Unit 5: Managing networks

By the end of this unit you should:

1. Know about networking management tools and technologies
2. Understand network management functions
3. Be able to carry out network management activities

Whether you are in school or college, passing this unit will involve being assessed. As with most BTEC schemes, the successful completion of various assessment criteria demonstrates your evidence of learning and the skills you have developed.

This unit has a mixture of pass, merit and distinction criteria. Generally you will find that merit and distinction criteria require a little more thought and evaluation before they can be completed.

The colour-coded grid below shows you the pass, merit and distinction criteria for this unit.

To achieve a pass grade you need to:	To achieve a merit grade you also need to:	To achieve a distinction grade you also need to:
P1 Describe network technologies		
P2 Outline the purpose of networking tools		
P3 Identify emerging network technologies	**M1** Describe the potential impact of emerging network technologies	
P4 Explain the functions of network management	**M2** Explain the goals of fault management	**D1** Justify the inclusion of routine performance management activities within a network manager's role
P5 Interrogate a network to identify the network assets and their configuration		
P6 Undertake routine network management tasks	**M3** Keep accurate records of network management tasks	**D2** Design a network security policy for a small organisation

Introduction

Managing networks is a 10-credit unit that focuses on the management aspect of networking, acting as a complementary unit to Unit 10 (*Communication technologies*).

From SoHo (Small Office Home Office) to large organisations, the seismic IT shift from standalone PCs to networked facilities witnessed over the last 20 years has brought many benefits. In addition, there is the realisation that increasingly complex networks require well-trained and experienced network managers.

This unit is geared towards introducing the role and responsibilities of the network manager, touching on both the theoretical knowledge and practical skills required.

Equal emphasis will be placed on understanding network design as well as how network activity can be monitored and maintained through an appreciation of the assets and tools commercially available.

How to read this chapter

This chapter is organised to match the content of the BTEC unit it represents. The following diagram shows the grading criteria that relate to each learning outcome.

You'll find colour-matching notes in each chapter about completing each grading criterion.

5.1 Know about networking management tools and technologies

This section will cover the following grading criteria:

P1 D1

Make the Grade P1

P1 requires you to be able to describe network technologies. This could be tested through a report, a presentation, a podcast, a wiki or a video.

Your content should include examples from all four key elements listed in section 5.1.1 (operating systems, protocols, layout and devices).

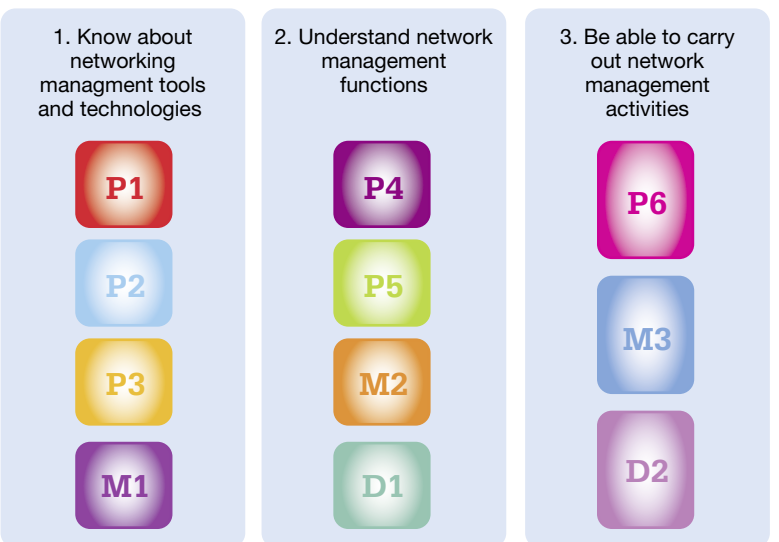

Figure 5.00

5.1.1 Network technologies

Successful network management involves a number of different types of technologies:

- Network operating systems
- Protocols
- Layout
- Devices

Let us examine each in turn.

5.1.2 Network operating systems

A **network operating system (NOS)** is a type of **systems software** that is specifically written to support networking functions, particularly over an LAN.

Its functions can include:

- implementation of networking protocols (e.g. ICMP);
- user login and authentication;
- mechanisms for sharing files and resources such as printers;
- facilities for managing administrative functions such as security;
- email support

A network NOS commonly consists of a **server part** and a **client part** – the latter needs to be installed on each device (e.g. workstation) that wants to communicate with the server.

Excluding Microsoft®'s popular NOS, other well-known examples of commercial NOSs include the following.

Novell®

Novell® is an American corporation that led the NOS market for many years before the rise of Microsoft's Windows NT® and Windows 2000® systems. Perhaps its most popular software is known as **NetWare®** and its last separate product version was Netware 6.5®.

NetWare® uses Novell®'s proprietary network and transport layer protocols called **I**nternetwork **P**acket E**x**change **(IPX)** and **S**equenced **P**acket E**x**change **(SPX)**, which were based on earlier **X**erox **N**etwork **S**ervices **(XNS)** instead of the more common TCP/IP protocol pairing. IPX became so popular in its heyday that even Microsoft® incorporated IPX protocol support into its Microsoft Windows® operating systems. More recently, the accelerated rise of the internet has made TCP/IP much more common.

NetWare®'s new Open Source policy has also proved popular, encouraging support for other network-based technologies such as **Apache® HTTP server**, **MySQL** relational database management system, **Perl** scripting, **PHP** server-side scripting and Apache® **Tomcat** (web-based Java™ applications).

NetWare® is also part of Novell®'s **O**pen **E**nterprise **S**erver **(OES)** 2®, which was released in 2009. Aimed as an **Enterprise-level** solution, OES can manage typical NOS duties (as listed earlier) but also has the advantage that it can interface with a **Linux platform**, offering an organisation a potentially lower (and therefore attractive) **T**otal **C**ost of **O**wnership **(TCO)**.

For more on Novell® visit: www.novell.com/products/openenterpriseserver/

Linux

Linux is an operating system initially designed and coded by Linus Torvalds. Originally intended to be a version of Unix running on x86-based PC architecture, Linux has flourished and been embraced by the **Open Source community** and now exists in hundreds of different distributions (called '**distros**'). It has still not beaten Microsoft's Windows® OS as the desktop operating system of choice; this has mainly been down to commercial software availability and perceived ease of use.

A distro is typically built by individuals, coding teams and some professional organisations. They often include a number of additional system software utilities (e.g. installers) and ready-made applications. Linux has attracted many high-profile supporters in the industry; these include IT heavyweights such as IBM, Novell® and Hewlett-Packard. Common distributions include: Ubuntu, Mint, Suse, Fedora Core and Debian. Full details on Linux distributions can be found here: http://distrowatch.com.

Linux is available in many different implementations, **ported** across to many different hardware platforms; from colossal supercomputers to humble PDAs and from Sony's Playstation® 3 games console to high-street smartphones.

In its more general form, Linux distributions come in **workstation** or **server installations**; both include detailed NOS elements. Indeed, **L**inux forms the first component of the **LAMP solution** '**stack**' that also includes the **A**pache® HTTPD web server, **M**ySQL relational database system and **P**HP (for server-side scripting).

A major attraction of Linux is its cost: it's free for download (although commercial distributions may charge for printed documentation and support).

Linux NOS scorecard

+ Free – means a lower total cost of ownership (**TCO**) for the organisation.
+ Ease of migration – Linux integrates well with other NOS.
+ Provides robust network infrastructure and administration tools.
+ High level of reliability.
+ High level of security.
+ Avoids vendor lock-in by providing access to a vast library of Open Source software giving an organisation free choice.
+ World-wide support community.
– Can be difficult to configure and administer at the start.
– Different distributions can cause confusion as some elements may be incompatible or implemented differently.

Linux NOS has other advantages; it can access Windows® **FAT** (**F**ile **A**llocation **T**able) or **NTFS** (**N**ew **T**echnology **F**ile **S**ystem) **disk partitions**, can integrate with Microsoft®'s networking system via **Samba**, which allows it to act as a **P**rimary **D**omain **C**ontroller (**PDC**) or be part of the more modern **Active Directory** system. It can therefore also provide file and print services for clients using Windows®.

Activity 1

Linux server installation

1 Select a server implementation of a popular Linux distribution.
2 Install this distribution onto a spare PC.
3 Enable its networking support and add it to an available LAN.
4 Enable server services such as FTP and HTTP. Attempt to access them from another workstation client on the same LAN.

5.1.3 Networking protocols

A network manager needs to be aware of a number of different protocols, especially those that exist in the **Application Layer** of the 7-layer ISO OSI model.

These protocols can be implemented on many different types and sizes of computer platforms (e.g. Apple™ Mac, PC running Microsoft Windows®, PC running Linux, Nintendo Wii™, Sony PSP® etc.).

Each protocol uses a specific network **port** (or ports) and these must be left 'open' in any software or hardware **firewall** in order for the protocol to work properly.

