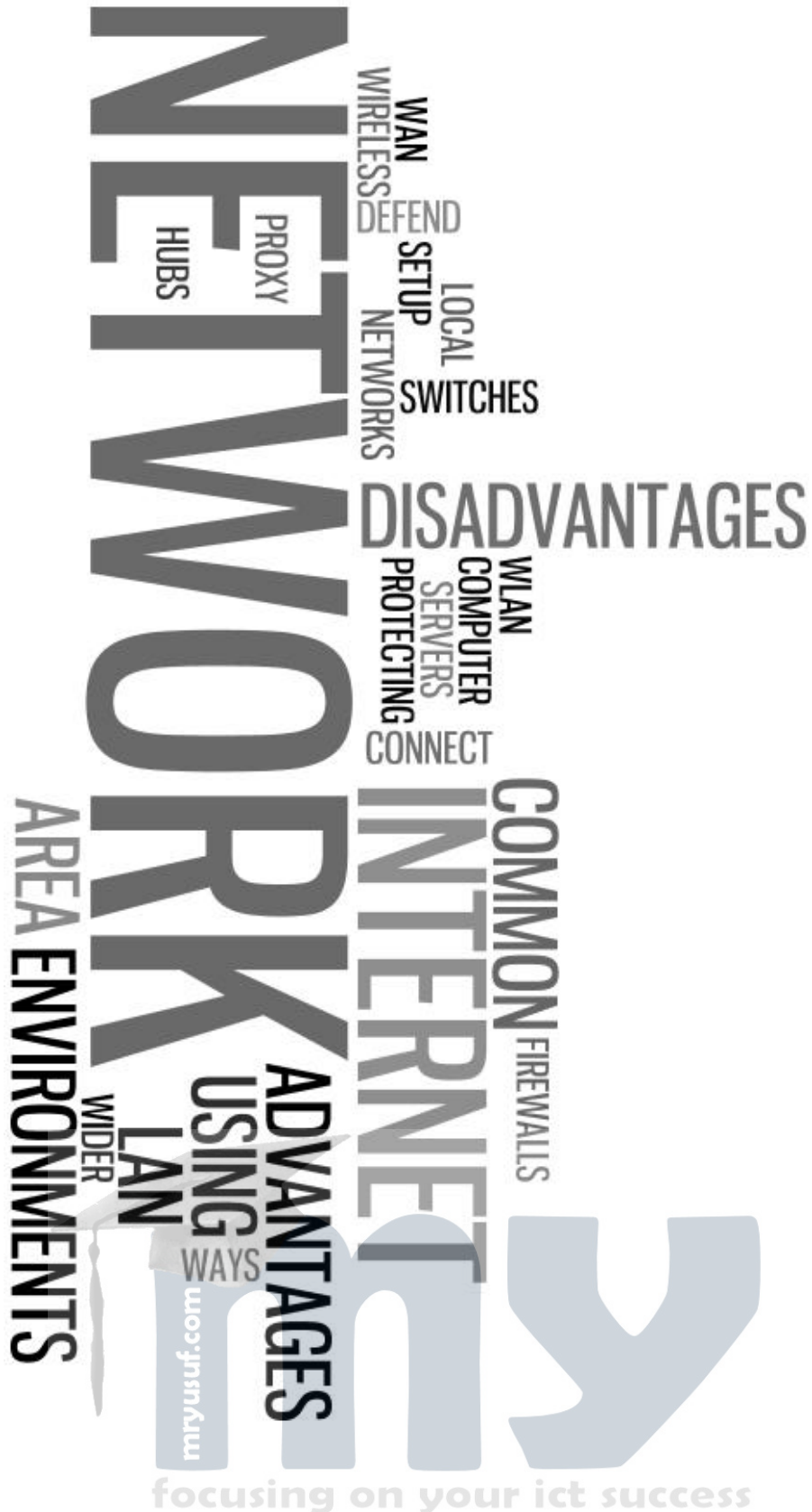
SECTION 4


NETWORK
WAN
WIRELESS
DEFEND
PROXY
HUBS
SETUP
LOCAL
NETWORKS
SWITCHES
DISADVANTAGES
WLAN
COMPUTER
SERVERS
PROTECTING
CONNECT
INTERNET
COMMON
FIREWALLS
AREA
ENVIRONMENTS
WIDER
LAN
USING
WAYS
ADVANTAGES
mryusuf.com
focusing on your ict success

