Computer Networks - AQA Computer Science Cheat Sheet

by [deleted] via cheatography.com/56036/cs/15127/

What is a Computer Network?

A digital telecommunications network which allows nodes (i.e. computers) to share resources.

Pros and Cons of Networks

Advantages:	**Communication**: becomes easier as a result of technology like texting, emailing, etc.
	Flexibility: if information is stored on a network, it means users can access it from anywhere in the world.
	Sharing resources: sharing files and information over a network, including software (can be streamed using web applications) and access to printers.
Disadvantages:	**Hardware**: routers, network cards etc are required to set up a network. This is expensive and requires professional expertise to set up.
	Vulnerability: hackers can break into networks. Malware can spread and damage files on many computers via a network.
	Dependence: users relying on a network might be stuck without access to it.

Wired vs Wireless

Wired Networks

> The computers are physically connected by wires (e.g. coaxial copper cables, fibre optics). They are arranged in **topologies**.

Wireless Networks

> There is no physical connection, as radio waves (e.g. in the form of WiFi) are used to communicate data instead.

Which is Better?

> It is dependent on situation. Wired networks are more reliable, as there is less interference. Security is also easier to manage. However, cabling and other physical components can make it very expensive. Wireless networks allow mobility and flexibility, but are much less secure and interference can occur. Data transfer may also be slower.

Why is network security important?

Network security is a broad term for any measures that protect a network from unauthorized access, misuse, destruction, or the sharing of confidential information. It is important because otherwise sensitive data may be shared or lost. It is also essential from a legal persepctive. For businesses, corporate espionage is another a potential issue.

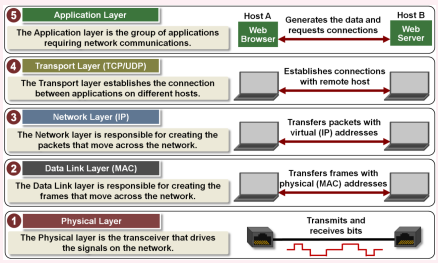
Methods of Network Security

Authentication	Checking the identity of a user, usually by requiring them to input a password or biometric ID.
Encryption	Encoding data it using a key, meaning that the same key is needed to decrypt the data. This is how HTTPS works.
Firewalls	Protects a network from unauthorised access.
MAC Address Filtering	Allows devices to access or be blocked from accessing a network based on their physical address embedded within the device's network adapter.

TCP/IP

TCP	**T**ransmission **C**ontrol **P**rotocol, a protocol dictating how to establish and maintain a network conversation.
IP	**I**nternet **P**rotocol
TCP/IP	A 4-layer model that is essential to networking.
Application Layer	Where the network applications, such as web browsers or email programs, operate. Examples: HTTP, HTTPS
Transport Layer	Sets up the communication between the two hosts and they agree settings such as 'language' and size of packets.
Network Layer	Addresses and packages data for transmission. Routes the packets across the network.
Data Link Layer	This is where the network hardware such as the NIC (network interface card) is located. OS device drivers also sit here.

TCP/IP Diagram



http://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

Computer Networks - AQA Computer Science Cheat Sheet

by [deleted] via cheatography.com/56036/cs/15127/

Network Protocols

Ethernet	A family of protocols that dictate how devices on the same network segment format and transmit data.
Wi-Fi or **WLAN**	A family of protocols that deal with wireless transmission.
TCP	**T**ransmission **C**ontrol **P**rotocol: splits (and later reassembles) data into packets. Also involves error checking, as expects an acknowledgement transmission within a set time frame.
UDP	**U**ser **D**atagram **P**rotocol:
IP	**I**nternet **P**rotocol: each device has an IP address. Packets are 'addressed' to ensure they reach the correct user.
HTTP	**H**ypertext **T**ransfer **P**rotocol: used to access a web-page from a web server.
HTTPS	**H**ypertext **T**ransfer **P**rotocol **S**ecure: u7ses encryption to protect data.
FTP	**F**ile **T**ransfer **P**rotocol: handles file uploads and downloads, transfers data and programs.
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol: handles outbound email. SMTP servers have databases of user's email addresses.
IMAP	**I**nternet **M**essage **A**ccess **P**rotocol: handles inbound emails.

A **network protocol** is a set of rules/conventions that dictate how a network operates.

Network Topologies

What is **network topology**?

> The way that a network is physically structured.

What is **star topology**?

> A network where there is a central **server** that all of the computers and peripherals are connected to.

Advantages of star toplogy:

> 1. If a computer fails, there is no impact on the other devices.
> 2. Security is good, because the data only passes through the server, not any other devices.
> 3. There are no data collisions.

Disadvantages of star topology:

> 1. If the server fails, it's a catastrophe.
> 2. Lots of cabling is need to connect all the devices individually, so it's quite expensive.

Network Topologies (cont)

What is **bus topology**?

> A network where there is a central backbone of cable connecting every computer. At each end of the cable is a **terminator** to stop data from continually being moved around.

Advantages of bus toplogy:

> 1. Cheap.
> 2. Easy to add more devices.

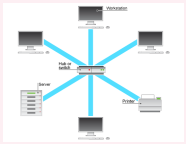
Disadvantages of bus topology:

> 1. Only appropriate for small networks, otherwise data transmission is too slow.
> 2. Data collisions are likely.
> 3. If the backbone is severed, all computers are impacted.

Bus Topology

http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/networkt-opsrev1.shtml

Star Topology



http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/2network-srev6.shtml

Types of Network

PAN	**P**ersonal **A**rea **N**etwork - a network comprising only a small number of devices belonging to only one individual (e.g. Bluetooth).
LAN	**L**ocal **A**rea **N**etwork - a network that encompasses a small area (e.g. one company's network).
WAN	**W**ide **A**rea **N**etwork - a network comprising many devices and covering a large area (e.g. the Internet). Often under collective ownership.