

Introduction

A complete network can be a mix of two modes of connection

- Connected with physical cables and/or
- Connected with wireless technology

As well as the hardware and cables needed to do this, the network must also stick to an agreed set of standards that sets out *how* the devices will talk to one another.

If every device keeps to the same standard then they will be able to exchange data with one another.

The main standard for wired connections is Ethernet.

There are two very popular standards for wireless connections, namely Wi-Fi and Bluetooth.

This section will describe these standards.

2. Ethernet

Ethernet is a *family* of standards that covers

- The physical design of plugs, sockets and cables
- How devices will start, stop and handle data exchange
- How to handle network errors



In any network, the plugs must fit into the sockets; the cable must behave the same way no matter who you buy it from. You should be able to purchase network cards from one supplier and know that they will work with cards

from another supplier. And so part of the Ethernet standards covers all these physical details.

3. Ethernet - data standards

Most networks break up the data they want to exchange into separate chunks called a packet. Each type of network formats its packets differently, adding or removing certain bits of extra information. For example, packets sent over the Internet will have IP-address information.



In Ethernet networks, the format for a packet is called a 'frame'. Frames include:

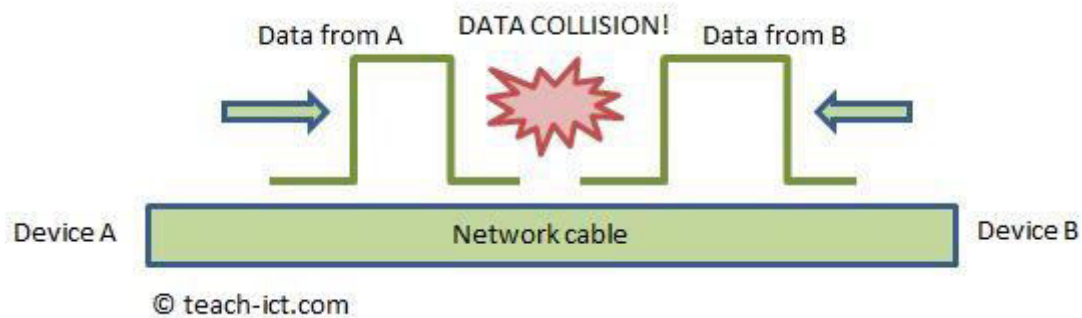
- The data being sent
- The MAC address of the device sending the packet
- The MAC address of the device receiving the packet
- Error checking bits

The error checking bits are, as their name suggests, checked by the receiving computer device to ensure the packet arrived intact. If it finds an error, the device either sends back a request to re-send that packet or it discards the packet.

4. Ethernet - avoiding data collisions

Just like a good traffic controller, Ethernet describes how devices must take turns to send their data.

This helps avoid two devices trying to send their data through a cable at exactly the same time which results in a 'data collision'



The Ethernet rules are

- Check that the cable is unused before sending out a data packet
- If two packets do collide then each device must wait a short random time before re-sending their packet. This lessens the chances of it happening again.

The network term for this taking-turns process is called 'handshaking'.

5. Wireless network - Bluetooth



Bluetooth is a type of radio communication and networking protocol combined.

It was developed so devices close to one another could exchange data, without any need for a physical connection and yet use very little power. Making it ideal for mobile and portable devices.

By close, we mean within about 10 metres of one another even if there is a wall in-between.

This method of network connection is popular with:

- Smart-phone to car entertainment systems
- Blue tooth enabled speakers and headphones
- Downloading from digital cameras.
- Connecting to blue-tooth enabled printers.

Uniquely in 2020, blue-tooth, is a key part of the UK Covid-19 contact tracing app. This scans for nearby blue-tooth smart phones and warns if someone positive has been too close for too long.

The picture opposite shows a typical setting-up screen on a smart-phone fitted with blue-tooth. It allows you to switch it off if you want and it shows all the nearby devices the phone can connect to.

6. Wireless - Wi-Fi



Wi-Fi is a communication technology that makes use of radio waves in order to connect to a local area network.

It is also widely used to connect to the internet from a laptop or smart phone whilst out and about.

The word Wi-Fi is actually a trade name owned by the Wi-Fi alliance. The alliance is a group of about 300 companies from around the world. They work together to make sure that all 'Wi-Fi' enabled devices are compatible with one another.

All laptops have Wi-Fi built in.

The key device is the Wireless Access Point or WAP that handles all the data exchange. The WAP is hard-wired to the local area network or is built into a home hub to allow local Wi-Fi.

Encryption is used to help avoid data being accessed without the right password.

7. Wi-Fi limitations

Wi-Fi is very useful as a network technology. But there are some issues with it that means hard-wired networks will always be with us as well.

1. *Security*

Wi-Fi broadcasts your network data over radio waves and these are easily picked up by other devices within range.

Early Wi-Fi networks were open to virtually anyone. Some people made a hobby of driving around looking for open networks. But now most private networks are password enabled so it is harder for someone to break into the network.

2. *Limited connections*

Just like a normal radio, Wi-Fi uses a small number of radio channels to work.

This is no problem at home where only a few connections are needed. But in a busy office, this lack of channels may mean difficulty in making a connection.

3. *Limited range*

Wi-Fi is a radio technology and so it is affected by things such as walls getting in the way. For example, at home the router might be downstairs and so the signal upstairs may be very weak. This can be overcome by using a 'wi-fi extender' located somewhere in-between. It acts like a bridge, such as the extender shown in the picture which was plugged in a kitchen.

1. Introduction

Encryption is the process of scrambling data in such a way that only legitimate users can read it.

This is what *plaintext* i.e. unencrypted data looks like

Humpty Dumpty sat on a wall.

and this is what *ciphertext* i.e. the encrypted version might look like

jkd2f*hkdfh7\$171kjfh7d1h4d

Encryption works by scrambling the original data using an *encryption algorithm*.

