Networking

What is networking?

Networking is the means by which we connect people, enabling them to communicate with each other and share information using computers. Networks can range from the mainframe host and terminal model, which proliferated in the early days of the industry; to the local area network (LAN) that connects desktop PCs in a company; to wide area networks (WANs), such as the Internet or a global corporation's connections among multinational sites. LANs are high-speed, low-error data networks that cover a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited areas.

1.1 Benefits of Networking

A network allows users to share files, applications and printers. By connecting the computers in your company together, you can increase communication, workflow and productivity.

The vast majority of LAN environments will be based on a client/server architecture. A client/server network uses dedicated "server" systems to supply information to the "client" systems that sit on users' desks. This architecture implies that the server performs some processing.

Clients

At the centre of every network exists the PC. Most of these PCs are user desktop systems, also called clients, that access another system's network resources for file access, print services, e-mail and so on. A client system typically doesn't provide any services to other clients on the network. A network can encompass just a handful of client systems, or it can link hundreds of thousands. Typically, the companies you sell into will have networks of between 100 and 1,000 users (although you may find yourself selling into much larger accounts).

Servers

A server is any system that provides network-based services to the (client) users on the network. Usually, a network will have more than one server. Most servers offer some sort of security or protection against unauthorized use, for example, logins, passwords and group access rights.

Advantages of Networking within a workplace:

- Files can be stored on a central computer (the file server) allowing data to be shared throughout an organisation.

- Files can be backed up more easily when they are all on a central fileserver rather than when they are scattered across a number of independent workstations.

- Networks also allow security to be established, ensuring that the network users may only have access to certain files and applications.

- Software and resources can be centrally managed.

- Network versions of software often allow for their speedy installation on workstations from the file server.

- Expensive devices such as laser printers or scanners can be shared.

- Users can access their files from any workstation

Disadvantages of Networking within a workplace:

- The cabling, interface cards, file servers etc. that are required to set up a network are expensive.

- If one computer, cable or interface breaks the whole network may stop operating and you may not be able to use any of the computers until the fault is repaired. In practice this rarely happens. The exact effect of a failure will depend on the topology of the network.

- Viruses stored on a computer on a network can spread to other computers over the network.

- The files stored on computer networks can be accessed, stolen and edited more easily that files stored on a non-networked computer could be. Appropriate security measures must be implemented to prevent this.

Network Operating Systems:

Definition:

A Network Operating System (NOS) is an operating system that includes special functions for connecting computers and devices into a local-area network (LAN). Some operating systems, such as UNIX and the Mac OS, have networking functions built in. The term network operating system, however, is generally reserved for software that enhances a basic operating system by adding networking features. For example, some popular NOS's for DOS and Windows systems include **Novell Netware**, **Artisoft's LANtastic, Microsoft LAN Manager,** and **Windows NT.**

Summary of a NOS & How it Works:

A Network Operating System controls the network in the workplace; this control entails many different tasks at different layers in the layered architecture. For example, a major function of an NOS is to provide security to all the PCs but still allow easy access for legitimate users. An NOS such as Windows NT 4 provides the network administrator with a range of tools to manage such tasks. Some examples of this are:

- *RAS administrator;* this is used to manage remote users

- *User Profile Editor;* this tool defines user profile. A profile is a collection of settings that apply to user accounts.

- *Server Manager;* this is used to administer the properties of other servers on the Network.

Various Costs, Performance & Security associated with the installation of a Network

The cost, performance and susceptibility of a network can depend on such factors as size and network architecture. Thus Cost will increase in accordance to the size and complexity of the architecture .The most common network architecture are listed below:

- **Small Networks:** with a few users normally use Ethernet or token ring networks with one or two servers or no servers at all if Peer-to-Peer is in operation.
- **Medium Networks:** with a few hundred users will have the need to segment the network into logical parts. Client server is common with this type of architecture. There may be 10 or more servers or hardware such as routers and switches to provide the segmentation. Ethernet or token ring is still common with this size network.
- **Large Networks:** usually involve many floors or areas in a building and serve a large organisation with diverse needs. This again is segmented into logical parts for security to share the load on servers and the need to balance bandwidth for best performance.

Network Costs:

Organisations can use external suppliers to maintain a network, & even setting up a specific LAN for specific sites in their companies. It is therefore important for managers of the company to know the competition between external suppliers and the possibility of cost saving to the company.

The cost of implementing a network will include charges from the service providing company such as:

- A *Network Connection Fee*. This will be a one off charge relating to the cost of Hubs and Switches.
- A *Network Access Fee*. This will be an ongoing charge for the duration of the service provided, usually billed per month.
- The Cost of *Workstation Interface cards*.

Evaluating the overall cost of providing an organisation with networked facilities must take into account various factors like:

- Maintenance & replacement of equipment.
- Depreciation
- Monitoring staff usage of workstations

<u>Network Security Issues</u>

Hackers attack networks for profit, to be malicious or just because they exist. They do not need any specific knowledge or tools for this as there are many web sites on the Internet for this and a list of how to attack networks with a list of latest hacks.

Even if you have a complete system backup, you must be sure the backed-up data was secure before the backup was created.

The kinds of damage that hackers are capable of are:

- Stealing your company's data,
- Fraudulent use of your data or funds,
- Changing your data for any given reason & introducing Viruses.

Therefore a high percentage of a companies profit/time may be spent on their network security updates to prevent such loses to their data which may be very expensive to generate and which loss or damage may put them out of business. To prevent such damage to networks there are many precautionary measures that can be taken.

Firewalls are a common example. A *firewall* is a piece of software usually but not always running on a dedicated computer or piece of hardware such as a router. It acts by controlling access to your network from the outside. A firewall defines which part of the internal system can be seen from the outside and vice versa: its can control what services are visible and available to the clients on the network.
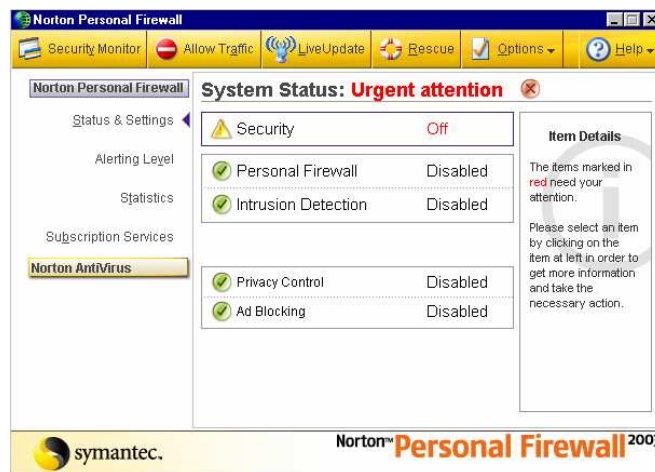
2.1 Design / Evaluation of Networks

Layering in Networks

Once you have PC connected together & there is a need for them to communicate, a whole set of new problems arise. The components in each of the PC's are made by different companies, as is the software at the operating system level and applications. As with many ideas in computing, there is a published standard that lays down an ideal specification. In networking this is called the **OSI 7 Layer Model.** This is an *idealised layered architecture*, manufacturers usually use there own simpler layers i.e. in software engineering there is the *Waterfall Process Model* to help the engineers be more efficient in design & analysis of the Software.

The reason a layered approach is so effective in network design is that any layer can be changed without changing the overall aim to communicate.

The seven layers of the OSI model are:

- **Application (Layer 7).** The Application Layer implements application-specific behaviour, such as the ftp protocol or http (web) session.

- **Presentation (Layer 6) –** this layer controls formatting and data exchange behaviour such as data compression and encryption e.g. JPEG, MPEG, GIF.

- **Session (Layer 5) –** this defines how to start, control & end conversations (called *sessions*). Coordinates movement from Client to Server. E.g. SQL, NetBios.

- **Transport (Layer 4) –** this layer provides data delivery & can split into packets and reassemble those packets on the receiving side.

