Networks

Security in the IP

Despite being initiated by the Military (ARPA), the Internet protocols were mostly designed(?) and developed in Academia

Networks

Security in the IP

Despite being initiated by the Military (ARPA), the Internet protocols were mostly designed(?) and developed in Academia

This has had a great effect on the *security* of the Internet

Networks

Security in the IP

Despite being initiated by the Military (ARPA), the Internet protocols were mostly designed(?) and developed in Academia

This has had a great effect on the *security* of the Internet

The Internet was developed in a “safe” academic environment where little regard was given to issues of privacy or authentication

Networks

Security in the IP

Despite being initiated by the Military (ARPA), the Internet protocols were mostly designed(?) and developed in Academia

This has had a great effect on the *security* of the Internet

The Internet was developed in a “safe” academic environment where little regard was given to issues of privacy or authentication

And the models are also weaker on security than they ought to be

Networks

Security in the IP

OSI says “security should be involved at all layers”. Not particularly helpful

Networks

Security in the IP

OSI says “security should be involved at all layers”. Not particularly helpful

The Internet Model says even less

Networks

Security in the IP

OSI says “security should be involved at all layers”. Not particularly helpful

The Internet Model says even less

Compounding the issue of lack of support for security in the Internet protocols, early TCP/IP implementations were woefully poor: many exploitable bugs

By default:

By default:

- Data in transit is east to read and modify as it is passed through the various machines on the path to the destination

Networks

Security in the IP

By default:

- Data in transit is east to read and modify as it is passed through the various machines on the path to the destination
- Many protocols used are not resistant to malicious interference

Networks

Security in the IP

By default:

- Data in transit is east to read and modify as it is passed through the various machines on the path to the destination
- Many protocols used are not resistant to malicious interference
- Authentication mechanisms are weak to non-existent

Networks

Security in the IP

By default:

- Data in transit is east to read and modify as it is passed through the various machines on the path to the destination
- Many protocols used are not resistant to malicious interference
- Authentication mechanisms are weak to non-existent

And the implementations were very fragile and easily hacked

Note the two separate issues here:

Note the two separate issues here:

- the protocols are fragile and easily breakable

Note the two separate issues here:

- the protocols are fragile and easily breakable
- the implementations of those protocols were often poor

Note the two separate issues here:

- the protocols are fragile and easily breakable
- the implementations of those protocols were often poor

A good implementation of a bad protocol is bad

Networks

Security in the IP

Note the two separate issues here:

- the protocols are fragile and easily breakable
- the implementations of those protocols were often poor

A good implementation of a bad protocol is bad

A bad implementation of a good protocol is bad

Many of these issues have since been tackled (not always successfully), particularly when commerce got involved

Networks

Security in the IP

Many of these issues have since been tackled (not always successfully), particularly when commerce got involved

But there are still several areas that could be improved: see the routing to Youtube problem earlier; and that wasn't even maliciously intended

Networks

Security in the IP

Many of these issues have since been tackled (not always successfully), particularly when commerce got involved

But there are still several areas that could be improved: see the routing to Youtube problem earlier; and that wasn't even maliciously intended

New protocols and secure (we hope) extensions to existing protocols are now available: e.g., HTTPS for the Web, SMTPS for email

Networks

Security in the IP

Many of these issues have since been tackled (not always successfully), particularly when commerce got involved

But there are still several areas that could be improved: see the routing to Youtube problem earlier; and that wasn't even maliciously intended

New protocols and secure (we hope) extensions to existing protocols are now available: e.g., HTTPS for the Web, SMTPS for email

Management and use of cryptography has an overhead. This is an extra workload on servers: some people are unwilling to pay this price

Networks

Security in the IP

Many of these issues have since been tackled (not always successfully), particularly when commerce got involved

But there are still several areas that could be improved: see the routing to Youtube problem earlier; and that wasn't even maliciously intended

New protocols and secure (we hope) extensions to existing protocols are now available: e.g., HTTPS for the Web, SMTPS for email

Management and use of cryptography has an overhead. This is an extra workload on servers: some people are unwilling to pay this price

More on security later

Long term plan

We shall now work our way up the layers, looking in detail at what TCP/IP does for each

Long term plan

We shall now work our way up the layers, looking in detail at what TCP/IP does for each

This is going to be a long journey!