Common network protocols are shown in Table 5.01.

Table 5.01 Common network protocols

Protocol abbreviation	Protocol full name	Description
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	SNMP is a protocol that performs network management by **monitoring devices** for **adverse conditions** that require administrative attention (e.g. data traffic bottlenecks, overloaded CPUs). Devices that support SNMP include: • servers and workstations (various operating systems); • network devices (routers, switches, hubs, WAPs etc.); • networked devices (scanners, photocopiers, printers etc.); • UPS (Uninterruptible Power Supply). SNMP works by server-based 'manager' processes polling 'agents' (SNMP processes running on devices) to find out how well they are performing. The 'manager' process then reports these statistics to the network manager. Some 'manager' processes can then make changes to device performance via its 'agent'. In addition, each 'agent' is able to generate an alert (called a '**trap**') when something unexpected occurs that requires immediate attention. As a result, SNMP enables network managers to check network performance, discover and fix network problems. This helps them to make sensible plans for network growth. By default, SNMP uses a number of ports; these include: 161, 162, 199 and 705. A number of SNMP versions exist. The original v1 specification can be found here: www.ietf.org/rfc/rfc1157.txt The current version is SNMP version 3, adding remote configuration and additional security. Also see **RMON** (section 5.1.7 Emerging technologies).
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol	ICMP is used as a tool to help technicians (and operating systems) to discover problems during IP data transmissions. One of the most common manual uses of ICMP messages is '**ping**', which uses **echo request** to test connectivity between two IP devices by forwarding and acknowledging receipt of a chunk of data (and the time taken for the transmission to take place).

Protocol abbreviation	Protocol full name	Description
FTP	**F**ile **T**ransfer **P**rotocol	FTP is a protocol that is used to transfer **text** or **binary files** over a TCP/IP connection (i.e. over the internet). FTP requires two pieces of software: an **FTP server** and an **FTP client**. Port use is complicated: The FTP server listens on port 21 for requests (file downloads or logins etc.). It is this port that is used to send and receive FTP commands between the server and client. It is called the **control stream**. Different ports are used to transfer the actual data that form the files being transferred; a common technique is for the server to use port 20 connected to a randomised port (above 1023) on the client ('active mode'). This is called the **data stream**. Some FTP transfers require an FTP server login username and password, others use an **anonymous login** (common on the internet), which may just request an email address (but not actively check its authenticity) for logging purposes. FTP transfer is usually **insecure** as the data sent is unencrypted. Most web browser software (e.g. Microsoft Internet Explorer®, Mozilla Firefox® etc.) support basic FTP operations.
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol	TFTP is often seen as a **simplified** (and therefore less capable and secure) version of FTP, relying on TCP/IP for data transfer support. From a network management perspective, most common use of TFTP is to transfer files from a network server to a client when it wishes to perform a **network boot** (rather than load its operating system from a hard drive – it might not have one). As noted, it lacks many of the important FTP features such as the ability to use passwords and browse directories on the server. TFTP commands are essentially limited to 'GET' (download) and 'PUT' (upload) data files. Another common use for TFTP is to upload **firmware upgrades** for networking equipment such as **switches** and **routers** (similar to flashing a PC's BIOS) to improve their functionality or to update device configuration files. By default, the TFTP server listens on port 69 for requests.
HTTP	**H**ypertext **T**ransfer **P**rotocol	HTTP is the set of rules used by a **web browser** for requesting files (assets such as images, text, sound, video etc.) from a **web server**. As such, it is a common element of network traffic that represents intranet or internet browsing. HTTP usually uses port 80 although others may be used, e.g. 8080. A full HTTP standards reference can be found here: www.ietf.org/rfc/rfc2616.txt
NTP	**N**etwork **T**ime **P**rotocol	NTP is a protocol used for **synchronising** the **internal clocks** of computer systems over a typical packet-switched network. This would, for example, enable all servers and workstations on a LAN to have the same time. Another form of the protocol, **Simplified NTP** (**SNTP**), was developed in 1995 – this makes NTP easier to install and use on typical PC systems. By default, NTP uses port 123.

Examples of network protocols in use:

HTTP

The following example demonstrates an HTTP request made from a web browser client (Mozilla Firefox®) to an Apache® HTTPD web server.

Figure 5.01 Apache® HTTPD web server is started

In this example, the Apache® HTTPD server is started (on IP address 192.168.123.3); it listens on port 80 for HTTP requests.

In Figure 5.02, a request is made by Mozilla Firefox® (running on IP address 192.168.123.7) for a file called 'test.html' using the 'GET' HTTP command. The version of HTTP being used is 1.1.

Apache® serves the file ('test.html') to the browser where it is rendered on screen.

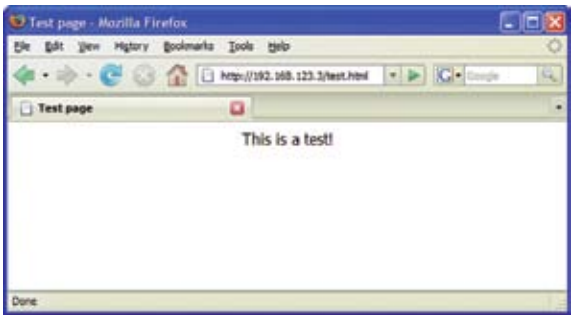

Figure 5.02 Mozilla Firefox® requests and receives a specific document

An examination of the Apache® HTTPD server **access log** reveals:

```
192.168.123.7 - - [09/
Apr/2007:13:50:09 +0100] "GET /
test.html HTTP/1.1" 200 109
```

HTTP has many different **status codes**; code 200 is used to indicate that the request was fulfilled.

109 is the size of the object sent back to the browser client; 'Test.html' is actually 109 bytes in size.

FTP

The example in Figure 5.03 and 5.04 demonstrates a user logging onto a remote FTP server, in this case NASA's (National Aeronautics and Space Administration) anonymous FTP server.

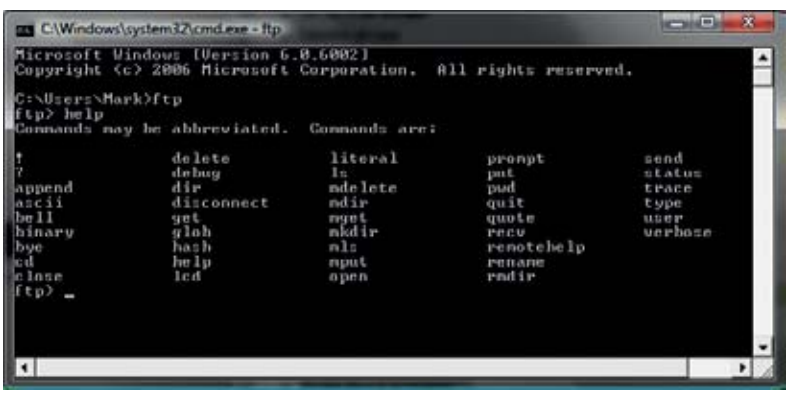

Figure 5.03 Windows® FTP client and its command set

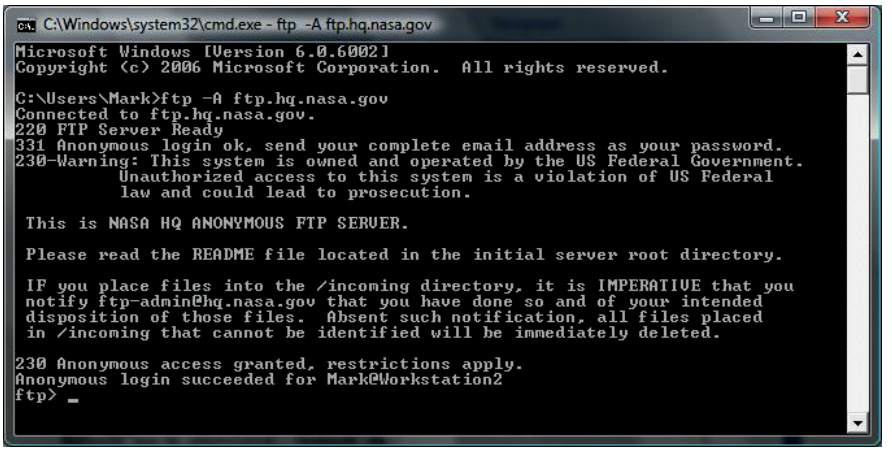

Figure 5.04 Windows® FTP client accesses the NASA anonymous FTP server

Windows® has its own **command line interface (CLI)** FTP client.

It can be accessed by opening a **command prompt** and typing 'FTP' and pressing the Enter key.

A network tool such as **Wireshark** (formerly known as **Ethereal**) can be used to examine the resulting network traffic and protocols used.

In the example shown in Figure 5.05, it should be possible to track the network communication from NASA's FTP server (198.116.65.46) to the local FTP client (192.168.123.2) using the FTP protocol. As we can see, a 220 status code indicates that the FTP Server is ready to accept further FTP commands.