- **Network (Layer 3) –** provides the service we think of as network services: routing, flow control etc.

- **Data link (Layer 2)** – this layer controls transmission & retransmission of data. E.g. ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol).

- **Physical (Layer 1)** – this layer actually moves bits to and from some kind of network medium, weather it's a 10 Base-T cable, a satellite link or a modem connection.

Types of Networking

A **LAN (local area network)** is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A piece of hardware called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
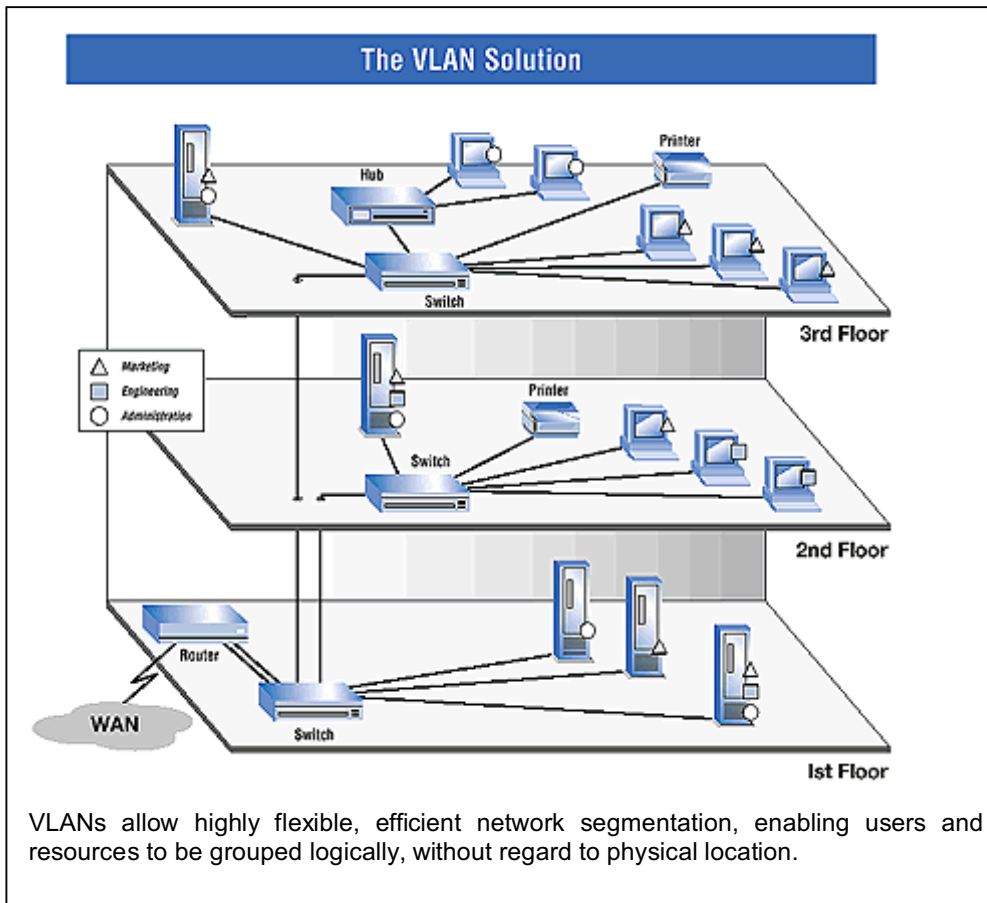
A **WAN (wide-area network)** spans a large physical distance. A WAN like the Internet spans most of the world. A WAN is a geographically dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address. WANs differ from LANs in several important ways. Like the Internet, most WANs are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs use technology like ATM, Frame Relay and X.25 for connectivity.

A **MAN (Metropolitan Area Networks)** is a relatively new class of network, it serves a role similar to an ISP, but for corporate users with large LANs. There are two important features that distinguish MANs from LANs or WANs:

- The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.

- A MAN (like a WAN) is not generally owned by a single organisation. The MAN, its communications links and equipment are generally owned by a consortium of users or by a single network provider who sells the service to the users.

Use of MANs to provide regional networks that share the cost of access to a WAN
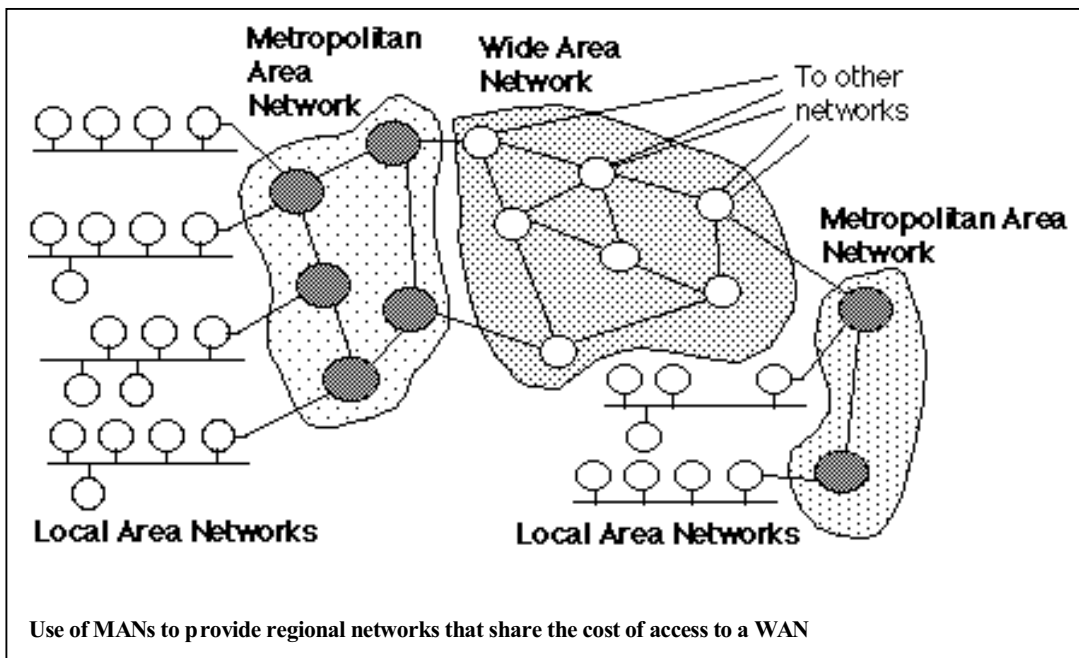
A **VLAN (Virtual Local Area Network)** is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment even though they may not be. For example, all marketing personnel may be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, at the IT manager's discretion.

VLANs allow highly flexible, efficient network segmentation, enabling users and resources to be grouped logically, without regard to physical location.

Benefits of VLANs

1. **Flexible Network Segmentation**
   Users and resources that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is largely contained within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

2. **Simple Management**
   The addition of nodes, as well as moves and other changes can be dealt with quickly and conveniently from the management console rather than the wiring closet.

3. **Better use of server resources**
   With a VLAN-enabled adapter, a server can be a member of multiple VLANs. This reduces the need to route traffic to and from the server.

4. **Enhanced network security**
   VLANs create virtual boundaries that can only be crossed through a router. So standard, router-based security measures can be used to restrict access to each VLAN as required.

5. **Increased performance**
   VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.

