# The "Barefoot" Network Engineer

**Presented by John Brock**

John Brock is an electronics engineer with over 20 years experience in the electronics industry, with the last 5 years concerned with microprocessor based development. He has designed communications equipment for the South African Air Force as well as time and attendance systems. He also has designed a series of micro controllers for time and data process applications. In more recent times he has written communications and network applications software for the PC, as well as designed an internal modem card for an overseas customer. As an independent consultant he provides development, support and backup facilities for individual and corporate clients.

John has been involved in the design and presentation of the Barefoot Engineer series of courses for over five years.

# Contents

**Local Area Networks**

Local area networks cover distances up to a mile, sorry 1.6 kilometre. A network connects a variety of electronic devices, including microcomputers and main frame computers. Process control of an industrial plant can be done using a network. An office of microcomputers can be made highly efficient by the addition of an interconnecting network. Connections can be metal cable of twisted pairs, similar to phone wiring, or can be coaxial shielded cable or even fibre optic cable. Each type of connection has its own advantage; whether it is immunity to lightning in the case of fibre optic cabling, or low cost in the case of twisted pair copper wires.

**Wide Area Networks**

Wide area networks cover areas such as countries or continents and may soon become global in scope. The inclusion of satellite links into the telecommunications circuits allows for users using a notebook and a radio link to login to a global network from anywhere in the world. The Post Office provides a digital network of high reliability for communications between computers using the X25 protocol.

# Network Topologies

**ARCnet (2.5 Mbits/Sec) & ARCnetplus (20 Mbits/Sec)**

ANSI standard : ATA/ANSI 878.1 Local Area Network Standard.

Cabling :         RG62/U 93 Ohm coaxial cable using 75 Bayonet Connectors (BNC)
                  Twisted pair using RJ45 connectors

ARCnet stands for Attached Resource Computing Network. ARCnet is a baseband, token-passing network system that offers flexible star and bus topologies at a low cost. Transmission speeds are 2.5 Mbits/sec and later 20Mbps. ARCNET uses a token-passing protocol on a token bus network topology, but ARCNET itself is not an IEEE standard.

Datapoint developed ARCNET in 1977 and subsequently licensed it to other companies. Standard Microsystems Corporation developed the first single-chip LAN controller based on the ARCNET token-passing protocol in 1981. A new chip set technology supporting bus topology was introduced in 1986.

ARCNET cards are available from many vendors, including SMC (Standard Microsystems Corporation) and Thomas-Conrad. Standard coaxial boards have a BNC connector attached to the back. Some later cards were fitted with both coaxial and UTP type connectors. When ARCNET is configured as a linear bus, T- connectors are used on the cards, and jumpers must be set to specify the configuration to remove the built-in terminators from the circuit.

It is possible to make the pc a diskless workstation, to do so a boot eprom must be fitted into the socket on the card for the network system.

ARCNET interface boards have a dip switch on which you set the node address for the workstation. You must assign each node on the network a unique address in the range of 1 to 255. Record this assigned number in a log book and on the workstation

Arcnet packets have five different types of frame formats as specified in the ARCNET protocol. All the frames start with an alert burst that contains six binary ones. The frames are summarised as follows: *The invitation to transmit (ITT) is the token frame. Workstations obtain the token when they want to transmit.

**Limitations**

The maximum cable distance between stations at the extreme ends of an ARCnet network, must not exceed 6098 metres. The maximum distance between an active hub and another active hub or network station, is 610 metres. The maximum distance between an active and passive hub is 30 metres. The maximum distance between a passive hub and a network station is 30 metres. A passive hub may not be connected to another passive hub. All ports on a passive hub must be terminated. You may only run an active hub off the server or another active hub.

**Ethernet - (CheaperNet) (IEEE 802.3) (10.5 Mbits/Sec)**

Ethernet is a linear bus system. All the stations are connected directly onto a central length of cable called the trunk or bus. The network signals travel along the bus using a "contention cable access" scheme. When a workstation needs to send a packet to the file server, it checks if the line is already busy, and if the line is free, it then transmits its packet.

Cabling :        0.2 inch RG58/U 50 Ohm coaxial cable (thin cable) using 50 Ohm BNC
or unshielded twisted pair (UTP) using RJ45 connectors.
0.4 inch RG213/U 50 Ohm coaxial cable (thick cable)

## The 'Electronic Envelope'

Networks are based upon a simple 'electronic envelope' which carries data from one 'node' to another reliably. Just like an ordinary envelope it has a destination field like the front of the envelope with the address. As well as the return address contained in a field called the source address.

All these fields and data are binary and are transmitted over the cable by the network cards as a collection of bytes. A byte is 8 bits and a bit is either a '1' or a '0'.

## An Ethernet 'Frame' or 'Packet'

| Preamble | Destination address | Source address | Type | Data | Frame check sequence |
|---|---|---|---|---|---|
| (8 bytes) | (6 bytes) | (6 bytes) | (2 bytes) | (up to 1500 bytes) | (4 bytes) |

**Limitations - Thin cable**

The maximum length of a trunk segment is 185 metres. Trunk segments may be connected by repeaters to form a trunk with a maximum of 925 metres. A maximum of 30 stations, including repeaters, may be connected to any trunk segment. Each end of the trunk segment must be terminated by a terminator, and only one end need be grounded. The minimum distance between stations is 0.5 metre.

**Limitations - Thick cable**

As with thin Ethernet cable, the maximum number of trunk segments is five. The maximum length of a trunk segment is 500 metres. The maximum trunk length is 2500 metres. A maximum of 100 stations is permitted per trunk segment. Transceivers may be up to 2.5 metres apart and the maximum transceiver cable length is 50 metres. Packet lengths can vary from 64 to 1526 bytes of information. A data block in the packet contains approximately 1500 bytes, the rest are destination address, source address, error control codes and network control information. The practical limitation to Ethernet is that all nodes must hear part of a packet at the same instant. This sets the limit on maximum size/length of the network.

**Fast Ethernet - IEEE 802.3u (100Mbits/Sec)**

100BASE-TX and T4 supports 100 Mbps transmission over four pairs of category 5 twisted-pair Ethernet (TPE) wiring.  Three pairs of wire are used to send and receive. A fourth pair is used for collision detection.  Segment lengths are limited to 100 meters with 100BASE-TX for signal timing reasons.  This complies with the EIA 568 wiring standard.

**Token Ring (IEEE 802.5) (4 or 16 Mbits/Sec)**

In this ring system, all stations are connected in a physical ring. The network signals travel from station to station, using a token passing scheme. When a station needs to send a message, it has to take control of the token. The token also moves from station to station. When the signal has been transmitted, the sending station frees the token for use by other stations.

**Limitations**

The maximum number of stations is 96. Only 12 multi-access units (MAU's) may be used. The maximum patch cable distance between a MAU and station is 45 metres. The maximum patch cable distance between  two MAU's is 45 metres. The total cable distance connecting all MAU's is 120 metres.

**Network Configurations**



BUS TOPOLOGY (eg: ETHERNET)

STAR TOPOLOGY (eg: ARCnet)

RING TOPOLOGY
(eg: TOKEN RING)
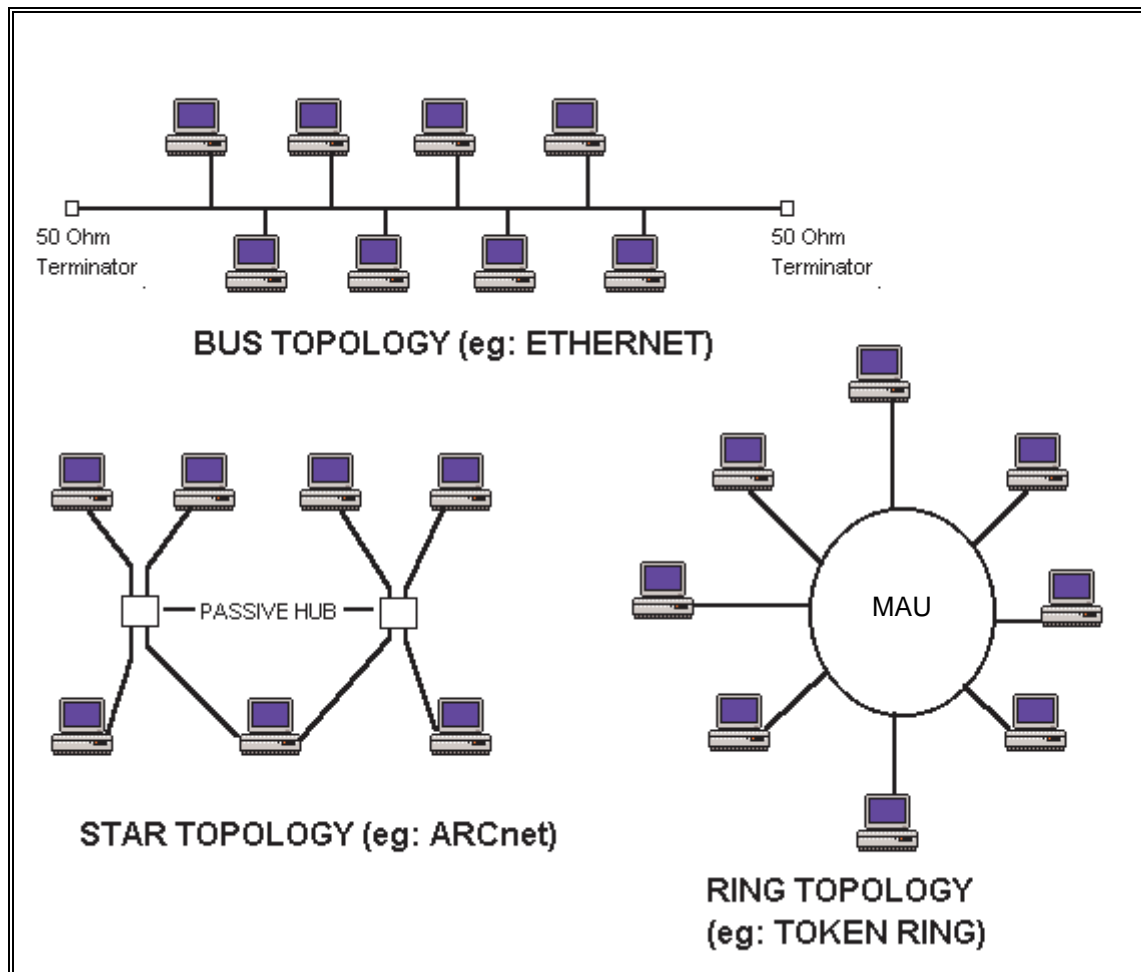
## Cabling and types of connection

Co-Axial cable and Twisted pair cable are the two main ways of connecting pc's.

**Co-Axial Cable**
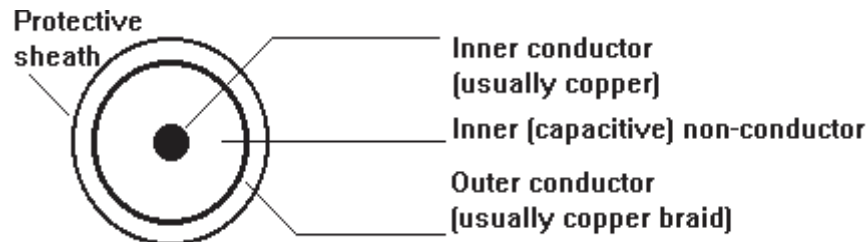


The following table list some advantages and disadvantages of coaxial cabling.

| Advantages | Disadvantages |
| --- | --- |
| | |
| Low maintenance costs | Limited distance and topology |
| Simple to install and tap | Low security; easily tapped |
| Better resistance to signal noise over longer distances | Difficult to make major changes to the cabling topology |
| Cable cost is higher than that of twisted pair, although electronic support components less expensive | |

**Twisted Pair Cable**
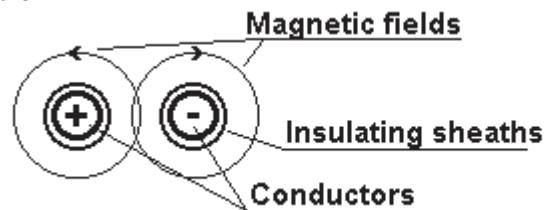


The following table list some advantages and disadvantages of twisted-pair cabling.

| Advantages | Disadvantages |
| --- | --- |
| | |
| Well-understood technology | Susceptible to noise |
| Least expensive medium | Distance limitations |
| Pre-existing phone wire may be in place to connect workstations | Requires expensive support electronics and devices |
| Easy to add computers to network | Limited maximum bandwidth |
| Same medium as telephones | Easiest to tap |

## Twisted-Pair Ethernet (TPE) cabling

TPE cabling is also known as RJ-45 cabling, Unshielded Twisted Pair (UTP), and 10BASE-T cabling.

The RJ45 connector can use 22, 24, or 26-gauge UTP cabling. The cable must comply with the IEEE 802.3 10BASE-T standard for Category 3, 4, or 5.

The cable between the computer and the hub must be less than 100 meters long.

### Recommended cables

| Manufacturer | Model number | No. of pairs |
|---|---|---|
| Belden | 9562 | 2 |
| Data Set | 2402 | 4 |
| Belden | 9566 | 6 |

### Cable and connector pinouts

If you need to repair a cable or provide connectors for UTP cable, wire straight through as shown in the following table.

```
Function            Pin                     Pin

  TX+                1     <-------->          1
  TX-                2     <-------->          2
  RX+                3     <-------->          3
  RX-                6     <-------->          6
```

Use only four of the eight pins. Pins 1 and 2 must be a pair, and pins 3 and 6 must be a pair.

To allow for a straight-through cable, hubs provide an internal transmit/receive crossover function. This means the transmit circuit of the network card is connected to the receive circuit of the hub and vice versa.

### Pinout for the RJ45 connector

```
     ----------                -------------------------
1 |--          |        8 |-----------               |
2 |--          |        7 |-----------               |
3 |--      ---  |       6 |-----------               |
4 |--          |        5 |-----------               |
5 |--       |  |        4 |-----------               |
6 |--      --- |        3 |-----------               |
7 |--       |  |        2 |-----------               |
8 |--       |  |        1 |-----------               |
     ----------                -------------------------
END                      TOP
```
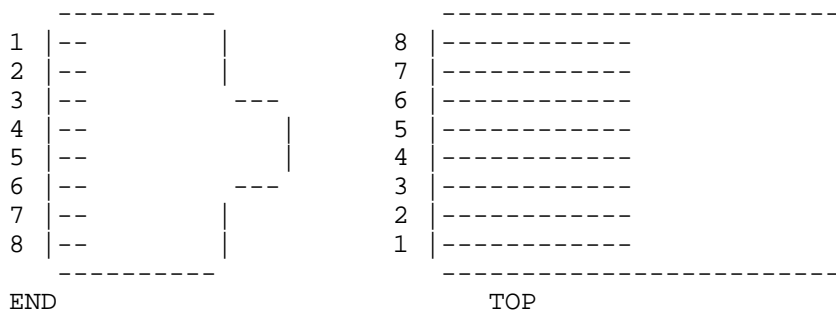
**Pin    Function**

1    Transmit Data Plus. The positive signal for the TD differential pair. This signal contains the serial output data stream transmitted onto the network.
2    Transmit Data Minus. The negative signal for the TD differential pair. This contains the same output as pin 1.

3       Receive Data Plus. The positive signal for the RD differential pair. This signal contains the serial input data stream received from the network.
4       Not used.
5       Not used.
6       Receive data minus. The negative signal for the RD differential pair. This signal contains the same input as pin 3.
7       Not used.
8       Not used.

## Connecting two workstations without a hub

10BASE-T uses a star topology. This means a hub or concentrator is in the centre of a star, and each workstation or server is connected to this hub.

For test purposes, you can directly connect two workstations or a workstation and a server without using a hub. This setup requires a special cable incorporating the crossover function described earlier in this document.

| Function | Pin | | Pin | Function |
|---|---|---|---|---|
| TX+ | 1 | <--------> | 3 | RX+ |
| TX- | 2 | <--------> | 6 | RX- |
| RX+ | 3 | <--------> | 1 | TX+ |
| RX- | 6 | <--------> | 2 | TX- |

NOTE: This is not an IEEE-supported configuration and should be used for test purposes only.

## Cable Characteristics

The chief property of either type is its characteristic impedance Zo, which ideally is a resistance. It can be regarded as the input impedance of an infinite length of the line. More practically, it is the input impedance of any length of the line connected at the far end to (ie: terminated by) an impedance Zo. The correct termination is vitally important, as this is the value which assures maximum power transfer from source to termination. A mismatched line gives rise to standing wave effects on that line with high and low voltage points at points along the line. The worst case termination is of course either a short circuit or open circuit and this can give rise to complete loss of signal at other points on the line. Signals do not travel down the line at the speed of light as might be expected, but at a velocity determined by the cable characteristics. This velocity is typically 0.66 that of light (300 million metres per second).

