3.3.3 Networks and Communications

(a) LAN, WAN and Virtual Networks

A network joins together a number of computers and other devices so that they can communicate and exchange data. The actual method of communication varies from network to network and depends to some extent on the physical size of the network. Small networks are often constructed with simple cable connections linking computers, printers and so on. Large scale networks may use fibre optic and satellite links. Because of these differences, small scale or LAN networks are considered separately from large scale or WAN networks.

LAN Networks

Local Area Networks are installed within a single room, building or site normally connecting PCs together although they may include a mini computer. Normally a LAN network will have a file server to manage backing storage centrally although in some networks the link is between one PC and the next without a file server. This is called a peer to peer network.

A principal advantage of having a LAN is the ability to share printing and other peripherals such as scanners and the facility to send and receive messages using the network. Network printing may be via a dedicated or non-dedicated printer server. If there is a file server then this may act as printer server too. Network printout would be spooled to disk allowing a number of computers simultaneous access to the printer.

LAN cable may be fibre optic or simple twisted pair although many LAN networks also use wireless communication. Data is usually transmitted digitally as pulses and, since pulses cannot travel any distance along an electric cable without distortion, this limits the maximum length of cable that can be used for a wire based LAN. Each LAN computer will need a network card to allow connection to the LAN and to deal with communication with it. Network operating software will have to be installed on both the local workstation and on any servers present on the LAN.

WAN Networks

Wider Area Networks link computers - usually including mainframes, PCs and dumb terminals situated on different sites. These may be in different towns, countries or continents either using public telephone links or a dedicated landline to communicate data. If the link is electrical then a modem will be needed at each node. Electric cabling is now being replaced by fibre optic that can transmit digital data directly so that a modem is not required. In addition a single fibre optic cable can carry a large number of different transmissions simultaneously and it is not subject to the electrical interference associated with wire transmissions.

Virtual Networks

When something is virtual it appears to exist but is not, in fact, really there. The virtual network uses the physical connections and hardware of a real LAN or WAN but the user's computer does not 'see' that actual network but only a certain part of it.

As an example, suppose a school has a LAN that is used for pupils (curriculum) and also for administration. There might be a single LAN infrastructure that is used by both administration and curriculum computers. However the network administrator could set up two virtual LAN networks. Computers on the administration network would see only other administration computers. Curriculum computers would be able to communicate only with other curriculum computers. If a teacher, for example, needed to log on to the administration network, he or she would have to use an administration computer.

Each set of computers would, as far as the users were concerned, appear to be on different networks with each having their own file and printer servers These two different networks are called virtual networks because, although this is what the users and their computers experience, there is in fact only one physical network present. A virtual network can be categorised as LAN or WAN depending on its physical size. The letter 'V' is usually used to identify it as a virtual network (VLAN and VWAN).

(b) Intranets, Extranets and the Internet

A network allows users to share resources such as data and, on a LAN, hardware devices. It also serves as a medium for communication and this aspect of network use is becoming more important.

Intranets

Many businesses, schools and other organisations now use their local area network to provide Internet like services such as email from a private server. The services may also extend to the presentation of information, links and files in a web page format, using a hyperlink based interface. Other Internet-like features may also be made available on the network. These might include email, conferencing as well as specialised services such as an electronic meetings diary.

A private network providing Internet like services, but for which access is restricted to employees or people belonging to the organisation, is called an Intranet. An Intranet is not necessarily connected to the Internet and, if it is, external access to the intranet is likely to be restricted.

Where the Intranet is connected to the Internet communication can be two way so that connection from the Internet to the Intranet is possible. This external access can be restricted to employees and security will be maintained by use of a firewall. This type of access may allow employees to work from home for part of the week while still maintaining an electronic presence in the office. Access to the company Intranet will provide them with the information that they need to carry out their work and also all them to submit memos, reports and other data while also keeping in contact with colleagues who themselves may actually be working from home. This pattern of working is often referred to as teleworking.

Extranets

Sometimes a company will want to allow limited access to its Intranet to others, perhaps to the employees of another company with which it does business, so that data can be exchanged. The network is then called an Extranet to distinguish it from the private, more restricted access of an Intranet.

An extranet could be used to allow authorised dealers to order supplies from a company or to find information about new product launches that the company would not want to be generally available outside its dealer network.

