UNIVERSITY
OF LONDON

Data communications and enterprise networking Volume 2

P. Tarr

CO2222

2005

Undergraduate study in
Computing and related programmes

Goldsmiths
UNIVERSITY OF LONDON

This guide was prepared for the University of London by:

P. Tarr

Acknowledgements

I am indebted to David Brownrigg, Ida Pu, Iain Sharpe and my son, Greg, for reading the draft of this subject guide and providing helpful comments and advice. P. Tarr, May 2005

This is one of a series of subject guides published by the University. We regret that due to pressure of work the author is unable to enter into any correspondence relating to, or arising from, the guide. If you have any comments on this subject guide, favourable or unfavourable, please use the form at the back of this guide.

In this and other publications you may see references to the 'University of London International Programmes', which was the name of the University's flexible and distance learning arm until 2018. It is now known simply as the 'University of London', which better reflects the academic award our students are working towards. The change in name will be incorporated into our materials as they are revised.

University of London
Publications Office
32 Russell Square
London WC1B 5DN
United Kingdom

london.ac.uk

Published by: University of London

© University of London 2005

The University of London asserts copyright over all material in this subject guide except where otherwise indicated. All rights reserved. No part of this work may be reproduced in any form, or by any means, without permission in writing from the publisher. We make every effort to respect copyright. If you think we have inadvertently used your copyright material, please let us know.

Contents

Chapter 1: Introduction

1.1 Aims and objectives

The CIS222 unit aims to provide you with a good grounding in data communications and enterprise networking. It is a Level 2 unit, building on material taught in Level 1 units. The unit concentrates on breadth of understanding rather than depth, and attempts to cover a wide range of networking topics by means of a structured high-level approach. If you desire a deeper understanding of any of the topics covered in this subject guide, you should refer to the recommended texts.

Networks have become increasingly important in recent years. Hardly any applications are now stand-alone. Most applications communicate over a network, either between a client PC and a server in the same building over a Local Area Network or between computers in different cities, countries or continents over a Wide Area Network. The study of networks and applications that make use of networks is now an important part of any undergraduate computer science programme. An understanding of how networks operate will be useful in any computing career you may choose to follow.

The main objective is for you to build a logical framework in which networking topics can be studied, analysed and understood. This will stand you in good stead if you subsequently work in the computer or networking industry and have to design, develop or manage systems that make use of networks. This subject, like many in Computer Science, develops rapidly and new network protocols and technologies are emerging all the time. If you have built a framework which you then can use to analyse and understand these new developments, this will ultimately be of more use than a detailed understanding of current technologies.

A further objective is to help you be able to make informed choices amongst the many competing technologies that are available in the marketplace, if in a subsequent career you are required to make such choices.

The CIS222 unit replaces the CIS208 unit entitled ‘Telecommunications and computer communications’. Some of the material in the CIS208 unit has become very dated, as new technologies have emerged and data transmission speeds have increased way beyond what was imagined possible 10 years ago. Certain promising technologies which were considered important in the CIS208 unit have also failed to come into widespread use, mainly as a result of the phenomenal success of the Internet which did not have a very high profile in CIS208. As a result of this, the new CIS222 unit unlike CIS208 is very much focused on the Internet and its protocols.

1.2 Learning outcomes

On completion of this unit you should be able to:

- describe the technologies deployed in enterprise networks and make informed choices among the competing technologies
- explain how enterprise networks are managed with particular emphasis on performance and security management
- design and cost simple enterprise networks that meet specified requirements
- demonstrate transferable skills in spreadsheet modelling.

1.3 Course outline

The CIS222 unit consists of two distinct parts, which correspond to the two volumes of the subject guide. The first part of the unit is called 'data communications' and is an introduction to the terms, concepts and network architectures required to understand how data is transmitted through communications channels and networks. This, of necessity, requires a technical approach and some knowledge of the physics of transmission as well as the study of network architectures and protocols. The second part of the unit is called 'enterprise networking' and is more concerned with the design and management of networks used by businesses and other large organisations. It therefore concentrates more on the business and management issues that arise.

This volume of the subject guide is more business focused than Volume 1, but does still have a significant technical content. It concentrates on network technologies used by enterprises. It includes a study of the network marketplace and the different products and technologies considered and used by enterprises in designing, building and managing networks. This volume contains eight chapters. This chapter will introduce the unit. Chapter 2 will introduce some marketing concepts and will analyse the main types of company that market network products. The next three chapters will build on material presented in Volume 1 to examine specific technologies used in enterprise networking. Volume 1 followed a top-down layered approach, but in these chapters we will discuss technologies that cross many layers or do not fit neatly into the hybrid reference model that we are using. Chapter 3 will examine technologies used by Personal Area Networks (PANs), Storage Area Networks (SANs) and Local Area Networks. Chapter 4 will examine the technologies used by Metropolitan Area Networks (MANs) and Wide Area Networks (WANs). Chapter 5 will examine how these technologies can be integrated into a single cohesive internetwork and will include studying aspects of IP networks, particularly routing, that were not considered in Volume 1. Chapter 6 will consider the exacting requirements of multimedia networking and the attempts to re-engineer the Internet to meet them. It will also examine Asynchronous Transfer Mode as an alternative technology for multimedia networking. The final two chapters return to a more business-oriented approach. Chapter 7 will consider the task of designing enterprise networks and some of the techniques that network designers use. Finally, in Chapter 8, we will examine how enterprise networks are managed using the ISO[1] Network Management Framework, concentrating on performance and security management, as these are the areas that cause most concern to network managers today.

This subject guide will contain practical activities that can be carried out to gain further understanding of the topics covered in the unit. These activities can be carried out in a laboratory or at home. You are strongly advised to spend time on these activities, as the extra insight you will obtain will stand you in good stead for the examination, and any coursework assignments.

1.4 How to use this subject guide

This subject guide is intended to provide a logical structure in which to study the subject of enterprise networking. It is not intended to replace your need to read around the subject to improve your understanding. You may wish to

[1] *International Organization for Standardization.*

follow some of the further reading referenced at the start of each chapter. An alternative or supplement to the further reading is to follow the links on the course web site[2] to study the topics in each chapter.

How to best use this subject guide will depend on your personal approach to study and whether you are studying on your own or at an institution.

One suitable approach would be to start with reading a chapter of the subject guide, followed by some of the further reading, if any of the material has not been understood or more information is desired. Then attempt the sample exam questions at the end of the chapter, which can be checked with the model answers and hints in Appendix B, before reading the learning outcomes. If you feel that these have not been fully achieved, go back to the further reading or to the web links, in order to make sure that you have understood each topic. You should also carry out the activities in each chapter, as they provide further insight to the topics being studied.

This subject guide makes use of a large number of acronyms. When a new acronym is introduced, it is expanded in full. Subsequent references will often just use the acronym. A list of acronyms used in the subject guide can be found in Appendix C.

1.5 Reading list

Because of the very varied material presented in this unit, there is no one book that covers the whole unit (or even the majority of it) and that can be recommended for essential reading. You may wish to obtain your own copy of one of the general networking books listed below or use library books and web sites for further reading material.

Canavan, John E. *Fundamentals of Network Security.* (Artech House), first edition, 2001.

Carr and Snyder *Management of Telecommunications.* (McGraw Hill), second edition, 2003.

Fitzgerald and Dennis *Business Data Communications and Networking.* (John Wiley and Sons), eighth edition, 2005.

Forouzan, Behrouz, A. *Data Communications and Networking.* (McGraw Hill), third edition, 2003.

Kurose and Ross *Computer Networking – A Top Down Approach featuring the Internet.* (Addison Wesley),third edition, 2005.

Porter, Michael *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* (Free Press), 2004.

Stallings, William *Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003.

Tanenbaum, Andrew S. *Computer Networks.* (Prentice Hall International), fourth edition, 2002.

1.6 Useful web links

The world wide web is a very dynamic medium and publishing a large number of web links in a subject guide is likely to result in the frustration of a ‘File Not Found’ response at some point in the future. Instead, an up-to-date list of useful links relevant to the unit will be maintained on the CIS222 course web site at

http://doc.gold.ac.uk/∼mas01pt/cis222/study/volume_2 .htm

In the event of this URL changing during the life of the subject guide, please follow the links to the author’s home page from the staff page of the Goldsmiths’ Department of Computing web site, and then follow the link to this page.

[2] *http://doc.gold.ac.uk/~mas01pt/cis222.*

Two links are particularly useful:

http://www.rfc-editor.org/rfc.html
contains the full text of all the Internet standards which are known as Requests for Comments (RFCs [3]).

http://www.protocols.com/protocols.htm
contains descriptions of most network protocols.

1.7 Study time

If you are studying this unit full time then it should take approximately one quarter of your total study time for an academic year. In a typical institution you will probably spend about four hours per week on each unit during term time in formal teaching. It is recommended that you spend at least three hours per week in reading and private study. You should also on average spend a further three hours per week in attempting sample exam questions at the end of each chapter and in doing the activities, plus formal coursework, in the lab or at home. If you are studying entirely on your own, then you should aim to spend an additional four hours per week in private study, to compensate for the hours that students in institutions receive formal teaching.

You should aim to spend a total of 300 hours on the whole unit, including formal teaching. This total should also include time spent revising during reading weeks, vacations and prior to examinations. This time is applicable to an average student who aims to do well in the unit. Some students who work more slowly may need to devote more time than this.

In order to complete this volume of the subject guide in one (10-week) term, you should aim to complete one chapter per week. This will leave two weeks spare for consolidation at the end or to allow for some slippage.

If you are studying part-time, over a longer period than one term, then you will have to adjust this recommended study time accordingly. Revision for examinations should be in addition to the above.

1.8 Examination

Important: the information and advice given in the following section are based on the examination structure used at the time this guide was written. However, the University can alter the format, style or requirements of an examination paper without notice. Because of this, we strongly advise you to check the rubric/instructions on the paper you actually sit.

The examination will be a single three-hour written paper, usually sat in May, which will consist of a total of six questions. Three questions will be on the first half of the unit (data communications) and three on the second half of the unit (enterprise networking). You will be expected to answer four questions in all: two from the first half of the paper and two from the second half of the paper. Specimen exam questions can be found at the end of each chapter and a complete specimen examination paper can be found in Appendix A. Some model answers and hints can be found in Appendix B.

The overall mark for the unit will be calculated from the examination results and the coursework marks.

[3] *Requests for Comments.*

Chapter 2: Network markets

Further reading

Carr and Snyder *Management of Telecommunications.* (McGraw Hill), second edition, 2003, Chapter 1.

Porter, Michael *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* (Free Press), 2004, Chapters 1, 2.

This volume of the subject guide is concerned with enterprise networking. An enterprise is simply an organisation. It can be a business (such as a public or private company), a partnership (such as a firm of accountants or management consultants), a not-for-profit organisation (such as a charity or a university) or a government body (such as a government department, a local government council or independent government agency).

Some types of networking are appropriate for both consumer and business (or enterprise) markets. Others are mainly intended for use by enterprises. It is these types of networking that we will be studying in this volume. The difference between enterprise networking and the types of networking associated with the consumer market, is that enterprise networks require more investment in time to design networking solutions and also further effort to manage these networks. The types of networks that support consumers do not require much, if any, design or management by the consumers themselves, but they do require considerable design and management by the network operators and these networks can be thought of as enterprise networks built and managed by network operators to support their customers. These public networks will also be studied in this volume. Enterprise networks can therefore range from that of a small business supporting a few PCs connected to an Ethernet hub, to a very large network owned by a network operator, supporting millions of customers. Enterprise networking is often thought to be limited to data, but enterprises will always have a requirement for voice and video networks, and enterprise networking must also include these, particularly as the integration of these very different types of network is becoming more important.

In this chapter, we shall examine the main drivers that affect the various markets for network products and services. We shall firstly look at this from a marketing perspective and introduce several marketing models that can be used to analyse markets. A study of these markets is useful, as networking professionals not only have to decide on technical solutions, but also have to choose suppliers. It is often the latter as much as the former that determines the best solution. To be able to evaluate suppliers, an appreciation of how markets work and the various strategies employed by the suppliers in the network marketplace is extremely useful.

2.1 Strategies to gain competitive advantage

According to McGaughey, Snyder and Carr, **competitive advantage** is the ability to excel in the marketplace due to price, product, service level or performance. Most enterprises regard obtaining competitive advantage as an imperative. The achievement of competitive advantage ultimately determines whether an enterprise is successful.

Some enterprises, particularly public enterprises, such as government departments or other not-for-profit organisations do not operate in a marketplace and are not driven to seek competitive advantage as there are no competitors. But even these enterprises have constraints on costs that force them to seek improvements in performance, and sensitivity to public opinion which force them to provide services, and service levels that meet exacting requirements. Other public or not-for-profit organisations, such as universities do operate in some sort of competitive market and are driven to seek competitive advantage.

Central to the study of competitive advantage is the concept of a **market**. A market essentially consists of the customers and potential customers to whom a product or service can be sold. A **product** or service is literally anything that is produced, is offered for sale and that satisfies a want or need. In terms of networking, the product usually provides the ability to communicate and is packaged in such a way that it has a well-defined set of functions, service levels and a price (or tariff).

The ultimate size of the market for a product is determined by the strategy of the seller. Companies selling products and services will often restrict their sales to just a part (or segment) of the total potential market. It is this market segmentation strategy that is often crucial to gaining competitive advantage. Before we consider strategies we shall take a closer look at competition.

Michael Porter has identified five forces that drive competition within a market or market segment.

These are:

- the intensity of rivalry among existing competitors – factors that increase rivalry include many competitors, equal market shares, slow growth, high fixed or storage costs, low differentiation, low switching costs and high exit barriers.
- the threat of entry by new competitors – factors that reduce the threat from new entrants include patents, economies of scale, product differentiation, brand loyalty, high capital costs, high switching costs, good distribution channels and government regulation.
- the pressure from substitute products – factors that reduce the threat from substitutes include high switching costs, low prices and brand loyalty.
- the bargaining power of customers – factors increasing the bargaining power of customers include a small customer base, the size of the customer and the size of the orders the customer makes.
- the bargaining power of suppliers – factors increasing the bargaining power of suppliers include the number of potential suppliers, low switching costs and the uniqueness of the product being bought.

All of the above forces will act on a company seeking competitive advantage in a market. The companies must develop strategies to counter these competitive forces.

2.1.1 Generic strategies

Competitive advantage can be obtained using three generic strategies, also identified by Michael Porter. In general, to be successful, the enterprise should choose just one of the strategies below.

Cost leadership

In this strategy, the enterprise seeks to have the lowest costs in its industry, often achieved through economies of scale, operating efficiencies, proprietary technology or preferential access to materials. If cost leadership can be achieved, then the enterprise can offer its products and services to a broad market at the lowest price and thus seeks to achieve or maintain a high market share. It does not attempt to provide unique features and only enhances its products and services in response to market demand.

Low cost does not automatically lead to low price. A cost leader may, if it has a large enough market share, choose to offer its products and services at higher prices and improve its profit margins, but can quickly reduce its prices if threatened by a new entrant or competitor.

There is usually only one cost leader competing within a market. When two enterprises aim to be cost leaders within a market, the result is likely to be a price war from which a single cost leader will emerge.

If an enterprise can obtain cost leadership, it acts as a disincentive to new entrants into the market, as they are unlikely to achieve the same level of costs and if new entrants do arrive, cost leadership can be used to undercut the prices of its competitors.

Cost leadership as a strategy is very vulnerable to new technology. If a competitor can offer a similar product based on a new and cheaper technology, cost leadership and ultimately market share will be lost.

Differentiation

In this strategy, the enterprise attempts to offer products or services, with unique features that customers value, to a broad market. The perceived added value (whether real or not) allows the enterprise to sell its products or services at a premium price. The advantage of this strategy is that the enterprise can maintain its market share because of brand loyalty. This will also deter competitors and new entrants selling substitute products and services.

There can be any number of differentiators competing within a market each with its unique product features.

The disadvantages of this strategy is that competitors may eventually create imitation products and services that may tempt customers away, particularly if there is a price advantage. A differentiation strategy is likely to require continuous innovation. Customer tastes may also change and the value of the differentiating features may diminish over time.

Focus

In this strategy, instead of offering a product or service to a broad market, the enterprise focuses on a particular homogeneous market segment or niche, thus narrowing its market, but aiming to be dominant within its own chosen market niche. The focus within the market segment can either be related to cost or to differentiation. The advantage of focus as a strategy, is that the enterprise can become dominant in the market segment chosen and can maintain a close relationship with its customers and hence better understand their needs and maintain loyalty. The main disadvantage is that the enterprise sells its products and services less widely and thus is subject to higher costs as it is often at the mercy of its own suppliers with whom it has much less leverage than enterprises who target a broader market. The big risk of this strategy is that cost leaders' or differentiators' products or services might also be targeted at the niche market segment.

An initial market segmentation, popular with network operators is to decide whether to aim products and services at individual consumers or other enterprises. Fixed line operators will often call these segments residential and business. New operators often target businesses as they are often more profitable, due to higher usage, geographical location (they tend to be in city centres) and lower selling costs (a single purchaser will often buy on behalf of the whole enterprise).

For consumers the following market segments can be identified:

- **geographic**, based on a particular region, climate, population density or population growth rate
- **demographic**, based on age, gender, social class, occupation, nationality, ethnicity, religion, education, wealth, income or family status
- **psychographic**, based on personality type, hobbies, pastimes, values, attitudes or lifestyles
- **behavioural**, based on usage rate and patterns, price sensitivity, brand loyalty or benefits sought.

For businesses, the following market segments can be identified:

- **geographic**, based on a particular region, customer concentration, regional growth rates and other economic factors.
- **customer type**, based on the type or size of the organisation, its industry or its role.
- **buyer behaviour,** based on organisational structure (centralised or decentralised purchasing), loyalty to suppliers, usage patterns, price sensitivity or order size.

The personal computer market with which you will be familiar, can be used to illustrate the above three generic strategies. In this market Dell, because of its market share and efficient operations that benefit from economies of scale, is able to follow a cost leadership strategy. Many other manufacturers follow a differentiation strategy. Apple Computer is perhaps the best example of a differentiator in this market. It differentiates its products by means of many unique features. Other manufacturers, tend to follow a focus strategy. A good example of a company who now follows this strategy is IBM. Although they invented the de-facto PC standard, they found that they could not compete in the consumer market and pulled out of this market, to focus on the niche business market.

2.1.2 Growth strategies

In order to be competitive and give a good return to its shareholders, an enterprise must seek to grow its business. It can do this within an existing market or create a new market with either an existing product or a new product.

The various possibilities for generating growth were analysed by Ansoff[1] in a matrix.

Table 2.1: Ansoff's Matrix

Product Market	Existing	New
Existing	market penetration	product development
New	market development	diversification

With **market penetration**, the enterprise markets its existing product, without any alteration, to existing customers by promoting it or by repositioning the brand, with the aim of increasing its share of the market.

[1] *H.I. Ansoff 'Strategies for Diversification' in* Harvard Business Review, *1957.*

With **market development**, the enterprise markets the existing product, without any alteration, to a new market segment. This could be a new geographic or a new demographic market, for instance. With **product development**, the enterprise creates a new product or enhances an existing product and markets it to its existing customers. Finally, with **diversification**, the enterprise markets a completely new product to completely new customers. Diversification can either be related or unrelated to existing products and markets.

These growth strategies have different levels of risk. The order in which they were discussed above is in increasing order of risk.

2.1.3 Product strategies

The Boston Consulting Group created a matrix to analyse the life cycle of products in a company's portfolio, in the form of a matrix, known as the Boston Matrix.

Table 2.2: The Boston Matrix

Market Share Market Growth	High	Low
High	Star ←	Problem child
Low	↓ Cash Cow →	Dog

The matrix compares market growth and market share and can be used to track a product's desired life cycle, shown by the arrows. The terms it coined, such as cash cow, are now very well known.

When an innovative new product is launched, it will often have a low market share but hopefully high market growth. If so, it is a **problem child**, because its launch will have been costly and the revenue obtained from its sale will not recover these costs for a long time. If the product does not have high growth, then it is unlikely to be profitable and hence it is a **dog**. If it does have high growth, it will obtain a high market share and hence it is a **star**. Stars are profitable, but maintaining growth is also costly. But eventually, there are limits to how much growth can take place and the rate of growth must at some time slow down. At this stage with a high market share and low growth, it is a **cash cow**, so named because the revenue from the product can be 'milked' without much effort. Finally, the product is likely to lose its market share to substitute products at which point it becomes a dog.

The ideal strategy is to use this matrix to analyse the position of all the products in a company's portfolio of products and to plan the launch of new products in such a way that the portfolio contains a balance of each type (except dogs). This means that the revenues from cash cows can be used to develop new problem children and turn them into stars and then cash cows to replace the existing cash cows when they become dogs. A company cannot rely on milking its cash cows for ever. These will ultimately turn into dogs as competitors offer substitute products and steal market share. Companies must continually innovate new products to survive.

2.1.4 Partnership strategies

In order to obtain or retain competitive advantage, it is often necessary to form partnerships or alliances with other companies within the same or related markets. Participation in forums to develop standards is one example of this. Without clear standards, customers are often reluctant to buy products due to fear that the market will move in a different direction and they will end up with a product that few others are using. This is particularly true in the area of networking, where customers want to be able to mix and match products from different suppliers, so that they are not locked into a single supplier and thus can gain bargaining power over their suppliers.

Partnerships are often required to develop innovative products. Research and development is an expensive activity and by collaborating with partners in developing new products both the cost and the risks can be shared.

Companies also sometimes enter into partnerships with their suppliers or even their customers. Such partnerships are often necessary to distribute products, if the company which has developed the product does not have the geographical reach or organisational structure in place to distribute the product.

2.2 Market studies

In this section, we shall firstly introduce some tools (PEST and SWOT analysis) that can be used to analyse an enterprise and its business environment. We shall then go on to study the fixed and mobile network markets, followed by the ISP[2] market and the network equipment market. Finally, we shall have a look at the market for a network application in an industry sector, the Global Distribution Systems (GDSs), used by the travel industry. This has been chosen, as it is one of the few industry sectors that has built a large global network that you may have used, unknowingly, when booking holidays.

PEST analysis examines a companies environment under the following headings:

- **political** factors such as government policies and the regulatory environment (which is particularly important for telecommunications services)
- **economic** factors such as interest rates, inflation rates, unemployment rates, disposable incomes and economic growth rates
- **socio-cultural** factors such as customer attitudes, leisure time and demographics
- **technological** factors such as technical innovations, patents and the development of new systems and distribution channels.

SWOT analysis is a subjective examination of a company's Strengths, Weaknesses, Opportunities and Threats. PEST analysis and Porter's five forces listed in section 2.1 and the company's generic, growth, product and partnership strategies discussed in Sections 2.1–2.4 can be used to help identify some of the factors under each heading.

- **Strength** are positive aspects internal to the organisation.
- **Weaknesses** are negative aspects internal to the organisation.
- **Opportunities** are positive aspects external to the organisation.
- **Threats** are negative aspects external to the organisation.

[2] *Internet Service Provider*

You should use these tools to analyse companies that operate within your country in the activities at the end of each section. The subject guide attempts to describe the various network markets from a global rather than national perspective.

2.2.1 Fixed network operators

Fixed network operators are usually classified according to whether they are incumbents, who historically provided telecommunications services in a protected market or insurgents who entered the market when it became open. Thirty years ago, it was commonly believed that telecommunications services within a country were best provided by a single operator, as telecommunications along with other utilities were regarded as natural monopolies. These operators were often owned by governments or else were private companies that governments entrusted to run all the telecommunications services in their countries. The PTTs[3] and RPOAs[4] were all powerful within their countries and would often insist that customer premises equipment (CPE) such as telephones, PABXs[5] and modems, were provided by themselves. Some would allow customers to buy their own CPE and connect it to the network, but only after the equipment had undergone rigorous 'permission to connect' testing which aimed to ensure that the equipment was totally safe and would not apply a mains voltage to the line and electrocute one of the PTT's employees. Because of these and other monopolistic and restrictive practices there was no competitive market in telecommunications. PTTs were slow to innovate and tended to provide a restricted number of low quality services at excessively high prices. The profits made by the PTTs were often regarded as an extra source of revenue by governments and the PTTs found it hard to obtain capital for investment in new technology, as it would increase government borrowing. Many PTTs did not have sufficient line plant to meet demand and they imposed a waiting list for service and line sharing schemes.

There were however some positive aspects to this situation. The PTTs were engineering led and as a result constructed and designed networks that were technically sound, within the constraints of the technology of the times. The markets and prices were stable and growth was steady, if unspectacular. The organisations often had a good public service ethos, as befits a part of government and they were obliged to provide service in any part of their countries. This is known as a **Universal Service Obligation (USO)**. Finally, by working together in CCITT[6], which became the ITU-T[7], they were able to develop inter-working standards. The fact that the global telephone network is probably the largest single system mankind has ever built and that all of the individually managed networks can interconnect and inter-work with each other is a testament to this standardisation process.

The operators forged bilateral interconnection agreements with each other, which required the operator on whose network a call originated to pay the operator on whose network a call terminated a per minute charge. This charge was not related to cost and for many years the operators made huge profits out of international telephone traffic paid for by their captive customers, whom they usually called subscribers, thus reflecting their attitudes to customer service.

All this began to change in the 1968, when the US Federal Communications Commission allowed other businesses to connect their equipment to the **incumbent** (monopoly) network owned by AT&T[8]. This decision was shortly followed by another ground-breaking decision that allowed a small upstart company called MCI[9] to provide long distance telecommunications services

[3] The Government Departments that ran posts and telecommunications as monopolies were known as Post, Telegraphs and Telephones (PTTs).

[4] Private companies that ran telecommunications services as monopolies were known as Recognised Private Operating Agencies (RPOAs).

[5] Private Automatic Branch Exchange – a customer owned and managed telephone switch.

[6] Comité Consultatif International Téléphonique et Télégraphique.

[7] International Telecommunications Union – Telecommunications Standardization Sector

[8] American Telephone & Telegraph who were the RPOA that owned the Bell network in the USA.

[9] Microwave Communications Incorporated.

in competition to AT&T. MCI started out by setting up a high speed communications network using microwave links between major US cities, but had to fight AT&T all the way through the courts and by lobbying Congress, until eventually won an important anti-trust case in 1984 which resulted in AT&T reorganising its 22 Bell Operating Companies and divesting them into seven separate Regional Bell Operating Companies (RBOCs)[10], and a long-distance (inter-state) carrier which retained the name AT&T. At the same time AT&T also divested itself of Bell Labs and its manufacturing arm Western Electric[11]. MCI and other new carriers such as GTE, Sprint and Worldcom were then able to compete fairly with AT&T for the long distance market. But within each region there the RBOC still had an effective monopoly. The RBOCs, who were also known as Incumbent Local Exchange Carriers (ILECs), gradually merged with each other and other new operators to form the US operators that we know today such as BellSouth, Qwest, SBC and Verizon. At the time of writing both Qwest and Verizon are bidding to take over MCI and SBC has bid to take over AT&T. Other companies known as Competitive Local Exchange Carriers (CLECs) were allowed to compete with the RBOCs for local lines and calls.

Meanwhile in Europe, things were beginning to change in the UK. The British Government had split the Post Office's telecommunications business from its postal business and began to privatise it as British Telecommunications (BT) plc[12]. At the same time just one new operator called Mercury Communications Ltd (MCL) was licensed to compete with BT. This was owned by a consortium which included Cable & Wireless (C&W) Limited, which had also only recently been privatised and was the incumbent operator in a number of British colonies and ex-colonies (notably Hong Kong). MCL built a modern fibre optic network alongside railway tracks and attempted to compete against BT in all its markets, including unprofitable pay phones. As a result, this strategy was not particularly successful. MCL should have focussed on profitable niches rather than attempting to compete in all markets. MCL was eventually forced to focus on niche business markets and the residential parts of MCL's business were eventually sold off to the cable TV company NTL with the business parts being re-absorbed into C&W.

In 1991, the British government abandoned its duopoly policy and announced that there would be no restrictions on the number of telecommunications operators that would be licensed. This led to a large number of new entrants to the UK market which eventually consolidated into a smaller number of successful operators such as Colt (which started out as City of London Telecommunications), Energis (which ran its fibre optic cables over the UK electricity grid) and Thus (which started out as Scottish Telecom).

The other players in the UK fixed telecommunications market are the cable TV companies. These were started up in the 1980s, with heavy investment from the US RBOCs, to provide cable TV and telecommunications services in franchised areas. The heavy costs of laying cables in residential areas and competition from satellite TV has caused many problems for the cable TV companies in the UK and they have now consolidated into NTL and Telewest and may consolidate further.

The UK policy of privatising its PTT has now been followed by most countries throughout the world (sometimes with partial privatisation) and has changed the face of the telecommunications market. It is generally felt that competition leads to lower prices, more innovation and better service. Also, governments, as the owners of the PTTs, were able to collect large revenues when the newly formed telecommunication companies were floated. Many of the well-known global players have their origin as PTTs. These include BT in

[10] *Also sometimes referred to as 'Baby Bells'.*

[11] *Now Lucent Technologies.*

[12] *Now BT Group plc.*

the UK, Deutsche Telekom in Germany, France Telecom in France, NTT in Japan, Telecom Italia in Italy, Telefonica in Spain, TeliaSonera in Scandinavia, Telstra in Australia and SingTel in Singapore. Many countries however have not followed the UK and US policy of encouraging infrastructure competition where new companies are licensed and encouraged to build new large-scale local networks. Instead the emphasis in many countries has been on service competition where the incumbent is heavily regulated and has to offer wholesale services to service providers who then sell to customers in competition with the incumbent itself. As a result of this policy, in many countries, there is only a limited amount of infrastructure that is not owned by the incumbent, but providing regulation is effective, this does not prevent a vibrant competitive telecommunications services market developing. Most regulators have ensured that all operators are given equal access to the incumbent's local loops.[13] This has been achieved primarily through forcing the incumbents to offer carrier pre-selection (where customers can pre-select their local, national and international carriers without having to dial access codes), Local Loop Unbundling (LLU). With LLU, the incumbent's local telephone switch is bypassed altogether and the loop is terminated on equipment belonging to another operator) and number portability (where customers can retain their numbers when they switch between operators).

During the 1980s and 1990s there was a boom in the telecommunications industry and many new entrants emerged intent on building new infrastructure. As a result new operators, such as Interoute, Global Crossing and Level 3, have laid optical fibres in many parts of the world and with the ever increasing transmission speeds and bandwidth which can be used in the existing fibres, there is now a glut in capacity and as a result bandwidth prices have fallen and network bandwidth has become a commodity product. This has been something of a problem for the new operators.

Amongst network operators, the incumbent (ex monopoly) operator is rarely the cost leader. This is because they tend to have large overheads and they own an expensive inefficient legacy network, as well as having a Universal Service Obligation (USO) which means that they have to provide services to parts of the country that are uneconomic. The strategy of incumbents is usually to attempt to maintain their large market share by differentiating themselves on service with slightly higher prices than the new entrants. The incumbents have two main cash cows, resulting from their legacy investment in infrastructure. These are voice calls over the PSTN[14] and the sale of private circuits. Both of these are mature markets which have limited growth opportunities. In developed countries, the number of customers for the PSTN voice has reached the point of saturation, where nearly everyone has a phone line. Because of this lack of growth the fixed network operators are looking for new stars and see broadband access in this light. It has high growth potential. They also are looking to diversify, particularly with business customers, where they aim to provide systems integration and outsourcing services adding value to basic telecommunications or to offer new mobile or IP based services. In many countries, the fixed network operators have used their market strength, customer base and distribution channels to successfully diversify into these related markets and many are now the dominant mobile network operator and Internet Service Provider in their countries. Eventually, both PSTN voice and private circuits are likely to become dogs as voice calls are substituted by Voice over IP (VoIP) and to some extent mobile phone calls and e-mail. Private circuits are also likely to be substituted by broadband access to managed services. This presents an interesting dilemma for fixed network operators as they have to decide at

[13] The pair of cables that connect the customer's premises to the local exchange.

[14] Public Switched Telephone Network, see Section 4.2.4 of this volume.

what point to start abandoning their cash cows and launching services such as VoIP (Voice over IP) which will compete against their own traditional PSTN services. This process of companies launching products that compete against their own cash cow products is called **cannibalisation**. If they do not do this, they risk losing everything, as competitors will certainly launch these services. A similar dilemma exists between traditional private circuits and ATM[15] or IP services provided over broadband access.

The new entrants often known as **insurgents** or alternative network operators (or **altnets**) have had to focus on niche markets (usually in the business sector and in restricted geographical areas such as city centres) in order to survive. They are often much more innovative and adaptable than the incumbents. They have the advantage of not being encumbered by legacy technology, regulation or a universal service obligation. Their lower cost base, resulting from this, means that they have the potential to be cost leaders and to implement a cost focus strategy to compete against the incumbent on price, although start-up costs, particularly investment in infrastructure act as barriers to entry into the market, as do regulatory hurdles. Unlike the incumbents, the new entrants are able to achieve high growth for their PSTN voice and private circuit offerings, as they encourage customers to switch from the incumbents by their lower prices. These services, as well as newer services such as broadband, are all stars for the new entrants.

Many fixed network operators have tended to restrict their operations to their own country, but have involved themselves in partnerships with each other to develop new standards, launch satellites and form bilateral agreements for international services.

Those that have strayed outside their own countries, have often done so in partnership with other operators. Examples of these partnerships are Concert (now split up between AT&T and BT), Global One (now merged with Equant and owned by France Telecom), Infonet (being acquired by BT at the time of writing) and Unisource (whose network assets were acquired by Infonet). However most of these partnerships ultimately failed and reverted to single ownership, mainly due to problems between the partners, often over the control of the partners' home customers who also had global interests.

In summary, competition in fixed telecommunications markets has certainly led to large reductions in prices, more choice for customers, more innovation and improved levels of customer satisfaction.

Activity 2.1

Make a list of the main fixed network operators who provide services in your country. Look at their web sites and other information on the web to discover what markets they are focused on, what products they are selling and what strategies they are following. Carry out Five Forces, PEST and SWOT analyses on each of the companies.

2.2.2 Mobile network operators

The mobile network operators have only existed since the 1980s. The earliest mobile phone networks were built in Scandinavia where the costs of providing fixed communications to remote communities were prohibitive. The mobile network operators tend to be young dynamic companies that have created a whole new market and have seen it grow at a phenomenal rate. Some mobile network operators are owned by fixed network operators, but where this has happened, the mobile operation is usually run at arms length from the fixed line business. Often this is for regulatory reasons, as regulators want to ensure that the operators do not cross-subsidise their

[15] Asynchronous Transfer Mode, see Section 6.5 of this volume.

mobile operations from their monopoly revenues. But also, most fixed line operators realise that the culture of a mobile operator is very different and that the mobile operation needs to be much more dynamic and entrepreneurial, which will be much harder to achieve within an ex-PTT organisation.

Another difference between mobile and fixed network operators is that with the former there is usually no incumbent, because governments have, in most cases, issued multiple licenses to encourage competition. All operators have had to start with a clean sheet and build their networks and their customer base from scratch. Building a mobile network requires a huge investment in infrastructure (radio masts, base stations, mobile switches and private circuits which have to be leased from fixed network operators). In addition to this, governments have recently realised that they can generate huge revenues from the sale of radio bandwidth and the licenses to use a part of the radio spectrum are now often auctioned, so that mobile network operators have to compete for them. Despite the large investments, the rewards are also great. Customers are willing to pay a premium price for the flexibility to make mobile phone calls. There is also a revenue stream that comes from calls made between fixed networks and the mobile networks. The fixed network operator who bills the call, has to pay a termination charge to the mobile network operator who receives the call and vice versa. There are further opportunities to make revenue from roaming, where the customer makes or receives calls on a mobile network in another country. Another source of revenue comes from text messages and the downloading of ring tones. Finally, with the advent of data services and third generation mobile phone services, the mobile network operators are also expecting to make significant revenues from always-on data services.

Because there is no incumbent and competition is both fierce and fair, mobile network operators tend to use a differentiation strategy. They attempt to launch new features and services that will give them an edge (albeit a small one) over their competitors. They are also notorious for developing complicated tariff structures that make it very difficult to compare prices between operators. A common technique for subscription accounts is to provide handsets free or at a reduced price, but with customers paying a higher monthly subscription. This was vital, in the early days of mobile telephony, when handsets were very expensive and customers were put off by the up-front cost of buying a handset. An important and fairly recent innovation that has led to increased market penetration, particularly amongst the younger generation who do not have the credit history to open a subscription account, is the use of pre-payment where there is no monthly subscription, but calls are paid for in advance by purchasing a card. The use of pre-paid cards has increased the market for mobile phones, which was once for businessmen and the wealthy professional classes, so that now it is a truly mass market which covers the whole population.

To a mobile network operator, voice services are all stars, possibly to become cash cows in the near future. There is still a good potential for growth left in the market as they can continue to grow their subscriber bases as well as growing revenue per user. There are signs however that growth in subscribers in some countries is tailing off, as a saturation point is close to being reached. Future high growth is dependent on the success of the related diversification into new data and third generation services. These services are currently problem children with a high growth rate and the potential to become stars.

Because the mobile phone market is so competitive and there is little difference between the product offerings of the operators, there is a tendency among customers to switch operators. The movement of customers from one operator to another is known as **churn**. Operators try to prevent churn by locking customers into lengthy contracts and by selling handsets that can be blocked from use on other operators' networks.

Mobile network operators have historically tended not to form partnerships with each other in their own markets, but they have entered in partnerships with suppliers and distributors and with other international operators for roaming. There has also been considerable international takeover activity between mobile network operators (sometimes hostile) and expansion into new countries, forming large multinational operators such as Orange (owned by France Telecom), T-Mobile (owned by Deutsche Telekom), Hutchison Whampoa Limited (based in Hong Kong, but successfully launched Orange in the UK before selling it to France Telecom and acquiring several 3G licenses around the world, marketing under the global brand name '3'), NTT DoCoMo in Japan, who have been highly successful in launching I-mode data services, and Vodafone, which was just a start-up company in 1985 when it won one of the first analogue licenses in the UK. Vodafone has been most successful in its expansion and acquisitions, and after acquiring Airtouch in the US, it is now the global market leader. It is the largest company listed on the London Stock Exchange with a market capitalisation many times larger than BT (the UK's largest fixed network operator).

The mobile network operators have therefore consolidated into a small number of global brands, in contrast to the fixed network operators who were predicted to do this, but have yet to achieve it.

Activity 2.2

Make a list of the main mobile network operators who provide services in your country. Look at their web sites and other information on the web to discover what markets they are focused on, what products they are selling and what strategies they are following. Carry out Five Forces, PEST and SWOT analyses on each of the companies.

2.2.3 Internet Service Providers

The Internet Service Provider (ISP) market was created in 1994, when the US Government commercialised the Internet. Up until then, the Internet's NSFNET[16] backbone could only be used for educational and research purposes. Commercial providers were encouraged to build or acquire and operate their own backbones and regional access networks, to interconnect with each other via Commercial Internet Exchanges (CIXs), and then to sell their services to the general public and the business community. Some of the companies that became involved in this were fixed network operators, such as Ameritech (acquired by SBC), MCI, MFS (acquired by WorldCom), Pacific Bell (also acquired by SBC), Sprint, WorldCom (who acquired MCI and eventually reverted to the MCI brand). In other parts of the world the fixed network operators, such as France Telecom (with Wanadoo), Deutsche Telekom (with T-Online) also provided ISP services (usually via a subsidiary which can be dynamic and entrepreneurial), and in many countries they have become the dominant ISP, being able to exploit the large customer bases of their parents. A number of ISPs were start-up companies, such as Performance Systems International (PSI) in the US and Demon Internet (acquired by Thus), Pipex (now owned by MCI) and FreeServe (acquired by Wanadoo) in the UK, who foresaw the commercial potential of providing subscription-free internet access. Others providers were the on-line

[16] *National Science Foundation Network.*

computer service/information providers, such as America On-Line (AOL), CompuServe (acquired by AOL), Prodigy and UUNet (also now owned by MCI). AOL has been able to build a very large global customer base through aggressive marketing and international expansion.

The ISP market is highly competitive. The products it offers are in great demand and growth has been spectacular, but still with potential to grow further, as market penetration improves. They are certainly stars and ISPs have had to differentiate themselves by means of continuous innovation. One of the innovations, which has made a big difference to the market was the provision of 'free' internet services. In the early days, in most countries, customers paid their ISP a monthly subscription and then paid their fixed network operator a per minute telephone call charge[17] whenever they dialled-up their ISP. In the UK a start-up company called FreeServe (now owned by and rebranded as Wanadoo) realised that they could offer a subscription-free service by offering Internet access via a local call fee access number where revenue from the billed call was passed onto the ISP by the fixed network operator. This was an attractive proposition for customers, who could now access the Internet without having any monthly paid contract with the ISP. As a result of this and using a good retail distribution channel, FreeServe was able to come from nowhere to be the market leader in the UK (for a period). Tiscali enjoyed similar success in Italy and has now expanded, mainly by mergers and acquisitions to cover most of Europe.

Since then, the ISP market has largely reverted back to a subscription based model, as there was huge pressure from customers to remove per minute phone call charging which was a disincentive to use the Internet. This pressure built up on the fixed network operators who were forced to offer un-metered dial-up Internet access via wholesale products for the ISP to offer to their customers. The same model is also used for broadband Internet access, although some products restrict the volume of data that can be downloaded.

ISPs are also beginning to diversify into offering services that have traditionally been offered by fixed network operators. Such services include broadband access taking advantage of Local Loop Unbundling, or wholesale products. The ISPs are often more innovative than the incumbent operator (or its ISP subsidiary) and can differentiate themselves with higher speed connections and new features. They also compete aggressively on price. They are beginning to offer a VoIP service that will be able to substitute normal telephone calls which may ultimately turn the incumbent's cash cows into dogs.

In summary, the ISP market is still a young dynamic market experiencing high growth rates which appears to have potential to compete with the incumbents' telephone services.

Activity 2.3

Make a list of the main ISPs which provide services in your country. Look at their web sites and other information on the web to discover what markets they are focused on, what products they are selling and what strategies they are following. Carry out Five Forces, PEST and SWOT analyses on each of the companies.

2.2.4 Network equipment manufacturers

The other big players in the network market are the equipment manufacturers. A number of these such as Alcatel, Ericsson, Fujitsu, Lucent Technologies, Marconi, NEC, Nortel and Siemens, began as telephony equipment manufacturers selling to the PTTs and network operators. Many of these companies were originally based in just one country and had a cosy

[17] *In North America, and now some other countries too, local telephone calls are not charged on a per minute basis. The cost of calls is recovered through a higher monthly rental charge and as a result ISP customers are not charged for connect time and can afford to remain on-line for long periods of time.*

relationship with their incumbent operator from whom they milked a cash cow. However, with increasing competition in these markets, both new entrants and incumbents were prepared to buy from alternative foreign suppliers and the network equipment market was globalised. The countries of origin of these now global companies are still apparent in the location of their head offices. These companies have tended to continue to sell WAN equipment to network operators and other companies, although some of them, notably Ericssons and Siemens, have carried out a related diversification into mobile network equipment. One company, Nokia has re-invented itself several times in its history. Sometimes the diversification has been related, sometimes it has been unrelated. Nokia was founded in 1865 as a paper manufacturer. It diversified into a conglomerate company that manufactured many different products, including rubber, chemicals and telecommunication cables. It later carried out a related diversification into manufacturing telecommunications equipment. In 1992, Nokia sold all its other businesses and focused entirely on telecommunications. It was in the right place (Scandinavia) at the right time (when mobile phones were about to be launched) and it was able to capture a large share of both the mobile handset and the mobile base station and switch markets. As a result of this it is the dominant supplier of mobile handsets in the world.

Several other manufacturers were founded more recently to address gaps or create products in the markets for LAN or internetworking equipment. Such companies include 3Com, Cisco Systems, Foundry Networks and Juniper Networks. Of these companies 3Com and Foundry Networks started out in LAN hub and switch markets, but are moving into in routers and layer three switches, while Cisco Systems and Juniper Networks started in the router market (Cisco invented the router and is still dominant in this market), but has diversified into LAN switches.

Cisco Systems

Cisco Systems is an extremely successful company. It has become the leader or the second player in every market in which it competes. It has achieved this mainly by means of clever acquisitions. Cisco is always on the look-out for small start-up companies with good ideas for promising new products. It then acquires them, integrates them and continues to develop the new products finally marketing them under the Cisco brand. Cisco has carried out this process many times and has a lot of experience at integrating these start-up companies. Many of their executives have stayed with Cisco, continuing to develop their product and some have also become Cisco executives. Cisco has also focused on excellent customer service and has practised what it preaches in terms of using networks to gain competitive advantage. Cisco has developed its business systems to be accessible over the web and employees, customers and suppliers are able to do most of their business with the company using these systems. Cisco always has a portfolio of products at different stages of their product life cycles where the cash cows can provide the revenues to fund the problem children and the stars. Cisco also successfully outsources some of its activities such as manufacturing, but is able control its suppliers closely and ensure timely delivery and quality. Cisco also has put together a certification programme for engineers who design or maintain Cisco networks. This programme has become an industry standard networking qualification and is also taught at many educational institutions. It gives Cisco a real competitive advantage, as anyone studying for these qualifications becomes familiar with Cisco's products. It has used its certification programme and technical forums on its web site to create a community of experts who will often support each other without involving Cisco's own technical support.

Juniper Networks

Juniper is a start-up company, founded in 1996, that has focused on the market for high specification routers which it develops and sells to ISPs and network operators. No company can tackle Cisco head-on in all its markets, but there is room for competition in niche markets such as this.

