Networks

Local Area Networks

What is a Computer Network?

Two or more computers connected together to share information and resources. This can involve physical or wireless connections, or both.

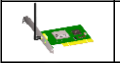
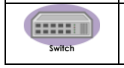
What is a LAN?

A LAN is a Local Area Network. It is a connected set of computers and other devices. Each device is called a node (e.g. computer, printer, etc.). A LAN is installed on one site, over a small geographical area and the network equipment will be owned by the organisation.

Advantages & Disadvantages of Networking Computers

Advantages	Disadvantages
-It allows communication between workers or students -It allows data to be shared -It allows peripherals (e.g. printers) to be shared -It allows computers to be upgraded more easily -It allows distributed processing: the ability for a single program to be run simultaneously at various computers.	-Expertise required to set up and maintain a large network (costly) -Security issues from unauthorised access to data -Measures to secure a network include: *Passwords – strong passwords use a range of character types* *Changing passwords frequently* *Not allowing users to install software* *With wireless access, use encryption*

Devices of a LAN

Image	Equipment
	At least two computers (Nodes)
	Each computer needs a Network Interface Card (either wired or wireless). The NICs convert the data signals from the nodes into data signals that can be transferred across the network.
	Data Transfer Media – the medium through which data is transferred (Wires or Wireless Technology)
	Hub – Connects devices together. Not intelligent – data is sent to all nodes across the whole of the network.
	Switch – Connects devices together. An intelligent device that can sends data to the nodes that the data is intended for, which makes networks faster. *A LAN needs either a hub or a switch, not both*.

Wide Area Networks

A Wide Area Network (WAN) covers a large geographical area – may even be worldwide. Some of the devices in this network may be provided by telecom companies, such as phone lines and satellites.

The Internet

The biggest WAN in the world is 'The internet'. It is a massive network of networks. A ginormous collection of connected computers.

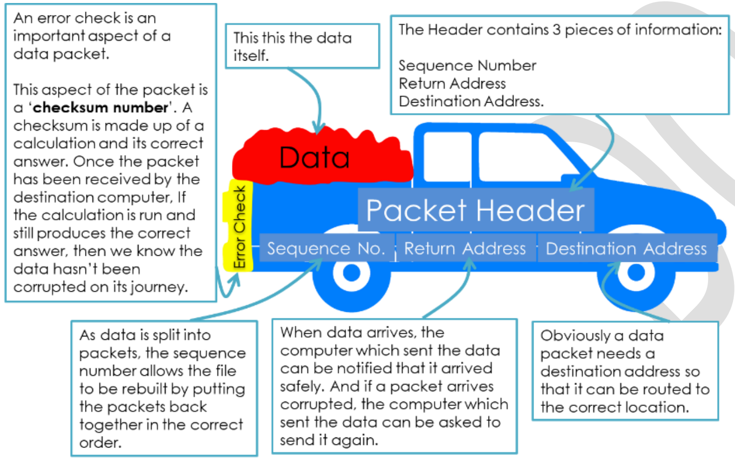
Key Vocabulary

Key Word	*Definition*
Network	Two or more computers connected together to share data and devices
LAN	A network over a small (local) area (building or site)
Network Interface Card	A piece of hardware which converts computer signals into a form that can be sent over a network (and convert them back when network data is received)
Switch	A device which passes networked data to the correct nodes
Data Packets	These are created from the splitting up of a file when data is sent across the internet. It is reassembled at the receivers' end to reform the file.
WAN	A network over a large (wide) area (town, country, the world)
Internet	The largest WAN – A network of networks spanning the world
Internet Protocol Address	The unique address of a website or computer (written in digits)
Internet Service Provider	The company that provides your connection to the internet.
Uniform Resource Locator	The technical term for a web address.
Domain Name Server	Like a "telephone directory" of the internet's websites.

Data Packets

When files are sent across a network, they are split into millions of data packets. Packets get sent by different routes according to availability so therefore some parts of the file might travel one way around the world and other parts may go in the opposite direction! Packets are reassembled at receiving end.