Networks

Hardware

First, hardware

Networks

Hardware

First, hardware

There are several popular hardware implementations. Some you should have come across are

- Ethernet: a wired network
- ADSL and VDSL: telephone networks
- Wi-Fi: a short range wireless network
- Cellular: mobile phones

Networks

Hardware

First, hardware

There are several popular hardware implementations. Some you should have come across are

- Ethernet: a wired network
- ADSL and VDSL: telephone networks
- Wi-Fi: a short range wireless network
- Cellular: mobile phones

We shall look at some of these

Exercise How many different radio/wireless systems does your mobile phone support?

Networks

Ethernet

Ethernet arose in 1982, from DEC, Xerox and Intel, based on the earlier *Aloha* protocol

Networks

Ethernet

Ethernet arose in 1982, from DEC, Xerox and Intel, based on the earlier *Aloha* protocol

The original Ethernet supported 10Mb/s

Networks
Ethernet

Ethernet arose in 1982, from DEC, Xerox and Intel, based on the earlier *Aloha* protocol

The original Ethernet supported 10Mb/s

Note: Mb/s = megabit/sec; MB/s = megabyte/sec

Networks

Ethernet

Ethernet arose in 1982, from DEC, Xerox and Intel, based on the earlier *Aloha* protocol

The original Ethernet supported 10Mb/s

Note: Mb/s = megabit/sec; MB/s = megabyte/sec

In comparison, current consumer Ethernet runs at 1Gb/s, while typical top-end Ethernet runs at 100Gb/s, with 400Gb/s starting to be used in datacentres and plans for 800Gb/s and 1.6Tb/s

Networks

Ethernet

To be a bit more precise, the original Ethernet had a 10Mb/s *signalling rate* (also known as *line rate*)

To be a bit more precise, the original Ethernet had a 10Mb/s *signalling rate* (also known as *line rate*)

The signalling rate is the rate of delivery of bits across the physical network

Networks

Ethernet

To be a bit more precise, the original Ethernet had a 10Mb/s *signalling rate* (also known as *line rate*)

The signalling rate is the rate of delivery of bits across the physical network

Due to layering encapsulation and other physical overheads, this is overwhelmingly *not* the rate of delivery of bits to the application you are running

Networks

Ethernet

To be a bit more precise, the original Ethernet had a 10Mb/s *signalling rate* (also known as *line rate*)

The signalling rate is the rate of delivery of bits across the physical network

Due to layering encapsulation and other physical overheads, this is overwhelmingly *not* the rate of delivery of bits to the application you are running

For example, there is always a gap between packets where data is not being transmitted!

However, the signalling rate is the number marketers like to use

Networks

Ethernet

However, the signalling rate is the number marketers like to use

The rate actually realised can be much lower; e.g., a 54Mb/s Wi-Fi 3 (802.11g) network might only deliver half that figure to an application

The Ethernet standard covers both the PHY and the MAC layers, so we shall look at them together

The Ethernet standard covers both the PHY and the MAC layers, so we shall look at them together

And we begin with the frame format

Networks

Ethernet

Ethernet frame

Numbers are byte counts: so, e.g., the destination address is 6 bytes long

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

Numbers are byte counts: so, e.g., the destination address is 6 bytes long

- 2 byte type indicates what kind of network layer data follows, e.g., (hex) 0800 for an IP packet

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

Numbers are byte counts: so, e.g., the destination address is 6 bytes long

- 2 byte type indicates what kind of network layer data follows, e.g., (hex) 0800 for an IP packet
- The data, maximum 1500 bytes

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

Numbers are byte counts: so, e.g., the destination address is 6 bytes long

- 2 byte type indicates what kind of network layer data follows, e.g., (hex) 0800 for an IP packet
- The data, maximum 1500 bytes
- **Minimum 46 bytes.** The data must be padded with extra bytes if fewer than 46 bytes are supplied

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

- A higher layer must detect and remove this padding when necessary

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

- A higher layer must detect and remove this padding when necessary
- 4 byte checksum, also called *cyclic redundancy check* (CRC)