Alliances

As a result of intense global competition there has been a great deal of acquisitions and mergers amongst network equipment manufacturers and the market has consolidated so that there is now a relatively small number of global suppliers who offer a wide range of networking products. These suppliers compete aggressively with each other, but they also have to collaborate on the development of standards and sometimes on new products which are expensive to develop. Most of these suppliers participate in standards bodies[18] such as the IEEE, the IETF and the ITU-T as well as various forums to progress particular standards such as the ATM and Frame Relay Forums. The reason they do this is because customers are generally reluctant to buy networking products until standards are agreed and suppliers do not want to develop products that are then made obsolete by standards. By participating in standards bodies the suppliers aim to influence the standards in ways that may favour their companies, as well as assisting in developing markets for new products.

Activity 2.4

Explore Cisco Systems' web site (www.cisco.com) and investigate the factors that have given Cisco Systems competitive advantage in its chosen markets.

2.2.5 Global Distribution Systems

Network-based Computerised Reservation Systems (CRSs), or Global Distribution Systems (GDSs) as they are now called, were originally developed for internal use by the airlines in the 1960s. American Airlines came up with the idea of providing terminals to travel agents and a network to connect them to their mainframe computer and started to roll out this network in the 1970s. It called this system SABRE (which originally stood for Semi-Automated Business Research Environment), which it had jointly developed with IBM. This innovative idea had many advantages for American. The main advantage being that travel agents could make the bookings direct without American having to employ staff in call centres to answer telephone calls from the agents and make the bookings on their behalf. Secondly, by providing the terminals and the network, it encouraged loyalty from the travel agents who would often choose American flights for their customers in preference to other airlines.

As far as the agents were concerned the CRS network had arrived at just the right time. The US airline industry was about to be deregulated. Many new airlines came into existence, competition became cut-throat, prices were changing rapidly. Passenger numbers were expanding and the major airlines were moving towards a hub and spoke route structure, which meant that more booking for connecting flights were required. The existing manual ticketing systems and procedures just could not cope much longer, so the travel agents were desperate to connect to American's CRS network, as it was the only one available. This gave American a huge competitive advantage over other airlines who were at least a year behind in deploying similar

[18] *See Volume 1, Section 3.3.*

networks. Given this head start with a new product in the new CRS market, American were soon able to turn their SABRE from a problem child into a star. Having achieved market dominance, SABRE diversified to support hotel, car-hire and other airline bookings in addition to its own flight bookings. It was able to demand a fee from any other company whose bookings could be made using SABRE as it owned the main distribution channel to the travel agents. As a result of this, SABRE was a huge commercial success and soon American was earning more profit from SABRE than it was from its flights. It created a separate company for this new business, which reported along with American Airlines to a holding company called AMR. In 1992, Robert L. Crandall, the CEO of AMR said: 'If you told me I had to sell either the airline or the system, I'd probably sell the airline'.

The other airlines, who were at a considerable disadvantage, decided to develop their own systems in partnerships (United and Eastern collaborated with IBM to produce a system called PARS which further developed into three separate systems: Apollo used by United; Worldspan used by Delta, Northwest and TWA; and SystemOne used by Continental and Eastern and later Texas Air).

With market dominance, American was able to exploit SABRE to the advantage of its airline. When displaying possible flights to travel agents, SABRE would present American flight at the top of the screen and competitors' flights further down. Agents were thus more likely to book flights with American. They also charged airline competitors more than partners for holding information on SABRE. This was clearly anti-competitive and eventually American's competitors won an anti-trust case that prevented American from continuing these practices. This created a more competitive market.

In Europe and Asia Pacific, American were not able to obtain market dominance, as the airlines in these parts of the world developed their own systems based on those already developed by the American carriers. A consortium of European airlines including BA, KLM and Aer Lingus developed Galileo based on Apollo and another consortium including Air France, Iberian and Lufthansa developed Amadeus based on SystemOne. In the Asia Pacific region, Singapore Airlines and Cathay Pacific and others developed Abacus based on SABRE.

The Global Distribution Systems, as the CRSs became known, were probably one of the first examples of e-commerce, even though they started with mainframe transaction processing technology, low speed modem networks and the limited block graphics of dumb teletext terminals. They now exploit web technologies, high speed networks and high resolution graphics supported by PCs.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. A problem child has low market growth and low market share

ii. Unlike the mobile network operators, the fixed network operators have not been consolidated into global companies.

iii. It is virtually impossible for the incumbent fixed network operator to become the dominant ISP in its home country because it lacks the necessary dynamism.

v. Network equipment manufacturers usually work together in standards bodies and industry forums as customers will often not buy products until standards have been agreed.

(b) List the five forces that drive competition within a market as identified by Michael Porter.

(c) Describe the main difference between the markets of the fixed and the mobile network operators.

(d) Describe the factors that enabled Nokia to become dominant in the mobile handset market.

(e) Describe the factors that gave American Airlines competitive advantage when they connected travel agents to their SABRE network.

Learning outcomes

At the end of this chapter, you should be able to:

- describe the five forces that drive competition in a market, as identified by Michael Porter
- describe the various strategies that companies employ to gain competitive advantage
- analyse network markets using SWOT analysis combined with PEST analysis, Porter's five competitive forces and the strategies used to gain competitive advantage
- describe the historic development and strategies employed by the fixed network operators
- describe the historic development and strategies employed by the mobile network operators
- describe the historic development and strategies employed by the ISPs
- describe the historic development and strategies employed by the network equipment manufacturers
- describe the historic development and strategies employed by the Global Distribution Systems.

Notes

Chapter 3: Network technologies – PANs, SANs and LANs

Further reading

Fitzgerald and Dennis *Business Data Communications and Networking.* (John Wiley & Sons), eighth edition, 2005. Chapters 6, 7, 8.

Forouzan, Behrouz A. *Data Communications and Networking.* (McGraw Hill), third edition, 2003. Chapters 14, 15.1, 15.2, 16.3.

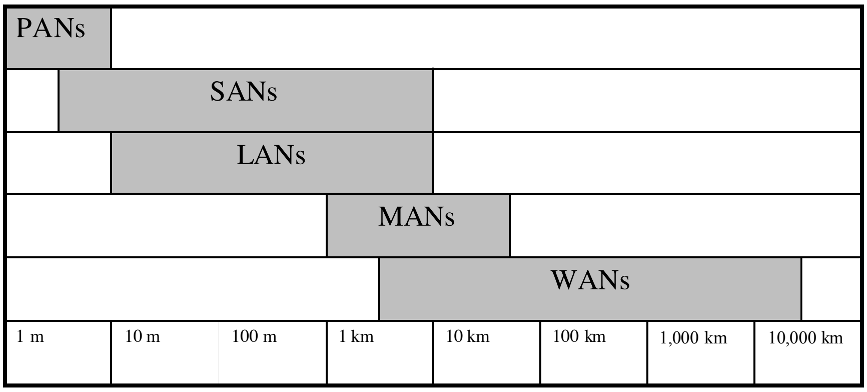
Stallings, William *Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003. Chapters 15.3, 16.2, 16.4, 17.2.

Tanenbaum, Andrew S. *Computer Networks.* (Prentice Hall International), fourth edition, 2002. Chapters 4.3, 4.4, 4.6, 4.7.6.

In this chapter and the next chapter, we will examine the technologies used in enterprise networking. Some technologies will also be discussed that are predominantly used in consumer markets, but they are also used by employees of enterprises for business purposes and it is appropriate to consider them in this part of the course. Many of these technologies cover more than one layer of the hybrid reference model, so they do not fit neatly into the structure of Volume 1 of the subject guide, which considers each layer in a separate chapter.

For convenience, we will classify the technologies by the type of network that they are designed to support. The types of network are Personal Area Networks (PANs), Storage Area Networks (SANs), Local Area Networks (LANs), Metropolitan Area Networks (MANs) and Wide Area Networks (WANs). All of these, apart from SANs were introduced in Volume 1 of this subject guide. The type of network is characterised by the range of distances over which they operate. Table 3.1 below shows roughly how the different types of network compare with each other against a logarithmic scale of distances.

Table 3.1: Approximate ranges of each type of network



In this chapter we will look at PANs and consider the Universal Serial Bus (USB) and FireWire as examples of wired PANs and Infra-red Data Association (IrDA), Bluetooth and IEEE 802.15 as examples of wireless PANs.

We will consider the special networking needs of SANs and Fibre Channel as the main technology used to support these networks.

Finally, we shall examine the main technologies used in Local Area Networks, concentrating on the many variants of Ethernet, but also considering Token Ring and Fibre Distributed Data Interface (FDDI).

3.1 Personal Area Networks (PANs)

Personal Area Networks (PANs) typically cover a short range (a few metres) close to a person or their personal equipment such as PCs, Personal Digital Assistants (PDAs) or telephones. PANs can be wired or wireless. Wired PANs include external computer buses such as the Universal Serial Bus (USB) or Firewire. Wireless PANs include infra-red communications as sometimes used between PCs and keyboards as well as high-speed radio communications used between intelligent mobile devices.

3.1.1 Universal Serial Bus (USB)

USB has a maximum data rate of 12 Mbit/s (480 Mbit/s for USB 2) and can support up to 127 devices on the same external bus, which consists of up to five metres (without repeaters) of four pairs of UTP[1] cable. It can support multiple devices at 1.5 Mbit/s or one device at 12 Mbit/s. Multiple devices can be daisy-chained by being connected to other USB devices or daisy-chained from a USB hub in a bus-star topology. USB also distributes low voltage power to peripherals, which no longer require separate low voltage power supplies. USB supports plug and play attachment (i.e. automatic assignment of resources to devices) and all devices are hot pluggable (i.e. that can be attached and start working without crashing or having to restart the PC). When a new device is plugged into the bus, the change in power levels is detected and an address is assigned to the device, which is unique on the bus. USB avoids contention by operating a master–slave protocol. USB uses NRZI[2] encoding with bit-stuffing and CRC[3] error detection.

3.1.2 FireWire[4]

FireWire was invented by Apple Computers and Texas Instruments for local area networking, but has been standardised by the IEEE. It has a maximum data rate of 400 Mbit/s (or 800 Mbit/s for 1394b) and can support up to 63 devices on an external bus, which consists of up to 4.5 metres (without repeaters) of three pairs of STP cable. Devices typically have three Firewire ports and they can be connected in a cascaded star topology network. FireWire also distributes low voltage power to peripherals, which no longer require separate low voltage power supplies. FireWire supports plug and play attachment and all devices are hot pluggable.

It removes the possibility of contention by means of TDM[5] and allocates separate channels to each device connected to the bus. It is therefore ideally suited to carrying fixed bandwidth transmissions such as video. Sony have licensed FireWire for their camcorders and have branded it as iLink.

FireWire uses Data-Strobe (DS) coding with NRZ[6] signalling. It transmits two signals on different pairs: a data signal and a strobe signal, which is produced by a bitwise XOR[7] operation on the data signal and an alternating clock signal. At the receiver the data and strobe signals are XORed to reconstruct the clock signal and hence maintain synchronisation.

Unlike USB, it is a peer-to-peer protocol, although one station still has to act as a bus manager. This means that any two FireWire devices can communicate with each other, unlike USB where two slaves are unable communicate with each other directly.

[1] *Unshielded Twisted Pair, see Volume 1, Section 8.3.1.1.*

[2] *Non Return to Zero Inverted, see Volume 1, Section 8.3.6.4.*

[3] *Cyclical Redundancy Check, see Volume 1, Section 7.3.6.*

[4] *IEEE 1394*

[5] *Time Division Multiplexing, see Volume 1, Section 2.3.1.*

[6] *Non Return to Zero, see Volume 1, Section, 7.3.6.*

[7] *Exclusive OR (either one or the other but not both).*

Activity 3.1

Satisfy yourself that Data Strobe coding works by taking an arbitrary byte of data and produce a strobe signal by XORing the data with a byte containing an alternating pattern of 1s and 0s that represents a clock signal. Take the strobe signal and XOR it with the original data and check that you can regenerate the clock signal.

3.1.3 Infra-red Data Association (IrDA)

The Infra-red Data Association was founded in 1993 to develop and promote a standard for infra-red data communications. Its earliest members were Hewlett Packard, IBM and Sharp. It was designed for short-range digital communications between a PC and devices such as a keyboard, personal digital assistants, digital cameras, mobile phones and intelligent watches. The signal range is up to one metre, in normal light conditions and within a 30° cone from the transmitter. It can operate at speeds ranging from 9.6 kbit/s to 4 Mbit/s and uses three different modulation/coding techniques depending on the data rate. Below 115.2 kbit/s it uses asynchronous transmission (with start and stop bits), CRC-16 error checking and byte stuffing. It uses a coding scheme similar to RZ[8] with a zero represented by a pulse in the first part of the bit period and a one by no pulse. For data rates between 576 kbit/s and 1.152 Mbit/s, synchronous transmission with bit stuffing and CRC-16 error checking and a similar coding scheme is used. 4Mbit/s transmission is also synchronous but without the need of bit or byte stuffing. It uses CRC-32 error checking and a modulation technique known as pulse position modulation, which uses the position of pulses in time to represent the data.

The IrDA standard include its own mandatory data link protocol (IrLAP), management protocol (IrMP) as well as optional transport protocols and other protocols to support particular functions.

3.1.4 Bluetooth

Bluetooth is a low-cost, low power short-range radio technology developed by the Bluetooth Special Interest Group made up initially of Ericsson, Intel, Nokia and Toshiba but now also containing Microsoft and many other members. It is has been designed to carry voice and/or data between mobile devices, such as mobile phones, hands-free headsets, digital cameras, lap-top computers and Personal Digital Assistants within a noisy radio environment in the unlicensed 2.4 GHz band. Bluetooth's signalling rate is 1 Mbit/s and it can support asymmetric data rates of 721 kbit/s and 57.6 kbit/s or symmetric rates of 432.6 kbit/s within a range of 10 metres. Bluetooth can also use this bandwidth to support up to three full duplex 64 kbit/s voice channels. Data is supported by Asynchronous Connection-Less (ACL) point-to-multipoint links and voice is supported by Synchronous Connection-Oriented (SCO) point-to-point links.

Up to eight active Bluetooth devices can form an ad-hoc network, called a piconet. One of the devices has to act as a master. Communication can only take place between a master and a slave. Two slaves cannot communicate with each other directly. A piconet can also support up to 255 non-active (or parked) devices, which can only become one of the eight active devices if there are less than eight active devices or if one of the active devices becomes parked. Up to ten piconets can exist and inter-operate in the same room as a scatternet formed when a slave of one piconet becomes a master of another and each bridging traffic between two piconets. Bluetooth uses TDMA[9],

[8] *Return to Zero, see Volume 1, Section, 8.3.6.4*

[9] *Time Division Multiple Access, see Volume 1, Section 7.3.8.*

under the control of the master, to allocate channels to timeslots and FHSS[10] to transmit the timeslots and minimise the effects of interference. Each piconet follows a different frequency hopping pattern. Severe interference is likely to reduce the data rate, but will not stop Bluetooth from working altogether.

Bluetooth uses a 48-bit addressing scheme similar to that used by IEEE 802. It uses a FSK[11] modulation technique and CRC-16 error detection. For SCO, detected CRC errors result in frames being discarded. Three error correction techniques are used: ARQ[12] is used for ACL and two optional types of FEC[13] for both ACL and SCO. 1/3 FEC is applied to packet headers for both ACL and SCO and for some ACL data fields. It simply repeats bits three times. 2/3 FEC is used by some ACL and packet types and uses Hamming codes.

Bluetooth has a Link Management Protocol to set up and control links and a Logical Link Control and Adaptation Protocol (L2CAP) which is its data link protocol and a protocol above this known as RFCOMM[14] which emulates a EIA-232 serial interface, so that software that normally runs over a serial interface can also run over Bluetooth.

Bluetooth incorporates a Service Discovery Protocol that allows applications to discover what functions are supported by other Bluetooth devices. Bluetooth creates a database of trusted devices following authentication which involves pairing the devices by entering PIN numbers on both.

It supports three modes of security: Mode 1 offers no security and is used by devices that have no secure applications. It can be used for transferring information such as business cards or calendar information between PDAs. Mode 2 offers service level security by means of authentication and encryption which can be varied for different applications. Mode 3 offers link mode security where all data links are encrypted from the time they are established using keys derived from the authentication process.

The physical and data link layers of Bluetooth is now being standardised as Wireless Personal Area Network (WPAN) by the IEEE 802.15 committee in conjunction with the Bluetooth Special Interest Group. It should be noted that Bluetooth uses the same frequency range as IEEE 802.11b[15] and that Bluetooth is likely to cause interference when used near WiFi hotspots. The IEEE have set up a task group to make recommendations that will help the two to co-exist.

Activity 3.2

Find some information about the protocol layers used by Bluetooth and how they relate to the hybrid reference model.

Activity 3.3

Research the application functions that are supported by Bluetooth technologies on mobile phones.

3.2 Storage Area Networks (SANs)

SANs are similar in their range to local area networks but are dedicated networks that connect computers to data storage devices. Historically, computers have used external parallel buses such as the Small Computer Systems Interface (SCSI) to connect their data storage devices. With the advent of disk arrays and data warehousing, a requirement grew to build networks to allow many machines to access many storage devices. There are two distinct ways that this can be done. Network Attached Storage uses conventional LANs (or WANs) to carry a disk block protocol such as SCSI

[10] *Frequency Hopping Spread Spectrum, see Section 3.3.5 of this Section.*

[11] *Frequency Shift Keying, see Volume 1, Section 8.3.6.3.*

[12] *Automatic Repeat Request, see Volume 1, Section 7.3.6.2.*

[13] *Forward Error Correction, see Volume 1, Section 7.3.6.2.*

[14] *Radio Frequency Communications*

[15] *Also known as WiFi, see Section 3.3.5 of this chapter.*

over the IP network layer protocol. This solution is good for a file server accessing whole files. But when the computer's operating system wants to transfer blocks of raw data efficiently, this is not an effective solution, in terms of latency and processing overhead. To do this a Storage Area Network running a specially designed protocol called Fibre Channel is preferred.

3.2.1 Fibre Channel[16]

Fibre Channel was invented by IBM and has been standardised by ANSI as an integrated set of standards. It was designed as a high speed protocol, supporting 100, 200, 400 and 1,200 Mbit/s over several kilometres of optical fibre (it can also be implemented over copper). It was specifically designed for use between computers and data storage devices to carry a number of block-based protocols, but is mainly used to carry SCSI. It can also carry IP.

Fibre Channel can support three different topologies. The simplest is a point-to-point topology between just two devices. The second is an arbitrated loop, which is a ring topology that supports up to 127 devices. Before transmitting a device must arbitrate to gain control of the loop. Contention is resolved by giving control to the device that has the lowest physical address. This device then has control of the loop for as long as required, but it is not allowed to arbitrate again until all the other devices have had the opportunity to arbitrate. The loop is often collapsed into a Fibre Channel hub, to simplify the wiring and protect the loop from breaking. The third topology is known as fabric, named after the cross-point switch it uses. This allows many devices (up to 2^{24}) to communicate with each other at the same time.

Three main classes of service are supported: Class 1 is a connection-oriented service equivalent to a dedicated fixed bandwidth physical connection; Class 2 is an acknowledged connectionless service and Class 3 is an unacknowledged connectionless service.

Fibre Channel supports flow control, which operates buffer-to-buffer or end-to-end using credit, which defines the rate at which devices can accept data. Each device must indicate its credit before establishing communications. Fibre Channel uses unique 64-bit port addresses known as WorldWide Names (WWNs), which are allocated to manufacturer's by the IEEE in a similar way to MAC addresses[17].

Fibre Channel uses 8B/10B[18] encoding and CRC-32 error checking.

Activity 3.4

Search for some information about the protocol layers used by Fibre Channel and how they relate to the hybrid reference model.

3.3 Local Area Networks (LANs)

Local Area Networks became popular in the 1980s as a means to share data and expensive peripherals (such as printers) between PCs in offices. The IBM PC had just been launched (without any networking capability) and was being installed in large numbers by departments of many companies. Because the original PC was a stand-alone device, its introduction presented a number of problems. Firstly, data produced on one PC often had to be transferred to other PCs. The only way to do this was by means of a $5^{1}{}_{4}$ inch floppy disk. The actual transfer of data was not so much a problem, the real problem was ensuring that everyone using the data was working the most up-to-date version of it. There was therefore a need for central file storage, where everyone in the department could access the latest versions of data files. The other problem was that hard disk drives and peripherals such as

[16] *ANSI X3T11*

[17] *Media Access Control addresses. See Volume 1, Section 7.3.2.*

[18] *8 Binary / 10 Binary, See Volume 1, Section 8.3.6.4.*

printers were in those days rather expensive and a great deal of money could be saved if users were able to share them. This all led to the urgent need for a centralised file server and print server and a network over which files could be transferred. LANs were the solution to these problems they were soon being widely implemented by enterprises.

This itself created further problems as different departments within enterprises often implemented their own LANs and these were sometimes incompatible. A need arose to connect LANs within a building or across a campus. This could and sometimes had to be done using network layer protocols such as IP, but is often desirable to do this at the data link layer. Although it could be done by creating a single large LAN using bridges or swithes, it is often preferable to link LANs together using a higher speed LAN that is used solely for that purpose and does not have any stations directly connected to it. Such a LAN is called a Backbone LAN. A common design is to implement a separate LAN on each floor of a building using switches and then connect these switches to a Backbone LAN that runs in the vertical risers between the floors.

3.3.1 Ethernet

Ethernet was developed in 1976 by Xerox at their Palo Alto Research Center (PARC). The protocol was based on an earlier packet radio protocol (ALOHA) developed by the University of Hawaii and used to provide a packet switched radio data network between the Hawaiian Islands. It solved the multiple access problem using CSMA/CD[19] as its access method. Although Ethernet broadcasts over a wired medium (originally a coaxial cable) the contention problem between devices was the same as that experienced and solved by ALOHA. The developers of Ethernet therefore chose to implement a CSMA/CD protocol with a binary exponential back-off algorithm.

Ethernet was marketed by a consortium of Digital, Intel and Xerox, known as the DIX consortium. It was the first protocol specifically designed for local area networking. Some earlier LANs had been built using HDLC[20]. Ethernet arrived on the market at just the right time for enterprises trying to share data and peripherals between PCs. Ethernet met this need and quickly became the de facto standard for local area networking. The mass production of Network Interface Cards (NICs) which could be installed in the expansion slots of PCs and servers led to a reduction in prices and the cost of installing LANs could easily be justified. As a result LANs, and Ethernet in particular, came into widespread use in offices. Along with other LANs, Ethernet uses 6-byte MAC addresses burnt into the NICs. The protocol supports unicast, multicast and broadcast addresses.

There are currently two variants of Ethernet frame formats[21] in use today. There are subtle differences between them regarding such things as the last byte of the preamble, but the main difference is in how the protocol indicates which network layer protocol is being carried.

- **Ethernet II.** The original Xerox protocol (Ethernet I), which is now obsolete, had a length field but no field for de-multiplexing network layer protocols. The DIX consortium redefined the protocol as Ethernet II and replaced the length field with a type field which allows it to multiplex and de-multiplex the different network layer protocols that it can carry. The IETF[22] standardised on Ethernet II for carrying IPv4.
- **IEEE 802.3.** The Ethernet protocol standardised by the IEEE[23] is known as 802.3 after the sub-committee that specified it. IEEE 802.3 returned to using the length field and uses the SSAP[24] and DSAP[25] fields in the LLC[26] header for multiplexing and de-multiplexing different network layer protocols. A version of 802.3 without an 802.2 sub-layer known as

[19] Carrier Sense Multiple Access with Collision Detection, see Volume 1, Section 7.3.8.

[20] High-level Data Link Control, see Volume 1, Section 7.5.

[21] Ethernet II and IEEE 802.3, see Volume 1, Section 7.8

[22] Internet Engineering Task Force, see Volume 1, Section 3.3.

[23] Institute of Electrical and Electronic Engineers, see Volume 1, Section 3.3

[24] Source Service Access Point, see Volume 1, Section 7.7.

[25] Destination Service Access Point, see Volume 1, Section 7.7.

[26] Logical Link Control, see Volume 1, Section 7.7.

IEEE 802.3 Raw, exists and is used by Novell. A number of suppliers, such as IBM, Novell and Microsoft supported IEEE 802.3 but Ethernet II remained popular because of the IETF specifications. Because LLC only allows one byte for specifying the network layer protocol used, as opposed to two bytes supported by Ethernet II, a further sub-layer has been defined to support to allow IEEE 802.3 to support the full range of Ethernet II types. This is known as the Sub-Network Access Protocol (SNAP). It does this by using an LLC SSAP and DSAP codes AA16 which signifies that a SNAP header follows the LLC header.

Ethernet, suffers from having a number of different frame format standards, but all is not as bad as it first appears, as the different formats can coexist on the same LAN. This is because the lowest value of the Ethernet type field has been defined as 0600_{16} and the maximum length of an Ethernet frame is 1500 bytes which is coded as $05DC_{16}$. An Ethernet implementation is therefore able to determine whether the frame structure being used is Ethernet II or IEEE 802.3 by the value of the length/type field and hence the meaning of the field.

Ethernets can operate at different speed over different media which have different characteristics such as maximum cable lengths. Ethernet CSMA/CD specifications require that the round trip time on any segment is less than that required to transmit the minimum frame size of 512 bits to ensure that all collisions are detected. This will limit the maximum segment length for different data rates.

3.3.1.1 Ethernet designations

A naming convention (which has evolved over the years and is now very complex and confusing) is employed to describe these different types of Ethernet, as described in Table 3.2 below. You are not expected to learn the meaning of all the various parts of the designation, but you are expected to know the basic structure and the first four fields in the table which are commonly used.

Table 3.2: Ethernet naming convention

Field	Values	Meaning
Data Rate	1	1 Mbit/s
	10	10 Mbit/s
	100	100 Mbit/s
	1000	1 Gbit/s
	10G	10 Gbit/s
Transmission (after Data Rate)	Base	Baseband
	Broad	Broadband
	Pass	Passband (using bandpass filters, as in VDSL)
Max. Segment Length	2	185 m (approx 2 x 100 m)
(after Base or Broad)	5	500 m (5 x 100 m)
	36	3,600 m (36 x 100 m)
Media (after Base)	-C	Copper (Twinax cable)
	-F	Fibre
	-LH	Long Haul over dark fibre
	-T	Twisted pair (can also occur after Pass)
	-VG	Voice Grade twisted pair
Fibre Wavelength (after Base)	-E / -Z	Extra Long Wavelength(1550 nm)
	-L	Long Wavelength (1310 nm)
	-S	Short Wavelength (850 nm)

Table 3.2: Ethernet naming convention (cont.)

Field	Values	Meaning
Fibre Configuration (after Base)	-B	Bi-directional Point-to-Point
	-P	Passive Optical Network (Point-to-Multipoint)
Fibre Type (after -F)	B	Backbone
	L	Long
	P	Passive (without repeaters)
Twisted Pair Type (after -T)	S	Short Reach
	L	Long Reach
Coding (after -E, -L, or -S)	R	64B/66B
	W	WAN Interface Sublayer (64B/66B in SDH)
Coding (after -E, -L, -S, -B, -P, or -Z)	X	8B/10B
Fibre Mode (after -LR)	M	Multimode
Max. Segment Length (after BX, LX or PX)	10	10 km
Max. Segment Length (after PX)	20	20 km
Number of Fibres/Cable Pairs (after -T or X)	2 4	

Table 3.3 below gives examples of Ethernets (for reference) using the naming convention. You are not expected to know the details contained in this table, but you are expected to be able to recognise the speed and type of commonly implemented Ethernets (discussed in later this chapter) from their designations.

Table 3.3: Ethernet designations

Ethernet designation	Duplex	Media	Max segment length(m)	Comments
1Base5	Half	2 Cat 3 UTP	500	1 Mbit/s Star-based LAN using Twisted Pairs - Obsolete
2Base-TL	Full	1 Cat 3 UTP	2.700	2 Mbit/s Ethernet in the First Mile (EFM) over SHDSL
10Base5	Half	Thick Coax	500	10 Mbit/s Thicknet Coaxial Bus
10Base2	Half	Thin Coax	185	10 Mbit/s Thinnet Coaxial Bus
10Base-T	Full	2 Cat 5 UTP	100	10 Mbit/s Hubbed/Switched Ethernet
10Broad36	Half	Thick Coax	1,800	10 Mbit/s Coaxial Bus (3,600m between two stations) – Obsolete
10Base-FB	Half	2 MMFs	2,000	10 Mbit/s Backbone Ethernet using Multimode Fibre
10Base-FL	Full	2 MMFs	2,000	10 Mbit/s Ethernet using Multimode Fibre
10Base-FP	Half	2 MMFs	500	10 Mbit/s Ethernet using Multimode Passive Fibre
10Pass-T	Full	1 Cat 3 UTP	750	10 Mbit/s Ethernet in the First Mile (EFM) over a VDSL
100Base-BX10	Full	1 SMF	10,000	100 Mbit/s EFM over a single bidirectional point-to-point SMF
100Base-FX	Full	2 MMFs	2.000	100 Mbit/s Fast Ethernet over dual Multimode Fibre
100Base-LH	Full	2 SMFs	80,000	100 Mbit/s Fast Metro Ethernet – Long Haul over dark fibre
100Base-LX	Full	2 SMFs	5,000	100 Mbit/s Fast Ethernet using long wavelength LASERs
100Base-LX10	Full	2 SMFs	10,000	100 Mbit/s EFM using long wavelength LASERs
100Base-T2	Full	2 Cat 3 UTP	100	100 Mbit/s Fast Ethernet using 2 Twisted Pairs
100Base-T4	Half	4 Cat 3 UTP	100	100 Mbit/s Fast Ethernet using 4 Twisted Pairs
100Base-TX	Full	2 Cat 5 UTP	100	100 Mbit/s Fast Ethernet using Twisted Pair
100Base-VG	Full	4 Voice Grade UTP	100	Not strictly Ethernet - uses polling and not CSMA/CD
1000Base-BX10	Full	1 SMF	10,000	Gigabit EFM over a single bidirectional point-to-point SMF
1000Base-CX	Full	2 Twinax Cables	25	Gigabit Ethernet using Twinax cables - Obsolete
1000Base-LH	Full	2 SMFs	70,000	Gigabit Metro Ethernet – Long Haul over dark fibre

Table 3.3: Ethernet designations (cont.)

Ethernet designation	Duplex	Media	Max segment length (m)	Comments
1000Base-LX	Full	2 SMFs/MMFs	5,000	Gigabit Ethernet using Long Wavelength LASERs
1000Base-PX10	Full	1 SMF	10,000	Gigabit EFM over point-to-multipoint SMF using passive optics
1000Base-PX20	Full	1 SMF	20,000	Gigabit EFM over point-to-multipoint SMF using passive optics
1000Base-SX	Full	2 SMFs/MMFs	550	Gigabit Ethernet using short wavelength LASERs
1000Base-T	Full	4 Cat 5 UTP	100	Gigabit Ethernet using two Twisted Pairs
1000Base-ZX	Full	4 SMFs	70,000	Gigabit Metro Ethernet using extended wavelength LASERs
10GBase-CX4	Full	4 Twinax Cables	15	10 Gb Ethernet using Twinax cables - Obsolete
10GBase-ER	Full	2 SMFs	40,000	10 Gb Metro Ethernet over dark fibre
10GBase-EW	Full	1 STM-64 SDH cct	40,000	10 Gb Metro Ethernet over SDH WAN circuit (actually 9.95 Mbit/s)
10GBase-LR	Full	2 SMFs	10,000	10 Gb Metro Ethernet over dark fibre
10GBase-LRM	Full	2 MMFs	220	10 GbE over MMF using electronic dispersion compensation
10GBase-LX4	Full	2 SMFs	10,000	10 GbE (300 m over MMF or 10km over SMF using 4 WDM channels
10GBase-LW	Full	1 STM-64 SDH cct	10,000	10 Gb Metro Ethernet over SDH WAN circuit (actually 9.95 Mbit/s)
10GBase-SR	Full	2 MMFs	300	10 Gb Ethernet using short wavelength LASERs
10GBase-SW	Full	1 STM-64 SDH cct	300	10 Gb Metro Ethernet over SDH WAN circuit (actually 9.95 Mbit/s)
10GBase-T	Full	4 Cat 7 UTPs	100	10 Gb Ethernet using Unshielded Twisted Pair cables

3.3.1.2 Traditional Ethernets (10 Mbit/s)

Bus Ethernets

The original DIX Ethernet (10Base5[27]) used a thick (10mm) coaxial cable, similar to that used to connect TV sets to aerials, in a bus topology with stations being connected on a spur via a transceiver (sometimes called a vampire tap) that were tapped into the cable at intervals along its length. The physical interface used on the spur cable which could be up to 50 meters long was defined as the Attachment User Interface (AUI). As a result of the thick cable, it is sometimes referred to as Thicknet. More commonly though it is called 10Base5, with 10 indicating the data rate, Base indicating that it uses baseband signalling and 5 indicating that the maximum cable length is 500 meters.

An alternative and cheaper Ethernet is known as 10Base2[28] (sometimes called Thinnet or Cheapernet) cabling method used a thinner (5mm) coaxial cable and a 3-way connector of a type known as BNC[29] rather than a vampire tap. The PC could again be connected to the 3-way connector on the bus via a spur cable and a transceiver or more often an internal transceiver on the NIC card was used which allowed the 3-way connector to be directly connected to the NIC card at the back of the PC. The thin coaxial cable could only carry signals 185 meters and using the standard naming convention this type of Ethernet is known as 10Base2.

Both 10Base5 and 10Base2 were quite expensive to install. The coaxial cable was expensive and because it is so heavy and inflexible, it is difficult to run it through ducts.

Cabling for both 10Base5 and 10Base2 is expensive, bulky and quite difficult to install.

Traditional Ethernets use baseband signalling (the digital signals are not modulated onto another frequency) at 10 Mbit/s with Manchester encoding[30] at the physical layer.

[27] *IEEE 802.3*

[28] *IEEE 802.3a*

[29] *Bayonet Neill Concelman (after its inventors) sometimes also erroneously called British Naval Connector.*

[30] *See Volume 1, Section 8.3.6.4.*

Hubbed (or half duplex) Ethernets

Attempts were made to run local area networks using UTP cable in a star configuration. At the centre of the star was an active hub which when it receives a frame on port will broadcast it out on all the other ports (apart from the one from which it received the frame). A hub can therefore be regarded as a multi-port repeater. Thus the star network is able to emulate the standard bus network running the same Ethernet protocol and can be described as a physical star and logical bus network. This type of network running at 10Mbit/s is known as 10Base-T[31]. The star network is now the preferred topology for all types of Ethernet.

Switched (or full duplex) Ethernets

A further improvement can be made by replacing the hub by a switch. The switch is an intelligent device that examines a frame's destination MAC address and only forwards the frame out of the one port to which the device with that physical address is attached. It learns the physical addresses of each device from the frames that it receives in the same way as a bridge. If it receives a frame with a destination address that it does not recognise, then it broadcasts the frame out of all its ports, apart from the one on which it was received. Using a switch rather than a hub greatly improves the efficiency of an Ethernet, as it converts a single collision domain, where transmissions from any device can collide with transmissions from any other device, to multiple collision domains, where there is usually only one device able to transmit on the physical medium. As a result switched Ethernets can support much higher throughput than hub-based or bus Ethernets.

Hubbed and switched Ethernets often provided dedicated media for each direction of transmission. This means that for switched Ethernets no collisions can ever occur and there is no requirement for CSMA/CD. Attached devices can receive and transmit at the same time and hence can operate in full duplex mode. Also the segment length limit requiring the RTT[32] to be less than the time taken to transmit 512 bits is no longer required and hence segment lengths can be longer. If the same media is shared for both transmitting and receiving (as is the case with a hub) then a single device will be unable to receive and transmit at the same time and will hence operate in half duplex mode. Full duplex Ethernets also double the effective capacity as 10 Mbit/s can be carried simultaneously in both directions giving an overall maximum theoretical capacity of 20 Mbit/s.

Switches can operate in different modes.

- Store and Forward mode is where the whole frame is stored in a buffer and the CRC field is checked before forwarding.
- Cut-through mode is where the switch starts to forward the frame as soon as the destination physical address has been received.
- Fragment Free mode is where the switch starts to forward the frame after the first 64 bytes have been received. Fragments of 64 bytes or less (also called runts) are often created by collisions and by checking that no collision has occurred while the first 64 bytes of a frame have been received the switch can ensure that no fragments are generated.
- Adaptive mode is where the switch continually monitors the number of collisions and errors and determines which mode is best to use.

Clearly, cut-through mode is superior in its delay performance, but only if the number of collisions and hence errors are low. Cut through mode is ideal with full duplex Ethernets where collisions never occur. Store and Forward mode will delay every frame, but will ensure that frames containing errors

[31] *IEEE 802.3i*

[32] *Round Trip Time.*

are not forwarded and will perform best in half-duplex Ethernets that have a high collision rate. Fragment Free is a compromise between the two, while Adaptive mode can dynamically adjust the mode depending on the collision rate.

3.3.1.3 Fast Ethernet (100 Mbit/s)

Fast Ethernet works at 100 Mbit/s and was originally intended for use in backbone LANs, but is now used routinely in LANs supporting servers or many PCs requiring high bandwidth services. The upgrade path from 10Base-T to 100Base-TX[33] or 100Base-T2[34] or from 10Base-FL[35] to 100Base-FX8[36] is relatively straightforward as the same cable can be used, as they support the same maximum segment lengths. 100Base-TX requires an extra cable pair, but Cat 3 cable always comes with two pairs, only one of which is used in 10Base-T. Only the Network Interface Cards and switches need to be changed or reconfigured to work at a higher speed.

Fast Ethernet supports the same frame structure, minimum and maximum frame lengths and addressing as traditional Ethernet as well as the MAC layer including the CSMA/CD access method (if appropriate). This means that both types of Ethernet are fully compatible and that a switch can actually support both speeds. Typically lower specification PCs can be connected to the switch at 10 Mbit/s and servers and high specification PCs and trunk links to other switches can be connected at 100 Mbit/s. The speed mismatch will not usually cause any problems because frames received at high speed ports are likely to be destined for many low speed ports and it is unlikely that any 10Mbit/s port will ever need to receive frames at a higher data rate than that supported. On most switches, it is possible to configure switch ports for autonegotiation where the speed at which a device is operating is detected by the switch and configured accordingly. This allows a single device to be configured to work at either speed without having to reconfigure the switch.

100Base-T Ethernets do not use Manchester encoding but uses various alternative more modern coding methods, such as MLT-3[37] for 100Base-TX, PAM5[38] for 100Base-T2, 8B/6T NRZ[39] for 100Base-T4 and 4B/5B[40] NRZI for 100Base-FX.

100Base-VG[42] was an attempt to produce a single LAN standard for 100Mbit/s backbone LANs. It used four pairs of Cat 3 UTP (also known as voice grade) and hence the initials. It is also sometimes called 100VG-AnyLAN as it was designed to carry both Ethernet and Token Rings frame types on the same hub. It was originally proposed by HP[43] and the IEEE started to standardise it as an 802.3 protocol, but because it used a polling access method to overcome segment length limitations rather than CSMA/CD, it was decided to progress the standard via a new committee (802.12). It was not successful and is now practically extinct as CSMA/CD protocols were developed that could support 100m segment lengths.

3.3.1.4 Gigabit Ethernet (1 Gbit/s)

Gigabit Ethernet (GbE) supports speeds of 1 Gbit/s and was designed for use over backbone LANs. It is required because many organisations upgraded their LANs to Fast Ethernet which put huge traffic loads on their backbone LANs. GbE is also required for server farms and may ultimately be required at the desktop for applications that require very high bandwidth. GbE supports the same frame structure, maximum frame lengths and addressing as traditional and Fast Ethernet as well as the MAC layer including the CSMA/CD access method (if appropriate), but the minimum frame size has

[33] *IEEE 802.3u*

[34] *IEEE 802.3y*

[35] *IEEE802.3u*

[36] *IEEE802.3u*

[37] *Multi-Line Transmission – 3-level, see Volume 1, Section 8.3.6.4.*

[38] *Pulse Amplitude Modulation – 5 state.*

[39] *Non-Return to Zero, see Volume 1, Section 8.3.6.4.*

[40] *4 Binary / 5 Binary, see Volume 1, Section 8.3.6.4.*

[41] *Non-Return to Zero Inverted, see Volume 1, Section 8.3.6.4.*

[42] *IEEE 802.12*

[43] *Hewlett Packard*

been altered. The rule that restricts segment lengths so that the RTT is no more than the time taken to transmit 512 bits will result in the maximum segment length being impractically short. The 512 bit limit is therefore changed to 4096 bits and frames are padded out so that they are always at least 4096 bits (512 bytes) long. This is known as carrier extension. Another change introduced with GbE allows a station which has a number of short frames awaiting transmission to burst them consecutively as a single transmission, to avoid the overhead of carrier extension.

Although the GbE standard has gone to a lot of trouble to implement CSMA/CD for half duplex operation to be backwards compatible, it is rarely implemented and most GbE is full duplex, so the limits on maximum segment length are governed by signal strength rather than collision detection issues.

GbE can be implemented over copper or fibre. Early copper implementation, such as 1000Base-CX[44] used a special twin coaxial cable (known as twinax) and 8B/10B[45] coding, but modern implementations use 1000Base-T[46] which uses 4 Cat 5 UTPs and PAM5 coding.

Fibre implementations of GbE cannot use LEDs[47] as they cannot be switched on and off quickly enough, so LASERs[48] have to be used. These can use short (1000Base-SX[11]), or long (1000Base-LX[11]) wavelengths and also use 8B/10B coding.

3.3.1.5 10 Gigabit Ethernets (10 Gbit/s)

The main driver for 10 Gigabit Ethernets (10GbE) is the need to switch large volumes of Internet traffic between ISPs across a shared LAN in a building that acts as an interconnection point between ISPs[49]. 10GbE will also be useful for large corporations who have a requirement to switch large amounts of data between servers and their Intranets or the Internet.

Unlike other Ethernet standards 10GbE has from the outset been designed to support MAN and WAN communications. Also, unlike other Ethernet standards, it always runs in full-duplex point-to-point mode, so there is no possibility of any collisions and hence no need for collision detection. With 10GbE, Ethernet has finally freed itself from its CSMA/CD access method origins.

10GbE uses short (S) or long (L) wavelength LASERs with 8B/10B (X) or 64B/66B coding (R). 10GBase-T uses 4 Cat 7 UTPs and PAM-12 line code.

3.3.1.6 Metro Ethernet

An important requirement for many organisations is to interconnect their LANs over a metropolitan area network. This was often done in the past by routing over private circuits using HDLC, or using public networks such as frame relay, or ATM[50] or SMDS[51]. Only the latter two could support LAN speeds and network operator charges for these services were high. Using routers and a different data link protocol also introduced inefficiencies and reduced throughput. An ideal solution would be to buy fibre capacity from the network operator and run Ethernet protocols over the fibre between two LAN switches. Network Operators offer high speed LAN extension services but their tariffs normally increase significantly with speed, but some operators are willing to sell 'dark fibre' where optical connectivity is provided between two sites without LASERs and detectors. Customers can then buy their own LASERs and detectors to 'light' the fibre at whatever data rate they require. This allows customers to set up their own high speed LAN interconnections where the costs do not increase so severely as data rates increase.

[44] *IEEE 802.3z*

[45] *8 Binary / 10 Binary, see Volume 1, Section 8.3.6.4.*

[46] *IEEE 802.3ab*

[47] *Light Emitting Diode*

[48] *Light Amplification by Stimulated Emission of Radiation*

[49] *Such as the London InterNet eXchange (LINX)*

[50] *Asynchronous Transfer Mode, see Section 6.5 of this volume.*

[51] *Switched Multi-megabit Data Service, see Section 4.1.1 of this volume.*

100Base-LH can provide long haul connectivity up to 80 km while 1000Base-LH and 1000Base-ZX can reach up to 70 km. 10GBase-LR (using 64B/66B coding), 10GBase-LX4 (using 8B/10B coding) and 10GBase-LW can reach 10 km while 10GBase-ER (using 64B/66B coding) and 10GBase-EW can reach 40 km. 10GBase-LW and 10GBase-EW both operate over WANs using 64B/66B coding and encapsulate Ethernet frames within SDH[52] frames. They actually operate at about 9.95 Mbit/s to match the SDH STM-64 speed.

3.3.1.7 Ethernet in the First Mile (EFM)

EFM is a recent development of the protocol to run over broadband copper or fibre in the first mile (or the local loop) between customer premises and the public network. It makes sense to implement Ethernet here as Ethernet provides a simple and familiar interface which can operate at a range of speeds and for which standard Network Interface Cards exist and because of mass production they are very cheap. EFM is not only required for residential access, but is also required for business purposes to replace existing private circuit solutions and to provide integrated high speed access to various network services.

A number of solutions have so far been proposed for various media and topologies. For point-to-point services over copper at lower speeds 2Base-TL (for Twisted Pair Long Reach, but also sometimes called 2Base-S for SHDSL[53]) provide the equivalent of a 2Mbit/s private circuit to carry data over SHDSL circuits of up to 2.7 km. Currently a small business may lease a number of Nx64 kbit/s circuits to provide data communications to other sites or access to public data networks. These could all be carried over a single 2Base-TL circuit at greatly reduced cost.