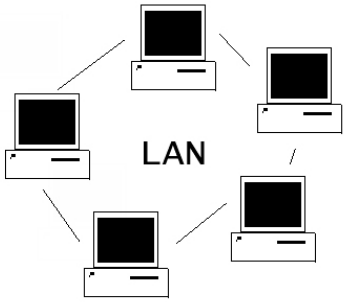
SECTION 4 – Computer Networks

Networks

We will begin by answering the question as to 'what is a network?' A computer network describes any situation in which two or more computers are linked together via some form of communications medium for the purpose of exchanging and sharing resources. Almost all organisational computing takes place in a networked environment. Non-networked use of computers i.e. 'stand alone' is still the case around most people's homes; this is also the case in very small businesses.

One way of categorising networks is by considering their scale. Using this approach, two major categories have emerged – Local and Wide Area Networks.

Local Area Network (LAN)

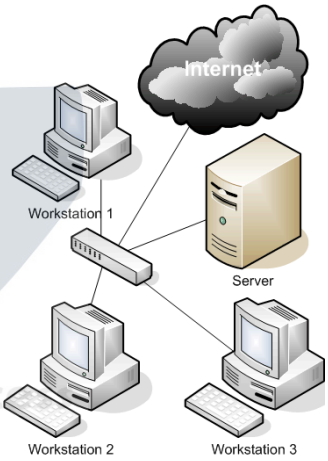


This is a network that is confined to a small geographical area, usually within one building or closely connected group of buildings, e.g. a university campus. The main mode of communication is physical cabling, usually a combination of fibre optic and copper cabling, although there is growing use of wireless devices in LAN environments.

Another defining feature of a LAN is that all of the network resources are owned and managed by the organisation that uses them.

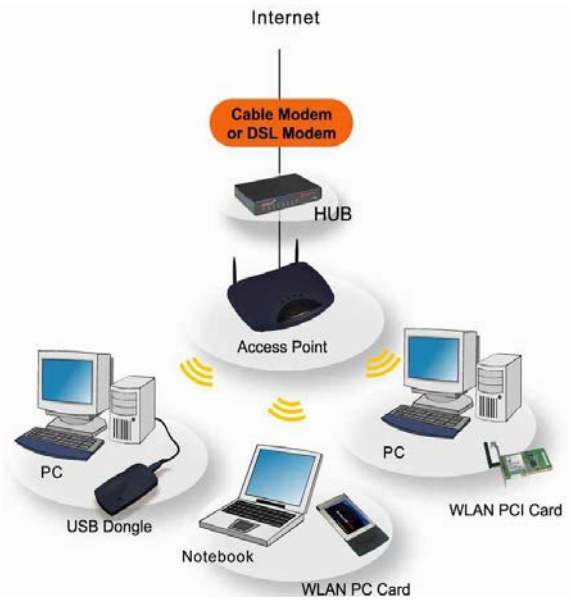
Wider Area Network (WAN)

This is a network that spreads across a wider geographical area, connecting LAN's via a wide range of communications media. In addition to physical cabling, wireless and satellite technologies may be used to complete a network that may be literally world-wide.



Working in a WAN environment will involve using network resources owned and managed by a wide range of organisations. WAN's can be further sub-divided into public WAN's like the internet for example, which is the largest example of a WAN.

A Wireless LAN (or WLAN)



Is a wireless local area network, which is the linking of two or more computers or devices without using wires or cables. WLAN uses spread-spectrum or OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) modulation technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. 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.

How to setup a network

Part 1: Introduction: Set Up a Small Network with Windows XP Home Edition

This guide describes how to quickly set up a small network that is practical for home users. It should only take part of a day to set up shared access to hard disks, folders, CD-ROM drives, printers, and the Internet. In your new peer-to-peer network, all the computers share their resources.

Part 2: Buying the Network Hardware

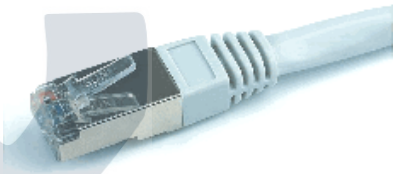
If we exclude 'wireless connections' your computers can communicate with each other only if they are physically connected. To physically connect them, you must have some hardware. Many manufacturers offer starter kits that make setting up your first network easier. However, you can also obtain all the components separately. You must have the following components to connect your computers:

- One Ethernet network card per computer.
- One network cable per computer.
- A signal distributor (hub/switch).