Networks

Ethernet

Destination address	Source address	type	Data	CRC
6	6	2	46-1500	4

Ethernet frame

- A higher layer must detect and remove this padding when necessary
- 4 byte checksum, also called *cyclic redundancy check* (CRC)
- Use to check for corruption errors in the frame

The sending host fills in the other fields and computes and fills in the CRC

The sending host fills in the other fields and computes and fills in the CRC

The receiving host computes the CRC on what it gets and compares with what is in the CRC field

The sending host fills in the other fields and computes and fills in the CRC

The receiving host computes the CRC on what it gets and compares with what is in the CRC field

If they differ, it is very likely the packet was corrupted

Networks

Ethernet

The sending host fills in the other fields and computes and fills in the CRC

The receiving host computes the CRC on what it gets and compares with what is in the CRC field

If they differ, it is very likely the packet was corrupted

(There is a small chance that the CRC alone got corrupted and the other fields are good; or an even smaller chance the frame *and* the CRC both got corrupted in ways they still match)

The sending host fills in the other fields and computes and fills in the CRC

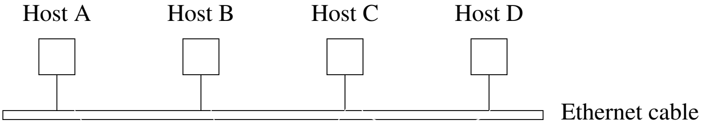
The receiving host computes the CRC on what it gets and compares with what is in the CRC field

If they differ, it is very likely the packet was corrupted

(There is a small chance that the CRC alone got corrupted and the other fields are good; or an even smaller chance the frame *and* the CRC both got corrupted in ways they still match)

Ethernet just drops corrupted frames; no more action is taken

(Original) Ethernet is *shared*, so every host sees every frame on the local network

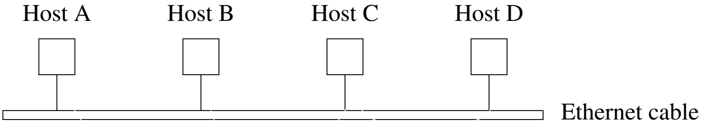


Original Ethernet

Networks

Ethernet

(Original) Ethernet is *shared*, so every host sees every frame on the local network



Original Ethernet

So how is a frame matched up to the intended destination host?

Networks

Ethernet

Every Ethernet card has a unique address built into it

Networks

Ethernet

Every Ethernet card has a unique address built into it

(Not the full story, but true enough for now)

Networks

Ethernet

Every Ethernet card has a unique address built into it

(Not the full story, but true enough for now)

So the destination address on the frame allows an Ethernet card in a host to recognise that a frame is for it and so can read and process it

Networks

Ethernet

Every Ethernet card has a unique address built into it

(Not the full story, but true enough for now)

So the destination address on the frame allows an Ethernet card in a host to recognise that a frame is for it and so can read and process it

There is a security issue here…

The source address on the frame allows a host to determine who sent the frame and so it can reply if needed

Networks

Ethernet

The source address on the frame allows a host to determine who sent the frame and so it can reply if needed

`000010000000000000100000100110100011010011011101` is an example Ethernet address, a 48-bit value

Networks

Ethernet

The source address on the frame allows a host to determine who sent the frame and so it can reply if needed

`000010000000000000100000100110100011010011011101` is an example Ethernet address, a 48-bit value

For convenience we write this as `08:00:20:9a:34:dd`, six hexadecimal numbers

Networks

Ethernet

This address is enough for when the destination is on the local Ethernet network: we have to work harder if the destination is non-local

This address is enough for when the destination is on the local Ethernet network: we have to work harder if the destination is non-local

And the destination might not be on an Ethernet, so how can we specify such a destination?

Networks

Ethernet

This address is enough for when the destination is on the local Ethernet network: we have to work harder if the destination is non-local

And the destination might not be on an Ethernet, so how can we specify such a destination?

This is the job of the next layer, IP, which we look at later

This address is enough for when the destination is on the local Ethernet network: we have to work harder if the destination is non-local

And the destination might not be on an Ethernet, so how can we specify such a destination?

This is the job of the next layer, IP, which we look at later

Ethernet is purely a local area network technology

What of the signalling on the wire?