For higher speed point-to-point services at 10 Mbit/s over copper, 10Pass-T (also sometimes known as 10Pass-V for VDSL[54]) can support 10 Mbit/s over 750m. VDSL, like ADSL[55] and unlike SHDSL, does not use baseband signalling as it splits off voice signals by means of a low pass filter, so it is described as using passband signalling. The maximum segment length is insufficient to reach a network operator's premises in most cases, so the operator has to install an Optical Network Unit in a street cabinet within reach of the customer's premises.

For 100 Mbit/s point-to-point services over fibre 100Base-LX10 can reach up to 5 km and for 1 Gbit/s point-to-point services over fibre 1000Base-BX10 can reach 10 km.

Finally, technology is currently being developed to offer point-to-multipoint services over a Passive Optical Network (PON). With this technology multiple sites are connected to a single tree topology fibre network and sites can communicate with each other using a particular wavelengths of light. The switching in the network is therefore carried out by users selecting different wavelengths and the network itself is completely passive. Because the network is point-to-multipoint it is ideal for broadcasting and multicasting. This capability is also useful for data communications and Ethernet protocols have been developed for use over Passive Optical Networks. 1000Base-PX10 and 1000Base-PX20 can carry Gigabit Ethernet over 10 and 20 kms respectively.

Activity 3.5

Find out the designations (E.g. 10Base-T etc.) of the all the different types of Ethernet are used by your institution or place of work to support the desktop and in the backbone. Find some information about all the Ethernet types you discover.

[52] *Synchronous Digital Hierarchy, see Section 4.2.1.1 of this volume.*

[53] *Symmetric High-bit-rate Digital Subscriber Line.*

[54] *Very-high-speed Digital Subscriber Line*

[55] *Asymmetric Digital Subscriber Line.*

3.3.1.8 Virtual LANs (VLANs)

LANs were historically set-up and administered on a departmental basis, but companies tend to reorganise and move employees around quite regularly, which causes a problem for the network managers who sometimes have reconfigure ports on switches and if the switches are not collocated then some new cabling will be necessary. Another issue is security. Some departments, notable Human Resources, Finance and Marketing departments hold sensitive information and are concerned that this information can only be accessed by members of their own departments. There has therefore been some resistance to merging or even bridging departmental LANs. Another problem results when LANs are merged or bridged is that of **broadcast storms**. A broadcast storm occurs when there is a sufficiently large number of broadcast messages on a LAN which collide with other messages and can make the LAN virtually unusable. Sometimes a faulty NIC card can cause a broadcast storm, but often they are caused by protocols that use an excessive amount of broadcasting. Clearly the larger the LAN (including a multi-switch LAN), the bigger this problem can be.

A solution to all of the above problems is to use Virtual LANs (VLANs). A VLAN can be thought of as a LAN that is configured by software on a LAN switch. The switch is configured to support a number of workgroups. Each workgroup is assigned its own VLAN. If an employee changes workgroups or moves to a different part of the building then any reconfiguration required can be done in the VLAN configuration rather than by reconfiguring ports on the switches.

Traffic between VLAN cannot be switched, but it can be routed. Routers however provide security functions that allow very tight control on what traffic can be routed which is not possible with switches. Network managers can therefore easily control traffic going to particular VLANs, by only allowing approved access and, by default, only members of the appropriate workgroup will be able to access systems on the VLAN. Furthermore, ensuring that all traffic between VLANs is routed and not switched, means that broadcast storms will not be forwarded from one VLAN to another, thus the larger LAN can be protected from broadcast storms on individual VLANs.

The network manager can define VLAN workgroups by:

- defining which switch ports belong to which VLAN (Port-based VLAN)
- defining which MAC addresses belong to which VLAN (MAC-based or Layer 2 VLAN)
- defining which IP addresses or which IP multicast address group belong to which VLAN (IP-based or Layer 3 VLAN)
- defining which multicast IP address belongs to which VLAN
- defining which applications can use the VLAN by means of the transport layer port number.

In a multi-switch LAN, when a switch receives a frame over a trunk from another switch, it must be able to tell which VLAN the frame relates to. There are three ways in which this can be done:

- Each switch can maintain a table of their VLAN members and can broadcast this table to the other switches periodically.
- TDM can be used on the trunk so that, for instance, frames for VLAN 1 always appears in timeslot 1.
- Each frame can be tagged with an additional header field that identifies the VLAN. This requires a change to the data link layer protocol or an additional sub-layer, but is the most common way of trunking VLANs.

Activity 3.6

Check whether Virtual LANs are used in your institution or place of work and if so, find out the names/identities of all the VLAN workgroups.

3.3.2 Token Ring[56]

The Token Ring network was invented by IBM for use with its office automation products and the specifications were handed over to the IEEE for standardisation.

The Token Ring as its name implies uses a ring technology with a token passing access method. It can operate at 1, 4 or 16 Mbit/s and uses Differential Manchester[57] encoding and the same 6-byte addressing scheme as Ethernet. The ring is connected using segments of Cat 3 UTP between stations. Each station, when powered, acts as a repeater for the signals circulating around the ring. If a station is switched off then a relay on the Network Interface Card operates to make a passive electrical connection through the card. This ensures that signals can pass through a station that is switched off. One of the stations has to act as an Active Monitor which must continually check that the ring is operating correctly and particularly that the same frame is not circulating the ring more than once and that the token is being circulated. If the Active Monitor detects that a frame has circulated more than once, it removes it from the ring. If it does not see a token before a timeout expires, it assumes that the token has been lost and creates a new one.

The token is a special 3-byte bit pattern that is passed from station to station around the ring. When a station wishes to transmit, it has to wait for the token to be received. It then takes the token off the ring, transmits its frame and the station which has the physical address indicated in the destination address field of the frame header retrieves the frame, performs a CRC check on it and if successful, it sets some bits in the frame status field to indicate that the frame has been successfully received by the correct station. When the frame returns to the transmitter with these bits set, it is removed from the ring and the token is then forwarded to the next station on the ring.

The token passing access method used ensures that a station is able to transmit a frame within a fixed time and that each station is treated fairly, apart from the use of priority and a scheme called early token release that is only used on 16 Mbit/s rings to improve efficiency. An upper bound on access time and fairness is not possible with Ethernet protocols, as under severe congestion the CSMA/CD algorithm means that an arbitrary time elapses before a frame is successfully transmitted without a collision. In the worst case, the frame may be discarded after the maximum number of attempts has been exceeded. Token Ring is therefore a deterministic protocol while Ethernet is non-deterministic.

Token Ring networks are vulnerable to cable breaks which will cause catastrophic failures. The danger of a cable break can be reduced by changing to a star topology (similar to that used by twisted pair Ethernet). The ring is effectively collapsed into a central hub known as a Multi-Station Access Unit (MAU) with spurs of twisted pair cables going out to each station and back to the hub. The relay that detects when a device is switched off is located in the hub and it will also be able to detect a cable failure and will close to bypass the spur going out to the device.

[56] *IEEE 802.5*

[57] *See Volume 1, Section 8.3.6.4.*

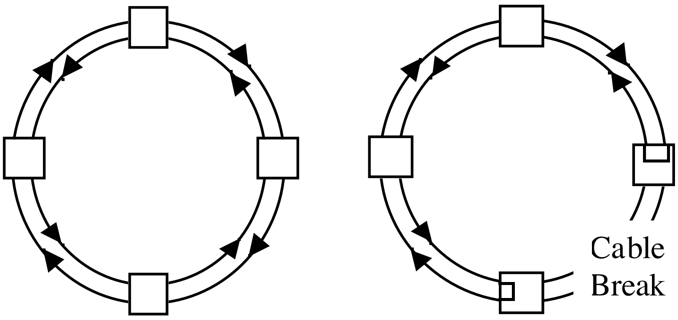
In many ways Token Ring is technically superior to Ethernet, but it has not been as successful in the marketplace. This is largely because Ethernet had a head start over Token Ring and is slightly simpler and cheaper to implement. As in most things success breeds success and the large number of Ethernets being implemented led to economies of scale and hence cheaper equipment. There may also have been some suspicion regarding IBM's involvement in its development, as at the time companies were attempting to escape the stranglehold of IBM's SNA[58] networking protocols.

3.3.3 Fibre Distributed Data Interface (FDDI)[59]

Unlike virtually all other popular LAN protocols, FDDI was not standardised by the IEEE. It was in fact standardised by ANSI[60] and ratified by ISO[61]. It was designed as for use in LAN backbones. It is highly compatible with other LAN protocols, such as Ethernet and Token Ring when connected via bridges. It operates at 100 Mbit/s uses a dual fibre ring topology with data circulating in different directions around each ring. It can use mono-mode or multi-mode fibre. Within a building multi-mode is likely to be used for cost reasons, but mono-mode may be used over a campus as it supports longer cable lengths. FDDI uses a token passing access method, similar to token ring, 4B/5B encoding, NRZI signalling and IEEE 802 MAC addressing.

At any one time, one ring is deemed to be the primary ring and the other the secondary ring which is always on hot-standby in case the primary ring breaks. If both rings break in the same place as in Figure 3.1 below, then the FDDI nodes either side of the break can loop the fibres together to make a single double size ring and thus maintain communications.

Figure 3.1: FDDI Recovery from a single cable break affecting both fibres



As with Fibre Channel and Ethernet hubs and Token Ring MAUs, the FDDI ring is best collapsed into a box known as a concentrator with fibre spurs going out to individual stations and back that can be bypassed when the station is switched off or when there is a cable fault. The need for this is even greater for FDDI as optical power limitations mean that it would not be feasible to bypass a station on a large ring, but it can be done when the ring is collapsed into a concentrator.

A copper version of FDDI, known as CDDI, has also been defined that operates at 100 Mbit/s over a dual collapsed ring with spurs of up to 100m of STP[62] going to and from the desktop. This was specified to allow FDDI to be extended to the desktop using cheaper technology than FDDI.

Neither FDDI and CDDI have enjoyed long-term success in the market place, although they are resilient and deterministic in the maximum time they take to transmit a frame. The protocols are complex and the technology is

[58] Systems Network Architecture

[59] ANSI X3T12

[60] American National Standards Institute, see Volume 1, Section 3.3.

[61] International Organization for Standarization see Volume 1, Section 3.3.

[62] Shielded Twisted Pair see Volume 1, Section 8.3.1.1.

expensive and could not compete with Ethernet which could not only be developed to offer equivalent speeds at less cost, but could also eventually provide an upgrade path beyond 100 Mbit/s.

3.3.4 Wireless LANs (WLANs)

WLANs have become increasingly popular in the last few years. The main reasons for this are that it is very expensive to cable a building and companies often move their offices to new buildings. Every time they do so, there is a large cost. Secondly a large number of employees now own lap-top computers and expect to be able to use them anywhere within the building. There is a considerable extra cost of providing spare LAN ports for lap-tops and a certain amount of hassle for users in finding these ports and connecting their lap-tops to them. Even then, the user cannot roam around the building and maintain a continual connection with the network. Users have experienced the flexibility that has come with mobile phones and expect something similar for data. Wireless LANs have been standardised by the IEEE 802.11 Committee who have defined two service sets.

- The Basic Service Set (BSS) consist of a number of wireless stations and a single Access Point (AP) or base station which has a connection to the fixed network, usually in the form of a wired IEEE LAN.
- The Extended Service Set (ESS) also includes multiple BSSs with their Access Points and stations. The APs are connected by a Distribution System (DS) which can be any IEEE LAN (wired or wireless).

There are three types of station supported:

- No Transition Mobility, where the station always remains in the same BSS
- BSS-Transition Mobility, where the station can move from one BSS to another but must stay within the same ESS
- ESS-Transition Mobility, where the station can move between ESSs.

IEEE Wireless LANs are based on Ethernet, but they cannot use the CSMA/CD access method. This is because listening for collisions while transmitting is not feasible. It would require duplicate radio circuitry which would double the cost of the equipment. Wireless stations therefore have to switch between transmitting and receiving and thus work in a half duplex mode. Also, even if the station could transmit and receive at the same time, it is quite possible that it would not be able to detect collisions caused by other stations in the BSS due to obstacles that cause fading and to the attenuation of the signals. For the above reasons another access method must be devised and the method chosen is CSMA/CA where CA stands for Collision Avoidance. With this method, a station wanting to transmit follow the following procedure:

- Before transmitting, it puts its radio into receive mode and senses the power levels at the carrier frequency.
- If it does not sense a transmission, it waits for a short period and transmits a Request to Send (RTS) frame. The RTS frame includes an indication of the length of time that will be required to transmit the frame.
- If it detects another station is transmitting it will carry out a binary exponential back-off and sense the carrier frequency again later, until it detects no other transmission, after which it will send its RTS frame.
- The receiver will respond to the RTS frame with a Clear to Send (CTS) frame which also includes the indication of the length of time it will take to transmit the frame.

- If no CTS is received, a collision is assumed and the transmitter backs off.
- Once the transmitter has received the CTS, it knows that it has access to the channel and can transmit its data frame after a short wait.
- The collision avoidance method works because all other stations in the BSS will see the RTS or the CTS and know how long the channel will be occupied for. They can therefore delay their next attempts to transmit accordingly.
- The transmitter must then await an acknowledgement from the receiver that the frame has been received. The acknowledgement is necessary, as the transmitter would have been unable to detect any collision while it was transmitting the frame.

The CSMA/CA access method is mandatory for all 802.11 WLANs. It is known as the Distributed Coordination Function (DCF). It is ideal for carrying data traffic and scales well as the number of stations on the WLAN grow. Like Ethernet it is non-deterministic and there is no upper limit to the time that it can take to transmit a frame, or a guarantee that a frame will be transmitted at all. For certain applications, such as voice, it is desirable to have an upper bound on frame transmission time. 802.11 allows this to be done by an optional polling method called Point Coordination Function (PCF). With PCF, the Access Point eliminates contention by polling each station in turn and therefore an upper bound to frame transmission time can be guarantied. PCF and DCF can coexist on the same WLAN by allocating different timeslots to each method. PCF does not scale as well as DCF, as the single Access Point in a BSS cannot poll an ever increasing number of stations.

802.11 defines a number of services offered by the Distribution System. These are:

- association, which allows the station to associate itself with an Access Point
- disassociation, which allows the station to remove itself from an association with an Access Point
- re-association, which allows a station to change its BSS by associating with a different Access Point which can be done without any loss of data during the handover
- distribution, which forwards frames to the correct destination via the Distribution System
- integration, which converts frame formats, where necessary, between the 802.11 protocol and the protocol of the Distribution System.

Other services are offered by the stations. These are:

- authentication, which allows stations to establish their identities by responding to challenges using their secret keys prior to transmitting data to each other
- de-authentication, which allows an authentication relationship between two station be terminated
- privacy, which allows stations to encrypt and decrypt the data they are transmitting using the RC4 algorithm
- data delivery, which allows data to be transmitted unreliably between stations.

The original 802.11 specification supported relatively low data rates (1 or 2 Mbit/s) using three alternative transmission schemes. These were:

- Direct Sequence Spread Spectrum (DSSS) operating in the 2.4 GHz band, where each bit from each transmitter is replaced by a sequence of bits (known as the chip code) which has the effect of spreading the signal across a large frequency range and increasing its immunity to noise.
- Frequency Hopping Spread Spectrum (FHSS) also operating in the 2.4 GHz band, where the carrier frequency hops over a range of frequencies according to an agreed sequence.
- Infrared using infra-red light which cannot pass through solid objects and is affected by the presences of sun-light. It was therefore not a popular choice of technology.

The original specifications have now been supplanted by separate specifications that offer higher data rate. The main ones are:

- IEEE 802.11a, which offers between 6 and 54 Mbit/s in the 5 GHz band and uses Orthogonal Frequency Division Multiplexing (OFDM), which is similar to FDM except all the sub-bands are used by the same transmitter at the same time
- IEEE 802.11b, which offers 1, 2 5.5 and 11 Mbit/s in the 2.4 GHz band and uses High Rate Direct Sequence Spread Spectrum (HR-DSSS) which is similar to DSSS but operates at lower frequencies and can hence support a higher data rate
- IEEE 802.11g, which offers 54 Mbit/s in the 2.4 GHz band and also uses OFDM.

Activity 3.7

Find some information about the protocol layers used by IEEE 802.11 LANs and how they relate to the hybrid reference model.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. A Bluetooth piconet consists of a master and up to 7 active slaves, but the slaves cannot communicate with each other directly.

ii. IN IEEE 802.11 LANs, authentication is a service provided by the Distribution System which allows the station to authenticate itself to an Access Point.

iii. Token Ring operates at 1, 4 or 16 Mbit/s and uses Manchester encoding.

iv. Implementing VLANs not only provide better security but they reduce the effect of broadcast storms.

(b) Describe the main differences between USB and FireWire.

(c) Describe the four switching modes of an Ethernet switch and indicate under which conditions each is best used.

(d) Explain the advantages of implementing VLANs rather than using a single large multi-switch LAN.

(e) Describe how the CSMA/CA protocol works so that a frame can be transmitted without a collision.

Learning outcomes

At the end of this chapter, you should be able to:

- identify the approximate ranges over which PANs, SANs, LANs, MANs and WANs operate
- outline how the USB and FireWire protocols operate

- outline how the IrDA and Bluetooth protocol works
- outline how the Fibre Channel protocol works
- distinguish between and describe the various main types of Ethernet from their designations
- describe how Ethernet has evolved to higher speeds and to wider areas
- describe why VLANs are required and how they work
- outline how the Token Ring and FDDI protocols work
- describe the drivers for and main features of Wireless LANs and the CSMA/CA access method.

Chapter 4: Network technologies – MANs and WANs

Further reading

Carr and Snyder *Management of Telecommunications.* (McGraw Hill), second edition, 2003. Chapter 14.

Fitzgerald and Dennis *Business Data Communications and Networking* (John Wiley & Sons), eigth edition, 2005. Chapters 9, 10.

Forouzan, Behrouz A. *Data Communications and Networking.* (McGraw Hill), third edition, 2003. Chapters 9.2, 9.3, 17.1, 17.2, 18.

Stallings, William *Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003. Chapters 8.2, 10, 11.

Tanenbaum, Andrew S. *Computer Networks.* (Prentice Hall International), fourth edition, 2002. Chapters 1.5.2, 2.4 – 2.7.

In this chapter, we will examine the various technologies that can be deployed by enterprises for metropolitan and wide area networks. MANs and WANs are different from LANs, in that enterprises cannot, in general, own the communications infrastructure. This is because, the provision of underground cables and the use of radio frequencies are heavily regulated and usually require licences that can only be obtained by network operators. In order to provide MANs and WANs, an enterprise therefore is forced to buy telecommunications services from network operators which are expensive and usually proportional to both data rate and distance. There are many such services on offer employing different technologies and with very different features, management options and prices. Designers of enterprise networks must be aware of the different services and technologies available and be able to choose the ones that best meet the enterprise's requirements. We will not discuss Internet and ATM technologies in this chapter. These will be considered in the next two chapters on Network Integration, as they are both examples of technologies that are being used to integrate different communication services.

4.1 Metropolitan Area Networks (MANs)

MANs are networks whose sizes lie somewhere between that of a LAN and that of a WAN. They usually cover distances of between about 1 and 80 km, and are often implemented across a city or a part of a city or a large campus. There are a few technologies that were designed for use by MANs, such as SMDS[1] and Cable TV technologies, but they are often implemented using technologies used in LANs, such as Ethernet or WANs, such as Synchronous Digital Hierarchy (SDH[2]). They can also be built using dark fibre, which is optical fibre that is leased from a network operator without any LASER transmission or detection devices. These devices can then be purchased and connected up to 'light' the fibre and can operate at any desired data rate using any desired protocol. The advantage of this approach is that the charges for leasing the fibre are not dependent on the data rate used. MANs can also be implemented using network operator's Asynchronous Transfer Mode services.

4.1.1 Switched Multi-megabit Data Service (SMDS)

SMDS is strictly speaking a service rather than a technology. The service, which is connectionless, was specifically designed for MANs that carry data and was standardised by the IEEE although SMDS can also be deployed in

[1] *Switched Multi-megabit Data Service.*

[2] *Synchronous Digital Hierarchy, see Section 4.2.1.2 in this chapter.*

WANs. It was specified by Bell Communications Research (Bellcore)[3] and supported by ANSI[4] in the USA. It is offered by many network operators as a high-speed data service specifically designed for LAN interconnection and is usually offered as a WAN service as well as a MAN service. SMDS defines a subscriber to network interface, known as the SMDS Interface Protocol (SIP) which is a three layer protocol. SIP Level 3 is a network layer protocol that can carry datagrams of up to 9,188 bytes and SIP Level 2 is based on the IEEE 802.6 Distributed Queue Dual Bus (DQDB) MAN standard and is a data link layer protocol that segments the Level 3 frames into 53 byte cells (the same size as ATM cells which makes it easy to carry SMDS over an ATM network). DQDB uses two unidirectional buses, carrying data in opposite directions and each device is connected to both buses and can therefore view all data passing in both directions. Frames are generated by a frame generator located at the end of both buses. Often these buses are configured in a loop, but one station then has to be the head of both buses. DQDB is able to manage a distributed queue fairly, because devices are able to indicate that they require a place in the queue by sending a request in the opposite direction to which they wish to send data. All of the upstream devices are able to see the requests and hence they know which other devices are ahead of them in the queue to transmit.

SMDS can use a number different data link protocols as well as DQDB. SIP Level 2 can be replaced by the Data eXchange Interface (DXI) based on HDLC, Frame Relay or ATM.

Because SMDS can carry datagrams of variable length up to 9188 bytes, it can encapsulate frames from virtually all LANs. Data rates usually supported range from 200 kbit/s to 45 Mbit/s, eventually possibly rising to 155 Mbit/s.

For addressing, SMDS uses the ITU-T's E.164[5] telephone numbering scheme and uses these addresses to validate authorised users and to ensure that data from one customer on the public network cannot be received by any other customer.

SMDS charging involves connection charges for access circuits that are speed related plus monthly rental charges that are speed related. Both these charges are usually distance independent. Some network operators also have usage based charging where users also have to pay for a charge based on the amount of data they have transferred.

One of the main advantages of SMDS is that, like LANs, it supports both connectionless networking and multicasting. Most WAN technologies even when they support connectionless networking, do not support multicasting. This means that SMDS is an ideal solution for LAN interconnection at speeds from 1 to about 45 Mbit/s. SMDS is also very compatible with ATM and network operators can carry SMDS traffic over their ATM networks. Its main disadvantage is that it does not support delay sensitive traffic such as voice and video, although DQDB itself can support such traffic.

Activity 4.1

Study how the DQDB works from a textbook or web site. Satisfy yourself that the protocol can implement a fair queuing system without any centralised control.

4.1.2 Cable TV Networks

Cable TV companies have laid networks across metropolitan areas primarily to carry analogue or digital TV signals from the cable TV head-end to individual homes. These networks have therefore been designed as cascaded star networks with the head-end as the central hub, transmitting simplex broadcast TV channels using FDM and/or TDM.

[3] *Now known as Telcordia*

[4] *American National Standards Institute*

[5] *See Section 4.2.3 of this volume.*

Cable TV networks can usually support about 400,000 subscribers from a Regional Cable Head (RCH). Originally Cable TV networks used copper coaxial cables from the RCH via a series of splitters and amplifiers to the homes, but modern networks have been re-engineered to use optical fibre cables, but the cost of running these to each home is prohibitive, and the optical network is converted back to copper at Fibre Nodes in street cabinets. The RCH feeds a number of Distribution Hubs which can support about 40,000 subscribers via switches and Fibre Nodes. The Fibre Node will split the TV signals and transmit them over the coaxial cables which will provide service to about 1,000 homes using a tree topology.

These systems are known as Hybrid Fibre-Coaxial networks. They can be adapted to provide a backwards channel to support interactive services, and most cable TV companies have adapted their networks in this way so that they can support broadband services using cable modems and the DOCSIS[6] standard. The coaxial cables, as well as carrying TV signals, will also carry a downstream and an upstream data channel.

Cable TV companies also support voice services, but these are usually supported by a separate UTP cable, which is carried within the outer sheath of coaxial cable, and then carried over separate channels to the RCH where these voice channels are connected to a PSTN switch.

In order to support DOCSIS, the cable TV company must install a Cable Modem Termination System (CMTS) at the head end, which is connected to the Internet. The CMTS will route traffic to and from the Internet and, if necessary, between cable modems supported by the CMTS. The CMTS provides similar functions to those provided by the DSLAM[7] on DSL broadband systems.

Cable TV companies offer similar products to enterprises as do other fixed network operators. These are mainly WAN services such as private circuits, LAN extension, ATM, frame relay and IP VPNs[8]. The cable TV network is used to provide access to these WAN services access charges for use of the cable TV network are subsumed within the prices charged for the WAN services.

Activity 4.2

Visit the web sites of some of the network operators who offer telecommunications services in your country and check what products they offer to support high speed LAN interconnection over metropolitan areas. Check whether they are priced by distance and/or by data rate.

4.2 Wide Area Networks (WANs)

Wide Area Networks are typically used where communications are required between sites which are separated by at least one public road (although this is also true for many MANs). WANs can usually only be provided by licensed network operators (or other utilities such as gas, water and electricity companies) who are allowed to dig up roads to lay cables or pipes. As a result very few organisations can run their own telecommunication cables between sites that are separated by roads. There are a few exceptions, notably the gas, water and electricity companies mentioned above, who can run and often do run fibre optic cables within their pipes or ducts. Another notable exception and railway and waterway companies and who own long strips of land between major cities. Many railway companies lay fibre optic cables at the trackside for communication between stations and to control railway signals.

[6] *Data Over Cable Service Interface Specification, see Volume 1, Section 8.6.*

[7] *Digital Subscriber Line Access Multiplexer, see Volume 1, Section 8.5.*

[8] *Virtual Private Networks, see Section 5.6.3 in this volume.*

Most new entrant operators have laid their cables alongside railway tracks, canals, within underground pipes or ducts used by other utilities or alongside the overhead power cables of the electricity grid.

Other companies have to rely on buying telecommunications services from licensed network operators for wide area communications. It is this more than anything else that distinguished WANs (and many MANs) from LANs. Buying communications from network operators is expensive and the charging is often based on the data rate used. With LANs customers can upgrade the data rate and only have to worry about the one-off cost of new hardware. With WANs, upgrades in speed will produce recurring increases in costs. Charges are also often related to distance and this also has a big effect on costs, particularly for international communications. Other ways in which WANs differ from LANs, and to a lesser extent MANs, are that because of the distances involved and propagation and other distance related delays, RTTs[9] become significant. WAN cables have to survive in a much less friendly environment than LAN cables. They are prone to weather problems, particularly copper local loop cables, but also any cables that are carried overhead or underground. Underground copper cables and any electronic equipment is vulnerable to flooding and underground or submarine cables are vulnerable to accidental excavation or trawling. Overhead cables (or the poles that support them) are vulnerable to the wind and they can fall over in violent storms. As a result of all this, failures on WANs are much more common than on LANs, and often take longer to fix. Furthermore WAN circuits are much more prone to errors than LANs, due to the longer cable lengths and the effects of noise and electrical interference on copper cables and electronic equipment. Finally, LANs because of their topologies and access protocol, can easily support broadcasting and multicasting. This is much harder to do with WANs as they tend to use point-to-point communications between nodes in a mesh network which is not well suited to handling broadcasts and multicasts.

4.2.1 Private circuit networks

Many enterprises implement their own private circuit networks to carry both voice and data traffic and sometimes also video-conferencing. Historically, it was often cheaper for enterprises to build their own private networks, rather than use public networks. This was particularly true for voice communications where network operators charge each telephone call on a per minute basis. The economics of private circuits are often compelling. A 2 Mbit/s private circuit between two offices can carry 30 simultaneous telephone calls and even if the circuit is not used to anything like its full capacity, it will often be cheaper to lease a private circuit than to pay for individual telephone calls over the public network. Enterprises would therefore often link the PABXs[10] in their main offices using a partial mesh network of private circuits. Very large enterprises would use higher capacity circuits at 34 or 45 Mbit/s or higher and would use TDM[11] equipment to multiplex their 2 Mbit/s voice channels, thus forming a private TDM network. With such networks in place, it made sense, as requirements for data communications began to materialise, to also carry data over these TDM networks. This was usually done by configuring data channels, at the appropriate speeds across the TDM network. Using TDM networks in this way was an early example of network integration, if only at the physical layer.

Private circuits are carried by time division multiplexing over the network operators' transmission networks. They are always-on and provide a dedicated data rate between two points known as the A end and the B end[12].

[9] Round Trip Times.

[10] Private Automatic Branch Exchange – a privately owned and managed telephone switch.

[11] Time Division Multiplexer, see Volume 1, Section 2.3.2

[12] When ordering a private circuit, the customer specifies which end is the 'A' end and which is the 'B' end. The 'A' end is usually the main office or a computer centre.

The private circuit follows a route through the TDM network known as a path. The path is made up of a number of lines in series. Lines are physical circuits between multiplexers. The line then is split into a number of sections in series between repeaters.

Private circuits normally incur a one-off connection charge related to the speed, and a monthly rental charge related to both the speed and the distance between the A and B ends. International private circuits are priced as two half-circuits with separate pricing schemes for each end, often priced in different currencies. The price of international circuits, just depend on the two countries concerned. They do not usually depend on the locations within each country.

4.2.1.1 The Plesiochronous Digital Hierarchy (PDH)

Network operators support private circuits on their own large TDM networks, called transmission networks. These networks support the circuits that the operator uses to carry its PSTN traffic and data networks as well as private circuits. These TDM networks are hierarchical with low speed circuits carried by higher speed circuits. Earlier transmission networks were based upon the Plesiochronous[13] Digital Hierarchy (PDH). There are actually several different hierarchies used in different parts of the world. In North America the hierarchy is based upon the 1.5 Mbit/s T1 carrier circuit (Table 4.1), while in Europe and most other parts of the world[14], the hierarchy is based upon the 2 Mbit/s E1 carrier circuit (Table 4.2). At each layer of the hierarchy, bits from each of the input channels (called tributaries) are interleaved with bits from other input channels onto the higher speed output channel.

Table 4.1: The North American Digital Hierarchy

Name	Multiplexed from	Approximate data rate
T1	24 x 64 kbit/s channels	1.5 Mbit/s
T2	4 x T1s	6 Mbit/s
T3	7 x T2s	45 Mbit/s
T4	6 x T3s	274 Mbit/s
T5	120 x T1s	400 Mbit/s

Table 4.2: The European Digital Hierarchy

Name	Multiplexcd from	Approximate data rate
E1	32 x 64 kbit/s channels	2 Mbit/s
E2	4 x E1s	8 Mbit/s
E3	4 x E2s	34 Mbit/s
E4	4 x E3s	140 Mbit/s
E5	4 x E4s	565 Mbit/s

Network operators can also provide private circuits at lower speeds. The data rates of theses circuits are these days usually 64 kbit/s or multiples of 64 kbit/s and are known as Nx64 or sometimes fractional services. Some network operators still provide circuits at lower speeds than 64 kbit/s, but these are rarely used today. The network operator will provide and install a Network Terminating Unit (NTU)[15] that supports physical interfaces such as X.21 or V.35 at the customers premises ‘A’ end. The NTU will be connected over a 4-wire circuit to the network operator’s Primary Multiplexer (PMUX)

[13] Plesiochronous means nearly synchronous. Both ends of a circuit operate separate, but quite accurate clocks, which occasionally lose synchronisation. Extra bits are sometimes inserted into input channels when clocks begin to drift and these bits are extracted when the channels are demultiplexed, but there are also occasional frame slips when a whole frame is lost.

[14] There is yet another hierarchy used in Japan which is prefixed by the letter J and has the same data rates as T1, T2 and E5 but J3 operates at 32 Mbit/s and J4 at 98 Mbit/s.

[15] In North America, the network operator does not provide an NTU. Instead, the customer provides a Channel Service Unit / Data Service Unit (CSIIDSU), sometimes it is incorporated into customer premises equipment such as routers and multiplexers.

at the local exchange. The PMUX multiplexes the circuit with others onto a E1 or T1 circuit and these are then further multiplexed over a number of high-speed optical fibre systems to another PMUX, where it is demultiplexed back to 64 kbit/s for delivery to the NTU at the 'B' end. For Nx64 kbit/s private circuits, the network operator installs an NTU and a PMUX on the customer's premises and provides an E1 or T1 circuit over a 4-wire copper cable to multiplexers on its own premises and then configures an appropriate number of 64 kbit/s channels which are then routed over its transmission network. For E1-4 circuits, the network operator will normally just install an NTU on the customer's premises which will then be connected to customer premises equipment, such as multiplexers, routers and PABXs.

There were several disadvantages with PDH. Not least being the different standards used in different parts of the world which makes international inter-working difficult. Reliability problems also occur because of the way low speed circuits are routed through many multiplexers up to high speed carriers and often are de-multiplexed and re-multiplexed at intermediate points along the route. Cables have to be connected between multiplexers and the many connectors involved increase the potential for errors. It is difficult to monitor the performance of PDH systems, which are also prone to frame slips that result in lost data. It is also difficult to connect a new private circuit through the TDM network or change its data rate and it is impossible to add a insert a new low speed channel on a high speed channel without de-multiplexing to the speed of the new channel.

4.2.1.2 The Synchronous Digital Hierarchy (SDH)

The solution to all of these problems as well as the need to support even higher speeds which can now be achieved on optical fibres, was to change from plesiochronous working to truly synchronous working. The resulting transmission network is called the Synchronous Digital Hierarchy (SDH) standardised by the ITU-T. SDH is based on a 155 Mbit/s carrier which can accommodate an E4 circuit. In North America, the standard used is slightly different, and it is called Synchronous Optical NETwork (SONET) defined by ANSI. SONET supports the same carrier speeds as SDH, and a few more. SONET is based on a 51.84 Mbit/s[16] carrier that can accommodate a T3 circuit.

SDH uses the abbreviation STM[17] for its naming convention and SONET uses OC[18] and STS[19] for its naming conventions. The basic E1-4 and T1-4 private circuits are still supported, but instead of having several stages of multiplexing, they can be multiplexed immediately up to 52 (SONET) or 155 (SDH) Mbit/s using an Add-Drop Multiplexer (ADM), where for example a new 2 Mbit/s channels can be added to a 155 Mbit/s SDH circuit or dropped out of the circuit without disrupting any other channels being carried over the circuit. 52 Mbit/s and 155 Mbit/s are the basic data rates at which SONET and SDH respectively operate. The speeds and frame structures were chosen carefully so that all the existing E1-E4, T1-T4 and J1-J4 private circuits could be carried over the 155 Mbit/s bearer. Above 155 Mbit/s SDH and SONET standards have defined further hierarchies, some of which are standard throughout the world and others specifically accommodate particular circuit speeds in one of the regions, although many of data rates defined in the standards have never been implemented. The common data rates supported by SDH and SONET and their respective names are listed in Table 4.3 below.

[16] *OC-1/STS-1*

[17] *Synchronous Transport Mode*

[18] *Optical Carrier.*

[19] *Synchronous Transport Signal*

SDH protocols have four sub-layers:

- The **photonic** sub-layer defines the physical properties of the fibre and the signals.
- The **section** sub-layer defines how SDH operates between repeaters.
- The **line** sub-layer defines how SDH operates between multiplexers.
- The **path** sub-layer defines how SDH operates on an end-to-end channel at a specific data rate.

Table 4.3: The main data rates that SDH and SONET have in common

SDH Name	SONET Name	Approximate data rate
STM-1	OC-3/STS-3	155 Mbit/s
STM-4	OC-12/STS-12	622 Mbit/s
STM-8	OC-24/STS-24	1.2 Gbit/s
STM-16	OC-48/STS-48	2.5 Gbit/s
STM-64	OC-192/STS-192	10 Gbit/s
STM-256	OC-768/STS-768	40 Gbit/s
STM-1024	OC-3072/STS-3072	160 Gbit/s

All network operators are migrating their PDH networks to SDH/SONET and these are used to carry the PSTN, data networks and private circuits. But with SDH, operators can also offer very higher speed private circuits at some of the rates in Table 4.3. You are not expected to learn this table, apart from the fact that the basic data rate for SDH is 155 Mbit/s. Network operators usually configure their SDH/SONET networks in rings called Shared Protection Rings (SPRings), for resilience.

Activity 4.3

From a textbook or web site, examine the frame structures used by PDH and SDH.

Activity 4.4

Visit the web sites of some of the network operators who offer telecommunications services in your country and check what products they offer for private circuits and at what data rates. Check whether they are priced by distance and/or by data rate.

4.2.2 Satellite networks

Satellites have been used for communications from the early days of space travel in the 1960s. Satellites can provide high bandwidth between distant points on the earth's surface by receiving signals from a transmitter and relaying them to a receiver using microwave radio. The transmitters and receivers can be large or small dishes or even portable satellite telephones. The equipment on the satellite that relays the signal is known as a transponder.[20] The transponder merely relays the signal it receives at a different frequency. It is unable to amplify it significantly, as this would be a drain on the satellite's power. Each satellite is able to transmit and receive signals from an area of the earth's surface known as the satellite's footprint. The size of the footprint will depend on the height of the satellite's orbit and to what degree the satellite focuses the beam of its signal. The footprint can be as large as a third of the earth's surface or as small as a few hundred kilometres. The period of a satellite's orbit is related to the height of the orbit (the higher the orbit, the longer the period). There is a special orbit where the orbital period is the same as the earth's rotational period. In this orbit

[20] *Transmitter/Responder*

(about 35,785 km above the earth), known as geo-stationary orbit or Geosynchronous Earth Orbit (GEO), the satellite will always be in the same position above the earth's surface. This is the most popular orbit for communications satellites (as they appear stationary to receivers who therefore do not have to track them) and it is now very crowded. It is essential to maintain a minimum distance between satellites in this orbit so that they do not interfere with each other. The positions in GEO are controlled by the ITU-R[21] and virtually all positions are now occupied. Satellites tend to drift from their assigned positions over time and they need to use small rocket motors to adjust their positions from time to time.

It is possible to use orbits below GEO, but in these orbits footprints are smaller and satellites have to be tracked as they move across the sky. Medium Earth Orbit (MEO) is between 8,000 and 20,000km above the earth with an orbital period of between two and 12 hours. It is currently not used for communications, but is used for the navigation with the Global Positioning System (GPS).

GPS uses 24 satellites in six MEOs so that there are always four satellites visible at any time from any point on the earth's surface. Each GPS satellite broadcasts a timing signal and the receivers are able to measure the delays from the four GPS satellites and calculate their position on the earth's surface using triangulation.

Low Earth Orbit (LEO) is between 500 and 2,000 km above the earth with an orbital period of a few hours. They are useful for communications, because the satellites are nearer to the earth, so less power is required in the terminals and propagation delays are much less. There is also plenty of room in LEO for launching new satellites. The only disadvantage is that satellites will move out of range as they cross the sky.

Satellite communications is generally quite expensive, mainly due to launch costs (including insuring against the risks of failure), the costs of providing reliability and resilience within the satellite, as maintenance visits are impractical, and the costs of the terminals which often do not have a mass market. Added to these costs is the inconvenience of long propagation delays. As a result satellite communications cannot compete with land-based communications and have therefore now become associated with niche applications. The high costs also results in companies forming consortia to share the costs and risks of satellite launches. The Eutelsat, Intelsat and Inmarsat satellites were launched by inter-governmental organisations but are now owned by consortia of mainly incumbent fixed network operators and institutional investors.

4.2.2.1 Communications satellites

Communications satellites are normally placed in GEO and use frequency division multiplexing to support a number of transponders and within each of the transponders' uplink and downlink channels they use TDMA[22] techniques to support a number of simultaneous users.

Satellites were originally mainly used to carry private circuits, PSTN and TV links between continents. Network operators have built a network of large satellite dishes which are called earth stations that link to their land-based networks. Satellite communications suffer a major disadvantage for voice communications and interactive services in that the propagation delays to GEO and back are quite significant, of the order of 250-300 ms. This is noticeably disruptive for real-time communications and because of this most international telephone traffic now uses fibre optic submarine and

[21] International Telecommunications Union – Radiocommunications Sector.

[22] Time Division Multiple Access, see Volume 1, Section 7.3.8.

underground cables. Communication satellites are still useful in parts of the world which are not so well served by cables and for particular applications, particularly those which require broadcasting.

Satellites are still used for telephony to countries that are not well served by fibre optic cable. Satellite circuits are often booked by broadcasters who want to transfer news footage or other programming material for broadcasting later. It is unlikely that live television involving any interaction will be carried over a satellite circuit, due to the delay.

Satellite communications are also used to support aeronautical and maritime communications. Inmarsat is an example of a network of satellites which cover the whole of the surface of the earth with four satellites in GEO.

4.2.2.2 Direct Broadcasting by Satellite (DBS)

Another application for GEO satellites is Direct Broadcasting by Satellite (DBS) where hundreds of TV channels can be beamed up to the satellite from an earth station and down across a wide footprint to consumers' satellite TV dishes which are mounted on the sides of houses.

4.2.2.3 Very Small Aperture Terminal (VSAT) networks

Very Small Aperture Terminals (VSATs) are satellite dishes that are about one metre in diameter that form a network together with a hub within the footprint of a satellite in GEO. The hub usually has a larger dish and controls the VSAT network. The hub site can broadcast information to the VSATs and VSATs can communicate with each other, but only via the hub, which switches the traffic between the VSATs. It is difficult to switch traffic in the satellite, so traffic between VSAT terminals is switched on the ground and hence requires a double hop which doubles the propagation time. VSATs are ideal for applications where large volumes of data are broadcast from the hub site to many VSAT sites or where many VSAT sites have to send information back to the hub site, but are less useful for applications where information has to be sent between two VSAT sites. VSAT networks can also be used to provide relatively cheap telecommunications to remote areas where there is no land-based network.

4.2.2.4 Satellite mobile communications

Satellites in LEO can be used to support mobile communications. These systems use a number of different satellites in polar orbits, which can cover the whole surface of the earth. It is possible for the handsets to hand over from one satellite to another as each satellite passes overhead, rather like mobile phones hand over to different base-stations as users move about. Each satellite acts as a switch and can switch calls to another satellite or down to a terminal. A number of LEO satellite systems, such as Iridium and Globalstar have been launched to provide personal communications to handset users that can be absolutely anywhere, but none have been particularly successful. This is mainly due to the success of land-based mobile telephony which is much cheaper, but there is a niche market for it in remote parts of the world.

4.2.3 Public Switched Telephone Network (PSTN)

The PSTN was designed to carry voice communications. It was originally an analogue network which used Frequency Division Multiplexing to carry multiple telephone calls between analogue mechanical telephone switches. In order to use bandwidth efficiently, it limits the bandwidth available to each telephone call to 3.1 kHz. However, all transmission and switching on the PSTN is now digital, apart from transmission between the customer's premises and the local exchange.[23]

The PSTN is a circuit switched network. The setting up of calls is under the control of customers who signal they wish to make a call by lifting their telephone handset which closes the local loop and enables the phone to be powered via a 50 Volt direct current from the local exchange. The closure of the loop is detected by the local exchange which then allocates equipment to connect a call and confirms this by returning an audible 'dial tone' to the telephone. The caller then signals the telephone number they wish to call to the local exchange using Dual-Tone Multiple Frequency (DMTF) or loop disconnect signalling (for very old rotary dial phones). The success or otherwise of their call attempt is signalled by the transmission of various audible tones. The local exchange then uses a complex set of digital signalling protocols known as **Signalling System Number 7** (**SS7**) to attempt to connect the call. SS7 is sometimes called common channel signalling, because the signalling related to each call is carried out on a separate common channel rather than the channels being used by the calls.

SS7 is defined by the ITU-T in a set of standards commencing with 'Q.7'. It is a complex set of standards that define a connection-oriented signalling system and uses network layer similar to X.25 packet switching.[24] Telephone numbers are allocated according to the ITU-T's telephone numbering plan.[25] They can be up to 15 digits long and are hierarchically structured into a country code (one two or three digits), a national destination code that defines the area within the country and a subscriber number that identifies an individual phone line. Sometimes the subscriber number is further subdivided into a local exchange code and a local number. The different hierarchical levels of the number codes are used to route calls across the PSTN. At each switching stage the appropriate code is looked up in tables within switches to determine the next switch to be involved in setting up the call.

At the destination switch the subscriber's number is looked up to determine which local loop it relates to and the status of the loop is determined. If the loop is closed then the phone is off-hook and the line is engaged and this is signalled back to the caller's exchange via SS7 and an 'engaged tone' is returned to the caller. If the loop is open, then the phone is on-hook and therefore free, so an alternating ringing current is sent down one of the wires to ring the telephone bell. SS7 confirms that the phone is free and requests that a 4-wire circuit is set up from the caller's exchange to the destination exchange to connect the caller's 2-wire local loop to the destination 2-wire local loop. A 4-wire circuit is required so that signals can be repeated at various places along the route. This can only done if signals travelling in different directions uses separate circuit pairs. A ringing tone is then transmitted back along this circuit from the destination exchange to indicate that the destination phone is ringing. If the destination handset is lifted, the loop closure is detected, the ringing current and ringing tone are stopped and speech can be carried between the two phones.

[23] *The two wire circuit between the customer's premises and the local exchange is often called the local loop as a loop is formed when the telephone handset is lifted.*

[24] *See Section 4.2.7 in this volume.*

[25] *ITU-T Recommendation E.164.*

At the local exchange, once a call has been answered, the voice signals are coded using Pulse Code Modulation[26] into a 64 kbit/s data stream. This 64 kbit/s channel is then switched digitally onto a channel within a T1[27] or E1[28] bearer circuit to another exchange, where de-multiplexing back to 64 kbit/s and further switching can take place. This process continues, potentially many times, until the destination exhange is reached. At this point, the 64 kbit/s channel is decoded and converted to a Pulse Amplitude Modulation (PAM) signal that approximates the original voice signal which was encoded and it is this signal that is transmitted to the receiving telephone.

