A WAN covers a much larger geographical area than a LAN. The largest WAN is the Internet. Smaller examples of a WAN would include a **national ATM network** used by a bank.

**IP Addressing**. An Internet Protocol (IP) address is a unique address number which is given to devices that uses the Internet Protocol.

Each address has to be unique as it is used to identify one device on a network, allowing data to be sent to the correct device and returned to the device that requested it. An IP address can be **private**, (for use on a LAN) or **public** (for use on the Internet or another WAN).

**MAC Addressing**. In computer networking, a Media Access Control address (MAC address) is a unique 48-bit number which is given to any hardware device used to connect to a network. MAC addresses can be using on a LAN. MAC addresses are usually displayed as hex.

**Data Packets**. Modern computer networks, including the Internet, carry data by breaking it down into data packets, rather than sending it as a continuous stream of data. A typical data packet might contain 1,000 to 1,500 bytes.

**//Technology packet switching** makes the network more efficient because the network can balance the load across various pieces of equipment and if there is a problem with one piece of equipment in the network then packets can be routed around it.

**Protocols**. A communications protocol is rules for hardware/software how to communicate with digital data. The protocol may also define how devices authenticate themselves and may define how error checking and correction takes place.

Examples of communications protocols used for the Internet:

**The Internet Protocol (IP)** – used to route data packets between networks and over the Internet.

**The Transmission Control Protocol (TCP**) – used to exchange data between two networked computers.

**HTTP (HyperText transfer Protocol):** used on the World Wide Web for transferring web pages ;

**FTP (File Transfer protocol):** used for transferring files from one computer to another.

**SMTP (Simple Mail Transport Protocol)**: used for email;

**TLS/SSL (Transport Layer Security / Secure Sockets Layer):** Encryption protocols used with secure communications over the Internet.

**Network security techniques**. A network needs security to prevent unauthorized access to the information stored on the network. **User access levels**: most network security involves users having different levels of user access to the network. The network manager will have full access to all software on the network but other users may be not allowed to some areas of the network, only have READ access to files .

**Suitable passwords:** a password is used in combination with the username to prevent unauthorized access to a network. A suitable (strong) should include a mixture of upper-case and lower-case letters, numbers and even symbols . Many network authentication systems will require users to regularly change their passwords.

**Access restrictions**: users can log in special hours of the day from their computers.

**Encryption**: files can be encrypted making the data sensless without the correct numerical key to decrypt it.

**Physical security**: CCTV, door locks, laptop lock-down cables and swipe-card systems etc. can be used to physically restrict access to networked computers.

**Firewall:** this can be a device or be software-based. Its purpose is to control network transmissions between networks.

**Antivirus software**: Many viruses are designed to bypass security systems and having up-to-date antivirus software installed will reduce this risk.

**Proxy server:** this can be a device or be software-based and uses a set of rules to check that the file, connection or web page the user requests is acceptable. It can filter network traffic by IP address or protocol. If the request is valid then the proxy server makes the connection .

**Wi-Fi access restrictions** should be in place to allow only legitimate computers to connect to the network. All data transmitted over Wi-Fi should be encrypted using the highest level available.

**Filtering:** certain websites can be blocked by filtering. However, this only increases security if the sites are known security risks, for example they distribute viruses.