The encryption algorithm is a set of mathematical steps applied to the original text to change it into cyphertext. Each standard algorithm has a name, such as the AES-256 algorithm.

The algorithm uses a very large digital number (key) to do the conversion. It is extremely difficult for a normal computer to work out what is the correct key in a reasonable amount of time.

Encryption can also be applied to 'real-time' streaming data for copy protection purposes.

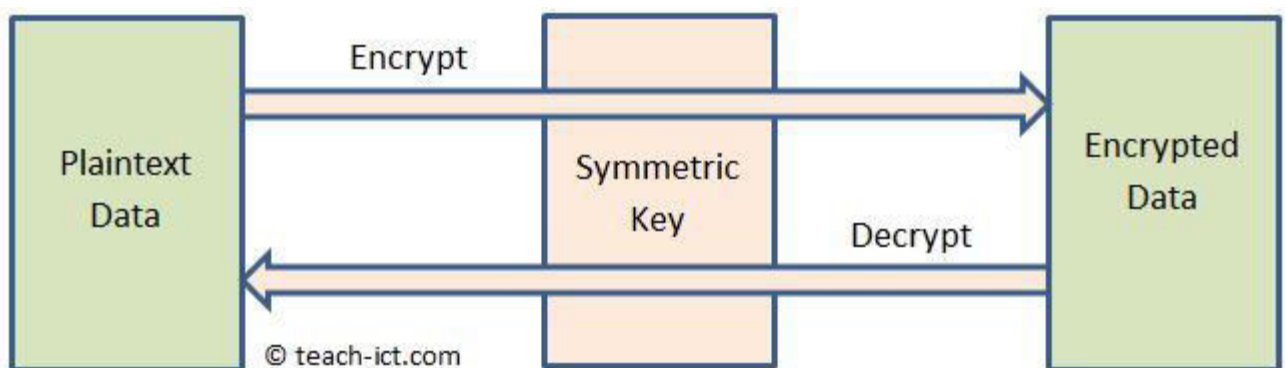
For example only paid-up subscribers are able to access encrypted commercial entertainment streams or satellite broadcast channels.

This section will describe two types of technologies

- Symmetric key encryption
- Assymmetric key encryption

2. Symmetric Encryption Key

The word 'symmetric' is used because the *same* key is used for both encryption and decryption.



The symmetric key must be kept secret by legitimate systems using it.

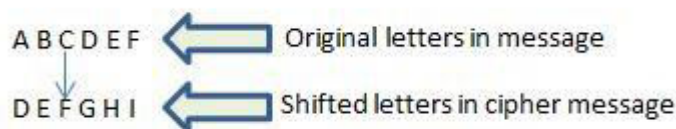
A symmetric digital key must be long enough that it becomes unlikely that a normal sized computer has enough processing power to crack the encrypted message in a reasonable amount of time.

The strength of the key is determined by its bit length. For example a 128 bit symmetric key would take a maximum of 2^{128} brute force attempts to guess it.

An example of a symmetric key algorithm is AES-256 (short for Advanced Encryption Standard - 256 bits), and it is the standard algorithm used by governments and other organisations for really sensitive information.

Caesar cipher

People have been using non-digital symmetric keys for at least two thousand years. One of the earliest known ciphers is the Caesar cipher, used by the Roman Emperor Julius Caesar for his correspondence. The cipher was very simple - take each letter in the message and swap it for another letter an agreed number of positions up the alphabet. For example if the rule is 3 shifts, A becomes D, B becomes E and so on. It is trivial for a computer to crack this code, but for centuries it was quite good.



Book cipher

You have probably seen this used in wartime spy movies. Agent A and Agent B agree to use a certain book, the huge 'War and Peace' book maybe. Then the message is created by referencing a letter or word in various pages within the book.

For example the code might be 434. Meaning use the 34th letter on page 4.

The whole scheme relies on no-one knowing which book is being used.

3. Symmetric key across a network

Symmetric key ciphers are excellent as long as the key is kept secret.

This is not too difficult if only a few people need to share the key. Perhaps they could physically meet and agree on a strong digital key which is stored on a memory stick, for example. Then this can be used to exchange encrypted messages with one another.

Another way may be to use a hardware 'dongle' that calculates a key in a time-specific way. The other end also knows the key by doing the same calculation based on current time i.e both ends are effectively sharing the same key. For

example a remote employee could be given a hardware key dongle to let them open a VPN connection (Virtual Private Network) back to the office.



However, with the rise of the internet, email etc, it becomes much more difficult for two random people to share a key because they have to *exchange the key* over a network.

They would have to send the key unencrypted, or the other party wouldn't know how to decrypt the message. But if the unencrypted key is intercepted, then they have lost any security.

A clever solution was the development of an *asymmetric key system*. Described on the next page

