in the AP

Wireless Security

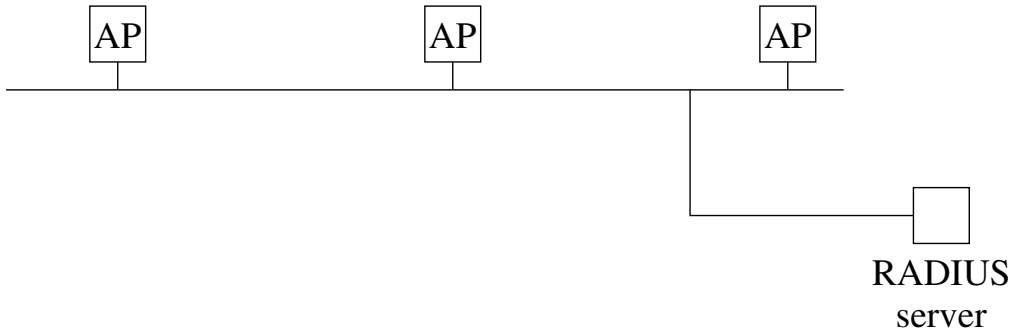
For WPA-PSK the secret key is usually derived from a password for ease of use

The password is communicated off-line, e.g., written down somewhere

Everybody on the network shares the same key/password; authentication is done in the AP

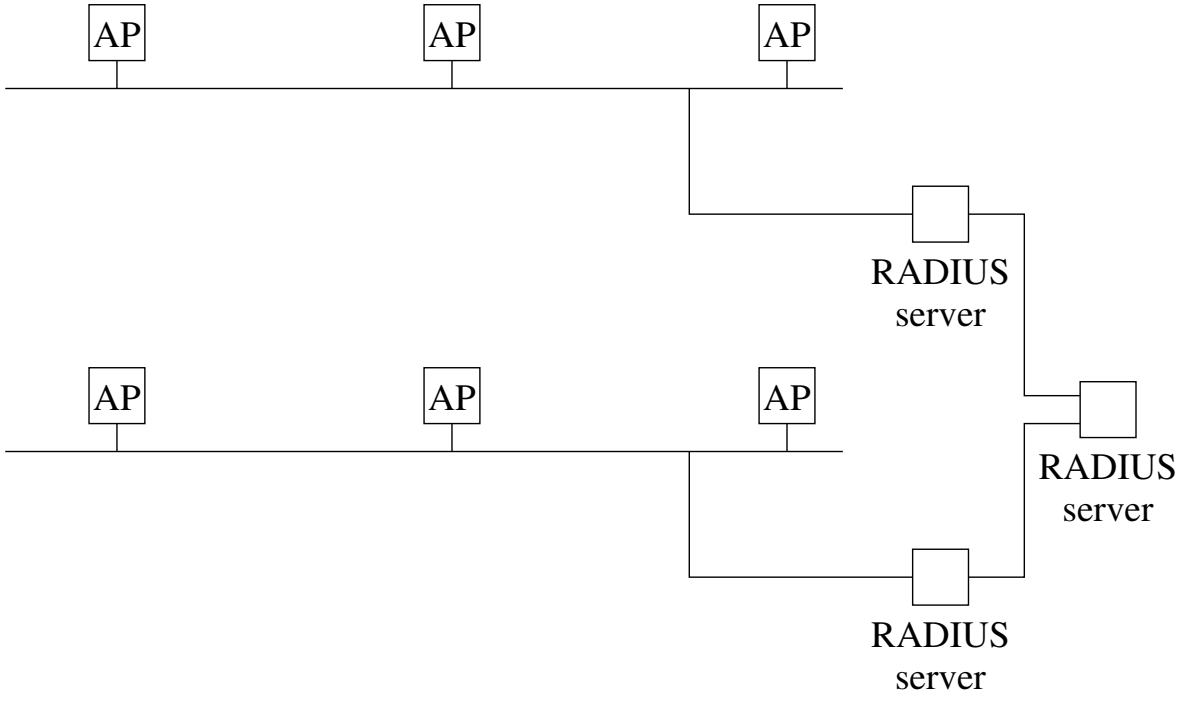
WPA-Enterprise is more complex

Wireless Security



RADIUS authentication

Wireless Security



Multi-institution

Wireless Security

For WPA-Enterprise each user has their own key/password

Wireless Security

For WPA-Enterprise each user has their own key/password

Authentication is done in the RADIUS server on both the username and the password