## Immunity

It should be noted that cable is used to connect computers for transfer of data and any external electrical signals should be suppressed to ensure reliable communication. The Co-Axial cable relies upon its braid for electrostatic shielding and some cables are made with double braid to provide extremely high immunity to interference. Twisted pair cables rely upon the electrical balance between the two conductors for its immunity. A ratio of 200:1 (46db) is typically required and any small dissimilarity between the two halves can reduce this ratio dramatically.

**Optical Fibre**

Optical fibres are used to carry digital data signals in the form of modulated pulses of light. An optical fibre consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding.

There are two fibres per cable-one to transmit and one to receive. Optical fibre cable transmissions are not subject to interference and are very fast (currently transmitting about 100 Mbps with demonstrated rates of up to 200,000 Mbps).

The following table shows some advantages and disadvantages of optical fibre cabling.

| Advantages | Disadvantages |
|---|---|
|  |  |
| High bit rates | More expensive than other cabling types |
| Lowest transmission loss over longer distance | Cabling is inflexible; can't be bent sharply |
| Not subject to interference | Lack of standard components |
| Good for network "backbones" | Limited (practically) to high-traffic, point-to-point |
| Supports voice, data, video | Requires skilled installation and maintenance |
| Difficult to tap | High installation costs |

**Fibre Optic links**

Fibre optic cable has total immunity to external interference, including lightning, and has improved its loss figures over the last few years. The expensive part is the transducers that convert the electrical data signals to light. The bandwidth of fibre is almost infinite such that high data throughput can be achieved. Fibre is being used to upgrade telephone trunk cabling between major city centres.

**Connectors**

Co-Axial cable invariably makes use of "Bayonet" type connectors, usually called "BNC" connectors. BNC stands for bayonet Connector. BNC connectors are useful up to 500MHz and provide reliable connection at low (0.1 dB) loss. Twisted pair connectors are of the telephone type RJ235 or RJ45 connector, which are low cost and easy to connect to cable.

---

## File Servers

A centrally located computer that acts as a storehouse of data and applications for numerous users of a local area network. Most of the file servers in use are adapted PCs. Newer servers were designed specifically for file-server purposes. Multiprocessor based microcomputers offer the highest possible performance.

## Workstations

The term widely used to describe the input/output device where an operator enters and retrieves electronically stored data. A workstation may be a "dumb" terminal, without a processor, an 80X86 based PC or Motorola 68000-series Macintosh, or a high-end RISC.

## Peer to peer networks

A data-exchange method in which two or more nodes can initiate communication with each other. Usually describes a network in which all nodes are capable of sharing resources, so a dedicated file server is unnecessary.

## Hubs

A wiring concentrator or repeater that brings together the connections from multiple network nodes. Although the true physical configuration of a hub-based network-called the network's topology-seldom fits the description exactly, such networks are described as being "star wired."

## Fast Ethernet Hubs and Switches

The two basic types of hubs are shared hubs and switching hubs. At 100 Mbps, a TX type hub or switch is required.

## Shared hubs

In a shared network environment, computers are connected to repeaters called hubs. All ports of the repeater hub share a fixed amount of bandwidth, or data capacity. On a 100 Mbps shared hub, all nodes on the hub must share the 100 Mbps of bandwidth. As stations are added to the hub, the effective bandwidth available to any individual station gets smaller. Shared hubs do not support full duplex.

On a shared hub all nodes must operate at the same speed, either 10 Mbps or 100 Mbps. Fast Ethernet repeaters provide 100 Mbps of available bandwidth, ten times more than what's available with a 10BASE-T hub/repeater.

Repeaters use a well established, uncomplicated design, making them highly cost effective for connecting PCs within a workgroup. These are the most common type of Ethernet hubs in the installed base.

## Switching hubs

In a switched network environment, each port gets a fixed, dedicated amount of bandwidth. Also data is sent only to the port that leads to the proper destination station. Network bandwidth is not shared among all stations, and each new station added to the hub gets access to the full bandwidth of the network.

If a new user is added to a 100 Mbps switching hub, the new station receives its own dedicated 100 Mbps link and does not change the 100 Mbps bandwidth of another station. Switching hubs can effectively increase the overall bandwidth available on the network, significantly improving performance. Switching hubs can also support full duplex operation.


## Repeater

A device that regenerates and amplifies signals to extend the transmission distance. It is designed to compensate for the degradation of the signals on the cable. It amplifies the signals travelling on the cable in both directions.


## Router

A device that connects LANs at the network layer and supports protocols required for the routing of packets. Contrast this with a bridge (a protocol-independent device for connecting networks at the MAC layer).


## Gateway

A device connecting two or more dissimilar networks or a network with a mainframe. Gateways can be pc's operating as modem sharing stations or fax gateways.

Gateways operate at the session, presentation, and application layers.


## Bridge

A networking device that connects local or wide area networks using the same data-link layer protocol. Bridges operate at the data link layer in the OSI reference model. Contrast with router.


## What's the difference between a Bridge and a Router?

A Bridge operates at the data link layer and is protocol independent. It doesn't know about the network topology and cannot perform alternate routing. It has a high data throughput.

A router operates at the network layer and is protocol dependent. It does 'know' the network topology and can perform alternate routing. It has moderate data throughput.

## Network Construction

Here is a typical File Server type network with a single hub, patch panel and one of many points.
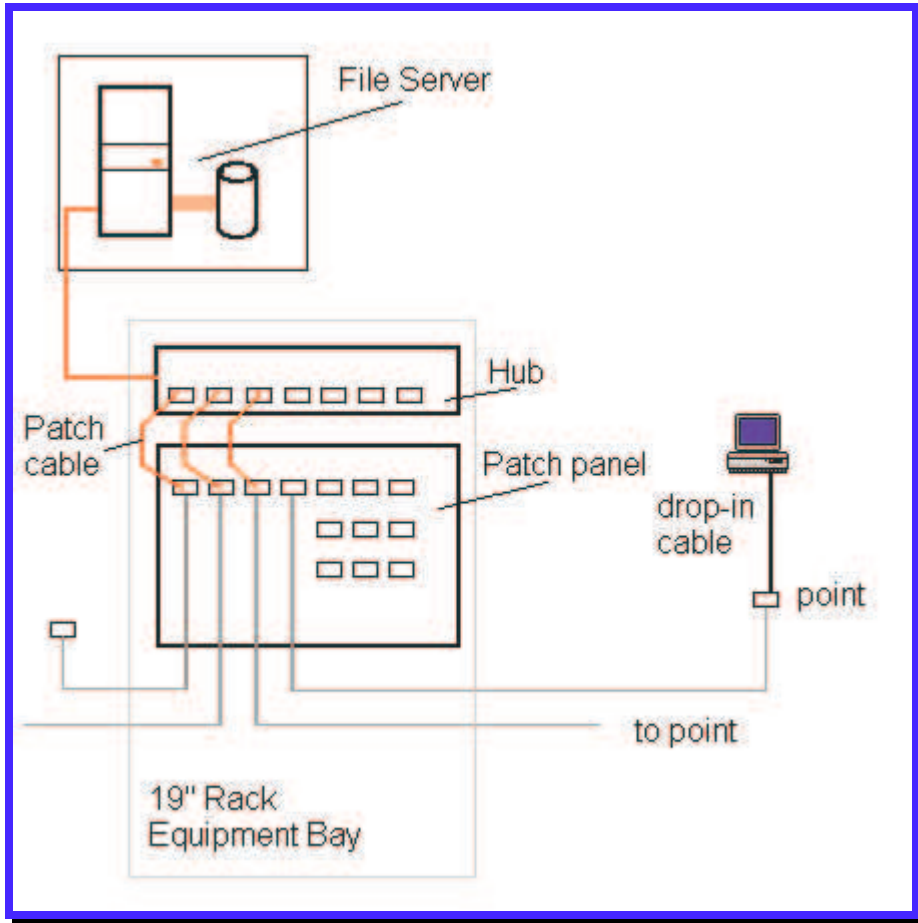


The connection between server and hub may be coax cable, twisted pair or even fibre optic cable. The short patch cables (< 0.5m) are used to connect the 'ports' of the hub to the patch panel connectors. The inside connection of the patch panel connector is wired to the rear of the bay and out to the respective point on the network. A short length of cable (< 10m) is used to connect the workstation to the point in the office.

This type of contruction has been used for the last few years as it provides easy connection of new users and movement of workstations from point to point. It is initially more costly than the coaxial cable network but repays that cost with serviceablity and ease of extension.

# Network interface adapters

Network adapter cards for interfacing the PC to the cable connection come in all shapes and sizes with a variety of specifications. Two of the three main types are discussed here.
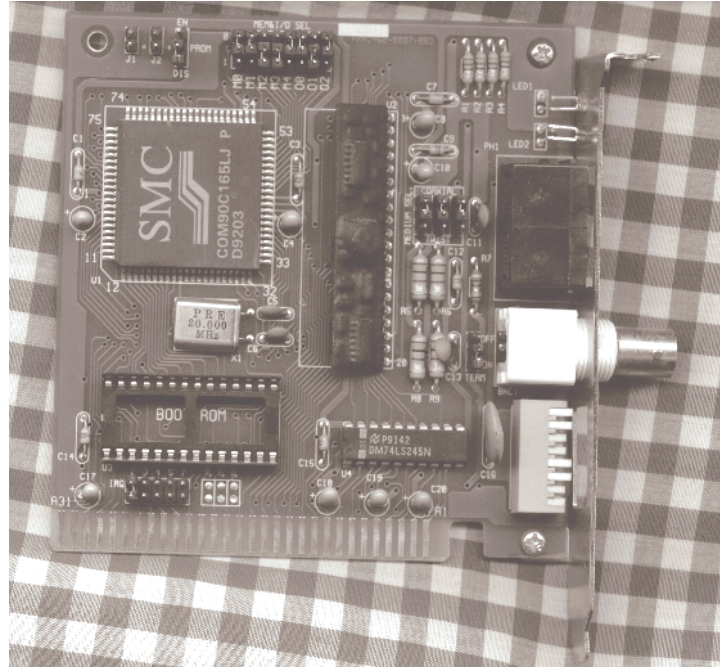


## ARCnet adapters

Largely obsolete, ARCnet was for a long time the cost effective network. The adapter cards are still available and provide for cable termination or high impedance connection. This allows the card to be used without the need for passive or active hub units. The cards conformed to a hardware port of 2E0h and used IRQ2/9 with a shared memory buffer of D000-D7FFh. This last was to give major problems when installing Windows, as the setup program would attempt to initialise a non-existent 8514A VGA card and would disconnect the ARCnet adapter from the network. The card had to have a network node number selected on the card by means of a dip switch. The accidental use of duplicate node numbers would disconnect both parties from the network. All this aside the use of ARCnet was easy and the resultant network robust and impervious to interference. It is not used now because Ethernet adapters have come down to the same price and the throughput of Ethernet is four times as fast.

**Ethernet adapters**
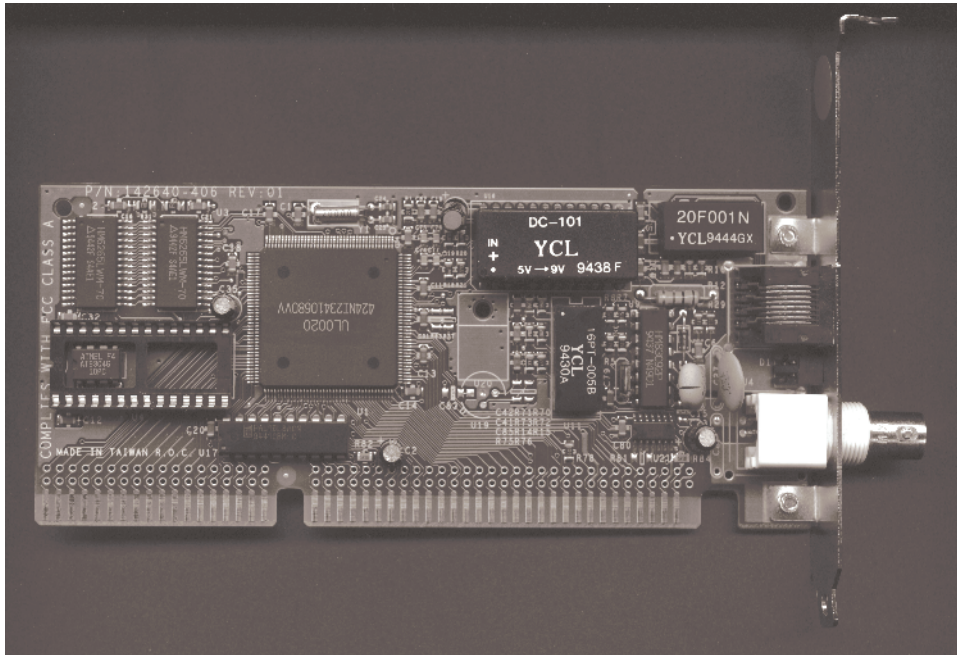


Ethernet adapters conform to a hardware specification of port address default of 300h and a default IRQ of 3. This clashes with the IRQ of Com2, the secondary serial port. Some cards have a shared memory buffer of D000-D7FF and others use what is called "Programmed I/O", using successive reads or writes of a port to transfer data. The shared memory buffer cannot be used by anything else and must be excluded from EMM386's use of the upper memory area. The throughput of these cards is about 10% better than the programmed I/O types. If they are used it would be best to move the memory address to say C800h so as to make the upper memory area one large continuous block.

# Interrupt clashes

One of the worst design features of the IBM PC has been the inadequate number of interrupts for hardware interfacing. Note that these interrupt connections may not be shared in the ISA/AT design, unlike PCI and Microchannel. This problem area is hazardous to your social life! An interrupt conflict is probably the first thing you should consider when installing a network adapter card.

| Interrupt level | Usage |
|---|---|
| NMI | Motherboard RAM parity and I/O channel check. |
| IRQ0 | System timer output channel 0. |
| IRQ1 | Keyboard scan code interrupt. |
| IRQ2 | Cascade to IRQ9. |
| IRQ3 | Asynchronous communication (COM2) and SDLC communications. |
| IRQ4 | Asynchronous communication (COM1) and SDLC communications. |
| IRQ5 | Parallel printer (LPT2). |
| IRQ6 | Floppy diskette drive. |
| IRQ7 | Parallel printer (LPT1). |
| IRQ8 | Real-time clock. |
| IRQ9 | Redirected IRQ2. |
| IRQ10 | Available for use. **** Suggested use for Ethernet adapter |
| IRQ11 | Available for use. |
| IRQ12 | Available for use. |
| IRQ13 | Maths Coprocessor. |
| IRQ14 | Hard disk drive controller. |
| IRQ15 | EIDE second hard disk controller |

**NOTE :** The two printer ports interrupt assignments are hardly ever used as the hardware does not interrupt reliably. The newer printers ports (ECP & EPP) do use the interrupts for bi-directional communications so don't use them for network adapters.

# Port addresses.

The second most problematical area in installing a network card is a port address conflict, which may give rise to loss of connectivity or machine rebooting. With the AT design more port addresses were decoded but unfortunately not all cards have been updated to the newer decoding methods.

A good example of this problem is the following :-

**Q**     When I print on my local printer the connection to the network goes dead and I have to reboot to reconnect.

**A**     The printer port address was 378h and the Ethernet adapter card was at port address 360h. The Ethernet card uses 32 addresses from 360h to 37Fh and so printing would output to the card as well as the printer.

## AT & ISA I/O Address Map

| Address range in Hexadecimal | Usage |
|---|---|
| 3F8-3FF | **Asynchronous Communications (Com1)** |
| 3F0-3F7 | **Diskette controller** |
| 3E0-3E7 | Reserved |
| 3D0-3DF | **Colour Graphic display adapter. (CGA)** |
| 3C0-3CF | **Enhanced Graphics Adapter** |
| 3B0-3BF | **IBM Monochrome Display adapter.** |
| 390-3AF | Reserved |
| 380-38F | SDLC Communications adapter |
| 378-37F | **Parallel Printer port 1** |
| 350-377 | not used |
| 330-34F | Typically SCSI controller adapter cards |
| 320-32F | not used |
| 300-31F | Prototype Card (USER I/O) or **Ethernet adapter card**. |
| 2F8-2FF | **Asynchronous, Communications (Com2)** |
| 2F0-2F7 | Reserved |
| 278-27F | **Parallel printer port 2** |
| 220-24F | Reserved |
| 210-217 | Reserved |
| 20C-20D | Reserved |
| 200-207 | **Game Control/Joystick port** & Tape streamer hardware. |
| 1F0-1F8 | **Hard disk controller.** |
| 0F0-0FF | **Math coprocessor I/O** |
| 0C0-0DF | **DMA Controller no 2  8237** |
| 0A0-0BF | **Interrupt controller 8259 Slave** |
| 080-09F | **DMA Page Registers** |
| 060-06F | **8042 Keyboard controller** |
| 040-05F | **Timer 8254** |
| 020-03F | **Interrupt controller 8259 Master** |
| 000-00F | **DMA Controller 8237** |

# Uninterruptable power supply (UPS)

Definition: A battery-backup system that provides continuous power in the event of power failure or fluctuation.

The mains power can fail for a variety of reasons, lightning, an earth leakage current tripping the breaker, temporary overload of fuse or breaker, and so on.