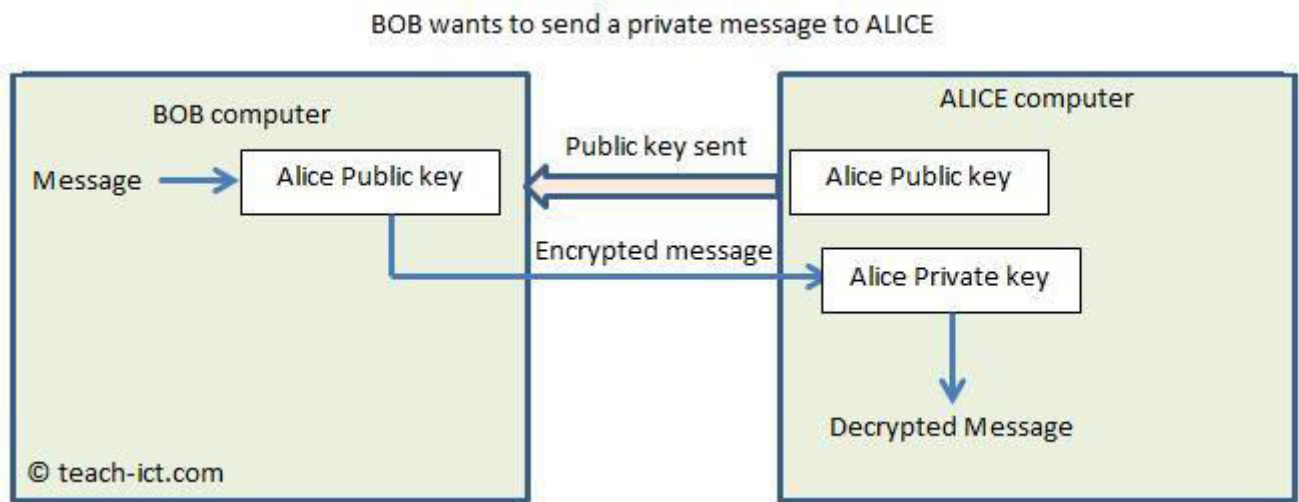
4. Asymmetric key - Public-Private keys

With the Public-Private key system there are two keys involved, a public key and a private key.

The public key is used to *encrypt* messages, but it can't be used to *decrypt* them. So it's safe to send across the internet to anyone. To decrypt a message encoded with the public key, you need to have the second, private, key. This is never sent across a network, so it remains secret and safe.

It work like this:-

Bob wants to send a private message to Alice. And so he requests her *public key*, which she sends over the public network as it does not matter who knows the public key.



Bob uses Alice's public key to encrypt his message and transmits it over the public network. Nobody can use the public key to decrypt the message, so it is safe. Once the message arrives, Alice uses her private key that only she knows. This is the key used to decrypt messages, and without it the data is unreadable.

The same applies the other way around, Alice requests Bob's public key and composes her message with it, only Bob has the private key needed to decrypt the message.

This is called an *asymmetric key system* because one key encrypts and a different one decrypts.

TLS (Transport Layer Security) is the most widely used secure protocol used on the internet - it is the protocol used when you see 'https' in the URL of a secure page, such as a login screen. (It replaced the old SSL protocol)

TLS uses both symmetric and asymmetric algorithms at different stages of the connection.

5. Comparing methods

The biggest problem with using encryption is that your computer needs to use a lot of processing time to encrypt and decrypt messages.

This can affect performance, which is why usually only sensitive or private data is encrypted.

The shorter the key, the less processing time is needed. But at the same time, encryption using shorter keys is much easier to break.

Symmetric keys are much stronger than asymmetric keys of the same length, since the asymmetric key is in two smaller pieces. But while they are stronger, it is much more difficult to exchange symmetric keys safely. This is why asymmetric encryption remains popular.



6. Summary

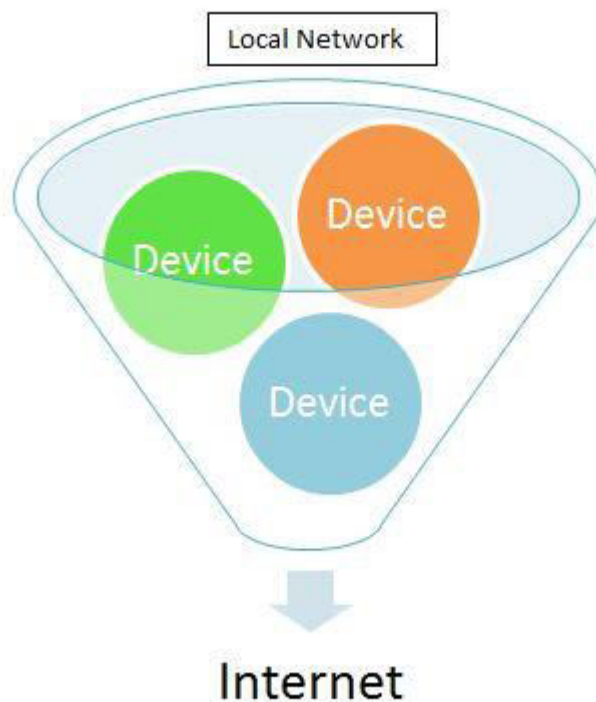
- Encryption is the process of scrambling data in such a way that only legitimate users can read it.
- Symmetric encryption means the same key is used for both encryption and decryption.
- 128 to 256 bit symmetric keys are considered to be strong enough for ordinary use.
- If a symmetric key is made known, then any message using it can be decrypted.
- Asymmetric encryption means one key (the public one) is used to encrypt a message and another one (the private one) is used to decrypt it
- AES-256 is an example of a symmetric key algorithm.
- TLS is the protocol behind https and is the basis of most secure transactions on the internet.

IP and MAC addressing

1. Introduction

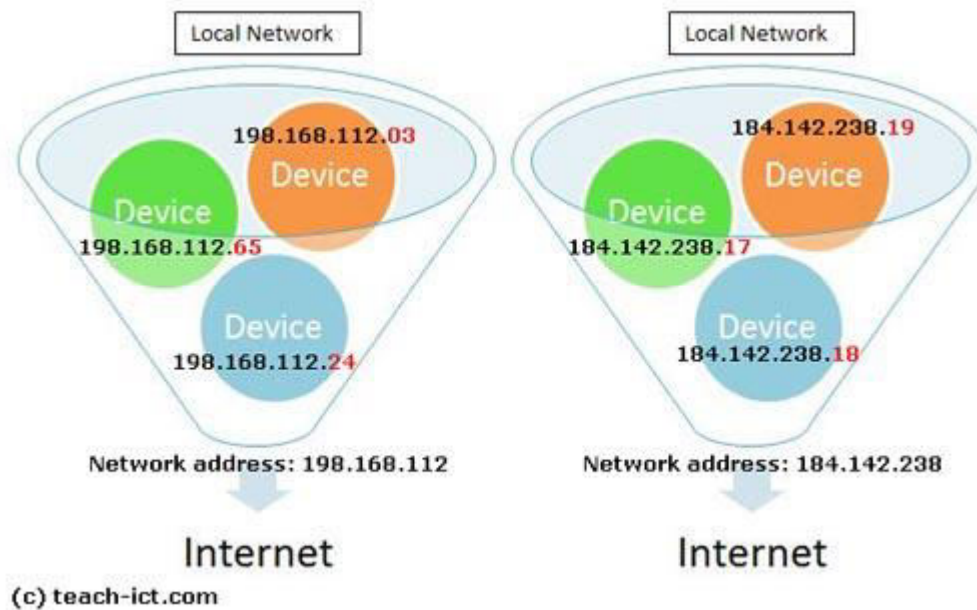
A local area network is a set of connected devices that can share data with one another. And the most popular protocol for enabling this exchange is called TCP/IP. The IP part stands for Internet Protocol.