Wireless Security

Exercise Read about how Eduroam uses WPA-Enterprise

Exercise Read about RADIUS: *Remote Authentication Dial In User Service*

Wireless Security

Some APs have *Wi-Fi Protected Setup* (WPS), a simplified way of setting up WPA/WPA2 security

Wireless Security

Some APs have *Wi-Fi Protected Setup* (WPS), a simplified way of setting up WPA/WPA2 security

Designed for those people who find typing in a password too challenging

Wireless Security

Some APs have *Wi-Fi Protected Setup* (WPS), a simplified way of setting up WPA/WPA2 security

Designed for those people who find typing in a password too challenging

It is seriously broken and should be disabled on your AP

Wireless Security

Some APs have *Wi-Fi Protected Setup* (WPS), a simplified way of setting up WPA/WPA2 security

Designed for those people who find typing in a password too challenging

It is seriously broken and should be disabled on your AP

Exercise A common system we see on public Wi-Fi is a redirect to a login web page: sometimes called a *captive portal*. What kind of security (privacy and authentication) does this provide? Note this is *not* WPA-Enterprise

Wireless 802.11

The frame layout for Wi-Fi is the same as Ethernet

Wireless 802.11

The frame layout for Wi-Fi is the same as Ethernet

In particular it has the same format MAC addresses, e.g.,
`00:04:ed:f1:ef:8a`

Wireless 802.11

The frame layout for Wi-Fi is the same as Ethernet

In particular it has the same format MAC addresses, e.g., `00:04:ed:f1:ef:8a`

This allows the transparent mixing of Wi-Fi and Ethernet in a single network

Wireless 802.11

The frame layout for Wi-Fi is the same as Ethernet

In particular it has the same format MAC addresses, e.g., `00:04:ed:f1:ef:8a`

This allows the transparent mixing of Wi-Fi and Ethernet in a single network

An AP can pass on a Wi-Fi frame unchanged to an Ethernet; and vice versa

Wireless 802.11

The frame layout for Wi-Fi is the same as Ethernet

In particular it has the same format MAC addresses, e.g., `00:04:ed:f1:ef:8a`

This allows the transparent mixing of Wi-Fi and Ethernet in a single network

An AP can pass on a Wi-Fi frame unchanged to an Ethernet; and vice versa

Exercise What implication does this have for Ethernet collision domains?

PHY Sublayers

This is a good argument for sub-dividing the physical layer!

PHY Sublayers

This is a good argument for sub-dividing the physical layer!

Exercise For hardware hackers: read about the IEEE layers:

- *Physical Medium Attachment* (PMA) for things like frames
- *Physical Coding Sublayer* (PCS) for things like 4B/5B
- *Physical Medium Dependent* (PMD) for the hardware

PHY Sublayers

This is a good argument for sub-dividing the physical layer!

Exercise For hardware hackers: read about the IEEE layers:

- *Physical Medium Attachment* (PMA) for things like frames
- *Physical Coding Sublayer* (PCS) for things like 4B/5B
- *Physical Medium Dependent* (PMD) for the hardware

But it does mean we don't have to discuss Wi-Fi any further!

Other Wireless

Many other wireless networks exist, from local to wide-area

Other Wireless

Bluetooth gives short range, point-to-point communication

Other Wireless

Bluetooth gives short range, point-to-point communication

Point-to-point: just two hosts in the network

Other Wireless

Bluetooth gives short range, point-to-point communication

Point-to-point: just two hosts in the network

A range of 10m

Other Wireless

Bluetooth gives short range, point-to-point communication

Point-to-point: just two hosts in the network

A range of 10m

Also uses 2.4GHz band

Other Wireless

Bluetooth gives short range, point-to-point communication

Point-to-point: just two hosts in the network

A range of 10m

Also uses 2.4GHz band

Not really designed to run IP, but can by layering a suitable protocol (see PPP, later)

Other Wireless

Bluetooth gives short range, point-to-point communication

Point-to-point: just two hosts in the network

A range of 10m

Also uses 2.4GHz band

Not really designed to run IP, but can by layering a suitable protocol (see PPP, later)

Bluetooth Low Energy (BLE), is a non-backwards-compatible evolution designed to reduce power consumption

Other Wireless

Exercise Read about *Adaptive Network Topology* (ANT and ANT+) for short range low power wireless, similar to BLE, but for use with fitness (and other) sensors (by Garmin)