The call is terminated when the caller replacing his handset and disconnects (or opens) the loop. The local exchange detects this and issues the SS7 command to notify all the exchanges involved that the call is to be terminated. This instruction is carried out by each exchange on the route and SS7 confirms that the circuit has been disconnected.

Network operators bill their customers a rental charge for the their phone line and per minute usage charges (usually related to distance and time of day) for the calls that they have made. Operators also often create packages whereby the customer pays a higher monthly rental and is offered free calls. The full cost of calls is normally billed to the calling party. Many network operators now offer packages with higher rentals and a limited or unlimited number of free calls. The free calls can be of different types, local or national. There are often several different options of rental charges with different quantities of free calls included. All this makes price comparisons between different operators very difficult.

The PSTN consists of a larger number of separately managed networks which are interconnected into a global system using SS7. Network operators forge bilateral agreements with other operators to handle international traffic, while interconnection agreements are required between network operators within each country. These agreements will contain accounting arrangements between the operators. The network on which the calls originate and which bills the calls has to make per minute payments to the networks to which the calls are forwarded. Networks are connected together using high-speed interconnect circuits.

It should be noted that the PSTN has been dimensioned to carry only a fixed amount of traffic. It is assumed that only a small proportion of customers will wish to make calls at the same time. If every subscriber lifts their handset at the same time, then only a small proportion of them will receive dial tone. Network operators will treat certain phone lines, such as those used by doctors and the emergency services, with priority in such circumstances. There are occasions when parts of the PSTN become overloaded. This happens when disasters occur but can also happen when a phone number is advertised for competitions or special offers. In order to avoid the collapse of the whole network, in such circumstances, network operators have built traffic management systems. These systems monitor traffic patterns and allow controls to be issued at local exchanges, so that only a small proportion of call requests to overloaded numbers are allowed through the local exchange. The majority of calls to the overloaded numbers fail at the local exchange and will receive engaged tone from this point instead of congesting the whole network. Because the PSTN is connection oriented, it is much easier to take steps to maintain a consistent quality of service, and today, this is generally achieved in most developed countries. The proper functioning of the PSTN is vital to the economy and to society.

[26] *See Section 8.3.6.2 of Volume 1.*

[27] *1.5 Mbit/s digital circuit used in North America.*

[28] *2 Mbit/s digital circuit used in Europe and elsewhere.*

The PSTN is used primarily for voice communications, but it can support low speed data and facsimile by means of modems, but the bandwidth limitations o the PSTN severely reduce the rate at which data can be transmitted to 56 kbit/s or less.

Activity 4.5

Determine the structure of the E.164 Telephone Numbering Scheme operated within your country. Do all numbers have a fixed length and are they all structured in the same way? What digits are used as a prefix for dialling long distance and international numbers? What dialling codes are used for local call fee access, national call rate access, premium rate calls and what dialling codes are used to identify mobile phones?

4.2.4 Integrated Services Digital Network (ISDN)

The main weakness in the PSTN is the local loop in the access network. Because it uses analogue transmission and signalling, it is subject to noise. The noise is also worse in the local loop than in other parts of the PSTN, as they are usually copper wires rather than optical fibre which predominates in other parts of the network. They are therefore prone to electromagnetic interference from many sources, including cross-talk from other circuits. Sometimes the loops have poor insulation that can be affected by water. The majority of faults within the PSTN occur in the local loop. In order to improve service on this part of the network, it is necessary to use digital transmission and signalling. Network operators achieved huge increases in reliability and performance by using digital transmission and switching within their distribution and core networks. Integrated Services Digital Network (ISDN) was an early attempt to do this for the access network and to integrate voice, data and to a lesser extent video onto a single network platform.

ISDN is a digital access technology deployed over local loops. Once ISDN calls enter the local exchanges they are carried through the PSTN using SS7 signalling and PCM coding just like analogue phone calls. The service provided by ISDN is very similar to that provided by the PSTN, except that it performs better due to digital transmission being extended to the customer premises. The numbering scheme used for ISDN is E.164 and ISDN numbers are normally indistinguishable from PSTN numbers.

ISDN is charged in the same way as PSTN, but with higher connection charges and monthly rental charges reflecting the fact that ISDN can provide two speech channels and requires more expensive line cards at the local exchange. Calls are charged in exactly the same way as on the PSTN (by duration, distance and time of day).

4.2.4.1 Basic Rate Interface (BRI)

The ISDN Basic Rate Interface (BRI) provides two 64 kbit/s bearer channels (B channels), which can be used for two simultaneous calls to different numbers, and one 16 kbit/s data channel (the D Channel). The D channel is designed to carry digital out-of-band signalling information such as that required to set up and clear down calls, but it can also be used to carry low speed packet switched data. Basic Rate ISDN is often referred to as 2B+D. In addition to the 144 kbit/s required to support the B and D channels, The BRI uses 13 kbit/s for synchronisation and another 3 kbit/s for network management, giving a total data rate of 160 kbit/s. B channels can, if required, be bonded to form a single higher speed data channels. This is an example of inverse multiplexing. With BRI a computer can make use of both B channels and can operate at 128 kbit/s.

At the physical layer, ISDN uses a 2B/1Q[29] line code in N. America and 4B/3T[30] line code in Europe. It also uses echo cancellation techniques to improve transmission quality and Time Division Multiplexing (TDM) to derive the B and D channels. The D channel uses a version of HDLC similar to LAPB[31] called LAPD[32] at the data link layer and a signalling protocol specified in Q.931 at the network layer. BRI cannot be supported over local loops more than about 5 km from a local switch. It uses baseband transmission, so unlike ADSL[33], it cannot co-exist with analogue voice.

BRI requires special terminal equipment that supports the ISDN protocols. ISDN support can be integrated into the terminal equipment or into a separate piece of equipment known as a Terminal Adaptor (TA), sometimes also called an ISDN modem.

The ISDN BRI standards define a number of different interfaces at which equipment can be attached. For BRI, ISDN can be extended around a customer's premises on a 4-wire bus (known as the S/T bus) operating at 192 kbit/s which can support up to eight devices.

ISDN is mainly used for voice communications. BRI usage is not very common. BRI has not been anything like as successful in the marketplace as might have been expected. There are many reasons for this. It was expensive compared to using analogue lines with modems for data, which were soon able to offer speeds that were not significantly less than those offered on a single ISDN B channel. Few applications were developed that made full use of ISDN's capabilities. Home based video conferencing was expected to do this, but never really took off. ISDN was a technology led development rather than a market led one. The network operators in most countries did not really sell ISDN very hard, as the cost of upgrading line cards in exchanges was high and the extra revenue potential was limited. Finally, new access technologies such as ADSL were being developed that could offer much higher data rates with which ISDN could not hope to compete. BRI can be used to provide higher speed data access or a second line for home users, but its use is being displaced by ADSL in those areas where it can be supported mainly due to its higher capacity and the absence of per minute call charges. ISDN can also be used for remote access to corporate networks by home workers, but again this usage is being displaced by ADSL. BRI is used by enterprises for communications that only require occasional connections and for dial back-up for 64 kbit/s 128 kbit/s private circuits and data network access circuits. Routers can be purchased with cards that support BRI and which will automatically dial a configured phone number when a connected private circuit fails. But because ISDN calls are charged per minute, it can be expensive if the circuit is down for a long period. ISDN is also sometimes used for relatively infrequent transactions, such as credit card validations, as setting up calls is much quicker using ISDN than using the PSTN.

4.2.4.2 Primary Rate Interface (PRI)

The ISDN Primary Rate Interface (PRI) is intended for use by enterprises. It supports 23 (N. America) or 30 (other parts of the world) 64 kbit/s B channels and one 64 kbit/s D channel for common channel signalling. These services are known as 23B+D and 30B+D respectively. The 30B+D system uses one other 64 kbit/s channel for synchronisation making a total data rate of 2.048 Mbit/s while the 23B+D system uses an extra eight bits per frame for synchronisation and network management, making a total data rate of 1.544 Mbit/s. PRI uses the same frame structure and line code as the private circuits that operate at these speeds. 30B+D uses E1 frames and HDB3 line code, while 23B+D uses T1 frames and B8ZS[34] line code.

[29] *2 Binary / 1 Quaternary, see Volume 1, Section 8.3.6.4.*

[30] *4 Binary / 3 Ternary, see Volume 1, Section 8.3.6.4.*

[31] *Link Access Protocol Balanced, see Volume 1, Section 7.5.*

[32] *Link Access Protocol Digital.*

[33] *Asymmetric Digital Subscriber Line, see Volume 1, Section 8.5.*

[34] *Bipolar 8 Zero Substitution, see Volume1, Section 8.3.6.4.*

PRI has been more successful in the marketplace than BRI. This is because it served a real need. Companies with multiple telephone lines, could replace them with a much smaller number of ISDN lines, save money and achieve much better quality of service through the use of digital transmission. Most PABXs were now digital and providing PRI access meant that enterprises' voice communications could be entirely digital which improved quality. PRI was economic even for a relatively small number of phone lines and once it was installed the ISDN line could be reconfigured to support more lines up to a maximum of 23 or 30.

Enterprises could also bond several ISDN B channels together to support high-speed video conferencing, which became popular and resulted in savings of both travel cost and time.

PRI is also used by ISPs to provide a higher quality of service to their dial-up customers. It is this use of ISDN to provide a digital connection from the ISP right through to their customers' local exchanges that allows 56 kbit/s modems to work.

Finally, PRI could be used to backup data circuits between 192 kbit/s and 1,920 kbit/s, although call charges could be very expensive if circuits were out for long periods of time. Some network operators would offer ISDN backup as an enhancement to their private circuit products with a premium price but where availability could be guaranteed and customers would not pay the ISDN call charges.

4.2.4.3 Broadband ISDN

The ITU-T saw ISDN as an interim technology for integrating services over a digital access network and onto the PSTN platform. It envisaged that a higher-speed digital technology would eventually replace it. It coined the term Narrowband ISDN to describe BRI and PRI versions of ISDN and Broadband ISDN to describe the much higher speed digital integrated networks that were being developed. Broadband ISDN was eventually realised in ATM technology.[35]

Activity 4.6

Visit the web sites of one of the network operators who offer telecommunications services in your country and check the prices (connection, rental and usage) for BRI. Compare these with the price for a 100km 128 kbit/s private circuit (including connection charges) over a one-year period. Calculate how many minutes per day at the peak-time national rate between two sites 100 km apart would justify the use of a private circuit rather than ISDN BRI.

Perform a similar calculation over a one year period, comparing the price of PRI with an E1 or T1 private circuit, to determine how many minutes a day would justify the use of a private circuit instead of PRI.

4.2.5 Intelligent networks

Intelligent networks are used to provide enhanced services for the PSTN that require access to a database called a **Service Control Point** (**SCP**). The telephone switches are able to request information from the SCP using SS7. This allows new software to be developed to provide enhanced services without having to make any major changes to the telephone switches.

Such services include number translation services, where the customer dials a special code followed by a number that is then translated to a real telephone number and the call is completed to this number, but the billing arrangements are different from those of a normal call.

[35] *See Section 6.5 of this volume.*

The translation used can take account of the caller's location, time of day and other factors. Such services include **free phone** calls (using 800 dialling codes), **local call fee access** calls, **national call fee access** and **premium rate** calls (using dialling 900 codes). These services allow enterprises to route customer traffic to appropriate call centres using a single advertised number. They can also be useful for telemarketing campaigns, where a company can be called from any location by means of a free or local rate call. They are also used for competitions and votes (both usually using premium rate) and to access recorded information or charged customer support (again often using premium rate).

Intelligent networks use the E.164 telephone numbering scheme, but with special non-geographic codes.

With all number translation services except free phone, where the owner of the called number pays the full cost of the call, a proportion of the revenue that is billed to the customer (the proportion will depend on whether the call is local, national or premium rate) is passed to the service provider who owns the called number. This is a useful source of revenue to the service provider, particular for premium rate calls, but it is also useful for local call fee access. It is this share of the call revenue, that made it possible for Internet Service Providers to offer free (no subscription) dial-up internet access.

Other services that are made possible by the use of intelligent networks are charge cards where calls made at any location are billed to home phone numbers using PIN[36] validation, personal numbering where customers can be reached by a single number, regardless of their location on the PSTN (or also potentially on a mobile network), number portability, where customers can change their network operator, but retain their existing number.

Intelligent networks also make Virtual Private Networks (VPNs) possible, where business customers can use the PSTN to switch calls between their PABXs, but with their own private numbering schemes and without the normal PSTN call charges. VPNs can also allow calls to break-out to the PSTN and break-in from the PSTN at remote locations so that they are carried by the VPN and are only charged at the rate appropriate to the part of the call that is not using the VPN (i.e. often at local call rates where the call is carried by the VPN over a distance that would normally attract national call rate). VPNs are offered often alongside a service where network operators offer all the features normally supported on customers' PABXs using public telephone switches. This service is known as Centrex.

4.2.6 Mobile networks

A mobile network can be thought of as a PSTN with wireless access and an intelligent network that supports mobility. The intelligence allows the network to keep track of the location of its users, so that they can make and receive calls regardless of their location and even while actually moving about.

The switched core network and intelligent network used by mobile phones networks uses the same architecture, addressing scheme and signalling protocols (SS7) as are used in the PSTN. The access network is very different. The PSTN local loop is replaced with a wireless access network with complex access protocols.

Mobile networks have been designed to inter-work with the PSTN and use the same E.164 numbering scheme with different National Destination Codes that identify the mobile network operator. The mobile networks are

[36] *Personal Identification Number – a numeric code only known to the owner of the charge card, used for authentication.*

connected to the PSTN from the special telephone exchanges, designed to handle mobile traffic, known as **Mobile Switching Centres** (**MSCs**) using E1 or T1 interconnect circuits.

Mobile network operators charge for voice services using a system similar to that used for the PSTN with monthly rentals and calls charged by duration and distance (international only). The only difference is that the call charges are much higher and more customers are using packages with higher rentals and a limited number of free calls.

They also have implemented a pre-pay service where customers buy credit in advance to be used to make calls. It is these pre-paid services that have allowed the market to grow from a niche business market to the mass consumer market it is today.

Messages are normally charged at a fixed rate per message, but again a limited number of free messages can be offered in the packages.

Circuit-switched data services at multiples of 9.6 or 14.4 kbit/s are normally charged by the minute (at the same rate as a voice call using the channel would be) for the total number of channels used.

Packet-switched data services are normally charged by the total number of kilobytes transferred.

There have so far been three (and a half) generations of mobile phone networks, although a fourth generation is currently being developed, which aims to offer data rates of 100 Mbit/s by 2010.

4.2.6.1 1G Mobile networks

The first generation was based on an analogue wireless access network using FDMA[37]. First generation mobile phones were very expensive in terms of both hardware and call costs. Handsets were bulky and heavy and battery life was short. They had a niche market amongst the business community, but were not a consumer product. The system employed in the UK was the Total Access Communication System (TACS) in North America a similar system operating in a different frequency band called Advanced Mobile Phone System (AMPS) was implemented. First generation networks only supported voice and are now obsolete.

4.2.6.2 2G Mobile networks

The second generation is a low speed digital wireless access network that supports voice and limited data features. We shall only consider the commonly used second generation technology called **Global System for Mobile Communication (GSM)** and its so called 2.5G enhancements to carry higher speed.

Network architecture

The 2G mobile access network consists of **Base Stations Systems** (**BSS**) which comprise one or more **Base Transceiver Stations** (**BTSs**) and a Base Station Controller (BSC). The BTS contains an antenna, radio transceivers and multiplexers and can receive signals from and transmit signals to mobile phones within range of the antenna, and allocate radio bandwidth to individual calls. The area around a mast where the signal is stronger than signals coming for other masts is known as a cell and as a result these types of networks are also known as cellular networks. The cells are designed in hexagonal patterns, although in practice the ranges of the antennae will not conform to this pattern due to topography, local radio conditions and the actual location of the antenna which sometimes, for practical reasons, cannot be sited at the centre of the cell. BTSs in adjacent cells use different

[37] *Frequency Division Multiple Access, see Volume 1, Section 7.3.8.*

frequency ranges to avoid interference, but a few cells further away, the frequencies can be reused as they will not interfere with each other. In built-up areas where a large amount of traffic is generated, a cell area can be split into a number of smaller cells each with its own antenna and frequency ranges but operating with less power. Within each cell, more traffic can be supported and interference from other cells minimised by using three or six directional antenna using different frequencies.

Mobility comes from the ability of the mobile phone to constantly monitor the strength of signals from nearby masts and 'hand-off' to another base station when a stronger signal is detected. This hand-off is carried out between the two BSCs quickly enough, for it to be imperceptible to users of the network. With fixed networks the switching function is only required at the beginning and the end of a call, but with mobile networks, calls can be switched at any time due to hand-offs, as the phone moves between cells. Switching in mobile networks is therefore much more complex than it is in fixed networks.

Each BSC is linked to a **Mobile Switching Centre** (**MSCs**)[38], which is connected to all the BSCs in its coverage area using E1 or T1 private circuits. The Mobile Switching Centres are telephone switches similar to those used within the PSTN but they are part of an intelligent network which is able to track the location of individual mobile phones, so that calls can be delivered to the BTS that is currently serving the called mobile phone. They must also be able to support the switching required for hand-offs when a mobile phone moves to a cell within the coverage area of a different MSC.

Each MSC has access to a number of databases via SS7. The **Authorisation Centre** (**AuC**) is used to check the validity of users and their authentication keys. The **Visitor Location Register** (**VLR**) stores information about the location of all the mobile phones in the MSC's coverage area including the phone's current BSS. The **Home Location Register** (**HLR**) is used to store permanent and semi-permanent information about the mobile phone customer, including details of the current VLR serving the mobile phone. The VLR is updated whenever a mobile phone hands off to another base station in the MSC's coverage area and the HLR is updated whenever the mobile hands off to a base station in another MSC area. The **Equipment Identity Register** (**EIR**) contains information on the mobile phone itself and its capabilities.

Calls are circuit switched by the MSC between BSCs and to or from the PSTN or other mobile networks. Because a large proportion of calls are switched between a mobile network and other fixed or mobile networks, MSCs are often used that do not support BSCs but are dedicated to switching traffic to and from other networks. These are called **Gateway Mobile Switching Centres** (**GMSCs**).

Network operation

GSM operates at frequencies around 900 MHz, although similar technology is also deployed at other frequencies, such as 1800 MHz and 1900 MHz. It uses both FDMA and TDMA. The available bandwidth is divided 124 analogue 200 kHz channels using FDM. To avoid interference, adjacent base stations do not use the same frequencies. Each of these FDM channels is then further subdivided into eight TDM channels each capable of carrying a 13 kbit/s compressed voice signal or up to 14.4 kbit/s of data. All signalling takes place via a common control channel.

An important aspect of GSM is the **Subscriber Identity Module** (**SIM**) card that stores information about the subscriber including identification, the mobile phone number that has been allocated and a secret key. Access to the

[38] Also known as Mobile Telecommunications Switching Office (MTSO) in North America.

SIM card is usually protected with a password or a PIN number. The SIM card can also be used to store information that customises the phone or to support applications such as mobile banking. By storing all this information on the SIM card, a customer can insert the SIM card in another mobile phone which will then offer the same profile as the previous phone.

When a handset is switched on, it has to register with the network via its nearest BSS. The handset scans all the control channel frequencies to find the BSS with the strongest signal. It then performs a handshake with the MSC via this BSC, to identify itself and so that the MSC can register its location in the VLR. This scanning process is repeated periodically, to check whether there is a need to hand-off to another BSS.

The handset user indicates that he wishes to make a call to another mobile phone by keying its number or by selecting the number from a pre-configured list and then pressing a call button (note that there is no dial-tone on a mobile phone). The call is processed by the MSC in a similar way to a fixed network call using SS7 on the control channel except that the MSC has to access the HLR and VLR using SS7 to discover how to route the call. If the call can be completed, the MSC allocates a two-way radio channel between the phone and the BSS to be used for the call. The handset then tunes to these frequencies. The MSC will connect these radio channel to radio channels that have been allocated for the receiver at its BSS. The MSC signals the progress of the call to the handset which produces audible tones as well as updating the screen display on the handset.

When the receiving MSC (assuming it is a different one) receives the incoming call it has to page the receiving mobile phone. It does this by issuing a message to the handset over the control channel for the BSS on which it is registered. The user can accept the call by pressing a button on the handset. At this point, the MSC will allocate a two-way radio channel between the receiving BSS and the phone, to which the phone will tune. It will also issue an SS7 message to the calling MSC to say that the call has been answered. This message as it passes through any other MSC will cause a connection to be set up between the two phones via their BSSs for this call.

Hand-offs can occur at any point whether a call is in progress or not. There are five type of hand-off that can occur:

- **Intra-Cell** hand-off, where interference or other disturbance occurs on the channel.
- **Intra-BSC** hand-off, where hand-off is required between BTSs managed by the same BSC. This will occur when a phone moves between the sectors.
- **Intra-MSC** hand-off, where hand-off is required between different BTSs controlled by the same MSC.
- **Inter-MSC** hand-off, where hand-off is required between different BTSs controlled by different MSCs.
- **Inter-System** hand-off, where hand-off is required to a BTS on another mobile network. This is quite rare as most networks do not allow this type of hand-off.

In order to decide when a hand-off should take place, the phone measures the signal levels of its nearest sixteen cells and reports the best six signal levels to its BSC. The decision to hand-off can be made by the phone or the BSC or the MSC. The BSC or the MSC may decide to hand-off if it is getting busy and there is a need to balance loads. The handoff is managed by the BSC or MSC depending on the type of hand-off. For BSC managed hand-offs the MSC has to be informed after completion to update the VLR. The hand-off can typically be completed within 300 ms without only tens of ms disruption to the call.

GSM also includes a facility to send and receive short text messages, of up to 160 characters, known as the Short Message Service (SMS). GSM also offers Multimedia Messaging Service that will allow photos, voice and video messages to be transmitted.

4.2.6.3 2.5G Mobile networks

Data Rates on GSM were originally limited to 9.6 kbit/s on a normal circuit switched voice channel which is very low compared to fixed networks. There has been considerable pressure to improve this and a number of ways providing higher data rates have been devised. They are known as 2.5G as they are enhancements to 2G technology, prior to the widespread introduction of 3G technology. The data services offered are:

- **High Speed Circuit-Switched Data** (**HSCSD**), which boosts the data rate of a GSM channel from 9.6 kbit/s to 14.4 kbit/s and allows channels to be bonded so that 28.8 kbit/s can be supported over two GSM channels or higher rates using more channels.
- **General Packet Radio System** (**GPRS**) achieves a theoretical maximum speed of 171.2 kbit/s by using all eight GSM TDM channels on an analogue FDM channel. Other demands on bandwidth in the GSM cell mean that users are unlikely to be able to achieve this data rate in many cases. GPRS provides an 'always on' packet switched data service.
- **Enhanced Data rates for Global Evolution** (**EDGE**) improves on the data rates achieved by GPRS by using 8-PSK modulation in the same FDM channel that is used by 8 GSM voice channels. EDGE can achieve data rates of 384 kbit/s.

4.2.6.4 3G Mobile networks

The third generation is called Universal Mobile Telecommunications System (UMTS). As its name implies and, unlike the previous generations, it is a universal standard, which is designed to carry high speed data for multi-media communications.

The path from second to third generation mobile technology is evolutionary rather than revolutionary. The new technologies have been designed to work with the existing MSC infrastructure for voice and to provide a separate core data network, using IP and ATM technologies. Eventually, we can expect both voice and data services to be combined on a core IP network. UMTS operates at around 2000 MHz and is a true third generation technology. It does completely replace the 2G radio interface, replacing the FDMA and TDMA of GSM with Wideband Code Division Multiple Access (WCDMA) using direct sequence spread spectrum techniques. It can operate at up to 2 Mbit/s over short distances. It has been designed to interwork with GSM, and calls can be handed off between the two networks.

4.2.6.5 Mobile data protocols

A number of different approaches have been offered to define protocols to carry application level data over mobile networks. The main ones are:

- **Wireless Application Protocol** (**WAP**) allows mobile phones to access Internet content over 2G, 2.5G or 3G networks. WAP defines a wireless protocol stack, similar to a cut-down version of TCP/IP. It is controlled by the WAP Forum whose founder members were Ericsson, Motorola, Nokia and Unwired Planet. A low functionality microbrowser is incorporated into the phone, which acts as a client to a WAP gateway where most of the intelligence resides. Content is delivered via the XML-based Wireless Mark-up Language (WML), which the gateway fetches from special web pages coded in WML or it fetches HTML and filters the content into WML. The gateway not only translates the application protocols, it also translates between TCP/IP and the equivalent WAP protocols. WAP was badly over-hyped when it was first marketed. It was sold as the wireless Internet which, given that it only provided 9.6 kbit/s over a connection that took a while to establish, and that it offered a limited amount of suitable content shown on a very basic screen, was something of an overstatement. As a result of this and high prices, WAP has not so far, been as successful as it was expected to be.

- **iMode** is a proprietary set of protocols invented and owned by NTT DoCoMo (the mobile arm of the Japanese incumbent). It uses a simple packet switched protocol called the Lightweight Transport Protocol (LTP). It also can run over any 2G, 2.5G or 3G data service and it uses the Compact Hyper-Text Mark-up Language (cHTML), a subset of HTML at the application layer. A gateway is required to translate TCP/IP to LTP. However, no translation is needed for cHTML as it is a proper subset of HTML. It has been extremely successful in Japan (over 35M subscribers have joined the service in three years). Its success can be put down to it being an always on packet switched service (no wait needed to establish a circuit switched connection), low PC ownership in Japan which means that it is the primary source of on-line information, support of the Japanese graphic alphabet, low prices, and it not being over-hyped as the mobile Internet.

Activity 4.7

Find out how many mobile network operators offer GSM or equivalent mobile services in your country and what dialling codes are used to identify their networks? What frequency range does each network use (800, 900 or 1800 MHz)? What data services do they offer? Do they support WAP or iMode? Do they also offer 3G (UMTS) services?

4.2.6.6 Messaging applications

GSM was launched with a messaging application, also known as text messaging or texting. Because it was originally aimed at the business market and businessmen found its user interface to be unfriendly (if they knew about it at all), it was hardly ever used. It was only when the GSM phone became a consumer product that was popular in the youth market that messaging took off. Messaging is now a major source of revenue for the mobile network operators.

The original messaging service on GSM was the Short Message Service (SMS). It uses the control channel to transmit text messages of up to 160 bytes using 7-bit codes to a Short Message Service Centre which uses a store-and-forward technique to pass the messages to the recipient phone. GSM also supports the Unstructured Supplementary Data Service (USSD) that supports a session-based service over the control channel that is much faster than SMS and can transmit messages of up to 182 bytes. Multimedia Messaging Service (MMS) is an enhancement to SMS that runs over WAP and GPRS and allows images, sounds and videos to be sent, again using store-and-forward techniques. MMS can also use a GSM 9.6 or 14.4 kbit/s data channels. It uses Synchronised Multimedia Integration Language (SMIL) at the application layer.

4.2.7 Public Packet Switched Data Networks (PPSDNs)

These networks had their origins in the late 1970s, at about the same time as the Internet was evolving in the USA. They are often called **X.25** networks after the protocol suite which was used to access them. The X.25 protocol suite was defined by the CCITT[39] (now the ITU-T[40]) which was predominated by the incumbent PTTs. Because of their background in telephony, the standards developed were connection-oriented, unlike the connectionless network protocol being developed for the Internet. The X.25 standard defined the interface between the user's terminal equipment (DTE) and the operator's packet switch (DCE). It did not attempt to define the protocols used between packet switches, although many operators also used the X.25 protocols between their switches. X.25 was specified in a time when only low speed analogue circuits were available (typically 300 bit/s to 48 kbit/s). It therefore had to cope with high error rates. The PPSDN supports both SVCs[41] and PVCs.[42] All packets use virtual circuit numbers for addressing. SVC Call Request packets use an addressing scheme called X.121 which is coded by up to 14 Binary Coded Decimal digits. The first three digits are the Country Code and the next digit is used to identify the network within the country. The first four digits are known as the Data Network Identification Code (DNIC). It is interesting to note that the ITU-T thought that most countries would not require more than 10 PPSDNs and those that did were just allocated additional country codes. The USA were actually allocated six country codes. X.25 supported Closed User Groups (CUGs) for security where groups of X.121 addresses could be defined as belonging to a CUG and only addresses defined in this group could communicate with each other.

In addition to the X.25 protocol, CCITT also specified a protocol (X.29) to allow low-speed asynchronous character-mode terminals to access a PPSDN via a Packet Assembler Disassembler (PAD) and also a protocol (X.75) that could be used to interconnect two PPSDNs and negotiate facilities offered and support accounting between operators. In their early days, the PPSDNs were very successful, because they were much more reliable and cheaper to use than the only other alternative – the international phone network. Within a short time, most countries had implemented a PPSDN and had interconnections with other countries forming a truly global data network. They were however overtaken by the Internet. The X.25 protocol suite became rather inefficient and cumbersome, as the quality and speed of circuits improved with digital transmission. Also the costs of using the Internet were not usage related and were much cheaper and more predictable than using a PPSDN, even though the quality was sometimes not as good. Finally, a new light-weight protocol with much less error control called **frame relay**, which was better suited to modern digital circuits, was devised and many X.25 implementations were migrated to frame relay.

PPSDN charges include connection charges for access circuits, depending on the speed of the circuit, and a monthly rental for the access circuit, again depending on speed. These charges are usually distance independent. In addition, there are rental charges for PVCs based on the amount of data sent over the PVC, which will probably also be distance independent, apart from international ones. SVCs are often charged on a per-minute basis, plus a charge for the total amount of data exchanged which was normally measured in kilocharacters or kilopackets or kilosegments (where a segment was a unit of data up to 64 bytes long).

PPSDNs and X.25 still exist, although they are usually associated with legacy applications or parts of the world where more sophisticated public networks have not been built.

[39] *Comité Consultatif International Téléphonique et Télégraphique.*

[40] *International Telecommunications Union – Telecommunications Standardization Sector.*

[41] *Switched Virtual Circuits.*

[42] *Permanent Virtual Circuits.*

4.2.8 Frame Relay Networks

In the late 1980s, as the performance of digital circuits improved, the need for a new connection-oriented light-weight protocol for business users was recognised. A number of suppliers and operators collaborated to produce a standard that did not have the sophisticated error checking and consequent protocol overhead that occurred with X.25. This new protocol became known as **Frame Relay** and the collaborators became the Frame Relay Forum. As its name implies, it simply relays data link layer frames without the need for a network layer protocol and at higher speeds than X.25 (typically 64 kbit/s to 2 Mbit/s). As such, it is ideally suited to carrying internetworking protocols, such as IP. Like X.25, it provides a connection-oriented service using virtual circuits identified by **Data Link Connection Identifiers** (**DLCIs**), which, in theory, can be switched or permanent. But unlike X.25, most frame relay implementations only support Permanent Virtual Circuits (PVCs) which are unidirectional and hence the data rates in each direction can be asymmetric.

Frame Relay networks use either the E.164 telephone numbering scheme or the X.121 data network addressing scheme for SVCs, but because most customers only use PVCs, they do not need to be aware of any addresses other than DLCIs which can be arranged to be globally unique on a customer's network and hence can be used for addressing within that network.

Frame Relay's error correction facilities are limited to discarding frames when errors are detected. When congestion occurs, frames are also simply discarded, but a Forward Explicit Congestion Notification (FECN) bit in the headers of subsequent frames to the destination can be set and a Backwards Explicit Congestion Notification bit in frames to the source.

Enterprises use frame relay as an alternative to building their own private networks. Instead of building a mesh network, the enterprise orders access circuits to the network provider's nearest frame relay node. To provide resilience, a dual-access circuit could be ordered. The enterprise then orders PVCs to be configured between each of its sites and the network operator configures these PVCs across the network. When ordering a PVC the enterprise has to specify its **Committed Information Rate** (**CIR**) in bits/s. The network operator will commit to being able to deliver frames at this rate, but will also be able to make its best effort to deliver frames when the CIR is exceeded. This process is known as bursting. Interestingly, the total capacity of all the PVCs carried over an access circuit can exceed the capacity of the access circuit. This is called over-subscription and it can be done, because frame relay traffic is bursty and it is unlikely that all PVCs will use their allocated capacity at the same time.

Frame Relay charges include connection charges for access circuits, depending on the speed of the circuit and a monthly rental for the access circuit, again depending on speed. These charges are usually distance independent. In addition there will be rental charges for PVCs per kbit/s based on the CIR which will probably also be distance independent, apart from international ones. There is a separate rate charge for being able to burst to a rate above the CIR. For SVCs, where they are offered, the charge is usually based on the total amount of data exchanged in kilobytes.

Frame Relay is ideally suited for transmitting large quantities of data many sites, particularly where the transmission between any two sites is bursty. This make it an ideal technology for LAN interconnections between the sites of an enterprise. It is generally cheaper to build and manage than a private circuit network, as the costs of building and managing the network (which is done by the network operator) are shared with other customers.

Activity 4.8

Visit the web sites of some of the network operators who offer telecommunications services in your country and investigate the frame relay products they offer. Check how these products are priced.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. SMDS is a connectionless network layer protocol that supports multicasting and the E.164 telephone numbering scheme.

ii. In North America all private circuits are terminated on an NTU owned and provided by the network operator.

iii. The GSM radio interface uses both FDMA and TDMA access methods.

iv. ATM cells are variable length packets up to 53 bytes long, including a 5-byte header.

(b) Describe the main differences between the PDH and SDH technologies used by network operators in their transmission networks.

(c) What are the main advantages and disadvantages of using satellite communications?

(d) Describe what happens when a mobile phone is handed-off from one base station to another one.

(e) Describe the main differences between X.25 and Frame Relay and the reasons why one has evolved from the other.

Learning outcomes

At the end of this chapter, you should be able to:

- outline how SMDS and Cable TV networks operate
- outline how private circuit and satellite networks operate and describe their main advantages and disadvantages
- outline how the PSTN, ISDN, intelligent and mobile networks switch voice calls
- outline the various mobile data options which are evolving for mobile phone users
- outline how X.25, Frame Relay networks operate and describe their main advantages and disadvantages
- distinguish between all the above MAN and WAN technologies and comment on their suitability for various types of application.

Notes

Chapter 5: Network integration (internetworking)

Further reading

Forouzan, Behrouz A. *Data Communications and Networking.* (McGraw Hill), third edition, 2003. Chapters 16.1, 16.2, 19, 21, 31.5.

Kurose and Ross *Computer Networking – A Top Down Approach featuring the Internet.* (Addison Wesley), third edition, 2005. Chapters 4.5, 4.6, 4.7.

Stallings, William *Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003. Chapters 12.3, 15.4, 15.5, 18.2, 18.3, 19.1, 19.2.

Tanenbaum, Andrew S. *Computer Networks.* (Prentice Hall International), fourth edition, 2002. Chapters 4.7–4.7.5, 5.2–5.2.8, 5.5.2, 8.6.3.

In the last chapter we studied a number of different network technologies that developed separately to meet different needs. In this chapter, we will study how some of these technologies can be integrated into a single network platform. There are two reasons why this should be necessary. Firstly, some of the technologies, such as those used by LANs have limited ranges and work over infrastructure that is owned by the enterprise itself, while others, such as those used by WANs have been designed to work over long distances over infrastructure owned by network operators. In order to support end-to-end communications, there is a requirement to connect up these technologies to provide an integrated service. This type of integration is known as internetworking. An internetwork is simply defined as a network of networks that is able to function as a single network. The networks forming an internetwork can be LANs, MANs or WANs using internetworking devices, such as bridges, routers, switches, relays and gateways.

In this chapter, we will consider the integration of different network technologies by internetworking and will structure our study using the layers of the hybrid reference model in which the integration takes place. In the data link layer we will study bridging and data link layer switching as a means of internetworking. In the network layer, we will study routing and network layer switching as a means of internetworking. We will also briefly consider transport layer relaying at the transport layer and gatewaying at the application layer. Finally we will study routing on the Internet, Intranets, Extranets and IP VPNs[1] and multicasting.

[1] *Virtual Private Networks.*

5.1 Internetworking

The network technologies that need to be integrated into an internetwork can be very different and need to be considered in any internetworking solution. The main areas of difference, taken mainly from Tanenbaum, are:

- type of service offered (connection-oriented or connectionless)
- type of media used
- topology used
- data rate used
- protocols used
- addressing scheme used
- support of multicast and broadcast addressing

- maximum payload (frame or packet) size
- quality of service mechanisms (present, different types or absent)
- error control mechanisms (reliable, ordered or unordered delivery)
- flow control mechanisms (sliding window, rate control, other or none)
- congestion control mechanisms (leaky bucket, choke packets etc.)
- security mechanisms (privacy rules, closed user groups, encryption etc.)
- parameters (different timeouts, flow specifications etc.)
- accounting mechanisms (by the minute, packet, byte or no mechanism)

Of these differences, perhaps the most fundamental is the type of service offered by the network. Internetworking between a connection-oriented (CO) and a connectionless (CL) technology is going to be difficult because of the completely different approaches to networking which cause many of the other differences above.

Directly connecting two different CO network technologies is fairly straightforward. The PDUs[2] from the virtual channels of one network can be translated into the format required for the other network and forwarded over the virtual channels of the other network. Connection requests can also be translated (including addresses, if necessary). The connection between the two networks is carried out by an internetworking device concatenating the virtual channels. The differences in the protocol mechanisms between the two networks do not really matter. Two reliable connections are being joined together. It doesn’t really matter what makes each of them reliable. Most of the difficulties are concerned with setting up the virtual circuits. Once they are established, assuming that both networks provide a similar quality of service, PDUs can be exchanged fairly easily.

Connecting two different CL networks together is more problematic. The internetworking device has to, where necessary, translate the format of the PDUs it receives to the format required by the other network and translate the addresses. The two protocols are likely to support many different functions encoded within the protocol headers. Some of the functions supported in one network will not be supported in the other. This is difficult to handle and unless the two protocols are quite similar, it is unlikely to be attempted. It is possible, for instance, to translate between IP and IPX[3], because they are similar.

There are other situations where it is also relatively easy to connect CO network and CL networks. This is where there are more than two networks and the source and destination network are of identical type and the intervening network(s) provides a compatible service. The technique is for an internetworking device to encapsulate PDUs from the source network within PDUs of the intervening networks and then for another internetworking device to de-capsulate them at the other end and forward them over the destination network. This technique is known as **tunnelling**. It is as if the original PDUs disappear into a tunnel as they are encapsulated to cross the intervening network(s) only to re-emerge at the destination network. There are two combinations of networks where this can be done.

Connecting two similar CL networks by tunnelling through a CO network is not difficult. The internetworking device receives PDUs from one of the CL networks and has to examine their destination addresseses, map them to the addresses used on the CO network, set up a virtual (or real) channel, if it does not already exist, and encapsulate and forward the PDU on this channel. At the other side of the CO network, the internetworking device has to de-capsulate the original PDU and forward it to the destination over the CL network.

[2] Protocol Data Units

[3] Internetwork Packet Exchange – Novell’s internetworking protocol.

The problem area is where a CO network is to be connected with a another CO network by tunnelling through a CL network. The problem here is that the CO networks will expect delivery of data in the correct order without loss or duplication, and the CL network cannot guarantee this. This combination of networks will not work, unless the connection takes place at the transport layer or above, using transport relays or application gateways as the internetworking devices. Then a reliable transport connection from one CO network can be connected via a transport layer relay to a reliable transport connection across the CL network and then via another transport layer relay to the destination CO network.

When deciding at which layer to internetwork and which internetworking devices to use, it is important to consider performance issues. Generally, layer 2 switches and layer 3 switches perform better than routers and bridges, as the former are usually hardware-based and the latter are software-based. There are other factors to consider. These relate to broadcast storm problems. Protocols such as the Spanning Tree Protocol run on bridged or layer 2 switched internetworks and will cause broadcast storms across a whole internetwork, as it is a single broadcast domain. This problem can be greatly reduced by using VLANs[4], as each VLAN forms its own separate broadcast domain. The problem of broadcast storms does not exist if routers or layer 3 switches are used as internetworking devices as they also separate broadcast domains.

5.2 Data link layer bridging and switching

There are six main reasons why bridges are used.

- Two similar networks are separately managed (e.g. Departmental LANs), but need to be connected and the bridge can act as a clear demarcation between the two LANs.
- Two dissimilar networks need to be connected (e.g Ethernet and FDDI[5], although this can be problematic due to incompatibilities in protocols, such as bridges not being able to fragment frames).
- Traffic on a network is too heavy for a single LAN, but could be carried by two separate LANs connected via a bridge. (e.g. an Ethernet is experiencing too many collisions which can be reduced if the network is segmented into two collision domains by a bridge).
- The total distance of cable required for a LAN is outside the specification, and the LAN has to be segmented into two LANs separated by a bridge, so that each LAN meets its specification.
- Reliability considerations may cause a large LAN to be segmented with bridges. A single rogue NIC card on a shared LAN can sometimes start broadcasting complete garbage and make a whole LAN unusable until it is located and disconnected. Segmenting the LAN using bridges will reduce the effect of this problem to a single segment.
- The two networks are remote and need to be connected via a point-to-point link or WAN service. Bridges that support protocols such as HDLC[6] or Gigabit Ethernet can be used as internetworking devices to connect to the point-to-point circuit.

Switching has become increasingly important in LANs. The main reason for the increase in popularity is the higher performance which can be achieved using hardware-based switches and the ease with which they can be configured as compared with software-based manually configured routers.

[4] *Virtual LANs, see Section 3.3.1.8 in this volume.*

[5] *Fibre Distributed Data Interface, see Section 3.3.3 in this volume.*

[6] *High-level Data Link Control, see Volume 1, Section 7.5.*

The use of VLANs has further increased the popularity of layer two switching since the main problem with bridging (broadcast storms) has been reduced because each VLAN is a separately switched broadcast domain.

There are two main types of bridges that are used with different types of LAN or protocols. These are **transparent bridges** (sometimes called spanning tree bridges) and **source route bridges**. Transparent bridges are used on Ethernets and source route bridges are used on token ring networks. It is also possible to have a translational bridge that translates between one data link protocol and another, although, as we will see there are problems to be addressed when doing this. A final, less common type of bridge is a **remote bridge** where two bridges are used to connect two LANs over a WAN. These are often translational bridges that translate LAN protocols into WAN protocols, such as HDLC or PPP[7], and vice versa. But with the advent of metro Ethernet, it is possible to use the same protocol on the LAN and WAN segments.

5.2.1 Transparent bridges

Transparent bridges are so called, because the hosts on the network do not need to know anything about the bridges, or even whether they exist. The bridges are completely transparent to the hosts. Transparent bridges learn how to work by observing traffic on the two LANs they are connecting and build a forwarding table of the source MAC addresses of all the devices that transmit on each LAN. The table is initially empty, but soon fills up as new MAC addresses are discovered. When the bridge receives a frame, it looks the destination MAC address up in the table to see if it knows on which LAN this address is. If the address is not in its table or if it knows that it is on the other LAN, then it forwards the frame to the other LAN. If it knows the destination address is on the LAN that it received the frame from, then it discards it. This process is known as **backward learning**. The bridge is a true plug and play device, it requires very little configuration, but learns which frames it should forward and which frames it should discard.

When building a network or internetwork with bridges, it is useful to build in some resilience, so that a single failure of a bridge or a LAN segment will not cause the network to be disconnected. However if resilience is provided in this way, there will loops within the network that will cause major problems. Suppose two LANs are connected by two bridges. A frame generated on one LAN and destined for a new unknown MAC address will be forwarded to the other LAN which will be picked up by the second bridge, and because the destination is unknown, it will be forwarded back to the first LAN, whereupon the process will be repeated and the frame will loop indefinitely.

In order to avoid these problems, the redundant links within the network must be blocked off, so that there is only one path between any two bridges. This results in a tree-like topology known as a **spanning tree** and it is created using the Spanning Tree Protocol (STP).[8] STP selects which bridge ports are to be used for forwarding frames and which ports are to be blocked. The STP specification defines a default cost for each LAN speed. These have been changed from time to time as LAN speeds have increased. The current default cost are given in Table 5.1 below.

Table 5.1: Default Costs for Different LAN speeds

LAN data rate	Default cost
10 Mbit/s	100
100 Mbit/s	19
1 Gbit/s	4
10 Gbit/s	2

[7] *Point-to-point Protocol, see Volume 1, Section 7.6.*

[8] *IEEE 802.1d*

Each bridge has a unique bridge ID formed from concatenating a user defined priority with one of the bridge's MAC addresses. The default priority is 32,768. The Spanning Tree Protocol starts by all bridges broadcasting Bridge Protocol Data Units (BPDUs). All the bridges in the broadcast domain will see all the BPDUs and the one with the lowest bridge ID will be elected as the **root bridge**. The root bridge then broadcasts another BPDU and all the other bridges forward the broadcast but add the cost of the LAN from which they received the frame into a field within the BPDU. Each bridge will therefore receive copies of all the BPDUs broadcasted from all the other bridges and it is therefore easy for a bridge, by comparing all the BPDUs it receives, to discover which of its ports has the lowest cost path to the root. This is known as the **root port** and it will be used for forwarding. From each LAN, each bridge can also determine the bridge port that has the lowest cost path to the root and this is called the **designated port**. This too will be used for forwarding frames. All other links are blocked. The root broadcasts BPDUs every two seconds which are forwarded down the spanning tree. The spanning tree is recalculated, by the above process, if these BPDUs are not received.