Networks

Ethernet

What of the signalling on the wire?

Ethernet uses *carrier sense, multiple access with collision detection* (CSMA/CD)

Networks

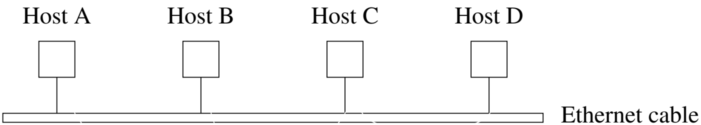
Ethernet CSMA/CD

Ethernet is a *multiple access* (shared) medium, meaning that several hosts use the same piece of wire to send data to one another

Networks

Ethernet CSMA/CD

Ethernet is a *multiple access* (shared) medium, meaning that several hosts use the same piece of wire to send data to one another



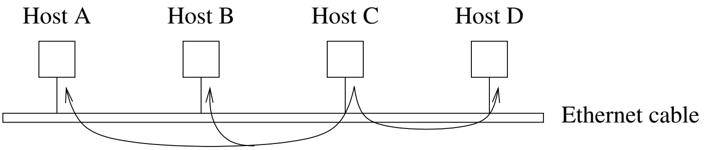
Original Ethernet

Suppose A wishes to send to B

Networks

Ethernet CSMA/CD

Ethernet is a *multiple access* (shared) medium, meaning that several hosts use the same piece of wire to send data to one another



Original Ethernet

Suppose A wishes to send to B

If C is already sending to D, the whole network is occupied with its signal, so A must wait

Networks

Ethernet CSMA/CD

If two hosts try to send simultaneously, there will be a *collision*

Networks

Ethernet CSMA/CD

If two hosts try to send simultaneously, there will be a *collision*

This is an actual physical condition where the electrical signals from the two hosts get mixed and thus corrupted

Networks

Ethernet CSMA/CD

If two hosts try to send simultaneously, there will be a *collision*

This is an actual physical condition where the electrical signals from the two hosts get mixed and thus corrupted

So before they send data, a host *listens* to the Ethernet to see if anyone else is using it at the moment: *carrier sense*

Networks

Ethernet CSMA/CD

If two hosts try to send simultaneously, there will be a *collision*

This is an actual physical condition where the electrical signals from the two hosts get mixed and thus corrupted

So before they send data, a host *listens* to the Ethernet to see if anyone else is using it at the moment: *carrier sense*

If not, it sends the data

Networks

Ethernet CSMA/CD

If two hosts try to send simultaneously, there will be a *collision*

This is an actual physical condition where the electrical signals from the two hosts get mixed and thus corrupted

So before they send data, a host *listens* to the Ethernet to see if anyone else is using it at the moment: *carrier sense*

If not, it sends the data

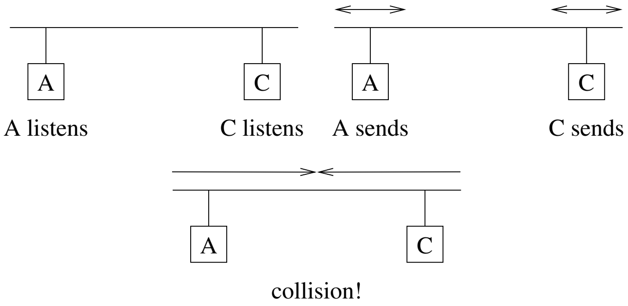
Otherwise it must wait, listening until the carrier is free

This still isn’t quite enough

Networks

Ethernet CSMA/CD

This still isn't quite enough

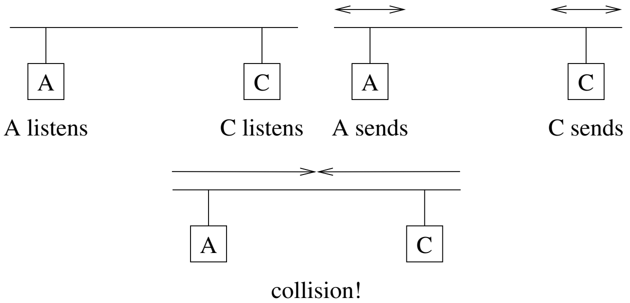


Frame collision

Networks

Ethernet CSMA/CD

This still isn't quite enough



Frame collision

So each host **continues to listen while transmitting** to make sure there are no collisions: *collision detection*