Help

HTTP and FTP status/response codes

A comprehensive list of HTTP codes may be found here:

www.w3.org/Protocols/HTTP/HTRESP.html

A similarly comprehensive list of FTP codes may be found here:

kb.globalscape.com/article.aspx?id=10142

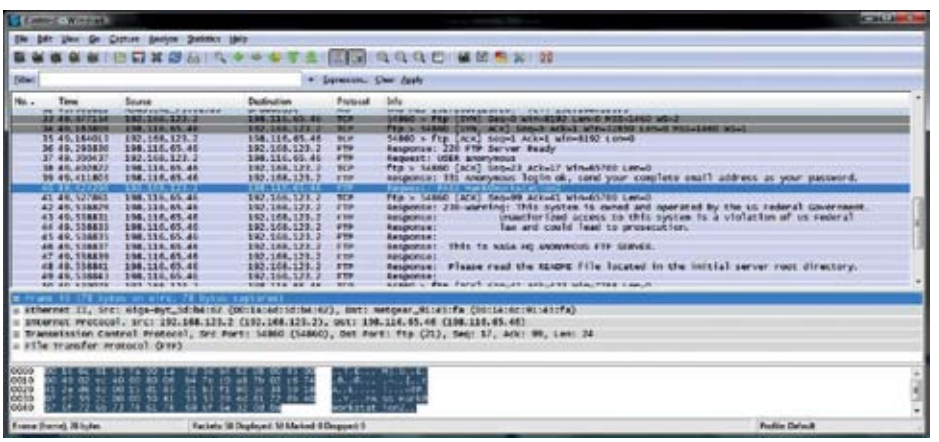

Figure 5.05 Wireshark capturing FTP traffic between the FTP server and its client

Help

Microsoft Windows XP® FTP command line client

You can find instructions here:

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ftp.mspx?mfr=true

You can find a full list of FTP commands here:

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ftp__subcommands.mspx

It is not uncommon for a network manager to enforce a strict **communications policy** that **prevents** the use of FTP clients to download files from remote servers. This is often done to reduce the likelihood of illegal downloads, virus infection or the knowing installation of prohibited software on workstations.

Such measures could be performed by simply **blocking** those network ports most commonly associated with the protocol (i.e. ports 20 and 21) on the network's primary firewall.

TFTP

As with FTP, Microsoft Windows® has native command-line interface (CLI) client support for TFTP but does not include a TFTP server (unlike UNIX and many Linux distributions).

The cross-platform example shown in Figure 5.12 demonstrates a TFTP transfer '**put**' request made from a Windows XP® client to a Linux (Fedora) TFTP server. This command will attempt to transfer a copy of a file from the local Windows XP® PC to a remote Linux workstation situation on the same network.

Firewalls on both the client and server have had port 69 unblocked for the TFTP protocol traffic.

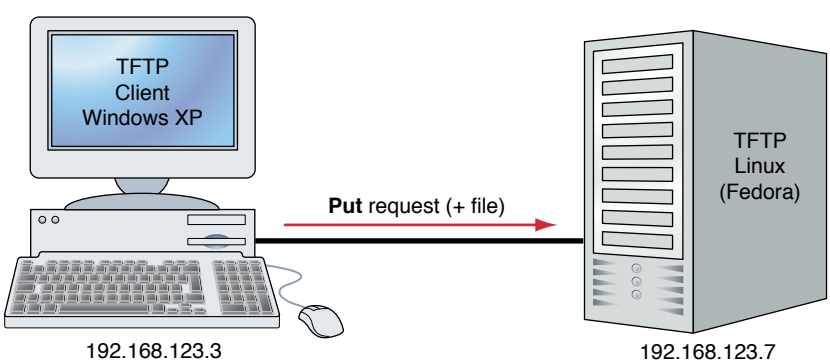

Figure 5.06 TFTP client and server

Activity 2

Using, monitoring and blocking FTP

1 Install a FTP client (e.g. OpenSight Software's Flash FXP) and download files (e.g. clipart, maps, text documents etc.) from a remote FTP server.

2 Install a network protocol analyser (such as Wireshark) to examine network traffic generated by using FTP clients.

Can you correctly identify the FTP protocol traffic?

3 Use a firewall to block network traffic on ports used by the FTP protocol.

On Windows®, a CLI is opened via the Command prompt (Figure 5.07).

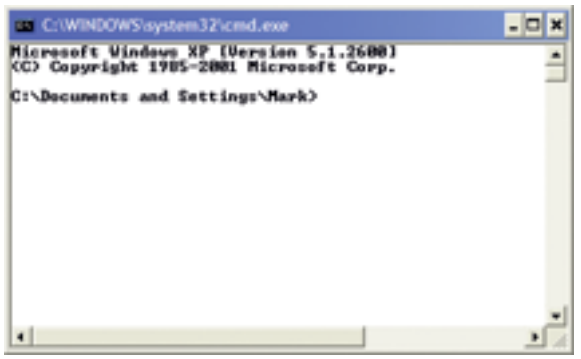

Figure 5.07 Windows® command line interface

The TFTP command is then typed – but the Enter key is **not yet pressed** (Figure 5.08).

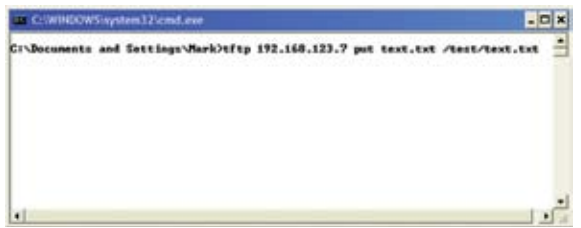

Figure 5.08 The TFTP client command is readied

This TFTP command will essentially send a text file called 'text.txt' (in the current directory) to a directory called 'test' on the Linux server.

On the Linux server, the TFTP **Server process** has to be started (Figure 5.09).

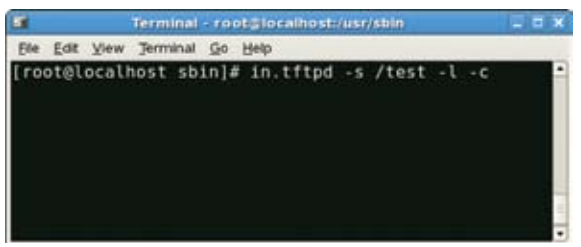

Figure 5.09 The TFTP server command is readied

(Guide to switches: **–s** Directory, **–l** Listen, **–c** Allow files to be created.)

We can examine the **background processes** ('daemons') running in Linux to see if the TFTP server is active … It is! (Figure 5.10).

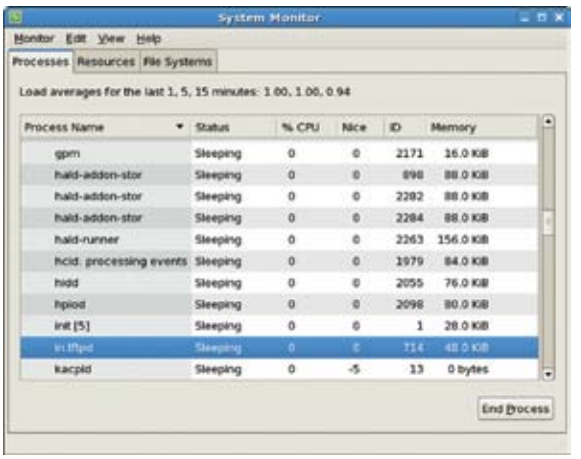

Figure 5.10 The TFTP server running as a process in the Linux Server's RAM

On the Windows® PC, we can now press Enter to execute the Put command:

Windows®' TFTP client connects to the Linux TFTP server and sends the file to the correct destination (Figure 5.11).

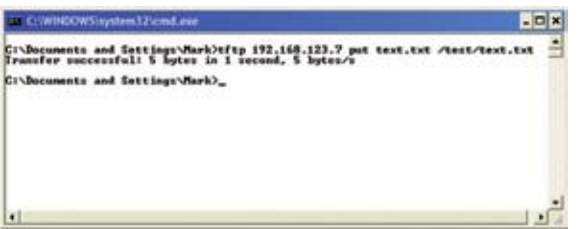

Figure 5.11 The TFTP command is executed and an acknowledgement is returned

As you can see, a short acknowledgement showing the **file size**, **time taken** and **transfer rate** (in bytes per second) is displayed.

This acts as confirmation of a successful TFTP data transfer.

Figure 5.12 shows the Linux file in its destination folder.