To keep computers running in the event of a power failure, various types of UPS can be used. Most are battery supplied inverter types and have sine wave output at 220 Volts 50 Hertz (Cycles per Second). To cover large power requirements (above 1.5kVA), primary battery and secondary diesel generator sets are used for such needs as a computer room or even a building.

Poorly designed UPS's have used car batteries, which are not designed to be trickle charged and don't last, or give square wave output voltage, which stresses the power supplies in the pc's. UPS's have been known to cause transient over voltage, which can cause sudden inexplicable equipment failure.

Modern designs of UPS incorporate software to monitor the mains voltage status, the battery voltage and can predict time to battery failure. The total up-time of the battery for the low power units is typically 15 minutes and depends mostly on loading. Lighter loads with lower power will last longer on battery power.


**Problem areas**

The file server with UPS backup may very well continue to operate during mains power failure. However workstations may very well fail with files open, transactions incomplete and all manner of software entanglements. Recovering from this situation is not simple.

# Protocols

A protocol is a standardised set of rules that specifies the format, timing, sequencing, and/or error checking for data transmission.

## The CSMA/CD Protocol

CSMA/CD governs all network access to the transmission media. Using this method, the network interface card (NIC) in each workstation listens for the presence of another station's transmitted signal. If the network is active (another node is transmitting), the station waits and continues to listen. If the network appears inactive, the station transmits but also continues to listen during transmission for the presence of any other signals. Should a station attempt to transmit while another transmission is already in progress a collision will result.

Propagation timing for Ethernet and IEEE 802.3 is based upon the assumption that two workstations at the opposite ends of a bus cable must be able to hear each other's signal in order to defer within a reasonable time. All transmission media have inherent and constant propagation delays, but the length of delay varies from one cable type to another.

## TCP/IP

TCP/IP is a set of protocols developed to allow co-operating computers to share resources across a network. It was developed by a community of researchers centred around the ARPAnet. Certainly the ARPAnet is the best-known TCP/IP network. However as of June, 87, at least 130 different vendors had products that support TCP/IP, and thousands of networks of all kinds use it.

The most accurate name for the set of protocols we are describing is the "Internet protocol suite". TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family.

# Network Interface Card driver software

## Novell drivers

Novell has over the years established its own standards for network interface adapter cards. These hardware specs usually start with NE eg: NE2000. These TSR programs interface the card to the various network redirection software supplied with the network operating system. The older IPX drivers are no longer recommended for use and have had no support from Novell for some time. The newer ODI drivers fit in with the newer VLM's (Virtual Load Modules).

## NDIS drivers

The Network Driver Interface Specification has been developed by Microsoft and Artisoft over the years in a similar manner to Novell's IPX/ODI drivers. These drivers usually have the extension .DOS for the real-mode interface drivers. NDIS has reached version 3 with these being 32 bit drivers for use by Windows for Workgroups and Windows 95.

## Packet Drivers

This specification was originally written in 1986 to enable FTP Software's PC/TCP to coexist with a proprietary LAN system.  It was enhanced and then released to the general public.  Volunteers write drivers for various cards and contribute the drivers to users through Clarkson University and FTP Software.

The "Clarkson collection", which consists of drivers and documentation, is available from several sources.  It includes a variety of standard Ethernet drivers (e.g., for 3Com, Novell, InterLan, Tiara, and Western Digital).  It also includes more exotic packet drivers: one for serial-line internet protocol (SLIP) and two piggybacking drivers that send IP packets by way of IPX and NetBIOS, respectively.

## Why 32-Bit drivers are better

Because Windows was designed for the 80286 and only 'patched' to Version 3, Windows suffers a lot of the restrictions of the obsolete 80286. Hardware interrupts, graphic device storage, and system resources all must 'live' in the bottom 1MB. A 1MB that is now full of network card drivers and other programs.

Windows for Workgroups brought with it a new set of hardware drivers and interrupt handlers that because they were written for the 80386, could use extended memory. This meant two things happened, the first is that the drivers performed faster and that the driver could release the bottom 1MB memory back to other programs including Windows.

## Workstation shells - Network Redirectors

The attachment to large remote hard disks requires that the operating system (DOS) should "see" these disks as attached drives in the operating system. A network redirector, which is a small program inserted between the application software and the network software, makes DOS use the remote disks as if they were local hard disks. Novell uses a workstation shell program called NETx.exe to provide access to the remote drives. Since DOS can support up to twenty six drive letters, (A: to Z:) most networks use the end of the alphabet as drive letters.

## DOS Configuration - CONFIG.SYS

DOS also needs to be configured for use with the network. CONFIG.SYS may need to adjusted for best use of "Upper memory blocks" to allow the loading high of network driver programs. If you are using PCMCIA adapters or Ethernet adapters with shared memory buffers, remember to exclude this memory in loading EMM386.exe.

```
eg:    device=c:\dos\emm386.exe NOEMS X=D000-D7FF
```

## Number of Files in use

If you are running an accounting package such as Pastel or a Database program you may need to increase the number of files that can be opened at any one time. In CONFIG.SYS the line that says "FILES=nn" may need to be increased.

```
eg: FILES = 80
```

When you do so remember to add a similar setting in NET.CFG.

```
eg: FILE HANDLES = 80
```

## The Lastdrive statement

With older versions of NETX the Lastdrive statement, if used should have the last DOS drive letter in it. With newer NETX versions using VLM's, it is necessary to use Lastdrive=Z. This is because the VLM driver is now set up as 'proper' DOS device driver called NETWORK. This is also applicable to Windows for Workgroups as well.

## Startnet.bat

This is the usual batch file that loads and runs the required drivers for the network on the pc. It will load the 'Link Session Layer' then the network card driver, a protocol driver and then the VLM program. All are configurable by adjusting lines in the NET.CFG text file which is usually in the same directory. The directory usually gets created by the Netware Client install program and is commonly called NWCLIENT.

## An example STARTNET.BAT

```
SET NWLANGUAGE=ENGLISH           sets the Netware language
LH C:\NET\LSL                     Loads the Link Session Layer
:DRIVER1
LH C:\NET\NE2000.COM              Loads  the  driver  for  the  NE2000
card
LH C:\NET\IPXODI                  Loads the IPX ODI driver
LH C:\NET\VLM /V4                 Loads   the   Virtual   Loadable
Modules
```

### Novell driver configuration - NET.CFG (was Shell.cfg)

The NET.CFG configures the Link Session Layer, the hardware card driver, the protocol driver and the NetWare shell (VLM.exe was NETx.COM). NET.CFG contains configuration values that are read and interpreted when the workstation attaches to the network. These values adjust the operating parameters of the NetWare drivers. The user can change the shell parameters contained in this file using any text editor such as the Windows accessory Notepad.

### An example NET.CFG

```
Link Driver NE2000
   Frame Ethernet_802.3
   Frame Ethernet_II
   Frame Ethernet_802.2
   Frame Ethernet_SNAP
      INT 10
      PORT 300
      FRAME Ethernet_802.3

NetWare DOS Requester
      FIRST NETWORK DRIVE = J
      NETWARE PROTOCOL = NDS BIND
```

The network card is a NE2000 'clone'. The protocols loaded are 802.3, Ethernet II, 802.2 and Ethernet snap. The INT refers to the interrupt setting of the card. The PORT the port address used. The final line in the first section specifies the default protocol as 802.3.

The first available network drive in this case is J: as the pc in question has C to F hard drives installed.

### Novell 32-Bit Client for DOS & Windows 3.x

Most networking people have heard about the 32-Bit Novell client for Windows 95. Not so many have heard about the 32-Bit Novell client for Windows 3.x. This client provides both DOS and Windows 3.x support for common network cards as well as a Windows Login program. The Netware User Tools supplied allows the user to do in Windows everything that he would have done in DOS. Mapping drives and connecting printers to queues.

# Network Operating Systems

## Lantastic and Novell Lite

Lantastic was developed some years ago using NetBIOS type operation by Artisoft. It originally used 2 Megabits per second adapter cards, but later a form of ethernet adapter card. It is a peer to peer network allowing sharing of hard disks and printers.

Novell lite and Personal Netware were a recent addition to the software supplied by Novell and are peer to peer network systems. It uses standard network adapter cards for interconnection of pc's. It is no longer supplied or supported by Novell.

## 10 Net and others

10 Net, 3Com, Lansoft and others have all produced peer to peer networks in great profusion. All are competing for the low end of the market which encompasses the ordinary office or "Workgroup" allowing sharing of data/files and resources.

## Lan Manager 2.0 (Obsolete)

Lan Manager was a centralised file server system operating on a 386 or better and provided hard disk and printing support services. It operated under OS/2 version 1.2.

LAN MAN 2 took advantage of the power of Intel 386 and 486 based servers, using a 32 bit version of the OS/2 1.2 High Performance File System and a 386 optimised network I/0 subsystem.

- Support for multiple processors.
- Centralised administration for multiple servers.
- Subdivision of administrative tasks.
- Peer services.
- Improved security system.
- Automatic replication of files across servers
- Fault tolerance
- Support for uninterruptible power supplies.
- Remote initial program loading (remote boot)

By implementing a powerful and robust server architecture, LAN Manager provides a high performance network server. This design of LAN Manager eliminated all performance bottlenecks, from the network to the file system to the disk system. This extremely efficient system gave the server more power to run server based applications for client-server computing.

On an Intel 80286 based server LAN Manager used multiple processes and threads for parallel processing of simultaneous networking requests, while for faster file access LAN Manager used the OS/2 High Performance File System.

If you had an Intel 80386 or 80486 based server, LAN Manager automatically installs a 386 optimised network I/0 subsystem and a 386 specific High Performance File System (HPFS-386). The combination of network I/0 subsystem and HPFS-386 with OS/2 gave LAN Manager the ideal architecture for networking: high performance file and print services and a protected mode pre-emptively scheduled platform for running powerful client-server applications.

For the highest level of performance on a 80386 and 80486 based server, LAN Manager could be implemented on two processors. This made more computing power available for network file service, distributed processing and non-dedicated server operation.

## Lan Server

Lan Server is the successor product to Lan Manager from IBM and is identical in operation. It operates under OS/2 Version 2.1.

## Windows for Workgroups 3.xx

Windows for Workgroups is a peer to peer network running on 386 or better personal computers. It provides shared access to hard disk drives and printers to other users on the network. The network is internal to the Windows operating system and runs as a pre-emptive multitasking system. Its application to small groups of personal computers is ideal and provides all the other facilities of a large network at a low cost. Electronic mail is standard as well as group diary and appointment storage. The network can be based on Ethernet or Token ring and must be run on a 386 or better CPU based pc to allow shared access. Other pc's can be connected using a "DOS Attachment" and can have access to the shared resources.

## Windows NT and Advanced Server

Advanced server is the new Microsoft product replacing Lan Manager. It provides high data security and software support for RAID hardware. It runs under Windows NT 3.1 to 3.5

## Novell 286 Netware Version 2.2 (Obsolete)

The Novell 286 Netware has grown out of the previous 286 operating system software and has many of the features that were added to Netware 2.15 to make it "System Fault Tolerant". It requires an 80286 processor as a dedicated or non dedicated file server. Non dedicated means that the file server can also run DOS programs as well as providing the central resources for the network. It provides an enhanced DOS compatible system, which is fully compatible with DOS, to provide access to large capacity hard disks and network printing services.

## Novell 386 Netware Version 3.xx

Netware 386 is a fully multitasking network operating system, which runs on a 386 or better processor. It provides both dedicated and non dedicated file server operation with all the features of previous versions of Novell. It provides enhanced operation by the use of "Netware Loadable Modules", which are re-entrant service modules for the operating system. NLM's can be used for network services, database servers and tape backup services.

## Netware 4.x

NetWare 4.0 has no bindery files! You login to a service, Yes, NetWare 4.0 has departed from the traditional understanding of having to login to a specific fileserver. Network managers must now start thinking of the network, its entire structure, fileservers, printers gateways, etc as an "entity" or "service" which users can access as allocated by network supervisor. For the purist - directory services.

So how do you know what is where and which "server" contains your data? You don't. You don't need to either.

Imagine yourself as a user, sitting in front of a PC workstation (of any description!) and you have a login name. That's all! Type your login name, which by the way uses conventions very similar to X.500 nomenclature.

NetWare 4.0 will automatically determine which services you are allowed to access (set up by the administrator) no matter where these services are located. This can be access to a database somewhere on the local area network, or even over a wide area link, or printers, gateways etc.

NetWare 4.0 will update the directory services database at timed intervals, the system supervisors can set these intervals, to every 10 Seconds or every 24 hours if they so wish, ensuring control of traffic across wide area links.

NetWare 4.0 has been totally re-written. The kernel is totally different from NetWare 3.x and according to reliable information this kernel will operate at up to 50% faster than the 3.x kernel. Don't think this means the LAN is 50% faster! It certainly isn't faster than a 3.xx server.

Devices can be named using the X.500 hierarchical directory structure, so users actually attach to a "named" device, not the old print queue LPT1.

Security was a hotly debated issue. What about passwords being de-bugged by sophisticated hackers? Sounds almost foolish, but it is possible, if you're a rocket scientist and have equipment to trap a user's login password on the network you can determine that user's password, and thereby hack into his system.

NetWare 4.0 is going to frustrate all the would be hackers! No longer does the "password" travel along the wire when you type your user name.

NetWare 4.0 keeps your encrypted password in a centralised database and every time you login, login.exe asks for your encrypted password from the server. NetWare 4.0 encrypts this AGAIN, sends it across the LAN to your workstation where it is decrypted by the public key, then decrypted by the private user key. Only then is your password validated.

Another very powerful feature NetWare 4.0 will have is vastly improved servicing of queued tasks.

There are 3 classes of queues. The first class is for those type of applications that need to run whenever possible, on a round robin type basis. (This is over and above interrupt driven tasks.) This class of queue gets priority treatment.

If there is nothing in this queue, NetWare 4.0 looks at the second class queue i.e. those type of tasks that are waiting for something to happen, i.e. disk read. In NetWare 3.x a disk read would take place when requested, terminate, and reactivate as other tasks received priority. NetWare 4.0 will now COMPLETE the task before returning the ball to the CPU.

The third class queue is a low priority queue for those tasks which seldom require attention, such as backup. You can prioritise your tasks accordingly, so backup would probably occur only when utilisation on the machine is very low. The third class priority task will therefore only work if the machine has nothing better to do.

Finally, NetWare 4.0 has much better memory protection. The 3 ring concept is employed in NetWare 4.0 where control of poorly behaved NLM's can be achieved in ring 2. Total protection is available in ring 2 giving developers a chance to make sure their NLM is bug free before adding to ring 1 or ring 0.

Once an NLM is well tuned it can be, added to ring 0, which is totally unprotected, knowing that it will not crash your system.

In summary, NetWare 4.0 is a radical departure from the confines of NetWare 3.x or 2.x. MIS managers will now define "objects" in their internet and assign users rights to directory services as and when required. Users need not know where their data resides even if it is across a wide area link. They will simply login and see what they need.

## EMM386.EXE and Upper Memory

Upper memory is the region of your 80386 or 80486 computer's memory that is used by the machine system. The IBM PC designers must have said "we'll give the user ten times what he is used to, and use the rest for adapters and video". As a result the area above 640k is not normally available for use by DOS and is allocated to video and other adapters.

The parts of upper memory that are not used are called "upper memory blocks" (UMB). With MS-DOS 5 and up, you can use UMBs for running device drivers and other memory-resident programs. This makes more conventional memory available for running programs. The MS-DOS upper memory manager is EMM386.EXE. You need to use MS-DOS 4.x or higher for EMM386.EXE to access upper memory.

| High Memory Area (HMA) | |
|---|---|
| Rom BIOS memory | 1024k |
| Upper memory blocks | Upper memory area |
| Video memory area | 640k |
| Program memory area | |
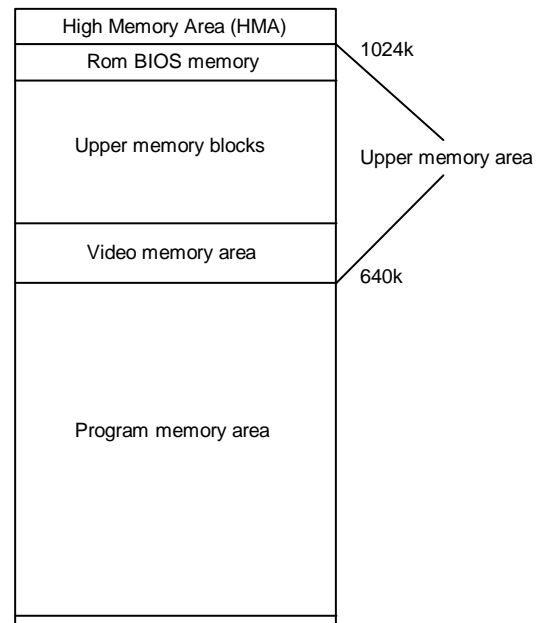
**NOTE:** EMM386 is not DOS version dependent and the latest (DOS 6.22) can be run on a machine with DOS 5.0.

