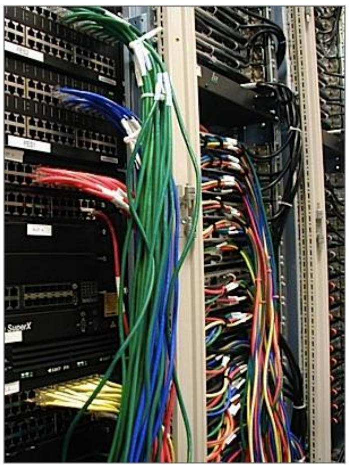
Computer Networks



The syllabus says that you should be able to:

a. describe a **router** and its purpose;
b. describe the use of **WIFI** and **Bluetooth** in networks;
c. describe how to **set up a small network** involving access to the Internet, understanding the need to set up the use of a browser, email and an ISP;
d. identify the **advantages and disadvantages** of using common **network** environments such as the **Internet**;
e. describe what is meant by the terms **user id** and **password**, stating their purpose and use;
f. identify a variety of **methods of communication** such as:
   - fax,
   - e-mail,
   - bulletin boards,
   - tele/video conferencing;

g. define the terms:
   - Local Area Network (**LAN**)
   - Wireless Local Area Network (**WLAN**)
   - Wide Area Network (**WAN**)

h. describe the **difference** between LANs and WANs, identifying their main characteristics;
i. describe the characteristics and purpose of common network environments, such as **intranets** and the **Internet**;
j. describe other common **network devices** (including hubs, bridges, switches and proxy servers);
k. discuss the problems of **confidentiality** and **security** of data, including problems surrounding common network environments;
l. identify the need for **encryption**, **authentication** techniques, including the use of user identification and passwords, when using common network environments such as the Internet.

Why Use Networks?

Using a computer connected to a network allows us to…

Saem Mashhud Tariq

What's on your mind?

View Photos of Me (56)
View Videos of Me (1)
Edit My Profile

Write something about yourself.

Information

Relationship Status:
Married
Birthday:
March 8, 1980
Current City:
Lahore, Pakistan

Abdullah Islam
Abdullah Islam matched you with one of his friends!
Your match: Find who's your match!
Saturday at 1:40pm via Best Match · Comment · Like · See Friendship · See Your Match

Syed Asad Rizvi hey sir wats up....
October 29 at 9:45pm · Comment · Like · See Friendship

Saem Mashhud Tariq was tagged in Mashal Sahir's album.
Wall Photos
The menace of child abuse - Mashal Sahir

Used Nokia set for Sale
mobile.pk
Wanna buy used Nokia Mobiles? Visit www.Mobile.pk to see 1000's of used Nokia cellphones for sale from all around Pakistan. Come in!

Lifebuoy Germ Strike

Arslan Shaukat
Jahanzaib Akram
Chat (21

- Easily **share files** and data
- **Share resources** such as printers and Internet connections
- **Communicate** with other network users (e-mail, instant messaging, video-conferencing, etc.)
- **Store data centrally** (using a file server) for ease of access and back-up
- Keep all of our **settings centrally** so we can use any workstation

In particular, if we use a computer connected to The Internet, we can…

- Make use of **on-line services** such as **shopping** (e-commerce) or **banking**
- Get access to a huge range of **information** for research
- Access different forms of **entertainment** (games, video, etc.)
- Join **on-line communities** (e.g. MySpace, Facebook, etc.)

Why Not Use Networks?

Using a computer connected to a network means that…

- The computer is vulnerable to **hackers**
- If the **network breaks**, many tasks become very difficult
- Your computer can more easily be attacked by a **virus**

In particular, if we use a computer connected to The Internet…

- We have to be careful about **revealing personal information**
- We have to be careful to **avoid suspect websites** that might contain **malware**
- We have to be aware that **information** found on The Internet is **not always accurate or reliable**

Computers in a Network

Computers connected together to create a network fall into two categories: **servers** and **clients** (workstations).

Clients

Client computers, or **workstations**, are the **normal computers** that people sit at to get their **work** done.

*When you use your Web browser, you are in fact using a Web **client**. When you type in the URL of a web page, you are actually providing the address of a Web **server**.*

*e.g. **www.bbc.co.uk** is the address of the BBC's web server.*

*Your Web browser/client asks this server for the web page you want, and the server '**serves**' the page back to the browser/client for you to see.*

Servers

Servers are special, powerful computers that provide '**services**' to the **client** computers on the network.

These services might include:

- Providing a **central**, common **file storage** area
- **Sharing hardware** such as **printers**
- Controlling who can or can't have **access the network**
- **Sharing Internet** connections

Servers are built to be **very reliable**. This means that they are much more **expensive** that normal computers.