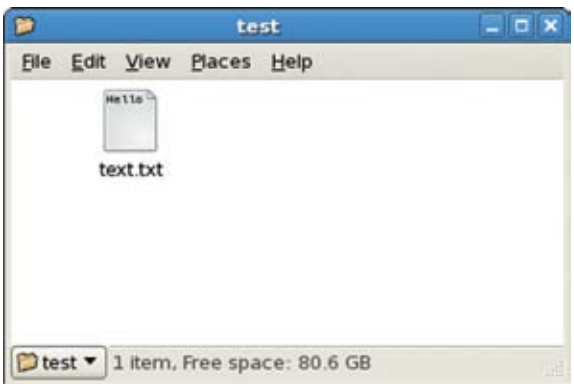

Figure 5.12 The received file 'text.txt'

Help

Microsoft Windows XP® TFTP command line client

You can find instructions here:

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tftpmspx?mfr=true

You can find a full list of Linux TFTP server commands here:

www.die.net/doc/linux/man/man8/in.tftpd.8.html

Activity 4

Changing system time with NTP

1 On either a Linux or Windows® server, request a system time update through an external NTP server.

2 Install a network protocol analyser (such as Wireshark) to examine network traffic generated by using the NTP protocol.

Can you correctly identify the NTP protocol among the network traffic?

3 Use a firewall to block network traffic on ports used by the NTP protocol.

B Braincheck 1

Match the network protocol description to its correct name!

A	For synchronising time on network clients	**1**	**SNMP**
B	For uploading and downloading files from network devices	**2**	**NTP**
C	For performing file transfers	**3**	**TFTP**
D	For returning diagnostic information on network data transfers, especially pinging	**4**	**FTP**
E	For performing network management and monitoring	**5**	**ICMP**

See the answers section for the solutions.

Activity 3

Using, monitoring and blocking TFTP

1 Use a combination of different NOS platforms (e.g. Windows® and Linux) to attempt both 'Get' and 'Put' operations with a correctly installed TFTP server and client.

2 Install a network protocol analyser (such as Wireshark) to examine network traffic generated by using TFTP clients and server.

Can you correctly identify the TFTP protocol traffic?

3 Use a firewall to block network traffic on ports used by the TFTP protocol.

5.1.4 Layout

Although LANs come in many different shapes and sizes, they generally use similar technologies and components.

The most common type of LAN is based on **Ethernet** technology, as originally devised by Digital, Intel and Xerox. This was used as the blueprint for the **IEEE's** (Institute of Electrical and Electronics Engineers) **802.3 specification**, which was released back in 1980.

Over the years a number of improvements have been made to Ethernet technology.

Wiring a building

One of the most challenging and disruptive elements of networking is installing the **cabled infrastructure**.

In simple terms, a **WAN connection** will enter the building on the ground floor. This is then piped to each floor using vertical cabling (also called the **backbone wiring**). As we have seen, backbones typically use **Gigabit Ethernet**.

On each floor a room (**wiring closet**) is set aside to distribute the backbone signals via **hubs** and **switches**. Fast Ethernet/Ethernet cables from these run from special **patch panels** into the walls and throughout the entire floor. From here, Ethernet/Fast Ethernet **patch leads** are connected from **RJ45 wall sockets** to individual workstations, servers, shared printers, photocopiers and so on.

In this way, each floor operates like a **separate star topology**, all connected via the same backbone.

Wireless technologies can provide **multiple wireless access points** through an organisation's building but the need for wired infrastructure will typically still exist.

Table 5.02

Type	IEEE standard	Speed	Connections and transmission media	Typical use
Ethernet				Max. run for 10Base-T is 100 m. Typically used for connecting workstations to switches etc., switches to switches etc.
10Base2 aka Thinnet	802.3a	10 Mbps	BNC, coaxial	
10Base5 aka Thicknet	802.3	10 Mbps	AUI, coaxial	
10Base-T	802.3i	10 Mbps	RJ-45, cat 3,4 and 5 UTP or STP	
Fast Ethernet				Max. run for 100Base-TX is 100 m. Although it can be used for connecting workstations, it is more commonly used for connecting the servers to the backbone infrastructure.
100Base-TX	802.3u	100 Mbps	RJ-45, cat 5 UTP	
100Base-FX	802.3u	100 Mbps	62.5/50 micron multimode optical fibre	
Gigabit Ethernet				Although the max. run for 1000Base-T is 100 m, both 1000Base-SX and 1000Base-LX offer long runs (275 m and 400 m, respectively). Gigabit Ethernet connections are most commonly used to provide high-speed backbone infrastructure.
1000Base-T	802.3ab	1000 Mbps	RJ-45, cat 5 UTP	
1000Base-SX	802.3z	1000 Mbps	62.5/50 micron multimode optical fibre	
1000Base-LX	802.3z	1000 Mbps	62.5/50 micron multimode optical fibre or 9 micron single-mode optical fibre	

Unit links

Topologies such as star, ring, mesh and so on are covered in greater detail in Unit 10 – Communication technologies, section 10.1.1, Computer networks.

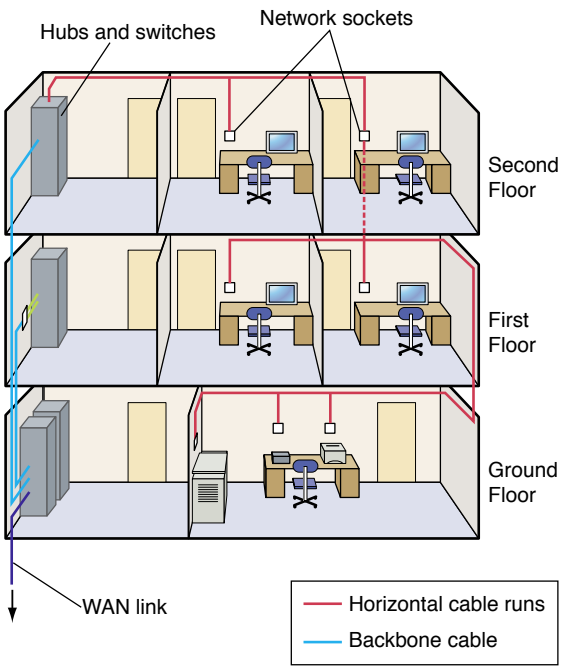

Figure 5.13 Cabled infrastructure

5.1.5 Network devices

In terms of hardware, and excluding connection media, the most common network devices are:

Servers

A number of different types of server could be placed on a network. These might include:

- **Mail server** for processing email (electronic mail) requests.
- **Web server** for processing **HTTP** (**H**yper**t**ext **T**ransfer **P**rotocol) requests for **HTML** (**H**ypertext **M**arkup **L**anguage) **files** and associated **assets** (images, video, sound etc.).
- **File server** for managing access to shared network drives and folders.
- **Print server** for managing print queues to network printing facilities.
- **Application server** for providing applications that can be shared with client workstations; they may even split some of the processing responsibility (especially for **thin clients** – see below).
- **Proxy server** for providing an **intermediary link** between (typically) the internet and client workstations on the network. For a web proxy server, it may be that a client's request is served from a **cached copy** on the proxy rather than downloading duplicated material again from the internet.
- **Workstations** – these are simple client computer systems connected to the network, these could be:
  - **a) Thick client** – a traditional workstation that has installed applications and is responsible for processing all of its own data. The only significant network communication may be generated by login authentication, remote file storage requests, email and accessing shared resources such as printers and internet access.
  - **b) Thin client** – a newer style workstation, which may be diskless, boot via the network and typically run applications from a centralised application server. Sometimes referred to as a **Network Computer** (NC) or Net PC. Citrix Presentation Server is a good example of a thin client system.

Scorecard – Thick client

\+ User experience is usually richer.
\+ Less stress on servers (so less expensive servers required).
– Difficult to standardise NOS application software across all workstations.
– Expensive as processing achieved by local resources so these costs are duplicated to each workstation.

Scorecard – Thin client

+ Easy to secure, fewer configurable options means less trouble.
+ Easy to maintain as can be server-controlled.
+ Inexpensive as processing power is required at server end (i.e. not on every client) only.
– Reliant on good and robust network to achieve processing.

- **Interconnection devices** such as bridges, hubs, switches, routers and so on.
- **Network interface cards (NICs)**, which could use standard wired media, fibre optic or wireless transmission (e.g. Wi-fi or Bluetooth).

Unit links

Interconnection devices and NICs are covered in more detail in Unit 10 – Communication technologies, sections 10.1.2 and 10.1.3.

- **Vendor specific hardware** (e.g. network monitor box).

Many network specialist organisations such as Cisco, 3Com and D-Link may manufacture proprietary **network-aware devices** for monitoring or controlling hardware functions.

An example of such specialised equipment is the Mutiny appliance server. Table 5.03 shows its monitoring capabilities.

When the Mutiny server is connected to a network, it can perform networking mapping and diagnostic functions on each network **node** it discovers (through SNMP polling).
Figure 5.14 shows an example of discovering the status of running **network services** on a node.