Internet

Across the world many different and separate networks have been linked together to form a complex super-network which is, in essence, a network of networks. This is called the Internet. When you use a broadband connection to link to your Internet Service Provider's computer you are linking to a computer that is connected to the Internet. It is providing you with the service of linking you to the Internet.

The Internet consists of the hardware, software and communication and addressing rules needed to allow these different networks to communicate with each other.

The Internet is used for a large number of different purposes. Perhaps the most frequently used of these is to provide access to the World Wide Web. The web consists of a very large number of web pages which use a special file format (HTML) so that, once downloaded they can be displayed by a web browser on any client computer. An important feature of the World Wide Web is that the HTML pages contain hyperlinks to other web pages. The World Wide Web therefore consists of a number of different web pages which can be linked using hyperlinks and which can be displayed on a computer using a web browser and when you view a web page you are using the Internet to download a part of the World Wide Web.

Other uses that the Internet has been put to include delivering email services, providing access to music, television and film downloads, gaming, shopping, banking and social networking.

(c) Client-Server and Peer-to-Peer Networks

A peer to peer network has no file server and there is no central storage, but each user stores his or her own work on their computer's local hard disk. Files and software on other network computers will be available through the network but access to them will normally depend on the owner having granted the necessary access rights. Similarly hardware devices attached to other computers will also be generally available if users choose to make them so.

A peer-to-peer network is less costly to set up since there is no expensive file server. It is also cheaper to maintain since there is no need to have a network manager responsible for maintaining the file server and a centrally held user password file.

However, with each user essentially managing his or her own computer and associated security, a peer-to-peer network is generally less secure than a client server network. Also, since files are held on individual computers rather than on a central server, each user will be responsible for his or her own backup.

Peer-to-peer networks are most often used for home networking.

A server-based network has a central file server which may store central copies of both software and data files. Each user will be allocated disk space on the server and access will be controlled by use of login names and passwords. This type of system is more dependent on the connection to the server being maintained. Cable failure or server crash disrupts the network and users may not be able to use their workstation at all – especially if software has been installed on the server rather than on the local hard disk.

In addition to a file server, this type of network will often have one or more print servers which will manage print jobs. Network printout would be spooled to the server disk to be despooled by the appropriate printer server. This approach allows a number of users to apparently access a single printer at the same time.

A server based network is more complex to set up than a peer to peer network and it needs a network manager to create users, grant access rights and allocate space on the server as well as install software on both the server and the workstations. Control and consequently a high level of security is therefore easier to maintain. Since users' data is stored centrally on the server, a proper backup strategy for the server will ensure that all data is safely backed up without relying on individual users remembering or bothering to back up their own data files.

(d) Bandwidth and Media Internet

The bandwidth of a communications channel is the difference between the maximum and minimum frequency of signal that it can carry. This is directly related to the capacity of the channel, that is, the number of bits per second that the channel can carry. In simple terms, more bandwidth means more data is transmitted faster.

While the signal strength and noise levels on the channel also affect the capacity, doubling the bandwidth will double the capacity. If the noise level (interference) increases then capacity decreases. The bandwidth and, to some extent the noise level, are decided by the medium used to carry the signal. Different media have different bandwidths and therefore different data carrying capacities. Moreover, because of the noise factor, the same medium under different external conditions may have a very different capacity.

The table gives the maximum capacity that can be achieved for various media. In practice external factors will mean that the actual data transmission rate is lower than that given.

Medium	Capacity
PSTN (Public Switched Telephone Network)	56 Kilobits per second
ISDN (combining two channels)	128 Kilobits per second
Twisted Wire	10 Megabits per second
Coaxial Cable	10 Megabits per second
Microwave (wireless)	100 Megabits per second
Fibre Optic Cable	10 Gigabits per second

Figure 21: Capacity of Different Media

(e) Network Components

Many different devices are used to construct networks. The actual devices needed depend on both the type of network being constructed and the medium being used to carry the data. Figure 22 shows some of these devices on a typical LAN and this section describes the roles of these and other devices that are commonly used.