But there is a problem - in order to exchange data, how does one device know the location of another device?



Well, the very simplest thing to do would be to give each one an unique identity in the form of a simple number. For example the green device could be called '1', the orange '2' and the blue '3'. Then they could swap information by attaching the correct address to each piece of information being exchanged.

But a local area network may also be connected to the internet - and it may want to exchange data with a device on another network, so a simple small number will not be enough.

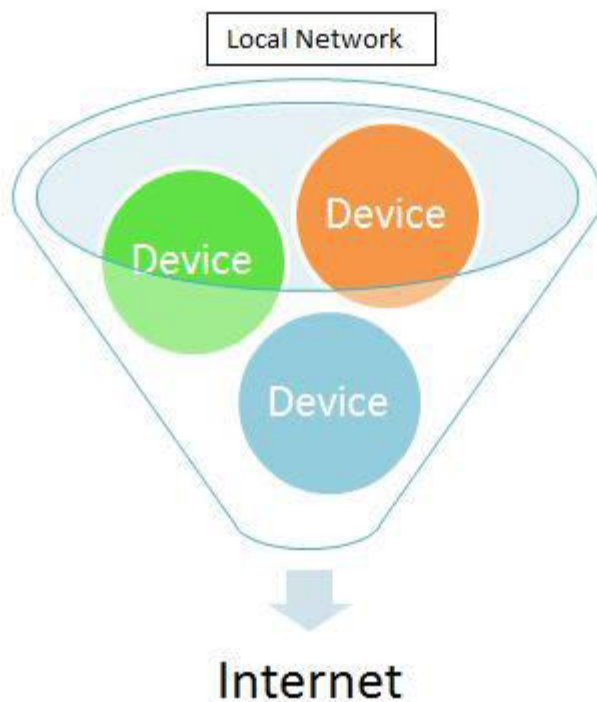


IP and MAC addressing

2. Addressing

The suggestion on the previous page of giving each device a simple number identity is fine in theory but in practice it has to be a bit more complicated. Because

- The numbering scheme has to be 'computer friendly'
- The scheme has to handle a vast amount of devices
- The scheme has to deal with more than one network



In terms of being 'computer friendly', the numbering scheme should be based on binary numbers, as that is what computers are designed to use.

A 32 bit binary number addressing scheme called 'IP' or 'Internet Protocol' was agreed upon more than forty years ago and it has allowed the internet to become the planet-wide network it is today.

IP and MAC addressing

3. Internet Protocol or IP

The Internet Protocol was designed to allow devices to exchange data over a network.



The word 'device' is used because they do not have to be computers. For example a factory may have dozens of digital controllers on the assembly line wanting to swap information. They can use IP for this.

The most dominant version of IP is called 'version 4' or IP v4.

Each address is made up of a 32 bit binary number like this:

10111000100011101110111000010001

A bit of maths will tell you that 2^{32} devices can be identified with this scheme or roughly four billion devices.

IP and MAC addressing

4. Human friendly method

Computers or other logic devices have no problem with a 32 bit number - they were designed to use binary.

10111000100011101110111000010001

But this is just not user-friendly enough for people to handle. So to make the scheme more practical, the 32 bit number is grouped into four 8 bit numbers like this:

10111000 10001110 11101110 00010001

Then each group is converted into its decimal equivalent

184 142 238 17

And then put a dot between each group to help keep them apart visually

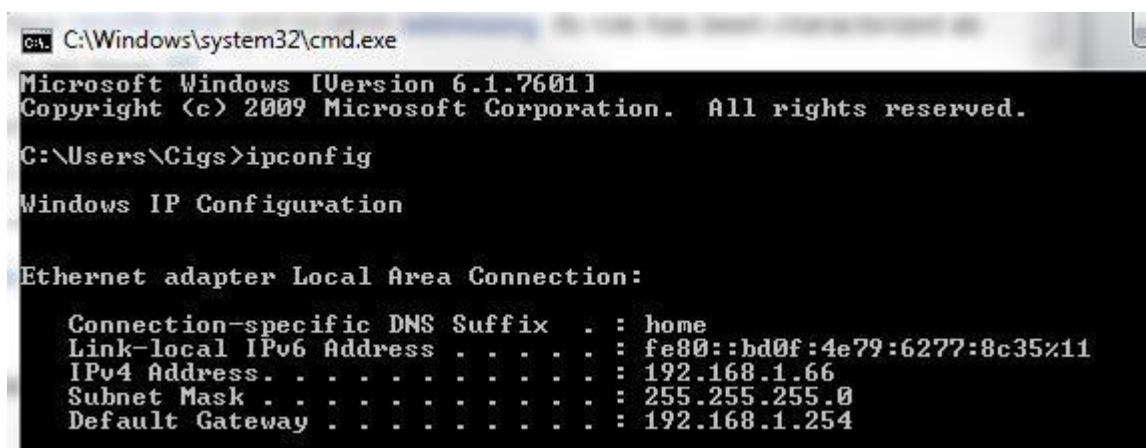
184.142.238.17

This is still a 32 bit binary number held within the device but network applications always present it in this form.