In a small network one server might provide all of these services. In a larger network there might be many servers sharing the work.

Types of Network

Local Area Network (LAN)

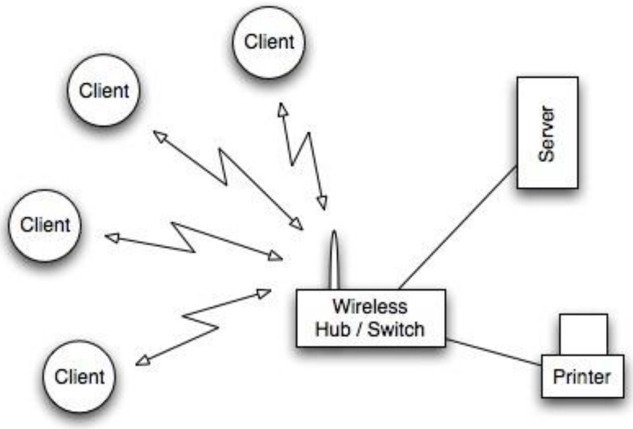
A Local Area Network is a network confined to **one building or site**.
Often a LAN is a **private network** belonging to an organisation or business.

Because LANs are geographically small, they usually use **cables** or low-power radio (**wireless**) for the connections.

Wireless Local Area Network (WLAN)

A wireless LAN (WLAN) is a LAN that uses **radio signals** (**WiFi**) to connect computers instead of cables.

At the centre of the WLAN is a **wireless switch or router** - a small box with one or two antennas sticking out the back - used for **sending and receiving data** to the computers. (Most laptops have a wireless antenna built into the case.)



It is much more **convenient** to use wireless connections instead of running long wires all over a building.

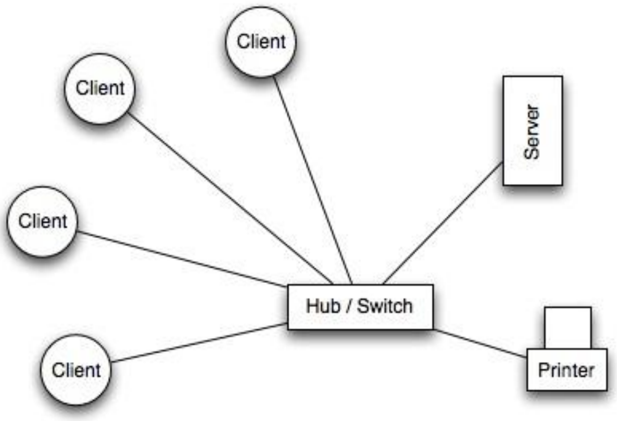
However, WLANs are more **difficult to make secure** since other people can also try to connect to the wireless network. So, it is very important to have a good, hard-to-guess **password** for the WLAN connections.

*Typically, the **range** of a wireless connection is about **50m**, but it depends how many walls, etc. are in the way.*

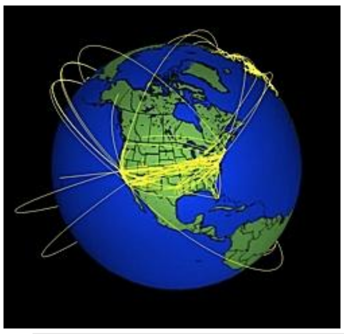
Wide Area Network (WAN)

A Wide Area Network is a network that extends over a **large area**.

A WAN is often created by **joining several LANs** together, such as when a business that has offices in different countries links the office LANs together.

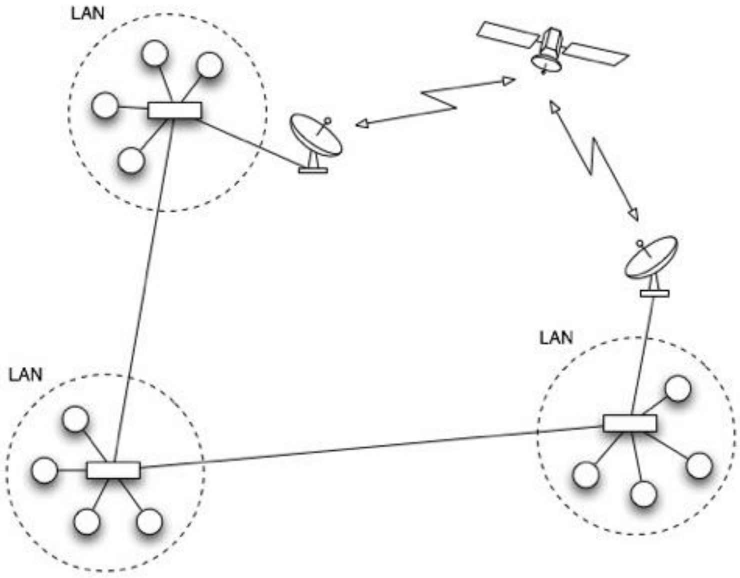


Because WANs are often geographically spread over large areas and **links** between computers are over **long distances**, they often use quite exotic connections technologies: **optical fibre** (glass) cables, **satellite** radio links, **microwave** radio links, etc.