Exercise Read about *Zigbee* for short range low data rate, low power wireless, for use in home automation and control

Other Wireless

We should also mention cellular networks, as used by mobile phones

Other Wireless

We should also mention cellular networks, as used by mobile phones

The first important digital system was *Global System for Mobile Communications* (GSM)

Other Wireless

We should also mention cellular networks, as used by mobile phones

The first important digital system was *Global System for Mobile Communications* (GSM)

Retrospectively named *2G*

Other Wireless

We should also mention cellular networks, as used by mobile phones

The first important digital system was *Global System for Mobile Communications* (GSM)

Retrospectively named *2G*

(1G was the preceding analogue system)

Other Wireless

We should also mention cellular networks, as used by mobile phones

The first important digital system was *Global System for Mobile Communications* (GSM)

Retrospectively named *2G*

(1G was the preceding analogue system)

Rates of 9.6Kb/s to 14.4Kb/s (similar to old analogue wired modems)

Other Wireless

We should also mention cellular networks, as used by mobile phones

The first important digital system was *Global System for Mobile Communications* (GSM)

Retrospectively named *2G*

(1G was the preceding analogue system)

Rates of 9.6Kb/s to 14.4Kb/s (similar to old analogue wired modems)

High Speed Circuit Switched Data (HSCSD) takes this up to 57.6Kb/s

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Uses several GSM channels

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Uses several GSM channels

Enhanced Data rates for GSM Evolution (EDGE) uses better encodings to get up to 384Kb/s, again using several channels

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Uses several GSM channels

Enhanced Data rates for GSM Evolution (EDGE) uses better encodings to get up to 384Kb/s, again using several channels

EDGE used by Third Generation (3G) systems

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Uses several GSM channels

Enhanced Data rates for GSM Evolution (EDGE) uses better encodings to get up to 384Kb/s, again using several channels

EDGE used by Third Generation (3G) systems

High-Speed Downlink Packet Access (HSDPA) ups this to 42.2Mb/s

Other Wireless

General Packet Radio Service (GPRS), packet based, up to 171.2Kb/s

Uses several GSM channels

Enhanced Data rates for GSM Evolution (EDGE) uses better encodings to get up to 384Kb/s, again using several channels

EDGE used by Third Generation (3G) systems

High-Speed Downlink Packet Access (HSDPA) ups this to 42.2Mb/s

Evolved High-Speed Packet Access (HSPA+) will do 168Mb/s

Other Wireless

4G is well established

Other Wireless

4G is well established

Using *Long Term Evolution* (LTE) with the promise of 300Mb/s

Other Wireless

4G is well established

Using *Long Term Evolution* (LTE) with the promise of 300Mb/s

LTE, marketed as “4G”, originally did not meet the proposed 4G standard as it did not satisfy the proposed technical specifications of a 4G system

Other Wireless

4G is well established

Using *Long Term Evolution* (LTE) with the promise of 300Mb/s

LTE, marketed as “4G”, originally did not meet the proposed 4G standard as it did not satisfy the proposed technical specifications of a 4G system

In particular, a 4G network should support 1Gb/s for a stationary host

Other Wireless

4G is well established

Using *Long Term Evolution* (LTE) with the promise of 300Mb/s

LTE, marketed as “4G”, originally did not meet the proposed 4G standard as it did not satisfy the proposed technical specifications of a 4G system

In particular, a 4G network should support 1Gb/s for a stationary host

The ITU (who say what “4G” is supposed to mean) actually gave in to commerce and retroactively changed the definition of 4G to allow for LTE

Other Wireless

LTE is data traffic only, and does not have a voice channel

Other Wireless

LTE is data traffic only, and does not have a voice channel

Currently on most LTE systems if you want to make a voice call it has to drop back to 3G (or even 2G)

Other Wireless

LTE is data traffic only, and does not have a voice channel

Currently on most LTE systems if you want to make a voice call it has to drop back to 3G (or even 2G)

Some phones and systems support *voice over LTE* (VoLTE) using a suitable digital encoding of sound over the data channel

Other Wireless

5G is currently being deployed

Other Wireless

5G is currently being deployed

It uses the available spectrum much more efficiently than 4G, and employs frequencies up to 86GHz (LTE uses up to 6GHz)