IP and MAC addressing

5. Ipconfig tool

If you want to view the network settings on your Windows computer, there is an useful tool called 'ipconfig' that comes with the operating system. This runs within the command console. As you can see below



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cigs>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

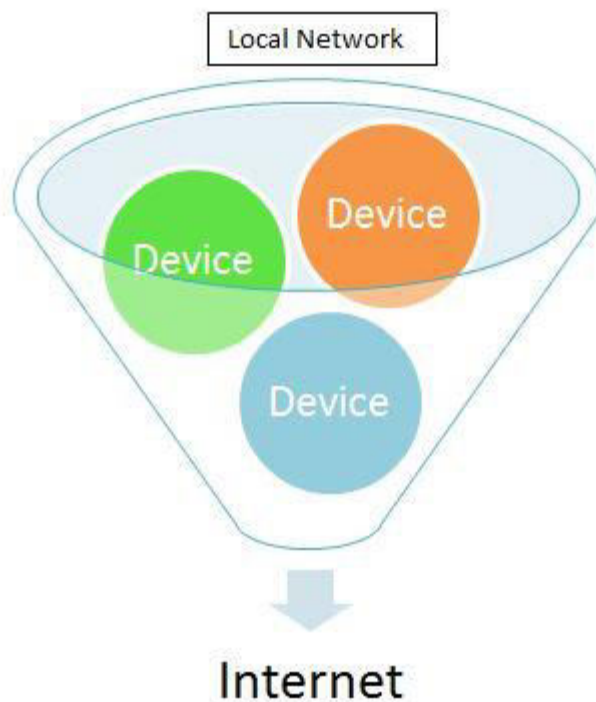
    Connection-specific DNS Suffix  . : home
    Link-local IPv6 Address . . . . . : fe80::bd0f:4e79:6277:8c35%11
    IPv4 Address. . . . . : 192.168.1.66
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

Type in ipconfig on the command line and it displays the IP address of the computer (IPv4 Address) in the dot format just explained, in this case 192.168.1.66

IP and MAC addressing

6. Networks and IP

A 32 bit number can identify four billion devices. But of course there isn't just one massive network across the planet - they are split into millions of smaller networks.



So the IP number is split into having two roles.

The first three numbers typically identify the network itself. Then the last number identifies the device within that network :

192 . 168 . 1 . 66

Network Device

(c) teach-ict.com

The scheme does not always have to use the first three numbers. Another number called the 'Subnet Mask' helps identify how many of the numbers to use. The picture below shows ipconfig showing the 'subnet mask' on my computer as 255.255.255.0 indicating that the first three numbers sets are to be used for my network.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cigs>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : home
    Link-local IPv6 Address . . . . . : fe80::bd0f:4e79:6277:8c35%11
    IPv4 Address. . . . . : 192.168.1.66
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

IP and MAC addressing

7. Internet Protocol version 6

You have read about version four of the Internet Protocol (IPv4) being able to discern over four billion addresses.

But over the last thirty years, the internet has expanded beyond anyone's expectations and four billion addresses is no longer enough.

In 1998, people could see that a much larger scheme had to be developed. One that could handle a vastly bigger internet. That scheme is called Internet Protocol version 6 or IPv6

IPv6 uses 128 bits rather than 32, and this offers 2^{128} addresses.

In a similar way to IPv4, IPv6 is made human friendly by grouping the address into hexadecimal numbers separated by double colons, like this:

fe80::bd0f:4e79::6277::8c35

The scheme has enough space to give every grain of sand on Earth its own IP address. That should be big enough!

In addition, the scheme adds better security and makes routers a bit more efficient.

A typical IPv6 network address is shown in the picture below

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cigs>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : home
    Link-local IPv6 Address . . . . . : fe80::bd0f:4e79:6277:8c35%11
    IPv4 Address. . . . . : 192.168.1.66
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

IPv6 and IPv4 are not compatible and for many years to come they will run side by side.

IP and MAC addressing

8. MAC Addressing

As well as the network IP address, there is another important type of *hardware* address and it is called the **Media Access Control** address or simply the MAC address.

This is the unique identifier assigned to a network card/controller, Wi-Fi or Bluetooth adapter.

It is a 48 bit binary number and is hard-wired into the device itself. It does not change - unlike the IP network address.

The code identifies maker of the card or device and the unique serial number assigned to it by the manufacturer.

To make it a bit more people friendly the MAC address is usually quoted as a set of six hexadecimal number like this:

MAC address: **0A-14-FF-32-11-23**

The first six numbers identify the manufacturer, for example Apple uses F1-F7-85 on all its hardware.

The MAC address has a number of uses which are described on the next page.

IP and MAC addressing

9. Uses of the MAC address

The MAC address identifies a specific hardware device and it does not change. This feature has a number of uses

Sending data

An individual ethernet data packet contains the 6 byte MAC address of both the source and destination devices. The packet itself is steered towards its destination by the IP address of the destination network. Once it enters the network, each network card, wi-fi or bluetooth connection checks its own MAC address to that inside the packet, if there is a match, it takes in the packet.

Security

The MAC address helps prevent unauthorised equipment from connecting to a network.



For example every card machine you see in the shops has its own MAC address. When it is used to accept payment, it tries to connect to the credit card network. The network has a database of authorised MAC addresses, if it does not match then connection is refused.

The same method is used in businesses to prevent unauthorised laptops or tablets making a Wi-Fi or Bluetooth connection to their network.



A network switch stores a list of all the MAC addresses present on each port. When a data packet comes along, it uses the MAC address inside the packet to steer it to the correct port and no other.

