TABLE OF CONTENTS

Section 3

NETWORKS

3.1 Network Fundamentals

Computer Network A computer system or set of systems which uses communication equipment in order to connect computers and share their resources and data.

Node Device on a Network

Server A Computer program, Software or Host Computer that fulfils requests from client programs and serves as a Central Repository of data and programs which are shared by these clients.

Client Computer Hardware or Software Device that accesses a service made available by a server, achieved by sending a request for service. (e.g. email software client requesting email server software to fetch new emails).

Unlike a Server, the Client does not share any of its resources, but requests content.

Hub Connection point for all devices on network, connected through Ethernet cables. Data from one device goes direct to the Hub, which share this to all devices.

The intended recipient accepts this data, all other devices ignore it.

Although transmission to every port ensures that data reaches its destination, the effect of this creates a lot of traffic on the network, which slows down transmission.

Switch	Also the connection point for multiple devices on a single network; however a Switch can identify which device is connected to which port, so can send Data to the Target Device directly. Because of this, Networks connected using a Switch have faster data transmission than those connected using a Hub.
Router	Used to join Multiple Networks and is used as an intermediary between these so data may be exchanged efficiently between devices (e.g. Connecting a home Network to the Internet).

Type of Networks (3.1.1)

Revised

Local Area Network (LAN)	Network devices are connected within a Limited Geographical Area (e.g. a room, home, school, office building, etc). Usually client-server mode of operation, with Shared Data and Resources (e.g. Peripheral Devices).
Peripheral Devices	Examples include Printers, Scanners, External Hard Drives which provide increased functionality.
Virtual Local Area Network (VLAN)	Different sections of a LAN may not want to access all the available shared data (e.g. Different departments in a School), as such a LAN can be split into separate VLANs, the new network is known as a Logical Separate Network. Each Logical Separate Network cannot access the other shared resources (e.g. Data, Peripherals) without being granted special access.

Wide Area Network (WAN/GAN)	Connects different computer systems or LANs from different geographical areas, can span over a city, country or the world (e.g. internet, different sites of organisations connected). A WAN would require Security; using login, passwords, security questions and encryption.
Storage Area Network (SAN)	Type of LAN created so that large storage devices can be accessible from servers in a convenient and easy way, and is able to handle large data transfers.
Personal Area Network (PAN)	Network covering individuals Workspace, essentially a LAN which only supports one person, instead of a group of people (e.g. Peripheral Devices connected through USB/Bluetooth).
Peer-To-Peer Network (P2P)	Network with no centralised server. All nodes are client and server at the same time, consuming and supplying resources from and to other peers. This makes resources more widely Available and supports File Sharing for Collaborative Work.

WIRELESS LOCAL AREA NETWORK (WLAN)

Like a LAN, a WLAN Connects nodes in a Limited Geographical area but achieves this without the use of cabling and wires.

This requires technology such as a wireless Router or Modem; Access points; Switch; Wireless Repeaters and so on.

Network Reliability depends on the strength of wireless signal and distance from router, and on the type of Network Topology and shape of surroundings. Furthermore, multiple connection points on the Network may reduce transmission speeds.

Advantages:

- Possibility of user collaboration and make access easier due to wireless transmission. Quick access with mobile devices; Anywhere in the scope of the WLAN and therefore do not need to be present at a workstation.
- Allows users to bring their own device which has a more familiar interface, could lead to greater efficiencies and fewer usability issues.

  Could lead to insecure devices, but could be resolved with clear company policy regarding use, Virtual Testing 'Sandbox' could protect against Viruses, MAC address authentication and testing, other security features in order to address.
- No extra equipment is needed for expansion after the initial set-up; which will save time and money.
- Reduces wiring therefore increases the safety for employees.
- User-mobility and Economical access points.

Disadvantages:

- Poorer Security as devices from outside can access the Network and Intercept Transmissions, since transmission goes 'through the air'.