Networks

Ethernet CSMA/CD

If a collision is detected, each host stops transmitting, waits a (small) **random** period of time and retries with the carrier sense

Networks

Ethernet CSMA/CD

If a collision is detected, each host stops transmitting, waits a (small) **random** period of time and retries with the carrier sense

The random wait means that a further collision is less likely as one host will come in slightly later than the other and see its signal while it is carrier sensing

Networks

Ethernet CSMA/CD

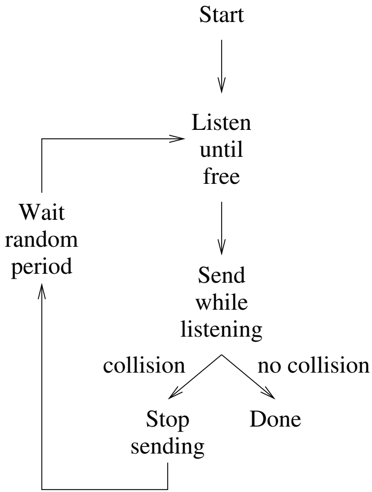
If a collision is detected, each host stops transmitting, waits a (small) **random** period of time and retries with the carrier sense

The random wait means that a further collision is less likely as one host will come in slightly later than the other and see its signal while it is carrier sensing

Detecting collisions on an Ethernet is simple: if the signal you are seeing on the network is not the same as the signal you are putting on the network, that means someone else is transmitting, too

Networks

Ethernet CSMA/CD



CSMA/CD flowchart

Exercise Explain why we need to go back to carrier sense after the random pause

Exercise Explain why we need to go back to carrier sense after the random pause

Exercise Read further about jamming signals and what to do if the transmission repeatedly fails

Collision detection is why there is a minimum frame size

Networks

Ethernet CSMA/CD

Collision detection is why there is a minimum frame size

The frames must be on the wire long enough that the hardware can detect a collision

Networks

Ethernet CSMA/CD

Collision detection is why there is a minimum frame size

The frames must be on the wire long enough that the hardware can detect a collision

The speed of the signal in the wire is the problem here!

Networks

Ethernet CSMA/CD

Collision detection is why there is a minimum frame size

The frames must be on the wire long enough that the hardware can detect a collision

The speed of the signal in the wire is the problem here!

(The speed of a signal in a cable is approx 2/3 c; 100m is 520 cpu cycles of a 1GHz cpu)

Networks

Ethernet CSMA/CD

Collision detection is why there is a minimum frame size

The frames must be on the wire long enough that the hardware can detect a collision

The speed of the signal in the wire is the problem here!

(The speed of a signal in a cable is approx 2/3 c; 100m is 520 cpu cycles of a 1GHz cpu)

And this is made worse with later faster Ethernets

Ethernet CSMA/CD

Collision detection is why there is a minimum frame size

The frames must be on the wire long enough that the hardware can detect a collision

The speed of the signal in the wire is the problem here!

(The speed of a signal in a cable is approx 2/3 c; 100m is 520 cpu cycles of a 1GHz cpu)

And this is made worse with later faster Ethernets

Exercise Find out how CSMA/CD differs from Aloha

Networks

Physical Ethernet

There have been many Ethernet physical layers

Standard	cable	max len	rate
10Base5	Thick coax	500m	10Mb/s
10Base2	Thin coax	200m	10Mb/s
10BaseT	Twisted pair	100m	10Mb/s
10BaseF	Fibre optic	2000m	10Mb/s

Base means *baseband*, namely using a single chunk of frequencies from 0 (the base) up to a single cut-off point

Networks

Physical Ethernet

And these evolved (just a selection here):

Standard	cable	max len	rate
100BaseT4	Twisted pair	100m	100Mb/s
100BaseT	Twisted pair	100m	100Mb/s
100BaseF	Fibre optic	2000m	100Mb/s
1000BaseT	Twisted pair	100m	1Gb/s
2.5GBaseT	Twisted pair	100m	2.5Gb/s
5GBaseT	Twisted pair	100m	5Gb/s
10GBaseT	Twisted pair	100m	10Gb/s