While STP is running, the bridge ports transition through four states, two of which (listening and learning) are transitory and the other two (blocking and forwarding) are permanent (until the next spanning tree calculation). There is a further disabled state, but this is not discussed here to keep things simple. All ports are initially in the blocking state. During the period when all the ports are broadcasting BPDUs, all the ports are in the listening state and for a period after STP has chosen which ports to block but before information frames are forwarded, the ports are in the learning state, while they check that there are no loops. At the end of the STP process each port will either be in the forwarding or blocking state. Table 5.2 summarises what happens in each state:

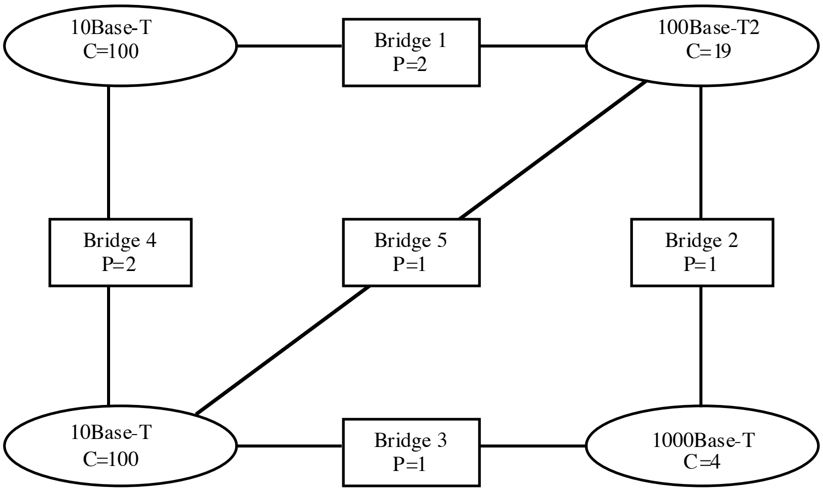
Table 5.2: Spanning tree protocol port states

State	Receives BPDUs	Processes BPDUs	Receives info frames	Forwards info frames	Event causing state transition	Next state
Blocking	✓	✓	✗	✗	Selected as root or designated port	Listening
Listening	✓	✓	✗	✗	Timer expires	Learning
Learning	✓	✓	✓	✗	Timer expires	Forwarding
Forwarding	✓	✓	✓	✓	STP recalculation	Blocking

The STP calculation can take between 30 and 50 seconds to converge. During this time no information frames can be forwarded on the whole network. This is a very long time for a network to be out of action and the IEEE have defined a new protocol called the Rapid Spanning Tree Protocol (RSTP)[9] which can converge in about three seconds. This is achieved by defining a back-up port as well as a designated port on each LAN and by greatly reducing the timeouts and the disabled, blocking and listening states are reduced to a single discarding state.

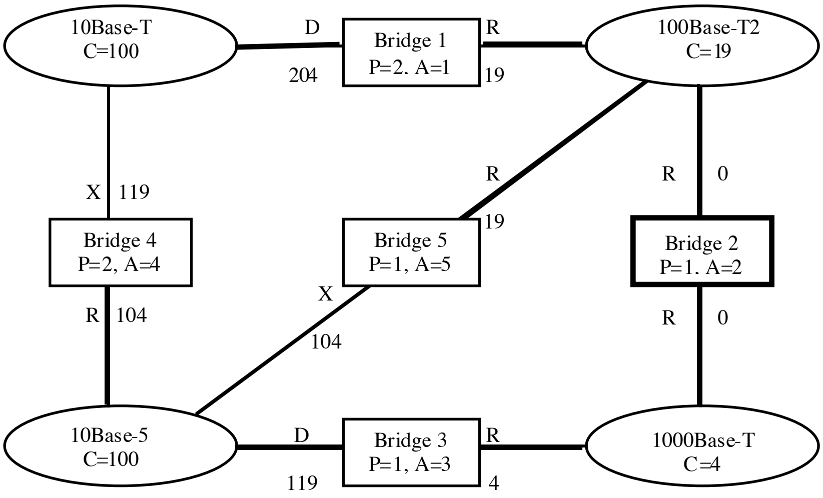
[9] *IEEE 802.1w*

Figure 5.1: Spanning tree protocol example



Bridge 2 is elected the root bridge, as it has the lowest bridge ID taking account of its priority (1) first and then its address (2). The least cost paths to the root bridge from each port, taking account of the default cost (C) of each LAN are calculated and the costs are marked. The port of each bridge that has the least cost path to the root bridge and all of the ports of the Root Bridge are called root ports and are marked R. Then, the designated port for each LAN is calculated as the port from each LAN that has the least cost path to the root bridge. In the event of ties, the ports with the lowest MAC address are chosen. The designated ports are marked D. All remaining ports are blocked and are marked X. The resulting spanning tree is shown with thickened lines.

Figure 5.2: Spanning tree protocol solution



Activity 5.1

In Figure 5.1, consider what happens when a host on the 10Base-T LAN in the top left hand corner send a frame addressed to a server on the 1000Base-T LAN in the bottom right hand corner, when there are no entries in the bridge tables of any of the bridges.

Carry out a simulation of what happens as each of the bridges receive frames with an unknown destination address on one port and then broadcasts it on the other port. Satisfy yourself that a copy of the frame will enter into a loop. Repeat this simulation for the network in Figure 5.2 with two bridge ports blocked and satisfy yourself that the frame will be delivered without a copy entering a loop.

5.2.2 Source route bridges

Source route bridges are not transparent. Hosts have to know the topology of the network and be aware of the shortest paths through the network to each destination. When the host transmits a frame it must specify the path that it should take through the network. They learn the topology and the shortest path routes by broadcasting a discovery frame to all of the hosts on the network. All the hosts respond to this frame with another broadcast and as the responses pass through bridges back to the host, the bridges add their own identifiers and the identifiers of the segment on which the frame was received to fields within the discovery frame and then re-broadcast the frame. The host will receive multiple responses to the discovery frames, indicating all the different possible paths between the two hosts and it is thus able to build its view of the network topology and determine the best route to each host on the network. This process on a large network can lead to a broadcast storm, particularly after a network failure when all the hosts are trying to discover the best paths.

Apart from the obvious point that transparent bridges are fully transparent to the hosts and source route bridges are not, there are many other differences between the two types of bridge:

- Source route bridging is best suited to connection-oriented networks, while transparent bridging is best suited to connectionless networks.
- Transparent bridges require little manual configuration, while source route bridges require a good deal of manual configuration.
- Transparent bridges do not provide optimal routes while source root bridges do.
- Transparent bridges learn how to forward frames by backward learning while source route bridges are told how to forward each frame by the source host which has learnt the optimal route from broadcast discovery frames.
- Transparent bridges recover from network failures by initiating a recalculation of the spanning tree. The hosts are not involved at all. With source route bridging, it is the hosts that initiate recovery by sending out discovery frames.
- With transparent bridges, the complexity resides within the bridges rather than the hosts, while with source route bridges it is the other way around.

5.2.3 Translational bridges

A translational bridge converts between one LAN protocol and another. This might sound easy, but there are many problems. Even when both LAN protocols are specified by the IEEE, there are many issues that occur, as identified by Tanenbaum. Bridging between fixed LANs such as between Ethernet or Token Ring and an FDDI backbone is relatively straightforward, but bridging between Ethernet and Token Rings and between fixed LANs and wireless LANs is very difficult. The issues include differences in frame formats, which can often be translated fairly easily, but some fields in one protocol may have no equivalents in the other. Secondly, the data rates can be very different. A Gigabit Ethernet could be passing data at full speed into an 11 Mbit/s 802.11b Wireless LAN and if the rate is sustained, buffers will eventually overflow. A serious problem is also caused by the different maximum frame lengths supported on different LAN technologies. No LAN data link protocols support frame segmentation and if a frame is larger than the maximum size supported will have to be discarded. Another issue occurs with security. Wireless LANs use encryption, but fixed LANs do not. Where data link encryption is used on a wireless LAN, no station on a fixed LAN will be able to decrypt it, forcing the wireless stations to drop encryption and expose itself to security risks. Finally, Ethernet does not support any quality of service while wireless LAN protocols and Token Ring do, so quality is service will be lost when these networks are bridged to an Ethernet. All these issues have to be addressed by the bridge's translation software. Some issues such as problems with different maximum frame sizes have to be resolved by ensuring that hosts do not transmit frames that will be too large for each LAN supported by the translational bridges.

5.2.4 Remote bridges

Remote bridges are used to connect LANs on different sites over a WAN. Each bridge connects to a LAN on one side and a WAN service on the other side which can be regarded as a segment without any hosts. The WAN service used could for example be PPP over a low speed point-to-point private circuit and the LAN frames could be encapsulated within the PPP frames. Alternatively, the LAN protocol headers could be stripped off by the bridges and the payload of the LAN frame could be encapsulated within PPP. This latter method will not provide end-to-end error checking, although there will be checking on each individual segment. At higher speeds, if all the LANs are Ethernets, it would be sensible to use metro Ethernet protocols for this WAN segment.

5.3 Network layer routing and switching

Internetworking can also be carried out at the network layer. This is desirable if different protocols are being used at the data link layer. As we have seen there are potentially many differences between network technologies that make bridging between different LAN data link layer protocols problematic. For this reasons, it is often best to internetwork using routers rather than bridges when different LAN technologies are being used.

A prerequisite for routing is that a **routable protocol** must be used. A routable protocol, is a protocol which supports hierarchical addresses where part of the address can be used to identify the destination network and the remainder of the address is used to identify the host on that network. This implies a network layer protocol, rather than a data link layer protocol, which has no concept of networks and has a flat addressing structure. It therefore is impossible to route data link layer protocols. Similarly, it is impossible to route SNA traffic at the periphery of an SNA network (up to Front End Processors), as it also uses a flat addressing structure in this part of the network. NetBIOS[10] Extended User Interface (NetBEUI), which is used in Microsoft local area networking, is another example of a non-routable protocol, as it uses flat MAC addresses. NetBEUI is often encapsulated in TCP/IP in the wide area.

The other pre-requisite for routing to take place is that routing information must reside in each router in order for them to route packets towards their destination over suitable paths. Although, it is possible to configure the

[10] *Network Basic Input/Output System.*

routing information in each router manually, this is unlikely to be practical for a large network and a means of automatically updating routing information in each router is required. To do this a **routing protocol** is required. Routing protocols allow routing information to be automatically distributed to each router, taking into account changes in network topology and possibly also traffic conditions. Note the difference between a routing protocol and a routable protocol. Routing protocols are usually encapsulated in the routable protocol for which they are carrying routing information.

5.3.1 Routers

Routers are network layer devices that perform the following functions on datagrams that they receive:

- read the network layer destination address
- extract the network part of the address
- look up the network part of the address in a routing table to determine where to forward the datagram
- forward the datagram towards its destination network either directly or via another router.

To read the network layer address, the router must de-capsulate the network layer datagram from the data link layer frame it receives. The network layer within the router just receives the network layer datagram. When it forwards the datagram, it must pass it to the data link layer which will encapsulate it again in a data link layer protocol. It doesn't matter therefore whether the two data link layer protocols are the same or different. This makes the router an ideal device for internetworking between different data link layers.

Most routers are described as multiprotocol routers. The use of the term multiprotocol refers to the ability of the router to carry more than one network layer protocol, even though these days many such routers only carry one network layer protocol (IP). A router could for instance carry IP datagrams along with IPX datagrams and forward them over the same data link. At the next router the data link layer software will use the type field to de-multiplex the datagram and pass it to the correct process (IP or IPX) to route the datagram. If the network layer protocol is not routable, then a multiprotocol router will act as a **brouter**[11] and will attempt to bridge the frame, at the data link layer.

Another potentially confusing term that is sometimes used for a router is a **gateway**. Historically, this is what routers were called and this term is used in the names of a number of routing protocols. A more modern use of the term, is to describe an internetworking device that carries a translation function between two protocols. This can be done quite easily if the two protocols are similar. A number of multiprotocol routers are able to translate between IP and IPX, for instance, but this is quite uncommon and most routers just forward datagrams using the same network layer protocol. Gateways, using the above definition can operate at other layers than the network layer.

A full gateway is an internetworking device that can perform this translation directly between two protocols on its own. A half gateway translates one protocol to an intermediate neutral protocol which is then forwarded to another half gateway, usually at a remote site, which translates the neutral protocol into a third protocol.

[11] *Bridge Router.*

5.3.2 Routing algorithms

Routing protocols are simply implementations of algorithms that are used to calculate, and distribute routing information.

ISO has defined a network hierarchy that provides a useful framework when studying routing algorithms and protocols. The terms used are:

- **End System** (**ES**) which has a full protocol stack and performs no routing or packet forwarding function. (e.g. terminals, printers or hosts)
- **Intermediate System** (**IS**) performs routing and traffic forwarding functions (e.g. bridge, router, relay or gateway)
- **Autonomous System** (**AS**) is a collection of networks under a common administration that share a common routing strategy
- **Area** (or **Domain**) is a contiguous subdivision of an AS that shares a common routing strategy.

Stallings[12] has identified a number of requirements for routing algorithms.

The algorithm should be:

- correct and be able to calculate valid routes through a network avoiding any loops
- simple so that routing software is not large and complex
- robust so that network failures can be discovered and overcome
- stable and not lead to situations where a route alternates between two states, as can happen if account is taken of network load (traffic on a route subject to a heavy load may be re-routed onto a route which has a much lighter load, but this then becomes heavy and the traffic re-routes back to the original route which has now become light again and this pattern then repeats itself)
- fair, so that equivalent traffic is not unfairly delayed
- optimal so that it can calculate optimum (or near optimum) routes
- efficient, so that it does not consume an inordinate amount of processing time or bandwidth.

Some of these objectives will conflict with each other and tradeoffs will be necessary. There are tradeoffs between correctness and simplicity, between robustness and stability and between fairness and optimality.

In order to calculate a shortest path, it is necessary to define a metric by which the cost of a path can be measured. Some algorithms use a single metric, others use a composite metric calculated from a formula involving a number of metrics.

The metrics used could include:

- hop count
- bandwidth
- delay
- distance
- Maximum Transfer Unit Size supported
- load
- circuit costs
- reliability.

Routing algorithms can be classified into various types.

[12] *Stallings, p.370.*

5.3.2.1 Unicast or multicast routing

Routing protocols can support unicast routing where just one copy of a packet is delivered to a single destination or multicast where multiple copies of the same packet are delivered to multiple destinations. The latter is much more complicated and requires special multicast routers that support this type of routing and routing protocols. Multicasting is much more efficient for applications that need to deliver the same data to a large number of sites.

5.3.2.2 Static (or fixed) versus dynamic (or adaptive) routing

In static routing, the paths selected are pre-determined and cannot be updated automatically. Routing tables are calculated manually using algorithms such as Dijkstra's to compute the shortest paths through the network and the tables in each router are configured manually. This is hardly an algorithm at all, but it can be useful for small networks. It does not scale well to larger networks and suffers from not being able to recover automatically from network failures (unless back-up routes can also be statistically defined). The PSTN actually uses static routing for call establishment, even though it is a very large network. It is a good routing strategy as the addressing structure (the dialling codes) are very stable and are not frequently changed and the network is also very stable and often fully meshed, so static routes with back-up routes do not need to be updated very often.

In dynamic routing, the paths taken are not pre-determined and can be changed automatically, as the topology of the network or conditions on the network change. There are three types of dynamic routing:

Isolated routing

In isolated routing, the routing decisions are made without reference to any externally generated information. Each router makes its routing decisions autonomously. There are various techniques that can be used:

- **Flooding** is a technique where the router always forwards the same packet on all its ports, apart from the port on which the packet was received. It guarantees that a packet will get through to its destination in the least time, but at the cost of a huge flood of packets. The flood can be reduced by using a hop count field in the protocol header (such as TTL[13] in IPv4) and discarding the packet after it has been routed a certain number of times. Sequence numbers can also be used to make sure that a router does not flood the same packet a second time. Flooding is used in certain military networks, where the nodes are subject to destruction by enemy action. Flooding is also used in ad-hoc radio networks and by some routing protocols.
- **Random routing** is where the router chooses the port on which to forward the packet randomly. It uses significantly less bandwidth than flooding, but a packet can take a very long time to reach its destination.
- **Hot potato routing** is where the choice of output port is made on the basis of which port has the shortest queue of packets awaiting transmission. It is good at load balancing, but suffers the same problem as random routing in terms of the long time a packet may take to reach its destination.
- **Backward learning** is a more sophisticated technique. The router examines all the packets it receives from each network and their hop counts. It can then choose the best route to a network by choosing the port on which packets were received from that network with the lowest hop count. In order to discover and recover from failures, the routers must revert to random routing so that routes can be recalculated.

[13] *Time To Live.*

Centralised routing

In centralised routing, a single central system, monitors the status of the whole network and calculates all the shortest path routes, using algorithms such as Dijkstra's. Whenever a router needs to make a routing decision it queries the central system. The network is vulnerable to a failure of this central system or communications to it and a back-up is required. The solution does not scale well, although it has been used in at least one PPSDN.[14]

Distributed routing

In distributed routing, the routing tables are calculated by each router based on routing information which is distributed amongst the routers by means of routing protocols. Distributed routing is much more robust and flexible than centralised routing, but it is more complex and there is a large overhead in processing power and bandwidth requirements. There are two main types of distributed routing algorithms and a third hybrid type:

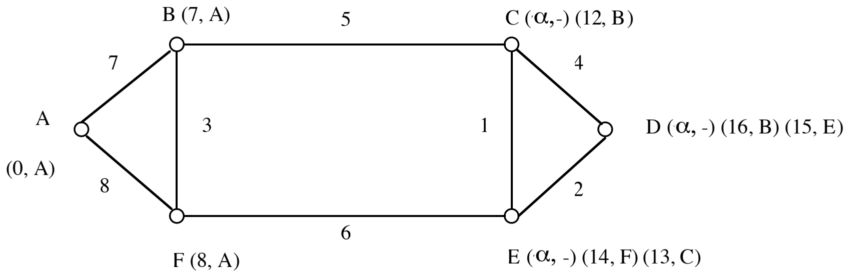
- **Distance Vector (DV)** routing algorithms involve the regular exchange of routing tables between immediate neighbours which then recalculate the shortest routes to each network from all the routing tables that they receive. Routers broadcast their routing tables over all their directly connected networks. Routes to distant network will be learned after several iterations of the algorithm. This algorithm was designed and used in the early days of the Arpanet. It is often called the Bellman Ford algorithm, named after its inventors. DV routing protocols can experience some serious problems with routing loops. One of the causes of these loops is the 'counting to infinity' problem. The occurrence of routing loops can be greatly reduced by means of techniques such as maximum hop counts, route poisoning, split horizon, poison reverse, hold-down timers and triggered updates.
- **Link State (LS)** routing algorithms do not involve the regular exchange of routing tables between neighbours. Instead, routers flood the network with the status of their links whenever this status changes and each router maintains an up-to-date topology of the whole internetwork and calculates the shortest paths to each destination network.
- **Balanced hybrid** routing algorithms mix some of the features of DV algorithms with LS algorithms. They hold a limited topology of the network to determine the best paths and check for loops, but exchange the full knowledge of the network between neighbours, but only when the status of links change. They use less processing power and bandwidth than LS algorithms.

Dijkstra's Algorithm

Dijkstra's Algorithm (sometimes also known as the Shortest Path First Algorithm) is one of a number of algorithms that can be used to compute the shortest paths through networks using a metric. It is named after its inventor, the famous Dutch Computer Scientist, Edgar Dijskstra.

[14] Public Packet Switched Data Network – public X.25 network. See Section 4.2.7 of this volume.

Figure 5.3: Example of Dijkstra's Algortithm



We will use Dijkstra's algorithm to compute the shortest path between A and D in the above network using the metrics shown which we will call distance. We start by labelling the nodes with the shortest known distance from A and the previous node on the shortest path from A. Initially, we can only label nodes A, B and F, as these are the only nodes for which we know the shortest distance and path. For all the other nodes, we have yet to compute the shortest distance and path. So we label these with a distance of "α" and show the previous node as "-". Next, we chose the node which is closest to node A which is node B and repeat the same process of labelling all of the nodes directly connected to B with the shortest paths so far found. We can now update the shortest path to node C. It is via node B and it is at a distance of 12 from A. We can therefore update the label for C to (12, B). We do not update the label for F, as the distance via B is longer than the direct distance from A. We then move to the next unvisited node nearest to A, which is F (we can determine this by examining the labels of all the unvisited nodes and choosing the one with the shortest distance) and repeat the process. This time we can calculate a shortest distance for E, which is 14 and we can label node E as (14, F). We then choose the next unvisited node nearest to A, which is C. We can now label node D as (16, B), but we can also re-label node E as (13, C) as there is a shorter route to E via C than the previously calculated shortest route via F. Next we visit node E as of the two unvisited nodes (E and D) it has the shortest distance to A. We recomputed the shortest distances from E and can update the label for D to (15, E). At this point we have visited all the nodes apart from D and the algorithm terminates as we have found the shortest distance to D. We can find the path taken by looking at the label for D and seeing that the shortest path was via E and then that the shortest path to E was via C and the shortest path to C was via B. The shortest path from A to D is therefore ABCED and has distance 15.

Activity 5.2

Read about DV routing in a textbook or a web site and study a simple example of how the algorithm works on a small network.

Activity 5.3

Read about the 'count to infinity' problem that occurs with DV routing protocols in a textbook or on a web site and study an example of the problem. Read about each of the techniques (listed in the DV bullet point above) which are used to minimise the occurrence of routing loops.

5.3.2.3 Single path (or deterministic) versus multi-path (or stochastic) routing

Some routing algorithms will select a single best path to each destination network, others will select more than one best path, which the router can then load share traffic over. Multi-path algorithms help reduce network congestion and cope better with network failures, as traffic can immediately follow an alternative route without a recalculation, if a router detects a failed link.

5.3.2.4 Flat versus hierarchical routing

Some routing protocols operating over small networks will treat all routers as equal and have access to the same routing information. Other larger networks have a hierarchical structure where some routers form a core network where the routers know the routes to all networks. Other routers which are not part of the core, know only some local routes and the route to the core network where most routing decisions are made.

5.3.2.5 Source (or host intelligent) versus hop-by-hop (or router intelligent) routing

With source routing, the intelligence about the network all resides within the hosts, who have to discover the optimum routes using techniques similar to that used in source route bridging. With hop-by-hop routing all the intelligence about the network resides within the routers. The host only needs to know the route to its 'default gateway'. Source routing was used in mainframe based network architectures, such as IBM's SNA.[15]

5.3.2.6 Interior (or intra-domain) versus exterior (or inter-domain) routing

Interior routing takes place within an Autonomous System (AS). The least cost routes are calculated from each router to all the networks within an AS. Exterior routing takes place between ASs. The least cost routes are calculated from routers at the boundary of an AS to networks in different ASs.

5.4 Transport layer gatewaying

It is possible to internetwork at the transport layer by means of a transport gateway. A transport layer gateway may be able to translate between two different connection-oriented transport protocols. This device is sometimes called a transport layer relay. But, we shall reserve the term relay to describe a device that simply forwards PDUs (which would be pretty pointless at the transport layer that normally operates end-to-end) and we shall reserve the term gateway for a device that also has a translation function. Two transport connections can be joined up so that the data from one transport connection is forwarded to the other. As transport protocols normally operate end-to-end, the gateway will have to convince both hosts that they are communicating end-to-end with each other. There is not much demand for transport relays, due mainly to the ubiquity of TCP, but it would be possible, for instance to gateway between a TCP connection and a proprietary protocol's transport connection.

5.5 Application layer relaying and gatewaying

Both application layer relays and gateways are much more common than transport gateways. In fact, a mail server, is a good example of both an application layer relay and a gateway. SMTP[16] messages are received by the mail server and it has to de-capsulate the messages in order to read the mail headers, to decide whether to store the messages, for its own users, or to forward them to other mail servers. If it needs to forward the message, it will do so also using SMTP and acts as a relay. If however, it stores the message, it will be subsequently be retrieved using a completely different protocol

[15] *Systems Network Architecture.*

[16] *Simple Mail Transfer Protocol, see Volume 1, Section 4.6.1.*

(POP3[17] or IMAP[18]) and it will act as a gateway. It is this ability to transmit the application data via different application layer protocols that makes mail servers true gateways.

5.6 The Internet

Having examined internetworking and routing in theory, we are now going to look at how it works in practice on the Internet.

The Internet is a connectionless internetwork with a unique (hierarchical) addressing structure and a single routable internetworking protocol (IP). It does however support a large number of different routing protocols.

5.6.1 Routing protocols

5.6.1.1 Routing Information Protocol (RIP)

RIP was the original interior routing protocol used on the Internet. It is a DV protocol that uses a hop-count metric with a maximum hop-count of 15. It uses route poisoning with a hop-count of 16 to represent an unreachable network. It uses split horizon and hold-down timers to counteract the 'count to infinity' problem and reduce routing loop problems. It uses regular updates that default at 60 seconds to exchange routing tables with immediate neighbours. It does support multi-path routes but only if they have the same cost. RIP1 only supports classful routing, but RIP2 supports Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Masks (VLSM).[19]

5.6.1.2 Interior Gateway Routing Protocol (IGRP)

IGRP is a Cisco proprietary interior DV routing protocol that uses a composite metric that can be configured in a formula. The default formula involves bandwidth and delay. The maximum hop count is 255, so IGRP can be used on a much bigger network than RIP. It uses route poisoning with a value of all 1s to represent an unreachable network. Like RIP, it uses split horizon and hold-down timers to counteract the 'count to infinity' problem and reduce routing loop problems. The default update time is 90 seconds. It supports multiple paths and flexible load balancing. IGRP only supports classful addresses and no VLSM.

Activity 5.4

Read about IGRP in a text book or by searching for web pages that describe it. Find the default formula that is used for calculating the composite metric.

5.6.1.3 Open Shortest Path First (OSPF)

OSPF is a link state interior routing protocol standardised by the IETF. It uses the Shortest Path First (SPF) algorithm (otherwise known as Dijkstra's algorithm). It operates within a hierarchy of areas within an AS. It supports one or more metrics which are configurable. If multiple metrics are configured the router can also take account of the IP Type of Service Field in making its routing decisions. OSPF supports CIDR and VLSM.

5.6.1.4 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary balanced hybrid interior routing protocol. It uses an algorithm called Diffusing Update Algorithm (DUAL) that allows it to check that updates from neighbours are loop-free. It is an enhancement of IGRP and supporting the same metrics and is compatible with IGRP. It uses triggered updates rather than regular updates. It is very robust and efficient.

[17] *Post Office Protocol 3, see Volume 1, Section 4.6.3.*

[18] *Internet Mail Access Protocol, see Volume 1, Section 4.6.4.*

[19] *See Section 6.4.2 of Volume 1.*

5.6.1.5 Intermediate System to Intermediate System (IS-IS)

IS-IS is a Link State interior routing protocol standardised by ISO originally devised to support the OSI Connectionless Network Layer Protocol (CLNP) but can also support IP. It uses a single arbitrary metric and supports a two level routing hierarchy. It supports VLSM and CIDR.

5.6.1.6 Exterior Gateway Protocol (EGP)

EGP is a DV exterior routing protocol standardised by the IETF that relies on a small number of core gateways to distribute routing information from all ASs. It was not scalable and has largely been replaced by BGP.

5.6.1.7 Border Gateway Protocol (BGP)

BGP is a path vector exterior routing protocol (similar to a distance vector protocol, but it chooses the path that traverses the least number of autonomous systems, taking account of policies). Routing information is exchanged with neighbouring ASs. Version 4 supports Classless Internet Domain Routing.

5.6.1.8 Administrative distances

A network, AS or an area can actually run a variety of routing protocols and a single router may obtain different least cost routes to the same destination network from different routing protocols. In order to decide which is the best route, a router takes account of **administrative distances**. Administrative distance is a measure of the trustworthiness of information from routing protocols and is configurable by network managers. Where a router obtains more than one route to the same destination network, it chooses the route received from the routing protocol with the lowest administrative distance. The default administrative distances for the routing protocols we have examined are given in Table 5.3 below.

Table 5.3: Default administrative distances

Route source	Default administrative distance
Direct connection	0
Static route	1
BGP	20
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
EGP	140
RIP	170
Unknown (not trusted or used)	255

Note that a router knows that it is directly connected to a network, by means of the IP address assigned to the port that connects it to the network. A directly connected network that it has learnt about in the way should obviously take precedence over a route that it learns to this network from a routing protocol. Also, a statically configured route will, by default, take precedence over a route learned from a routing protocol. The administrative distance of 255 can be set by a network administrator against any routing protocol, which will then be totally ignored.

5.6.2 Intranets and extranets

Many enterprises have built private networks using the same addressing structure and protocols as are used on the public Internet. These networks are known as intranets. They have built these networks because they want to control access to their computers and do not want to risk using the public Internet. They also do not want to be dependent on the variable quality of service that is offered by the public Internet and they would prefer to run networks which they can manage themselves. They have chosen to use Internet technology, because the technology is relatively cheap and well understood and also because it is a requirement for many of these private internetworks that they interwork with the public Internet. The connection between the intranet and the Internet is usually done via a firewall router which controls access to the intranet from the Internet and vice versa.

Intranets can be implemented using any combination of LANs, MANs or WANs. If the Intranet is all on one site, it can be implemented on LANs (and for a larger site MANs). If the intranet covers more than one site, it must also include a WAN component. This can be built from private circuits, frame relay PVCs[20], ATM[21], SMDS[22] or IP VPN[23] services.

Sometimes an enterprise wants to allow selected customers, suppliers or partners some limited access to their intranet, often from the public Internet, but also via whatever WAN technology is being used by the Intranet. When such access is allowed, it is called an extranet. Access is again controlled via firewall routers and is often limited to a single computer system which will also be protected by some other security mechanism such as usernames and passwords.

Where an intranet is totally separate from the Internet, an enterprise can implement its own private addressing scheme without having to apply for any assigned IP addresses, but if the intranet is connected to the Internet there is a distinct danger, if the enterprise uses its own addressing scheme, that the addresses it uses will clash with IP addresses that have been assigned to another organisation. To avoid this problem the IP addressing authorities have reserved some ranges of IP addresses for intranets that anyone can use without registering them and that will not clash with assigned addresses.

The IP address ranges which can be used for Intranets are given in Table 5.4 below.

Table 5.4: Private IP address ranges

Network	Address range	Number of addresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	2^{24} = 16,777,216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	2^{20} = 1,048,576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	2^{16} = 65,536

Many companies have chosen network 10 for their private intranet addreses, even though they do not need anything like the number of addresses offered in this range. Enterprises can use these private addresses without any problems providing their Intranet does not connect to the Internet, but if it does, then there is a distinct possibility that someone else is using the same addresses and also the Internet routing protocols do not advertise any routes to these networks. In order to connect a private intranet with the Internet, a means of mapping public IP addresses to private IP addresses is required. This function is called **Network Address Translation** (**NAT**) and is usually performed by the enterprise's firewall router that supports the connection to the Internet. The NAT device has to maintain a table of mappings between private and public IP addresses.

[20] *Permanent Virtual Circuits.*

[21] *Asynchronous Transfer Mode, see Section 6.5 in this volume.*

[22] *Switched Multi-megabit Data Service, see Section 4.1.1 in this volume.*

[23] *IP Virtual Private Network, see Section 5.6.3 in this chapter.*

The enterprise obtains a single IP address (or a small number of addresses) and it is to these addresses that the DNS[24] maps the enterprise's registered domain names to. All datagrams delivered to this address arrive at the firewall router where the destination address is translated into a private address with which the datagram is routed over the intranet. In the opposite direction, an intranet user can send a datagram to the Internet which will be routed over the Intranet to the firewall router. This time, NAT will translate the private source address into a public IP address. The translation can either be static (using a pre-configured table) or dynamic (building the table by taking the next available address). If the enterprise has only subscribed to a small number of IP addresses and there are many users accessing the Internet at one time, then an enhancement to this scheme is necessary. The translation of the source address is made to both a public IP address and a unique port number. When a datagram is received from the Internet, NAT looks up the port number in its tables and maps it to the correct private IP address. This system allows a single IP address to be used by up to 65,536 internal private addresses. NAT therefore greatly reduces the demands on IP address space from enterprise intranets. It does however have many critics. Tanenbaum[25] gives six objections to NAT. Of these the most serious are that:

- It violates the principle that every device on the Internet should have a unique network address.
- It effectively turns connectionless networking into connection-oriented networking. If the NAT system crashes the loss of the translations will mean that all TCP connections will need to be re-established.
- It violates the principles of protocol layering. The network layer is dependent on fields in the transport layer (port numbers) to carry out its function. If the format of TCP or UDP changes then the network layer will no longer work, unless it is also changed.

Not all enterprises use NAT. Some have been allocated a sufficient number of IP addresses for all their needs, but use of NAT does conserve IP address space and also has some security advantages. The private network addresses being used are totally invisible to the outside world, and access from the Internet to a small number of public addresses can be closely controlled.

5.6.3 IP Virtual Private Networks (IP VPNs)

IP VPNs are becoming increasingly popular with enterprises. IP VPNs allow enterprises to implement their wide area intranets over the public Internet instead of having to buy WAN services from network operators. The IP VPN is overlaid on the public Internet and provides secure network access to a closed user group. The IP VPN is used to transmit PDUs between firewall routers (which act as IP VPN gateways) using IP tunnels. The whole PDU which can either be a layer 2 frame, such as an Ethernet frame, or a layer 3 packet, such as an IP datagram, is encapsulated within an IP datagram with the destination address of a remote firewall router. By this means all of the data and protocol header information of the original frame or packet can be de-capsulated at the firewall router and forwarded at the data link layer or network layer depending on the type of PDU that was encapsulated. The original PDUs (including the protocol headers) are normally encrypted before encapsulation. By this means both the privacy and integrity of the PDUs can be assured as they are carried across the Internet. A further protocol overhead is required to support this. For layer 2 frames, the **Point-to-Point Tunnelling Protocol** (**PPTP**) or the **Layer 2 Tunnelling Protocol** (**L2TP**) can be used. These protocols are often used for access VPNs, as they are quite simple to implement. PPTP uses the same authentication schemes

[24] *Domain Name System, see Volume 1, Section 4.8.1.*

[25] *Tanenbaum, p.448.*

as PPP and does not provide strong encryption. L2TP addresses these shortcomings and is more secure. For Layer 3 VPNs, IPSec is normally used either in tunnel mode or in transport mode.

There are three main types of IP VPN. There are **Intranet VPNs** that just support the enterprise's intranet, **extranet VPNs** that support the enterprise's extranet, and **Access VPNs** that support remote access from any location to the Intranet or Extranet. Intranet VPNs tend to be provided by the same supplier (ISP or network operator), which means that it is possible to guarantee quality of service, if it is supported, and security is more easily managed. Extranet and, to a lesser extent, Access VPNs often make use of different IP suppliers and cannot support any guaranteed quality of service and security is more of an issue.

IP VPNs are considerably cheaper to implement than intranets build with WAN services bought from network operators, and it is very easy to extend the Intranet to a new site or to extend it to extranet sites. All that is required is an Internet connection. With VPN software installed on laptop computers, the corporate intranet can be extended to any location where an employee can access the Internet, using dial-up modems, ISDN, broadband connections or WiFi hotspots.

With VPNs, all the security concerns that have made enterprises reluctant to use the public Internet for their own inter-office traffic have been removed, but there is one serious disadvantage that still prevents some enterprises from using VPNs. This relates to the lack of control that enterprises have over the service offered by VPNs. When using WAN services to carry Intranet traffic, the enterprise can obtain a guaranteed quality of service and can decide when and where capacity needs to be upgraded, or when congestion occurs, it can determine which traffic is going to be given priority. This level of control is impossible to achieve when using the public Internet and enterprises have to accept that their quality of service may be affected by other users who are totally outside of their control.

Activity 5.5

Visit the web sites of some of the network operators who offer telecommunications services in your country and check what products they offer to support IP VPNs. Check whether they have flat or volume related prices and whether the prices are distance dependent.

5.6.4 Multicasting

Most routers on the Internet currently only support unicast routing. In order to support multicast routing, an overlay network of special multicast routers, called the MBone (Multicast Backbone) has been built. Multicast routers deliver multicast datagrams over the Internet using paths through tunnels between multicast routers. They exchange multicast routing information with each other using multicast routing protocols.

Hosts can join or leave multicast groups by means of the Internet Group Management Protocol[26] with which their local multicast router communicates with them. The original multicast groups would accept multicasts from any source. This is known as Any-Source Multicasting (ASM), and new version of multicasting has since been proposed called Source-Specific Multicasting (SSM) where a member of a multicast group can specify the source from which it wishes to receive multicast data.

[26] *See Section 6.6 of Volume 1.*

For each multicast group, the multicast routers co-operate with each other by using multicast routing protocols to create a spanning tree from the data source via intermediate multicast routers to the multicast routers on LANs which have hosts belonging to the group.

Many multicast routing protocols use a technique known as **Reverse Path Forwarding** or **Flooding** (**RPF**). At each multicast router, when a datagram is received, the multicast router determines the source network and checks that the datagram was received from the port that its normal routing table would forward datagrams to that network. If it wasn't, it assumes that the datagram was received on a non-optimum path and discards it. Otherwise, it assumes that this datagram has been received via an optimum path and it copies the datagram and forwards it via all its tunnels apart from the one on which the datagram was received. The spanning tree is pruned to remove paths to multicast routers that do not lead to any multicast group members. This results in the creation of a spanning tree rooted at the data source to each network that contains members of the multicast group.

In addition to limiting flooding by RPF, multicast routers can limit the life of multicast datagrams by imposing a threshold on each tunnel for the datagram's TTL[27] field and not allow it to enter the tunnel, unless the TTL is greater than this threshold.

There are three main multicast routing protocols in use. These are:

- Distance Vector Multicast Routing Protocol (DVMRP) which is an interior multicast routing protocol using RPF based on the RIP DV unicast routing protocol. Multicast routers participating in DVMRP must also run a unicast routing protocol as a separate process. DVMRP is encapsulated within IGMP.
- Multicast Extension to Open Shortest Path First (MOSPF) which is an interior multicast routing that is an extension to the OSPF link state unicast routing protocol and uses the SPF algorithm to create the spanning tree rather than RPF.
- Protocol Independent Multicasting (PIM). It is independent of routing protocols and is used between ASs and uses RPF. It has two modes: dense mode which uses pruning for densely populated receivers and sparse mode where all parties set up their paths via an intermediate rendezvous point.

Multicasting provides an efficient mechanism for broadcasting over the Internet, but it has not been used very much commercially. This is partly because it has not really made the transition from academic implementations to the ISPs. Very few ISPs have implemented multiprotocol routers and as a result even fewer enterprises have implemented them on their LANs. Until a very large overlay network of multiprotocol routers exists or the protocols are supported on normal routers, it is unlikely to reach a mass market.

Activity 5.6

Check the web sites of the main ISPs in your country and search for the terms multicast or multicasting, to see if they support it. You can also try some TV broadcasters web sites and Internet radio stations as well.

[27] *Time To Live.*

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. With source route bridging, the hosts must ascertain the topology of the network before they can transmit data.

ii. Distance Vector routing protocols flood the network with the status of their links whenever this status changes.

iii. The PSTN uses dynamic routing over a highly meshed core network.

iv. With Network Address Translation, it is possible for a whole large organisation to use a single IP address.

(b) List five differences between network technologies that may cause difficulties when connecting them in an internetwork.

(c) Describe five differences between transparent and source route bridging.

(d) Outline the main features of the RIP routing protocol

(e) Describe how tunnelling can be used to carry an Intranet over an IP VPN.

Learning outcomes

At the end of this chapter, you should be able to:

- describe the main differences between network technologies that may cause difficulties when connecting them in an internetwork
- describe why bridges are used and distinguish between transparent bridges, source route bridges, translational and remote bridges
- calculate which ports must be blocked in a network of bridges or switches to form a spanning tree using the Spanning Tree Protocol
- outline how a router routes datagrams
- describe the requirements of and the terms used to classify routing protocols
- distinguish between relays and gateways
- calculate the shortest path through a network using Dijkstra's algorithm
- classify the main routing protocols used on the Internet
- distinguish between internets, intranets and extranets and describe how the latter two can be implemented over the Internet using IP VPNs
- outline how Network Address Translation works
- outline how multicasting and multicast routing works.

Notes

Chapter 6: Network integration (multimedia)

Further reading

Forouzan, Behrouz, A. *Data Communications and Networking.* (McGraw Hill), third edition, 2003. Chapters 18.3, 23, 28.

Kurose and Ross *Computer Networking – A Top Down Approach featuring the Internet.* (Addison Wesley), third edition, 2005. Chapters 5.8, 7.

Stallings, William *Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003. Chapters 11, 19.3, 19.4.

Tanenbaum, Andrew S. *Computer Networks.* (Prentice Hall International), fourth edition, 2002. Chapters 5.4, 7.4.

In the last chapter, we considered how different technologies could be connected together to form a single internetwork. In this chapter, we will consider how a single network or internetwork can support the different requirements of multimedia applications. Historically, different technologies, have been designed with different applications in mind. Some have been designed to support the exacting real-time requirements of voice and video, while others have been designed to support the less demanding timing requirements but more exacting data loss requirements of data communications. If both of these technologies used totally separate infrastructures, there would be a huge duplication of infrastructure which would be inefficient. Cost savings are therefore an important driver for this type of network integration.

We will firstly consider the different classes of multimedia applications and then some techniques, such as compression and streaming, that are used by the application layer to make the handling of real-time multimedia data less problematic. We will then consider TDM[1] networks as a means of sharing common infrastructure between real-time circuit switched networks that support voice and video communications and non real-time packet switched data networks. We will also consider how the protocols used on the Internet, which were not designed to handle real-time applications, can be adapted to do so and also how the ATM[2] protocols have been designed with this purpose in mind.

6.1 Multimedia applications

Multimedia networking literally means networking that supports two or more different types of media. Media in this context is the content of the communication rather than the channel through which the content is communicated. The content can be text, graphics, animation, audio or video or an integrated mixture of any of these media. Multimedia also often implies some degree of continuity in the content, so that it is 'played'. The content can be stored and played on demand, or it may be live content, as would occur in a live broadcast. A degree of interaction is also implied, that at the very least results from a request to play or stop the content. If the media is stored then there could also be other interactions to pause, stop, rewind or fast forward the content. There may also be a much more interactive approach, as would be the case with on-line learning or gaming. Multimedia can also include the support of person to person communications with audio (voice communication) or a combination of video and audio (video conferencing).

[1] *Time Division Multiplexer.*

[2] *Asynchronous Transfer Mode.*

There are three separate classes of multimedia applications which we will consider:

- streaming live multimedia
- streaming stored multimedia
- real-time interactive multimedia.

The main characteristics of all of these classes of multimedia networking are that they are delay sensitive. Delays, in the case of real-time interactive multimedia, and variation in delays (jitter) in all of the classes, can affect the continuity of the content and, unless steps are taken to deal with it, will detract from the appreciation of the content. Each of the classes will also require a minimum throughput and failure to provide this will produce delays that affect continuity. All of the multimedia content that we are considering will require the transmission of large amounts of data and the occasional loss of data packets will often have little overall effect on the appreciation of the content. With multimedia networking, the timeliness of the delivery is frequently more important that the quality of the information delivered. This is the exact reverse of normal data communications where the quality of the content takes precedence over the timeliness of its delivery. With multimedia networking, if there is any error detection, there will be no requirement for any retransmissions. It will be preferable to discard a packet than wait for it to be retransmitted. More often than not, therefore, multimedia content will not be protected with error detection codes, or where it is they will use forward error correction codes to allow for recovery without retransmission.

6.1.1 Streaming live multimedia

Live multimedia is a broadcast application where many receivers are receiving data from a single source. It includes applications such as Internet radio, where an Internet radio station (which may or may not also be broadcasting over radio) feeds an audio signal to many receivers over the Internet and the live broadcasting in audio or video of events such as concerts, sports matches and lectures over the Internet. It is an ideal application for multicasting, as there are potentially many receivers in different locations all receiving the same information at the same time. Delays are not particularly important. It doesn't really matter if the content is received a few hundred milliseconds, seconds or even tens of seconds after it is transmitted. Jitter can be overcome by means of streaming,[3] but there will be a problem if the delay is very variable and the playback buffer is emptied. If this happens will then be a discontinuity in the video/audio stream. Unlike stored multimedia, there can be no fast forward function, although there could be a pause and rewind function, if the transmission is unicast. This type of streaming is supported on the Internet with the Real Time Streaming Protocol (RTSP).

6.1.2 Streaming stored multimedia

Stored multimedia requires similar software to live multimedia. The main difference is that multicasting cannot be used, as each receiver is receiving the streamed multimedia on demand. The use of unicasting does mean that the player has control of what is being played and all of the play functions available on a Video Cassette Recorder (VCR) can be supported. The user can rewind, pause, freeze or fast forward the audio/video stream at any point. Also, the use of stored multimedia means that users can be offered an almost unlimited choice of content to play and they are not restricted to the programming offered by a limited number of live channels. This type of

[3] See Section 6.2.2 of this chapter.

service where video is involved is often called **Video on Demand** (**VoD**). It also is supported on the Internet using the Real Time Streaming Protocol RTSP. There are also service providers who support VoD using ATM connections over ADSL which eliminates many of the problems encountered when transmitting real-time data over the Internet. It is generally acceptable for users to wait for up to 10 seconds initially for their selected programme to start playing and to wait up to two seconds for any control to be actioned.