WLAN (Wireless Local Area Network)

A Wireless Local Area Network (WLAN) implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use electromagnetic waves to transmit and receive data over the air, minimizing the need for wired connections, and WLANs combination of data connectivity, user mobility, and simplified configuration, make movable LANs possible.
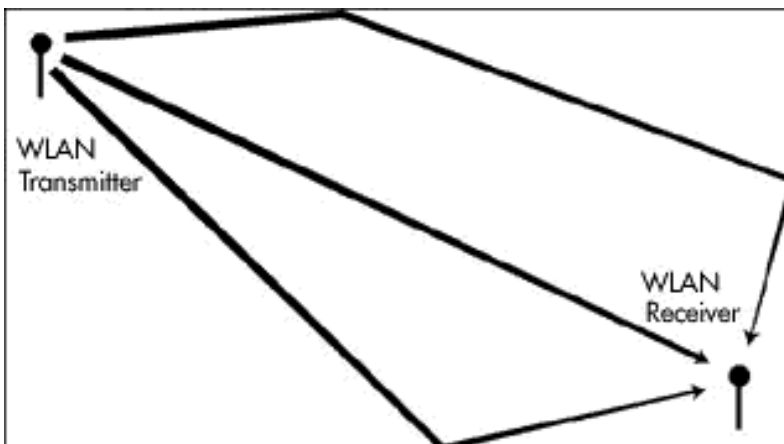
Radio Signals Travelling over Multiple Paths

LAN, WAN, MAN & their associated Topologies

LAN Topologies

LAN topologies define the manner in which network devices are structured. Four common LAN topologies exist: ***bus, ring, star, and tree***. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Bus and ring topologies, for example, are commonly structured physically as a star. A *bus topology* is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations.
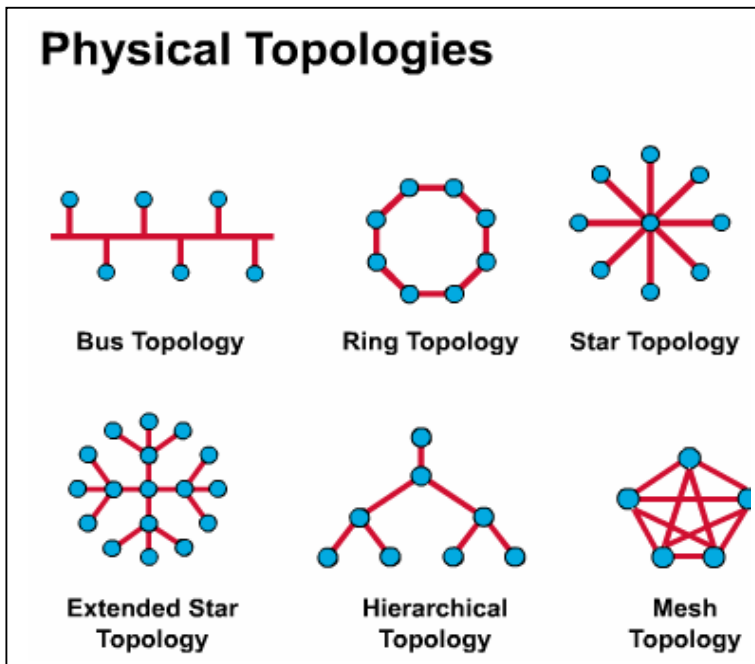
Ring Topology

A *ring topology* is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop, as shown in the figure above.

Star Topology

A *star topology* is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology.

Tree Topology

A *tree topology* is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case.

WAN Topology

A WAN spans a large physical distance. A WAN like the Internet spans most of the world. A WAN is a geographically dispersed collection of LANs. A network device called a router connects LANs to a WAN & the usual Topology of a WAN is in the form of a **Star or Mesh** Topology.

MAN Topologies

A MAN serves a role similar to an ISP, but for corporate users with large LANs. The WAN topology is usually of the **Mesh or Ring** Topology shown in the Physical Topologies Diagram.

3.1 Network Software

The Network Operating system that I am going to install is going to be Windows NT4 Server. Screenshots with corresponding notes are shown below:
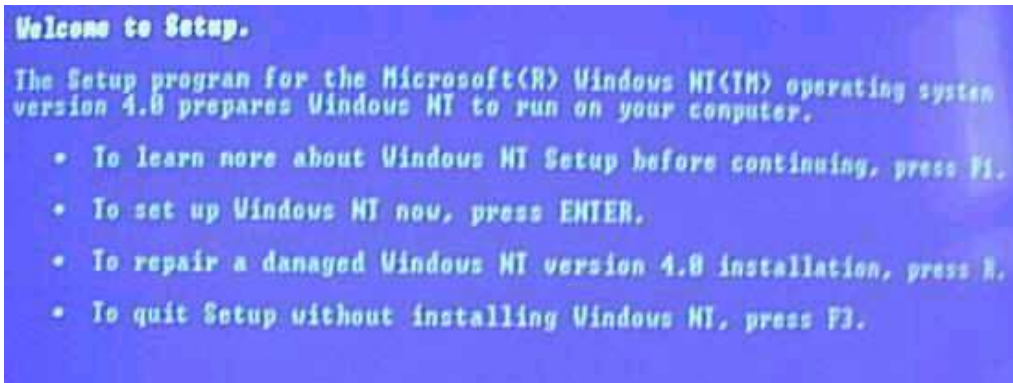
- **This is the Set-up screen and we press Enter to proceed with Windows NT Set-up.**
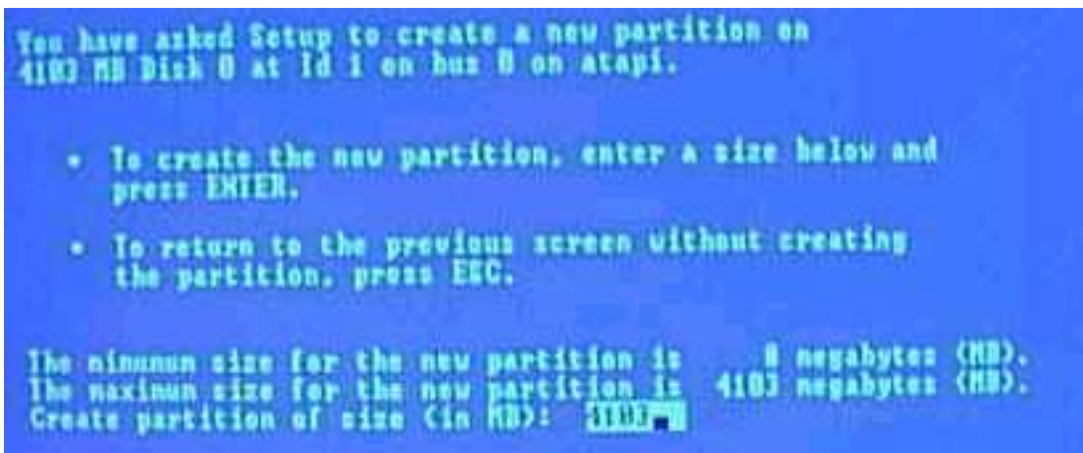
- Above we are being asked to partition the disk, after partition the user will be asked size of the hard drive. **(Note: if the user does not change this, the computer will use *default size* i.e. maximum size of hard dive.)**
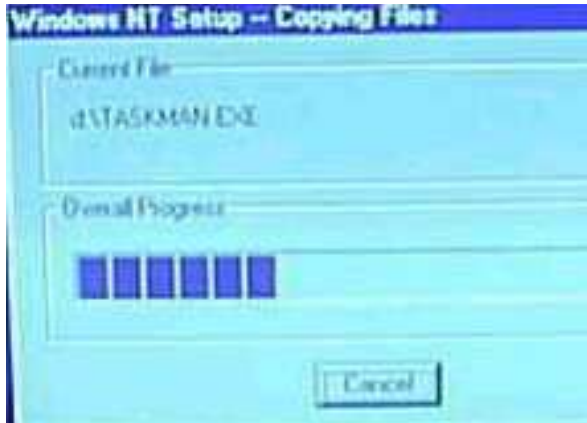
- After we have decided the drive to be copied to i.e. d:\ the Win NT process will then start copying files to this Drive on the PC hard drive.
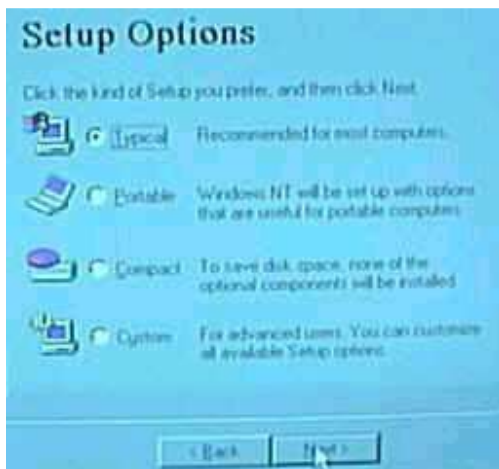
- Once the files have been copied to the selected drive, we are asked which set-up option we wish to have as our operating system, we choose typical option.