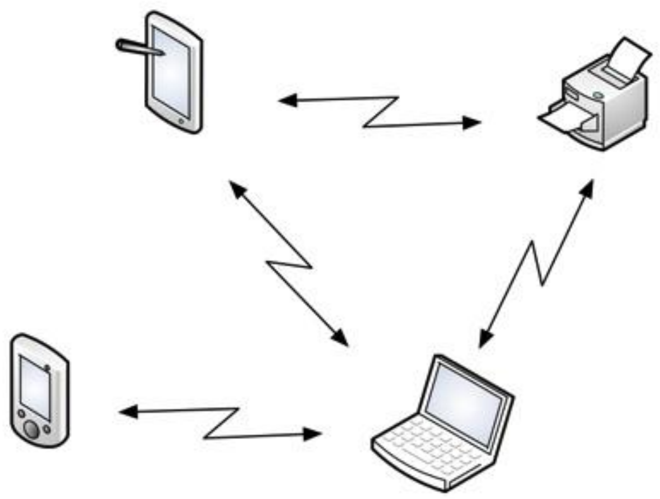
*The **Internet** is an example of a **global WAN** .In fact it is the world's largest WAN.*

Computers on the International Space Station are linked to the Internet, so the you could say the the Internet is now the first off-planet WAN!



Bluetooth (Personal Area Network)

Bluetooth is a wireless networking technology designed for very **short-range** connections (typically just a few metres).



The idea of Bluetooth is to get rid of the need for all of those cables (e.g. USB cables) that connect our computer to peripheral devices such as printers, mice, keyboards, etc.

Bluetooth devices contain small, **low-power** radio transmitters and receivers. When devices are in range of other Bluetooth devices, they detect each other and can be '**paired**' (connected)

Typical uses of Bluetooth:

- Connecting a **wireless keyboard** to a computer
- Connecting a **wireless mouse** to a computer
- Using a **wireless headset** with a mobile phone
- **Printing wirelessly** from a computer or PDA
- **Transferring data** / music from a computer to an MP3 player
- **Transferring photos** from a phone / camera to another device
- **Synchronising** calendars on a PDA and a computer

*Because Bluetooth networking only works over very short distances, and with devices belonging to one user, this type of network is sometimes called a '**Personal Area Network**'*

Networking Hardware

Network Interface Card (NIC)

Any computer that is to be connected to a network, needs to have a network interface card (NIC).

Most modern computers have these devices built into the motherboard, but in some computers you have to add an extra expansion card (small circuitboard)

*Some computers, such as laptops, have two NICs: one for **wired** connections, and one for **wireless** connections (which uses radio signals instead of wires)*

In a laptop, the wireless radio antenna is usually built in to the side of the screen, so you don't need to have a long bit of plastic sticking out the side of your computer!

Network Cable

To connect together different devices to make up a network, you need cables.

Cables are still used in most networks, rather than using only wireless, because they can carry much more **data per second**, and are more **secure** (less open to hacking).

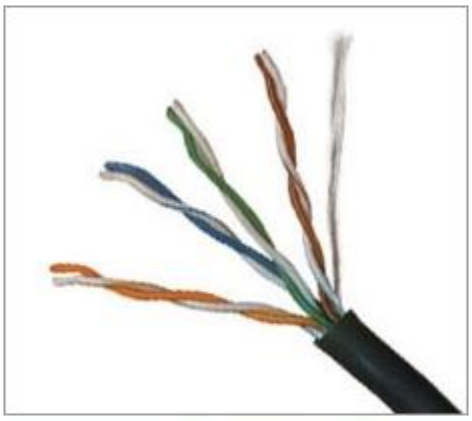
The most common type of network cable cable in use today looks like the one shown above, with plastic plugs on the ends that snap into sockets on the network devices.

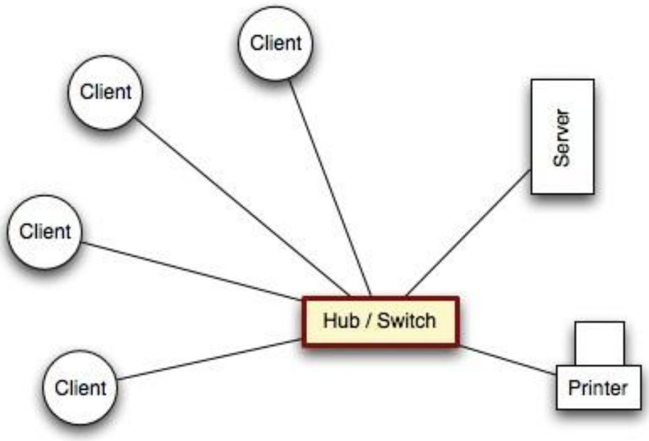
Inside the cable are several copper wires (some used for sending data in one direction, and some for the other direction).