Other Wireless

5G is currently being deployed

It uses the available spectrum much more efficiently than 4G, and employs frequencies up to 86GHz (LTE uses up to 6GHz)

Projections indicate users connected to a base-station will share 20Gb/s download and 10Gb/s upload rates

Other Wireless

5G is currently being deployed

It uses the available spectrum much more efficiently than 4G, and employs frequencies up to 86GHz (LTE uses up to 6GHz)

Projections indicate users connected to a base-station will share 20Gb/s download and 10Gb/s upload rates

And base-stations will support “millions” of devices per square mile (enabling the *Internet of Things*)

Other Wireless

5G is currently being deployed

It uses the available spectrum much more efficiently than 4G, and employs frequencies up to 86GHz (LTE uses up to 6GHz)

Projections indicate users connected to a base-station will share 20Gb/s download and 10Gb/s upload rates

And base-stations will support “millions” of devices per square mile (enabling the *Internet of Things*)

A device will be able to connect even if it is moving at 500km/h (e.g., in a plane); latencies will be 1ms, compared to the current 20ms on LTE

Other Wireless

Current sticking points over the adoption of 5G are:

Other Wireless

Current sticking points over the adoption of 5G are:

- lack of support in “old” mobile phones

Other Wireless

Current sticking points over the adoption of 5G are:

- lack of support in “old” mobile phones
- 5G chipsets currently suck a lot of power

Other Wireless

Current sticking points over the adoption of 5G are:

- lack of support in “old” mobile phones
- 5G chipsets currently suck a lot of power
- the need to build a lot more base stations (using higher radio frequencies means the range of a cell is smaller)

Other Wireless

Current sticking points over the adoption of 5G are:

- lack of support in “old” mobile phones
- 5G chipsets currently suck a lot of power
- the need to build a lot more base stations (using higher radio frequencies means the range of a cell is smaller)
- or upgrading old ones and re-purposing existing frequencies used by 3G

Other Wireless

6G? A new “G” appears roughly every 10 years, so maybe 2030, but this is uncertain as 5G has significant improvements planned. Maybe a standard will be published in 2025

Other Wireless

6G? A new “G” appears roughly every 10 years, so maybe 2030, but this is uncertain as 5G has significant improvements planned. Maybe a standard will be published in 2025

With targets of 100Gb/s using 100GHz to 1THz (terahertz) frequencies

Other Wireless

6G? A new “G” appears roughly every 10 years, so maybe 2030, but this is uncertain as 5G has significant improvements planned. Maybe a standard will be published in 2025

With targets of 100Gb/s using 100GHz to 1THz (terahertz) frequencies

THz is between microwaves and infra red, not ionizing; current mobile is MHz and GHz. The tech to generate THz waves is still very new

Other Wireless

6G? A new “G” appears roughly every 10 years, so maybe 2030, but this is uncertain as 5G has significant improvements planned. Maybe a standard will be published in 2025

With targets of 100Gb/s using 100GHz to 1THz (terahertz) frequencies

THz is between microwaves and infra red, not ionizing; current mobile is MHz and GHz. The tech to generate THz waves is still very new

(The base-stations will need really good onward connectivity!)

Other Wireless

2G and 3G signals are due to be phased out by 2033 so their frequencies can be reused by 4G and 5G

Probably 3G will go first, as 2G is widely used in things like Smart Meters, and as a low-power fallback, particularly in rural areas

Other Wireless

2G and 3G signals are due to be phased out by 2033 so their frequencies can be reused by 4G and 5G

Probably 3G will go first, as 2G is widely used in things like Smart Meters, and as a low-power fallback, particularly in rural areas

Many companies are looking at dates like 2025 for 3G removal

Other Wireless

2G and 3G signals are due to be phased out by 2033 so their frequencies can be reused by 4G and 5G

Probably 3G will go first, as 2G is widely used in things like Smart Meters, and as a low-power fallback, particularly in rural areas

Many companies are looking at dates like 2025 for 3G removal

Exercise Read about how this affects 4G not natively supporting voice and limited VoLTE support

Other Wireless

Exercise How many radios are there in your mobile phone?