6.1.3 Real-time interactive multimedia

Real-time interactive multimedia includes person-to-person communications such as Voice over IP (VoIP), Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) and video conferencing over IP, Frame Relay or ATM, as well as virtual reality and gaming applications.

Real-time interactive multimedia networking is much more demanding to implement than streaming. This is because variations in delay are less easy to smooth out using playback buffers as introducing extra delay could be noticeable and detract from the interactivity being sought.

It is generally accepted that delays of up to 150 ms are good and that in many applications, delays of up to 400 ms are acceptable. Delays greater than this do affect the user's perception of interactivity and impair it.

Whilst techniques do exist for managing jitter on VoIP services over the Internet, in general many interactive applications will require some reservation of resources so that quality of service can be guarantied.

6.2 Multimedia application layer techniques

There are a number of techniques that are used in multimedia networking, in order reduce to make it easier for networks to support real-time multimedia data.

6.2.1 Compression

Multimedia, particularly video and to a lesser extent audio, can consume a large amount of bandwidth. A broadcast analogue TV channel, depending on the standard, requires about 5MHz of bandwidth. If the analogue signal is digitised, this will convert to over 200 Mbit/s. But there will be a large amount of redundant information transmitted. Broadcast TV works by transmitting 50 or 60 still frames per second that gives an illusion of continuity to the human eye, but in many cases large parts of the frame are identical at each frame transmission. Clearly a large amount of bandwidth could be saved if only the changes between each frame were coded and transmitted, rather than the whole frame each time. The same is true of the frame itself. If it is coded as a bit map, there will be whole regions of the image that have the same colour and intensity. There are ways that the information in a still image can be coded much more efficiently than in a bit map. Similarly with voice communication, the PSTN standard is to code voice using PCM[4] at 64 kbit/s and transmit this over a circuit switched network. Sound waves are sampled 8000 times a second, and the amplitude is coded into one of 8 levels, but consecutive samples are often the same amplitude and in a typical two way conversation, for many samples there is no amplitude, due to one party listening rather than speaking and normal gaps in speech. Again, there is considerable scope for compressing the signal and using much less bandwidth. Finally, even text can be coded more efficiently.

[4] *Pulse Code Modulation. See Volume 1, Section 8.3.6.2.*

6.2.1.1 Text compression

Text compression is possible because some patterns of letters occur more frequently than others, but with standard ASCII code they all require 7 bits each. Techniques such as Huffman coding[5] and can be used to compress text, based on the frequency distribution of individual letters. Also there are some characters such as spaces and tabs that often occur in long runs. These can be coded by counting the number of occurrences and coding this number. This is called **run length encoding**. Also, some combinations of letters frequently occur together (e.g. Q and U or T and H in English) and codes can be devised that take account of common combinations of letters. Some algorithms such as the Lempel Ziv Welch (LZW) algorithm build up a dictionary of words and phrases used in the text and use pointers to signify where they occur.

6.2.1.2 Audio compression

The standard method used for voice digitisation is PCM which converts a limited analogue frequency range of 3400 Hz sampled at 8 kHz into a 64 kbit/s digital data stream. Various compression techniques can be used to reduce this data rate. **Adaptive Differential Pulse Code Modulation** (**ADPCM**), which measures the differences between samples rather than the samples themselves, can reduce the data rate to 16 kbit/s. GSM uses a complex compression algorithm to code voice at 13 kbit/s with little noticeable reduction in voice quality. More advanced techniques can reduce the data rate required for voice communication to as low as 5.3 kbit/s. Voice over IP (VoIP) uses such techniques and usually compress voice to data rates between 5.3 and 13 kbit/s.

While these techniques are suitable for voice communications, they cannot be used to reproduce music which needs a much larger frequency range to be coded than is necessary for voice. The standard method for digitising music, as is used on CDs, is to sample the sound waves 44,100 times per second to produce a 1.411 Mbit/s digital data stream. This is somewhat high for wide area communications and various techniques can be used to compress it without an appreciable loss of quality. One of the most common techniques is known as MPEG[6] 1 Level 3 (or MP3) which is used to compress music tracks for download via the Internet. MP3 can compress music to 96, 128 or 160 kbit/s.

6.2.1.3 Image compression

The data required to digitise and image will depend on the resolution and the number of colours represented. Bitmapped digital photographs typically require about 1 Mbyte of data. The transmission of such images over the Internet, as is done by most web sites, would be very slow if bitmaps were transmitted. Instead, a number of different compression algorithms to improve transmission times. Some of these lose information and the quality of the image received when it is decompressed is noticeably worse than the original. This type of algorithm is know as a **lossy** algorithm. With other algorithms the decompressed image has not lost information and the quality is as good as the original. This type of algorithm is known as a **lossless** algorithm.

The **Joint Photographic Expert Group** (**JPEG**) have defined a lossy compression algorithm known by this name that supports 16 million colours. It works by splitting the image into blocks of 8x8 picture elements (pixels) and performing a discrete cosine transform on each block before the quantisation process. It uses both run length encoding to compress runs of 0s and Huffman Coding to compress the quantisation values based on their

[5] See Section 4.3.10 of Volume 1.

[6] Motion Picture Expert Group

frequency distribution. Huffman coding is actually an option. The alternative is arithmetic coding which is patented. JPEG is best used for compressing colour photographs.

The **Graphics Interchange Format** (**GIF**) is a proprietary standard, originally invented for CompuServe but it uses the Lempel Ziv Welch (LZW) algorithm which Unisys patented and when they discovered it was used in GIF, they attempted to claim royalties. The patent expired in 2003. GIF supports 256 colours is lossless and also supports animation. It is best used for line drawing graphics requiring limited colours and can produce highly compressed images that can be decompressed without any loss of quality.

Portable Network Graphics (**PNG**) is an open lossless standard, slightly superior to GIF, but there is no support for animation. The standard was developed at a time when Unisys were claiming royalties from software that produced GIF.

6.2.1.4 Video compression

Uncompressed broadcast analogue TV when digitised will require data rates of over 200 Mbit/s. Even VCR[7] quality analogue video will require about 50 Mbit/s. Data rates such as these are totally impractical for most networks. Fortunately, video is highly compressible, for the reasons given at the start of this section. A set of standards has been produced by the Motion Picture Expert Group (MPEG). All the standards use complex algorithms involving Discrete Cosine Transformations and wavelets. MPEG 1 was designed for use on CD ROMs[8] and compresses video to 1.5 Mbit/s. MPEG 2 is used for digital television and DVDs[9] and compresses video to data rates usually between 3 and 6 Mbit/s. MPEG 3 was intended for high definition TV, but has been incorporated into MPEG 2 which can go up to 15 Mbit/s. MPEG 4 was originally intended for video conferencing, but is now commonly used for streaming video over the Internet. It can compress video to any rate from 28.8 kbit/s up to 1 Mbit/s.

6.2.2 Streaming

Streaming is a technique that can even out the jitter on a received data stream that represents an audio or video signal. It does this by buffering a quantity of data at the receiver and playing out the signal at a constant rate from this buffer which is known as the playback buffer. The player therefore does not start to play out immediately, but it does start to play out before all the data has been received. There is a timing constraint, in that data which has yet to be played must arrive before the playback buffer is emptied by the player. Jitter can be effectively eliminated at the expense of inserting extra delay, as the data is buffered. Streaming is a very useful technique provided there is no high degree of interactivity required as there would be for video conferencing.

Streamed multimedia is usually played via media player plug-in (or helper) applications that are executed by clicking on a URL[10] on web page in a browser window. The file type of the multimedia file selected will cause the appropriate plug-in to execute The browser does not usually request the multimedia file as a HTTP[11] object and then pass it to the media player, as it would then be transferred using HTTP which has to use TCP as its transport layer. Instead the browser requests an object known as a metafile which it passes to the plug-in and the media player requests the multimedia file using its own protocol, such as **Real Time Streaming Protocol** (**RTSP**) which usually runs over UDP which has more constant delays than TCP. There are other proprietary streaming protocols that can be used such as Progressive

[7] Video Cassette Recorder

[8] Compact Disk Read Only Memory.

[9] Digital Versatile Disk

[10] Uniform Resource Locator, see Volume 1, Section 4.5.

[11] Hyper-Text Transfer Protocol, see Volume 1, Section 4.5.

Network Audio (PNA) / Progressive Networks Media (PNM) from RealNetworks and Microsoft Media Server (MMS). Multimedia content can also be streamed via HTTP, but the use of TCP will affect the quality. The use of HTTP will however ensure that the content will get through firewalls.

The media player must buffer the data it receives to remove jitter, decompress the data and conceal any errors caused by lost or discarded packets. It must then control the play-out of the data and respond to any controls issued by the user.

Examples of such plug-ins are RealPlayer and Windows Media Player in the Microsoft Windows environment and QuickTime in the Apple Macintosh environment. These plug-in applications usually appear in a window that looks something like a TV set with buttons similar to those on a VCR remote control. The play position within the video/audio stream can also usually be controlled by a slide bar in addition to the buttons.

Activity 6.1

Find one or more of the media players listed above on your PC (or download one if you cannot find one) and read the some of the documentation in the help facility or the configuration facility. Find out which protocols and file types are supported and whether multicasting is also supported. Use the media player it to play some audio and video material from sites, such as www.bbc.co.uk over a limited bandwidth access link, such as dial-up. Observe whether there is any jerkiness in the playback, whether the frames occasionally freeze, whether the resolution is sometimes grainy and whether the audio sometimes sounds harsh or unclear. Observe also how the video player handles fast motion. A football game or other team sport is a good test of this.

6.2.3 Adaptive play-out delay

For real-time interactive services such as voice, which are intrinsically bursty, due to gaps in speech, it is possible to cope with a certain amount of jitter by means of adaptive play-out delay. With a fixed play-out delay, as used in streaming there is a trade-off between the length of the delay and the rate of packet loss. If the play-out delay is large virtually all the packets will arrive in time for play-out. If the play-out delay is small, then some packets will arrive too late for playback and the receiver must discard them. With fixed play-out delay for real-time interactive services, the delay must be small, or it will detract from the interactivity and so a large number of packets could be lost. Adaptive play-out delay makes use of the gaps in the speech to dynamically adapt the play-out delay.

This technique works by the receiver predicting, at the start of each speech burst, the likely delay and variance, and adjusting the play-out delay accordingly. This will mean that the gaps in speech at the transmitter will be lengthened or shortened as necessary, and this will not be noticeable at the receiver.

6.2.4 Loss recovery

Although occasional packet loss is not a major problem to many multimedia applications, if it becomes severe, quality will quickly deteriorate. There are several techniques that applications can use to minimise packet losses described in Kurose and Ross.[12]

These techniques include:

- The use of FEC[13] or by sending a low bit-rate stream just after a full bit-rate stream. For example a 64 kbit/s PCM[14] stream could be packetised and each packet appended with the contents of the previous PCM packet

[12] *Kurose and Ross, pp. 590–594.*

[13] *Forward Error Correction, see Volume 1, Section 7.3.6.2.*

[14] *Pulse Code Modulation. See Volume 1, Section 8.3.6.2.*

but coded at 5.3 kbit/s. If a packet is lost then it can be replaced by the 5.3 kbit/s version in the next packet and played out at lower quality. This lowering of quality for a single packet would not be noticeable.

- Interleaving can be used to re-sequence groups of bits before transmission in packets, so that groups adjacent bits in the original stream are sent in different packets. A loss of a single packet will therefore not result in a loss of a stream of adjacent bits from the original stream which may be noticeable, but will cause smaller bit losses in different places in the stream which will not be noticeable. This technique will increase the overall delay and is not suitable for interactive applications, but can be useful for streaming applications.
- Receiver based repair schemes attempt to replace lost packets by similar packets. Human speech contains a good deal of self-similarity and replacing one packet by a packet similar to the preceding and following packet is unlikely to be noticeable. This technique works well for speech for small loss rates and small packets.

6.3 TDM[15] Networks

We have already examined this type of network integration, when we considered the PDH and SDH technologies employed by network operators in their transmission networks. The network operators realised that both PSTN and private circuits and later data networks could all be carried on a single transmission network and by doing so they could make large cost savings, in terms of designing, efficiently using and managing this single integrated network. Imagine how inefficient and expensive it would have been if the network operators had built totally separate networks for the PSTN, private circuits and data. As a result of building transmission networks, virtually all telecommunications services, at least in part, will at some point be carried over a single integrated network infrastructure.

Enterprises can also make cost savings and improve the efficiency of their private network by carrying out network integration at the physical layer. Enterprises had, for many years, been using analogue private circuits between their offices to carry voice traffic. It is highly cost effective and cheaper than PSTN charges, even if the private circuit is only fully occupied for a small part of the day. When the private circuit is well utilised the savings are huge.

When private circuits were digitised, enterprises who were also upgrading their PABXs to digital started to use E1 (or T1) circuits to carry 30 (or 23) 64 kbit/s voice channels using Pulse Code Modulation. Using private circuits instead of the PSTN made even more economic sense. At the same time, enterprise also had a requirement for transmitting data between their offices and private data networks were being built to support remote job entry batch processing systems, as well as some on-line systems. These tended to be fairly low speed (1200 bit/s up to 48 kbit/s), as modem technology was not advanced. It soon became obvious that these data services could also be carried on the same private networks that were being used for voice, by using some of the 64 kbit/s channels. As the use of on-line data networks grew, so did the requirements for bandwidth and soon whole E1/T1 circuits were being occupied by data services, of various speeds. Enterprises now often had several E1/T1 circuits between offices used for voice, as well as a smaller number used for data. It did not require many such circuits before it became economic to multiplex them onto a higher speed private circuit (E2/T2 or E3/T3).

[15] *Time Division Multiplexer, see Volume 1, Section 2.3.1.*

They did this by building their own multiplexer-based mesh networks using private circuits and Time Division Multiplexers (sometimes called Bandwidth Managers) bought from network equipment manufacturers. These manufacturers, included Timeplex, Network Equipment Technologies, Newbridge Networks (acquired by Alcatel) and Racal Datacom (acquired along with Timeplex by NextiraOne, which is no longer a manufacturer). The multiplexers can support a large variety of interfaces and protocols. The multiplexers usually came with proprietary but powerful network management systems that allowed network managers to configure the multiplexers remotely, route fixed bandwidth channels across the network, diagnose faults and view the status and performance of the circuits, multiplexers and even, in some cases, individual interfaces using a graphical interface. The frame structures supported often had slight proprietary variations which, together with the proprietary management system, meant that it was impossible to build a multi-vendor network and customers were thus often locked-in to a single multiplexer supplier.

As voice compression techniques improved, these multiplexers began to support voice services over low speed channels (sometimes as low as 8 kbit/s) which further improved the economics of this type of network solution at the cost of a slight degradation in voice transmission quality.

Customer owned TDM networks provide savings in costs over building separate private networks for voice and data, but they do require a considerable resource commitment to design and manage them, particularly if they are international networks, where liaison with many network operators is required. These activities can be outsourced, but today, it is often cheaper (particularly for smaller enterprises) to buy managed services from network operators, such as their ATM and managed bandwidth services to provide this type of network integration.

6.4 The Internet

IP was designed to support normal data communications, although IP itself, as a connectionless protocol, has no support for error detection and retransmission. IP does not offer any guaranteed quality of service in terms of packet loss, throughput, delay or jitter. The lack of a guarantee regarding packet loss will not be a problem for many multimedia applications (as long as the losses are not excessive). Poor throughput, long delays and jitter will cause problems for multimedia applications. Most such applications will require a minimum throughput, a maximum delay with little variation and if these are not delivered, they will not work satisfactorily.

Because IP was not designed with multimedia in mind, much effort has gone into the application, transport and network layers to attempt to overcome the deficiencies of IP and support multimedia applications. This requires methods to reserve resources along the route that packets take and implies the need for a connection-oriented approach.

6.4.1 Real-time Transport Protocol (RTP)[16]

RTP is a simple transport protocol designed for use by real-time applications and has been standardised by both the IETF and the ITU-T. It normally runs on top of UDP but can in theory also run on top of TCP, but this would not make a lot of sense. Its main functions are to identify the payload it is carrying and to provide sequence numbering and timestamps. RTP does not guarantee the timely delivery of data or any other quality of service. Because it resides at the transport layer, routers are totally unaware that IP packets contain RTP data and cannot therefore give it any special treatment. RTP

[16] *RFC 1889 and ITU-T H.225.0*

does support multicasting. It has its own control protocol called Real-time Transport Control Protocol (RTCP) that works in conjunction with RTP and allows different streams such as audio and video to be synchronised. This is particularly important for video conferencing over the Internet. Without RTCP different delays in the audio and video streams could create a 'lip-sync' problem where the audio was out of step with the video. All participants in an RTP session exchange RTCP packets which are used to transmit statistics on packets sent, packets lost, jitter etc. which are used to control performance. RTCP attempts to limit its traffic to five per cent of the bandwidth available for RTP.

RTP is used by many different multimedia applications including RTSP and H.323 (the ITU-T's conferencing framework for audio and video conferencing). Table 6.1 below gives examples of some of the payload types supported by RTP.

Table 6.1: RTP payload types

Payload Type	Format
0	PCM μ-law audio (64 kbit/s)
3	GSM audio (13 kbit/s)
7	Linear Predictive Code audio (2.4 kbit/s)
26	Motion JPEG video
31	H.261 video
32	MPEG 1 video
33	MPEG 2 video

6.4.2 Real Time Streaming Protocol (RTSP)[17]

RTSP is a real-time client/server application protocol that usually sits above RTP and allows users to control multimedia presentations being received. It supports all the standard VCR play-out functions, such as play, pause, rewind and fast forward. It is used instead of HTTP by media players for fetching multimedia objects. The main reasons for not using HTTP is so that the media player does not have to wait until the whole file is received before it is played and that it is not transferred using TCP. TCP provides error recovery that is not required and can suffer from very variable delays and does not support multicasting. For these reasons a new application layer protocol was needed for transferring multimedia files.

RTSP does not actually specify how it is to be encapsulated, although it is usually encapsulated within RTP and UDP. Neither does it specify how the media player should buffer data.

6.4.3 H.323

H.323 is an ITU-T standard for the transmission of multiparty video conferences over packet based networks. It can be also be used to transmit audio (VoIP). H.323 really provides an architectural framework that references a suite of other standards for signalling, coding (multiple compression algorithms supported) and data transport. The end systems use a protocol called H.245 to negotiate the compression algorithm and the ISDN signalling protocol Q.931 is used for call signalling.

[17] *RFC 2326*

H.323 supports interconnection with the PSTN via a gateway and end systems in a zone can be controlled by a gatekeeper. H.323 uses E.164 telephone number addresses. The signalling and call control information are carried by TCP, while the multimedia content is carried by RTP and UDP. RTCP is also used and also carried by UDP.

H.323 can also interwork with T.120 to share access to application data, in conjunction with voice or video conferences.

6.4.4 Session Initiation Protocol (SIP)[18]

SIP is an IETF application layer standard that is used by a number of multimedia applications to establish and control sessions for audio, video and data multiparty conferencing (including games). It is a text-based protocol, similar to HTTP. SIP is becoming popular for VoIP, as it is so much simpler than H.323, has faster call set-up times and scales well.

SIP addresses are Uniform Resource Identifiers (URIs) which are similar to email addresses and are prefixed by sip: instead of mailto: and consist of a username, an @ sign, followed by a domain name, IP address or E.164 telephone number. SIP will map any mnemonic addresses to the appropriate IP or E.164 address using the DNS and vice versa.

SIP will set up a call, allow all parties to agree on the type of media and encoding to be used, will manage the call and terminate it afterwards. SIP can run over either TCP or UDP. Once a session is established, multimedia content is transferred using RTP over UDP.

Activity 6.2

Search the web for references to VoIP and read more about how it works. You may wish to experiment with it, using some free downloadable products or by using voice services supported by instant messaging applications, such as Microsoft's MSN Messenger, AOL Instant Messenger and Yahoo! Messenger.

6.4.5 Integrated Services (IntServ)[19]

IntServ is a flow-based quality of service mechanism that supports both unicast and multicast flows. Applications can specify the quality of service they require by means of a flow specification which the application layer can negotiate with the receiving application layers and the IP network layer. The flow specification can include parameters such as the token bucket rate (Bytes/s), the token bucket size (Bytes), the peak data rate (Bytes/s), and the minimum and maximum packet sizes (Bytes). If any party cannot meet the requirements of the flow specification or accept a lesser specification, then the flow must be rejected. If a flow specification has been accepted by all parties, then they are all committing to operate within the parameters specified. This means that sufficient resources (router memory, processing power and bandwidth) must be reserved to support the flow.

Resources are reserved using the **Resource Reservation Protocol** (**RSVP**). Because it has been designed to support multicasting to many receivers which could be in any location and some may not want to receive the multicast, the reservations are actually made by the receivers rather than the transmitter. The receivers learn the path to the transmitter from a PATH multicast message, which is sent at regular intervals from the transmitter. This establishes the path to each receiver and sets up some soft (periodically refreshed) state information in all the routers through which it passes. This state information is known as path state and it is used to record the address of the previous router on the path from the transmitter and other fields from the PATH message.

[18] *RFC 3261.*

[19] *RFCs 1633, 2212, 2215.*

When a receiver receives the PATH multicast message, it decides whether or not to participate in the multicast. If it decides to participate, it sends a RESV message back along to the path to the transmitter. At each stage on this path the routers will reserve the necessary resources for the transmission and will pass the RESV message on to the next router whose address was recorded in the path state.

If any router cannot commit the resources required to meet the flow specification, then an RESV-ERR message is returned to the host reserving the resources. This is RSVP's admission control mechanism that is used to ensure that performance can be guaranteed for all accepted flow specifications who must prioritise and schedule packets to meet the specification.

At any point the path can be torn down and all the reserved resources released by means of a PATH-TEAR or RESV-TEAR message.

The work on IntServ uncovered a number of concerns with regard to its scalability and flexibility. As a result, IntServ has not been implemented in ISP networks, but some of the ideas behind it and the RSVP protocol are used in MPLS[20] networks which many ISPs have implemented.

6.4.6 Differentiated Services (DiffServ)[21]

The IETF made a further attempt to support **QoS**[22] over the Internet with DiffServ standard. It makes use of a concept and an IP header field that was in the original IPv4 specification, but had rarely been used. This was the Type of Service field that contained three precedence bits to indicated whether minimum delay, maximum throughput or reliability were desired. This field was redefined as the Differential Services (DS) field. The scheme has also been taken up in the IPv6 standard as the Traffic Class field. The basic idea behind DiffServ is that all packets are classified according to their QoS requirements and this is coded in the IP header and used by routers in deciding the scheduling and discarding of packets awaiting transmission. With DiffServ, unlike IntServ, each packet is therefore handled independently and there is no need for state information to be held in the routers.

The traffic is classified at the edge of the network, either by a DiffServ enabled host or the first DiffServ enabled router. Classification can be carried out taking into account the values of header fields such as source and destination IP addresses and port numbers and the protocols carried.

Each user of the network will have a service level agreement that includes a traffic profile that defines the characteristic of the traffic that the network will be offered. This will define the committed data rate, the peak data rate and the maximum burst size, when the committed data rate is exceeded. Traffic is metered and shaped at the edge of the network to ensure that the agreed traffic profiles are met.

At each router, the DS field is examined and packets are queued for transmission or discarded (under congestion conditions), taking the classification into account. The routers can forward packets using three different **Per Hop Behaviours** (**PHBs**).

- **Default** (**DE**) PHB is the normal best effort IP delivery service
- **Expedited Forwarding** (**EF**) PHB ensures low loss, low delay, low jitter and a guaranteed throughput. It is ideal for real-time interactive applications.
- **Assured Forwarding** (**AF**) PHB is better than best effort, but not as good as EF and supports four different classes, further subdivided into three drop preferences, which are taken into account when deciding which packets within the class have to be discarded. Routers reserve bandwidth and buffering for each class, and minimum bandwidth can thus be guaranteed.

[20] *Multi-Protocol Label Switching, see Section 6.6 in this chapter.*

[21] *RFCs 2474, 2475, 3168, 3260.*

[22] *Quality of Service.*

DiffServ also has not been widely used on the Internet. Providing QoS on the Internet is intrinsically difficult, as the network was designed for best effort data transmission and not for real-time multimedia applications. To re-engineer the Internet will require the upgrade of all routers and all ISPs will need to co-operate in this. Finally, even if this could be achieved, the ISPs would then have to find a way of implementing differentiated pricing for their differentiated services and would also need complex accounting arrangements with other ISPs to support this. For the above reasons, ISPs do not offer DiffServ for the public Internet. Many ISPs do however offer DiffServ on IP VPNs that support customers' Intranets where the whole VPN is carried on the ISP's own network.

6.5 Asynchronous Transfer Mode (ATM) Networks

Asynchronous Transfer Mode is a complex high-performance protocol suite designed by the ITU-T (helped by the ATM Forum) to integrate all telecommunications services so that they can be carried together over a single network infrastructure. It therefore has to support real-time multimedia applications such as voice and video and non-real time data applications, offering appropriate grades of service to each. ATM has its origins in attempts by the ITU-T to define a Broadband Integrated Services Digital Network (B-ISDN) that would provide a single platform for carrying all conceivable high and low bandwidth services.

ATM is designed to transmit fixed size packets (called **cells**) each with a five byte header carrying exactly 48 bytes of data over virtual circuits between source and destination via ATM switches. ATM is sometimes also referred as cell relay. Using connection-oriented protocols and moving away from the variable length data link layer frames utilised by most other network layers, has many advantages, as it is much harder to control quality of service on a connectionless network or when a network has to handle packets of unpredictable length.

ATM uses Asynchronous Time Division Multiplexing which is another name for Statistical Time Division Multiplexing.[23] Although ATM uses synchronous physical media for bit transmission, the transmission of cells is asynchronous, as timeslots on the output channel are allocated to carry cells from input channels as and when needed. ATM is a connection-oriented virtual circuit network, but the unidirectional virtual circuits are called **virtual channels**. Because it is connection-oriented, ATM can reserve appropriate resources at each switch to guarantee a desired quality of service for each virtual channel. The virtual channels can either be permanent or switched. The unidirectional connection set up between end users is called a **virtual channel connection**, which is made up by joining together a number of virtual channels in series between ATM switches. Between any two ATM switches, virtual channels can be grouped together into **virtual paths**, where all the virtual channels start and end at the same ATM switches, but are typically routed via other ATM switches. This makes virtual channel mapping much easier as when a switch maps virtual path numbers, it maps all the virtual channels that they contain. A virtual channel is identified in ATM headers by the combination of a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI).

There are two formats for the five byte ATM header, depending on whether the ATM interface is a User-to-Network Interface (UNI) between a user and the ATM network or a Network-to-Network Interface (NNI) between ATM network nodes. The latter uses four bits to increase the number of virtual path identifiers while the former uses those four bits for generic flow control. In addition the header has a Payload Type field to define the type of data the

[23] *See Section 2.3.1 of Volume 1.*

cell is carrying and a bit to indicate cell loss priority. ATM, under congestion, will begin discarding cells which has this bit set to one. Finally, there is a Header Error Control (HEC) field which checks the header using an CRC-8.[24] The HEC also contains some error correcting codes that will allow a certain amount of error recovery.

ATM uses a form of addressing specified by ISO known as Network Service Access Point (NSAP) addressing. NSAP addresses can accommodate both E.164 and X.121 format addresses, but public ATM networks are specified to use the E.164 format.

It was hoped that ATM would be used as a LAN protocol as well as a WAN protocol and that it would carry multimedia services to the desktop over a single local and wide area network infrastructure. ATM has a facility called LAN Emulation (LANE) which allows it to emulate local area networks and carry the LAN frames inside ATM cells. ATM has not been successful in supplanting Ethernet for local area networks and has had similar problems in displacing IP in the wide area.

Activity 6.3

From a text book or web site, read about the structure of NSAP addresses.

Activity 6.4

From a text book or web site, read about ATM LAN Emulation (LANE).

6.5.1 ATM service categories

ATM supports several different grades of service, called service categories:

Table 6.2: ATM service categories

Service	Characteristics	Typical use
Constant Bit Rate (CBR)	Fixed data rate Low loss Low constant delay Low jitter	Circuit emulation Real-time uncompressed voice/video
Real-time Variable Bit Rate (rt-VBR)	Variable data rate Low loss Low delay Low jitter	Real-time compressed voice/video
Non-real-time Variable Bit Rate (nrt-VBR)	Variable data rate Low loss Variable delay Some jitter	Non-real-time data (e.g. business critical applications)
Unspecified Bit Rate (UBR)	Variable data rate Arbitrary loss Arbitrary delay Arbitrary jitter	Best effort service for TCP type traffic that can tolerate delay, losses and has a congestion control mechanism
Available Bit Rate (ABR)	Variable data rate Fair loss Fair delay Fair jitter	Traffic that requires fair allocation of resources and wants a minimum cell rate that can be increased if capacity is available (e.g. business applications)
Guaranteed Frame Rate (GFR)	Variable data rate Intelligent loss Arbitrary delay Arbitrary jitter	IP backbone traffic or LAN interconnect traffic where the discarding of a cell carrying a segmented PDU will result in all the other segments carrying the PDU also being discarded

[24] *8-bit Cyclical Redundancy Check, see Volume 1, Section 7.3.6.1.*

A complex mix of quality of service parameters is determined by the service category. These parameters are cell delay variation, maximum cell transfer delay, cell loss ratio, peak cell rate, cell delay variation tolerance, sustainable cell rate, burst tolerance (maximum burst size) and minimum cell rate. For each service category applications can define values for a different subset of these parameters. The application can establish a contract with the network using these parameters when requesting a virtual channel to be set up to define its own traffic profile and what it expects from the network. The network will then police the traffic offered to ensure that the user does not exceed the agreed parameters and will take appropriate action to ensure that the network meets the parameters it agreed.

6.5.2 ATM layers

ATM is a layered set of protocols that does not conform to the OSI Reference Model. It roughly covers layers 1 to 4 of the ISO model in three layers. The **Physical Layer**, the **ATM Layer** and the **ATM Adaptation Layer** (or AAL). The physical layer roughly corresponds to the OSI physical layer and has two sub-layers: the physical medium dependent sub-layer at the very bottom and the transmission convergence sub-layer above it which hides the details of the physical medium from the ATM Layer which is purely responsible for the transmission, switching and reception of ATM cells. There is no data link layer in ATM. The ATM network layer protocol sits directly on top of the physical layer. There is no facility to retransmit data on a link-by-link basis, as exists with data link layer protocols. If an ATM switch detects an error, it will attempt to correct it, but if this is not possible, the cell will be discarded and higher layer protocols at the destination (possibly the AAL if it supports error control) will detect the loss and request a retransmission from the source rather than the switch requesting a retransmission from its immediate predecessor. Congestion control is only provided for ABR services where a switch can notify the destination of congestion and the destination can then notify the source which can then adjust its rate of transmission.

The purpose of the AAL is to allow existing protocols (e.g. IP) and applications (e.g. voice) to run above ATM. The AAL therefore only resides in the source and destination, there is no need for an AAL in intervening ATM switches. Because of this, it is in many way similar to a transport protocol, particularly when real-time applications such as voice and video reside above it. However, thinking of the AAL as a transport protocol does not fit well with the fact that ATM is often used to carry the IP network layer protocol and sometimes even data link layer frames. It would be a breach of the OSI model for a network layer protocol to be carried over a transport protocol and even worse for Ethernet frames to then be carried over ATM. Internet engineers, often tend to think of ATM as a data link protocol because it can carry IP datagrams, while LAN engineers might think of ATM as a physical layer protocol because as it can carry LAN frames. As we have seen, ATM is much more than this. It is a fully fledged network layer protocol with hierarchical addressing and complex routing, but its level in the OSI model can be confusing to say the least.

The AAL also has two sub-layers. The lower sub-layer is the Segmentation and Reassembly (SAR) sub-layer which is responsible for segmenting data into 48 byte cells at the source and reassembling the data at the destination. The higher sub-layer is called the AAL Convergence Sub-layer (CS) which adapts the services provided by the ATM layer to meet the needs of the higher layers. There are four different AAL from which to choose.

6.5.3 AAL protocols

A number of different AAL protocols are available for different types of application, defined as service classes. The service class and hence AAL protocol chosen is theoretically independent of the service category, but certain combinations of service category and AAL protocols fit naturally with each other and others will make no sense. The service class and AAL should be chosen according to the following table.

Table 6.3: AAL service classes and protocol types

	Class A	Class B	Class C	Class D
	(CBR)	(rt-VBR)	(ABR / nrt-VBR)	(UBR)
Timing Relationship	Required		Not Required	
Delay Sensitivity	Sensitive		Elastic	
Bit Rate	Constant	Variable		
Connection Mode	CO			CL
AAL Protocol	AAL1	AAL2	AAL3/4 or 5	AAL3/4 or 5

AAL1 is suitable for connection-oriented circuit emulation applications which require a constant bit rate with synchronisation, such as real-time uncompressed video and audio.

AAL2 is still largely undefined, but is intended for connection-oriented applications which require the variable bit rate with synchronisation such as real-time compressed video and audio.

AAL3/4 is defined for general variable bit rate data applications that do not require synchronisation. Originally, AAL3 was going to support a connection-oriented service and AAL4 a connectionless service, but the specifications were so similar that it was decided to combine them into a single protocol. It is designed to support general data applications that require a variable bit rate and no synchronisation. ATM provides a connectionless service by means of a permanent virtual channel, which is always on, while a connection-oriented service is provided by a switched virtual channel.

AAL3/4 however was thought to have too much error control for TCP/IP applications and the ITU-T was pressurised into creating AAL5 to provide a Simple and Efficient Adaptation Layer (SEAL).

AAL5 is defined for use with variable bit rate data applications supporting a connectionless service that does not require synchronisation. It assumes that error control is performed by a higher layer connection-oriented protocol, which can thus manage without the extensive error control functions carried out by AAL3/4. Most data is now carried by AAL5, because of the prevalence of TCP/IP running above ATM.

In addition to the three layers, the ATM standards also define three planes. These are the **user plane** which provides data transfer along with error control and flow control; the **control plane** which supports the connection control functions that allow users to set up and clear down switched virtual channels and the **management plane** which supports management functions for all the layers and planes.

6.5.4 ATM deployment

ATM is currently mainly deployed within the high-speed core networks of network operators to support large IP networks, as it is a technology which can integrate multimedia and data services and provide an agreed quality of service for both. It is also used to provide high speed LAN interconnection and is the usual protocol used to carry IP over broadband Asymmetric Digital Subscriber Line (ADSL) physical links. While its use on ADSL lines is mainly to carry IP, its design is such that it could also carry high speed Video on Demand (VoD) and this is being offered by some network operators. Its main disadvantages are its complexity and expense, its protocol overhead (often called the cell tax) and the fact that it does not easily support broadcasting and multicasting. Lastly, because it was designed as a universal networking platform, it does not easily interoperate with other competing technologies. It does play an indispensable role in current networks and the huge investments network operators have made in the technology mean that it will be around for many years to come. But its long-term future is uncertain, as IP evolves to offer true quality of service and real-time multimedia capabilities. In future, running IP directly on top of physical transmission circuits or wide area Gigabit Ethernet may be prove to be a cheaper and more desirable option than deploying ATM.

Because ATM supports so many classes of service, it invariably has a complex pricing structure. There will almost certainly be connection and rental charges for access circuits, which will depend on the data rate and there will be rental charges for PVCs[25]. These may be distance dependent as well as speed dependent. SVCs[26], if they are offered, are likely to have volume related charges (per Kbyte) or duration charges (per minute).

Activity 6.5

Visit the web sites of some of the network operators who offer telecommunications services in your country and investigate the ATM products they offer. Check how these products are priced.

6.6 Multi-Protocol Label Switching (MPLS)

We have seen the difficulties of re-engineering the Internet to support Quality of Service. Attempts to do this such as IntServ and DiffServ have not met with universal acceptance amongst the ISPs and network operators. Yet clearly, the support of QoS is required. MPLS was another attempt by the IETF to achieve this long sought goal. It is based on an earlier proprietary scheme devised by Cisco called tag switching. This involved creating a new layer between layer two and layer three that attached tags (called labels in MPLS) in front of layer 3 packet. Alternatively, if the packets are being carried by ATM or frame relay networks, the ATM VCIs[27] or Frame Relay DLCIs[28] could be used as labels rather than creating a new layer.

MPLS sets up paths through **Label Switch Routers** (**LSRs**) by maintaining tables that can be used to map (or swap) labels attached to incoming packets to the outgoing port and the label to be used when forwarding the datagram. This mechanism is identical to that used in connection-oriented virtual circuit networks. By setting up connections in the MPLS layer, resources in the routers and bandwidth can be reserved. The switching is much simpler and faster than IP routing. The labels are added to packets at the edge LSR, which must decide on the route to be used and the first label. Other LSRs on the path will read the label, look up which label to use on which outgoing port, swap the label with the new label and forward the packet to the next LSR. When the packet arrives at the last LSR, the label is then removed and the packet forwarded over the next data link to the destination. The labels therefore allow the packet to tunnel through a network and emerge at the other side of the network where the label is removed. A packet can actually have more than one label attached to it. This is called stacking and the labels are stacked in a last in first out fashion, so it is always the latest label added to

[25] *Permanent Virtual Circuits.*

[26] *Switched Virtual Circuits.*

[27] *Virtual Channel Identifiers, see Section 6.5 in this chapter.*

[28] *Data Link Connection Identifier.*

the stack that is processed first. This is somewhat similar to ATM, which has two levels of stacking (virtual channels that are carried within virtual paths), except that there is no limit to the level of stacking allowed with MPLS.

Packets to the same destination address with the same class of service form a Forward Equivalence Class (FEC) and are treated with the same priority at each LSR.

The LSRs do need to know details of which labels to use for different destinations. This information is distributed by means of label distribution protocols. There are a number of protocols that can be used, some of them are well known routing protocols with Traffic Engineering (TE) extensions. The main protocols used are Label Distribution Protocol (LDP), Constraint-based Routing Label Distribution Protocol (CR-LDP), RSVP-TE[29], BGP4-TE[30], OSPF-TE[31] and IS-IS-TE[32].

MPLS can carry multiple protocols, hence its name. These not only include the common network layer protocols, such as IP and IPX, but can also include ATM, Ethernet, HDLC, Frame Relay, PPP, private circuits, video or voice. Furthermore MPLS can also be carried by ATM, DWDM[33], Ethernet, HDLC, IP, Frame Relay, PPP, or SDH. This make MPLS a very flexible protocol to deploy and many ISPs and network operators have implemented it and rely on it to provide QoS.

MPLS has finally given the Internet a QoS mechanism that has been widely implemented and that will work across multiple ISPs. But this has been achieved by using a connection-oriented approach below IP. MPLS allows QoS to be guaranteed whilst retaining all the flexibility and scalability of IP connectionless routing.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. JPEG image compression is a lossless algorithm best suited compressing colour photographs.

ii. Real-time Transport Control Protocol (RTCP) works in conjunction with Real-time Transport Protocol (RTP) and allows different streams such as audio and video to be synchronised.

iii. DiffServ redefines the TTL field in IP datagrams to create a new DS field that is used to signal the class of service to routers.

iv. MPLS can be implemented as a connection-oriented layer between layer 2 and layer 3.

(b) Describe the main characteristics of the three classes of multimedia applications.

(c) Describe how streaming multimedia content counteracts the effects of jitter.

(d) Explain why ATM is able to provide quality of service while IP on its own cannot.

(e) Outline the three attempts that the IETF have made to support quality of service on the Internet and give some reasons why two of them have not been widely implemented.

Learning outcomes

At the end of this chapter, you should be able to:

- describe the three classes of multimedia applications
- briefly describe the application layer techniques that are used in multimedia networking

[29] Resource Reservation Protocol – Traffic Engineering.

[30] Border Gateway Protocol 4 – Traffic Engineering.

[31] Open Shortest Path First – Traffic Engineering.

[32] Intermediate System to Intermediate System – Traffic Engineering.

[33] Dense Wave Division Multiplexing.

- describe how enterprises can use Time Division Multiplexing to integrate voice, video and data communications
- outline the main protocols used in multimedia networking
- outline the three IETF standards (IntServ, DiffServ and MPLS) that attempted to support the quality of service on the Internet as required by multimedia networking
- outline how ATM operates and how it supports quality of service for multimedia networking through the various service categories and ATM Adaptation Layer (AAL) protocols.

Chapter 7: Network design

Further reading

Carr and Snyder *Management of Telecommunications.* (McGraw Hill), second edition, 2003. Chapter 13.

Fitzgerald and Dennis, *Business Data Communications and Networking.* (John Wiley & Sons), eighth edition, 2005. Chapter 12.

In this chapter we will examine the process of network design. We will apply the knowledge that we have of network technologies and markets, to the task of designing networks. We will study a design methodology and the many factors that influence good design. We will also study different approaches to network implementation.

Carr and Snyder[1] define network design as 'the process of understanding the requirements for a communications network, investigating alternative ways for implementing the network and selecting the most appropriate alternative to provide the required capacity'.

Network design is a heuristic process. This means that good network designs cannot be produced by simply following a set of prescribed rules. Every design problem is different and they often needs to be tackled in different ways. Good designs evolve from a mixture of trial and error, intelligent guesswork, rules of thumb and incremental discovery. There is no single correct design that can be arrived at with certainty. There may be many good designs, but there are also many bad designs. It is the task of the network designer to explore the design space and select the best designs for more detailed examination and reject the worse designs. Once a good design has been selected, it is often not possible to prove that it is the best possible design. Network design therefore is a creative process often more akin to an art rather than a science.

7.1 Network design criteria

In order to produce a network design, we need to have some measurable criteria against which alternative designs can be evaluated. The design process often involves a trade off between these different criteria (and particularly against cost).

The main measurable criteria used to evaluate network design are outlined below:

7.1.1 Functionality

Functionality describes what the network is able to do. The functionality of a design can be measured against a list of requirements. The requirements are often classified as to whether they are essential or **mandatory** (must have), **desirable** (like to have) or **wish list** (nice to have). The way a design meets these requirements can then be scored by determining whether the requirement is fully met, partially met or not met. The assessment of functionality is usually subjective but in a very complex design it could be scored. It would be normal to reject a design out of hand if it does not meet all the essential requirements. The remaining designs can therefore be assessed in terms of how many desirable and wish list requirements are met, using a different score for each.

[1] *Carr and Snyder, p.586.*

Functionality may include requirements associated with sites, applications, traffic, interfaces, protocols, scalability, security and manageability.

7.1.2 Performance

Performance is a measure of how well a design meets the requirements when the network is in normal operation. There are many different performance criteria that can be used to evaluate a design which will be dependent on the type of network or application being used. Typical performance criteria may include:

- Round Trip Time (RTT), measured in milliseconds
- jitter, measured in standard deviations
- throughput measured in bit/s or packet/s
- bandwidth utilisation, measured as a percentage of available capacity
- error rates, measured in packet loss ratios (percentage of packets lost) or in errored seconds.

It is important to obtain information on the performance of an existing network prior to any new design. The performance data may already exist or may have to be obtained by measurement. This data is known as the **baseline** and when the new design is implemented the performance should be measured and compared with the baseline data.

7.1.3 Reliability

Reliability is a measure of how frequently the network or part of the network fails and how long it takes to recover from a failure

Typical measures of reliability may include:

- Availability (the ratio of up-time to total time), usually measured as a percentage over a long period, such as a year.
- Mean Time Between Failures (MTBF)[2] is a measure of reliability, derived from statistics or by a theoretical calculation. It is the average amount of time that a network or a network component can be expected to operate successfully before it fails. It is usually measured in days or years.
- Mean Time to Repair (MTTR)[3] which, if there is no redundancy, equates to average down-time per failure and is usually measured in hours.

7.1.4 Cost

Cost is a measure of how expensive a network is to implement and run over a period of time. In order to make a fair comparison, it is usually evaluated over a period of three to five years. A design with heavy one-off installation costs and lower running costs can then be compared with a design with lower installation costs but heavier running costs. To be fair, the cost of capital (interest that could be earned on capital if it was invested elsewhere) should also be considered.

Costs should include network equipment costs, circuit costs, metered call costs, client and server hardware costs (or upgrade costs), installation costs, maintenance costs, software costs, network management costs (including test and monitoring equipment), training costs and the cost of capital (loss of interest on the capital investment).

Costs can be obtained from published price lists, or on application to suppliers.

[2] *See Section 8.5.1 in this volume.*

[3] *See Section 8.5.1 in this volume.*

One way of determining costs, which is commonly used by enterprises for large purchases, is to issue a **Request for Proposal** (**RFP**). By doing this, costs are calculated and sometimes even designs are produced by suppliers. An RFP can be issued to a number of suppliers for a whole network, where a single vendor is to selected to design and provide or manage the provision of the whole network. Alternatively, an RFP can be issued for individual components of the network, such as WAN services or certain types of network devices, but the enterprise must then take responsibility for the design, implementation and integration of the network. Multi-vendor solutions will often offer the best functionality, reliability and performance at the best price. But there can be hidden management costs incurred in integrating products from different suppliers and, if problems occur, it is sometimes difficult to establish who is responsible and should fix the problem. Either way, costing is carried out by third parties, and the enterprise can review proposals from different suppliers and select the solution that best meets the requirements.

According to Fitzgerald and Dennis,[4] the RFP should contain background information about the enterprise, its organisation, the existing network and an overview of the proposed network and its goals.

It should specify the network requirements by outlining a number of alternative designs and providing a list of requirements, including security, management and performance requirements, all classified as essential, desirable and wish list. Guidance should be given regarding the supplier proposing a new design.