  Could be resolved by strong encryption/protocols, e.g. WPA-2 or use of trusted MAC addresses, and regular changes of the router password.
- Open to Misuse; as an administrator cannot directly monitor a specific user or device.
- Data transfer will Decrease (compared with a wired LAN) because the number of computers using the network increases and because the WLAN has a lower bandwidth than a wired LAN.
- Intermittent Connectivity due to physical barriers; this may result in Lower Transfer Speed, Weakening of Signal and may reduce Operations and Efficiency.
- Wireless signal could be weak in some placed; Leading to frustrated/ineffective users.

Internet

A Global WAN connected through an Internet Service Provider (ISP) in exchange for a monthly fee (Broadband cost).

The Internet is decentralised by design, any independent Computer able to access the internet and share resources becomes a Server of its own.

Ethical Issues include: Some information presented online may be deliberately incorrect and not subjected to validation and scrutiny; Further issues such as plagiarism and Intellectual Property.

Extranet

Computer network that utilises the Internet. Works like an External extension to a LAN. Part of a network that uses internet protocols to allow Limited access by specific users to a LAN or WAN.

(e.g. Business wants to share some data/ information with clients or partners but not all, so extends part of the network, creating an Extranet, available for access but with security/privacy measures).

Ethernet

Ethernet is more reliable as the strength of the signal is independent from the distance from the router (in comparison to Wireless Network transmission). There is also no issue with the network topology type and nature of the surroundings, so long as the user is connected. Connection does depend on the condition of the cables; any loose or broken cable connections will reduce or fail transmission.

The Speed of Transmission across a Network may vary due to different parts of the Network using different Media, Network congestion, Data Packets taking different routes; The Receiver may be busy or simply the Physical size of the Network.

Virtual Private Network (VPN) (3.1.5)

Revised

A VPN allows clients from distant locations to connect, that otherwise wouldn't be able to connect with LAN (too far through cables) or WAN (too far for signal to be picked up). Tunnelling allows the clients device to appear to be a node of the internal Network; thus affording the client full access to the Network resources. The Network protocols (e.g. IPSec or TSL) are still secure despite passing over an outside Network.

Transmission is always encrypted and provides a secure connection; established between sender and receiver (both sender and receiver are authenticated before transmission); therefore any unauthorised access will not be able to understand the data.

Data is hidden through the use of hidden IP Addresses, Encrypted connections, multiple Exit Nodes, Tunnelling (sending a Packet within a Packet and encrypting it).

Technology Required to Provide VPN (3.1.4)

Revised

- SSL 3.0 (Secure Socket Layer 3);

  TLS (with encryption - Transport Layer Security);

  IPSec (Internet Protocol Security) to encrypt and authenticate traffic over virtual tunnels.

  Requires special Client Software, whereas SSL and TLS are supported by all Web Browsers.

- Tunnelling protocols; Allows the data to be encapsulated (hidden) whilst travelling across the internet. Encryption protocols (IPSec) if hacked will not be decipherable. The use of Gateways allows the person to connect with the central Server.

- Hardware for pubic networks like the internet through tunnelling, which allows the network to send data via other networks connections as if connected to a LAN.

- Hardware/Software requirements like internet access, VPN software, routers.

Advantages of a VPN:

- Information can be accessed in remote places.
- Lower Cost; No need for long-distance leased lines.
- Enhanced Security; data intercepted is undecipherable and security properties of each tunnel are agreed by the administrators of the two Endpoints of the Tunnel.
- Nobody outside the VPN should be able to affect the security properties of the VPN.
- Multiple Exit Nodes; makes it hard to distinguish where the Data was Generated and thus More Secure.
- Can change Working Patterns; allowing Employees to work from home and reduce travelling time, beneficial for Workplace Efficiency and reduces Environmental Costs.

Disadvantages of a VPN:

- Needs professional with detailed understanding of security issues and configuration to ensure sufficient security and protection.
- Reliability of VPN is not directly under the organisations control, but under the ISP.
- Not all VPN products are compatible across different vendors.