IP and MAC addressing

10. Summary

- IP stands for Internet Protocol
- There are two standard protocols - IPv4 and IPv6
- IPv4 is a 32 bit binary number scheme
- An IPv4 address is presented as four decimal numbers separated by dots 198.234.034.002
- IPv6 is a 128 bit binary number scheme and can address vastly more than IPv4.
- Today, the internet uses both IPv4 and IPv6
- MAC is an unique 48 bit binary number assigned to a piece of hardware
- It is presented as a set of hex numbers like this: **0A-14-FF-32-11-23**
- MAC is used for sending data to the correct adapter
- MAC is used to prevent unauthorised hardware from connecting to a network

- MAC is used by a network switch to steer individual data packets to the correct port
- MAC is *not* used by the internet to direct data traffic because it does not contain location information, unlike the hierarchy within an IP address

Network protocols

1. Network protocol

A **network protocol** is an agreed way of how to communicate over a network. A protocol is often made formal by setting up a world standard.



In general, the word 'protocol' means an agreed set of rules of how to do something.

In terms of network communications having a protocol standard allows devices to exchange data with one another as long as they are all following the same rules.

There are many standard network protocols, some of which will be discussed over the next few pages.

Network protocols

2. Parts of a protocol

A good communication protocol should include the following details:

- How to set up a connection
- How to end a connection
- How to start a message
- How to end a message
- How to deal with corrupted data
- How to format the data being sent

With these rules in place, hardware makers are sure their devices will work on a network using that protocol. Software authors are confident that their networked applications will work.



Network protocols

3. TCP / IP

The protocol used for communicating over the internet is called **TCP/IP**, or "**Transmission Control Protocol / Internet Protocol**". It has two parts: TCP and IP.

TCP - Transmission Control Protocol

This protocol prepares messages for transmission and reassembles any received messages.

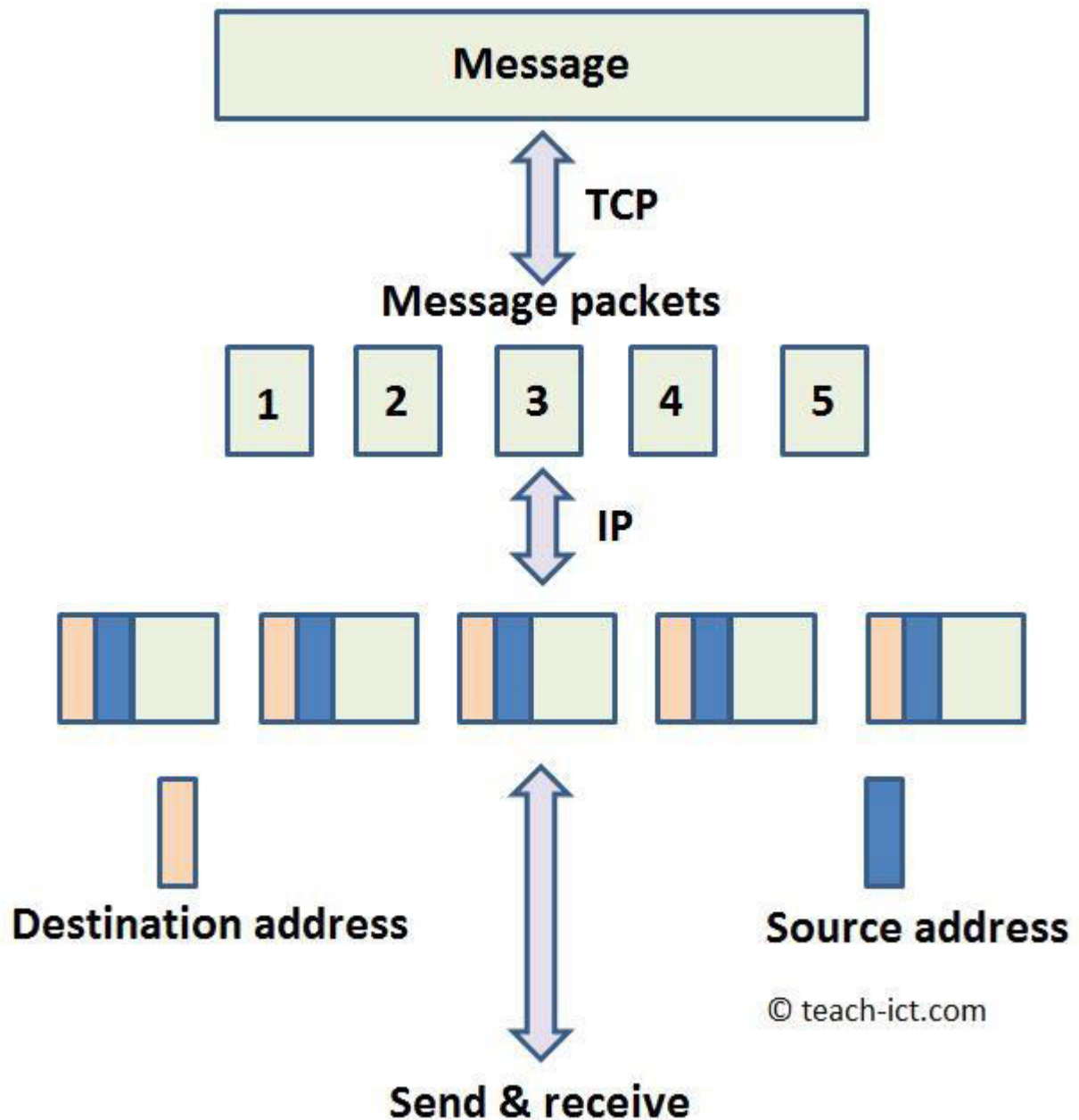
When *sending* data the TCP rules (protocol) include

- Dividing the message into packets
- Adding a sequence number to each packet so the message can be re-assembled
- Adding extra error-correction information, so errors can be spotted and fixed

When *receiving* data the TCP rules (protocol) include

- Examining each packet for errors by using the extra information that was added to it
- Fixing any errors (if possible) or requesting that the packet be re-sent
- Spotting missing packets and requesting them to be re-sent
- If all packets are present, using the sequence number of each packet to re-assemble the message

This TCP/IP process is shown in the diagram below.