Other Wireless

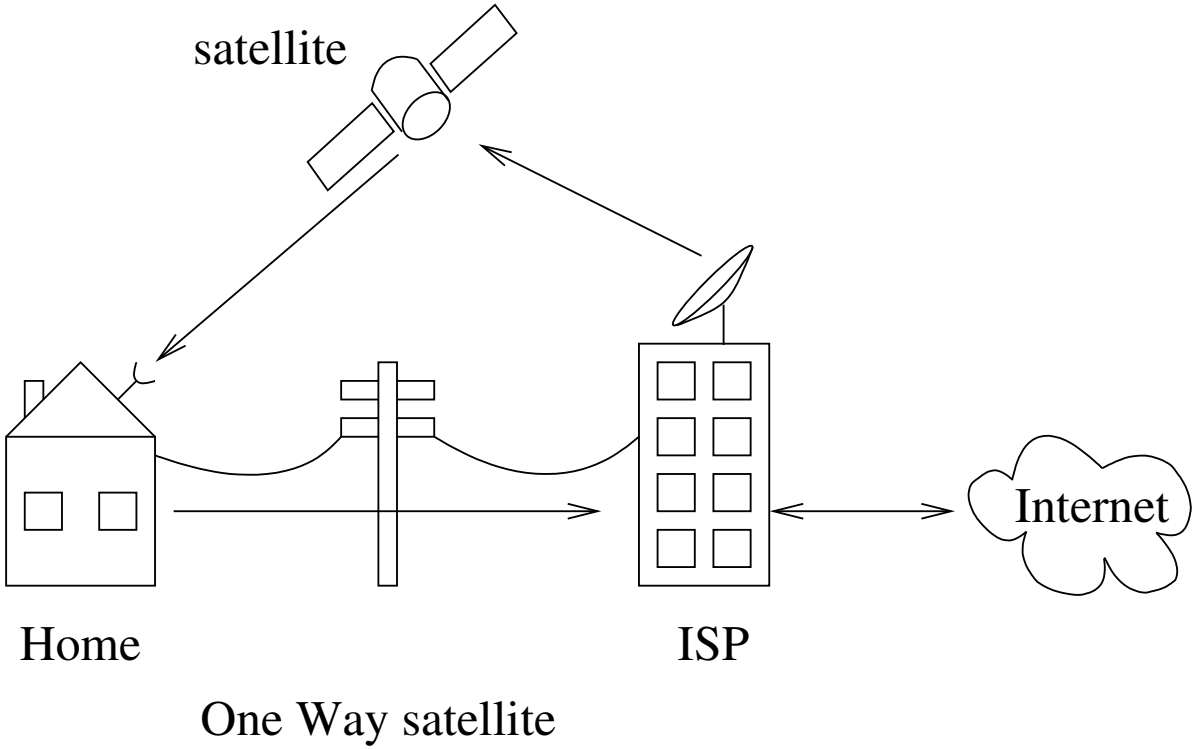
Satellite networks can be used outside of well-connected urban areas