**NOTE:** Some programs cannot be moved to upper memory. These include HIMEM.SYS, EMM386.EXE, and MS-DOS system data.

Programs such as DOSKEY, SHARE, FASTOPEN, RAMDRIVE.SYS, console and other device drivers are good choices for loading into upper memory. You can also load your TSRs into high memory if your MS-DOS version supports it. This includes network programs such as IPX, NETX, LSL, IPXODI and hardware driver programs.

**Note:** The only way to find out if a program can run in upper memory is to try it. Some programs do not run properly in upper memory. If the program does not execute correctly, or if the system locks up, run it in conventional memory.

To run device driver programs in upper memory, you must include the following commands in your CONFIG.SYS file for loading HIMEM.SYS and EMM386.EXE:

DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE NOEMS

The DEVICE command for EMM386.EXE installs EMM386.EXE as an upper memory manager. The NOEMS option tells MS-DOS to run EMM386.EXE to manage upper memory only. Since NOEMS prevents EMM386.EXE from emulating expanded memory, use NOEMS only if your programs do not require expanded memory.

The NOEMS option for EMM386.EXE is the most efficient setting for the Windows operating system.

If you want to use EMM386.EXE both for the upper memory area manager and to emulate expanded memory, use this command:

DEVICE=C:\DOS\EMM386.EXE   RAM

Note: The Microsoft Windows operating system will be unable to allocate expanded memory to programs that need it if you specify the NOEMS option when installing EMM386.EXE. If you use such programs, use the RAM option (or no options) instead.

Ensure that HIMEM.SYS is loaded first by putting the DEVICE command for HIMEM.SYS before the DEVICE command for EMM386.EXE. EMM386 cannot run without the high memory manager in place. Also the DEVICE commands for HIMEM.SYS and EMM386.EXE must appear before any other DEVICE commands.

If MS-DOS runs in upper memory, your CONFIG.SYS file will have DOS=HIGH,UMB instead of DOS=UMB.

**DOS 5 TIP:** To get more upper memory area for use with network driver programs, use the include option to tell EMM386 to use the expanded memory frame area of E000 to EFFF. eg: DEVICE=C:\DOS\EMM386.EXE NOEMS **I=E000-EFFF**. This will add another 64k to the upper memory pool. MS DOS 6.x users can ignore this as their EMM386 will use this memory if it is available.

**NOTE:** This does not work on all machines.

For more complete information on using EMM386, see the EMM386 reference at the end of this set of notes.

## Using MEM to check upper memory

To load programs into upper memory, check your memory layout by executing the MEM /c command. At the end of the output from the MEM /c command, note the size in the line Largest available upper memory block. Then look in the "Conventional Memory" section of the output and find the largest device driver or program that will fit into that upper memory block (UMB). Change the command in the CONFIG.SYS file for that device driver from DEVICE to DEVICEHIGH. For memory-resident programs, change the command in the AUTOEXEC.BAT file LOADHIGH (LH for brevity). Do this for one program at a time. You must restart your system each time.

**Example MEM output using the /c option:**

```
Modules using memory below 1 MB:

  Name         Total        =  Conventional   +  Upper Memory
  --------  ----------------   ----------------   ----------------
  MSDOS      17,293   (17K)     17,293   (17K)          0    (0K)
  SETVER        800    (1K)        800    (1K)          0    (0K)
  HIMEM       1,168    (1K)      1,168    (1K)          0    (0K)
  EMM386      3,120    (3K)      3,120    (3K)          0    (0K)
  SMARTDRV   31,520   (31K)      2,496    (2K)     29,024   (28K)
  PROTMAN       128    (0K)        128    (0K)          0    (0K)
  COMMAND     4,720    (5K)      4,720    (5K)          0    (0K)
  win386     40,016   (39K)      9,744   (10K)     30,272   (30K)
  WIN         1,568    (2K)      1,568    (2K)          0    (0K)
  COMMAND     6,944    (7K)      6,944    (7K)          0    (0K)
  USPI14      8,704    (9K)          0    (0K)      8,704    (9K)
  MOUSE      17,056   (17K)          0    (0K)     17,056   (17K)
  DBLSPACE   39,472   (39K)          0    (0K)     39,472   (39K)
  NE2000      9,184    (9K)          0    (0K)      9,184    (9K)
  WORKGRP     4,400    (4K)          0    (0K)      4,400    (4K)
  DOSKEY      4,144    (4K)          0    (0K)      4,144    (4K)
  Free      607,264  (593K)    607,264  (593K)          0    (0K)

Memory Summary:

  Type of Memory      Total   =    Used    +    Free
  ---------------   ----------   ----------   ----------
  Conventional         655,360       48,096      607,264
  Upper                142,256      142,256            0
  Reserved             393,216      393,216            0
  Extended (XMS)    15,586,384   14,537,808    1,048,576
  ---------------   ----------   ----------   ----------
  Total memory      16,777,216   15,121,376    1,655,840

  Total under 1 MB     797,616      190,352      607,264

  Largest executable program size       607,248   (593K)
  Largest free upper memory block             0     (0K)
  MS-DOS is resident in the high memory area.
```

## [DOS 5.0]

If you get an error with one of the programs you have loaded into upper memory, or the program or device driver is still running in conventional memory after you restart your system, it may be that the largest UMB is not large enough. Some programs require more memory when they are loaded than when they are running. Try using the SIZE= option with the DEVICEHIGH command. Modify the DEVICEHIGH command in your CONFIG.SYS file to specify the hexadecimal size of the driver from the Size in Hex column of the MEM output, and restart your computer. For example, if the information in the Size in Hex column from the MEM command output for MOUSE.SYS is 39E0, you would put this statement in your CONFIG.SYS:

DEVICEHIGH **SIZE=39E0** C:\WIN3\MOUSE.SYS

The SIZE= option takes effect only if needed. If using the SIZE= option doesn't allow your program to run, or if your system locks up during startup or when running the program, it is likely that the program cannot run in upper memory. Change the DEVICEHIGH command to DEVICE and remove LOADHIGH commands one at a time until the program works correctly.

Some hardware programs might attempt to use upper memory after EMM386.EXE has determined this memory is available for running device drivers and programs. To avoid this, you can use the x= option when you load EMM386.EXE. This option prevents EMM386.EXE from allocating a specified range of upper memory for its use. For example, to prevent EMM386.EXE from using the addresses D000h through D800h (An ARCnet adapter card's memory buffer), you can include the following command in your CONFIG.SYS file:

DEVICE=C:\DOS\EMM386.EXE NOEMS **X=D000-D800**

## [DOS 6.x]

With DOS 6 a new program called MEMMAKER arrived promising to automate the procedure of setting up UMB's and memory management. It isn't perfect and you can usually do better yourself.

## Fault Finding

If you think your computer is set up correctly to run device drivers and programs in upper memory, but nothing appears there when you use the MEM /c command, check the following:

1. [DOS 5.0] Make sure you are not running the Windows operating system version 3.x in 386-Enhanced mode when you execute the MEM command. The MEM command does not report the contents of upper memory when you are running the Windows operating system.

2. Your CONFIG.SYS file must contain the DOS=UMB or DOS=HIGH,UMB command.

3. The DEVICE command for EMM386.EXE in your CONFIG.SYS file must contain the NOEMS or RAM option. RAM is the default.

4. Your CONFIG.SYS file must contain a DEVICEHIGH command, or your AUTOEXEC.BAT file must contain the LOADHIGH command for each program you want to run in upper memory.

5. The DEVICE command for HIMEM.SYS must appear before the DEVICE command for EMM386.EXE; the DEVICE command for EMM386.EXE must appear before any DEVICEHIGH command in your CONFIG.SYS file.

Once programs are working successfully in upper memory, you can experiment to find the most efficient way to use available memory.

In general, load device drivers and programs in order of size, from largest to smallest. Do this because MS-DOS uses the largest remaining UMB, even if that program would fit into a smaller UMB. The optimal loading order depends on the sizes of programs you are loading and the sizes of available UMB.

## Network adapters and PCMCIA adapters

Unfortunately all is not perfect here either. ARCnet adapters, certain Ethernet adapters and the "yuppie" adapter, PCMCIA cards, all use some of your upper memory area.

ARCnet adapters use a shared memory buffer fixed at D000h to D7FFh (32k bytes) for interchange of data between cpu and the network cable. This memory area must be excluded from EMM386's upper memory arena. Use X=D000-D7FF after NOEMS to exclude this memory.

Ethernet adapters usually are designed to work as "programmed I/O" devices, using port addresses to interchange data between cpu and cable. Some slight performance increase can be achieved by the use of a shared memory buffer. This generally ends up at D000h but may be configurable to another address. It would be a good idea to move it down to CC00h, next to the rom bios attachment on the vga card. This keeps your upper memory in one medium sized block with a better chance of fitting those TSR's there. Again this memory area must be excluded from EMM386's upper memory arena. Use X=D000-D7FF after noems to exclude this memory.

PCMCIA adapters are not moveable and "live" at D000h to D7FFh, and this must be excluded from EMM386's upper memory arena.


## Config.sys (DOS configuration file)

Dos also needs to be configured for use with the network. Config.sys may need to adjusted for best use of "Upper memory blocks" to allow the loading high of network driver programs. If you are using PCMCIA adapters or Ethernet adapters with shared memory buffers, remember to exclude this memory in loading EMM386.exe.

**eg:**
> **device=c:\dos\emm386.exe noems X=D000-D7FF**


## The Lastdrive statement

With older versions of netx the lastdrive statement, if used should have the last DOS drive letter in it. With newer netx versions using VLM's, it is necessary to use Lastdrive=Z. This is because the VLM driver is now set up as 'proper' DOS device driver called NETWORK. This is also applicable to Windows for Workgroups as well.


## Workstation network configuration files. NET.CFG (was Shell.cfg)

The NET.CFG configures the Link Session Layer, the hardware card driver, the protocol driver and the NetWare shell (VLM.exe was NETx.COM). NET.CFG contains configuration values that are read and interpreted when the workstation attaches to the network. These values adjust the operating parameters of the NetWare drivers. The user can change the shell parameters contained in this file using any text editor.


## Network Redirector configuration file - PROTOCOL.INI

Protocol.ini configures the real mode NDIS drivers and the enhanced mode drivers. It adjusts the session operation parameters as well as sets the interrupt and port address values. It has the same structure as the Windows INI files with sections and parameter equalling a value. It can be edited using a normal text editor, though it is usually modified by the Windows network setup program.

# Setting up Windows 3.x for Networking.

Most companies have bought Windows for Workgroups 3.11 over the last couple of years. Some had Windows 3.1 already installed and some misguidedly bought Windows 3.11, because it was slightly cheaper. Windows had from version 3.0 networking support built in. The required interfaces and drivers were supplied with the installation disks. However with the threatened legal action by Novell against Microsoft for including the Novell drivers in Windows for Workgroups, had Microsoft removing the required drivers. It was then left to Novell to supply the drivers. Most users ignored this and left the situation as it was, badly adjusted. The newer VLM drivers use extended memory to hold large amounts of data, releasing conventional memory for programs and more importantly Windows resources. Windows resources has to be the most troublesome aspect of the Window 3.xx series.

Windows resources are storage elements that Windows uses to keep temporary data, data pointers, stacks and tables. Because of the 80286 design of Windows must reside in the bottom 1MB of the machine's memory. This inadequate amount of storage gives rise to the erroneous message "Insufficient memory to run application. Close some Windows and try again". This can even appear on a 32MB memory laden machine.

Most older and conventional network card drivers are for real-mode operation using DOS. Their application to Windows was a stopgap measure. The hardware drivers and protocol stacks that Windows 3.xx needs are 32 bit enhanced mode type drivers. Such drivers are NDIS 3 types for TCP/IP 32bit operation and the IPXODI NDIS (shim) driver that works with the VLM Novell drivers.

With the emphasis on Intranet/Internet working today with TCP/IP, it has become simpler. To reduce the amount of conventional memory used, use only 32bit TCP/IP drivers with Windows for Workgroups and remove the Novell drivers. Convert the Novell Server to TCP/IP operation if necessary.

## All those INI files. All those CFG files.

Windows uses initialisation files for just about every program. These usually are .INI files which are text with sections marked by the square brackets []. Each configuration value is given a name and assigned a value by a line such as "TimerCriticalSection = 10000". Editing them is straightforward. Use a plain editor such as Dos' EDIT or Notepad. The really important ones can easily be edited at the same time by SYSEDIT, which is an undocumented program residing in the Windows' system directory.

## The impact of Windows on Networking

Text based operating required few bytes to be transferred over the network cable. Thus the traffic was light and even ARCnet could cope. Windows 3.0 started the ball rolling with its ability to run DOS programs at the same time as the few available Windows programs. The Windows machines of the time were 386's with typically only 4MB of memory. Quite a few of these pc's were without hard disks, which gave rise to the first major disaster. Where do you put the swap file? On the server? A 4 to 8MB temporary swapfile had to be initialised by the server. With Novell 3.xx this meant that the server had to 'zero' out the file by filling it with zero bytes. This made the server work hard to cope with all this. The multiple swap file data, chunks of megabytes, had to be transferred over the network. This meant that the average traffic went sky high. Little wonder that hard disks were bought in great numbers.

Printing has also changed as a result of Windows' graphic operation. Our average a few years back was only a few thousand bytes per document. With scaleable fonts, inserted pictures and colour, our documents are now megabytes in size. All of which has to be transferred to the print server.

# Electronic mail and methods.

The majority of E-mail systems implement a "store-and-forward" delivery scheme. Similar to the way a print queue stores individual bytes of a print job in a file before printing the entire file as a logical unit, store-and-forward engines queue groups of messages until a connection with another system is scheduled or the number of queued messages reaches a certain threshold.

Some of these store-and-forward Email systems use a proprietary addressing method, so they expect to talk to themselves on the other end. Because each of these systems handles message exchange and addressing differently, connections to proprietary E-mail systems require a translation mechanism known as an E-mail gateway, an add-on product that provides a communications link to a unique E-mail system.

Developing E-mail gateways is complex; thus, proprietary E-mail systems often have limited connectivity options. More importantly, each gateway typically costs hundreds or thousands of dollars. In addition to the cost of the gateway software itself, a dedicated personal computer is often required to run the gateway software.

## Ms Mail

Microsoft has produced a solid and reliable product in MS MAIL 3.x with both DOS and Windows programs provided.

Version 3.0 included many new capabilities users had been hoping for, among them personal address books and group lists, multiple file attachments and features to help managers keep close track of mail messages. According to a company spokeswoman, Mail 3.0 was designed to provide functionality rather than performance, which was emphasised in version 2.0 and subsequently criticised by users. Other key features to aid the organisation of management of messages include custom message folders, which utilise a graphical user interface to drag and drop messages in the appropriate folders; an appended save feature, which aids message archiving; and a dial-up utility, which allows remote access. It is this version that was integrated into Windows for Workgroups. The current version is 3.2.

MSMail has recently changed again into Exchange/Windows Messaging and is bundled with Windows 95 and NT. Exchange can also use a POP3 unix style post office, so if you have a unix machine on the network, you could use that as your eMail store.

## MHS

Many organisations have adopted the Message Handling Service (MHS) developed by Action Technologies Inc. and Novell as their store-and-forward engine to avoid the need for proprietary gateways to other PC LAN software. MHS gives E-mail vendors a set of specifications for preparing messages and the protocols required for proper delivery to the recipient regardless of the target mail system. MHS will work with any E-mail package on a discrete LAN or stand-alone personal computer as long as it supports the MHS protocols. The use of MHS as a messaging backbone lets many diverse applications, such as word processing, groupware, and E-mail, coexist and cooperate. MHS is now supplied as part of the package with Netware 3.12.

## Windows for Workgroups Remote Access

Remote access has been included as part of Windows for Workgroups for some time. But RAS has not been able to accept incoming calls from a remote notebook or another network. With the RAS upgrade you can accept incoming calls or hook two networks together using asynchronous modems, X25 or ISDN. This allows access to the workstation and its resources. It also allows a remote user to send and receive his email and to use his diary.

To gain full access to the network, the machine should be running Windows NT. NT provides a higher level of security with this service.

If you want the Windows 95 version of RAS, you will need to purchase the Plus! Pack for 95. The Windows 95 server for RAS is only supplied with the Plus pack.

## Modems

Possibly the most common type of modem available today is the "Hayes" compatible modem. This comes from an "intelligent" modem designed by Hayes of the USA called the Hayes Smartmodem. This modem made use of a microprocessor to provide a command orientated operation from the host machine. It can dial a number, answer a call, negotiate the speed of the link and go on-line or off-line. Its operational commands are preceded by the letters "AT" for **AT**tention, and terminated by a carriage return.

Later models incorporated error correction into the design (Microcom Network Protocol MNP) and on the fly data compression to further increase throughput of data. Data rates on normal telephone lines can now achieve in excess of 33600 bits per Second. The X2 and 56k modems can achieve higher rates, the modems communicate at 56000bps in the 'down' direction and 33600bps in the 'up' direction.

