IGCSE Information Communication Technology (ICT)
Syllabus code 0417

Section 4:
Computer networks
Candidates should be able to:

(a) describe a router and its purpose
(b) describe the use of WIFI and Bluetooth in networks
(c) describe how to set up a small network involving access to the internet, understanding the need to set up the use of a browser, email and an ISP
(d) identify the advantages and disadvantages of using common network environments such as the internet
(e) describe what is meant by the terms user id and password, stating their purpose and use
(f) identify a variety of methods of communication such as fax, email, and tele/video conferencing
(g) define the terms Local Area Network (LAN), Wireless Local Area Network and Wide Area Network (WAN)
(h) describe the difference between LANs, WLANs and WANs, identifying their main characteristic
(i) describe the characteristics and purpose of common network environments, such as intranets and the internet
(j) describe other common network devices (including hubs, bridges, switches and proxy servers)
(k) discuss the problems of confidentiality and security of data, including problems surrounding common network environments
(l) identify the need for encryption, authentication techniques, including the use of user identification and passwords, when using common network environments such as the internet

Modem and its purpose

Modem stands for modulator-demodulator.

It is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information.

The sending modem modulates the data into a signal that is compatible with the phone line, and the receiving modem demodulates the signal back into digital data. Wireless modems convert digital data into radio signals and back.
Modems are generally classified by the amount of data they can send in a given time, normally measured in bits per second, or "bps". For example, a 56k modem can transfer data at up to 56,000 bits (7kB) per second over the phone line.

Faster modems are used by Internet users every day, notably cable modems and ADSL modems.

A modem works as an input and an output device because for outgoing signals it converts the digital signal into an analogue signal (modulation) and for incoming signals it works in the reverse way (demodulation).

http://upload.wikimedia.org/wikipedia/commons/4/49/Modem.gif

**What is Internet?**

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

The internet links private PCs, public networks and business networks together using telephone lines to form one vast worldwide network.

Over a billion people used the Internet in 2008. Of these, about 500 million use the Internet at least once a week, making them more-or-less permanent citizens of the Internet population.

Eric Schmidt, the CEO of Google, the world’s largest index of the Internet, estimated the size at roughly over 5 billion gigabytes of data.
**Evolution of internet**

**Time line**

1962: J.C.R. Licklider of MIT, first proposed a global network of computers, and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections.

1965: Lawrence Roberts of MIT connected a Massachusetts computer with a California computer over dial-up telephone lines. It showed the feasibility of wide area networking, but also showed that the telephone line's circuit switching was inadequate. Kleinrock's packet switching theory was confirmed.

1966: Roberts moved over to DARPA and developed his plan for ARPANET. These visionaries and many more left unnamed here are the real founders of the Internet.

1969: The Internet, then known as ARPANET, was brought online under a contract let by the renamed Advanced Research Projects Agency (ARPA) which initially connected four major computers at universities in the southwestern US (UCLA, Stanford Research Institute, UCSB, and the University of Utah).

By June 1970: MIT, Harvard, BBN, and Systems Development Corp (SDC) in Santa Monica, Cal. were added.

By January 1971, Stanford, MIT's Lincoln Labs, Carnegie-Mellon, and Case-Western Reserve U were added. In months to come, NASA/Ames, Mitre, Burroughs, RAND, and the U of Illinois plugged in. **After that, there were far too many to keep listing here.**

**Network topologies**

A computer network topology is the physical communication scheme used by connected devices.
There are six basic types of topology in networks:

- Bus topology
- Star topology
- Ring topology
- Mesh topology
- Tree topology
- Hybrid topology

Bus Topology

Bus networks use a common backbone to connect all devices. A single cable, the backbone, functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Advantages

- Ethernet bus topologies are relatively easy to install
- Don’t require much cabling compared to the alternatives.

Disadvantages

- Bus networks work best with a limited number of devices
- If more than a few dozen computers are added to a network bus, performance problems will likely result.
- If the backbone cable fails, the entire network effectively becomes unusable.

Ring Topology
In a ring Network, every computer or devices have two adjacent neighbors for communication. In a ring network, all the communication messages travel in the same directory whether clockwise or anti-clockwise.

Any damage of the cable of any cable or device can result in the breakdown of the whole network. Ring topology now has become almost obsolete. Ring topologies can be found in office, school or small buildings.

**Advantages**

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star topology under heavy network load
- Does not require network server to manage the connectivity between the computers

**Disadvantages**

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU’s are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load

**Star Topology**

**Star networks** are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer, which acts as a conduit to transmit messages. Star topologies can be implemented in home, offices or even in a building.

Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.
**Advantages**

- **Better performance:** Passing of Data Packet through unnecessary nodes is prevented by this topology.
- **Isolation of devices:** Each device is inherently isolated by the link that connects it to the hub. This makes the isolation of the individual devices fairly straightforward, and amounts to disconnecting the device from the hub. This isolated nature also prevents any non-centralized failure from affecting the network.
- **Benefits from centralization:** As the central hub is the bottleneck, increasing capacity of the central hub or adding additional devices to the star, can help scale the network very easily. The central nature also allows the inspection traffic through the network. This can help analyze all the traffic in the network and determine suspicious behavior.
- **Simplicity:** The topology is easy to understand, establish, and navigate.

**Disadvantages**

More devices and cable required: As compared to the bus topology, a star network requires more devices & cables to complete a network.

If the central connecting device such as hub, switch or router fails due to any reason, then ultimately all the network can come down or collapse.

**Tree Topology**

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices.

**Mesh Topology**

**Mesh networking** is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by “hopping” from node to node until the destination is reached.

A mesh network whose nodes are all connected to each other is a fully connected network.
Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops, and they generally are not mobile.

Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, this network is very reliable. This concept is applicable to wireless networks, wired networks, and software interaction.

A mesh network in which every device connects to every other is called a full mesh.

Partial mesh networks also exist in which some devices connect only indirectly to others.

**Hybrid Topology**

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit a hybrid network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: star ring network and star bus network.

A Star ring network consists of two or more star topologies connected using a multistation access unit (MAU) as a centralized hub.

A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network’s backbone).

**Common devices used in a computer network**

Let’s now look at the various components that are used in a LAN and in a WAN.

**Hubs**

In the old days the LAN comprised mostly of devices called hubs or a concentrator in other words. A hub or a concentrator was a way of concentrating network connections in a single point. Hub’s ran at 10Mbps and essentially if you put 10 machines into a wire that was running a 10Mbps you would see that every machine could probably only transmit at 1Mbps even if they were transmitting at their maximum.

Hubs were shared, they were slow, they were not optimal, primarily because you had a certain
number of devices that you plugged in and the performance of Ethernet would degrade to such an extent that it was preferable not to even work on the network.

**Switches**

Hubs then gave way to switches, the difference between a hub and a switch is that it when workstations started communicating with one another, they would essentially form a direct connection and even though other devices were connected these two workstations would talk directly to one another. They would create a virtual connection between the two devices that were communicating with each other. Once the conversation was complete that connection would be broken and then if a machine wanted to talk with a different workstation it would again create a virtual connection. As opposed to hubs, switches were much faster, there was less contention but they were also much more expensive.

**Routers**

So in the makeup of the LAN, we need something more. We use a Router. A **router** is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers. A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP’s network. Routers are located at gateways, the places where two or more networks connect. Very little filtering of data is done through routers.

**Bridge**

A device that connects two local-area networks (LANs), or two segments of the same LAN, that use the same protocol, such as Ethernet or Token-Ring.
**Gateways**

A node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the internet.

**Proxy Servers**

A proxy server, also known as a "proxy" or "application level gateway", is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security. In some cases, they monitor employees' use of outside resources. A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port. By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.

Some proxy servers are a group of applications or servers that block common Internet services. For example, an HTTP proxy intercepts web access, and an SMTP proxy intercepts email. A proxy server uses a network addressing scheme to present one organization-wide IP address to the Internet. The server funnels all user requests to the Internet and returns responses to the appropriate users. In addition to restricting access from outside, this mechanism can prevent inside users from reaching specific Internet resources (e.g., certain web sites). A proxy server can also be one of the components of a firewall.

Proxies may also cache web pages. Each time an internal user requests a URL from outside, a temporary copy is stored locally. The next time an internal user requests the same URL, the proxy can serve the local copy instead of retrieving the original across the network, improving performance.

**Securing computer networks**

- Access authorization restricts access to a computer to group of users through the use of authentication systems. These systems can protect either the whole computer - such as through an interactive logon screen - or individual services, such as an FTP server. There are many methods for identifying and authenticating users, such as passwords, identification cards, and, more recently, smart cards and biometric systems.
- Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).
- Application with known security flaws should not be run. Either leave it turned off until it can be patched or otherwise fixed, or delete it and replace it with some other application. Publicly known flaws are the main entry used by worms to automatically break into a system and then spread to other systems connected to it.
- Backups are a way of securing information; they are another copy of all the important computer files kept in another location. These files are kept on hard disks, CD-Rs, CD-RWs, and tapes. There is also a fourth option, which involves using one of the file hosting services that backs up files over the Internet for both business and individuals.
- Encryption is used to protect the message from the eyes of others. It can be done in several ways by switching the characters around, replacing characters with others, and even removing characters from the message. These have to be used in combination to make the encryption secure enough, that is to say, sufficiently difficult to crack.
- Firewalls are systems which help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic which can pass through them, based on a set of system administrator defined rules.
- Honey pots are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.
- Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.
- Pinging: The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer they can try a port scan to detect and attack services on that computer.
- Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.
Network Environments

Local Area Network

A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. On a typical LAN application, softwares and users’ data files are stored on a central computer called a file server (SERVER). Each computer on a LAN is called a workstation. To connect to a LAN, a workstation must have a network card. This is a device through which computers communicate with each other.