- Once we have entered the OEM number with a given name he/she can then create an administrator account.
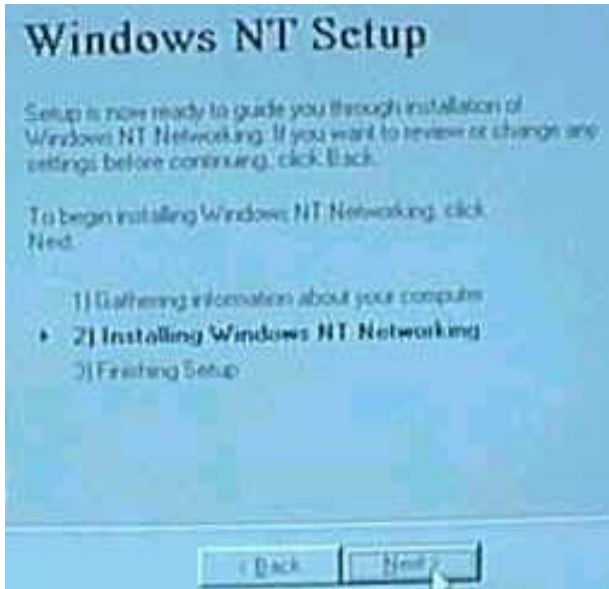
- After creating a rescue disk, the following screen appears, clicking next we follow the on screen instructions.
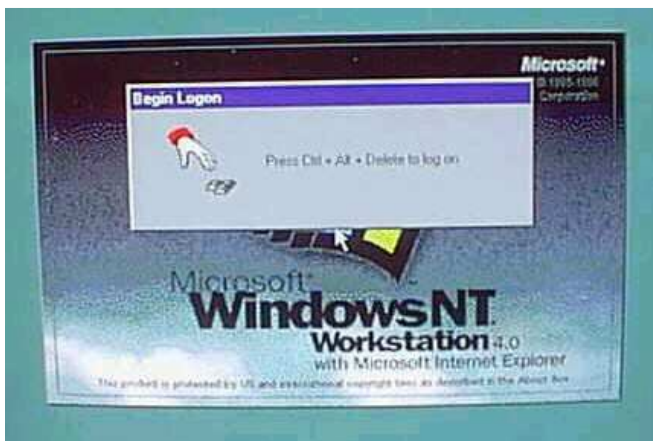
- After rebooting the computer you will arrive at the login screen, we then press "CTRL" and "ALT" and "DELETE" to enter password section
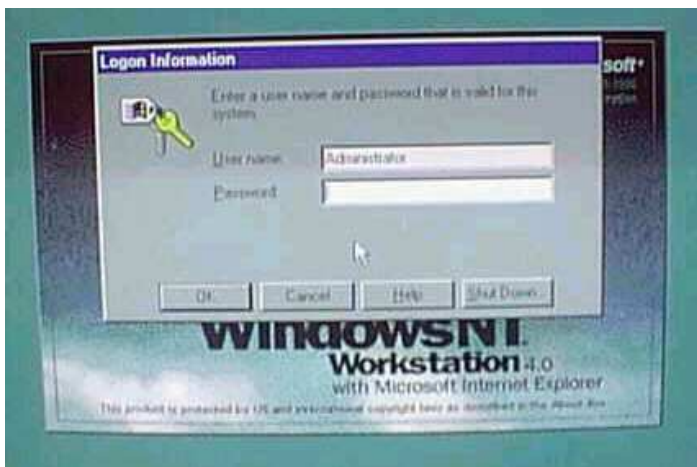
- Now we enter a password and press, "ENTER", if we didn't set one we can just press "ENTER".

- Finally the main screen starts up after the information has been inputted. This screen gives you tips on how to use the NT workstation.

Adding Users to the Server
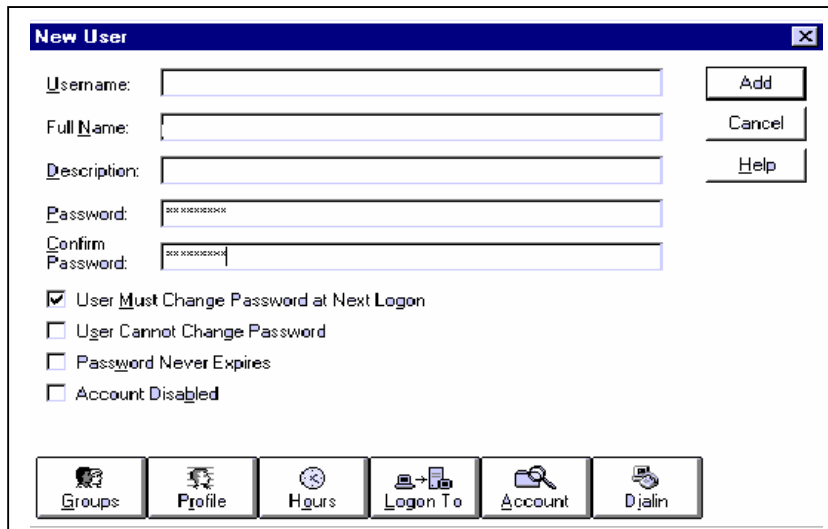
- Once we click on the "**add new user**" from the user manager, this screen will pop up. Administrator has to fill in the relevant details and select appropriate setting for the particular user. After inputting all the relevant details the administrator can also click on the button at the bottom of this screen for further setting.
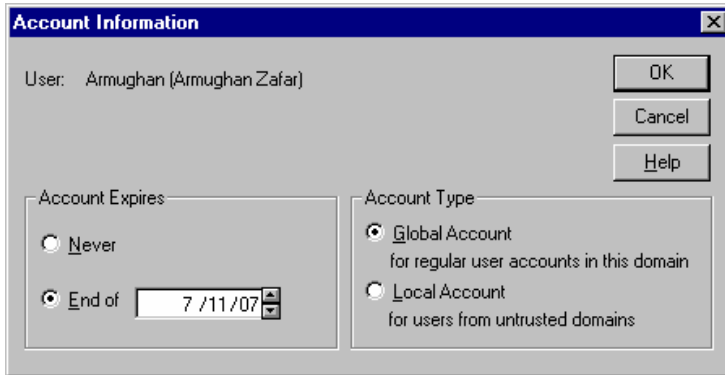
This is one of the options which administrator can choose.