---

## Printer port capturing.

---

### "Capture" & "EndCap"

Novell's Capture is a "Terminate and stay resident" program that redirects the printing stream to the print queue on the file server. This allows centralised printing to take place on a printer connected directly to the server or a remote printer connected to a workstation.

Endcap is a small program to disconnect the Capture program and to restore printing to a local printer.

### Print Queues and spoolers. "Pconsole" & "Pstat"

Pconsole and Pstat allow both supervisors and users to monitor the progress of a "print job" on a printer connected to the server or a remote printer connected to a workstation.

### Print managers.

A print manager (usually used with Windows) is an application that handles documents that have been sent to a printer. When printing, Print Manager works in the background, sending documents to the printer while you perform other tasks. It can also be used to control print jobs and adjust the order in which they print or to delete a job from the queue.

### Printer Assist.

Printer Assist is a remote printer utility that allows a workstation's printer to act as a shared printer. It uses IPX for communication on the network and thus the user at that workstation does not have to be logged in to the server.

### Print Servers

Print servers are used by Novell to print remotely print jobs that would be printed on a local printer. The Print server can be installed on the file server or remotely using RPRINTER. Print servers can accommodate many printers all connected to the file server but usually the hardware allows only three Centronics/Parallel printers and two RS232 connected printers.

## File server organisation

File server memory is used as caching buffers for the system. Volume labels are used to describe large areas on disk. The maximum size for a volume used to be 255 megabytes, but with NetWare 3.xx has risen to 2 Gigabytes.

### Operating system security

All information on a network is usually stored in a central location, the file server's hard disk. However, not all users should be able to access all information (such as payroll files). In addition, users should not always be able to access the same data file at the same time; otherwise, they may overwrite each other's work. To prevent problems like these, the operating system should provide an extensive security system to protect the data on the network. In Novell access can be granted on a directory level to individual users or groups of users. With Windows for Workgroups, the access can be granted to all users, with or without password protection.

Network security consists of a combination of three levels of security that together make the network safe against unauthorised access.

- **Login security**

    Login security includes creating user names and passwords and imposing station, time, and account restrictions on users. This is applicable to Novell but not Windows for Workgroups without additional supervisory software.

- **Trustee rights assigned to users and groups of users**

    Trustee rights control which directories a user can access and what the user is allowed to do with those directories, such as creating, reading, erasing, or writing to files. This is applicable to Novell. Windows for Workgroups is similar, where read-only access and full access to directories can be password limited.

- **Attributes assigned to directories and files**

    Directory and file attributes determine whether that directory or file can be deleted, copied, shared, viewed, or written to.

### Remote Server Operation - RConsole

NetWare v3.11 comes with many tools that make installing and administering your network easier. One such tool is a NetWare Loadable Module (NLM) called RCONSOLE (Remote CONSOLE). RCONSOLE gives you file server screen and keyboard access from any DOS workstation on the network, making that workstation a virtual file server console.

Since any workstation on the network-even a remote workstation can act as the file server console, RCONSOLE makes network administration more convenient. You can run NLMs and console utilities from the workstation of your choice (DOS, Windows, or OS/2 DOS Windows). You can also use RCONSOLE's remote file transfer capability to perform an upgrade or the bulk of an installation from a remote workstation. These capabilities allow you to manage networks at several different sites from a central location.

**Firewall - external access network security**

A dedicated system that sits between the internal network and the Internet. The system examines closely all network traffic and disallows transfer of any packets that would violate the security of the internal network.

---

# Back up procedures

---

Network data must be protected with a comprehensive and regular backup schedule.  When a desktop system fails, the results are unfortunate.  When a LAN fails, the results can bring down the company.  Your backup procedures should encompass data on network and local disks.

Backup procedures can be as simple as copying data to floppy disks or as comprehensive as using an off-site storage of tape cartridges.  You also need to plan for recovering and restoring data.

### Full, Incremental and Differential Backup

### Full

The Full backup backs up all selected files, regardless of whether or not they have changed since the last backup, and resets the archive bit.

### Incremental

The Incremental backup backs up all selected files that  have changed since the last full or incremental backup, and then resets the archive bit.  Use this backup type for the partial backups in your backup cycle if you work with different files each day, or if you need to save each day's version of the files you work with.

> **Note:**   You must save all incremental backup sets between full backups, since the files backed up in one incremental backup will not be included in the next unless they are changed.

### Differential

The Differential backup backs up all selected files that  have changed since the last full backup, and does not resets the archive bit.

Since the archive bit is not reset, the backed-up files will be backed up again in the next differential backup.  Use this backup type if you generally work with the same files each day.

## Tape Streamers

For backup of data at low to medium cost nothing comes close to tape backup. Tape storage has been used in the industry since the early days. Very large amounts of data can be stored on tape. Tape has a limited useful life in storage (1 to 2 years) and is susceptible to magnetic fields and temperatures.

Tape capacities vary, for example, a data cartridge such as the Teac 60, which is similar to the popular Philips-type audiocassette, holds only 60 megabytes; the 20-year-old quarter-inch 3M data cartridge can hold up to 250 megabytes; and its downsized brother the DC2080 holds 80 megabytes. Though with data compression techniques these figures can be doubled or tripled.

## Digital Audio Tape

DAT drives use helical-scan recording technology to increase storage density by creating diagonal rather than longitudinal tracks on the tape.

Most tape unit manufacturers use the Digital Data Standard (DDS) format for storing data. DDS is a de facto standard recently endorsed by the DDS Manufacturers' Group coalition.

DAT-drive heads require occasional cleaning to keep them working properly, and only data-grade cleaning cartridges should be used. Some drives are self-cleaning.

## Helical scan recording

Rather than locating a set of fixed heads in a tape path, helical scan recording uses a set of three heads mounted on a drum that rotates at 1800 rpm. The tape is then wrapped around the rotating drum in the shape of a distorted 'C' (C wrap) at an angle of about 5 degrees to the face of the drum. The recorded data is no longer a longitudinal path across the tape, but a track that extends at an angle from the bottom of the tape to the top of the tape. The recording of helical tracks, or stripes, offers several distinct technical advantages that otherwise must be overcome in conventional longitudinal recording.

The actual recording pattern on tape utilises a series of very narrow stripes (0.000098 inch) written acutely across the tape. Each stripe (3 inches approx.) represents a single rotation of the head. With the head travelling at 1800 rpm, data density increases dramatically. Each track can hold about 130 k bits, and there are 820 tracks per linear inch of tape. A 346 foot tape can store over 2 Gigabytes of data.

## Optical storage backup.

Optical disks have many advantages over traditional magnetic media for backup storage and network data management systems. An optical disk is less susceptible to environmental extremes than a magnetic disk or tape, provides better long-term data integrity and is removable for data security. Optical disks have an estimated shelf life of 10 to 50 years, compared to two years for magnetic tape. Write once read many (WORM) disks have large capacities and are designed for archival storage; erasable optical disks arrayed in 'jukeboxes' provide up to 50Gbytes of on-line storage and faster information transfer than tape drives. Optical disk systems are far more expensive than tape systems but nevertheless attract users because they provide random access. Magnetic systems nevertheless cost less per megabyte than optical media.

**Backup**
**[should be simple so that users have no excuse not to back up their data.]**

eg: using XCOPY /m. Here is a simple batch file to backup all DOC files on C:

```
Cls
Echo off
:LOOP
Rem Could be B: or a Network drive.
Echo  Put blank disk in drive A:
Rem this puts "Press a key when ready..." on screen.
Pause
Rem XCOPY supports errorlevels and can search subdirectories.
Rem You could make it a network drive instead of A:
XCOPY C:*.DOC A: /E /S /M
Rem ErrorLevel 4 is disk full
If ErrorLevel == 4 goto LOOP
Echo All done!
```

## PkZip options for making a full and incremental backup

Full backup
Use the -a+ option to create a full backup of files on your hard disk or network disk. For example:

**C:\> PkZip a:fullback -&s -a+**

This will backup the entire hard disk to a multi-disk Zip file called Fullback.zip on a set of disks in the a: drive

Incremental backup
-a+  Turn off archive attribute of added files. By using this option you can create a complete backup of your disk, while clearing the archive attributes to make the way for incremental archiving. Incremental archiving makes use of the archive attribute to take only the files which have been modified since the last backup.  In order for this process to work smoothly you must first have a complete backup and a clearing of the archive attribute for all files. For example:

**C:> pkzip f:backup.zip -a+ -rp**

## ARCserve.  Cheyenne's ARCserve  Version 3.0

ARCserve is a server-based backup system for NetWare.  ARCserve runs as a value-added process (VAP) on NetWare 2.x servers and as a NetWare Loadable Module (NLM) on NetWare 3.x servers. ARCserve provides for attended and unattended backup of DOS and Macintosh files stored on NetWare file servers, and DOS and OS/2 files on network workstations.  It does not support the OS/2 High Performance File System (HPFS).

ARCserve works with QIC, QIC-02, 8 mm helical scan, and DAT backup units. It is server-based backup software for NetWare.  ARCserve can back up a workstation's local drives.

ARCserve provides the same menu interface used by the NetWare utilities and provides a considerable amount of flexibility for selecting files for backup.  In addition, ARCserve uses the NetWare queuing functions (the same ones used for print service) to track and manage multiple unattended backup sessions.  ARCserve's scripting capability allows frequently used procedures to be saved and reused.  Scripts also allow you to define an automatic repeat interval, allowing for repetitive, timed backup.

ARCserve does have several limitations.  Because it is server-based, files cannot be restored unless the ARCserve host server is active.  In case of a server crash, files cannot be restored to

alternate locations, such as to a local drive or another file server. It also means that if the server operating system is changed from NetWare to something else, the files cannot be restored unless another NetWare server is available. (Cheyenne does have a version called ARCserve Solo that runs on a workstation, but it is only available through OEMs for a limited number of tape drives.)

Another drawback is that full administration requires access to the host file server as well as a workstation. Also, error message documentation is very limited.

ARCserve supports a wide range of tape drives and controllers. It is available from Cheyenne, its dealers and distributors, and OEMs such as Tecmar, HP, and Irwin Magnetic Systems Inc.

## Disk Mirroring, Disk arrays, LAN Shadow

As the requirement for more disk storage increases the chance of something going wrong with the hard disks increases. To cope with hard disk failures various schemes may be used such as disk mirroring and disk arrays using RAID technology. To provide the ultimate in backup, LAN shadow provides a complete "HOT STANDBY" option for a file server. Disk mirroring uses two identical hard disks which have identical data written to them. If one disk fails the other continues operation until the faulty unit can be replaced. Disk arrays are usually made up of RAID units. RAID stands for **R**edundant **A**rray of **I**nexpensive **D**isks.

## Application monitoring.

As we become more aware of software package licensing and restrictions upon multiple users, it becomes necessary to monitor and even refuse use of software to users on a network if the license allows only a certain number of users.

## FUNK SOFTWARE's AppMeter

AppMeter is a server-based software metering program that monitors usage of DOS and Windows applications, allowing the network administrator to honour network license agreements without overbuying. AppMeter logs all application usage and enables the administrator to view current and historical information organised by user, by application, or by workstation, and to view on-screen graphs of daily concurrent usage by the half-hour. The administrator can strictly limit the number of concurrent users of an application to a specified maximum, or can generate exception reports when that maximum is exceeded without denying access. AppMeter also provides virus protection by checking applications each time they run to make sure they have not been altered. AppMeter requires Novell NetWare 2.1x or above, or NetWare 386. Includes VAP and NLM. No TSR required.

The AppMeter software consists of the Enforcer, Supervisor, and Stubs. The Enforcer is an NLM for NetWare 3.x or a VAP for NetWare 2.x. It controls access to metered applications and performs the report bookkeeping.

Supervisor helps network managers register applications, set up rules for granting access, and view or print reports on current or historical usage. Once the manager establishes access rules, such as maximum number of concurrent users and authorised users, he or she can choose to deny access when the maximum is reached or simply generate "exception reports" and still allow user access.

The Stubs component transparently steps in between users and applications and communicates with the Enforcer to restrict usage.

---

## Application installation.

---

Usually this consists of copying programs and associated files onto the file server's hard disk. It can sometimes include making shared directories and assigning rights to those directories. Well written programs will provide most of this as part of the install program.

---

**NOTE:**
ASSIGN is a cure for installation programs that insist on running in drive A: but that you need to run in drive B:. Type ASSIGN A:=B: and then run the program from drive B:. It will think it's being run from drive A:.

---

**NOTE:**
For speed, copy your installation disks to the shared hard disk on the file server. Then run the installation after attaching to the server. No more "feed me - feed me" floppy disk insertions. Some packages - typically MS Office or Windows 3.x - have "administration" installations or "server" installations.

---

### Multi-user software.

Programs that share data between users on a network need to be "Network Aware" so that valuable data is not overwritten or lost due to the other users saving data. Since the advent of MS-DOS 3.0 networking support has been included as part of the operating system to allow for file locking and sharing. The DOS program "SHARE.EXE" can also be loaded to provide further protection against data file damage. Novell supplements this protection by transaction tracking and record locking as well as providing "semaphores" for use by applications.

### Share

Share is a terminate and stay resident program that provides file locking and protection against overwriting data.

Typically, you use SHARE in a network or multitasking environment in which programs share files. SHARE loads the code that supports file-sharing and locking in these environments. Once you install Share, MS-DOS uses the code loaded by Share to validate all read and write requests from programs. For example, if two people are accessing the same data file, SHARE manages the file so both people do not write to the file at the same time.

Share.exe does not have to be used with Windows or Windows for Workgroups. VSHARE.386 is a 32 bit replacement that can be installed in the System.ini file. MS Office will install it automatically in Windows and it is already present in Windows for Workgroups.

**Is Your Software Properly Licensed?**

Purchasing software is one of a network administrator's primary responsibilities, but wading through the various types of software-license agreements can be a nightmare. Once the software license is purchased, the next major chore is enforcing it. Remembering who purchased what, who's entitled to use what, and when they can use it can become a burden.

There are many factors to consider and many pitfalls to avoid when evaluating license agreements. Below are some simple definitions of the most common license agreements, which is intended to help you understand what these types of agreements really mean.

- License per machine. A license per machine requires customers to purchase a license for each PC that might use the software. For example, if you have a network of 150 PCs, you would need to buy 150 individual licenses. Licensing by machine is best for client operating system software.

- License per individual. Software that is licensed to a particular individual means it can only be used by that specific person.

This particular license raises many questions: Can the licensed individual use the package both at work and at home? Some say no it must be uninstalled at work before it can be used at home. Others argue that the individually licensed software is the property of the individual, and it therefore can be used anywhere. What if that individual leaves the department or company does the software go with that individual or can the license be transferred to another employee?

- Concurrent license. With a concurrent license, customers purchase licenses based on the maximum number of users accessing the software at any given time, This can save companies money, but determining the estimated peak usage is not always easy.

- Site license. When companies purchase many software licenses, vendors sometimes offer volume discounts, or a site license. A site license may consist of a discounted price on multiple copies of software, or it may be permission to make unlimited copies of a particular package.

- File-server license. A file-server license is a single copy of a program placed on a file server for use by an unlimited number of users. The license agreement generally prohibits you from installing the software on multiple file servers. This type of license is good for systems software programs and many network-management tools, because they do not require accurate user or PC accounts.

**Networkable & network-aware**

One other thing to watch out for when buying software for use on a network: Make sure the software is intended for network use. Some standalone software packages do not function correctly on a LAN. If you are going to install it on a network, always make sure you get the network version. Most popular software packages offer a network version.

"Networkable" and "network-aware" are terms that can be confusing to users. Networkable usually means the package is a standalone product that can function on the network without additional changes.

Network-aware packages, on the other hand, are specifically designed for LAN use and take advantage of the network operating system functions and features. Such as file locking and record locking.

No matter what license agreement you choose, you must have a well thought out policy. The policy should clearly indicate how your company feels about software piracy and what the company's penalties are.

And to make things easier, several useful metering and monitoring software systems are currently on the market. See the section on application monitoring further on.


**Network versions of software.**

Invariably network versions of software are more expensive due in the main part to more costly development as well as more users of the package reducing revenue.

# Methodology.

Companies that cannot afford full-time network administrators need to develop and implement the use of network office manuals so that users can refer to instructions in the event of a network failure. A manual should be configured so that any employee can use it and it should include solutions for regular problems encountered with normal network usage. The manual should also include directions for solving a variety of situations including log-on problems, equipment usage and for communicating with technical support personnel. Network manuals also aid in establishing and maintaining effective security programs.

## The network office manual

Network documentation frees the small business owner from being held hostage to a key employee who just "knows" how the LAN operates. A network office manual can be organised so any employee can consult it. In many instances, it holds the answers to the simple problems a network regularly presents. The network office manual also can reduce or eliminate potentially crippling problems that result from a lack of configuration or procedural data. Such a resource doesn't necessarily demand a great deal of time; you can create the beginnings of a manual in about four hours.

The network office manual proves useful for all sorts of problem situations, including when you don't understand why someone can't log into a directory or access a program, when you want to figure out where on the 180MB of tape the latest version of a file is, or when talking with technical support staff over the telephone. Most importantly, the network office manual can help you to develop and maintain a good security program for your network.