Networks

Physical Ethernet

The cables used in these PHYs change over time. Unshielded Twisted Pair (UTP) comes in various qualities:

- Category 1: No performance criteria
- Category 2: Rated to 1 MHz (used for telephone wiring)
- Category 3: Rated to 16 MHz (used for Ethernet 10BaseT)
- Category 4: Rated to 20 MHz (used for Token-Ring, 10BaseT)
- Category 5/5e: Rated to 100 MHz (used for 1000BaseT, 100BaseT, 10BaseT)

The cables used in these PHYs change over time. Unshielded Twisted Pair (UTP) comes in various qualities:

- Category 1: No performance criteria
- Category 2: Rated to 1 MHz (used for telephone wiring)
- Category 3: Rated to 16 MHz (used for Ethernet 10BaseT)
- Category 4: Rated to 20 MHz (used for Token-Ring, 10BaseT)
- Category 5/5e: Rated to 100 MHz (used for 1000BaseT, 100BaseT, 10BaseT)

Category 5 has been replaced by Category 5e which has slightly better construction specifications

Networks

Physical Ethernet

All the twisted pair cables are bundles of 4 pairs of wires with an RJ45 plug on the end

Networks

Physical Ethernet

All the twisted pair cables are bundles of 4 pairs of wires with an RJ45 plug on the end

Then we have shielded cables, where each pair has a metal foil wrapper:

- Category 6: Rated to 250 MHz
- Category 6a: Rated to 500 MHz
- Category 8.1: Rated to 2000 MHz
- Category 8.2: Rated to 2000 MHz, special end plugs

Plus extra rules on how the plugs on the end are joined on

You will see “Category 7” cable being sold

You will see “Category 7” cable being sold

It is not standardised, and does not use the usual RJ45 plugs

You will see “Category 7” cable being sold

It is not standardised, and does not use the usual RJ45 plugs

Even worse, you will see it being sold with RJ45 plugs on, to be compatible with most current consumer networks. This actually reduces its performance to something like Cat6, but at an increased cost

You will see “Category 7” cable being sold

It is not standardised, and does not use the usual RJ45 plugs

Even worse, you will see it being sold with RJ45 plugs on, to be compatible with most current consumer networks. This actually reduces its performance to something like Cat6, but at an increased cost

Currently (2023) the best cable to buy is Cat6a as it supports any speed your home network is likely to have and is fairly cheap

Networks

Physical Ethernet

Amusingly, you find reviews of Cat 8 cables on Amazon along the lines of “I installed Cat 8 instead of WiFi and now my home network is super-fast”

Networks

Physical Ethernet

Amusingly, you find reviews of Cat 8 cables on Amazon along the lines of “I installed Cat 8 instead of WiFi and now my home network is super-fast”

They forget using *any* kind of wired instead of WiFi is likely to be faster, less latency and more stable than WiFi

Networks

Physical Ethernet

Amusingly, you find reviews of Cat 8 cables on Amazon along the lines of “I installed Cat 8 instead of WiFi and now my home network is super-fast”

They forget using *any* kind of wired instead of WiFi is likely to be faster, less latency and more stable than WiFi

And they would very probably get the same benefit from the much cheaper Cat 5e or 6a

Networks

Physical Ethernet

Amusingly, you find reviews of Cat 8 cables on Amazon along the lines of “I installed Cat 8 instead of WiFi and now my home network is super-fast”

They forget using *any* kind of wired instead of WiFi is likely to be faster, less latency and more stable than WiFi

And they would very probably get the same benefit from the much cheaper Cat 5e or 6a

A connection cannot be faster than the slowest component: the device interface, the cable and the switch connecting them

Networks

Physical Ethernet

Amusingly, you find reviews of Cat 8 cables on Amazon along the lines of “I installed Cat 8 instead of WiFi and now my home network is super-fast”

They forget using *any* kind of wired instead of WiFi is likely to be faster, less latency and more stable than WiFi

And they would very probably get the same benefit from the much cheaper Cat 5e or 6a

A connection cannot be faster than the slowest component: the device interface, the cable and the switch connecting them

Currently very few home users will have anything faster than 1 Gb interfaces and switches