In this section administrator can tell the system to expire the user account according to information provided to him e.g. if the user is student then administrator and set expiry date when student course finishes. Also you can choose the account type. For example if college have different branches administrator can give rights to student to use the network services in different branches as well. As you can see the user here is a student called Armughan Zafar with a Global Account.
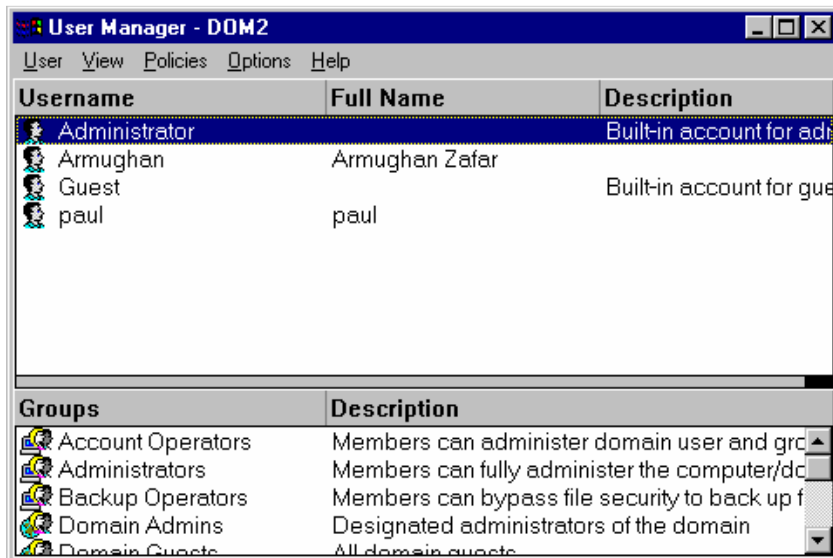
- Once the Administrator has added the new user he is free to add another user with new properties.
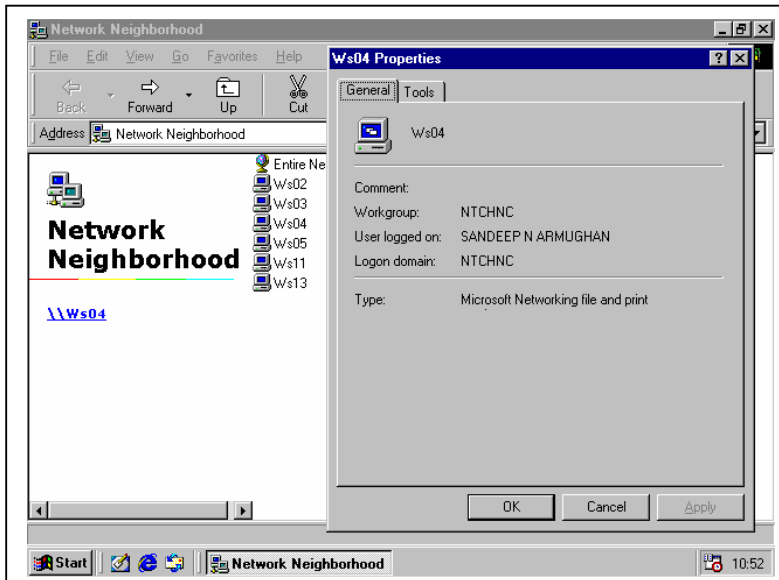
Installing Network Card

After choosing the card we have to select the location (drive) where the .exe file is so the system can get the required files to install the network card
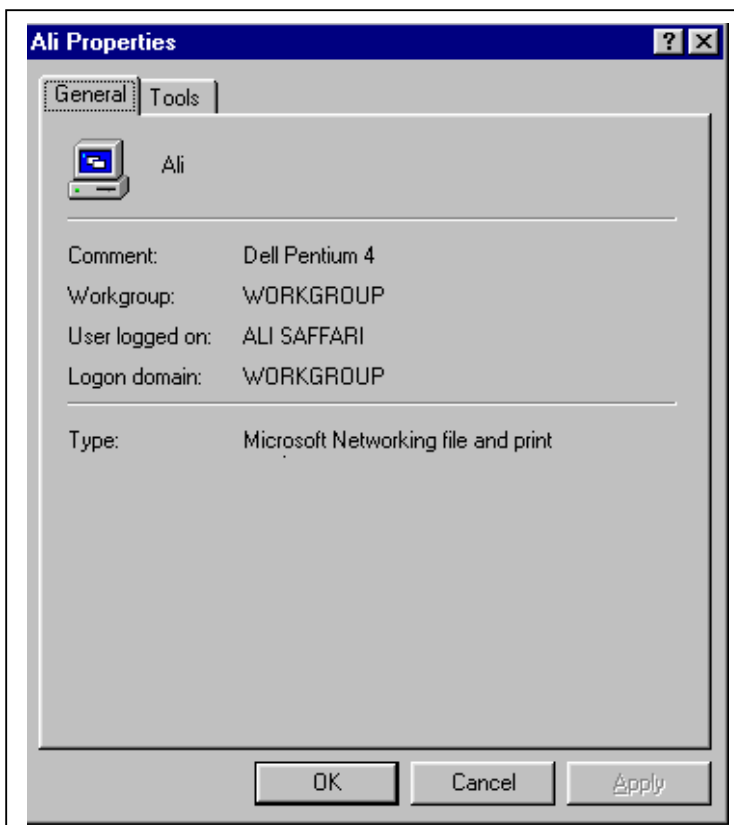

The 3COM EtherLink NIC Card was installed correctly & user has to click finish to complete the process.

Can the user logon to network?

This screenshot clearly shows that the user can log onto the network server.

The entire network and other users are clearly visible.

You can clearly see by this screen shot of this user, the "Domain Name", "User name" and also the "Workgroup".

This user can use the file and print sharing facilities as well shown at bottom of screen shot as "Type".

Installing network software

Windows 98 installation Set-up:

Step One: Preparing to Run Windows 98 Set-up

This "Welcome to Windows 98 Set-up" will eventually appear after we have completed on screen simple routine options from when the CD-Rom has auto booted up. Then we click "Continue" to move on.

Step Two: Collecting Information About Your Computer

During this step, Set-up collects information about your computer and prepares it for copying the Windows 98 files.

The License Agreement

After Set-up Wizard is loaded, the License Agreement is displayed. You must accept the License Agreement to continue.

Product Key

Set-up prompts you to enter the Product Key. This key number should already be filled in.

NOTE: The **Product Key** dialog box will not appear if you are installing Windows 98 from the network, depending on the requirements at your site.

Select Directory

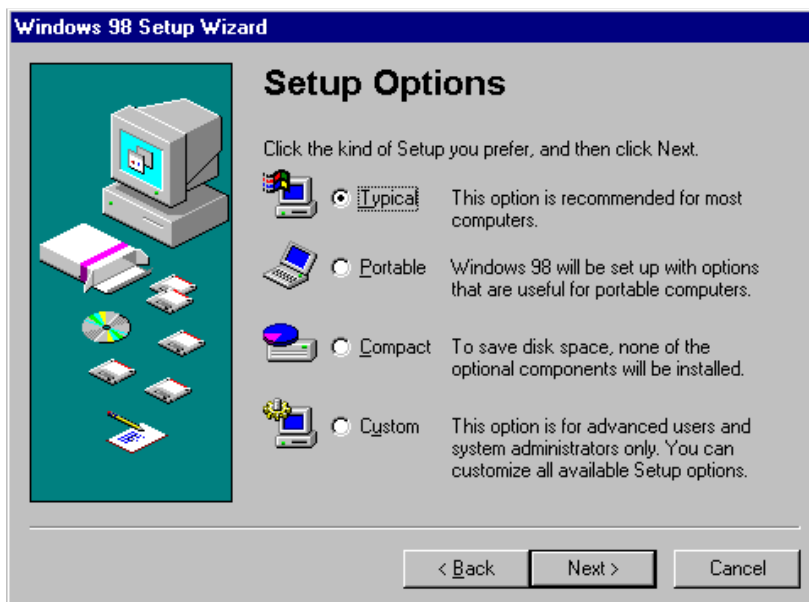After you enter your Product Key, the **Select Directory** dialog box appears

The default directory is C:\Windows, press next to continue with installation.

Preparing Directory

Set-up checks for installed components and then checks whether there is adequate disk space for the files

Set-up Options

Once Set-up finishes setting up the directory structure, it prompts you to select the type of Set-up you want through the **Set-up Options** dialog box.

Each Set-up option contains a specific set of components to install. When you choose a Set-up option, Set-up selects by default a set of appropriate components based on your choice.

In the **Set-up Options** dialog box, click the Set-up option you want, then click **Next**. The **Typical** Set-up option is selected as the default.