## Network Documentation of both hardware and software.

All workstations should have a document that describes the workstation's hardware setup and its software configuration. It may also help to document what applications are being run on that workstation. How do you do this ? Well it depends on how much detail you desire and how much time you are prepared to devote to this documenting of the network. Most operators of networks don't bother and when things go wrong outside consultants are called in to sort out simple problems that could have been solved by reading the workstation documents.

## How to inventory the pc's hardware

You will probably be asked at some time for a complete list of all the pc's in your charge with all their details. Usually accountants want this sort of information. The Microsoft Diagnostic program MSD is not really a problem solver or diagnostic program. It will provide a complete list of hardware in the pc with its configuration information for memory, DOS and Windows as well as its network configuration.

MSD is a DOS and Windows supplied utility program that compiles a complete report on the pc. The report can be displayed on the screen or printed on a printer or a text file. The options can be viewed using **/?**. It can be set up to run at pc start-up and to print a report to a file for admin use later. This could delay the start-up and frustrate the user so perhaps a better way to do this would be to check for the existence of a report file and only print the report if it doesn't exist. This allows the administrator to delete the old report file, forcing a new file to be generated at start-up. This operation can be done in the AUTOEXEC batch file or in the login script.

## Anti-Virus measures

Virii (plural of virus) are going to be with us forever. Its a peculiar form of vandalism that has caused the loss of time, money and man-hours of repair. There are now over 15,000 different virii, though some are just variations of the original.

Virii are spread in several ways. By attaching themselves to programs; by inserting themselves into boot and partition sectors of disks or by attaching themselves to documents/spreadsheets as automatic macros.

They range in severity of damage from a simple joke message to re-writing the hard disk and destroying all data on the disk.

Protection against virii can be simple or complex with some measures slowing down system performance so much, that the users will complain about how long it takes to load a file or program. Simple measures like enabling 'boot sector' protection in the BIOS set-up will go a long way to stopping the severe virii. (This is demonstrated)

DOS has some virus protection built-in and some new programs have it built-in as well.

Scanning all 'outside' disks before using is a good plan as this will eliminate infection before it gets into the network system. However this means using a separate isolated pc for scanning.

DOS 6.x has both DOS anti-virus programs and Windows anti-virus programs. These were bought from Central Point and added to the DOS 6.x package. Unfortunately these are not being updated with new identities of the later virii. However both programs have the ability to warn of file changes which can come about when a virus infects a program.

## Network Anti-virus Measures

Nearly all the current anti-virus packages have a network protection scheme. Some like the original Dr Solomon's Netware Loadable Module were thrown out by system administrators. These would slow the server down so much that the users revolted. Later models run at pre-set times usually when everyone has gone home.

The only requirement here is that the system administrator or person responsible, reads the report generated by the program and acts upon it.

## Network troubleshooting summary

To summarise, here's a checklist to assist with diagnosing failures on Ethernet networks:

1.  Clean the gold fingers on the Network Interface Card with paper and reseat it in the workstation socket.
2.  Check the board jumper that selects the BNC or DB-15(AUI) or UTP cable output.
3.  Run the NIC diagnostics, if any are available. Use the appropriate cable terminator or network connection during loop back testing.
4.  Check the IRQ, shared memory and I/0 based addresses for conflicts with other boards. Check if EMM386.exe excludes the shared memory if used. If in doubt, remove all boards but the NIC and reinsert them one board at a time. Visually inspect the NIC for any jumpers that may have fallen off, or any DIP switches not firmly set. If repeaters are installed on cables, visually confirm that LED diagnostic lights indicate proper function.
5.  Confirm that CONFIG.SYS, AUTOEXEC.BAT and any device drivers in use are loaded properly upon start-up. Don't forget the line by line step option using F8.
6.  Verify that the transceiver, AUI cable and any applicable option on the NIC are set consistently for either Ethernet or IEEE 802.3.
7.  Use a Volt/Ohm Meter to determine whether a short has occurred, and a Time Domain Reflectometer to confirm the location of the short or open circuit.
8.  Check for unterminated cable ends or broken cables.
9.  Test terminators with an ohmmeter for a resistance between 48 and 52 ohms.
10. On thin coaxial cable, check for disconnected or poorly assembled T connectors.
11. Verify that RG-58A/U (50 ohm thin cable) is being used and not tv coaxial cable.
12. If software configurable node addressing has been used, use the NIC diagnostic utilities or a protocol analyser to check for duplicate node addresses.


## File server not found.

When a workstation is unable to establish a session with a file server, NetWare typically issues the error message "File server not found." To determine the cause of this condition, check for the following possible physical hardware anomalies:

*   Excessive traffic and collisions - too many on one trunk or one station talking too much ?
*   Improperly installed cable - maybe bent beyond endurance.
*   Malfunctioning transceivers
*   Malfunctioning repeaters or hubs
*   Bad connectors - poorly constructed "T" pieces and drop in cables.
*   Bad terminators - measure the resistance using a multimeter.
*   Crushed cable - installers or somebody in the false ceiling?
*   Bad network interface cards (NICS) - damaged by lightning or voltages on the cable.
*   A bad I/0 slot in a workstation node - this doesn't happen often.

If there are no physical problems, then check for the following network anomalies:

*   Two or more NICs with the same network address - especially with ARCnet.
*   Invalid or duplicate NetBIOS names (affects only NetBIOS applications)
*   Incompatible BIOSes - unlikely to occur these days, but old XT's used to do this.
*   Mismatched IPX drivers - ie drivers for older models of cards being used for new cards.
*   Conflicts with IRQS, I/0 port addresses, base memory, and DMAs
*   Insufficient number of routing buffers

When NetWare sends application error messages, check for the following possible anomalies:

*   Inefficient use of protocols
*   Incorrectly implemented protocols
*   Routing table errors
*   Insufficient number of routing buffers

## Fixing a Damaged Bindery

The bindery plays a crucial role in NetWare.  This database stores detailed information about objects and named entities known to a file server, including information concerning users, groups, file servers, print servers, and gateways.  For example, the NetWare login program queries the bindery to verify user security.

If the bindery is damaged, users and supervisors will have trouble accessing resources and, possibly, logging in to the file server.  Other possible bindery problems are the disappearance of user names and/or groups from the bindery file, and I/0 errors while accessing the bindery file.

The bindery comprises two files located in the system subdirectory of every file server.  The files are named NET$BIND.SYS and NET$BVAL.SYS for NetWare 2.x.  These files have the attributes "System" and  Hidden," which are automatically flagged at installation.  However, the SHOWFILE utility will reveal them.

Novell also provides two utilities, SECURITY and BINDFIX, which check for damaged binderies on the file server.  The SECURITY utility checks for possible security holes by examining the bindery and reporting on any inconsistencies.  The supervisor can use this utility on a regular basis to scan the bindery for problems before they have an impact on the network.  If the SECURITY utility does not execute properly, then you can use BINDFIX, a troubleshooting utility, to repair bindery damage.

You may need to run BINDFIX if you experience any of the following problems: User names cannot be deleted or modified; passwords or rights cannot be changed; or error messages indicate that a corrupted bindery is being displayed at the file server console.

Users should log out before you run BINDFIX, to guard against further bindery contamination.  When you run the utility, you create new NET$BIND.SYS and NET$BVAL.SYS files.  The previous versions of these files are renamed NET$BIND.OLD and NET$BVAL.OLD.  This procedure is also an excellent way to make a backup copy of your bindery.  After any major system configuration changes, BINDFIX should be run to backup the bindery for safekeeping.

Occasionally, BINDFIX makes the problem worse or does not run at all.  Then you should use BINDREST to restore a previous version of the bindery. BINDREST will rename the NET$BIND.OLD and NET$BVAL.OLD to NET$BIND.SYS and NET$BVAL.SYS.  If you cannot access the file server due to bindery problems, first back up your data, if possible.  Then reinitialise the hard drive, reinstall NetWare with the DEFAULT bindery and execute BINDREST using the backup copy of NET$BIND.OLD and NET$BVAL.OLD to restore your system configuration.  Next, using a backup copy of the data files and programs, restore your applications.  You should follow the detailed instructions for these utilities in the NetWare reference manual.

**ARCdiag**

The ARCDIAG program is designed to be a service tool for network administrator personnel for a network that uses ARCNET type hardware. The ARCDIAG program includes two diagnostic sections that will help during installation of an ARCNET network. The diagnostic software can be operated at any workstation during installation of the network or at any time while running the Novell Network Operating System.

The ARCDIAG program is not intended to isolate Novell Software problems except in those cases where the physical network hardware is the prime cause of the problem.

The program exercises the network card by testing all of its internal functions, RAM, RIM etc., and then displays a map of active nodes and packet counts. The latter also provides an indication of any reconfiguration that might be occurring.


**Cable fault locators.**

Finding an electrical fault on cable that disappears into the ceiling or into the subterranean depths of a building may seem daunting. But with a simple continuity meter (OHM meter) broken cables can be found easily in very little time. Meters can cost a thousand Rand for great accuracy, but the type needed here should not cost more than R200. Measure a known length of cable of the same type and work out the resistance per length in Ohms / Metre. The unit that you measured will tell you how far away is the short circuit when you measure the resistance across the cable. To check continuity of a terminated leg use the reading with some allowance for the resistance of the cable. The resistance measured has very little to do with the characteristic impedance of the cable as the meter is using direct current to measure only resistance. The meter is not capable of supplying the alternating voltage and frequency normally sent down the cable.

Open circuit cables cannot be measured in this manner and require the use of a "Time Domain Reflectometer". This fancy name really means a form of cable radar, which sends a pulse into the cable, measuring the time taken for a return pulse to arrive. TDR's are expensive and usually owned by specialists who will charge you for their services.

## SNIFFERS and other troubleshooting

Networks are real-world dynamic systems. To a network novice, the IEEE, ISO, CCITT, and ANSI specifications that govern what should be seen on network wires seem to speak of a very ordered communications system. A seasoned network manager knows a network is a very dynamic environment--almost as dynamic as the weather.

The protocol analyser was the first tool a network manager could use to make sense of the network's changes and to identify a variety of packets, their origins, if they were intact, and if they were going to the proper destination. A protocol analyser exposed the wire and its signals for the manager's scrutiny. But to be able to interpret the data presented by the protocol analyser, a network manager had to have a great deal of training and in the-trenches experience.

To lower the threshold of experience, some protocol-analyser manufacturers introduced rules-based or expert systems into their products. Protocol analysis then becomes the domain of an intermediate-level network manager.

Both Hewlett-Packard's Network Advisor and Network General Expert Sniffer attempt to submit the network's packets and protocols to rules-based expert-system software to make sense of what might otherwise be incomprehensible information. Both products capture packets and decode protocols; both detect problems and suggest causes. In addition, the Network Advisor has several active tests to produce information about a suspected problem. Neither product fixes anything; that's still up to the manager. Perhaps "auto-fix" is the next step in network analysers.

# Administering the users

**Novell's Syscon.**

Syscon is the Novell utility program to provide the user at a workstation or a supervisor the means of changing login scripts and rights to volumes and directories. New users can be inserted into the system and given passwords by the supervisor. The supervisor can also restrict access to certain times and specific directories.

**User rights to directories and disk volumes.**

Using SYSCON the supervisor can allow groups or individual users, rights of access, creation, writing and modification. He can MAP volumes to drives to allow access for users by changing their login scripts.

**Accounting.**

Novell provides accounting to audit usage of time on the network so that departments can be billed for computer time and costs.

**Login scripts.**

Security on a LAN also includes giving users selective privileges to read, write, modify, create, or delete files and directories. Access control can be the most complicated-but necessary-aspect of LAN security. If possible, apply passwords to entire subdirectories.

### The map command

The MAP command is a Novell DOS utility to substitute a drive letter for a sub-directory on the server's hard disk. This allows the logged in user to move from directory to directory on the 'tree', just by typing a drive letter. In NetWare, there are three type of drives: local, network, and search. *Local drives* are physically attached to a workstation. *Network drives* allow users to access particular locations in the directory structure. *Search drives* allow users to execute program files (such as applications or utilities) that are in a directory other than the user's current directory.

**eg: MAP G:= SYS:\PUB-DATA      sets drive G: to the sub-directory PUB-DATA**

**Volume SYS Mapping**

```
SYS\
 +---LOGIN
 +---SYSTEM               SEARCH1: = Z:. [JBCOMPUTING\SYS:\SYSTEM]
 +---PUBLIC               SEARCH2: = Y:. [JBCOMPUTING\SYS:\PUBLIC]
 +---MAIL
 │    +---1
 │    +---2000002
 │    +---4000001
 │    +---5000001
 │    +---6000001
 +---JOHN          Drive F: = JBCOMPUTING\SYS:\JOHN
 │    +---CLIENTS
 │    │    +---PKTDRV
 │    │    +---TCP32B
 │    │    +---WFWPTP
 │    │    │   +---PTPSVR
 │    │    │        +---SYSTEM
 │    │    +---CLIENT32.X
 │    │    │    +---CLTDR2
 │    │    │         +---16BIT
 │    │    │         │   +---NLS
 │    │    │         +---32BIT
 │    │    │              +---DOSWIN
 │    │    │              +---NLS
 │    │    │              +---WIN95
 │    │    +---N32CLT
 │    │         +---IMAGE
 │    +---FONTS
 │    +---UTIL
 +---CHARLOTT
 +---ELIZABET
 +---JULIE
 +---PUB-DATA      Drive  G: = JBCOMPUTING\SYS:\PUB-DATA
     +---WFW311          Drive  W: = JBCOMPUTING\SYS:\PUB-DATA\WFW311
     │   +---ADDPDRVS
     +---UTIL
     +---TCP32B
     +---WFWPTP
         +---PTPSVR
              +---SYSTEM
```

The picture shows a typical volume (SYS) mapped with drives F:, G:, W:, Y: and Z:. Using the MAP ROOT option the administrator can stop users from going above the directory on the tree.

Mappings are generally set in the login script for the user and don't have to be changed. In Windows the Netware User tools provides this drive to directory connection in a graphical format.

# Networking Windows

Windows 3.0 had support for Novell supplied as part of the Windows 3.0 package. This continued with Windows 3.1 with the network aware applications having the ability to map/connect drives or connect printers and queues.

Windows a few years ago was run on workstation pc's with no hard drive installed. This meant that the Windows swap file had to be created temporarily on the file server's hard disk. This meant enormous amount of network traffic as each pc's swapfile was created and modified. Most users got fed up with the long (several minutes) of boot up and bought hard disks.

Windows used to be prone to problems with Novell but finally has got easier. Windows for Workgroups can be made fully functional on a Novell network. But it does ask the question - if you can make WFW work, do you need Novell? A WFW pc can be a "Server" with no local processing. With 32 bit NDIS 3 drivers the performance outshines IPX/NETX drivers. Cost also figures strongly here, Novell is overpriced for numbers of users.

---

**NOTE** : By default, NetWare allows you access to only 40 files at a time. When you are running applications with Windows 3.x, you can exceed this limit rather quickly. If so, you might see unexpected error messages. To increase the file access limit, add the following line to your NET.CFG file:

  **file handles = 60**

You should also add the following to your CONFIG.SYS file:

  **files = 60**

---

### How to make Novell and Windows for Workgroups work together.

Windows 3.x originally had excellent support for Novell networking, but with the release of Windows for Workgroups 3.1 as a competing product, that all changed. Novell said that the licence to use IPX etc did not extend to Workgroups and threatened to sue. Microsoft therefore removed all Novell support files from Windows for Workgroups 3.11. This effectively disconnected Novell from the growing number Windows users, but upset Windows users who needed Novell connectivity.

It is possible to connect a Windows for Workgroups set-up PC to a Novell network and have both networks working. It requires the use of Novell's VLM's and a circuitous installation procedure. After installation do not change network set-ups without having a complete backup handy or your social life will disappear!

## Subdirectory entries (Novell & Windows)

A NetWare file server does not include the directory entries dot (.) and double dot (..) as DOS does. However, the NetWare shell (version 3.01 or higher) can emulate these entries when applications attempt to list the files in a directory. If you have problems listing files or deleting directories, turning on the Show Dots feature will help. Add the following line to your NET.CFG file:

**show dots = on**

Turning on Show Dots will cause problems with earlier versions of some 80286-based NetWare utilities, such as BINDFIX.EXE and MAKEUSER.EXE. Make sure you upgrade these utilities if you upgrade your NetWare shell.

## Redirected drives (Novell & Windows)

Redirected drives can look different in Windows for Workgroups from the way they did without Windows for Workgroups. For example, a device mapped as FileServerName/Volume:Directory will appear in Windows as FileServerName/Volume:\, showing the root of the file server's shared volume rather than the subdirectory. You can correct this with the MAP ROOT entry, as explained in the following information.

## Default directory (Novell & Windows)

In some cases, Windows-based applications may change the default directory on a drive. This might cause problems if, for example, your path includes the current directory on a network drive (that is, your path includes a drive letter without a specific directory, such as z: instead of z:\system).