Network protocols

4. TCP / IP continued

IP - Internet Protocol

When transmitting messages, this protocol is responsible for providing the destination address and to recognise incoming data packets.

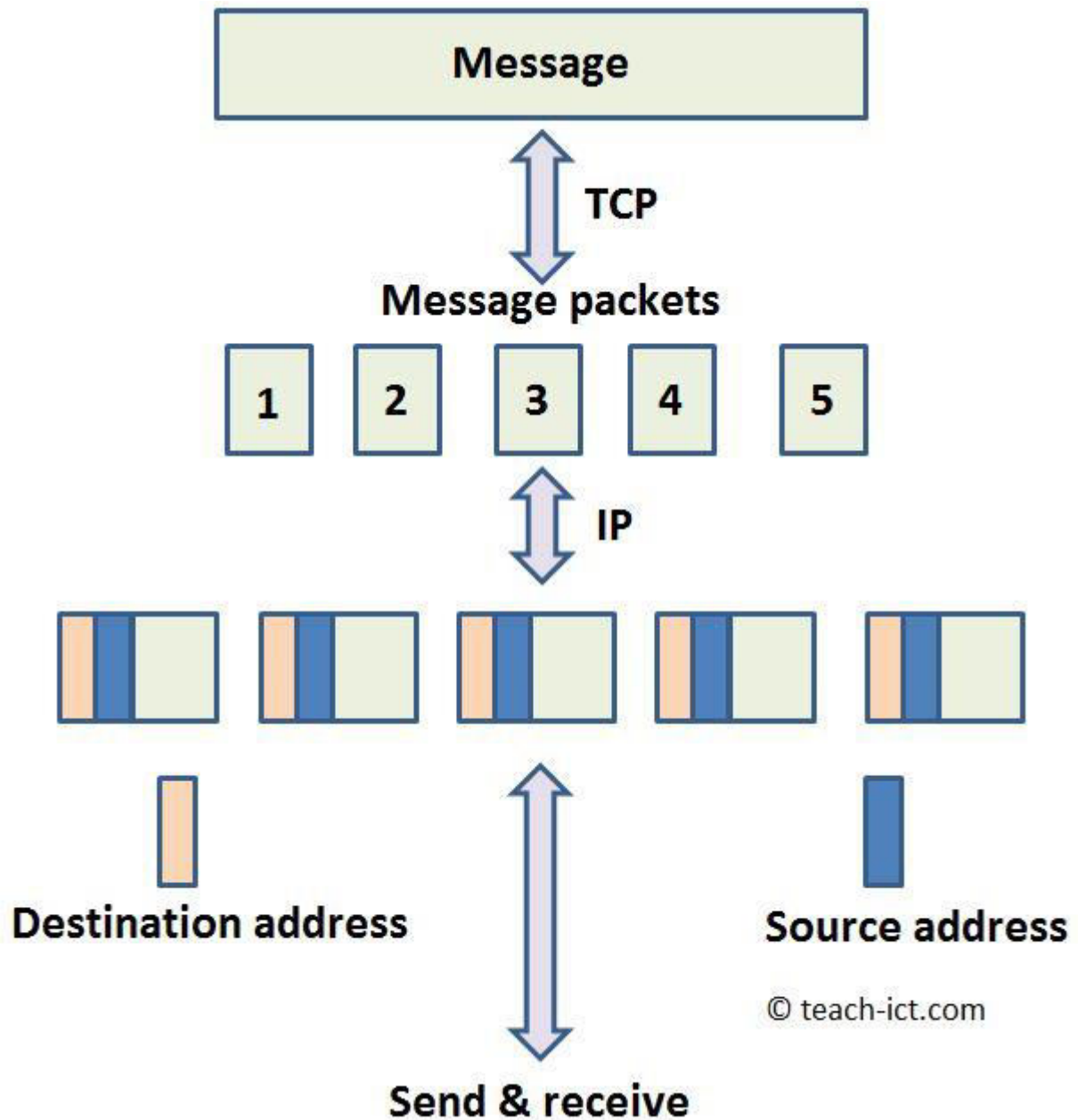
For *sending* data the IP rules (protocol) include

- Add the destination address to each data packet
- Add its own address to indicate where it came from

For *receiving* data packets the IP rules (protocol) include

- Accept data packets that have its own address attached
- Ignore all data packets that do not contain its own address

This TCP/IP process is shown in the diagram below.



Network protocols

5. HTTP and HTTPS

HTTP, or "**HyperText Transfer Protocol**", is the protocol underlying the World Wide Web.

Web pages are sent and received using the http protocol.



A web page is made up of a collection of individual files - text, images, styling, javascript and so on. The http protocol allows a browser to request these individual files from a web server in an orderly way. Once received, they are rendered into a web page such as the one you are reading at the moment.

A web page that begins with https:// is using this protocol.

HTTPS

There is a variation of it called 'https' (extra s on the end), meaning 'http secure'.

This protocol works like http, but also encrypts web page data before it is sent out of the browser or server, to make sure that nobody can intercept the data and read it themselves.

For example, if you are viewing a typical login page that starts with https:// the browser encrypts the user name and password before it is sent to the server. Only the server can decrypt the details.

Network protocols

6. FTP

FTP, or '**File Transfer Protocol**' is a standard network protocol used to transfer (i.e. upload and download) files between a client and server on a computer network.

The diagram below shows a typical FTP set up screen

Basic Advanced

Category

- Local Info
- Remote Info
- Testing Server
- Cloaking
- Design Notes
- Site Map Layout
- File View Columns
- Contribute
- Templates
- Spry

Remote Info

Access: FTP

FTP host: ftp.mywebsite.com

Host directory: public_html/

Login: Test

Password: Save

☒ Use passive FTP

☐ Use IPv6 transfer mode

☐ Use firewall Firewall Settings...