Click this option	If you want
Typical	All of the components that are usually installed with Windows 98.Most users should select this Set-up option.
Portable	To install the options generally required for portable computers.
Compact	The smallest possible installation of Windows 98. For example, you may want to perform a Compact installation if your hard disk does not have much free space. Setup then installs no optional components. If you later want to use an optional component, such as Games or WebTV for Windows, then you have to install it. To install an optional component after Setup is completed, use Add/Remove Programs in Control Panel.
Custom	To choose which optional components are installed. If you do not select a Custom installation, then Set-up installs only the optional components that are selected by default. If you know you are going to need certain Windows components, you may want to select a Custom installation and ensure that those components are included during Set-up. Pan European users should choose this option in order to select the required regional settings and keyboard layout for their locale. Pan European users should choose this option in order to select the required regional setting and keyboard layout for their locale.

User Information

After the Set-up Options, Windows 98 Set-up asks you to type your name and company name, which Windows 98 uses to identify you for various operations. You must enter this information for Set-up to continue.
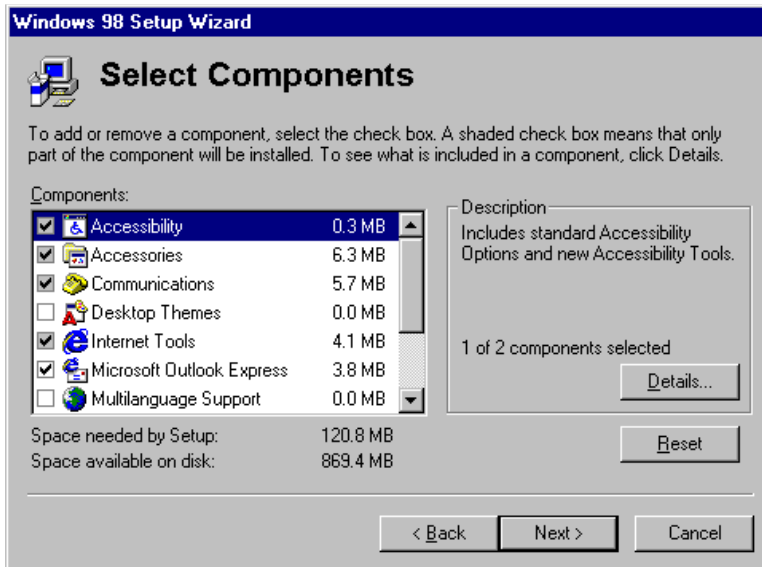
Windows Components
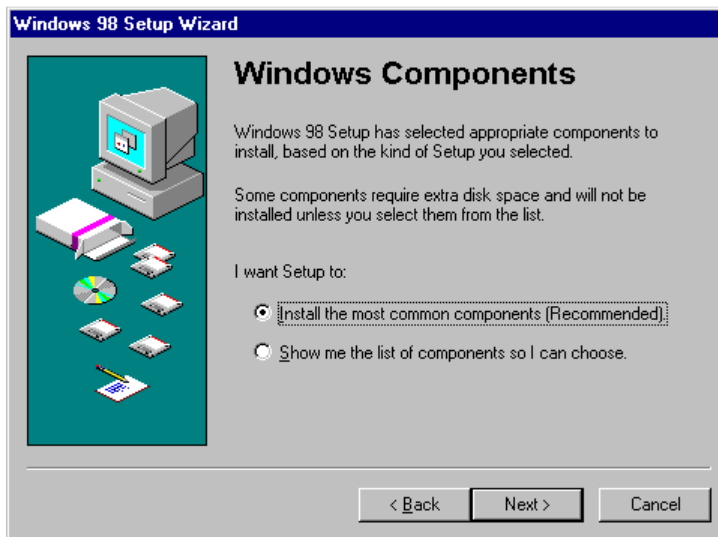
After you provide the user information, Set-up displays the **Windows Components** dialog box

If you select install the most common components, Set-up continues the installation. If you select "*Show me the list of components so I can choose"*, the Select Components dialog box appears:

Select Components

The **Select Components** dialog box lets you customise your installation by choosing the components you want to install
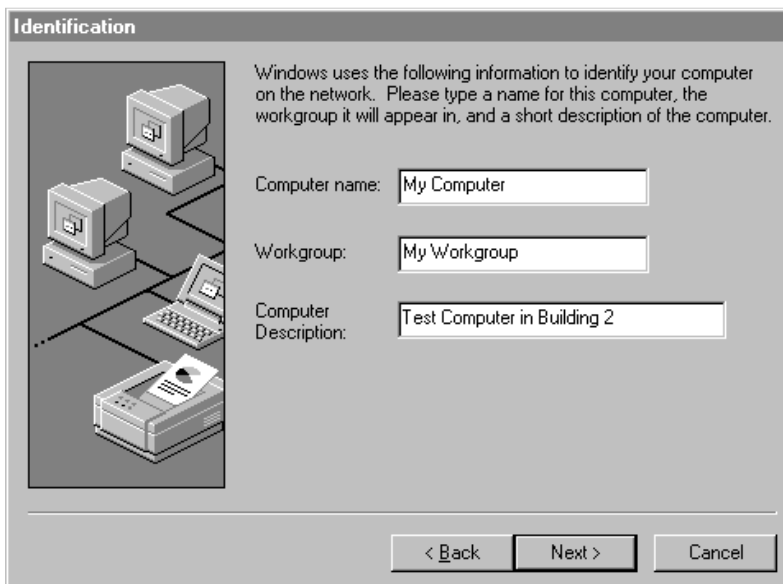
After you have selected which components you want to install, Set-up prompts you to identify how you want your computer to be identified on your network by displaying the **Identification** dialog box.

Establishing Your Location

Next, Set-up prompts you to establish your location by displaying the **Establishing Your Location** dialog box

Start-up Disk (Rescue Disk)

After establishing your location, Set-up prompts you to create a Windows 98 Start-up Disk by displaying the **Startup Disk** dialog box.

Start Copying Files

After Set-up finishes creating the Start-up Disk, the **Start Copying Files** dialog box appears. Click **Next** to start copying files.

Step Three: Copying Windows 98 Files to Your Computer

After Set-up has collected the information it needs from your computer, it begins copying the Windows 98 files to your computer. During this phase, Windows 98 Set-up does not require your input.

Step Four: Restarting Your Computer

After Set-up finishes copying the Windows 98 files to your computer, you are prompted to restart your computer. You can click the **Restart Now** button to restart your computer immediately; if you do not click the button or wait more than 15 seconds to click it, Set-up restarts your computer automatically.

Step Five: Setting Up Hardware and Finalising Settings

When Set-up finishes setting up hardware and configuring settings, Set-up restarts your computer and asks you to log on. If your computer is connected to the network, you may be asked for a domain name and a network password. After you log on, Set-up:

- Builds a driver information database.
- Updates system settings.
- Sets up personalised settings such as settings for the Internet Explorer 5 browsing software, **Start** menu, Online services, Volume Control, and Channels.
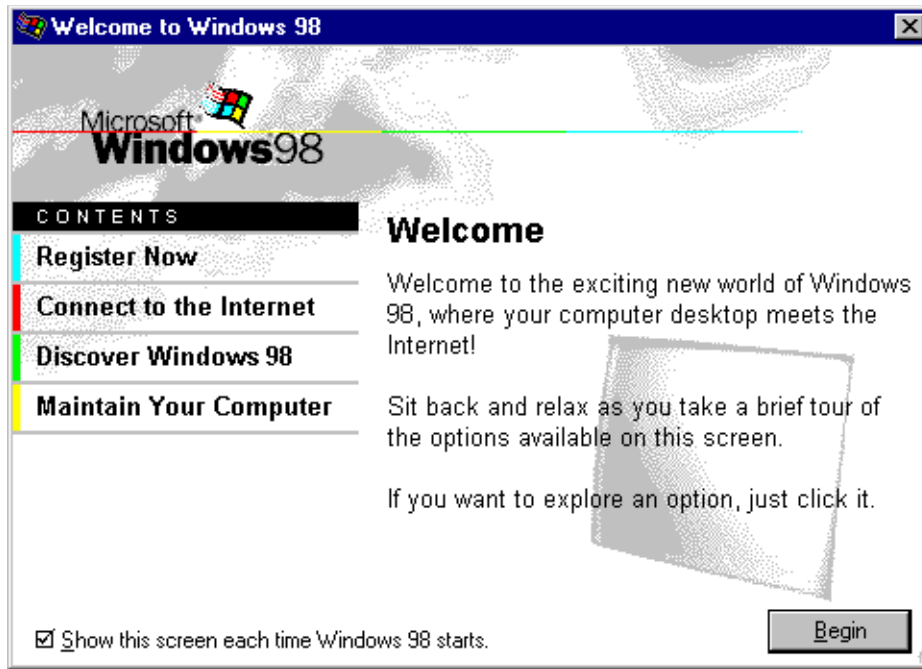
Then, Set-up displays the **Welcome to Windows 98** dialog box.
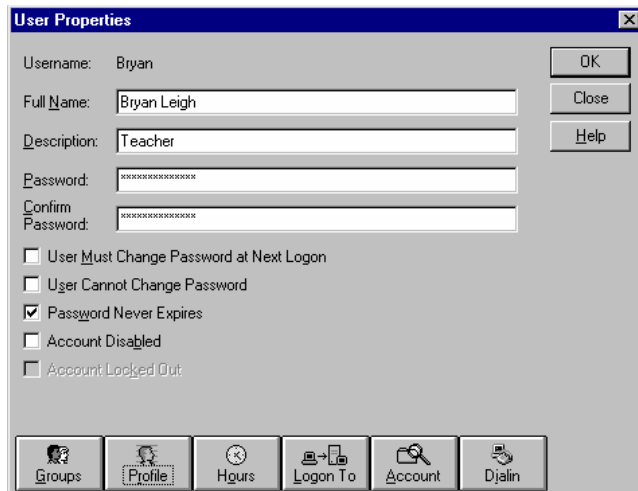
After changing the setting widows will restart and this screen will appear. Now user can start using windows 98.

Note: in NT environment user will have input user name and password other wise he will not be able to access the operating system.

4.1 Network Management

Apply control mechanisms in a typical network for managing users
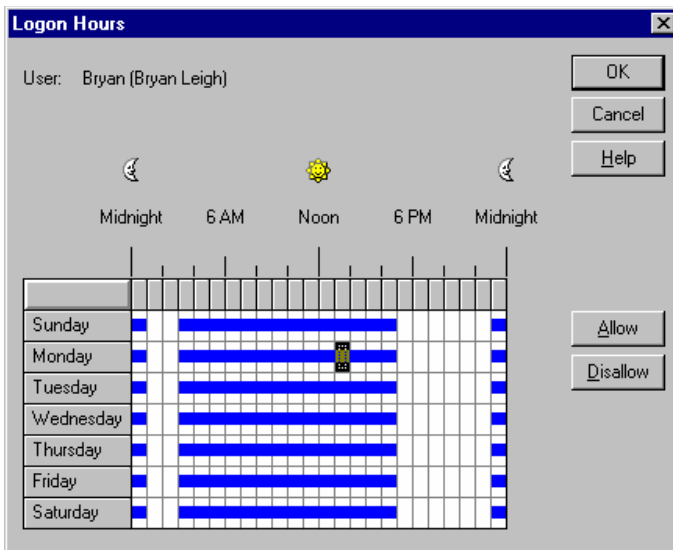
Setting User Passwords:

This picture show and user has been given password and this password will never expire.
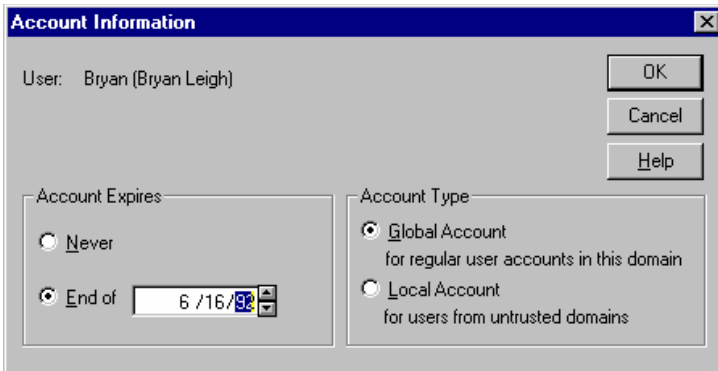
There are other options as well with regards to the password change, & the administrator can choose these setting depending on what he wants.

Restricting Logon hours:

As you can see that user can access the network at certain hours. Area, which is highlighted, shows the time when user can access the network.

Closing User Accounts

In this screen shot the administrator can choose when he wants the user account to expire. In this particular situation it is 16th of July 1992. The account type is global, this means user can access the network regardless which branch of the company he is in.

The close account is very useful feature e.g. if the account is for a student, we can set the account expiry date to coincide with the end of the course.

Control Printer Queues
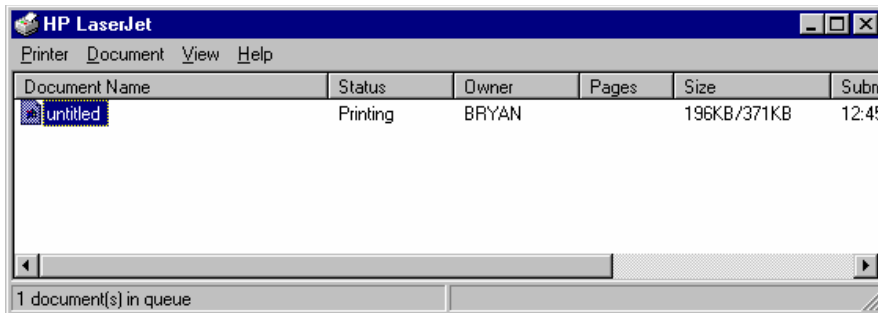
This screen shot shows that there is only one printing job to be completed. We can also see the menu on the top, which can provide help and assistance to the user & Administrator.
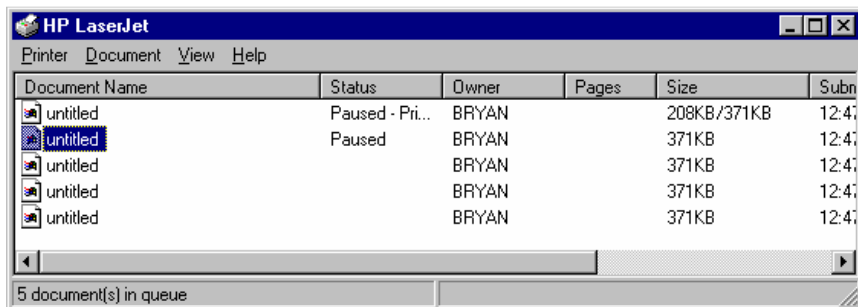
In this screen shot you can see that administrator has paused to jobs so other jobs get done first. In this instance we can assume that the other jobs were from company managers and administrator has give them priority.

Responsibilities of Network Managers

One or more individuals are responsible for every IP net or subnet, which is connected to the Internet. Their names, phone numbers and postal addresses MUST be supplied to the Internet NIC (or to the local or regional transit network's NIC) prior to the network's initial connection to the Internet, and updates and corrections MUST be provided in a timely manner for as long as the net remains connected.

In order to adequately deal with problems that may arise, a network manager must have either:

- System management access privileges on every host and router connected to the local network,

  Or:

- The authority and access to either power off, re-boot, physically disconnect or disable forwarding IP data-grams from any individual host system that may be misbehaving.

For all networks, a network manager capable of exercising this level of control MUST be accessible via telephone 8 hours a day, 5 days a week. For nets carrying transit traffic, a network manager **should** be accessible via telephone 24 hours a day.