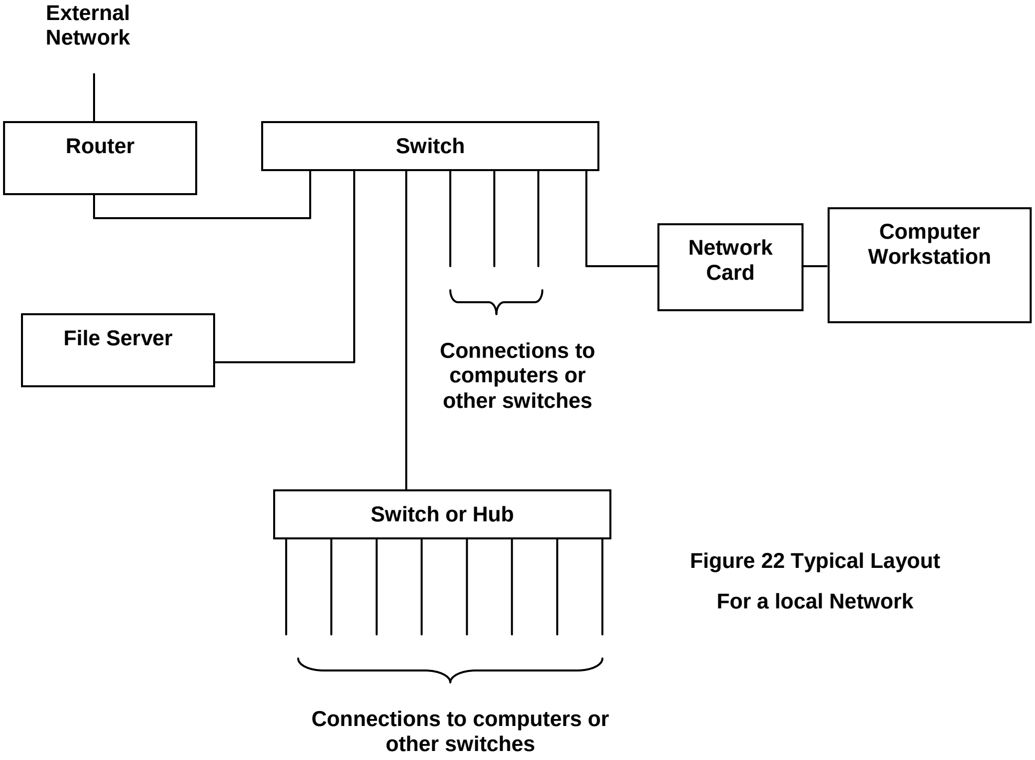
External Network
Router
Switch
Network Card
Computer Workstation
File Server
Connections to computers or other switches
Switch or Hub
Connections to computers or other switches

Figure 22 Typical Layout For a local Network

Switches

A switch consists of a number of connections or ports. Network devices or other switches can be attached to these ports. The switch's memory will store the addresses of each device that is attached either directly or via another switch to each port in its memory. When data is received via one port the switch will output the data to the port to which the intended destination is connected. This means that data being output from a switch is travelling only along cable that the destination device is directly or indirectly connected to.

A large LAN may have a number of switches connected together. Switches are used to reduce network traffic within a LAN and to provide connection points for devices including other switches.

Hubs

A hub is very similar to a switch and may, in fact, be identical in outward appearance. Like a switch, it contains a number of connections or ports, each of which can be linked to a computer or other network device. However, unlike a switch, a hub does not maintain a table of network addresses. This means that, when a hub receives data on one port, it does not know which of its ports is connected to the intended destination. It therefore copies the data to all the other ports. The data will be transmitted to its intended destination where it will be recognised and processed. It will also be transmitted to all other possible destinations where it will be ignored. Hubs therefore increase unwanted network traffic because they broadcast data to all ports rather than to just the one containing the destination for that data.

Wireless Access Points

A wireless access point is connected to a switch either directly or via an ordinary network socket. It is usually mounted on a wall and provides wireless (WiFi) access to the network using radio waves in the microwave part of the spectrum. An access point can carry data at up to 24 Mbps.

A number of different computers can access the network through a single access point although, since they are sharing a single communication channel, access for individual computers will be slower as the number increases. The bandwidth also gets less as the computer moves further from the access point and the radio signal becomes weaker. Each computer will need its own wireless network card to connect with the access point.