Hub

A hub is a device that **connects** a number of computers together to make a **LAN**.

The typical use of a hub is at the **centre of a star network** (or as part of a hybrid network) - the hub has cables plugged into it from each computer.





A hub is a '**dumb**' device: if it receives a message, it sends it to **every computer** on the network. This means that hub-based networks are **not very secure** - everyone can listen in to communications.

Hubs are pretty much obsolete now (you can't buy them any more), having been superseded by cheap switches.

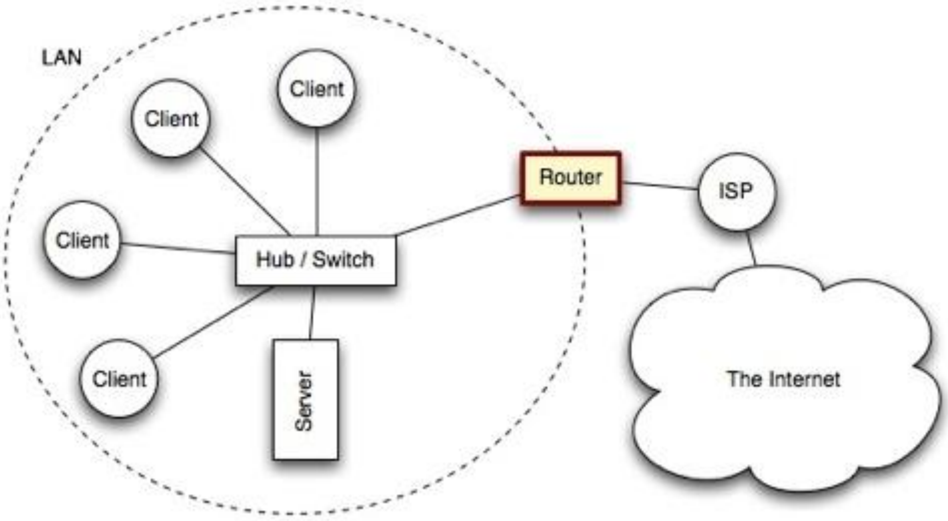
Switch

A switch, like a hub, is a device that **connects** a number of computers together to make a **LAN**.

The typical use of a switch is at the **centre of a star network** (or as part of a hybrid network) - the switch has cables plugged into it from each computer.

A switch is a more '**intelligent**' device than a hub: if it receives a message, it checks who it is **addressed** to, and only sends it to that **specific computer**. Because of this, networks that use switches are **more secure** than those that use hubs, but also a little more **expensive**.

Router



A router is a network device that **connects** together **two or more networks**.

A common use of a router is to **join** a home or business network (**LAN**) to the **Internet** (WAN).

The router will typically have the Internet cable plugged into it, as well as a cable, or cables to computers on the LAN.

Alternatively, the LAN connection might be wireless (WiFi), making the device a **wireless router**. (A wireless router is actually a router and wireless switch combined)

Routers are the devices that join together the various different networks that together make up the ***Internet****.*

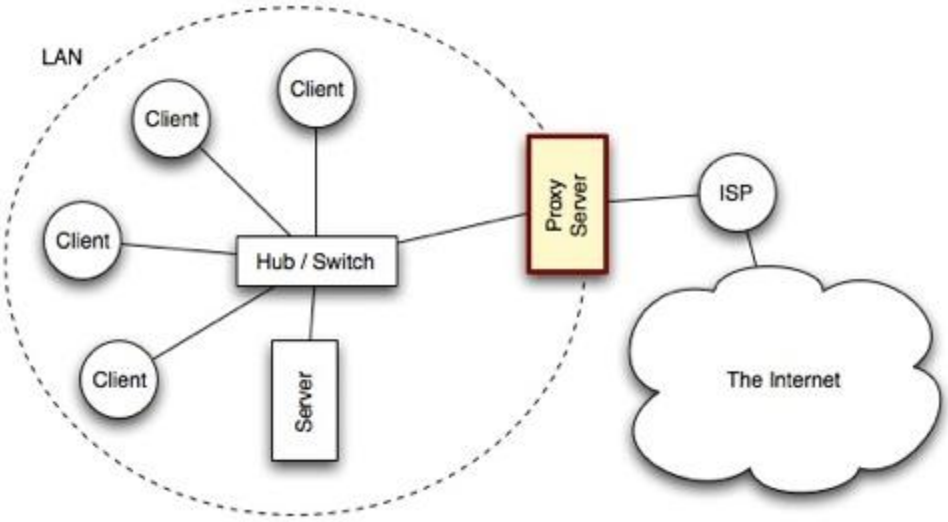
These routers are much more ***complex*** *than the one you might have in your home*

Proxy Server

A proxy server is a computer setup to **share a resource**, usually an **Internet connection**.