VPN VS EXTRANET	
Access and Transmission are always Encrypted	Limited level of Encryption
Users have Access to Everything	Only have access to Enabled and Specific Services
Authenticate the Sender before establishing a Tunnel	

Importance of Standards in Construction of Networks (3.1.2)

Revised

Common Rules and Standards are crucial to the formation of a Network, otherwise Systems may not be able to connect and communicate due to Incompatibility.

Standards play an important role in the construction of Networks; and can be thought of a common 'Language' that enables compatibility.

Network Communication Layers (3.1.3)

Revised

An application goes through different layers to send data between systems.

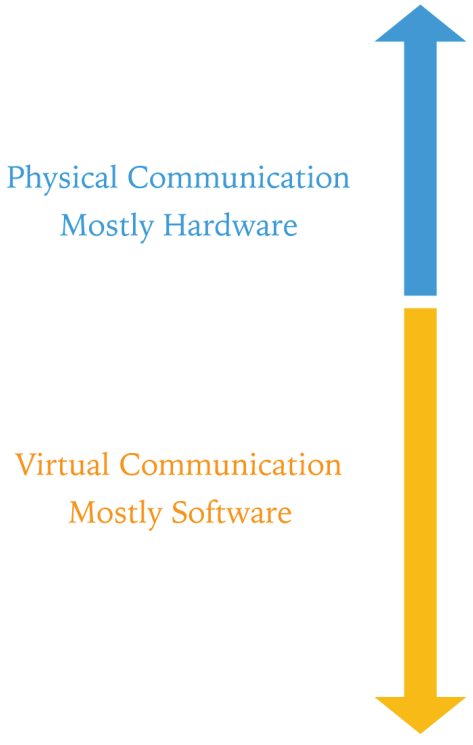
If one software application is trying to send Data to another software application, it must be encoded into a format which is understandable by both software applications; to achieve this data is broken into Packets (which contain the data and the address of its destination).

Each layer has its own protocols; and the most widely used Networking Standard is the OSI Model and works as a reference which describes and explains each stage of the network communication process.

Open Systems Interconnection (OSI)	Model This model define layers of network interaction.

The OSI is a standardised system/model for network connection and consists of 7 Layers, each dealing with specific parts of Network Communication (for example the physical layer which defines the physical connection).

1. **Physical** *(Cabling system components).*
2. **Data Link** *(Network Interface Card).*
3. **Network** *(Routing).*
4. **Transport** (*Transmission, Error detection).*
5. **Session** *(Retransmission of data if not received by device).*
6. **Presentation** *(Encryption and decryption of messages for security).*
7. **Application** *(The end-end-receiver application, e.g. email).*



3.2 Data Transmission

Unit of data for transmission with a format, it is part of a message made into a single package. Contains address and data.

It contains a set amount of data; it contains a fixed structure (or identify elements of the structure other than data); it contains data that is to be sent via a communications channel; it also contains specific details for transmission (e.g. address of sender and receiver, error codes, etc).

Data Switching (3.1.11)

Revised

Network communication method: Original file is divided into packets before transmission, each of these packets may follow a different path to the destination address.

- Packet Switching involves Splitting Data into Packets and sending these from source to destination through different routes, using Network Switches and Routers

- Network Switches and Routers are intermediate devices which determine how best to transfer the packet on the path to its Destination (rather than flowing over a singe wire).

- In order to achieve this, there are Rules and Standards used to compile and transmit each packet in a Standard Format. Packets must be constructed in exactly the same way so that the Receiver knows automatically how to decode its contents, and does not require further instruction for decoding the Packets.

- These will have Protocols that contain the Receiver Address, so the Packet knows where it needs to be sent and Packet Numbers which identify which Sequence the Packets are sent in.

NEED TO KNOW:

- **Address;**

  Have to be in standard format so that each switch/ routing station recognises the address.

- **Address of Sender;**

  Identifies the sending computer, so that any packets not received can be re-requested.

- **Address of Receiver;**

  Identifies intended recipient so it can be forwarded on correctly.