For service requirements, the supplier should be asked to provide implementation timescales and details about any training course and materials offered, support services (such as maintenance and technical support and recommended on-site spares). The supplier should also be asked to indicate the reliability and performance guarantees it can offer.

The RFP should also provide details of the bidding process, including the timescales, the ground rules, the criteria which the enterprise will use to evaluate the bids and the availability of additional information.

Finally, the RFP should also ask suppliers to provide information about their own organisation and experience. They should be asked to provide their own corporate profile, the experience they have with similar networks, any hardware and software benchmarks of equipment and a list of customer references, who the enterprise can approach to verify the supplier's credentials.

Activity 7.1

Use a search engine to search for the terms 'request for proposal' and 'network'. Some of the hits will represent some real network RFPs. Examine some of these documents to obtain an appreciation of what a real RFP looks like.

7.2 Network design methodology

Traditionally, network design has followed methodologies very similar to computer systems design. Often a network design is a part of a larger systems design. There is a network design life cycle, similar to a systems design life cycle that follows a sequential process of feasibility study, requirements analysis, specification, design, testing and implementation. There is no general agreement as to the exact number of sequential steps in this process or the precise deliverables at each step.

[4] *Fitzgerald and Dennis, pp.426–427.*

It should be noted that most network designs are for upgrades to networks that already exist. It is quite rare to design a totally new network from scratch. Because of this, a good deal of time has to be spent understanding and evaluation the existing network, before new requirements are considered.

Fitzgerald and Dennis[5] describes a design methodology which he calls building block design. Traditional network design is time consuming, expensive, rigid and inflexible. It does not easily cope with rapidly changing requirements and high levels of traffic growth. Finally, the balance of costs are changing. Equipment and circuit costs have reduced significantly over the years while the cost of employing skilled network designers has increased significantly. It is often not worth designers expending a lot of time to save a relatively small amount of cost by producing perfect designs.

In the building block methodology, users, servers, sites and circuits are all classified into a small number of categories. Often there are just two, one typical and one high volume. For each category of users, servers, sites and circuits there is an equivalent design. The whole network design is therefore built up from a set of smaller designs. This approach means that designs are not as customised as in the traditional approach, and hence the network designed is often not as efficient, but the process is much quicker and network designers are an expensive resource. The approach works best with LAN design and a managed network WAN design. It is not well suited to designing private circuit networks. According to Fitzgerald and Dennis, there are three steps: **needs analysis**; **technology design**; and **cost assessment**. The designer cycles through these steps several times, refining the design each time until a final agreed design emerges.

In this course, we will base our discussion of network design methodology on a modified version of the methodology previously recommended by Cisco Systems. This methodology has a structure suitable for this course and is a practical methodology that, until recently, was used by many network design professionals.

7.2.1 Requirements analysis

This part of the process is an essential pre-requisite to any network design, even when the customer has written a good statement of requirements, the items listed below should be verified by discussions with key members of staff.

Understanding the business requirements is essential. The purpose of the design must be clearly understood and the criteria for success must be established. The latter could have contractual significance as the designed network will not be accepted if the success criteria are not met. They will probably be based on a subset of the measurable criteria for evaluating designs described above. Another detail that ought to be discovered before any design begins is the available budget. This will often be a major constraint on the design. Required timescales may also have an effect on the choice of design. As part of this exercise, the designer ought to gauge the resources and skills available to work on the project and to identify the key decision makers who will decide on whether to implement the design. An appreciation of the politics within the customer organisation will also be useful.

In order to understand the technical requirements the following areas should be addressed:

[5] *Fitzgerald and Dennis, pp.415–428.*

- Application requirements: all of the applications using the network (including any new ones) should be identified and sized. Information should be collected on the numbers and locations of clients and servers, the hours when the use the application and any peak times when the application is busiest. The data flows between sites volume and sizes of PDUs should be assessed as well as what use is being made of broadcasting and multicasting. It should be noted that whilst at one time the level of traffic could be predicted from sizing the enterprise's applications, this is no longer the case. A large amount of traffic is now discretionary and results from web surfing, file transfers and email. This type of traffic is much harder to predict, but allowance must be made for it.
- Performance requirements: The requirements need to be identified for the network as a whole or for individual applications, if the requirements are different. These may include RTT, error rates, availability, utilisation, capacity and throughput.
- Security requirements: the main security concerns should be addressed, particularly with regard to external access to the applications.
- Management requirements: the requirements should address issues such as where the network is to be managed from, what network management protocols will be employed and whether the new network components needs to be integrated into the management system of the existing network. Requirements for the remote configuration, status, performance and usage monitoring and fault diagnosis should be identified. Requirements need to be identified regarding what information needs to be collected for the purpose of management reporting.

7.2.2 Current network assessment

A great deal can be learnt from a study of the current network. The assessment should include:

- The geographical and/or organisational structure of the network: many networks will be structured geographically, but sometimes the networks on a site reflect the organisational structure (e.g. department LANs or VLANs) rather than a strictly geographical structure (e.g. floors).
- Physical assessment: the designer should obtain (or draw) maps showing the network topology, showing sites, LANs, network devices and circuits.
- Logical assessment: the designer should obtain details of naming and addressing schemes, all protocols used (including routing protocols) and details of any traffic filtering that takes place at firewall routers.
- Applications assessment: the designer should identify which servers and WAN circuits and LANs support each application and should characterise the applications by type (e.g. real-time, database, groupware, web etc.).
- Traffic assessment: the designer should obtain information on traffic volumes, characterised by application or application type, over each WAN circuit and LAN including all the traffic that originates from or is destined for public networks. The designer should also identify any traffic bottlenecks within the existing network.
- Performance assessment: the designer should obtain reports on the performance of the existing network with regard to RTT, error rates, availability, utilisation and throughput.
- Security assessment: the designer should review all existing security policies and procedures (including physical security) and identify any weaknesses and risks.

- Management assessment: the designer should review all existing network management stations, remote monitors and diagnostic tools that are used.

It may be that some of the information on the current network does not exist, in which case the designer has to obtain it himself by visiting sites, interviewing staff and possibly monitoring network traffic.

7.2.3 LAN design

The designer must consider all the following factors in deciding on an appropriate LAN design.

- Technical solutions: the designer must select the most appropriate technology to use. The choice is between Ethernet, FDDI, Token Ring or Wireless LANs[6] and the likely deciding factors are indicated in Table 7.1 below. The choice these days is really between Ethernet and the various types of wireless LANs and it will be influenced by cost, existing wiring, reliability, mobility and possibly security requirements.

Table 7.1: Some reasons for choosing LAN technologies

Technology	Reasons for choosing
Ethernet	Cost
	Interface cards are standard on PCs
	Upgrade path to higher data rates
FDDI	Resilience
	Immunity from electromagnetic interference
	Well suited for backbone LANs
	Can be used to connect different technologies
Token Ring	Compatibility with IBM SNA[7] protocols
	Deterministic limit to frame transmission time
Wireless LANs	Data users requiring mobility
	Avoiding expense of cabling or cabling upgrades
	Not being able to lay cable in a listed building

- Capacity: the designer must assess the most appropriate capacity for each LAN bearing in mind the maximum utilisation level recommended for each LAN. Ethernets, for instance, should never have more than forty per cent utilisation. This task is probably easier than it sounds as the capacity of Ethernet LANs increases in factors of 10. It is therefore fairly easy to determine the appropriate capacity, even if information on traffic volumes is limited or inaccurate.
- Topology: the designer must chose an appropriate topology. The topology of each LAN will be determined by the technology chosen, but when LANs on the same site are connected via bridges, switches or routers, a topology must be selected that provides a suitable level of redundancy so that the network can recover from single link or node failures.
- Media: some media decisions will be determined by the technology selected but within a technology there may be choices to be made (e.g. between Coax, Twinax, different categories of UTP and STP, between monomode and multimode fibre or wireless). These choices will be determined by cost, capacity requirements, maximum segment lengths, ease of installation and electromagnetic interference issues. The designer should be aware of any legal requirements, such as building and safety regulations. For instance, in many countries a special type of fire-retardant cable is required, known as plenum cable, when run in

[6] *See Sections 3.3.1, 3.3.4 and 3.3.5 in this volume.*

[7] *Systems Network Architecture.*

overhead ceiling cavities or below a raised floor. Plenum cable also does not give off toxic fumes, if it does burn.

- Hierarchy: the designer should design using a hierarchical model, with LANs that support users and workgroups at the access layer and building backbone LANs, which do not support users directly, at the distribution/core layer. The core layer can be a campus LAN in a multi-site network.
- Redundancy: the designer will already have considered some redundancy issues when considering the topology. There are other issues to consider, such as the failure of the default router on a LAN, redundant NICs in servers, redundancy of data storage, load balancing on routes, Uninterruptible Power Supplies (UPS) and the fallback to a different computer centre for disaster recovery.
- Maximum segment lengths: these will depend on the technology chosen, but must be taken into account in the design. If they are exceeded anywhere, then the segment has to be split up by means of an appropriate internetworking device. There is a limit to the number of times a segment can be split by repeaters. The 5-4-3 rule states that a 5 segments can be connected with 4 repeaters as long as only 3 of the segments are populated with stations.
- Internetworking devices: the designer must choose which internetworking devices to use to split segments and/or switch traffic (repeaters, transparent bridges, source route bridges, translational bridges, hubs, layer 2 switches, layer 3 switches, VLAN switches, routers, relays or gateways). The decision is likely to depend on the factors given in Table 7.2 below. Layer 3 switches will do everything a router can (apart from WAN connections), but much faster and for less cost. Together with layer 2 switches, they usually represent the best choice for internetworking LANs on the same site. But routers are still required to interface with WANs and high performance routers can also now be hardware-based. The philosophy for a large network is usually to switch many times but only route once.

Table 7.2: Comparison of the main types of internetworking devices

Factors	Repeaters	Hubs	Transparent Bridges	Layer 2 Switches	Layer 3 Switches	Routers
Cost	Very low	Low	Low	Medium	Fairly high	High
Performance	Very good	Good	Medium	Good	Good	Usually poor
Separate collision domains	No	No	Yes	Yes	Yes	Yes
Separate broadcast domains	No	No	No	Only with VLANs	Yes	Yes
Filtering of data	No	No	Limited	Yes	Yes	Yes
Reduces traffic on segments	No	No	Limited	Yes	Yes	Yes
Connect unlike media	No	Yes	Yes	Yes	Yes	Yes
Connect unlike architectures	No	No	With some problems	With some problems	Yes	Yes
Isolation of faults	Poor	Poor	Fairly poor	Good	Good	Good
Ease of configuration	Very easy	Easy	Easy	Fairly easy	Fairly hard	Very hard
Ease of maintenance	Poor	Poor	Poor	Good	Good	Good
Bridging or Routing Protocol overheads	None	None	STP	STP	Routing Protocols	Routing Protocols

The designer has also to choose the supplier of the device and the correct hardware/software configuration (sufficient ports supporting the appropriate LAN protocols). This decision is likely to be influenced by cost, functionality, the number and types of interfaces required, reliability, scalability, reputation and manageability.

Activity 7.2

Try to find out what types of LANs are installed at your institution or place of work and what internetworking devices are used to connect them.

7.2.4 WAN design

Although this section is headed 'WAN design', the issues involved in designing MANs are very similar to those involved in designing WANs so any reference to WANs below should be interpreted as also applying to MANs. In fact, it is a very fine line that is drawn between the two, and many technologies can be deployed in both MANs and WANs.

Before looking at WAN design in detail, we will first consider some of the differences between LANs and MANs or WANs which makes MAN and WAN design very different from LAN design.

WANs, unlike LANs, are not confined to a single site and therefore will normally have to cross public roads. The distances are generally much longer than are covered by LANs. As a result, delays are greater, due to propagation delays over long distances and transmission and queuing delays at nodes. Only utilities and railway or canal companies are able to run cables over long distances, so apart from certain line-of-sight technologies, such as infra-red and LASERs, all WAN services have to be bought from network operators. Customers therefore invariably do not own WAN infrastructure and have to rely on network operators to provide and maintain this infrastructure. Because of cost of installing cables across large distances and the limited supply, bandwidth in the WAN is a much scarcer resource than it is in the LAN and, unlike LANs, customers are charged according to the bandwidth that they use. WAN applications therefore have to be designed so that they are not wasteful in their use of bandwidth. Another consequence of the distances and the vulnerability of WAN infrastructure is that it is much less reliable than LAN infrastructure. It is often affected by being accidentally dug up by other utilities or affected by adverse weather conditions. The connections through network operators' exchanges are also prone to being accidentally disconnected or looped. Breaks in service are therefore relatively common. Also, WAN services are much more prone to electrical interference and signal degradation which means that the error rates experienced by WANs is significantly higher than those experienced by LANs.

The designer must consider all the following factors in deciding on an appropriate WAN design.

- Technical solutions: the designer has a limited number of technical solutions to choose from, but there are more alternative technologies to be considered than there are for LANs. For WANs services are invariably provided by network operators. They include private circuits, PSTN, ISDN, X.25, frame relay, xDSL, ATM, SMDS, IP VPNs, and Metro Ethernet.[8] The design may use more than one WAN technology in different parts of the network. The choice will be influenced by capacity requirements, costs, existing network infrastructure, reliability and security. The designer must also select a WAN supplier. This choice is likely to be influenced primarily by cost and reliability.

[8] *See various sections: 4, 5.6.3, and 6.5 of this volume and Section 8.5 of Volume 1.*

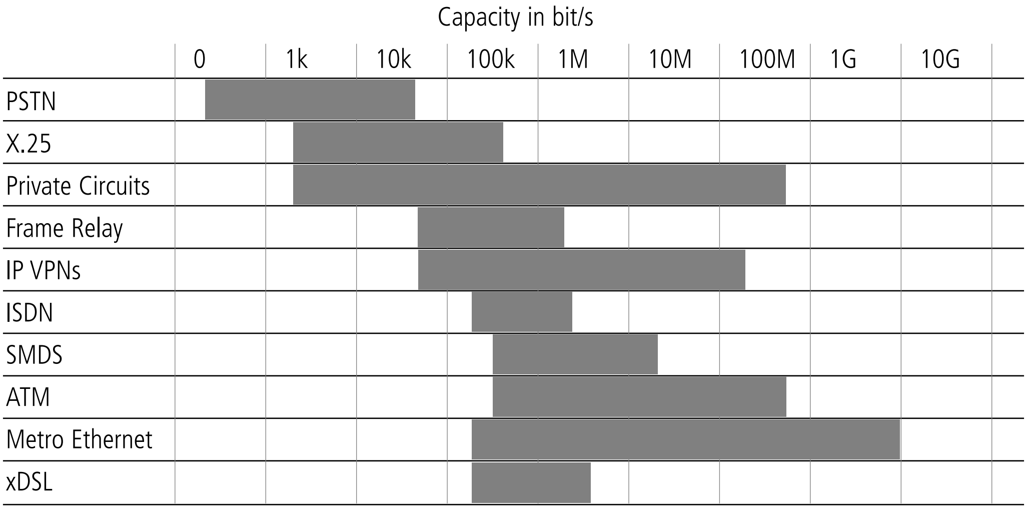
Table 7.3: Some reasons for choosing WAN technologies

Technology	Reasons for choosing
Private Circuits	Low, medium or high data rate with heavy constant usage Preference for self-built and self-managed networks
PSTN	Low data rate and infrequent use
ISDN	Medium data rate and infrequent use Back-up for medium other medium data rate WAN services
X.25	Low data rate with bursty and relatively infrequent use High error rates To some remote countries
Frame Relay	Medium data rate with bursty applications Low error rates Flexibility
xDSL	High data rate access to other WAN services
ATM	High data rate Integration between all types of data Guaranteed QoS, if required Flexibility
SMDS	Medium data rate with bursty applications LAN interconnect Applications requiring multicasting
IP VPN	Low, medium or high data rate with relatively infrequent use Low cost IP compatibility Security Flexibility
Metro Ethernet	High to very high data rates LAN interconnect Compatibility with Ethernet LAN protocols

Once the technology has been chosen, the designer must choose a supplier. The WAN services market is now very competitive in most countries and there are plenty of suppliers to choose from. The designer could choose an incumbent operator or a new entrant. The former may be regarded as a safe but expensive choice and the latter as a cheaper but more risky choice. This choice may be influenced by cost, reliability, support, ubiquity and reputation.

- Capacity: the designer must choose the appropriate capacity required between each pair of sites, from those supported by the technology bearing in mind utilisation. WAN services, in general, should not have a utilisation greater than 70 per cent. The granularity of WAN capacities is less than that for LANs and consequently more care has to be taken with traffic estimates and the selection of the most appropriate capacity. Table 7.4 below shows the approximate capacity ranges of various WAN technologies.

Table 7.4: Typical capacity ranges for WAN technologies using a logarithmic scale



- Topology: the designer has to choose a topology for private circuit solutions. For managed service solutions the topology design is carried out by the network operator. A topology must be chosen that provides the required reliability at an optimal cost. The choices are between full and partial meshes, stars, rings, and hybrid topologies, such as cascaded stars (star-star) and multiple overlapping rings (ring-ring). This is a difficult task as there is a very large number of options that could be considered. The use of an automated tool that can support network design, traffic modelling and costing is recommended. Alternatively, a managed network solution can be chosen where the topology is determined by the supplier.

A table summarising the advantages and disadvantages of different WAN topologies is provided in Table 7.5 below:

Table 7.5: Advantages and disadvantages of WAN topologies

Topology	Cost	Control	Worst Routes	Resilience	Scalability
Star	Low to High[9]	Centralised	Short	Poor	Good
Cascaded Star	Fair	Centralised	Fair	Poor	Good
Ring	Low	Distributed	Long	Good	Good
Overlapping Rings	Medium	Distributed	Long	Very Good	Good
Partial Mesh	Low to High[10]	Distributed	Fair to Long[10]	Good to Very Good[10]	Fair
Full Mesh	Very High	Distributed	Short	Excellent	Poor
Hierarchical	Fair	Distributed	Long	Good	Good
Managed	High	Delegated	Long	Very Good	Very Good

- Media: the choice of media is determined by the technology chosen and the designer does not normally have any control over the media (copper, mono-mode fibre, multimode fibre or radio) that the network operator uses to deliver the technology, but the media used will depend on data rate and distance.
- Hierarchy: the designer may want to design using a hierarchical model, with the part of the WAN supporting customer sites acting as a distribution layer connecting an access layer to a core layer that does most of the routing. The practical implications of this hierarchy is that there are

[9] Depends on the location of the central site in relation to other sites.

[10] Depends on the degree of meshing.

often a number of local access networks, a number of regional distribution networks and a national (or international) core network. The main design choice is how to split the network into regions and which nodes in each region connect to the higher level network. The regional networks are likely to reflect a similar geographical organisational structure. Also, the designer has to decide which nodes should form the core network. It is difficult to prescribe the best solution, that keeps circuit costs to a minimum while maintaining resilience. In general, it is the most important and busiest nodes that are likely to form the core network. But there are some situations where it is economic to use an unimportant node as a core node, if it can serve many other smaller nearby nodes. A network design tool, such as NetViz or Microsoft Visio, that can quickly cost or even calculate the best design will be very useful.

- Redundancy: the designer will already have considered some redundancy issues when considering the topology. There are other issues to consider, such as load balancing on routes, ISDN[11] back-up, Uninterruptible Power Supplies (UPS) and the fallback to a different computer centre for disaster recovery.
- Network devices: the designer must choose the appropriate network devices to use in the WAN. The choice will depend on the technology and protocols that need to be supported. The choice will include various types of multiplexers, modems, ISDN terminal adaptors, DSL Access Multiplexers (DSLAMs), Frame Relay Access Devices (FRADs), ATM switches, routers, or Packet Assembler/Disassemblers (PADs). The designer must also select a supplier and model number for this equipment and also its card configuration. This decision is likely to be influenced by cost, functionality, the number and types of interfaces required, reliability, scalability, reputation and manageability.

Activity 7.3

Try to obtain a price list for private circuits, frame relay and ISDN from a network operator in your country. The incumbent operator is most likely to publish these prices. If you cannot locate a price list you could use the BT electronic price list which can be found by searching for the term 'price list' on the www.bt.com web site.

Use the price list to calculate the price of a 128 kbit/s private circuit between two new sites 100 km apart, over a three year period. Include one-off connection charges as well as rental charges.

Carry out a similar calculation for setting up a frame relay access circuits at the two sites and a 128 kbit/s PVC between the sites. Compare the two prices. Then calculate the costs of implementing two Basic Rate ISDN (two 64 kbit/s channels) circuits at the sites and the cost per minute of calls made between the two sites at the peak daytime rate.

Calculate at what point (how many call minutes per working day) it becomes more economic to replace the ISDN service between the sites with a private circuit and a frame relay PVC.

Carry out the same calculations for a 2 Mbit/s private circuit, a 2 Mbit/s frame relay PVC and a Primary Rate ISDN (thirty 64 kbit/s channel) service.

Activity 7.4

Visit the web sites of some of the main network operators and ISPs that offer services in your country, including the Education and Research Network that provides services to the universities in your country. Try to find information about their network infrastructure, particularly a map showing their main nodes and the connectivity between them. Does there appear to be some hierarchy of networks or perhaps a multiple overlapping ring structure?[12] Attempt to find some reasons why they might have chosen the topology and structure that they have.

[11] Integrated Services Digital Network, see Section 4.2.4 of the volume.

[12] See Volume 1, Section 2.4.2.

Summary

Table 7.6 below provides a summary of the factors that influence both LAN and WAN design choices.

Table 7.6: Summary of factors influencing LAN and WAN design choices

Factors influencing	LAN and WAN design choices						
	Technology	Capacity	Topology	Media	Hierarchy	Redundancy	Devices
Cost	✓	✓	✓	✓	✓	✓	✓
Reliability	✓	✓	✓	✓	✓	✓	✓
Security	✓	✗	✗	✓	✗	✗	✓
Existing network	✓	✓	✓	✓	✓	✓	✓
Traffic levels	✓	✓	✓	✓	✓	✓	✓
Manageability	✓	✗	✓	✓	✓	✓	✓
Ease of installation	✓	✗	✓	✓	✓	✓	✓
Mobility	✓	✓	✗	✓	✗	✓	✓
Legal requirements	✗	✗	✗	✓	✗	✓	✓
Functionality	✓	✗	✗	✓	✗	✗	✓
Distances	✓	✓	✓	✓	✓	✗	✓

7.2.5 Specific protocol design

The next stage is to carry out the design activities necessary for each protocol supported by the network. For IP networks the key design issues are the addressing structure and routing protocol and packet filters to be used.

For IP addressing a decision must be taken whether or not to use Network Address Translation (NAT). If it is decided to use NAT then the address range must be chosen. If it is decided not to use NAT, then the existing IP address structure must be reviewed to ensure that sufficient addresses are available for all new devices and revised if necessary. In the worst case, it may be necessary to apply for a larger address range. In other cases it may be possible to reconfigure some or all of the subnetwork addresses or it may be that the existing structure is adequate.

All LAN segments and point-to-point WAN circuits should be treated as subnets and allocated a subnetwork address. The main requirement is that every physical interface must have a separate IP address. A point-to-point circuit is treated in a similar way to a LAN, so it is given its own subaddress and the two router ports that are connected by the circuit are regarded as belonging to the same subnet. For managed networks, such as frame relay or ATM, where a single interface multiplexes a number of virtual circuits, all of the router ports that connect to the managed network are regarded as belonging to a single subnet.

If there is no shortage of address space, it is easiest to use the same subnet mask for all subnets. This should be chosen so that there are sufficient spare bits in the host address to cope with any expected growth and sufficient bits in the subnet mask to cope with any expected growth in the number of subnets. Using a fixed length subnet mask for the whole network is particularly wasteful for point-to-point WAN circuits where there will only be two host addresses allocated for the router ports at each end of the circuit.

If there is a shortage of addresses, then different size subnets can use different subnet masks and support different numbers of hosts. This is called **Variable Length Subnet Masking** (**VLSM**) and it can only be used when the network uses a routing protocol that supports VLSM. Point-to-point circuits can thus be allocated a network address with prefix /30. This subnet mask allows just 2 bits for the host address, and hence four addresses. One of these is the network address ending 00, another is the broadcast address 11, leaving two addresses ending 01 and 10 for the router ports at each end of the circuit. Using /30 network addresses, is therefore quite efficient in terms of conserving IP address space.

The choice of IP routing protocols should take account of the complexity of the networks, whether CIDR[13] and VLSM are supported, whether the routing protocol should be Distance Vector or Link State, convergence times and the bandwidth, processing and memory overheads in running the routing protocol. With large networks using the OSPF[14] routing protocol, the network has to be partitioned into areas.

Packet filters (or access lists in Cisco terminology) also need to be designed on a per protocol basis for the firewall routers at each site to decide which packets to allow and which packets to discard. With IPX networks, the main issues are the control of broadcasts and the choice of IPX routing protocol. There is a danger from networks being flooded with Service Advertising Protocol (SAP) messages which are broadcast every minute and are by default forwarded by routers. It is wise to filter these broadcasts to restrict them to individual LANs.

For applications that use Microsoft's NETBUI or IBM's SNA protocols, it may be necessary to use bridges as these protocols are not routable. Other alternatives are available to encapsulate these protocols in IP. For multimedia applications, it is best to implement multicast routing and/or DiffServ.

Example 1 below shows how to design a subnet addressing scheme where address apace is severely limited. Example 2 shows how to design a subnet addressing scheme for a site where there are multiple LANs.

Activity 7.5

Using a spreadsheet, list all of the ways that each class of address (Class A, B and C) can be subnetted using one column to show the network prefix and other columns to show the number of bits in the subnet part, the number of bits in the host part, the maximum number of subnets and the maximum number of hosts per subnet. Use the 2N – 2 formula[15] for the last two calculations, where N is the number of bits in the address.

Subnet design example 1

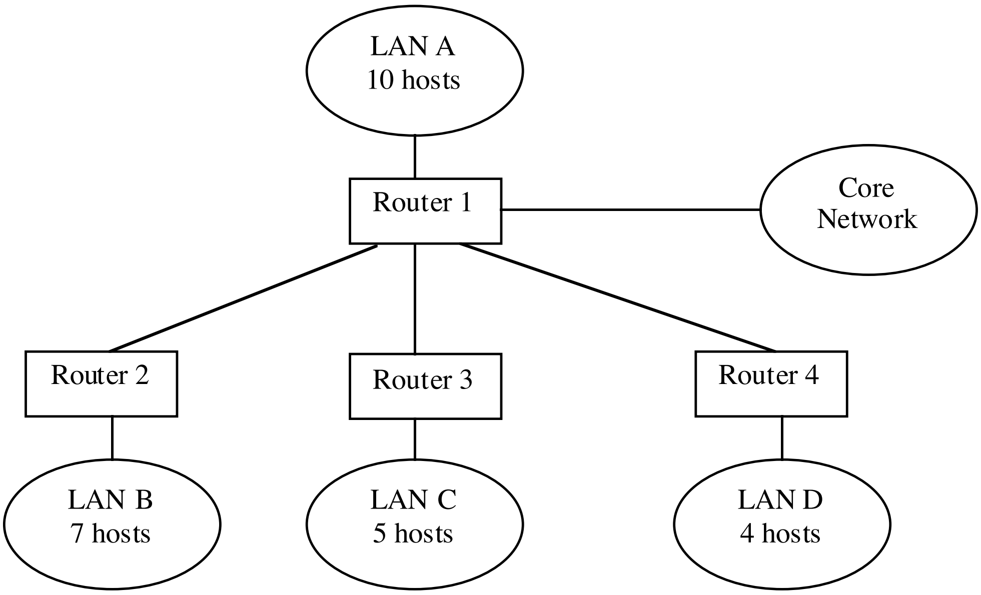
Figure 7.1 below shows a simple network for Region 1, which is the largest of 4 regional networks and a core network belonging to a hierarchical network with the Class B network address, 144.3.0.0/16. This regional network also has the largest number of LANs and the largest individual LAN on the whole network. You are to design a subnetwork addressing scheme that allocates addresses for each region and a scheme that allocates addresses to each LAN and WAN circuit in Region 1.

[13] *Classless Inter-Domain Routing, see Volume 1, Section 6.4.2.*

[14] *Open Shortest Path First, see Section 5.6.1.3 in this volume.*

[15] *The subtraction of the two is necessary because subnet and host Ids of all 0s and all 1s are not normally used. Subnet addresses of all 0s and all 1s would cause ambiguity with classful routing, between the network address of the network and the first subnetwork and between the broadcast address of the network and that of the last subnetwork. The all 0s host ID is the network address of the subnet and the all 1s host ID is its broadcast address, which should never be used to identify hosts.*

Figure 7.1: Subnet design example 1



Firstly, let's count the number of hosts in the region. There are 26. As this is the largest of four regions, there will be less than 104 hosts in the whole network. The network address range though will support 65,534 so there is no shortage of addresses.

The first decision is how many bits to allocate to the hosts. LAN A has 26 hosts and choosing 5-bit host addresses would not allow sufficient address space for expansion on this LAN. This LAN therefore requires 6-bit host addresses to support up to 62 (26 – 2) hosts. In this case, as there is no shortage of address space, it is simplest to use fixed length subnets with 6-bit host addresses, so that each LAN subnet can support up to 62 hosts.

We have to define subnet addresses for the three LANs, plus the three point-to-point WAN circuits that connect the routers up to each other and the WAN circuit that connects to a router within the core network. This makes a total of seven subnets. We also need to decide what is the maximum number of subnets that are likely to be supported in the region in future. We will assume that this maximum number of subnets required in the region (including point-to-point circuits) is 30. This provides plenty of scope for expansion. As there is no shortage of address space, we do not need to use VLSM and we can afford to waste some address space on the point-to-point circuits.

With a hierarchical network we also need to use some bits to identify the regional networks. As there are currently four regions, it would be sensible to use three bits to identify the regions, so that up to six regions could be supported.

We have now used three bits for regional networks, five bits for subnetworks in each region and six bits for host addresses, making a total of 14 bits. We have two bits spare, so we should allocate these to the part of the address that is most likely to run out. There is only scope for two more regions, while there is plenty of address space for new LANs in each region. It would make sense to add one bit for the region and one bit to the host addresses.

We will therefore design for 4-bit regional network addresses(/20), 5-bit regional subnetwork addresses (/25) and 7-bit host addresses. The core network will be treated as a regional network with just one subnetwork. When allocating subnets in Regions, there are so many spare addresses that it is sensible to only allocate LANs and WAN circuits to subnets with all 0s in the last byte, because they are easier to write down and work with. It is also worth putting LANs and circuits in different parts of the address space, so it is easy to distinguish between LANs and circuits. Table 7.7 details the /20 subnetworks used for the core network and each of the regional networks.

Table 7.7: /20 Subnets for Subnet design example 1

Network	3rd Byte	4th Byte	Subnetwork Address	First Host Address	Last Host Address
Not used	0000XXXX	XXXXXXXX	144.3.0.0/20	144.3.0.1	144.3.15.254
Core	0001XXXX	XXXXXXXX	144.3.16.0/20	144.3.16.1	144.3.31.254
Region 1	0010XXXX	XXXXXXXX	144.3.32.0/20	144.3.32.1	144.3.47.254
Region 2	0011XXXX	XXXXXXXX	144.3.48.0/20	144.3.48.1	144.3.63.254
Region 3	0100XXXX	XXXXXXXX	144.3.64.0/20	144.3.64.1	144.3.79.254
Region 4	0101XXXX	XXXXXXXX	144.3.80.0/20	144.3.80.1	144.3.95.254
Spare	0110XXXX	XXXXXXXX	144.3.96.0/20	144.3.96.1	144.3.111.254
Spare	0111XXXX	XXXXXXXX	144.3.112.0/20	144.3.112.1	144.3.127.254
…	…	…	…	…	…
Spare	1111XXXX	XXXXXXXX	144.3.240.0/20	144.3.240.1	144.3.255.254

These subnet addresses will be used in the routing tables of the core network routers, as they summarise all the subnetworks in each region. The core network does not require any knowledge of the subnets within each region.

Table 7.8 details the /25 subnetworks used within Region 1 for the LANs and point-to-point WAN circuits in that region.

Table 7.8: /25 Subnets of Region 1 in Subnet design example 1

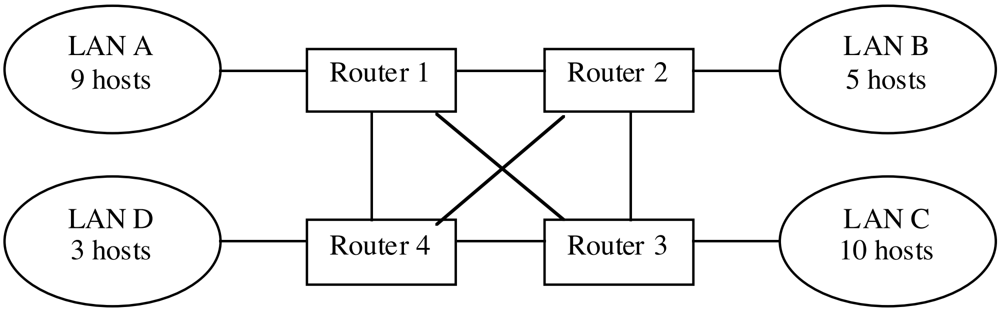
Network	3rd byte	4th byte	Subnetwork address	First host address	Last host address
Not used	00100000	0XXXXXXX	144.3.32.0/25	144.33.32.1	144.3.32.126
Spare	00100000	1XXXXXXX	144.3.32.128/25	144.3.32.129	144.3.32.254
LAN A	00100001	0XXXXXXX	144.3.33.0/25	144.3.33.1	144.3.33.126
Spare	00100001	1XXXXXXX	144.3.33.128/25	144.3.33.129	144.3.33.254
LAN B	00100010	0XXXXXXX	144.3.34.0/25	144.3.34.1	144.3.34.126
Spare	00100010	1XXXXXXX	144.3.34.128/25	144.3.34.129	144.3.34.254
LAN C	00100011	0XXXXXXX	144.3.35.0/25	144.3.35.1	144.3.35.126
Spare	00100011	1XXXXXXX	144.3.35.128/25	144.3.35.129	144.3.35.254
…	…	…	…	…	…
Spare	00100111	1XXXXXXX	144.3.39.128/25	144.3.39.129	144.3.39.254
Circuit 1	00101000	0XXXXXXX	144.3.40.0/25	144.3.40.1	144.3.40.126
Spare	00101000	1XXXXXXX	144.3.40.128/25	144.3.40.129	144.3.40.254
Circuit 2	00101001	0XXXXXXX	144.3.41.0/25	144.3.41.1	144.3.41.126
Spare	00101001	1XXXXXXX	144.3.41.128/25	144.3.41.129	144.3.41.254
Circuit 3	00101010	0XXXXXXX	144.3.42.0/25	144.3.42.1	144.3.42.126
Spare	00101010	1XXXXXXX	144.3.42.128/25	144.3.42.129	144.3.42.254
Circuit 4	00101011	0XXXXXXX	144.3.43.0/25	144.3.43.1	144.3.43.126
Spare	00101011	1XXXXXXX	144.3.43.128/25	144.3.43.129	144.3.43.254
…	…	…	…	…	…
Spare	00101111	1XXXXXXX	144.3.47.128/25	144.3.47.129	144.3.47.254

The subnetwork addresses allocated above will be used in the routing table of the routers in Region 1. Only these routers need to know about routes to these subnetworks.

Subnet design example 2

The network in Figure 7.2 below has been allocated the Class C IP Address, 192.5.8.0/24. The label for each LAN indicates the name of the LAN and the number of host IP addresses that need to be supported. The lines between the routers are point-to-point circuits. Design a subnet addressing scheme that could be used for this network.

Figure 7.2: Subnet design example 1



First we must determine the size of subnet we will use for each LAN. We need to allow some address space to add new hosts to each LAN and to allow for new subnets to be added to the network. We need to assign subnet addresses to each of the four LANs and each of the six WAN circuits. Therefore we need to assign ten subnetwork addresses.

LAN A, with nine hosts, will theoretically require 4-bit host addressing to support up to 14 hosts, but we could then only add a further five hosts to this LAN. It will therefore provide more scope for growth if we use 5-bit host addressing to support up to 30 hosts on this LAN. If we use fixed length subnet masks, we will therefore only have three bits to identify all the subnets and this will not be enough. We are therefore forced to use VLSM.

LAN B with five hosts, will theoretically require 3-bit host addressing, but for the same reason as above, it would be wise to use 4-bit host addressing for this LAN to support up to 14 hosts. Similarly, LAN C with 10 hosts is also best served with 5-bit host addressing to support up to 30 hosts. LAN D with three hosts like LAN B, is probably best served with 4-bit host addressing, supporting up to 14 hosts.

We therefore require two /27 subnets supporting up to 30 hosts and two /28 subnets supporting up to 14 hosts. Again it would be wise to allow for some spare subnetwork addresses, so we will initially design for four /27 subnets and four /28 subnets. Address space for point-to-point circuits is best conserved by using /30 subnets. We have five such circuits. To allow for growth, we will initially design for eight /30 subnets.

At this stage, it is sensible to check how many addresses we have allowed for, but counting all the subnets and hosts including those with all 0s and all 1s which we do not allocate to hosts and revise our scheme if necessary to utilise the address space efficiently.

We have to allocate four /27 subnets with 32 addresses each, plus four /28 subnets with 16 addresses each, plus eight /30 subnets with 4 addresses each. This makes a total of 224 addresses, which means that our scheme currently has 32 addresses totally unaccounted for. We could either use these to support another spare LAN with 30 hosts, two other LANs with 14 hosts, one other LAN with 14 hosts plus four more point-to-point circuits or eight other point-to-point circuits. It perhaps makes more sense to allow for another spare LAN with 14 hosts plus four more point-to-point circuits, but this address space could be re-assigned later if necessary. We will therefore design for four /27 subnets, five /28 subnets and twelve /30 subnets.

We will firstly allocate the subnet addresses for the /28 subnets. The first possible subnet is subnet 0 (all zeros in the subnet part of the address), which historically has not been used as it is impossible to distinguish between the address of this subnet and the network address itself. However, when network addresses space is scarce, as it often is when VLSM is used, it is permissible to use the all zeros subnet and the all ones subnet. We therefore can allocate the subnetwork address for LAN A to be 192.5.8.0/27.

We can similarly use subnet 2 for LAN C, which also requires 30 host addresses. The subnet address for LAN C can therefore be 192.5.8.32/27. We will leave the next two subnets spare for growth.

Table 7.9 shows the /27 subnets used for the larger LANs.

Table 7.9: /27 Subnets for Subnet design example 2

LAN	4th byte	Subnetwork address	First host address	Last host address
A	000XXXXX	192.5.8.0/27	192.5.8.1	192.5.8.30
C	001XXXXX	192.5.8.32/27	192.5.8.33	192.5.8.62
Spare	010XXXXX	192.5.8.64/27	192.5.8.65	192.5.8.94
Spare	011XXXXX	192.5.8.96/27	192.5.8.97	192.5.8.126

The next available subnet will be used by LAN B and will be configured to support 14 hosts. This subnet will be 192.5.8.128/28. The next available subnet 192.158.144/28 will be used for LAN D and will also support up to 14 hosts. The next three subnets will be the same size and will be spare.

Table 7.10 shows the /28 subnets used for the smaller LANs.

Table 7.10: /28 Subnets for Subnet design example 2

LAN	4th byte	Subnetwork address	First host address	Last host address
B	1000XXXX	192.5.8.128/28	192.5.8.129	192.5.8.142
D	1001XXXX	192.5.8.144/28	192.5.8.145	192.5.8.158
Spare	1010XXXX	192.5.8.160/28	192.5.8.161	192.5.8.174
Spare	1011XXXX	192.5.8.176/28	192.5.8.177	192.5.8.190
Spare	1100XXXX	192.5.8.192/28	192.5.8.193	192.5.8.206

The remaining subnets will be used for point-to-point circuits and need to support just two host addresses for each subnet which are the addresses of the router ports to which the circuit is connected.

Table 7.11 shows the /30 subnetworks used for the point-to-point WAN circuits.

Table 7.11: /30 Subnets for Subnet design example 2

Circuit	4th byte	Subnetwork address	First host address	Last host address
1	110100XX	192.5.8.208/30	192.5.8.209	192.5.8.210
2	110101XX	192.5.8.212/30	192.5.8.213	192.5.8.214
3	110110XX	192.5.8.216/30	192.5.8.217	192.5.8.218
4	110111XX	192.5.8.220/30	192.5.8.221	192.5.8.222
5	111000XX	192.5.8.224/30	192.5.8.225	192.5.8.226
6	111001XX	192.5.8.228/30	192.5.8.229	192.5.8.230
Spare	111010XX	192.5.8.232/30	192.5.8.233	192.5.8.234
Spare	111011XX	192.5.8.236/30	192.5.8.237	192.5.8.238
Spare	111100XX	192.5.8.240/30	192.5.8.241	192.5.8.242
Spare	111101XX	192.5.8.244/30	192.5.8.245	192.5.8.246
Spare	111110XX	192.5.8.248/30	192.5.8.249	192.5.8.250
Spare	111111XX	192.5.8.252/30	192.5.8.253	192.5.8.254

7.2.6 Network management design

The design for network management should include the following:

- Network management system: the designer should select an appropriate network management system that can be used for network configuration, real-time status monitoring, performance monitoring, usage monitoring, alarm handling and fault tracking. This can be integrated into a single system, or some of these functions can be implemented in separate systems.
- Devices: the designer should make sure that all devices acquired have the correct network management agent software.
- Network management protocols: for SNMP[16] the designer must define all the objects to be contained in the Management Information Base (MIB).[17]
- Remote monitors: the designer should decide on the systems to be deployed on each LAN to provide remote monitoring of LAN traffic.
- Test equipment: the designer should evaluate and select appropriate test equipment for testing and diagnosing faults on the network.
- Security: the designer should select appropriate security devices for authentication and authorisation and should design packet filters for firewall routers and include demilitarised zones (that contain publicly accessible servers), proxy servers and intrusion detection systems within the design, if appropriate.

All of the above network management equipment and software should be selected on the basis of cost, functionality, compatibility with other systems. Account may also be taken of the existing management systems and the skills and training of the staff.

7.2.7 Design testing

It is important that potential designs are tested throughout the design process. It is impossible to build a test network that can simulate the customer's real network running applications. But some types of testing are still possible:

[16] *See Section 8.7.3 in this volume.*

[17] *See Section 8.7.3 in this volume.*

- Network simulations: designers can run software simulations of designs for the network, using commercial tools, such Opnet and Comnet and freeware tools, such as NS.
- Pilots: small networks or small parts of larger networks can be tested in a laboratory containing a few LAN segments or a simple WAN topology can be tested for simple functionality and connectivity using real network equipment. Sensitivity tests can be carried out by failing one or more links and verifying that the network recovers and measuring the time it takes to recover. This type of testing is relatively cheap and well worth carrying out as discovering a fixing a problem at the design stage is much cheaper than discovering and fixing a problem at the implementation stage.
- Prototypes: critical parts of larger network can be tested in a laboratory using real equipment and traffic simulators, which can generate floods of traffic that will emulate the applications to test complex functionality, connectivity, applications and routing. The testing will be of a subset of the whole design involving both WAN and LAN components. This type of testing is very expensive and only needs to be carried out if the customer requires proof that the design will work.

7.3 Design document

The design document should be a dynamic document built up throughout the design process, but at this stage it should be finalised and agreed. Information should, wherever possible, be presented graphically on maps. The design document should contain the following sections:

- Executive summary: should be aimed at the non-technical decision makers who may not have the time or the technical understanding to read through the design. It should describe the purpose of the document and the design and contain a list of strategic recommendations, the benefits of the solution (related to the customer's business objectives) and a description of how it meets the customer's requirements. An outline timescale and overall cost should also be provided.
- Design requirements: should include a description of the existing network and its health and a description of current applications. It should also contain a complete definition of the requirements obtained during the requirements analysis, including business requirements, constraints and application, security, performance and management requirements.
- Design solution: should contain sufficient detailed information for a project manager to prepare a project plan and be able to purchase all the equipment, software and network services required by the design, and for implementers to be able to install and configure all of the equipment and software correctly. This section should also contain a top-level breakdown of the cost, together with any predicted savings that the new design offers.
- Summary: should be a concise technical summary of the solution and how it meets the requirements and its main benefits. It should also include an implementation strategy.
- Appendices: should contain all the details of the design. The appendices should include the following:
  - contacts
  - detailed timescales
  - addressing schemes
  - equipment details
  - circuit details

- network Management System details
- training requirements
- test results
- detailed costs.

7.4 Approval

New or upgraded networks require the investment of large sums of capital. In an enterprise there are many competing demands on capital and a process is required for senior management to evaluate and decide on investment proposals. This process usually involves the preparation and presentation of a business case. Once design and costing is complete, a business case must be made for senior management approval and the benefits of the network investment must be sold to them.

The format of the business case will vary from enterprise to enterprise, but there are a few key principles that should be followed.

Firstly, senior managers are not normally interested in technical detail, but they are interested in how proposals meet business requirements. The language of the business case and any presentation must use business terminology and not technical jargon.

Secondly, senior managers do not have the time to study proposals in great detail. They need to see an executive summary which should be the first section of the business case that contains the essential details of the case, in business terms, and should focus on the business benefits. The case for network investment may well be related to the development of a new application, in which case it should be part of the case for investing in the development of the application and the business benefits that the application provides should be used to justify the network investment.

Thirdly, senior management should be made aware of the negative consequences of not accepting the proposal. It may be useful to include charts showing the trends in the growth of traffic growth and the consequences on response times. The proposal may provide better reliability for a business-critical application, in which case the consequences and costs of network failure should be stressed.