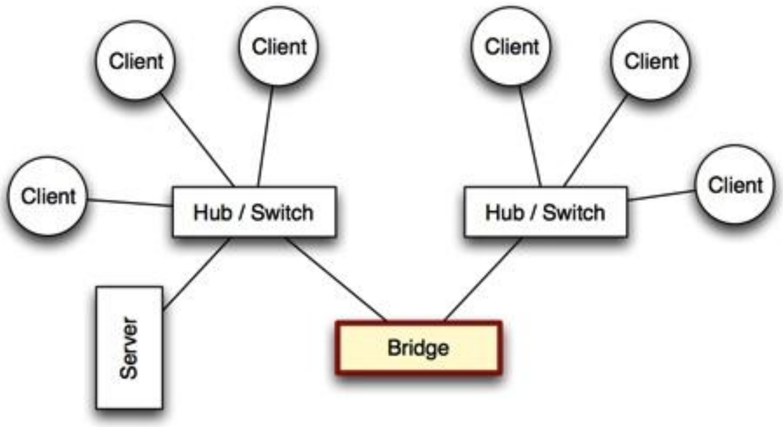
Other computers can request a web page via the proxy server. The proxy server will then get the page using its Internet connection, and pass it back to the computer who asked for it.

Proxy servers are often used instead of router since **additional software** can be easily installed on the computer such as anti-virus, web filtering etc.



Bridge

A bridge is a network device that typically **links** together **two different parts of a LAN**.

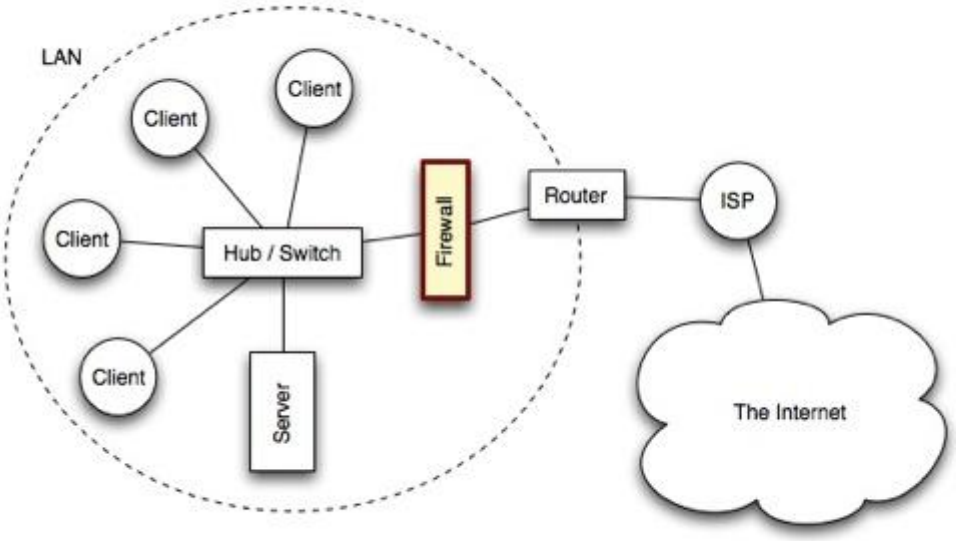


Whereas a router is usually used to link a LAN to a WAN (such as the Internet), a bridge links independent parts of a LAN so

that they act as a single LAN.

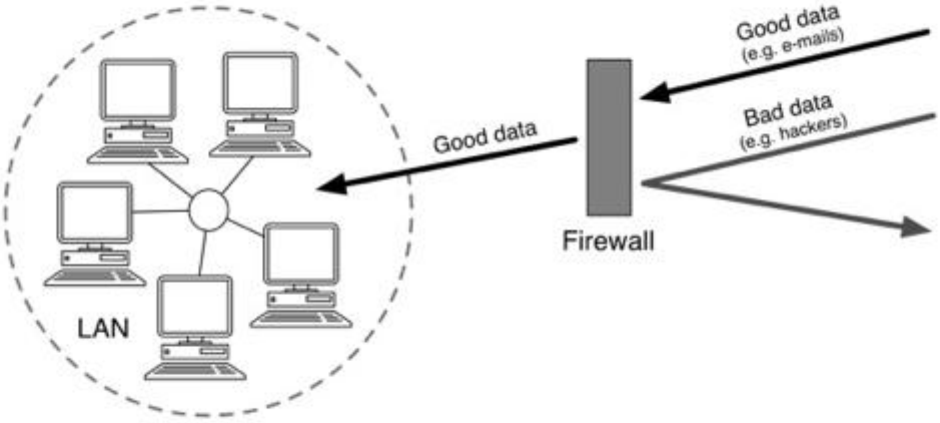
Firewall

A firewall is a **device**, or a piece of **software** that is placed between your computer and the rest of the network (where the hackers are!)