- **Protocol;**

  Must be identified so that the correct rules are followed.

- **Size of packet/fields;**

  All packets/fields must have the same size so that data can be reassembled.

- **Sequence Number;**

  So that packets can be reassembled in correct order.

- **Transmission Codes;**

  To show whether the data packet is transmitted or re-transmitted.

- **Control Bits;**

  To Maintain the integrity of the data by ensuring that the data received is the same as the data sent.

- **Error-Checking Code;**

  When an error is detected, an algorithm either corrects the error or requests that the packet is resent.

Protocols (3.1.7)

Revised

Sets of rules for transmission; to facilitate a process being carried out correctly.

In the case of Data Transfer, protocols are rules that ensure data is transferred correctly between systems. A protocol recognised as the standard for a certain type of transfer is called a 'Standard Protocol'.

Protocols ensure the presence of an identified Sender and Receiver and the agreed Method of Communication. It also provides rules about Format; Data Compression; Error Checking/Validation and the Recovery and Resending of Data.

WHY PROTOCOLS ARE NECESSARY:

- **Data Integrity**

  Ensures data is not changed or corrupted during transmission.

- **Flow Control**

  Network infrastructures have limited memory and bandwidth, the Transport Layer (4) is responsible for using Protocols to manage situations where an overload of resources occurs.

  (e.g. Transport Layer could request a Sending Application to slow down its data flow rate to manage Network Congestion).

- **Deadlock Prevention**

  Prevents situation where two or more Network competing actions are each waiting for the other to finish, and thus neither ever does.

- **Congestion Management**

  Prevents requests on network resources from exceeding capacity.

- **Error Checking**

  Ensures the validity of data

EXAMPLES OF INTERNET PROTOCOLS:

- **Hypertext Transfer Protocol (HTTPS)**

  Creates a secure transmission of data from Client to Server.

- **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**

  Encryption protocols used on the Internet. Allows for things like secure payment.

- **Internet Protocol Security (IPSec)**

  Encrypt and authenticate traffic to ensure secure transfer over VPN tunnel.

- **Dynamic Host Configuration Protocol (DHCP)**

  Allows the server to automatically assign IP address to client device.

Data Compression (3.1.9)

Revised ☐

Data Compression reduces the size of files to be transmitted over a Network; which will take up less Bandwidth and reduce overall Transmission Time. The recipient will have a program that can decompress the contents of the File.

Lossy Compression — Permanently deletes certain information, only part of the original data is displayed when compressed.

This is an acceptable solution for formats such as JPEG, GIF, MP3 as the difference isn't easily noticed.

Lossless Compression — Only eliminates data which has 'statistical redundancy', all original data is still available when decompressed.

This is typically used for Word files, which are small and easily decompressed.

TRANSMISSION MEDIA

Wireless — Compared to metal cabling (Ethernet) and Fibre Optics, wireless is the least reliable and slowest; but is the cheapest form of transmission.

(e.g. Microwave, Radio Signals, Satellites, WiFi).

Metal Conductor — Faster, more reliable and expensive than Wireless but still cheaper than Fibre Optic cabling.

(e.g. Copper cable, UTP Cable, Coaxial (TV) Cable).

Fibre Optics — Fine optical Fibres carrying beams of Light as signals. Fastest, most Reliable and Secure but also the most Expensive transmission option.

FACTORS THAT AFFECT SPEED OF TRANSMISSION

- Bandwidth (theoretical speed of the Network).
- Data transfer Rate of Storage Devices (interference, traffic, number of connected devices, errors, type of Files, malicious software).
- PC System Performance (CPU Speed; RAM)

3.4 Network Security

Encryption Altering a message into undecipherable form to those unauthorised. Only a recipient with the correct Key can decode the message and read it.

Symmetric-Key Encryption (3.1.15)

Revised

The same Single or 'Secret' Key is used for Encryption and Decryption; each device uses this to Encrypt a packet before it is sent over an Untrusted Network.