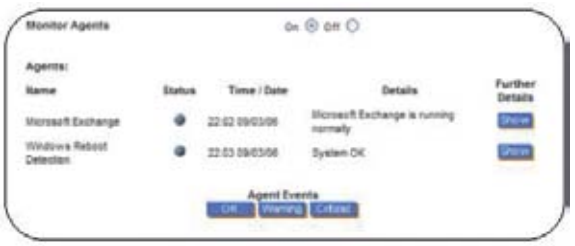

Figure 5.14 Mutiny server appliance

Table 5.03 (*Source*: http://www.mutiny.com/hardware.php)

Monitoring capabilities	
ICMP	A simple ping action determines whether the node is responding to network communications.
Interfaces	Monitors utilisation, errors and connectivity on switch and router ports.
SNMP	A poll action determines whether SNMP-based data can be retrieved from the node.
CPU load	A measure of how efficiently the node's processing unit is performing its operations.
Memory usage	The amount of a node's total memory capacity in use.
Disk usage	The amount of a node's hard disk capacity in use.
Processes	Indicates the state of the processes running on the node.
IP service	TCP layer tests for application availability.
Remote agents	Expandability and customisation, including Hardware RAID alerts.

5.1.6 Networking tools

A network manager often makes use of specialised software tools in order to make the day-to-day running of the network easier. Network Managers can also assist with making strategic decisions, for example, investing in new technology to improve poor performance that has been identified.

Make the Grade P2

P2 requires you to outline the purpose of networking tools. This is discussed in section 5.1.6.

In order to prepare an answer for this criterion, you should think about what the tool is used for rather than what the tool is called!

As a form of **Enterprise-level** software, these tools often provide **top-level** (i.e. **summary**) **information** about the state of the network but permit a '**drill down**' for specific facts when required.

Usually, these types of tools are used for either: **management of faults** or **management of performance –** although these are often intertwined!

Examples of common network management tools include the following:

Zabbix

Zabbix is an **open source** network server application (typically running on a Linux operating system) that is free to download from http://www.zabbix.com/download.php.

It can be used to **auto discover** network resources, monitor them and report errors, faults or low resource levels (e.g. RAM, hard disk space) to a network manager via a user-friendly web-based front-end.

Activity 5

Interrogating a network

Try using Zabbix to interrogate a LAN at school or college.

Discover the network topology, devices and assets available.

What steps did you take to achieve this?

Although Zabbix can use SNMP, it is also possible to install a Zabbix 'agent' service on a client computer system to provide information for the server. A bootable LiveCD version of the Zabbix server is also downloadable as are pre-compiled agents for Microsoft Windows®.

HP OpenView

Hewlett Packard's OpenView is not a single product but rather the name of a family of enterprise-level applications, which collectively provide a complete IT management solution.

Part of this suite includes comprehensive Network/System/Storage Management; giving quick information about the availability and performance of **heterogeneous** (different types of) network, server and storage assets.

CiscoWorks

Cisco System's eponymous CiscoWorks is another suite of management tools, primarily written in Java™, which help to monitor a Cisco network via web-based interfaces.

Although there are a number of separate CiscoWorks tools, for example, **I**nternetwork **P**erformance **M**onitor (**IPM**), CiscoView and **D**evice **F**ault **M**anager (**DFM**), Cisco bundles several together to form a number of packages such as **S**mall **N**etwork **M**anagement **S**olution (**SNMS**) and **L**AN **M**anagement **S**olution (**LMS**).

The LMS package is particularly useful as it integrates the process of configuring, administering, monitoring and troubleshooting a Local Area Network. It aims to:

- maximise security of the network;
- increase the accuracy and efficiency of network support staff;
- improve network availability by anticipating potential problems before they occur.

LMS achieves this by:

- creating automated tasks for managing devices;
- highlighting a network's health and capabilities;
- identifying and localising network problems.

Wireshark

Used in conjunction with **pcap** (a software utility to capture network data packets in real time), Wireshark can be freely downloaded from http://www.wireshark.org/ and can be used to analyse network traffic by host, destination and protocol used. Recognising over 100 different protocols, it can allow the network manager to investigate network traffic and transmission problems.

Activity 6

Enterprise level tools – how much?

Find out the retail price of current versions of Ciscoworks and HP OpenView.

How might this compare to the savings made by improved fault finding and performance improvements?

5.1.7 Emerging technologies

Key terms

Emerging technologies are generally accepted as being new ideas, products or services that may not yet be standardised or integrated but that are likely to have a significant impact on an industry.

This is, of course, particularly true for the IT industry as the rate of change experienced by a network manager can be simply breathtaking at times.

The early adoption of such technologies often gives an organisation a distinct business advantage over their competitors in the marketplace.

Some examples of emerging technologies are detailed below.

Server virtualisation

Virtualisation can work in a number of different ways but perhaps the most common approach is that shown in Figure 5.15.

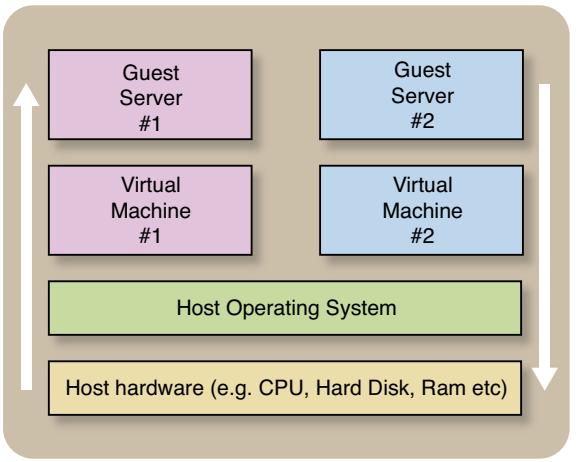

Figure 5.15 Server virtualisation

Using this technique, a physical '**host**' (a powerful computer system) creates **virtual hardware layers** for multiple '**guest**' server operating systems to use. Each server operating system thinks it is talking to its own hardware and each is effectively given its own set of resources (e.g. CPU, RAM, disk space, network connection etc.) to manage and use – but in physical terms they don't really exist. This is called the **Virtual Machine** model.

Mobile networking

The use of Wi-Fi and Bluetooth technologies have encouraged the use of **mobile networking** by removing the need for network devices to be (a) in a fixed location and (b) tethered to a single point of network access by a wired communication media.

Mobile networking is typified by the perceived shift from fixed workstations to more portable laptops, notebooks, PDAs, mobile telephones and tablet PCs.

Unit links

Wireless technologies such as Wi-Fi and Bluetooth are covered in greater detail in Unit 10 – Communication technologies, sections 10.1.5 and 10.2.5.

Web interfacing

In the past, devices were often controlled through the installation of operating system-specific applications. The disadvantage of this technique is that separate versions of the application would be needed for each different OS.

The use of **web interfacing** (as seen in Figure 5.16) where the device runs a simple HTTP service that can be controlled or interrogated via a simple web browser, is very attractive – web browsers have a recognisable and familiar user interface and are typically available on all workstations and (some) mobile devices.

Make the Grade P3 M1

These two criteria are clearly linked. P3 asks you to identify emerging technologies – a simple list with a brief description should be sufficient.

M1 asks you to describe the potential impact of these emerging technologies. The 'Emerging technologies' scorecard in this section may be helpful here. A report, presentation, leaflet or wiki may be suitable ways of evidencing these criteria.

In addition, the ability to web interface means that an organisation's network systems may be accessed, maintained and monitored remotely. This can improve productivity and timeliness of response; for example, a network administrator can repair a network issue while at home rather than travelling back to work to physically sit in front of the troubled server.

Many NOS now support the concepts of remote monitoring (see RMON) and remote desktops (e.g. as provided by Citrix, TightVNC etc.).

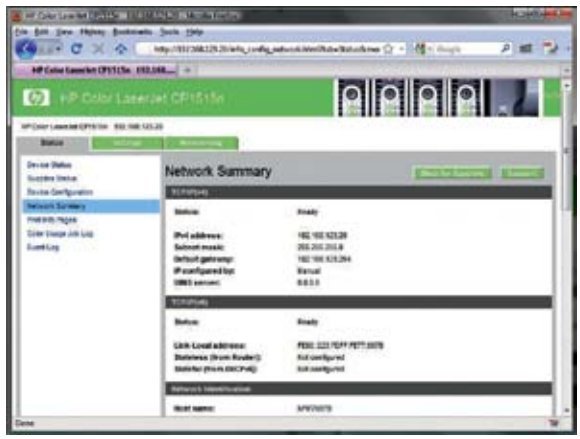

Figure 5.16 Web interfacing with a shared network laser printer

Remote monitoring (RMON)

Key terms

Remote monitoring (RMON) is a standardised monitoring specification that enables different network monitors and console systems to share network-monitoring data.

RMON can provide network managers with more freedom when selecting their network-monitoring probes and consoles, selecting and mixing features from different systems that meet their own organisational needs.

RMON's **M**anagement **I**nformation **B**ase (**MIB**) comprises nine different groups, as shown in Table 5.04 on page 18.