<u>Some Computer Jargon</u>

- Network — The complete mechanism by which computers and peripherals are connected.

- Shared computing resource — A networked computer and its peripherals that can be used by more than one person.

- System manager — The person or group responsible for the operation and security of one or more networked computers (the person or group with system privileges).

- System administrator — The person having executive authority over one or more networked computers.

For more help on computer & hi-tech definitions visit this site:

- http://www.computeruser.com/resources/dictionary/index.html?term=T1

User rights and responsibilities

User rights and responsibilities of using a computer network can be clearly seen in the following statement from Northwestern University. As I am also a student I have chosen to use this university as an example, as oppose to a high street company.

©
"Rights and Responsibilities for the Use of Central Network and Computing Resources at Northwestern University

Information Technology (IT) is the University organization that provides access to the network for Northwestern students, as well as for many Northwestern faculty and staff. The Northwestern computer network consists of a campus-wide backbone network, local area networks, and many shared computers as well as personal desktop computers. IT works to insure that network rights and responsibilities are not violated.

Rights

Members of the Northwestern community can expect certain rights as they use the network and its services.

- **Intellectual Freedom**: The University is a free and open forum for the expression of ideas, including viewpoints that are strange, unorthodox, or unpopular. The University network is the same. Network administrators place no official sanctions upon the expression of personal opinion on the network. However, such opinions may not be represented as the views of Northwestern University.
- **Safety From Threats**: While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications should bring them to the attention of University Police. Electronic threats are taken as seriously as voiced or written threats, consistent with University policy.
- **Privacy:** Data files and messages traversing the University network are not private communications. The University reserves its right, as owner of the network and the computers in question, to examine, log, capture, archive, and otherwise preserve or inspect any messages transmitted over NUNet and any data files stored on University-owned computers. All members of the community must recognize that electronic communications are by no means secure, and that during the course of ordinary management of computing and networking services, network administrators may inadvertently view user files or messages. In addition, if a user is suspected of violations of the responsibilities as stated in this document, that user's privacy is superseded by the University's requirement to maintain the network's integrity and the rights of all network users. Should the security of a computer be threatened, user files and messages may be examined under the direction of the vice president for information technology, the associate vice president for information technology, or a director of information technology.

Responsibilities

There are also responsibilities that must be met as part of the privilege of network access. Network users are expected to live up to these responsibilities. If you knowingly violate a network responsibility, your network access will be suspended. Depending on the seriousness of the violation, you could be referred through the University disciplinary procedure process. Violations that also violate federal or state laws will result in referral to the appropriate legal authority.

1. You are responsible for the use of your network ID (NetID) and all computer accounts that are assigned to you. You may not give anyone else access to your NetID or computer accounts. You must not use a NetID or an Northwestern University computer account that was not assigned to you. You may not try in any way to obtain a password for another user's NetID or computer account. The NetID and its associated password are the property of Northwestern University Information Technology. Applications and services that require their use must be approved by the Office of the Vice President for Information Technology or by a director within NU IT.
2. You may not misrepresent yourself or your data on the network.
3. You are responsible for the security of your passwords. This includes changing passwords on a regular basis and making sure no one else knows them.
4. You must not use NU's network resources to gain or attempt to gain unauthorized access to remote computers.
5. You must not deliberately perform an act that will seriously impair the operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
6. You must not run or install on any of NU's computer systems, or give to another, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
7. You must not attempt to circumvent data protection schemes or exploit security loopholes.
8. You must abide by the terms of all software licensing agreements and copyright laws. You must not make copies of or make available on the network-copyrighted material, unless permitted by a license. Please see the more complete discussion of software copyright protections available on NUInfo.
9. You must not deliberately perform acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of other users. Any person operating a network-intensive application or a defective computer that overloads University networks will be notified and steps will be taken to protect the overall University network. This may include disconnecting the offending computer system from the University network until the problem is resolved. If the condition is an imminent hazard to the University network or

disrupts the activities of others, then the offending computer system or the subnet to which it is attached may be disconnected without prior notice.

10. You may not place on any University-owned computer system information or software that infringes on the rights of another person or gives unauthorized access to another computer account or system.

11. You must not attempt to monitor another user's data communications, nor may you read, copy, change, or delete another user's files or software, without permission of the owner.

12. Computing and networking resources are provided to support the mission of the University. These resources may not be used for commercial purposes.

13. Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows, as well as to the policies listed here.

14. All University computing and networking facilities are provided for use by faculty, staff, and students for relevant academic, research, or administrative pursuits. Like all other University facilities, private use must be approved in advance in keeping with policies expressed in the Northwestern University Employee Handbook and the Northwestern University Student Handbook.

15. Information servers - responsibility for content. The content of any information made available to others via the University's network is the sole responsibility of the person who created that information. It is that person's responsibility to be aware of all applicable Federal laws, State laws and University policies. That person will be liable for any violations of Federal laws, State laws, or University policies.

The IT security coordinator and the appropriate authorities should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of any computer systems and networks at Northwestern."
©

The rights & responsibilities of the users at this university are clearly shown (inside of the © sign). Most universities have similar user rights & responsibilities with respect to there IT network, which may be at anytime updated and changed by the administrator of the university.

Cost of Installation of the Laboratory/Office Network

The following text will show the rough evaluation of installation and relevant equipment needed to set-up the Laboratory/Office network. Please note that this is only a rough guide and that prices and quotations may vary according to size of purchase and place of acquisition.

Essential Network Hardware

- Category 5e Solid Core Cable - 305m box - £40.00 (incl. VAT)
- RJ45 Plug (x 20) - £2.50 (incl. VAT)
- Network Interface Cards - Dlink PCI Network Card 10/100 Mb OEM - £10.58
- N.O.S – (Windows 2000 Server) for 25 Clients - £849.99
- Desktop Operating System will be Windows 2000 - £499.99
- Application: Microsoft Office 2000 Professional - £194.99
- NetWare 5.1 Server - £699.99
- Internet Access: Internet Bandwidth: 2Mbps: £1'200 Per Month or £10,800 per annum. (http://www.newnet.co.uk/leasedlines/#prices)
- Network Maintenance – Depending on the Size & Network Protection Standards etc the approximate cost of maintaining a Network is 80% of the IT budget & can be quite expensive.

TOTAL APPROXIMATE COST: £ 13'000 – £14'000 per annum.

Reference & Bibliography

Using The Harvard Referencing System as a guide, these are my points of reference and the textbooks that I used to complete the assignment.

Reference List

- B.HELLINGSWORTH, P.HALL & H.ANDERSON (2001), *Higher National Computing,* Newnes.

- DOUG LOWE (2001), *Networking for Dummies*, Hungry Minds Inc

- ANDREW TANENBAUM (2002), *Computer Networks,* Prentice Hall.

- SYBEX (2002), *Networking Complete,* Sybex International.

Web Site References:

- http://www.it.northwestern.edu/policies/itpolicy.html, "Rights and Responsibilities for the Use of Central Network and Computing Resources at Northwestern University", accesses on 20/11/2002

- http://dlis.gseis.ucla.edu/people/pagre/network.html, "Networking on the Network", accessed on 20/11/2002.

- http://networking.ittoolbox.com/default2.asp, "Networking Knowledge Base", accessed on 20/11/2002.

- http://www.google.co.uk/, "Google", accessed on 21/11/2002.

- http://www.gateway.com/work/sb/solutions/networking.shtml, "Connect your Business", accessed on 21/11/2002

- http://www.jigyo.com/TheNetworkersPlace/networkingFacts.htm, "networking Facts", accessed on 21/11/2002

- http://www.microsoft.com/catalog/navigation.asp?subid=22&nv=2, "Operating Systems & Servers", accessed on 22/11/2002

- http://www.computeruser.com/resources/dictionary/index.html?term=T1, "Welcome to the Computer User Hi-Tech Dictionary", Accessed on 23/11/2002

Reference Index