Reasons For:

- Faster than using a Public Key
- Uses less computer resources

Reasons Against:

- Keys must be shared before they are used.
- Risk or Key becoming known by unauthorised individuals, another one must be used.

Public Key Encryption (3.1.16)

Revised

Also known as 'Asymmetric-Key Encryption'. A Public Key for Encryption and a Private Key for decryption are both mathematically linked. SSL and TSL Protocols use this form of Encryption.

Reasons For:

- Both sender and recipient don't need to share Key beforehand to communicate.

Reasons Against:

- Messages take longer to encrypt and decrypt.
- Authenticity of public key needs to be verified.

'MEDIA ACCESS CONTROL' ADDRESS (MAC)

- The MAC Address identifies a specific device through its unique 12 Characters (via Network Card/Controller) which is checked against a list of approved addresses — if not on this Whitelist then Access is Denied.

- This prevents Unauthorised Access very difficult, unless the NIC has been cloned; but generally provides an Additional Layer of Security since data sent to a specific MAC Address can only be accessed on the specified device.

Reasons For:

- Extra Security

Reasons Against:

- Danger of allowed list of MAC addresses being discovered.
- Difficult to manage the list as it grows.

User ID — Uses password to access networking device and/or another password to access the web interface used to set up a Wireless Router or Access Point.

Reasons For:

- Easy to use.
- Prevents unauthorised access.

With web interface password, a person cannot access web-based utility page of router/modem/ access point unless they have the password.

Reasons Against:

- Entering password each time may be time consuming and inconvenient.
- Weak passwords are easy to crack and gain access.

Firewall

Either as; Software installed on each device, or Router Hardware firewall that protects from Hackers accessing devices through wireless connection.

Filters incoming traffic and can block some messages coming through, as well as control/limit users own access to the internet. Extent of firewall use depends on an Organisation's Policy

(e.g. One organisation ay not only allow communication between users and outside the network via email, but restrict website access also)

Reasons For:

- Software firewall monitors traffic between device and network and prevents unauthorised access.
- Router hardware firewall prevents unauthorised persons getting access to the network.

Reasons Against:

- May slow down the device.
- Issues about censorship with software firewall, depending on the organisation.

Router hardware firewall prevents unauthorised persons getting access to the network.

METHODS TO INCREASE NETWORK SECURITY

- Giving each user appropriate Login Details and Strong Passwords.
- Different Access Rights for Students, Teachers, Admins, etc.
- Encryption of all Passwords and Files.
- Use of the latest WiFi Protocol (WPA2) Security.
- Require MAC Address and Authentication.

BRANCHING STATEMENTS:

break	Terminates a loop when a value is found or statement block complete (expressed at the end of the statement block).
return	Exits from the current method and returns to where the method was originally invoked. By specifying a value with return, the exit can be achieved whilst sending the value back (e.g return num1;)

OBJECT CREATION:

A Class contains Constructor Methods that are invoked to create objects from the Class template.

Constructor Methods always share the same declaration name as the Class.

To create a new Bicycle object called myBike, the Constructor Method is called by the new operator. Creating an Object is the same as 'instantiating a Class'.

```
public Bicycle(int startGear, int startSpeed)
                        {

. . .

Bicycle myBike = new Bicycle(2, 0);
```

Therefore myBike is an instance of the class of Bicycles and has attributes startGear of 2 and startSpeed of 0 both of type int.

OBJECT REFERENCE:

In order to refer to the Fields within an object outside of the current class, an 'object reference' expression must be used with the dot operator:

Fields

```
motorBike.startGear;
```

You can use 'object reference' to invoke (call) an Object's Method. Additionally, any arguments within the parentheses can be provided:

Methods

```
myBike.setName(nameBike);
```

Parameters are the list of variables in a method declaration (also typically separated by commas).

Arguments are the actual values passed in when the method is invoked.

When an argument, stated inside the parameters, is passed through the Method; the internal processes of the Method use the argument temporarily in order to perform a calculation.