You can prevent this problem by using MAP.EXE and LOGIN.EXE versions 3.0 and later to set up false roots, or by choosing the MAP ROOT function when mapping a connection in File Manager. This feature simulates the MS-DOS **subst** command, which sets the root of a given drive to a directory designated by the user instead of to the true root of the volume.

For example, suppose you normally mapped drive F to the HOME\TERRI directory on the SERVER\SYS volume, and then included F: in your path. You would do this by including the following command in your AUTOEXEC.BAT file or by typing the command before starting Windows:

**map f:=server\sys:home\terri**

The default directory on drive F would then be HOME\TERRI. To prevent Windows from changing this, you would replace the command above with the following:

**map root f:=server\sys:home\terri**

This command would make the directory HOME\TERRI appear to be the root of drive F.

## Drive mappings  (Novell & Windows)

If Windows for Workgroups is running in 386 enhanced mode, you can adjust the way Windows handles your network drive mappings by using the Network option in Control Panel.

Usually, when you quit Windows, all of your drive mappings are restored to the way they were before you started Windows, and all changes you made while running Windows are lost. If you clear the Restore Drives option in the settings dialogue box for NetWare, the mappings you made in Windows will remain when you quit.

Typically, each instance of MS-DOS Prompt you start from Windows has its own set of drive mappings. Changes you make in one instance do not affect another. If you set the NWShareHandles option, drive mappings will instead be global, and changes to the mappings or the current drive, made in one instance of MS-DOS Prompt will affect all other applications. If you are running a NetWare 286 server, setting NWShareHandles increases the number of workstations that can be connected to the server before the server runs out of available connections.

See the Help available in the Network dialogue box in Control Panel for more information on these options.

## Printing extended ASCII characters  (Novell & Windows)

If you have applications or files that use extended characters (ASCII characters above 128) and you have problems viewing or using them, try adding the following line to your NET.CFG file:

**special uppercase = on**

## Connecting & disconnecting from resources  (Novell & Windows)

When connecting or disconnecting network resources from File Manager,  Print Manager, or Control Panel, pay attention to the state of the Permanent check box. If this option is selected when you make a connection, the connection is automatically made each time you restart Windows. To stop reconnecting, disconnect with the Permanent check box selected. If the option is not selected when you disconnect, the connection is removed for the current Windows session but is reconnected when you restart Windows for Workgroups.

## Using IPX & SPX  (Novell & Windows)

If you want to use IPX-based applications with Windows or Windows for Workgroups running in standard mode, you must be sure to load the TBMI2.COM memory-resident program before starting Windows for Workgroups. This file is included on the Windows for Workgroups Setup disks. You can use the MS-DOS **expand** command to copy it to your hard disk if it is not already there.

If anything has captured the imagination in networking recently it must be the Internet. Even accountants know about it! What started as a defence project in the Cold War Years, has become a global network of interconnected computer systems. More information that you can ever use can be obtained about any subject.

In 1957, the US formed the Advanced Research Projects Agency (ARPA) within the Department of Defence (DoD) and during the next two decades, this agency was to build ARPANET - the computer network, which is the granddaddy of today's internet.  With the establishment of the NSFNET research network in 1986, which had an initial backbone speed of 56Kpbs, there was an explosion of educational connections across the US.  By 1990, ARPANET had become defunct, but the Internet was growing exponentially.  With the addition of the commercial sector to the Internet community in 1990 a new phase of internet expansion was triggered.  By mid-1991, the commercial sector had already overtaken educational and research institutions as the biggest user of the Net.  Although traffic on the NSFNET backbone passed the 1 trillion bytes/month mark in 1991 and 10 trillion bytes/month mark in 1994, in early 1995, the NSFNET reverted back to a research network, and Internet traffic began to be routed through interconnected network providers.

The "language of the internet", TCP/IP (Transmission Control Protocol/Internet Protocol) was initially designed "on the back of an envelope in a hotel lobby in San Francisco" in March of 1973, according to Vinton Cerf, its originator.  Many of the basic internet services such as FTP and Telnet were designed in the early to mid seventies, as well with the first recorded email message being sent in 1972.  Most of these were only widely implemented after the official adoption of TCP/IP on ARPANET in January of 1983.  In 1992, the World Wide Web was released on an unsuspecting world, and in the same year the first MBONE audio and video multicasts took place - both of these developments set the pace for the next few years' growth.  By March 1995, Web traffic became the Internet service with the most traffic.

In terms of global development, the then pseudo Internet only went international in 1973, with the first international connections to ARPANET University College of London (England) and the Royal Radar Establishment (Norway).  Today nearly a hundred countries have full internet connectivity, including some 8 on the African continent.  The beginnings of South Africa's University and research network UNINET were in the late 1980's and by the end of 1991, South Africa had a dedicated connection to the NSFNET backbone.  In 1993, the Internet Company of South Africa (TICSA) began providing commercial Internet access.  South Africa is now the 15th fastest growing country in numbers of Internet users and has over 20 commercial Internet service providers, and an estimated 200 000 Internet users.

**Your very own Internet - an Intranet**

You have just been promoted - from Network Administrator to - Web Master! You need help, lots of help.

I have said this before on the course, write it down, the plan that is, for your new web server set-up. Start planning what needs to be done. Every client I have talked to recently has wanted either a "presence" on the Net or an in-house net (intranet). It seems that all this needs Pentium Pro machines with NT4 and 32MB of ram, main-frame hard disk capacity and so on. Oh I forgot, you need to be able to generate web pages in html and lots of java input. Which means a very expensive Web page production package.... Get the picture?

It seems that most have forgotten the roots of the Internet and the World Wide Web. You don't need a heavyweight machine, lots of memory and disk space for an in-house web server. The requirement is very basic a 386 will do, even a 386sx, say 8MB of memory, 120MB hard disk, Network adapter, vga mono monitor and a keyboard. You have a choice of operating system, no not NT, though you can purchase a server version, which will allow many users. No the choice is either Windows for Workgroups with TCP/IP 32bit or Linux. The 32 bit TCP/IP upgrade for WFW is free, yes free and available for download from Microsoft.com. Linux is totally free and can also be downloaded for free from a great many sites on the net. It is also available on CD-ROM, where the cost of distribution is the cost of the package. The system - Linux - is a 'free' form of unix for Intel and other processors.

[This machine and software configuration is suitable for experimentation purposes as well.]

**The Linux option**

Linux has TCP/IP networking built in, an ftp server and unix system administration. The last may be a drawback as it uses command line driven utilities with inscrutable options. Various Web Servers are available, again for free, which can be set up from other workstations if necessary. The NCSA's httpd web server can be downloaded from their site for free. The Apache web server is also freely downloadable. Both work well and can serve workstation pc's on the network running all the current browsers.

**The Windows for Workgroups option**

The 32bit TCP/IP upgrade can be downloaded for free and applied to an existing 386SX pc on a network. If you do so, set the slider control to network runs fastest in the control panel applet for the network. You won't be using this pc for applications so it makes sense to make it a 'server'. A shareware web server is available called whttpd. Shareware is a concept, which you may not be familiar with; it concerns your 'honour'. You get to use the software for 30days usually and then if you wish to continue using it, you must pay the author of the software for the use of it. This is usually a small amount of US dollars, unfortunately with our current exchange rate this tends to be pricey, but not as much as a branded product.

This does however allow you to set up a web server with html pages and access it from your networked pc's.

## Step 1 - Network set-up

Your first requirement is to change your network protocols to TCP/IP. This can be easy or expensive, depending on your existing network. If you have Novell installed this could get messy and is one of the reasons why Novell has lagged way behind in the Intranet/Internet stakes. TCP/IP add-ons for Novell have been expensive in the past as they were additional packages. With Windows for Workgroups 3.x the addition of a new protocol is very easy. The software is cheap - in fact it's free! With NT, TCP/IP is already there, simply add it from the master disks or CD. With Windows 95, TCP/IP is also on the CD and is simplicity itself to add. There is one 'gotcha' though, the choice of the node numbers. You must know if your network is to be connected directly to the Internet. If it is, the node numbers for all your user pc's and servers will have to be 'registered'. This will cost around R400 to R500 and is to ensure that no duplicate nodes are connected to the net. If it is never to be connected, your life is simpler, but not completely so.

*Remember to document the numbers for each pc. You can do this using MSD.*

There is a recommended set of IP numbers for networks that are not going to be connected to the internet contained in RFC1597. RFC1597 details IP addresses for use by 'private' networks. This allows you to accidentally connect to the Internet without causing grief. Addresses are :-

```
10.0.0.0            to        10.255.255.255
172.16.0.0          to        172.31.0.0
192.168.0.0         to        192.168.255.255
```

**NOTE:** I suggest that you copy the 32bit protocol addition to a shared directory on a network pc and install from there. Go to each pc and install over the network.

If you have DOS based pc's that are networked, don't despair, packet drivers are freely available for TCP/IP connection. A packet 'shim' of software is also available for WFW networks that rides on top of NDIS drivers, allowing DOS attachments as well called DISPKT. This is also available for download. This allows you to use packet software such as NCSA's Telnet and FTP to communicate with your Unix server.

## Step 2 - Acquire an 'old' pc for the Server.

You only need an 80386 or low end 486 for the Web Server. It will need a network adapter, a moderate (100 - 250MB) hard disk, and 4 to 8MB memory.

**Option a)**

Set it up with Windows for Workgroups 3.11 or 3.1 and install the TCP/IP 32bit protocol as the only (default) protocol. This will keep prying eyes from playing with your disk.

Then install the Whttpd Web Server on the C: disk of the server. Add it to the startup group so that it runs whenever the pc starts. Transfer html files to it and start browsing the pages you have added. This won't take very long, probably an hour to install and get running. Don't forget to update the HOSTS file on everybody's pc.

**Option b)**

Download Linux and NCSA's httpd Web Server from the net or buy the CD's. Install Linux as the operating system and NCSA's Web Server (httpd). You can upload html files to the server using Windows FTP. Start browsing the pages you have added. This will take a little longer than option a, but provides unlimited users, higher security and eMail (POP3) all built-in.

## Step 3 - Install browsers

Your favourite browser has been getting fatter and heavier recently. Try using a lean one for those users who don't have 16MB plus. I would suggest Internet Explorer 2.0 for Windows 3.x as it will work quite happily in 8MB. The new Internet Explorer 3.0 for Windows 3.x has also appeared and is supposed to be very light on system resources.

## Browsers

Whilst Microsoft's browser, Internet Explorer, is free and downloadable, it is heavy on system resources and will take a long time to download. It is available for both Windows 3.x, Windows 95 and Windows NT. Netscape Navigator is not free and but can be obtained over the net and used for a limited period. The NCSA has also created 'Mosaic', a free browser which works well but requires Win32s added to Windows to function. Win32s is the 32 bit application interface written to allow 32 bit programs to work under Windows 3.x as well as Windows NT. It is now obsolete, but needed for several net applications that run under Windows.

## File Transfer programs

FTP is a standard method for transferring files over the net. FTP programs are freely available and most browsers also have a sub-function ftp module. This allows your user to select files using the browser and to download them easily to his/her pc's disk. For serious downloading the Ws-Ftp windows program works much better than a browser, using a split window arrangement similar to file manager.

### News server

Usenet style news can also be run on a Linux box.

The idea of network news was born in 1979 when two graduate students, Tom Truscott and Jim Ellis, thought of using UUCP to connect machines for the purpose of information exchange among Un*x users. They set up a small network of three machines in North Carolina.

Initially, traffic was handled by a number of shell scripts (later rewritten in C), but they were never released to the public. They were quickly replaced by ``A'' news, the first public release of news software.

``A'' news was not designed to handle more than a few articles per group and day. When the volume continued to grow, it was rewritten by Mark Horton and Matt Glickman, who called it the ``B'' release (a.k.a. Bnews). The first public release of Bnews was version 2.1 in 1982. It was expanded continuously, with several new features being added. Its current version is Bnews 2.11. It is slowly becoming obsolete, with its last official maintainer having switched to INN.

### Html page creation

Again the proprietary software applications do have add-ons, some free and some not. However you can download free add-ons for Word and WordPerfect or you can obtain shareware packages that create and view html pages. Html is not a complex formatting process and you can learn it in a few hours and type it in Notepad to generate pages.

### The next step from here

You have a company database that your colleagues need to access. You can set the web server to serve your users data with search facilities as well. The facilities can be easily set up using Visual Basic or QBasic.

> **NOTE:** Want a free copy of Visual Basic? VB is freely available on the server. It is VB4 and is limited in certain capabilities, but allows full design and later compilation with the full product.

The company newsletter or in-house magazine can now be issued weekly, with real life pictures and text with up-to-the-minute information. This assures the best-informed employees, with the information really at their fingertips.

**Table 1: IEEE 802.3 data-packet format.**

| Byte | Description |
|------|-------------|
|  |  |
| 00-61 | Preamble.  These bytes are transmitted before each packet and stripped by the NIC as they are received. |
|  |  |
| 62-63 | Start of Frame Delimiter.  Indicates that the meat of the packet is about to start and is stripped with the preamble. |
|  |  |
| 64-69 | Destination Address.  Address of the interface board to which this packet is destined. |
|  |  |
| 70-75 | Source Address.  Address of the interface board for which this packet was generated. |
|  |  |
| 76-77 | Length.  Number of bytes contained within the body of this packet. |
|  |  |
| 78-??? | Data.  The body of the packet. |
|  |  |
| ?+1-?+4 | FCS.  A 32-bit CRC appended to all packets. |

**The OSI seven layer model.**

The International Standards Organisation (ISO), developed the Open Systems Interconnect reference model generally known as the OSI model. The model groups logically the functions and sets of rules, called protocols, needed to establish and conduct communication between two or more parties. The model has seven layers corresponding to those functions.

**1 The Physical Layer**

This is the physical media over which the data is to be transmitted in a bit stream. It specifies the type of cable, connectors, signal voltages, bit rate, data encoding method, modulation method and method for detecting collisions in contention networks.

**2 The Data Link**

This layer describes the rules for transmitting on the channel, such as the format of the information or frames, and procedures for gaining control of the channel, transmitting the frame and releasing the physical media.

**3 The Network Layer**

This layer is not necessary for a single local area network as all stations connected onto a LAN share the same channel. It is however needed for controlling switching between links in a multihop network. It applies to gateway, communication server, and dial-up communication applications.

**4 The Transport Layer**

This layer ensures end-to-end message integrity and provides for the required quality of service for exchanged information. Acknowledgements and flow control are performed by this function.

**5 The Session Layer**

This layer establishes and terminates logical connections between network entities. This layer is also responsible for the mapping of logical names into network addresses.

**6 The Presentation Layer**

Any translation, format conversion, or code conversion to put the information into a recognisable form is done by this layer.

**7 The Application Layer**

Distributed databases and electronic mail are examples of this layer. The end user application software does not form part of this layer. This layer provides network based services to the end user.

**8 Network Management**

Network management is responsible for the operational planning, which includes gathering of operational statistics such as errors and traffic. It is also responsible for network initialisation and maintenance. Network management is applicable to all seven layers of the model.

## RAID - What does it mean?

**R**edundant **A**rray of **I**nexpensive **D**isks (RAID) levels 0 through 6 and 10 specify standards for combining disk drives for fault-tolerant data redundancy. These standards are not official but can indicate which level might satisfy users' needs. Level 0 is not redundant and has no fault tolerance but uses disk striping to write across multiple disks. Level 1 duplicates every byte of data by having mirrored or shadowed disks, that is a duplicate of every disk. Level 2 uses bit interleaving to spread data across all drives without duplicating all disks. Level 3 modifies level 2 for microcomputers. Level 4 remedies level 3's inability to perform simultaneous input/output (I/O) by placing one transfer block on each drive rather than interleaving data across all drives. Level 5 remedies the inability of levels 1 through 4 to write one transaction at a time. Level 6 is proposed to add one additional parity section per disk to level 5, which provides one section per disk. Level 10 combines levels 0 and 1.

There are six generally accepted levels of RAID. Each level is described below.

**RAID level 0.** This level uses disk striping, in which data is written across multiple disks rather than on just one disk. For example, segment 1 is written to drive 1, segment 2 is written to drive 2, and so on. When the system reaches the last drive, it starts writing to the next available segment of drive 1.

RAID 0 has no data redundancy: If one drive fails, the entire drive subsystem goes down. It is ideal for high-performance applications that don't need data protection.

Because it has no fault tolerance (remember our definition of a RAID system), RAID 0 is technically not true RAID. Every time a vendor claims it supports RAID 0, it is talking about disk striping and not a true RAID technology. RAID 0 and RAID 1 can be combined to achieve fault tolerance.

**RAID level 1.** Often called mirrored or shadowed disks, RAID 1 has a duplicate disk of each disk in the system.

Data redundancy is obvious; every byte is duplicated. Although simple and relatively easy to implement, RAID 1 is twice as expensive as the single, non-redundant drive approach. Read performance can be improved substantially because both drives can read different pieces of data at the same time. RAID 1 has slightly slower average access times than does a single drive. It has better seek times when reading and worse when writing.