If you wish to **protect** your whole LAN from **hackers** out on the Internet, you would place a firewall **between the LAN and the Internet connection**.

A firewall **blocks unauthorised connections** being made to your computer or LAN. Normal data is allowed through the firewall (e.g. e-mails or web pages) but all other data is blocked.

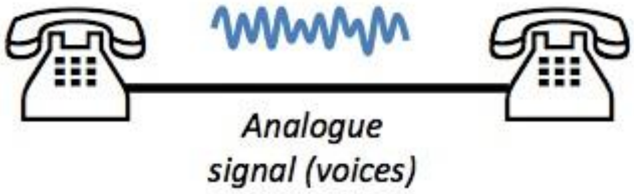


In addition to physical devices, firewalls can also be software.

In fact most computer operating systems have a software firewall built in (e.g. Windows, Linux and Mac OS)

Modem

Before the days of broadband Internet connections, most computers connected to the Internet via **telephone lines** (**dial-up** connections).



The problem with using telephone lines is that they are designed to carry **voices**, which are **analogue** signals. They are **not** designed for **digital data**.

The solution was to use a special device to join the digital computer to the analogue telephone line. This device is known as a modem.

A modem contains a DAC and an ADC.

The DAC in the modem is required so that the digital computer can send data down the analogue telephone line (it converts digital data into **noises** which is exactly what the telephone line is designed to carry.)

The ADC in the modem is required so that the analogue signals (noises) that arrive via the telephone line can be converted back into digital data.

The reason telephone lines were used is that almost every building in the world is already joined to every other via the telephone system.

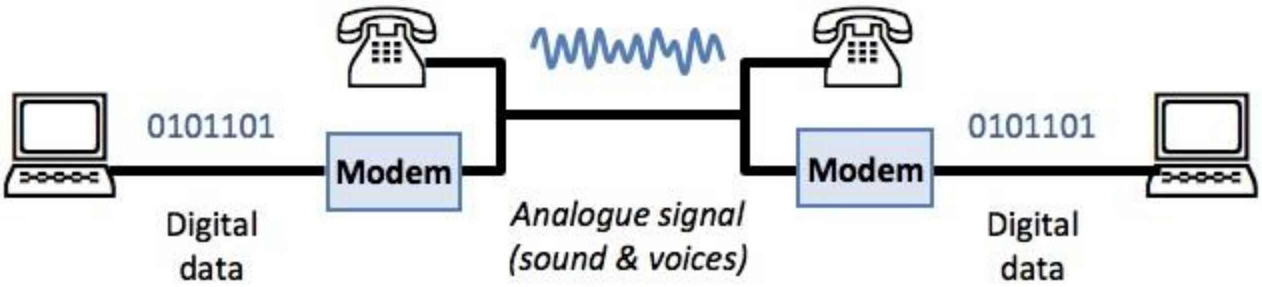
Using the telephone system for connecting computers meant that people didn’t have to install new wires to their houses and offices just for computer use.

In the last few years however, this is exactly what people have done. Special cables have been installed just for Internet access.

These special cables are designed to carry digital data, so no modem is required.

*The word modem is an abbreviation of **MO**dulator **DEM**odulator.*

A modulator acts as a DAC, and a demodulator acts as an ADC.



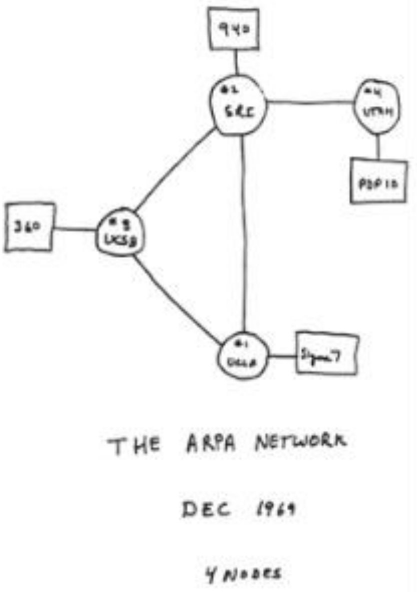
So, simply put, a **modem** is required because **computers are digital** devices and the **telephone system is analogue**. The modem **converts** from digital to analogue and from analogue to digital.