A signal distributor (hub/switch) connects computers with each other; controls data flow and can negotiate data transfer between 10 Mbit/s and 100 Mbit/s connections. For your small network, use either a dual-speed hub or a dual-speed switch

Part 3: Connecting the Computers

With every computer, make sure they have a network card - each with a cable connector attached to one end and the other end connector to the hub or switch.



Hubs and Switches

Hubs

A network hub or repeater hub is a device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single network segment (entity). The device is thus a form of multiport repeater.

The availability of low-priced network switches has largely rendered hubs obsolete but they are still seen in older installations and more specialized applications.

Switches

A network switch is a broad and imprecise marketing term for a computer networking device that connects network segments.

As with hubs, Ethernet implementations of network switches support either 10/100 Mbit/s or 10/100/1000 Mbit/s ports Ethernet standards. Large switches may have 10 Gbit/s ports. Switches differ from hubs in that they can have ports of different speed.

Continued on next page…

Protecting a Network

It is a fact that the greatest virtue of a network is also its main weakness. They allow users to connect to each other and beyond that, via the internet, to an uncontrolled global network. This brings enormous benefits in terms of the sharing of resources, the efficient transfer of files and data, and access to remote sources of data. The same connectedness, however, also creates a point of vulnerability. The network is to a determined hacker, the equivalent of a window to a burglar, which is a possible point of entry. Whether the network is the equivalent of a cracked window in a rotten frame or triple-glazed security glass in a fixed metal frame will depend on the security measures that the organisation employs or implements.

The security threats that network administrators need to be aware of, fall into three broad (wide) categories:

1. Non-malicious attacks

The aim of the intruder is simply to break through the network's defenses just to prove that they can. It is, as far as the hacker is concerned, a type of game where their skill is pitted against the security resources of the system. These attacks can, none the less, create a great deal of damage.

2. Malicious attacks

In this case, the intruder wishes the organisation harm. They want to cause as much damage as they can to the ICT systems. They may achieve this by causing crashes, introducing viruses or corrupting data.

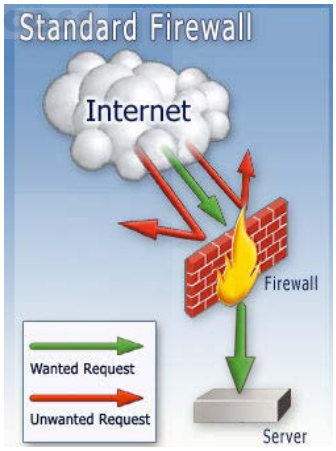
3. Criminal activity

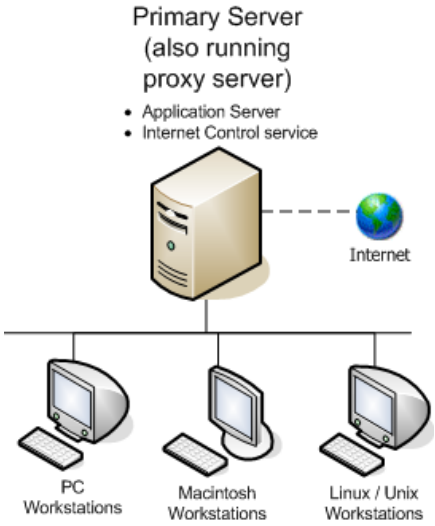
The prime aim of the intruder is not to cause damage but to commit a criminal act, e.g. by viewing or altering data for financial gain, deleting records or by stealing information that has commercial value.

Ways to defend a Network

Network Firewalls

Firewall for networks is a security device designed to protect a network from intrusion via the internet connection. It may consist of a dedicated computer running firewall software or a specific piece of hardware that looks very much like a router (a device that routes information between interconnected networks).





Whatever form it takes, its primary function is to authenticate incoming messages and verify legitimacy of users trying to enter the network via an internet connection.

Proxy Servers

A proxy server is a computer used on some corporate networks. It is used for all World Wide Web traffic, such as the viewing of Web pages. It can be used for the filtering of Web sites to prevent people from going to certain types of sites, but more commonly it is used on networks where there is not a direct connection to the Internet available for all computers (or where a direct connection would be too expensive).