Data Packet Structure



An error check is an important aspect of a data packet.

This aspect of the packet is a '**checksum number**'. A checksum is made up of a calculation and its correct answer. Once the packet has been received by the destination computer, If the calculation is run and still produces the correct answer, then we know the data hasn't been corrupted on its journey.

This this the data itself.

The Header contains 3 pieces of information:

Sequence Number
Return Address
Destination Address.

As data is split into packets, the sequence number allows the file to be rebuilt by putting the packets back together in the correct order.

When data arrives, the computer which sent the data can be notified that it arrived safely. And if a packet arrives corrupted, the computer which sent the data can be asked to send it again.

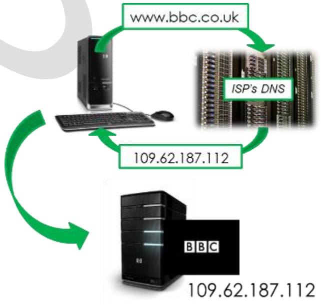
Obviously a data packet needs a destination address so that it can be routed to the correct location.

IP Addresses, ISPs, URLs and DNS

There are many acronyms to understand, when studying how the internet works.

Acronym	Description
IP Address	This means INTERNET PROTOCAL ADDRESS. It is a unique number given to every computer on the internet – no two computers can have the same address. E.g. 109.62.187.112. It's just like a postal address – used to identify a house – no two houses have the same address!
ISP	This means INTERNET SERVICE PROVIDER. This is simply the company who provide you with your internet connection. (e.g. BT or Sky)
URL	This means UNIFORM RESOURCE LOCATOR. This is simply a fancy name for a web address, such as: http://www.bbc.co.uk http://www.google.com
DNS	This means DOMAIN NAME SYSTEM. This is the system used to find the computer which hosts the website you are looking for.

How does DNS work?



1. Computers can only connect to other computers if they know their IP address. However, humans can't easily remember IP addresses!
2. So, when we want our computer to connect to a website (e.g. BBC website), instead of typing in the BBC's IP address, we type in the BBC's website URL.
3. The URL is sent to our ISP (internet service provider) and they look up the URL in their DNS 'address book'. They find it and send back the website's IP address.
4. Now our computer can communicate with the BBC website computer (which hosts the website on the internet), directly.

Network Threats & Preventions

Threats

Threat	Description
Malware	Malware is 'Malicious Software'. Examples of malware are viruses, spyware, adware and scareware. Whereas viruses aim to damage the computer system, spyware, adware and scareware all target the user.
Phishing	Phishing seeks to acquire sensitive information about a user such as their usernames, passwords, bank details etc. The way in which this is done is usually through the form of direct electronic communications (emails / phone calls). These emails or phone calls try to impersonate legitimate companies (such as banks) and ask you to give away sensitive information.
Brute Force Attacks	A Brute Force Attack is were criminals will use trial and error to hack an account by trying thousands of different possible passwords against a particular username.
Denial of Service	This method seeks to bring down websites by using up the web server's resources. This is done by acquiring multiply computers (often through malware) to repeatedly try to access (or log into) a website.

Preventions

Prevention	Description
Penetration Testing	'Penetration Testing' is where a company will invite / employ experts to try to simulate a range of network attacks such as Denial of Service attacks (DoS), SQL injections and Brute Force Attacks.
Anti-Malware	Anti-malware software is dedicated to finding and destroying malware files.
Firewalls	When files are sent across the internet, they are broken down into small packets of data. The part of the computer which receives these packets is made up of 256 ports (you can think of these ports like a country's ports, which manage people in and out of the country). A firewall monitors the data which flows through the ports.
Passwords	Passwords are in place to ensure that a network has no unauthorised access. As seen before, it is important that passwords are strong (long and with a combination of alpha and numeric characters) so that they are harder to crack under a Brute Force Attack.
Encryption	Encryption is where data is scrambled before being sent across a network so that it is unreadable if intercepted.