Other Wireless

Satellite networks can be used outside of well-connected urban areas

There are two main variants

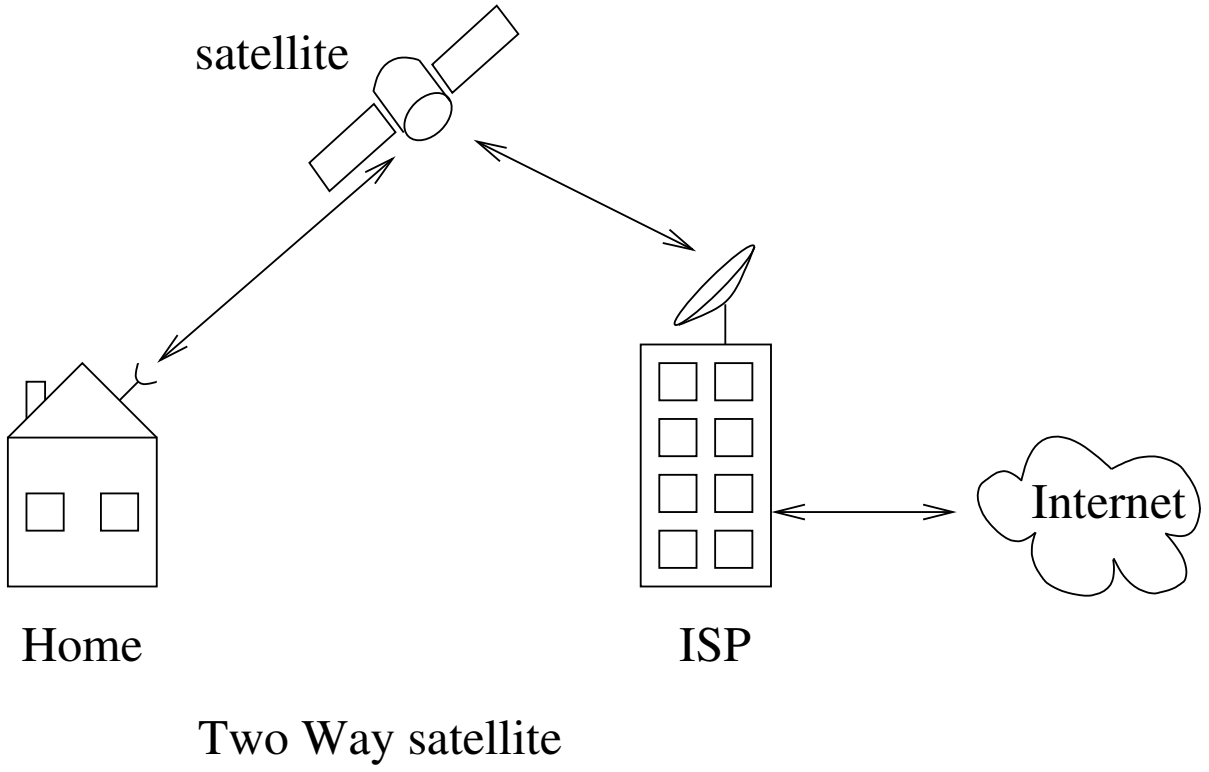
Other Wireless



One way satellite

One way satellite: this employs the usual asymmetry. Data away from the home travels by telephone wire; data towards the home travels through a satellite connection

Other Wireless



Two way satellite

Two way satellite: satellite connections both ways. More expensive in equipment in the home, but not reliant on a telephone network

Other Wireless

Satellites are very expensive to put up and to run

Other Wireless

Satellites are very expensive to put up and to run

They cover a large area with a reasonably good bandwidth

Other Wireless

Satellites are very expensive to put up and to run

They cover a large area with a reasonably good bandwidth

They are good for remote and undeveloped areas with no other local infrastructure

Other Wireless

Geostationary satellites have a large latency: about 1/10 sec, which can be very noticeable in highly interactive applications (games)

Other Wireless

Geostationary satellites have a large latency: about 1/10 sec, which can be very noticeable in highly interactive applications (games)

So lately providers are putting satellites into low orbits, but this means they are forever moving (from the perspective of someone at ground level)

Other Wireless

Geostationary satellites have a large latency: about 1/10 sec, which can be very noticeable in highly interactive applications (games)

So lately providers are putting satellites into low orbits, but this means they are forever moving (from the perspective of someone at ground level)

This is fixed by having a large number of satellites so there is always one overhead

Other Wireless

Geostationary satellites have a large latency: about 1/10 sec, which can be very noticeable in highly interactive applications (games)

So lately providers are putting satellites into low orbits, but this means they are forever moving (from the perspective of someone at ground level)

This is fixed by having a large number of satellites so there is always one overhead

Lower latency $\Longrightarrow$ lower orbit $\Longrightarrow$ faster moving satellites $\Longrightarrow$ more satellites needed to maintain coverage

Other Wireless

Starlink (amongst others) are currently building a low orbit satellite network

Other Wireless

Starlink (amongst others) are currently building a low orbit satellite network

Targets are 300 Mb/s at 20ms latency

Other Wireless

Starlink (amongst others) are currently building a low orbit satellite network

Targets are 300 Mb/s at 20ms latency

But this will need 10s of thousands of satellites (a problem for astronomers!)

Other Wireless

Starlink (amongst others) are currently building a low orbit satellite network

Targets are 300 Mb/s at 20ms latency

But this will need 10s of thousands of satellites (a problem for astronomers!)

Due to the cost, this may turn out to be a “top up” service for the hard to get at places; not a general connection for all

The Physical Layer

We have seen some implementations of the physical layer

The Physical Layer

We have seen some implementations of the physical layer

There are very many more

The Physical Layer

We have seen some implementations of the physical layer

There are very many more

There are many implementations as there are many physical requirements of networks (distance, speed, power, etc.)

The Physical Layer

We have seen some implementations of the physical layer

There are very many more

There are many implementations as there are many physical requirements of networks (distance, speed, power, etc.)

Fortunately, as we go up the layers, the amount of variety decreases!