Wi-Fi

Wi-Fi is the trade name for the popular wireless technology used in home networks, mobile phones, video games and more. Wi-Fi technologies are supported by nearly every modern personal computer operating system and most advanced game consoles, printers, and other peripherals (see section 1). The purpose of Wi-Fi is to hide complexity by enabling wireless access to applications and data, media and streams. The main aims of Wi-Fi are the following:

- Make access to information easier.
- Ensure compatibility and co-existence of devices.
- Eliminate cabling and wiring.
- Eliminate switches, adapters, plugs and connectors.

In addition to restricted use in homes and offices, Wi-Fi can make access publicly available at Wi-Fi hotspots provided either free of charge or to subscribers to various providers. Organizations and businesses such as airports, hotels and restaurants often provide free hotspots to attract or assist clients. Many consumer devices use Wi-Fi. Routers which incorporate a DSL-modem or a cable-modem and a Wi-Fi access point, often set up in homes and other premises, provide Internet-access and internetworking to all devices connected (wirelessly or by cable) to them.

Bluetooth

Bluetooth is a wireless protocol utilizing short-range communications technology facilitating data transmission over short distances from fixed and/or mobile devices, creating wireless Personal Area Networks (PANs). The intent behind the development of Bluetooth was the creation of a single digital wireless protocol, capable of connecting multiple devices and overcoming issues arising from synchronization of these devices. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, GPS receivers, digital cameras, and video game consoles etc.

Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device. Bluetooth enables these devices to communicate with each other when they are in range. The devices use a radio communications system, so they do not have to be in line of sight of each other, and can even be in other rooms, as long as the received transmission is powerful enough.

Application use

- Wireless control of and communication between a mobile phone and a hands-free headset.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communications with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of contact details, calendar appointments, and reminders between devices.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used, like in mobile phones.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Two seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3 use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computer or PDA using a data-capable mobile phone as a modem.

Email

Electronic mail, often abbreviated to e-mail, email, or originally eMail, is a store-and-forward method of writing, sending, receiving and saving messages over electronic communication systems. The term "e-mail" applies to the Internet e-mail system based on the Simple Mail Transfer Protocol, to network systems based on other protocols and to various mainframe, minicomputer, or intranet systems allowing users within one organization to send messages to each other in support of workgroup collaboration. E-mail is often used to deliver bulk unsolicited messages, or "spam", but filter programs exist which can automatically block, quarantine or delete some or most of these, depending on the situation.

Spamming and computer viruses

The usefulness of e-mail is being threatened by four phenomena: e-mail bombardment, spamming, phishing, and e-mail worms. Spamming is unsolicited commercial e-mail. Because of the very low cost of sending e-mail, spammers can send hundreds of millions of e-mail messages each day over an inexpensive Internet connection. Hundreds of active spammers sending this volume of mail results in information overload for many computer users who receive voluminous unsolicited email each day. More on Spamming in Section 6.

Privacy concerns

E-mail privacy, without some security precautions, can be compromised because e-mail messages are generally not encrypted, e-mail messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages, many Internet Service Providers (ISP) store copies of your e-mail messages on their mail servers before they are delivered. The backups of these can remain up to several months on their server, even if you delete them in your mailbox.

Application use

- Send a message to another user or group of people.
- Print the messages.
- Delete or move messages to a folder
- Attach a file to send or download an attachment.
- Read any message which is displayed in the mailbox.
- Send a reply to a message and forward a message.
- Search for a message in a mailbox.

Advantages of email (over post)

- With email there is less use of paper.
- Mail can be read and replies made without printing.
- A letter can be written using a word processor and transmitted directly without the need to print.
- Messages can be received almost immediately after they are sent.
- The cost is usually the same to anywhere in the world which is less than the cost of a stamp and envelope.

Disadvantages of email (over post)

- Email can only be sent to people who subscribe to the service and uses it regularly.
- A user does not know any mail has been received until he or she logs on.
- It is expensive to use when taking the cost of hardware and subscriptions to the internet.
- The widespread use of email might threaten the job of postal staff.
- A user can't send physical attachments digitally , like a DVD film for example.