Wireless Local Area Network (WLAN)

A wireless LAN (WLAN) links two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops. Public businesses such as coffee shops or malls have begun to offer wireless access to their customers; some are even provided as a free service. Large wireless network projects are being put up in many major cities.

Wide Area Network

A wide area network (WAN) is a computer network that covers a broad area (i.e. any network whose communications links cross metropolitan, regional, or national boundaries). Less formally, a WAN is a network that uses routers and public communications links. The computers in a WAN are not permanently connected to each other with data cables. They communicate with each other through telephone lines, radio signals and satellite links. The largest and most well-known example of a WAN is the Internet. Computers need a MODEM to communicate with others computers on Internet.

Computer network
A **computer network** is a group of interconnected computers. A network is a collection of computers and devices connected to each other. The network allows computers to communicate with each other and share resources and information.

**The advantages of networking:**

- Computers can **communicate and share data and files**.
- **Storage facilities, Hardware** peripherals such as printers can be **shared**.
- Data from all the computers can easily be **backed up centrally**.

**The disadvantages of networking:**

- **One of the major reasons behind the spread of computer viruses.**
- **As data is shared there is a greater need for security.** Users of the network have to have **user ids and passwords**.
- **If the server fails, all the workstations are affected.** Work stored on shared hard disk drives will not be accessible and it will not be possible to use network printers either.
- **Installing a network is expensive as it involves purchasing of networking hardware such as Hubs, cables, network cards, bridges, routers etc.**
- Large networks require specialist to maintain them, which again involves time and money.

**Bluetooth and Wifi in Network**

**What is Bluetooth?**

Bluetooth can be defined as a wireless form of communication that enables devices to send and receive communication. It is a global initiative set up by manufacturers such as IBM, Intel, Ericsson, Toshiba and Nokia to create a standard for linking up devices such as mobile phones, mobile PCs, handheld computers and other peripherals.

Bluetooth relies on short-range radio technology to allow the wireless connectivity. The key features of Bluetooth are robustness, low power and low cost. Both data and voice transmissions can be handled simultaneously. Examples of innovative solutions which users can perform include printing or faxing capabilities, synchronising PDA, laptop or computer and making or receiving calls from a mobile phone, with many more applications available.
What is Wifi?

Wifi is short for ‘wireless fidelity’ and is a limited-range wireless networking code which is used in many airports, hotels or other services, who offer public access to Wifi networks, to allow people to log on to the Internet and receive emails whilst on the move. As Wifi is a reasonably fast method of transmitting information in wave form, it is often used in computers and also notebooks. In future, it will become possible to access the Internet from just about anywhere, without the use of any wires. The advantages of using Wifi are that the networks are fairly cheap and straightforward to set up. Wifi is also quite inconspicuous and can hardly be noticed unless it is being looked for specifically, whilst in a Wifi ‘hotspot.’ For a wireless network to be created, communication is transferred like a two way radio, using radio waves.

Advantages of Bluetooth

- Bluetooth can connect devices from point-to-point and probably better on security than Wifi, as it can cover shorter distances.
- Bluetooth offers an optional two levels of password protection.
- Up to seven devices can be connected at any one time which makes it easier to find and connect the device being searched for, as Bluetooth highlights itself to the other devices.
- Bluetooth technology is also more ideal for consumer electronics devices as it has a smaller power requirement.
- Another advantage is concerning voice communication. For an office or home environment, Bluetooth can be used in a cordless phone within a 10m range, without the need to be passed around.

Advantages of Wifi

- The most prominent advantage which Wifi has over Bluetooth is that Wifi operates at a much faster rate - of about 11mbps, whereas Bluetooth only operates at a much slower rate of around 720kbps.
- Wifi is also designed to link up entire networks, rather than computer to computer. Wifi can achieve this too but it is not its real purpose.
- It is now often being used for increasingly more applications, such as Internet access, gaming and basic connectivity for home electronic appliances such as televisions or DVD players. Wi-Fi may be used by cars in highways, as standards rise in development, in support of an Intelligent Transportation System to increase safety, gather statistics, and enable mobile commerce.