If you have ever used a dial-up connection, you have probably heard the noises sent by the modem down the telephone line.

They sound like a horrible screeching beeping sound.

The Internet

The Internet is a **world-wide network** that has grown and evolved from an experimental network (ARPANet) created by the US military back in the 1960s. Over the years, as more and more computers and networks have connected to this network, it has grown into the Internet that we know today.



The Internet connects millions of people, and thousands of businesses, governments, schools, universities and other organisations.

What Can We Use the Internet For?

The Internet provides the network connections that links computers together. There are many ways that we can use these connections:

- View **web pages** on the WWW (World-Wide Web)
- Sending and receiving **e-mail** messages
- **Sharing files**
- Communicating using **voice** (VOIP) and **video** (video-conferencing)
- Playing **multi-player games**

- Listening to **streamed music** or watching **streamed video**

The small, hand-drawn map above show the plan for the first connections between four computers on the ARPANet. It was drawn by one of the engineers who created the network back in 1969.

From these tiny beginnings, the Internet has grown to a size that would be hard to believe forty years ago.

Statistics published at the start of 2008 show that 1.3 billion people now have access to the Internet (20% of world population).

Intranets

An intranet is the name given to a **private network** that provides **similar services** to The Internet: e-mail, messaging, web pages, etc.

However, these services are **only for the users of the intranet** – they are **private**, not public (unlike Internet services which are generally public).
Businesses and other organisations often have intranets for use by their **employees**.
Typical uses of an intranet would be:

- Viewing **internal web pages** (e.g. company calendars, etc.)
- **Internal e-mail** and **instant-messaging** between workers
- **Sharing of internal documents**

Network & Data Security

As soon as your computer is connected to a network, you have to start thinking about **security** – security of your files, information, etc.

A network allows a person who does to have physical access to your computer (they are not sitting in front of it) to **gain access** all the same. If your computer is connected to a network, other people can connect to your computer.

A person who gains unauthorised access to a computer system is often called a **hacker**.

Preventing Unauthorised Access

There are a number of security measures that you can take to prevent hackers accessing your computer and all of the data stored on it:

Physical Security

The first thing to make sure of is that no unauthorised people can **physically access** (sit down in front of) any of the computers on your network.

For example, by **keeping office doors locked**.

Use a Username and Have a Good Password

The most common way to protect your computer's data is to setup **user accounts** with **usernames** and **passwords**. Anyone not having a username, or not knowing the correct password will be **denied access**.

For this to be effective passwords must be chosen that are **not easy to guess**. Passwords should be a random combination of lowercase letters, uppercase letters and numbers (and symbols if this is allowed):

- 'Weak' passwords: *password, 123456, david, 27dec1992*
- 'Strong' passwords: *s63gRdd1, G66ew$dQ, gdr298783X*

Some computer systems replace the typing of usernames and passwords with other forms of user identification such as **ID cards**, **fingerprint** readers, **voice-print** recognition, etc.

Strong passwords are often hard to remember. Here is a good method for creating a password that is very strong, but also easy to remember:

*Think of a **phrase** that you will never forget...*

"My favourite food is chocolate ice cream"

*Take the **first letter** of each word...*

mfficic

*Change some **letters to similar numbers**: I to 1, o to 0, s to 5, etc. and make some letters (e.g. the first and last) uppercase...*

Mff1c1C

A random-looking mixture of letters and numbers. As long as you like chocolate ice cream you will never forget your password!

Always Install and Use a Firewall

A firewall is a device, or a piece of software that is placed **between** your computer / LAN and the rest of the network / WAN (where the hackers are!)

You can read about firewalls in the Networking Hardware section.

Securing Your Data

Often we have data that is **private** or **confidential**. This data needs to be protected from being viewed by **unauthorised** people. This is especially true if the data is to be sent via a **public network** such as The **Internet**.

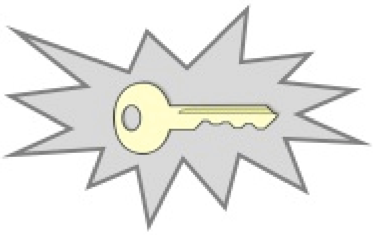
The best way to protect data is to **encrypt** it...

Data Encryption

Encryption is the process of converting information into a form that is meaningless to anyone except holders of a 'key'.

For example, if Alice wants to send important, personal messages to Bob, she must go through the following steps...

Encryption has been used for centuries to protect secrets.



Military leaders as far back as roman times have used encryption to protect important messages sent to their armies, messages that must be kept secret from the enemy.