Table 5.04

Group	Responsibility
Statistics	Provides raw network traffic statistics about a networking device.
History	Creates a historic network data sample over a period for future analysis.
Alarm	Compares monitored values against an allowed threshold, raises an event if this value is dangerously exceeded.
Host	Contains information about each device (usually a server or workstation) that is discovered on the network.
HostTopN	A prepared table of 'top' hosts based on recorded statistics.
Matrix	Can track conversations between two devices based on selected addresses.
Filters	Permits traffic to be selected for future processing based on a given criterion.
Packet capture	Captures network traffic.
Events	Controls the logging, handling and raising of an exceptional event as experienced by a device (possibly as the result of an alarm).

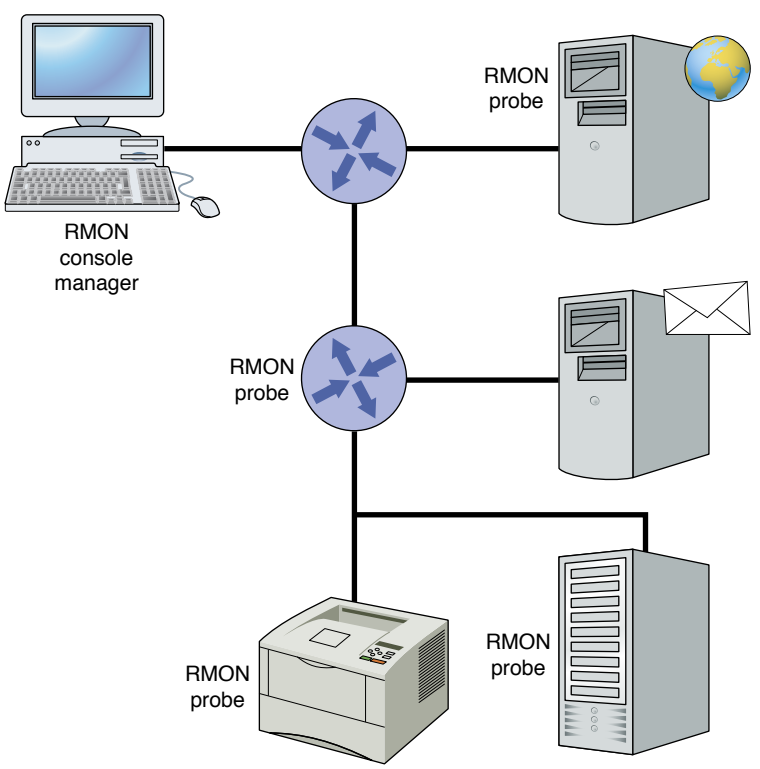

Figure 5.17 RMON agents reporting back to console manager

RMON works when each device runs an **SNMP-compliant agent** (known as a '**probe**') which reports back to a workstation running a suitable monitoring application (known as the '**console manager**') when it encounters odd behaviour (Figure 5.17).

VoIP

Key terms

Voice over Internet Protocol (VoIP) is a popular emerging technology that is used to transmit ordinary telephone calls over an organisation's privately managed intranet or the publicly available internet using **packet-switched** routes. This feat is usually achieved without any perceptible loss of signal quality.

It is also called **IP telephony**.

Unit links

VoIP is also examined in Unit 10 – Communication technologies, section 10.3.1.

Web2.0

As the name suggests, **Web2.0** is a popular term used to describe the improvements in web technologies, content and usage that are needed to improve the World Wide Web's (WWW) social integration and business functionality.

The term 'Web2.0' was originally coined by O'Reilly Media back in 1994.

Web2.0 is thought to encompass such second generation WWW concepts and elements as:

- improved social interaction (as a business opportunity);
- use of web-based and web-served applications;
- encouragement of business through services and **micro-transactions** (commerce between end users);
- improved functionality and usability;
- improved level of user interaction;
- improved rationalisation and categorisation of information (e.g. use of newsfeeds);
- embrace of new development technologies such as AJAX, XML, CSS, Open Source solutions such as LAMP (Linux, Apache®, MySQL and PHP).

5.1.8 Impact of emerging technologies

Adoption and integration of emerging technologies into an organisation can lead to:

- enhanced network capabilities (e.g. faster solutions, larger storage capacities, faster access);
- improved management information and capabilities;
- better information on which to plan future network developments;
- new workflows (e.g. home working over VPNs).

Emerging technologies scorecard

Server virtualisations

\+ Reduces **'server sprawl'** by reducing quantity of server boxes.
\+ Improves ability to test servers.
\+ Can improve disaster recovery.
\+ More accurate control and allocation of server resources.

Mobile networking

\+ Increased flexibility, workflows can be more adaptable.
\+ Equipment can be shared more easily (not limited to cable runs).
– Reduced security – it's harder to secure from outside threats.
– Equipment more portable so can become damaged, stolen or lost.

Web interfacing

\+ Instant user familiarity with interface.
\+ Easy 'as needed' deployment – application version is always current.
\+ Processing is mainly server-side, giving possibility of thin client use.
– Limits to web-based environment (e.g. cannot harness full hardware capabilities).

Remote monitoring (RMON)

+ RMON helps to spot problems before they occur (and trouble users).
+ No need to visit equipment; it's possible to manage remotely.
+ RMON only reports when alarms trigger an event; this generates far less network traffic than continually polling each device to see how it's working (RMON is more autonomous).

VoIP

+ Increases network utilisation (improves value-for-money).
+ Reduces need for licensed telephony system (saves money).
+ Improves telephone service (more organisational control).
– Requires power for network.
– Some audible silences occur due to packet-based nature of the network traffic; 'late' packets may be dropped in periods of heavy usage.

5.2 Understand network management functions

This section will cover the following grading criteria:

P4 P5 M2 D1

Make the Grade P4 M2

P4 asks you to explain the functions of network management – this is essentially covered throughout section 5.2.1 and could be evidenced through a presentation, a leaflet, a poster or a written report.

M2, which is linked to P4, asks you to explain the goals of fault management. Remember, this isn't about explaining the faults, just what you as a network manager are trying to achieve through proactive fault management.

5.2.1 Network management functions

The initial phase of management function is to plan, design and install the network.

Let's examine each of these stages in turn.

Planning a network

The goals of a network are reasonably simple to understand.

Networks should:

- provide the services required by their end users;
- improve communications within an organisation;
- improve sharing of resources within an organisation;
- provide these services with acceptable response times;
- be cost effective and within a planned and agreed budget;
- work reliably and flexibly;
- be expandable without requiring major changes;
- be easy to manage on a day-to-day basis;
- have good support documentation.

Networks represent an expensive but necessary investment for modern organisations; as such it is very important that planning is performed in a responsible and thorough manner. Any mistakes made in the planning and design phases could have costly repercussions later.

This phase links neatly to the design phase.

Designing and installing a network

Planning and implementing new networked solutions can be a mission-critical undertaking, with many of the organisation's internal functions (e.g. purchasing, manufacturing, sales, payroll, communication etc.) relying on the development of a robust and reliable system.

The stages of a new network resemble (to a degree) a typical **system life cycle** or **program development** cycle as shown in Figure 5.18.

Table 5.05 shows each stage in more detail.

In addition, once the network has been installed, the network manager has to cope with a number of different issues that relate to its day-to-day running.

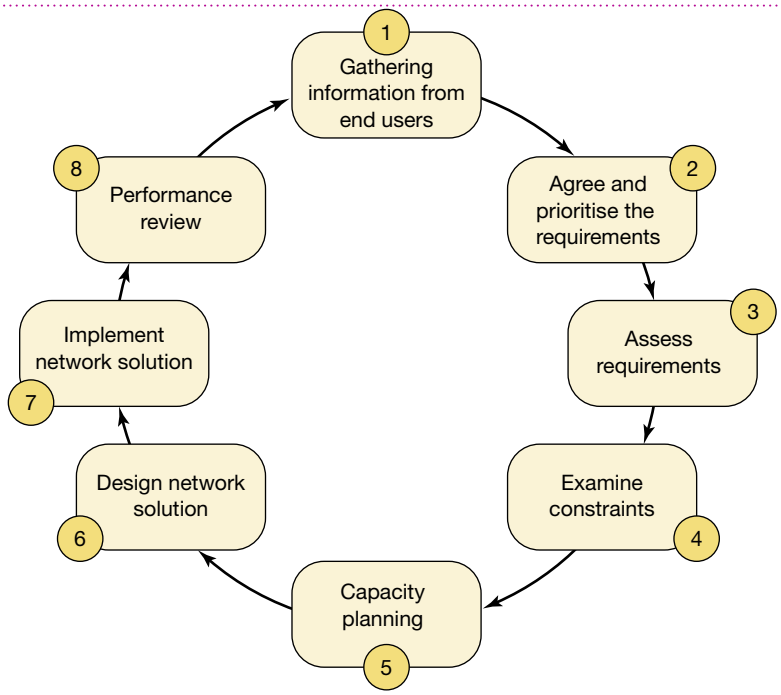

Figure 5.18 Network life cycle

Table 5.05

1	Gather information from end users	Find out which services (e.g. email, internet access, online sales etc.) are required by end users.
2	Agree and prioritise the requirements	Define which requested services and features are critical ('must haves'), which are desirable ('would be nice') and which are worth noting but are either luxuries or possible future developments.
3	Assess requirements	It is necessary to assess all the requirements which have been identified so that requirements (what is wanted) can be converted into deliverables (what will be paid for and completed). Things that will affect the decision: • Commissioning costs (getting the project started); • Project management fees; • Hardware costs (including upgrades, new purchases and safe disposal of old equipment); • Software costs (including NOS – see section 5.1.1); • Consultancy costs; • Ongoing support and maintenance costs; • Training costs.
4	Examine constraints	Obvious limiting factors such as time, money etc. However, there may be other physical constraints such as cable installation (if for example the premises are old or of historic significance it may be more appropriate to envisage wireless networking), issues for placement of new servers or equipment.