User identification and passwords

User ID

Users in a computing context refer to one who uses a computer system. Users may need to identify themselves for the purposes of accounting, security, logging and resource management. In order to identify oneself, a user has an account (a user account) with a username and in most cases also a password. Users employ the user interface to access systems.

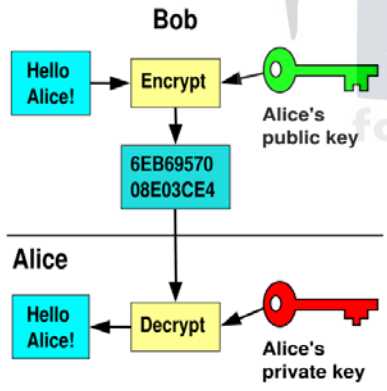
Password

In computing, a password is a word or string of characters that is entered, often along with a user name, into a computer system to log in or to gain access to some resource. Passwords are a common form of authentication. Full security requires that the password be kept secret from those not allowed access. Passwords are used to control access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc.

A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers such as Yahoo, Gmail or Hotmail, accessing programs, databases, networks, web sites for online banking and shopping, and even reading the morning newspaper online. Despite the name, there is no need for passwords to be actual words.

***Note:** The term pass code is sometimes used when the secret information is purely numeric, such as the personal identification number (PIN) commonly used for ATM access or an online bank account. Passwords are generally short enough to be memorized, but it highly recommended that it should be mixed with letters and numbers for added security.

Encryption



In cryptography, encryption is the process of changing (transforming) information using an algorithm (or program) to make it unreadable and meaningless to anyone trying to access it.

The result of the process is encrypted information which can only be understood by the use of a decryption key to make the encrypted information readable again (i.e. to make it unencrypted).

This encryption process provides security for sensitive data and protects against results of unauthorised access whether intentionally from a hacker or unintentionally. **However, encryption does not prevent a hacker from deleting data.** It just can't be read.

Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. Why would you want to authenticate, you might ask? Perhaps you might want users to submit some personal information before browsing your site, or perhaps you might have sensitive information that you want accessible to only selected members – like a web forum. There are numerous amounts of reasons why a web site might need to let only certain set of people view their pages.

Impact on the general public

High speed Internet connectivity has become more widely available at a reasonable cost and the cost of video capture and display technology has decreased. Consequently personal video teleconference systems based on a webcam, personal computer system, software compression and broadband Internet connectivity have become affordable for the general public. Also, the hardware used for this technology has continued to improve in quality, and prices have dropped dramatically. The availability of freeware (often as part of chat programs) has made software based videoconferencing accessible to many.

Deaf and hard of hearing individuals have a particular interest in the development of affordable high-quality videoconferencing as a means of communicating with each other in sign language. So videoconferencing can be used between two signers.

Impact on education

Videoconferencing provides students with the opportunity to learn by participating in a 2-way communication platform. Furthermore, teachers and lecturers from all over the world can be brought to classes in remote or otherwise isolated places.

Students from diverse communities and backgrounds can come together to learn about one another. Students are able to explore, communicate, analyze and share information and ideas with one another. Through videoconferencing students can visit another part of the world to speak with others, visit a zoo, a museum and so on, to learn.

Impact on medicine and health

Videoconferencing is a very useful technology for telemedicine and tele-nursing applications, such as diagnosis, consulting, transmission of medical images, etc., in real time in countries where this is legal.

Using VTC, patients may contact nurses and physicians in emergency or routine situations, physicians and other paramedical professionals can discuss cases across large distances. Rural areas can use this technology for diagnostic purposes, thus saving lives and making more efficient use of health care money.

Impact on business

Videoconferencing can enable individuals in faraway places to have meetings on short notice. Time and money that used to be spent in traveling can be used to have short meetings. Technology such as VOIP can be used in conjunction with desktop videoconferencing to enable low-cost face-to-face business meetings without leaving the desk, especially for businesses with wide-spread offices. The technology is also used for telecommuting, in which employees work from home.

Impact on law

Videoconferencing has allowed testimony to be used for individuals who are not able to attend the physical legal settings.

Teleconferences

Alternative terms for teleconferencing include audio conferencing, telephone conferencing and phone conferencing. Internet telephony involves conducting a teleconference over the Internet or a Wide Area Network. One key technology in this area is Voice over Internet Protocol (VOIP). Popular software for personal use includes Skype, Google Talk, Windows Live Messenger and Yahoo Messenger.