If the messenger was caught by the enemy, the message, being encrypted, remained secret because they didn't know the code to decrypt it.

First Alice needs to **generate** a secret '**key**'.

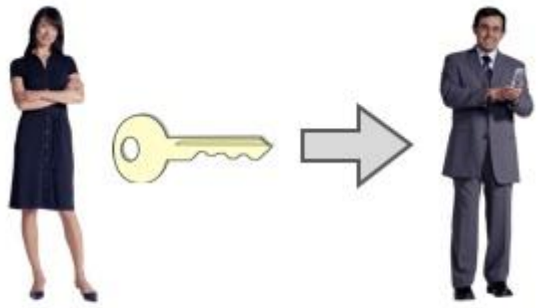
The key is usually a very long, random number.

The encryption scheme shown here is called Symmetric Key, or Single Key encryption.

There are many better schemes, such as Public Key Encryption, but the one shown here is the easiest to understand!

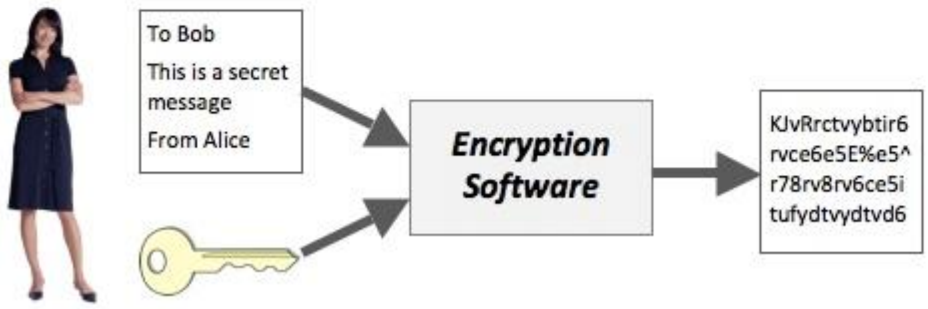
Alice must then **give a copy of this key to Bob**. She must make sure that nobody else can get to the key

(So maybe Alice will visit Bob and give him a copy of the key on a memory stick or floppy disc).



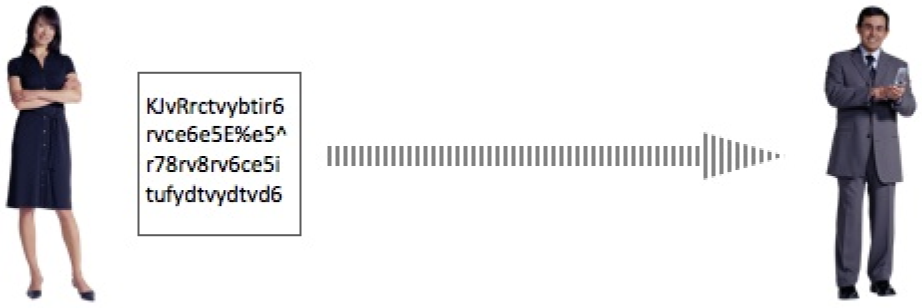
Now that Bob has a copy of the key, each time Alice needs to send him a message she starts by **encrypting** it using special **encryption software** and the **secret key**.

The encrypted message now looks like a jumble of **random letters and numbers**.



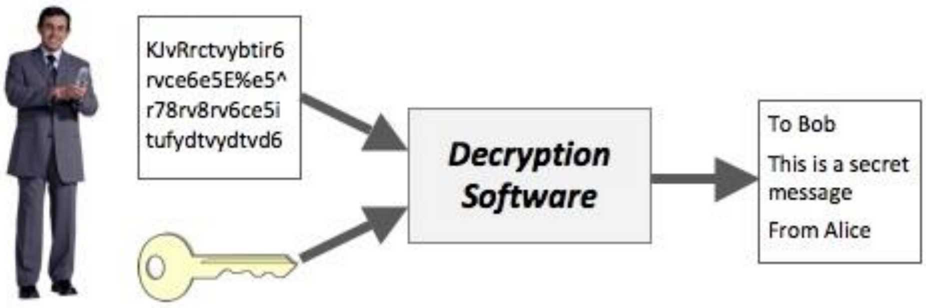
Alice then **sends** the **encrypted message** to Bob.

She can use a **public** network like the Internet, since, even if it gets stolen, the encrypted message **cannot be read or understood without the key**.



When Bob receives the message, he uses special **decryption software** and his copy of the **secret key** to **decrypt** the message.

Bob can now read the **original message** from Alice.


KJvRrctvybtir6
rvce6e5E%e5^
r78rv8rv6ce5i
tufydtvydtvd6
Decryption Software
To Bob
This is a secret message
From Alice