5	Capacity planning	The anticipated and required capacity of the network has a big impact on the network design and implementation stages. Good planning accounts for capacity load and therefore maximises resources and provides a good, reliable service to the organisation's internal (employees) and external customers. Capacity planning should look at: • User needs and populations (i.e. maximum potential simultaneous logins) • Application behaviour (its generated network traffic) • Identifying baseline network requirements • Project heaviest network loading (identify potential bottlenecks) • Constraints on performance (equipment, transmission media) Without a live network to test this, special **projection analysis** tools may be needed. Alternatively, a small study and 'test' network may be created to simulate the issues.
6	Design network solution	Need to plan a solution that covers: • Servers and workstations • NOS, tools and application selection • Selection and placement of network devices • User groupings and their needs • Network services required • Capacity needs identified • Cabling infrastructure (topology) • External links for internet connection • Security • Impact on organisation • Contingency plans (what to do when things go wrong) • Schedule of deployment (e.g. Gantt chart) All choices and reasoning should be fully justified and documented. The design may go through many changes (it's an **iterative process**) before it is finally refined and agreed by all concerned parties. Each modification should be documented in a **change log** for future reference.
7	Implement network solution	Implementation will probably be **phased** (i.e. in stages). Start by educating employees by telling them what to expect (workflow changes, disruption during installation etc.), the benefits of the network, what they can do to help etc. **Pilot installations** may be attempted and these could be tested by end users to discover possible problems, performance issues etc. This is called **acceptance testing**. Full implementation will typically include: • Purchasing • Cable infrastructure installation (this may be performed by an external agency for speed purposes) • Networking device installation and configuration • Server installation and configuration (e.g. mail server, intranet etc.) • Domain and user account configuration • Installation and configuration of required network services • Creation of log-in scripts • Quality of Service (QoS) configuration for important data/services • Training

8	Performance review	Examining and reviewing network performance is critical. Performance variables to look at include: • Network data **throughput** • Network **collisions** and **congestion** • **User response times** (log-in, file transfers, email requests etc.) • **Line utilisation** • **User satisfactions** (through focus groups, questionnaires, online surveys or feedback etc.) The use of network monitoring tools (see sections 5.1.6, 5.3.2) will certainly help this process and enable the network manager to modify the network and improve its performance.

Make the Grade P5

P5 requires you to interrogate a network to identify its assets and their configuration; it's clearly a practical task.

Any tool that collates SNMP data should used here (e.g. Zabbix) and evidence could be screen captures from its web-based interface showing the network topology, its connected devices and their assets.

These include:

- Configuration
- Fault management

Make the Grade D1

D1 is a more complex assessment criterion as it asks you to justify the inclusion of performance management activities within a network manager's role.

You should ideally link to aspects of both performance management and fault management as the two are often related (e.g. examining performance variables often identifies early faults and can prevent these from happening, in turn ensuring a good quality of network service for its users).

Your response here is likely to be in the form of a report or a presentation.

Whether faults occur through failure (e.g. hardware) or poor configuration (e.g. software or user settings), there are essentially four key elements of network fault management:

- detecting the fault;
- recognising the cause of the fault;
- correcting the fault;
- logging the fault and its solution to help trend analysis (i.e. is there a pattern forming?)

The goals are clear:

1. Reduce frequency and severity of network faults by
2. early detection of network issues and
3. timely prevention through proactive network management.

See the part of section 5.1 relating to networking tools for useful ways of identifying network faults.

- Account management (see section 5.3.1)
- Performance management

Any network will generate usable performance data over a period of time. Certain variables can be examined and tracked to enable network management decisions.

Typical performance variables, often gathered through SNMP (see Table 5.01 on page 5), include:

- network throughput – volume of data being transmitted over a timed period;
- network response times – time taken for users to receive network replies to requests made;
- link utilisation – how busy network connections are;
- server loading – typically CPU, RAM and hard disk usage on a network server.

- Security
- Reporting

Braincheck 2

1. From where is information for a network's requirements gathered?
2. What is the difference between a critical and a desirable feature?
3. Name three concerns that will affect requirements assessment.
4. What is a constraint?
5. Name two concerns that contribute to capacity planning.
6. Name five items that should be part of a network design.
7. What is the first recommended stage of network implementation?
8. What is QoS?
9. Name three different types of performance variables.
10. What type of software can be used to gather performance variables?

See answer section for the answers to these questions.

Design considerations

When designing a network, there are a number of different aspects that should be taken into consideration:

- **Speed**
  How much bandwidth is required?
  What kind of media is required to support this speed?
  How expensive is this type of media?
  What kind of data will be transmitted over the network?
  What kind of response times are wanted by the end users?
  What is the slowest response time/data transfer rate tolerated?
- **Usability**
  Is the network quick and easy to use? Does it reward a user's investment of time?
- **Functionality**
  What types of functions will the network support?
  Does the functionality meet the identified needs of the end users?
  Will the network functions have room to grow (scalability)?
- **Cost**
  How much will the design cost?
  How much will the implementation cost for:
  – transmission media
  – network devices
  – servers
  – software (NOS, applications, licensing agreements etc.)
  – installation (wiring and infrastructure)
  – ongoing maintenance
  – upgrading
  – leasing of external lines (if required).
  How much will the installation disruption cost the organisation?
  How much will training cost?
  How much will upgrades and maintenance cost?
- **Flexibility**
  Will the network be able to alter, shrink or grow to meet changing organisational needs?
  How easy will it be to alter the network configuration:
  – **physically** – wiring and infrastructure, new hardware (servers, network devices);
  – **logically** – upgrade of NOS, email facilities, security requirements, applications etc.?
- **Available expertise**
  Does the organisation have enough internal expertise to design the network?
  Does the organisation have enough internal expertise to implement the design?
  Does the organisation have enough internal expertise to maintain and manage the live network?
  If the answer to any of these questions is 'no', can the organisation buy in experience through external contractors (a short-term solution), recruit new staff or train existing staff?
- **Complexity**
  This tends to increase with size; size increases with demand. Is the proposed solution scalable and still manageable?
- **Security requirements**
  Typically involves the creation of a **communications policy**, which determines a user's rights and an organisation's expectation of **responsible usage**.
  This may include such aspects as:
  – user rights and privileges
  – password creation and confidentiality
  – software installation
  – desktop customisation and system configuration

- use of removable media (e.g. floppy disks, USB flash drives, CD-ROM, DVD-ROM)
- creation and content of email (both for internal and external use)
- downloading files from the internet
- internet activities (also see below)
- any legal responsibilities covered under the Data Protection Act, Computer Misuse Act etc.

It would be likely that a new employee would be introduced to this policy during their induction and asked to obey its guidelines. Where employees fail to abide by the policy, evidence (through **logging** or **computer forensics**) may be required to provide suitable proof in any disciplinary matter. It may be the network manager's responsibility to collect such information. In addition, the network itself would require both logical and physical security.

This may include such protections as:

- firewalls (hardware or software)
- use of 'Honeypot' or 'Honeytrap' servers to lure and frustrate unsuspecting hackers
- user authentication services (including emerging technologies such as biometrics)
- anti-virus software
- anti-spyware software
- network traffic logging
- network traffic filtering
- diskless workstations
- encrypted data traffic
- locked servers and server rooms
- regular backup of application data (some off-site)
- regular audit of network assets (hardware, software etc.)
- regular monitoring of network performance (to detect bottlenecks, emerging problems etc.)
- use of UPS (Uninterruptible Power Supplies)
- use of subnets for greater control of network traffic
- regular installation of fixes and patches to software to protect against security flaws
- correct set-up of security on wireless broadcast devices (i.e. encryption, antennae strength etc.)

- **Internet access**
  Is internet access actually needed?
  If so, what types of services are required?
  What sort of services should be prohibited (see Security requirements on page 24)?
  Who should have internet access: all members of staff or just selected groups?
  Should internet access to non-related material (i.e. websites) be permitted? If so, when?