**RAID level 2.** Using a bit-interleave process that spreads data across all of the drives in the array, RAID 2 gets around the 100 percent disk overhead of RAID 1. In this way, the first drive in the array contains the first bit, the second drive contains the second bit, and so on. Additional drives contain error correcting code (ECC) or parity information. RAID 2 was designed for mini, mainframe, and supercomputers rather than microcomputers, which track drive errors through internal checksums on the disk and standard error flags performed by the drive and controller. As a result, RAID 2 systems are too robust for microcomputers, and the error isolation data is redundant.

**RAID level 3.** Basically, RAID 3 is RAID 2 for microcomputers. RAID 3 has two or more data drives and only one parity (ECC) drive. Again, data is interleaved across all data drives. Data can be interleaved at bit level, byte level (the most common), or any other logical size.

Because data is interleaved across all data drives, a single read request is performed by multiple drives. Each drive reads a portion of the data and all of the drives transfer their portions to the controller in parallel. This yields high transfer rates, making RAID 3 ideal for applications that need high I/O bandwidth. But only

one I/O transaction can be processed at a time, because every drive is involved in each read or write transaction.

RAID 3's parallel data transfers often work well for workstations that require fast sequential access to single large files such as image processing systems. It is generally not recommended for transaction processing systems or environments in which most I/O transactions are for small amounts of data.

**RAID level 4.** RAID 3's primary disadvantage is its inability to perform simultaneous I/O transactions because large blocks of data are interleaved across all drives. RAID 4, on the other hand, places the entire first transfer block on the first data drive, the second transfer block on the second drive, and so on. This process improves disk performance by enabling multiple reads. However, there is still only one parity drive present. The parity drive contains the parity for all the data drives and is involved in every write transaction, forcing them to be performed one at a time. This is RAID 4's primary disadvantage.

A multitasking operating system can process independent read transactions for each data drive in the array. In an array with four data drives, for example, the array can perform four times as many reads as a single drive can in the same time period.

**RAID level 5.** The use of dedicated parity drives in RAID levels 1 through 4 limits each of these architectures to one write transaction at a time. RAID 5 eliminates the need for a dedicated parity drive. Each drive in a RAID 5 array contains both data and parity blocks. As in RAID 4, an entire transfer block is placed on a single drive and the parity for that block of data is stored on another drive. When a drive fails, its data can be reconstructed from the remaining drives. Eliminating the dedicated parity drive removes the single-write bottleneck and lets RAID 5 perform multiple read and write transactions in parallel.

Compared to a single drive, an array with four drives can perform four times as many reads and two times as many writes (because each write involves two drives) in a given time interval. In a combined read-write environment, the virtual transfer rates could be increased by a factor of one half the number of drives in the array, compared to the single drive.  As the ratio of reads to writes increases, the transfer rate increase factor approaches the number of drives installed. Therefore, as you add drives to the array, performance increases, although not in linear proportion to the number of drives (there are other factors such as number of host controllers). Still, this makes expansion even more justifiable.

Because NetWare is a multitasking operating system, RAID 5 makes the most sense in a NetWare environment. RAID 5 provides the reliability of RAID 3 and RAID 4 without the performance degradation associated with large transfer blocks or random disk access. This is also why many vendors offer RAID 5 arrays for NetWare servers.

**RAID level 6.** Although no final design has yet won industry approval, several vendors have proposed an implementation similar to RAID 5 but with two sections of each disk set aside for parity. It is highly redundant, and therefore more expensive, but offers higher fault tolerance than any existing implementation.

**RAID level 10.** The level known as RAID 10 is a combination of RAID 1 and RAID 0. Several vendors offer RAID 10, but some call it RAID 1/0 or simply RAID 0 with fault tolerance.

**EMM386.EXE Reference.**

Provides access to the upper memory area and uses extended memory to simulate expanded memory. This device driver must be loaded by a <DEVICE> command in your CONFIG.SYS file and can be used only on computers with an 80386 or higher processor.

EMM386 uses extended memory to simulate expanded memory for programs that can use expanded memory. EMM386 also makes it possible to load programs and device drivers into upper memory blocks (UMBs).

**Syntax (Config.sys)**

    DEVICE=[drive:][path]EMM386.EXE [ON|OFF|AUTO] [memory] [MIN=size]
    [W=ON|W=OFF] [Mx|FRAME=address|/Pmmmm] [Pn=address] [X=mmmm-nnnn]
    [I=mmmm-nnnn] [B=address] [L=minXMS] [A=altregs] [H=handles] [D=nnn]
    [RAM=mmmm-nnnn] [NOEMS] [NOVCPI] [HIGHSCAN] [VERBOSE]
    [WIN=mmmm-nnnn] [NOHI] [ROM=mmmm-nnnn] [NOMOVEXBDA] [ALTBOOT]


**Parameters**

[drive:][path]

Specifies the location of the EMM386.EXE file.


[ON|OFF|AUTO]

Activates the EMM386 device driver (if set to ON), or suspends the EMM386 device driver (if set to OFF), or places the EMM386 device driver in auto mode (if set to AUTO). Auto mode enables expanded-memory support and upper memory block support only when a program calls for it. The default value is ON. Use the EMM386 command to change this value after EMM386 has started.


memory

Specifies the maximum amount of extended memory (in kilobytes) that you want EMM386 to provide as expanded/Virtual Control Program Interface (EMS/VCPI) memory. This amount is in addition to the memory used for UMBs and EMM386 itself. Values for memory are in the range 64 through the lesser of either 32768 or the amount of extended memory available when EMM386 is loaded. The default value is the amount of free extended memory. If you specify the NOEMS switch, the default value is 0. EMM386    rounds the value down to the nearest multiple of 16.


**Switches**

MIN=size

Specifies the minimum amount of EMS/VCPI memory (in kilobytes) that EMM386 will provide, if that amount of memory is available. EMM386 reserves this amount of extended memory for use as EMS/VCPI memory when EMM386 is loaded by the DEVICE=EMM386.EXE command in your CONFIG.SYS file. EMM386 may be able to provide additional EMS/VCPI memory (up to the amount specified by the MEMORY parameter) if sufficient XMS memory is available when a program requests EMS/VCPI memory. Values are in the range 0 through the value specified by the MEMORY parameter. The default value is 256. If you specify the NOEMS switch, the default value is 0.

If the value of MIN is greater than the value of MEMORY, EMM386 uses the value specified by MIN.

W=ON|W=OFF

Enables or disables support for the Weitek coprocessor. The default setting is W=OFF.

Mx

Specifies the address of the page frame. Valid values for x are in the range 1 through 14. The following list shows each value and its associated base address in hexadecimal format:

```
1 => C000h    8 => DC00h
2 => C400h    9 => E000h
3 => C800h    10 => 8000h
4 => CC00h    11 => 8400h
5 => D000h    12 => 8800h
6 => D400h    13 => 8C00h
7 => D800h    14 => 9000h
```

Values in the range 10 through 14 should be used only on computers that have 512K of memory.

FRAME=address

Specifies the page-frame segment base directly. To specify a specific segment-base address for the page frame, use the FRAME switch and specify the address you want. Valid values for address are in the ranges 8000h through 9000h and C000h through E000h, in increments of 400h. To provide expanded memory and disable the page frame, you can specify FRAME=NONE; however, this may cause some programs that require expanded memory to work improperly.

/Pmmmm

Specifies the address of the page frame. Valid values for mmmm are in the ranges 8000h through 9000h and C000h through E000h, in increments of 400h.

Pn=address

Specifies the segment address of a specific page, where n is the number of the page you are specifying and address is the segment address you want. Valid values for n are in the range 0 through 255. Valid values for address are in the ranges 8000h through 9C00h and C000h through EC00h, in increments of 400h. The addresses for pages 0 through 3 must   be contiguous in order to maintain compatibility with version 3.2 of the        Lotus/Intel/Microsoft Expanded Memory Specification (LIM EMS). If you use the Mx switch, the FRAME switch, or the /Pmmmm switch, you cannot specify the addresses for pages 0 through 3 for the /Pmmmm switch.

X=mmmm-nnnn

Prevents EMM386 from using a particular range of segment addresses for an EMS page or for UMBs. Valid values for mmmm and nnnn are in the range A000h through FFFFh and are rounded down to the nearest 4-kilobyte boundary.

The X switch takes precedence over the I switch if the two ranges overlap.

I=mmmm-nnnn

Specifies a range of segment addresses to be used (included) for an EMS page or for UMBs. Valid values for mmmm and nnnn are in the range A000h through FFFFh and are rounded down to the nearest 4-kilobyte boundary.

The X switch takes precedence over the I switch if the two ranges overlap.

B=address

Specifies the lowest segment address available for EMS "banking" (swapping of 16-kilobyte pages). Valid values are in the range 1000h through 4000h. The default value is 4000h.

l=minXMS

Ensures that the specified amount (in kilobytes) of extended memory will still be available after EMM386 is loaded. The default value is 0.

A=altregs

Specifies how many fast alternate register sets (used for multitasking) you want to allocate to EMM386. Valid values are in the range 0 through 254. The default value is 7. Every alternate register set adds about 200 bytes to the size in memory of EMM386.

H=handles

Specifies how many handles EMM386 can use. Valid values are in the range 2 through 255. The default value is 64.

D=nnn
Specifies how many kilobytes of memory should be reserved for buffered direct memory access (DMA). Discounting floppy-disk DMA, this value should reflect the largest DMA transfer that will occur while EMM386 is active. Valid values for nnn are in the range 16 through 256. The default value is 16.

RAM=mmmm-nnnn

Specifies a range of segment addresses to be used for UMBs and also enables EMS support. If you do not specify a range, EMM386 uses all available adapter space to create UMBs and a page frame for EMS.

NOEMS

Provides access to the upper memory area but prevents access to expanded memory.

NOVCPI

Disables support for VCPI applications. This switch must be used with the NOEMS switch. If you specify the NOVCPI switch without specifying the NOEMS switch, EMM386 does not disable VCPI support. If you specify both switches, EMM386 disregards the MEMORY parameter and the MIN switch. Disabling support for VCPI applications reduces the amount of extended memory allocated.

HIGHSCAN

Specifies that EMM386 use an additional check to determine the availablity of upper memory for use as UMBs or EMS windows. On some computers, specifying this switch may have no effect or cause EMM386 to identify upper memory areas as available when they are not. As a result, your computer might stop responding.


VERBOSE

Directs EMM386 to display status and error messages while loading. By default, EMM386 displays messages only if it encounters an error condition. You can abbreviate VERBOSE as V. (To display status messages without adding the VERBOSE switch, press and hold the ALT key while EMM386 starts and loads.)


WIN=mmmm-nnnn

Reserves a specified range of segment addresses for Windows instead of for EMM386. Valid values for mmmm and nnnn are in the range A000h through FFFFh and are rounded down to the nearest 4-kilobyte boundary.

The X switch takes precedence over the WIN switch if the two ranges overlap. The WIN switch takes precedence over the RAM, ROM, and I switches if their ranges overlap.


[NOHI]

Prevents EMM386 from loading into the upper memory area. Normally, a portion of EMM386 is loaded into upper memory. Specifying this switch decreases available conventional memory and increases the upper memory area available for UMBs.


[ROM=mmmm-nnnn]

Specifies a range of segment addresses that EMM386 uses for shadow RAM random-access memory used for read-only memory (ROM). Valid values for mmmm and nnnn are in the range A000h through FFFFh and are rounded down to the nearest 4-kilobyte boundary. Specifying this switch may speed up your system if it does not already have shadow RAM.


[NOMOVEXBDA]

Prevents EMM386 from moving the extended BIOS data from conventional memory to upper memory.


[ALTBOOT]

Specifies that EMM386 use an alternate handler to restart your computer when you press CTRL+ALT+DEL. Use this switch only if your computer stops responding or exhibits other unusual behavior when EMM386 is loaded and you press CTRL+ALT+DEL.


## Syntax: (Dos prompt)

EMM386 [ON|OFF|AUTO] [W=ON|W=OFF]

To display the current status of EMM386 expanded-memory support, simply type  EMM386 at the DOS prompt.

**Parameters**

ON|OFF|AUTO

Activates the EMM386 device driver (if set to ON), or suspends the EMM386 device driver (if set to OFF), or places the EMM386 device driver in auto mode (if set to AUTO). Auto mode enables expanded-memory support only when a program calls for it. The default value is ON.


W=ON|W=OFF

Enables (if set to W=ON) or disables (if set to W=OFF) Weitek coprocessor support. The default value is W=OFF.


## Novell Asynchronous Services Interface (NASI)

When users on a LAN only use modems occasionally, to dial out to on-line services, for example, a modem pool can be an economical approach. With a pool of modems installed on a dedicated server, a company can avoid buying a modem for every user.

Novell  was one of the first companies to offer software that turns a PC on a LAN into a dedicated asynchronous communications server (ACS). Workstations on a LAN can access modems attached to the ACS.

In the Novell model, LAN workstations are installed with the Novell Asynchronous Services Interface (NASI), which runs as a terminate-and-stay-resident program.  The workstations load a shared copy of a NASI-compatible asynchronous communications package from a network file server.

The ACS is installed with a board supporting between four and 16 modems.  It also runs Novell Asynchronous Communications Server (NACS) software, which allows the modems attached to the server to be shared on the LAN.

Here are six asynchronous communications programs that support NASI:-

1.  Crosstalk Mk.4 version 2.0 from Crosstalk Communications/DCA (a division of Digital Communications Associates Inc.).
2.  Datastorm Technologies Inc.'s network version of Procomm Plus Network version 1.0.
3.  Dynamic Microprocessor Associates Inc.'s (DMA's) Ascom IV Network version 1.42.
4.  Hayes Microcomputer Products Inc.  Smartcom Exec version 2.0
5.  Microcom Inc.'s Relay Gold version 4.0.
6.  SoftKlone Distributing Corp.'s Mirror III LAN version 2.0.

Certain features are especially important when using network asynchronous communication software, since a shared copy of the program is being used.

One important feature is the ability to have separate configuration files and dialing directories for each user.

Another is a facility for encrypting or "compiling" scripts, making the contents unreadable so that passwords contained in scripts are secure.

All of the above programs offer some way of using private dialing directories.

The programs support a variety of file-transfer protocols.  For fast file transfers between dissimilar systems, the Zmodem protocol has become fairly popular.  Only Smartcom Exec and Crosstalk Mk.4, however, support this protocol while using a NACS.

When purchasing network communications software, users should also consider the cost per license and the number of copies of documentation included in the base package.

An NACS can also be a relatively expensive way to share modems over NetWare. A base NACS configuration costs $1,495 for server software and $895 for a Novell Wide-area Network Interface Module (WNIM) board with four communications ports.

### Drawbacks

Users are limited to communications software that supports the NASI application programming interface (API). The API also takes up approximately 40K bytes on each workstation.

### Using NetBIOS & Windows for Workgroups.

If you were running Novell NetBIOS before you set up Windows for Workgroups, the Setup program attempts to remove it when you set up Windows for Workgroups. The following procedure describes how to install Novell NetBIOS after you have set up Windows for Workgroups.

**Note:** This example assumes that you have one network adapter running Microsoft NetBEUI. For information about the settings used in this example and how to change them, see the SYSINI.WRI online document.

To install Novell NetBIOS after you have set up Windows for Workgroups:

1. Add the following line to the [network] section of your SYSTEM.INI file:

**exclude=0**

2. Add the following line to the [386Enh] section of your SYSTEM.INI file:

**V86ModeLANAs=0**

3. If you plan to start the network before you start Windows (run the real-mode network), this line should read as follows:

**V86ModeLANAs=0,1**

You should also add the following line to the [network] section of your SYSTEM.INI file:

**LANAs=0,1**

You should also add the following line to your AUTOEXEC.BAT file:

**net start netbeui**

This line should come after the **net start** command and after the line that loads NETBIOS.EXE, but before any other network commands.

4. In your AUTOEXEC.BAT file, make sure that the line that loads NETBIOS.EXE comes after the initial **net start** command and after the **msipx** and **netx** commands but before any other commands that load components of the Windows for Workgroups networking software (for example, commands such as **net start netbeui** or **net logon**).

## Information sites on the WEB

| | |
|---|---|
| www.quantum.com | hard disks |
| www.seagate.com | hard disks |
| www.conner.com | probably going to disappear |
| www.cirrus.com | vga adapters |
| www.compaq.com | pc's |
| www.hp.com | Hewlett Packard for printer drivers etc. |
| www.ibm.com | ibm who? |
| www.microsoft.com | software drivers, converters |
| www.novell.com | networking software |
| www.kyocera.com | laser printers etc. |

### network adapters

| | |
|---|---|
| www.accton.com.tw | network adapters |
| www.smc.com | ftp site ftp.smc.com /pub |
| www.3com.com | network adapters |
| www.intel.com | network adapters and other components. |

## Using named pipes (Novell & Windows)

After Windows is installed, applications that use named pipes to communicate with NetWare servers may no longer work correctly. Applications that use named pipes to communicate with Microsoft LAN Manager servers will work with Windows.

Many network applications that use named pipes can also be configured to use another method of communicating on the network, such as IPX or SPX. Contact your network application vendor for additional details.