The distance within which an access point can be accessed depends on the thicknesses of floors and walls, the amount of metal pipe work and other environmental factors. However, typically, a single access point could provide wireless networking within a house or for several adjacent rooms in a school or office block.

If a single access point cannot provide sufficient coverage, then several may be used. Access points compatible with the 802.11b standard use a basic radio frequency of 2.4 GHz but small variations in this basic frequency provide a number of different broadcasting channels. This allows two or three access points to be placed to cover adjacent areas without them interfering with each other. Computers can be set up to roam across these points, automatically selecting the one with the best signal and connecting to it.

Wireless communication is very vulnerable to interception and so communication between and access point and a computer will normally be encrypted.

Wireless Access Points are particularly useful in situations where their use saves extensive and complicated network runs or where users need to use devices that need to move around and not be wired to a fixed network point. One example of this is the use of hand held card readers in restaurants. These allow staff to accept card payments at the customer's table.

Network Interface Cards

A network interface card (NIC) is inserted into one of the computer's expansion ports and it provides the interface between a computer and the network that it is connected to.

Each network card produced has a unique address, called its Media Access Control (MAC) address. This is built into the card when it is manufactured and, theoretically at least, no two cards will have the same MAC address. This allows the card, and therefore the computer it is part of, to be uniquely identified on a network.

The card will be responsible for providing the correct electrical connections (sockets) so that the computer may be physically linked to the network. It will also convert the digital signals on the network to the correct voltage, timings and format for internal use within the computer – and vice-versa.

Software drivers, supplied with the card, will allow the device to be set up for use in a particular system.

Wireless Network Interface Cards

A wireless network interface card allows the computer to connect to a wireless access point. It performs a similar task to an ordinary network interface card. Many laptop computers are supplied with a built-in wireless card. Small cards that plug into a USB socket are also available for computers without built-in wireless cards.

Together with appropriate software, the wireless card can allow the computer to identify which of several access points will provide the best connection. If the computer is moved from one area to another the card and software will switch access points to maintain the best possible connection at all times. This is called roaming.

Data moving between a wireless card and access point is usually encrypted to prevent the data being useable if it is intercepted. This extra level of security will need the user to enter an encryption key when first accessing the network via a wireless network card.

Routers

A router is responsible for deciding the best path to forward any data. The difference between a router and a switch is that the router will handle data moving between two networks.

When data arrives from the external network the router must be able to determine which local network address the data is destined for and forward it to that address.

A router, used as shown in the diagram on page 48, will have at least two ports or connections, one for the external network and one for the local network. In practice, routers usually include a switch within the same box, so that a single device will allow a number of computers or other switches to connect to it.

Repeaters

Data is transmitted within a LAN as a series of binary pulses that directly represent the binary data itself. This type of transmission is called baseband transmission. Typical transmission rates are 24 Mbits/second.

Baseband transmission allows for very fast data transmission but it has one major disadvantage. Electrical pulses flatten out when they travel through a long wire. This, together with other electrical factors imposes a maximum length restriction on LAN. The maximum length will depend on the type of cable used but it is typically around 1 to 2 km and may be as low as several hundred metres.

Repeaters can be installed to clean up and boost the signal at various points. This allows a single network to be extended beyond its normal maximum length. An alternative, as described below, is to split the network into a series of smaller networks and link these together using bridges.

Bridges

Rather than having a single large network for a building or site and use repeaters to boost the signal, it may be preferable to install several smaller local networks. These can be linked together using a device called a bridge. A bridge links two similar networks so that data can flow between them. Note that unlike a router that provides a link between an external network and a local network, a bridge will be linking two similar networks that are using the same sets of rules for communication.

Servers

A server is a computer that provides some service for other computers on the network. A file servers provide network storage space for users and may also store applications programs that users can run on workstations. A file server will also store user passwords and names and be responsible for handling network log in.

A typical network will also have one or more print servers which will manage print jobs. Network printout would be spooled to the server disk to be queued up and then sent to the appropriate printer. This approach allows a number of users to apparently access a single printer at the same time.

A mail server will handle email. This may be internal mail within the network, external mail to other servers or both.

The World Wide Web has many web servers which supply web pages on request. Each web server has a unique address which is known to routers within the system. When a web page is