5.3 Be able to carry out network management activities

This section will cover the following grading criteria:

P6 M3 D2

Make the Grade P6 M3

P6 requires you to undertake routine management tasks – this is clearly a practical task so could be evidenced through screen captures, photographs or videos.

In terms of what constitutes a routine maintenance task, you should focus on those activities listed in section 5.3.1 and how these are achieved in the network operating system you use in your classes.

M3 is a natural extension of this task as it asks you to keep accurate records of the management tasks you have performed. A written log, wiki or blog could be sufficient here.

5.3.1 Regular maintenance activities

Network management and day-to-day administration often involve the same types of activities.

These activities occur as a direct result of network usage and changes in organisational need (e.g.

Unit links

For more on security concerns please refer to Unit 7 – Organisational systems security. Aspects such as anti-virus and patches are also discussed in greater detail in Unit 2 – Computer systems.

new departments, employees, hardware, projects etc.). As such they are hard to avoid!

User account creation and deletion

The creation of **user groups** and **individual user accounts** is a vital aspect of network management.

The rights and privileges granted to a user as part of their account contributes to:

- the functionality they can access (i.e. which applications they can use, devices they can install)
- the data they can see (i.e. which files and folders they can access)
- the configuration and customisations they can make
- the shared resources (e.g. printers) they can use.

In addition, the use of user accounts and the individual responsibilities they bring contribute many of the practical aspects of any network security policy.

It is important that network accounts be managed regularly by updating rights and privileges where required (for example as a result of an employee being transferred to a management group through promotion) and deleting accounts of employees who have left the company. The latter is vital, especially if the individual has left under poor relations with the organisation (it is not unknown for an ex-employee to maliciously damage data or systems if the opportunity presents itself).

Key terms

A **login script** is a set of instructions (usually written in a scripting language, e.g. VBScript or a command line batch file for Microsoft Windows® NOS) that forces a networked workstation to perform specific actions when the user logs into their account.

A **default login script** is often created when a user account is created, based on the set actions required by the user group to which that user belongs. This can then be modified and personalised by the network manager or administrator as part of the user's **network profile**.

Login scripts are a key component of a network's security strategy and form the basis of the user's initial settings when they log into a workstation. Common elements of login scripts are:

- mapping network disk drives or folders to local logical device names. e.g. `net use G: \\MyFileServer\SMITHJO1`.
- redirecting printer output to a shared network printer e.g. `net use LPT1: \\MyPrintServer\HPLaser`.
- fixing a specified (organisational) screen saver or desktop wallpaper
- deleting temporary files
- automatically launching programs from the command line (e.g. monitoring programs).

It should also be noted that some NOS also permit **logoff**, **startup** and **shutdown** scripts.

File system maintenance

Routine maintenance should be performed on all native file systems.

This should include operations such as:

- anti-virus signatures
- back-up of settings, data files etc.
- file clean-up.

It is likely that these operations would be scheduled to run automatically at periods of low network activity.

5.3.2 Tools

We have already discussed networking tools for successful management in section 5.1.

You should gain some practical experience in using some of these tools; Zabbix and Wireshark form a particularly useful pair of tools as both are free to download and when used together provide much of the functionality required for day-to-day network administration.

5.3.3 Documentation

Documentation is a vital activity as it is the best way of creating a **knowledge base** for identified network problems, solutions and 'workarounds'.

A number of different forms of documentation are likely to occur:

- **Network design**
  Documentation as generated by the design phase in section 5.2.1. It should include full details of:
  - physical layout (cabling, topology, location of servers, networking devices, clients etc.)
  - network configuration (IP addresses, domain details etc., groups and users)
  - external linkage (e.g. leased lines, WAN connections, DNS – Domain Name Servers etc.)
  - application settings
  - administration/management information (administration passwords etc.).
- **Work logs**
  Acting as maintenance documents, work logs should provide auditable proof of:
  - the name and location of the device affected (model, serial number etc.)
  - who reported it?
  - when it was reported?
  - network problems (symptoms) reported
  - network faults diagnosed and then identified
  - solutions applied (in detail so that they can be referred to in the knowledge base)
  - who fixed the problem?
  - when was the problem fixed?
  - what resources were used to fix the problem?
  - whether user acceptance has been given.
- **Log resources and system testing**
  As with any maintenance duty, network repairs should be fully tested to make sure that the fix is reliable and that there are no consequential 'knock-on' effects. The use of service logs (e.g. HTTP logs, NOS event logs, FTP logs, network protocol traffic data) can also be used to check that devices are working correctly.
- **Upgrade plan (road map) or IT strategy document**
  As a vital component of an organisation's overall IT strategy, an agreed development route for network services is of paramount importance, particularly in terms of expansion and increased flexibility (e.g. taking advantage of emerging issues such as VoIP).
  It will inform business plans, purchasing, growth and capacity planning.

Make the Grade D2

D2 requires you to design a network security policy for a small organisation.

This should logically address aspects of sections 5.3.5 and 5.3.6 and is likely to be either presented as a written document (for employees to sign) or a web page (for the organisation's intranet).

Some useful templates are available from: www.sans.org/security-resources/policies/

5.3.4 Configuration options

A network manager will be expected to carry out the following operations:

- **user account location**
- **server and settings**
- **drive mappings**
- **virus scanning options**.

5.3.5 Security features

Consideration of security features is also vital for successful network management. This may involve such aspects as:

- **VPN access** – management of encryption, user accounts etc.
- **firewall management** – regular update of blocked websites, protocols, IP addresses etc.
- **access control lists** – setting access rights on network objects: users, devices, files, programs etc.
- **device hardening** – updating with security patches, switching off unused features, logging activity, changing default password etc.
- **policy review** – continuous review of policy, which adapts to meet changes in network usage, activity levels, faults or trends in unauthorised access.

5.3.6 Security policies and procedures

As noted in section 5.3.5, policies and procedures should be continually reviewed. This may have a knock-on effect for user access and their effective network rights (e.g. you may have to limit them further).

Other considerations should include:

- **penetration testing** – authorised checks on security by allowing **ethical security testers** to try 'cracking' network security to find vulnerabilities
- **security audits** – when they occur, what is recorded, what is reported and how often it occurs
- **access control lists review** – an examination of current network object security; does anything have to change?

Braincheck 3

1. Name three types of network server.
2. Name two examples of Enterprise-level network management software.
3. Give the speeds of Ethernet, Fast Ethernet and Gigabit Ethernet.
4. What is vertical wiring/cabling also known as?
5. What is the difference between a thick and thin client?
6. Give three different emerging technologies.
7. What is RMON?
8. Name three different aspects that might be in a login script.
9. Name three entries that might form part of the network design.
10. What are the three goals of fault management?
11. Name five entries that might be on a work log.
12. Name three aspects of network security.
13. What is penetration testing?

How well did you do? See the answer section.

Unit links

Unit 5 is a **mandatory unit** for the Edexcel BTEC Level 3 National Diploma and Extended Diploma in IT (Networking and Systems Support pathway) and **optional** for all other qualifications and pathways of this Level 3 IT family.

Qualification (pathway)	Mandatory	Optional	Specialist optional
Edexcel BTEC Level 3 National Certificate in Information Technology		✓	
Edexcel BTEC Level 3 National Subsidiary Diploma in Information Technology		✓	
Edexcel BTEC Level 3 National Diploma in Information Technology		✓	
Edexcel BTEC Level 3 National Extended Diploma in Information Technology		✓	
Edexcel BTEC Level 3 National Diploma in IT (Business)		✓	

Qualification (pathway)	Mandatory	Optional	Specialist optional
Edexcel BTEC Level 3 National Extended Diploma in IT (Business)		✓	
Edexcel BTEC Level 3 National Diploma in IT (Networking and System Support)	✓		
Edexcel BTEC Level 3 National Extended Diploma in IT (Networking and System Support)	✓		
Edexcel BTEC Level 3 National Diploma in IT (Software Development)		✓	
Edexcel BTEC Level 3 National Extended Diploma in IT (Software Development)		✓	

Achieving Success

This particular unit has 11 criteria to meet: 6 Pass, 3 Merit and 2 Distinction.

For a Pass:	You must achieve all 6 Pass criteria.
For a Merit:	You must achieve all 6 Pass and all 3 Merit criteria
For a Distinction:	You must achieve all 6 Pass, all 3 Merit and both Distinction criteria.

Further reading

Burgess, M. – *Principles of Network and System Administration, 2nd Edition* (John Wiley and Sons Ltd, 2003) ISBN 0470868074

Limoncelli, T. and Hogan, C. – *The Practice of System and Network Administration* (Addison Wesley, 2001) ISBN 0201702711

Olifer, N. and Olifer, V. – *Computer Networks: Principles, Technologies and Protocols for Network Design* (John Wiley and Sons Ltd, 2005) ISBN 0470869828

Subramanian, M. – *Network Management: An Introduction to Principles and Practice* (Addison Wesley, 2000) ISBN 0201357429

Websites

www.cisco.com

www.crest-approved.org