☐ Use Secure FTP (SFTP)

Server Compatibility...

☒ Maintain synchronization information

☐ Automatically upload files to server on save

☐ Enable file check in and check out

OK Cancel Help

Network protocols

7. Email protocols

POP

Post Office Protocol (POP) allows emails to be downloaded and /or deleted from a mail server and viewed offline by an email client.

The main disadvantages of this protocol are that

- it can only handle one mailbox
- messages, once downloaded, are removed from the email server and cannot later be viewed by other devices
- it does not support complex searches of emails on the server.

IMAP

Internet Message Access Protocol (IMAP) is similar in many ways to POP but it also offers more complex commands to manage emails on the server itself.

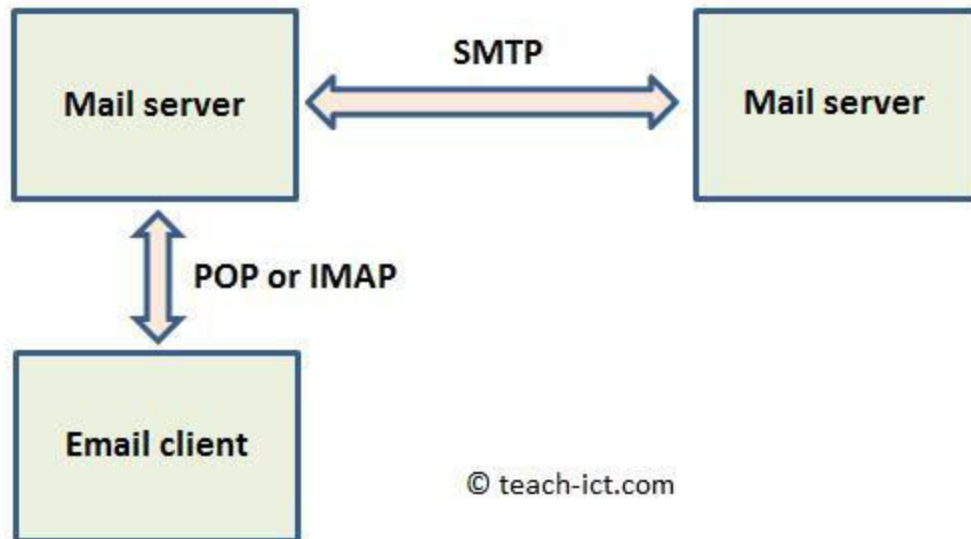
Unlike POP the email remains on the server even after being downloaded to the device. This means that you can use multiple devices and perhaps view your emails using your laptop and then access them from elsewhere on your smartphone and they will still look exactly the same.

IMAP allows you to:

- Set flags on emails showing whether they have been viewed (read), replied to, deleted etc
- Access emails on multiple devices i.e. PC, smart phone, tablet etc
- Synchronisation across devices - any email enabled device can access the email sever if they have the correct login details. When they do so, IMAP allows the device to be synchronised automatically with the latest emails.
- It allows complex searches to be carried out based on subject, headers and so on.
- It can handle more than one mail box.
- You can choose whether to download just the headers, full body or not to download attachments.

SMTP

Simple Mail Transport Protocol (SMTP) is used by the mail server itself to send and receive emails from all other mail servers across the internet.



Network protocols

8. The four layer model.

As you have seen, there are many different protocols and it would be easy to muddle them up. So to help you understand how these different protocols interact, a conceptual model has been developed.

It is important to understand that this is a model or 'representation of an idea', it is not something that actually exists.

This model is known as 'the four layer model' - simply because it has four layers!

A layer has a particular function to perform i.e. the role they play in network communication.

Each layer is given a number and a name (see table below).

The protocols in each layer can only communicate with those in the layers directly above and below it.

For example, TCP in layer 3 can only communicate with the protocols in layers 2 and 4.

Layer	Layer Name	Protocols	Purpose
4	Application Layer	FTP, HTTP, POP, IMAP, SMTP	The protocols in this layer provide access to files and websites across an IP network.
3	Transport Layer	TCP	The TCP part of the TCP/IP protocol resides in this layer. It is responsible for dividing messages into packets, adding sequence numbers and checksums for error correction information. It also checks for errors with errors of received data packets.
2	Internet Layer	IP	The IP part of the TCP/IP protocol resides in this layer. It is responsible for managing the source and destination locations.
1	Network / Data Link Access	ETHERNET, Wi-Fi	The protocols in this layer are responsible for actually transmitting and receiving data over a cable or wireless.

Benefits of using a layer model

- We use layers because it can be difficult to conceptualise a complex system such as network communication. By dividing the system of protocols into layers we can focus on a particular area individually without worrying too much about the other layers.
- The layer model is useful for manufacturers so that when they are developing new hardware they can ensure that it is compatible with existing protocols
- We can map how layers relate and interact with one another.
- We can recognise roughly what a protocol does by knowing which layer it resides within.
- When a new protocol is developed, it can be slotted into the appropriate layer.

Network protocols

9. Summary

- 'Protocol' means an agreed set of steps of how to do something.
- A protocol defines how to set up a connection and how to end it
- A protocol defines how to format a message using the connection
- A protocol defines how to detect errors and data collisions
- TCP/IP is the basic communication protocol of the internet.
- HTTP is the protocol used to send and receive web pages
- HTTPS is the secure (but slower) version of http
- FTP is a protocol to handle the upload and download of files
- POP and IMAP are email client protocols
- Ethernet is the most popular protocol to set up a LAN
- There is a four layer model to help relate protocols to one another
- The layers are Application, Transport, Internet, Network Access (or data link)
- Protocols can be declared to reside within one of the four layers