Finally, the case should aim to convince the senior managers that the proposal represents good value for money and that the best possible prices have been obtained to meet the enterprise’s business requirements.

7.5 Network implementation

Implementation is not strictly part of the design process, but it follows on from it, and without an implementation the design activity would be pointless. It is therefore appropriate to discuss it in this chapter. Once the proposed network has been approved by senior management, a project team should be established and a project manager appointed. The project team should include the following people:

- the project manager and any assistants
- an implementation manager who is the line manager or member of the installation staff
- the designer
- a user representative
- a representative from the support/helpdesk function.

For larger projects it may also be necessary to include purchasing, logistics, legal and finance specialists. It is also advisable for any project to have a senior manager, who will champion the projects, but will probably not be involved in the day to day management of the project, but will be able to iron out any difficulties with other senior managers.

The project manager must produce a project plan showing all the tasks necessary to complete the project and all the dependencies between tasks. The plan should show the earliest and latest possible completion dates for each task and should indicate the person who is responsible for completing the task on time. The tasks should include all purchasing, installation, testing, training and documentation activities. There are a number of approaches that can be followed when cutting over to the network. These approaches are:

- A pilot implementation, where the network is implemented for a small group of users in a limited location. This cautious approach is not always possible for a network, as it may be the case that the one particular group of users cannot be segregated in this way.
- A parallel implementation, where the new network is run alongside the old network for a period of time. This is also a cautious approach and it is not always possible to follow it, as the new network may be using some of the equipment or circuits used by the old network. Where it is possible it is an expensive approach to implementation as resources are duplicated and have to paid for while the two networks are running alongside each other.
- A chronological implementation, where different applications or functions are introduced onto the new network one at a time over a period. It is a relatively cautious approach and requires the dual running of the old and new network and is therefore not always possible but it is always expensive, due to the duplication of resources.
- A phased implementation, where different parts of the network (a whole site or a region for instance) are cut over to the new network at different times. This is a less cautious approach that does not require duplication of resources, unless it is combined with one of the other approaches above. It is less expensive, as the new network can be provided as and when it is needed in each location.
- A big bang approach, where all sites and applications cut over to the new network at the same time. This is certainly the most risky approach, and it is a brave project manager who attempts it. The old network is closed down and the new network brought up usually over a weekend (or preferably a weekend followed or preceded by a public holiday) and, if all goes well, the users are up and running on the network on the first working day after the implementation. It is the cheapest approach, providing it goes smoothly, as it requires no duplication of resources and the benefits of the new network are achieved everywhere at the earliest time. But if things go wrong, it could be catastrophic and could result in major expenditure to fix problems and possibly a severe loss of reputation and even customers, if the enterprise cannot function because no network is available. With the big bang approach, it is advisable to have a contingency plan to revert back to the old network, if there is a major problem.

Once the implementation is complete, a user acceptance test is carried out, either by users or by the project implementation team whose tests are observed by user representatives. If the criteria established for the acceptance test is met, then responsibility for the network is handed over from the project team to the operational staff. This is often described as the project going live or being handed over into maintenance.

The project should be reviewed immediately after the implementation to ensure that so that lessons are learnt from the experience and are documented. A full review of the success of the project and how it has met the business objectives should take place within six to 12 months of the handover.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. In most countries, it is a legal requirement to use plenum cable in overhead and under-floor cavities as they non-flammable.

ii. Layer 3 switches are always hardware-based and they perform the same routing functions as a router, but they are easier to configure, as they do not support WAN interfaces.

iii. A business case should focus on all the technical advantages of a proposed network design.

iv. The big bang approach to network implementation is the cheapest, if it succeeds, but is the riskiest of all the approaches.

(b) Compare the advantages and disadvantages of internetworking with Layer 2 switches against those of Routers.

(c) A company has four offices in different parts of the country. It is required that capacity be provided to allow for five voice calls between each pair of offices at any one time. Data requirements are that capacity must be provided to enable 128 kbit/s to be transmitted between each pair of offices at any one time. Low and constant delays are required for one of the applications. Although both data and voice traffic are busiest mid-morning, there are significant levels of traffic throughout the working day. A reliable network is critical to the company's business, although cost is also an important factor.

The design options you should consider are:

i. A managed solution using PSTN for voice and Frame Relay for data with each site having separate access circuits to the PSTN and the Frame Relay network.

ii. An integrated Internet based solution using Voice over IP with a dual access circuit to an ISP from each site.

iii. An integrated Time Division Multiplexed solution using private circuits between each office to carry both the voice and the data.

iv. An integrated managed ATM solution with dual access circuits to each site.

State which of the above design options best suits the customer requirements, giving your reasons for choosing this design and rejecting the other designs.

(d) Design a subnetwork addressing scheme for a network, with the network address 200.3.4.0, so that it can support four subnetworks of up to 30 hosts, six subnetworks of up to 14 hosts and eight point-to-point WAN circuits. List all the subnetwork addresses in dotted decimal form with prefix notation.

(e) Describe three different ways by which a design can be tested.

Learning outcomes

At the end of this chapter, you should be able to:

- describe the four measurable criteria used to evaluate network designs.
- describe the Request for Proposal process and outline the contents of a typical RFP.
- describe the process followed in the various steps of traditional network design and the outline the deliverables of each stage.
- assess various options available for LAN designs and select an appropriate option to meet given requirements, providing reasons for choosing the option.
- assess various options available for WAN designs and select an appropriate option to meet given requirements, providing reasons for choosing the option.
- design a subnetwork addressing scheme, including Variable Length Subnet Masking schemes, given a set of requirements.
- outline the typical contents of a network design document.
- describe the building block design methodology.
- describe the approaches available for implementing a new network design and the advantages and risks of each approach.

Notes

Chapter 8: Network management

Further reading

Canavan, John E. *Fundamentals of Network Security.* (Artech House) first edition, 2001. Chapters 1,2.

Carr and Snyder *Management of Telecommunications.* (McGraw Hill), second edition, 2003. Chapter 12.

Fitzgerald and Dennis *Business Data Communications and Networking.* (John Wiley & Sons), eighth edition, 2005. Chapters 11, 13.

Kurose and Ross *Computer Networking – A Top Down Approach featuring the Internet.* (Addison Wesley), third Edition, 2005. Chapters 8, 9.

Stallings, *William Data and Computer Communications.* (Prentice Hall International), seventh edition, 2003. Chapters 20.1, 22.3.

In this chapter, we will examine aspects of network management. Fitzgerald and Dennis[1] define network management as the process of operating, monitoring and controlling the network to ensure it works as intended and provides value to its users. Network management is a major factor in both the design and operation of a network. It also is a major cost element and has a huge impact on the performance (measured and perceived) of the network.

Firstly we will examine the responsibilities of the network manager, the importance of network management to the enterprise, and the necessity of proactive planning rather than reactive fire-fighting.

Then we will structure our consideration of network management using the **ISO Management Framework**[2], which forms part of the ISO OSI Reference Model[3]. The headings we will use are fault management, configuration management, accounting management, **performance management** and security management. Of these we will spend most time with performance and security management, as these aspects of network management are probably the main concerns of network managers today.

We will then look at some network management standards such as TMN and CMIP, but we will concentrate on SNMP which has become the de-facto standard for network management.

Finally, we shall look briefly at the Network Management Systems that support the network management function within enterprises.

8.1 Network manager’s responsibilities

A network manager is responsible for all aspects of the operation of the enterprise network. According to Fitzgerald and Dennis, the responsibilities and tasks of a network manager include:

- day-to-day operational management of the network
- supporting network users
- ensuring the network is operating reliably
- evaluating and acquiring network hardware, software and services
- managing the network technical staff
- managing the network budget with emphasis on controlling costs
- developing a strategic (long-term) and integrated networking and voice communications plan to meet enterprise’s policies and goals

[1] *Fitzgerald and Dennis, p.447.*

[2] *IS 7489-4, ‘Information Processing Systems – Open Systems Interconnection, Basic Reference Model, Part 4 – Management Framework’.*

[3] *It should be noted that ISO considers network management to reside in the application layer. Other architectures, such as ATM, regard management as occupying a totally separate plane to the user protocol layers.*

- keeping abreast of latest technological developments
- assisting senior management in understanding the business implications of network decisions and the role of the network in business operations.

Network management involves a wide ranging set of activities. The network manager has considerable responsibility. In many enterprises today, the business cannot function without its network, and the network manager therefore controls a resource that is critical to the success of the enterprise. The network manager usually has a number of staff who are located in a **Network Management Centre** (**NMC**) alongside sophisticated **Network Management Systems** (**NMSs**), test equipment and other tools that help the network management staff carry out their functions.

It should ideally be about planning and organising to predict and prevent problems. So often, it can easily become a fire-fighting activity, where network managers spend all of their time responding to and being controlled by events, and consequently have little time to plan and organise to predict and prevent problems. They can easily be caught up in a viscious circle of dealing with continuous immediate problems.

8.2 Fault management

Fault management is concerned with the detection, notification, isolation and correction of network faults.

8.2.1 Fault detection

Fault detection is an activity that continually monitors network devices and checks that they are functioning correctly. This can be done by a network management system regularly polling network devices to establish their status, or it can be done by processes within the devices monitoring components within the device to check that they are functioning correctly.

8.2.2 Fault notification

Once a fault has been detected, it must be reported. Where a monitoring process within a device detects a fault, it must generate an alarm message and forward it to a network management system. Where a parameter is being monitored to check that it does not exceed a threshold, the alarm generated is called a **trap**. If a network management system regularly polls devices and one fails to respond or responds with a value of a variable that is above a threshold, it must report this, in some way, along with any alarms or traps received from the monitoring process within network devices, to a network operator. At one time this was done by generating a text-based message that was written to an alarm log file and only appeared on a special monitor within the NMC, known as the network console. Sometimes these consoles would be inundated with messages and it was easy for an important message to be missed. Modern network management systems will process all this information and present it graphically, usually onto a network map, making use of different colours, flashing and sometimes even sound to bring an operator's attention to a fault.

Once an alarm has been reported, it needs to be investigated and resolved. One event, such as a circuit being disconnected could generate a number of separate alarms, from each end of the circuit and from the different protocol layers which are affected by the loss of the circuit. It is necessary to correlate these alarms, so that just one fault is investigated. This can be done manually, but it is best done by software at the NMC. The next stage is for a **trouble ticket** to be opened. The trouble ticket is used to record details of the fault and to track it through the various stages of resolution until the fault has been fixed and the trouble ticket closed. The trouble ticket can be created manually sometimes on a separate system, but many network management systems will integrate the trouble ticketing with the fault detection process. The trouble ticketing system will also be used to record faults reported by users, which can then often be correlated with those obtained from network monitoring.

Trouble tickets should contain the following fields:

- time and date of report
- name and telephone number of fault reporter
- time and date of the problem
- location of the problem
- nature of the problem
- why and how the problem happened
- who is responsible for fixing the problem
- the current status of the problem
- the priority of the problem
- notes about the diagnosis and all actions taken.

Trouble tickets are useful for:

- tracking a problem and ensuring it is being progressed
- ensuring that alarms and fault reports about the same problem are correlated
- prioritising of work, so that more serious faults receive attention first
- identifying the status and current owner of a problem
- producing performance reports on repair activities, particularly useful for measuring performance of suppliers
- post mortems where a serious problem is reviewed to see what lessons can be learned from it
- handovers between shifts at the NMC.

One of the main benefits derived from using trouble tickets, is that there is always a clear owner at each stage of the resolution and the ownership of the fault can be easily changed. Furthermore, all network management staff can access the same system and the owners can be presented with a prioritised list of faults they should progress. Most systems will require that trouble tickets are updated on a regular basis and if an update is missed, the owner of the fault will be notified. As an example, a fault may originally be received by a help desk operator who follows a procedure to make some rudimentary tests, but this procedure does not lead to a diagnosis of the fault, so the ownership is passed to first line technical support. If they cannot resolve the problem, it may be passed to an even higher skilled group in second-line support. The trouble ticketing system can also notify the NMC manager when the clearance time for a fault exceeds a threshold, who may then need to take an interest in the fault and find out why it is taking so long to resolve and, if necessary, commit more resource to it. This process is known as **escalation**. Trouble ticketing systems are a vital tool for network managers, and the data that they record is also extremely useful for performance monitoring of the fault management process itself, the various groups within the NMC and external suppliers.

8.2.3 Fault isolation

Fault isolation is the task of diagnosing the cause or location of a fault. It is a skilled task which requires a very good general knowledge of networking and of individual network products. The NMC staff can use a number of techniques in order to arrive at a diagnosis.

The aim of the first part of the process is to determine the next course of action to correct the fault or to progress the diagnosis. It will probably require some initial tests to be carried out remotely from the NMC. After this initial test, it may be necessary to dispatch a technician or even two technicians to different sites to carry out further on-site tests. But at this stage it is important to know the sites where they have to be dispatched and what skills and test equipment may be required.

At the NMC, the operator will have access to some test equipment and facilities. Firstly alarm logs can be examined and the network manager can also interrogate the status of devices and interfaces and various performance statistics using facilities within the network management system. The network manager can also use network test utilities such as ping and traceroute. Network operating systems, such as Windows NT and XP, have a number of network management applications that can be used to check LAN performance. **Remote Monitors** (**RMONs**) can be installed on shared LANs or embedded in hubs that are configured in promiscuous mode. They view all the frames on the LAN, recording traffic and utilisation statistics, as well as being able to record particular packet types for future analysis. It is also possible to embed RMONs in switches. Many network devices are able to record statistics on interfaces and protocols which can be examined remotely. Some devices, such as time division multiplexers, are able to loop a port and then generate a pseudorandom test pattern from another port to the looped port and back. Similar facilities can also be provided by intelligent patch panels. The data received can then be checked and an overall error rate can be calculated.

On-site testing requires the use of portable test equipment. These include:

- protocol analysers, which are able to record and analyse traffic on a LAN or WAN circuit and decode all the protocol headers at all layers
- cable analysers, which are able to test the characteristics (both analogue and digital) of the physical layer to ensure that it is within specification
- cable testers, which are able to test the physical connectivity of cables and ensure that different cable pairs have not been crossed, left open, or been looped or short circuited
- voltmeters, which can be used to measure voltages, electrical currents and the resistance of cables
- time domain reflectometers, which can be used to measure where along a length of cable a break has occurred
- breakout boxes, which can be used to view the electrical state on each pin of an interface – they also allow a different state to be forced onto a pin to attempt diagnose and resolve interface problems
- Bit Error Rate Testers, also known as BERT Testers, which will generate a pseudo-random bit test pattern which is sent down a channel that is looped so that the BERT Tester receives the pattern and can then compare it with the pattern that was sent to calculate the bit error rate.

Most network equipment is housed in racks and cables between equipment are connected via a **patch panel,** where a connecter on a cable connected to one device can be patched by a short patch cable to a connector on a cable connected to another device. The patch panel is a centralised flexibility point, where it is easy to unplug and reconnect a cable to connect to alternative equipment. It is also an ideal place to connect portable test equipment.

There are many potential causes of network faults. These include:

- exceeding media limitations
- interference
- wear and tear on cables and connectors
- congestion
- collisions
- inefficient protocols (broadcast storms)
- power supply problems
- telco circuit problems
- hardware overload
- poorly implemented protocol stacks (old implementations)
- garbage (e.g. rogue network interface cards)
- address resolution problems
- denial of service attacks
- internetworking problems.

8.2.4 Fault correction

There are many ways in which faults can be corrected. Firstly, there may be some temporary workaround that can be quickly implemented to restore service. Re-booting or reinitialising equipment will often fix a software fault. Many faults are caused by configuration errors which, once discovered, can easily be fixed. Some faults are caused by loose connectors or cards that are not correctly seated in equipment. Other faults will require the replacement of a cable or a piece of equipment or a card within the equipment. Finally, some faults can only be dealt with by third parties. Circuit faults must be reported to network operators and equipment faults are often reported to suppliers.

Fault correction will often require the dispatch of skilled technicians. Usually the technicians who were dispatched to carry out fault isolation can also resolve the problem, but they must have the right spares with them or have access to on-site spares, if any cables, equipment or cards need to be replaced.

8.2.5 End user support

End user support, is a network management function that is not completely covered by the ISO management framework but is partially covered by fault management. End user support includes the help desk function to which users report network problems. These problems may or may not be faults. Sometimes the user is not following a correct procedure or is having some finger trouble when entering commands. Such problems are not faults, but they still require resolution, usually in the form of some informal user education. The other aspect of end user support is training about the network and its facilities. This can either be formal classroom-based training or informal desk training.

The help desk function, which is often combined with the IT helpdesk function which should use the same trouble ticketing system as is used by the NMC, so that trouble tickets can be easily passed between the two. End user support should also include some technical support groups which also have access to the trouble ticketing system. In large enterprises, it is common to have at least two levels of technical support in addition to the help desk. The idea is that the majority of problems (about 75 – 85 per cent of problems) can be resolved by relatively unskilled staff at the help desk, who can follow well-documented procedures to take details of problems and to carry out some rudimentary diagnosis of faults. If the problem cannot be resolved by the help desk, they escalate it to first line technical support who are a more technically skilled and expensive resource. They should be able to resolve the vast majority of problems. There may also be a second-line technical support group consisting of very skilled people who are even more expensive to employ and retain, and who should be able to resolve most of the remaining problems. Finally, in large enterprises, it may be necessary to have a third-line technical support of technical experts, who are very expensive to employ and retain, and who only deal with very difficult problems. These people can resolve almost any problem. Often, third-line support is provided by the respective suppliers under maintenance contracts rather than an in-house group.

8.3 Configuration management

Configuration management is concerned with the monitoring, management and documentation of hardware and software configurations in network devices. This includes all configuration data held in the devices and details of all the hardware (serial numbers, card configurations and jumper settings, fault reporting contacts) and installed software (version numbers and license details for both applications and system software) as well as details of users, user groups and their access privileges and user login scripts.

Provisioning of new services and the installation or upgrading of circuits and devices is also part of configuration management.

Configuration management also includes the installation and upgrading of software on servers, PCs and network devices. This can be done manually with a CD ROM, or by electronic means using file transfer software or more sophisticated **Electronic Software Delivery** (**ESD**) systems such as IBM's Tivoli, Microsoft's Windows Installer or Novell's ZENworks. In order to run an ESD system, software has to be installed on each client device and on a server. The server software can then be instructed to download software to each client at specified times. This is often done overnight, but to do this PCs have to be left switched on overnight. ESD greatly reduces the cost of distributing and installing software on devices and as a bonus it also keeps accurate records of the software configuration on each device. ESD systems are proprietary and there are no standards agreed as yet.

Documentation is another important aspect of configuration management. People involved in fault isolation often need to be able to access configuration details, in order to diagnose faults. Similarly network designers and implementers need access to accurate configuration information, before they can design or implement any changes to the network. It is one of the tasks of configuration management to keep this information up-to-date. Because, configurations are constantly being changed, there is little point in attempting to keep paper records up-to-date. Instead, it is best to hold a single master configuration on-line that can be accessed from anywhere. Network management systems will support this and many systems are capable of automatically building such configuration information.

Configuration information is usually best displayed graphically. Devices can be selected from network maps which can be arranged in a hierarchy (core, region, area, site, LAN, device). Some proprietary network management systems can even follow this hierarchical graphical approach down to the card or port level and can even display the status of interface pins as coloured lights on a diagram of the interface connector. This is one of the advantages of using proprietary management systems to manage the equipment from the same supplier. To develop an open system that could display similar details from any device would be virtually impossible.

The NMC should also keep some paper documentation (which will also probably be available on-line). This will include manuals for each device on the network and each operating system and application as well as copies of protocol standards. Copies of all vendor contracts, maintenance agreements, software licenses should also be kept. A copy of a disaster recovery plan should be kept within the NMC and also at a back-up site, in case the NMC is inaccessible. The network manager should also keep copies of cost management information, such as annual budgets and finance reports on spending. Finally, copies of any legal requirements, such as data protection legislation and any health and safety requirements relevant to the network, should also be kept.

8.4 Accounting management

Accounting management concerns the measurement of resource usage for billing or cost apportionment and the setting of quotas for disk, printer and network usage. Some organisations, such as network operators, service providers and outsourcers are required to produce accurate bills, based on network usage. Also, in large groups of companies, the network is often owned by one subsidiary and it has to bill the other subsidiaries in the group for use of the network. Accurate billing is always required between two legal entities and is usually also subject to some form of taxation. In order to be able to bill network usage accurately, large quantities of data usually have to be collected and processed. Billing usually takes into account a combination of one or more of:

- access circuit speed data rates
- end-to-end data rates
- distance
- volumes of data transferred (packets or bytes)
- call minutes (often by time of day).

This activity can be quite a large overhead. In some networks, the application which uses the most network resource is the billing system. In corporate networks, which do not cover multiple companies, a simpler accounting scheme can be used. Most enterprises do not attempt to bill users based on accurate measurement of network usage. Instead they attempt to apportion the costs of running the network approximately but fairly to departments, product lines, projects or sites of the network, which are known as profit or cost centres, depending on whether they are targeted to make a profit or just to control costs. No bills are produced or paid. Instead there is an internal accounting transfer between the various profit and cost centres and the network cost centre. Apportionment is often based on a simple parameter. If there is only one profit/cost centre per site, it could be done on the basis of the access circuit data rate. If there is more than one profit/cost centre per site, it could be done on the basis of headcount or the number of PCs and/or telephones that belong to the profit/cost centre.

Even when there is no requirement for accurate billing information, it is still desirable to monitor network usage. This is needed to ensure that one group of users does not over-burden the network at the expense of others and to discover any inefficient or unnecessary use of the network. Furthermore, network design can be improved if more is known about the usage of the network.

A further responsibility of a network manager is cost management, which concerns the control (or reduction) of costs. This is not addressed in the ISO management framework, but it is associated with accounting management. The network manager must seek not only to recover the costs of running the network from the users, but he also has a responsibility to keep these costs as low as possible. This is done in conjunction with the network designers by selecting technologies and products from suppliers that provide good value for money. But these days the costs of circuits and equipment are less than the people costs required to manage and support the network and there is sometimes a trade-off between the two whereby people costs can be saved by investing in technology. The network manager must also control costs by running an organisation that is as efficient as possible.

In the LAN environment, a useful measure of cost is the **Total Cost of Ownership** (**TCO**) of a client computer, which can be calculated by dividing the total amount spent per year on hardware, software, maintenance, network management, training and support by the number of client computers. Some calculations of TCO also include a measure of the time wasted by users due to problems. TCO will often be about five times the cost of purchasing the computer, and TCO is the amount spent per year. So, over the typical lifetime of a PC, of three years, the TCO can be about 15 times the purchase price. In analysing TCO, it is management and end user support that dominate the other costs. Staff time is thus the largest contributor to TCO and the network manager must do everything in his power to keep people costs under control, without jeopardising the service that is being provided.

To reduce staff costs, the network manager should consider using a small number of standard builds for PCs, automating software installation with ESD, buying PCs with software pre-installed by the supplier, centralising the help desk function and moving to a thin client architecture. For wide area networks, network managers should maintain a good network inventory which can be used to check all bills, agree best price long-term contracts with benchmarking clauses, so that prices can be adjusted. It is also worth filtering undesirable traffic such as video streaming and MP3 downloads and to integrate voice, data and video services as much as possible (in future as far as the desktop).

8.5 Performance management

Performance management is concerned with the collection, processing and reporting of performance data and the maintenance of required levels of performance. There are many different types of performance data that are of interest to network managers. The main ones are those which provide measurements that relate to the main perceptions that users have of network performance. These are delay, jitter and throughput. There are other important measurements that effect these, such as utilisation and error rates, and further measurements relating to network reliability. The aim of performance management is to ensure that the network is operating as efficiently as possible and this achieved by monitoring performance, so that there are some objective measures of performance that can be regularly analysed, and taking action to control performance following this analysis, so that desired levels of service are maintained. On small networks, the extraction of performance data from devices and the processing and reporting functions can be done manually, but on larger networks the process must be automated.

Performance data is normally recorded and stored within network devices. The host can collect performance data on all protocol layers, but network managers are usually most interested in data regarding the transport, network and data link layers. Routers and layer 3 switches will collect data about the network and data link layers and layer 2 switches and hubs will only collect data about the data link layer. In addition to this information, for shared LANs, Remote Monitors (RMONs) can also collect useful performance data.

The performance data stored in these devices has to be collected on a regular basis via a network management system which then has powerful facilities for processing the performance data and producing useful graphical reports showing many aspects of network performance. Network management systems that have this capability include HL OpenView, SUN NetManager and Cisco Works. The former two are open platforms, but the latter is proprietary and is designed for use with Cisco routers and switches. The format of the reports produced by these systems are very flexible and can be easily customised to suit particular needs. In addition to regular performance reporting, there is also a need to detect urgent performance problems as and when they occur. This is done by setting traps that generate a message to the NMC whenever a performance threshold, such as an error rate, is exceeded. Traps use a fault management mechanism to report performance problems to the NMC and they will be treated like faults, but they are subtly different from faults. They usually result in a degradation of service rather than a complete loss of service and it is often a difficult decision as to whether or when to report these problems to suppliers. Performance problems with circuits are particularly difficult. An error rate slightly above normal often indicates that there is a problem on the circuit that will likely get worse over time and that also could cause a sudden total failure of the circuit. Reporting the problem to the network operator will be disruptive as the network operator may want to take the circuit into maintenance, where it will be looped and subjected to a lengthy bit error rate test. To do this the circuit will be out of action for some time and the network manager might decide that it is better to soldier on with the performance problem than to disrupt service. Then it can be handed over for a maintenance at a more convenient time.

When a performance report indicates a trend that could result in a problem, the network manager must take some action. In some situations it is relatively easy to upgrade data rates or memory within equipment to bring performance back on target. In other cases it may be necessary to carry out a thorough re-design. In the meantime, performance problems can often be alleviated by prioritising certain types of traffic or even discarding undesirable types of traffic. Real-time performance alarms must be treated and prioritised in a similar way as faults.

Regular (daily, weekly and monthly) performance reports should be produced that include reports on circuit and LAN utilisation, response times (both over data links and end-to-end), error rates at all layers, retransmission rates (over data links and transport connections), distributions of traffic by time of day and location and network availability. Other information on the performance of individual devices or on the performance of a supplier should be obtainable by a query, as and when needed.

Another benefit of regular performance reporting is that the network manager will have a clear objective view of the normal performance of the network and its components. This is the baseline performance, which we referred to in the last chapter. Designers must know the baseline performance of a network before commencing design work and the performance after the design has been implemented should be compared with the baseline.

As we have seen above, the line between fault and performance management can be somewhat blurred. In general, performance management is proactive and is mainly concerned with historical statistics and is a long-term non-urgent background activity, while fault management is reactive and is mainly concerned with real-time status and is short-term urgent activity.

8.5.1 Network reliability

Of all the performance measurements that we have looked at, the most important as far as users is concerned are those that measure network reliability. Most users would prefer a heavily degraded service to one that does not work at all. Network managers need a numerical measure of reliability. The most common measurement is **availability**. Availability can be measured for each individual network component such as a network device or a circuit, or it can be measured for an end-to-end connection or service. Frequently, an overall average of all end-to-end availabilities is calculated. This is known as the network availability.

Availability is a simple ratio between uptime (the length of time over a period for which the component is functioning properly) and total time (which is often one year but could be any period). Availability is often expressed as a percentage, and uptime and total time must be measured in the same units, usually hours.

Equation 1a, 1b, 1c: Formulae relating availability to uptime, downtime and total time

$$\text{Availability} = \frac{\text{Uptime}}{\text{Total Time}} = \frac{\text{Uptime}}{\text{Uptime + Downtime}} = \frac{\text{Total time - Downtime}}{\text{Total time}}$$

Before looking at an example we will consider what contributes to downtime which it total time minus uptime. Downtime is usually measured as an average over a long period or over many similar components, because any one loss of service has little statistical significance. The average period of Downtime is known as the **Mean Time to Repair** (**MTTR**) and this can be regarded as having three components. **Mean Time to Diagnose** (**MTTD**) is the time taken from the detection or reporting of a fault until the cause of the fault has been diagnosed. **Mean Time to Respond** (**MTTResp**) is the time taken between the fault being diagnosed and the start of fault correction. MTTResp often represents the time it takes for a dispatched technician to get to a site. Finally. **Mean Time to Fix** (**MTTF**) is the average time it takes to correct a fault, once corrective action has commenced. Mathematically,

Equation 2: Formula relating MTTR to MTTD, MTTResp and MTTF

$$\text{MTTR} = \text{MTTD} + \text{MTTResp} + \text{MTTF}$$

The **Mean Time Between Failures** (**MTBF**) of a component is the average time the component operates before it fails. It is a measure of the expected reliability of a component. It can be statistically based from a large sample of components or it can be calculated theoretically.

Availability, MTBF and MTTR are related to each other in the following equation:

Equation 3: Formula relating availability to MTBF and MTTR

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Also, the following formulae can be useful:

Equation 4a, 4b, 4c: Formulae relating failures to MTBF and MTTR

The expected number of failures in a given period

$$= \frac{\text{Length of period}}{\text{MTBF} + \text{MTTR}} = \frac{\text{Expected uptime in period}}{\text{MTBF}} = \frac{\text{Expected downtime in period}}{\text{MTTR}}$$

Finally, we shall look at what happens, as is often the case in networking, when several components are connected in series and the failure of any one component will cause the service to fail. The availability of a component can be thought of as the probability that the component is up at any random time. If a network service depends on several components in series then, assuming they can only fail independently of each other, the probability that the overall service will fail can be found by multiplying the component availabilities together.

For components connected in series:

Equation 5: Overall availability of components connected in series

Overall availability = Π (individual component availabilities)[4]

The overall availability of a service comprising two components in series is significantly less than the availability of the individual components that make up the service.

Where components are connected in parallel, so that one component backs up another one and the service will only fail if both components fail at the same time, the overall availability is given by:

For components connected in parallel:

Equation 6: Overall availability of components connected in parallel

Overall availability = 1 - Π (1 - individual component availabilities)

To derive this, calculate the probability of the service being down (i.e. both components being down at the same time) and then take this from 1 to obtain the probability of the service being up.

The overall availability of a service comprising two components in parallel is significantly higher than the availability of the individual components that make up the service. This equation is only true if the failure of the one component is independent of the failure of the other component. In cases where a single common failure will cause both components to fail, as would be the case with two circuits that are not completely diverse and perhaps share a common duct at some point or are not completely separate and are routed through the same network node, this equation will not necessarily hold.

Example 1

A circuit has an availability of 99.6%. Calculate the number of hours of circuit downtime that could be expected over a 1 year period and hence or otherwise calculate the MTBF of the circuit, if the MTTR is 16 hours.

[4] *The Π symbol denotes that all the individual component availabilities are multiplied together.*

Expected downtime per year = (1-0.996) x 365.25 x 24

= 0.004 x 365.25 x 24

= 35.064 hours

If MTTR is 16 hours, using Equation 4c,

Expected no of failures in 1 year = 35.064/16

= 2.1915

From Equation 4a,

MTBF = Expected Uptime/ Expected no of Failures = (365.25x24 – 35.064)/2.1915

= (8766 – 35.064)/2.1915

= 8730.936/2.1915

= 3984 hours = 166 days

Alternatively, the last part of the answer could be calculated directly with a little algebra and Equation 3, where M is the MTBF.

Availability = MTBF / (MTBF + MTTR)

0996 = M/(M + 16)

0.996 (M + 16) = M

M = 0.996M + 15.936

M – 0.996M = 15.936

0.004M = 15.936

M = 15.936/0.004

= 3984 hours = 166 days

Example 2

An optical fibre circuit comprises two long segments of fibre connected to each other via a single repeater. The availability of each segment is 99.98% and the availability of the repeater is 99.99%. Calculate the availability of the whole optical fibre circuit.

Using Equation 5,

Availability of circuit = 0.9998 x 0.9999 x 0.9998

= 0.9995

= 99.95%

Example 3

A communications service between two sites consists of a multiplexer at each site, each with an availability of 99.95%, and two separately routed private circuits, each having an availability of 99.8%. Calculate the overall availability of service between the two sites.

Using Equation 6,

Overall circuit availability $= 1 – (1 – 0.998)^2$

$= 1 – (0.002)^2$

= 1 – 0.00004

= 0.999996 = 99.9996%

Using Equation 5,

Overall service availability = 0.9995 x 0.999996 x 0.9995

= 0.998996 = 99.9%

Activity 8.1

Using a spreadsheet, calculate what each availability means in terms of downtime per year in both hours and minutes, for the 9 availabilities between 99.999% and 99.991%, the 9 availabilities between 99.99% and 99.91% and the 10 availabilities between 99.9% and 99.0%.

Activity 8.2

Using a spreadsheet, format four cells as percentages with 4 places of decimal. In the first two cells enter two component availabilities. In the next two cells enter the formulae from Equations 5 and 6, so that the overall availability of the service can be calculated if the components are connected in series and in parallel. Experiment with some different values of component availabilities and notice the effect on the two overall availabilities.

8.6 Security management

Security management concerns the control of access to network resources to prevent unauthorised users from gaining access to these resources and the data that they are holding or carrying. Security management requires that network resources are partitioned for security purposes and access to these resources is granted to authorised users and denied to others. The aim is to protect the network and data from being damaged by accident, incompetence, malicious damage (or alteration) and natural disasters. Specifically, it aims to guarantee data integrity, data availability and data confidentiality, using techniques such as authentication and authorisation. There is a need to balance the cost of security against the value of the assets being protected, the cost of security against the cost of a security breach, the probable against the possible and business needs against security needs. Security is essentially a management problem rather than a technical problem, although the technical aspects are obviously important.

Security management involves the assessment of threats, the identification of vulnerabilities and defence against attacks.

8.6.1 Threats

A **threat** is anything (natural, accidental or deliberate) that can disrupt the operation, functioning, integrity or availability of a system.

Viruses are executable programs that intend to create an unwanted event (harmless or destructive) and can propagate themselves by multiplying, often making use of email address books. Viruses needs to be carried within another program, or the boot sector of a floppy disk or as a macro within a document, and they pose the most serious threat to network security. They can also modify themselves as they multiply in an attempt to avoid detection.

Contrary to popular belief, the external hacker does not present as big a threat to security as an internal hacker. A disgruntled or even an incompetent employee poses a bigger threat to security than an external hacker.

Security threats can be classified into those that result in disruption, destruction or disaster and those concerned with unauthorised access.

8.6.2 Vulnerabilities

A **vulnerability** is an inherent weakness in the design, configuration, implementation or management of a network or system that renders it susceptible to a threat.

There are many vulnerabilities associated with security holes in all operating systems that hackers can use to attack systems. A number of vulnerabilities occur when data containing executable code is sent to a system which causes buffers to overflow. This code can then be executed which could then permit future security breaches.

Once a security hole is identified, the software developers are informed and they produce a patch that closes the security hole. It is important that network managers keep all their software up-to-date with the latest patches.

Vulnerabilities are notified by software suppliers, but they are also notified on a web site run by Carnegie Mellon University known as the CERT Coordination Center (CERT/CC). Information on vulnerabilities is now the responsibility of US-CERT (US Computer Emergency Readiness Team), a partner of CERT, which is actually part of the US Department of Homeland Security and whose main concern is defence against cyber-terrorism.

Activity 8.3

Visit the CERT/CC web site (www.cert.org) and look at some US-CERT Advisory and Incident Notes and some Vulnerability Notes. Also view the CERT Statistics on vulnerabilities and incidents reported and Vulnerability Notes published. Also visit the US-CERT web site (www.us-cert.gov) and look at Government Users and the statistics on incidents that have been reported.

8.6.3 Attacks

An **attack** is a specific technique that is used to exploit a vulnerability.

Attacks can be passive or active. With passive attacks there is no overt activity that can be monitored or detected. This type of attack includes the monitoring and recording of data, to eavesdrop or analyse traffic using packet sniffers. An active attack employs more overt methods, and hence is easier to detect, but is much more dangerous, as data can be altered or deleted. They usually involve the unauthorised altering, deletion or delaying of data or control signals and/or the masquerading of identities to circumvent security, to cloak the source of the attack or to deceive network users. There are many different types of active attack, the most common being the virus and the denial of service attack, which involve flooding a host site with so many unwanted packets that legitimate users are denied service.

Activity 8.4

From textbooks or using a search engine to find appropriate web sites, read about the following types of security attack and the means by which they can be controlled:

- viruses
- worms
- Trojan horses
- trap doors
- logic bombs
- port scanning
- spoofs
- DNS spoofs
- replay attacks
- password cracking
- social engineering
- sniffing
- web site defacement
- denial of service attacks
- bot attacks
- phishing and pharming.

8.6.4 Risk management

In order to formulate a security policy, the enterprise must assess the risks associated with various security threats. The basic steps in doing this are to identify and proritise the assets that need protection, identify vulnerabilities, identify threats and their probabilities, identify controls to reduce or eliminate the threats, carry out a cost benefit analysis and implement the necessary controls within the security policy.

Controls are mechanisms that reduce or eliminate threats to network security. John E. Canavan describes a security trinity to control security threats. The trinity consists of detection, prevention and response. Defence against attacks requires the development of controls for the three elements of the security trinity. **Intrusion Detection Systems** (**IDS**) and virus checking are examples of detective controls. Firewall routers, proxy servers, authentication servers, redundant equipment and halon fire protection systems are examples of preventative controls. Quarantining of detected viruses, disaster recovery plans, and closing security holes are examples of responsive controls. The controls can be located anywhere within the network.

Fitzgerald and Dennis[5] suggests that the risk assessment process is best managed through a control spreadsheet that lists the network assets in priority order vertically and the threats horizontally. As controls for each threat are determined, they are referenced in the cells of the spreadsheet.

8.6.4.1 Controlling disruption, destruction and disaster

To prevent or reduce the impact of disruption, destruction and disaster, there must be redundancy. This can include, spare equipment, circuits, fault tolerant servers, disk mirroring and duplexing and uninterruptible power supplies.

Controls for disruption and destruction are usually covered by the controls necessary to prevent unauthorised access. If these are working effectively there is little opportunity for disruption and destruction, unless it is caused by authenticated individuals who have the appropriate authority.

For disasters, the best means of control is to design the network and computer systems so that they are decentralised. Following the analysis of the risks of disaster, the enterprise must also develop and regularly test a disaster recover plan which should address various levels of response to a number of possible disasters. The plan should provide for the recovery of data, application software, network components and whole sites where they are critical to the enterprise.

Most enterprises will have a two level disaster recovery plan. At the first level will be procedures to recover from a minor disaster perhaps involving the loss of major server or a part of the network. At the second level will be procedures to handle the loss of a whole computer centre. This will involve the setting up of a fall-back centre with duplicate systems and network access. This can be provided by and used exclusively by the enterprise or it can be provided by a third party disaster recovery firm and shared with other potential users. Where managed network services such as frame relay and ATM are used, the disaster recovery centre can have the same size access circuit as the main centre and PVCs can be reconfigured.

8.6.4.2 Controlling unauthorised access

Controls to prevent unauthorised access include authentication and authorisation and deploying IDSs. Authentication is usually carried out by ensuring that all network users prove their identity by means of something they know (such as passwords, memorable names or dates), something they have (such as tokens, keys or cards that generate pseudorandom numbers) or

[5] *Fitzgerald and Dennis, pp.365–366.*

something they are (such as fingerprints, retina scans or voice recognition) or a combination of the above. Another form of authentication is the use of digital certificates, which use public key encryption techniques to prove the identity of users by his knowledge of their private keys. Authorisation is provided by defining user profiles and allowing access to certain resources to specified users and groups of users. IDSs constantly monitor the network for suspicious behaviour, such as unusual patterns of traffic or an excessive number of login attempts.

Network managers should make their networks secure from eavesdropping, by controls such as using shielded cables, locking equipment in cabinets and using encryption techniques.

Network managers must also keep abreast of vulnerabilities in operating systems and other software and always keep the versions up-to-date, so that known security holes are plugged. They should also not neglect physical security. They should ensure that all equipment racks and rooms are locked.

Finally, all network access points to the enterprise should be made secure. This means implementing **dial-back modems**, where users dial-in to the network over the PSTN and enter their user ID and password. The dial-back modem then hangs-up the call, looks up the user and dials them back on a telephone number that has been configured for them. Alternatively, with calling line identification enabled, the modem could be programmed to accept calls only from known numbers. For Internet access, a firewall router is essential with packet filters (access lists) defined to filter undesirable traffic. Application layer firewalls are also useful, where users access an intermediate host, and are possibly authenticated by this host, which then accesses the application. A proxy server is an example of an application layer firewall that accesses a web server.

Many enterprises set up a **De-Militarised Zone** (**DMZ**) between the firewall router and another an internal router. Within the DMZ are the enterprise's publicly accessible web servers, a public DNS server and a proxy server (possibly supporting NAT) to allow controlled access to internal servers.

Following risk analysis and after deciding which controls to implement to reduce the threats of unauthorised access, the network manager should develop a security policy to guide both network staff and end users. This policy should define the assets which are to be protected and the controls necessary to achieve this. The policy should be well publicised to all users of the network and any breaches of the policy should be dealt with forcefully.

Activity 8.6

Using a search engine enter the search term 'sample disaster recover plan' and visit some of the sites found to view a sample disaster recovery plan. Repeat this exercise with the term 'sample network security policy'.

8.7 Network management standards

At one time all network management systems were proprietary, and if equipment was acquired from multiple vendors, there would be multiple management stations, all with their own monitors sitting on network managers' desks. Worse still, there was no integration or sharing of data between these systems, which made fault diagnosis hard. This acted as a disincentive to build multi-vendor networks and hence users were often locked into a single supplier instead of being able to mix equipment from different suppliers and obtain the best prices. Different suppliers built sophisticated proprietary network management systems, such as IBM's NetView, that provided the desired level of integration, but users were then locked into the same supplier for all network purchases. The standards bodies realised that this was a serious problem and their efforts to produce open networking standards would be wasted if there was no open network management standard. Work only began on this in the 1980s, which was much later than the work on open networking standards. So far there have been three attempts to standardise network management from the ITU-T, ISO and the IETF.

8.7.1 Telecommunications Management Network (TMN)[6]

TMN is a pragmatic architectural approach to network management devised by the ITU-T and was specifically designed to meet the needs of the network operators who wanted to buy network equipment from different suppliers but manage the whole network from an integrated management system. It makes use of the ISO Common Network Management Protocol (CMIP) and the ISO Management Framework, but is essentially a useful architectural model that has been used by many of the network operators.

TMN has a Logical Layered Architecture. The top layer is the Business Management Layer which contains systems for high-level business planning. The next layer is the Service Management Layer which included the systems that focus on the services offered to customers. The next layer is the Network Management Layer that contains the systems that are used to monitor and control the network as a whole and the final layer is the Element Management Layer which contains the systems that manage different types of network devices, known as **Network Elements** (**NEs**).

TMN recognises that good proprietary management systems already exist for many of the devices that required integration, so instead of replacing all of these with a new management system, they defined a standard interface between their integrated NMS and these proprietary systems which are called **Element Management Systems** (**EMSs**). The EMS would manage NEs of the same type. The interface between the EMS and the NE would initially be proprietary, but it was hoped that they would migrate to open standards over time. The EMS could therefore act as a mediation device between the NMS and the NEs and only the appropriate EMS required a detailed knowledge of the workings of the NEs. This meant that the NMS could be much simpler and could focus on building an overview of network status and performance.

8.7.2 Common Management Information Protocol (CMIP)[7]

CMIP and the Common Management Information Service (CMIS), its service interface, were defined by ISO and the ITU-T. CMIP supports information exchange between a network management application and management agents residing in network devices. CMIP is an object-oriented protocol that runs on top of a full ISO protocol stack, and uses ASN.1 at the presentation layer, but it can also be run on top of TCP/IP. It is a complex and powerful protocol with good security features. CMIP is used mainly by the network operators within their TMNs, but not much elsewhere, due to its complexity and the availability of a simpler IETF protocol.

8.7.3 Simple Network Management Protocol (SNMP)[8]

SNMP was designed by the IETF to support network management applications on the Internet. It is a object-oriented connectionless application layer protocol that runs on above UDP and uses ASN.1 coding. Like CMIP, it requires that each managed device runs a software agent that communicates via SNMP with an NMS. The agent collects information about its objects and the messages it processes. This information (mainly counters appropriate to each object) is stored in a **Management Information Base** (**MIB**) along with

[6] *ITU-T Recommendation M.3000.*

[7] *IS 9595I6, ITU-T Recommendation X.700.*

[8] *RFC 1157.*

other information, such as trap thresholds. The objects will be dependent on the protocols being monitored. There will be a set of objects defined for Ethernet, another for IP and others for TCP, UDP and application layer protocols (including SNMP itself). The NMS is able to access the MIB in each agent and can request information from them as well as set parameters, such as trap thresholds. SNMPv2 is insecure, as its security is based on community strings, which are similar to passwords, and these are transmitted as plain text. Worse still some implementations do not change the default community strings of 'public' for read only access and 'private' for write access.

The MIB is structured as a tree of managed objects. Each object has a unique identifier that is encoded as a sequence of integers representing the branches taken at each level of the tree to reach the object from the root.

SNMPv1 only has four primitives:

- Get fetches data from a specified object from the MIB
- GetNext fetches the next object in the MIB
- Set updates a specified object, such as a threshold, in the MIB with new data
- Trap allows the agent to report that a threshold has been exceeded.

SNMPv2 adds two extra primitives:

- GetBulk fetches a whole set of data from the MIB
- Inform allows the agent to report an event that the NMS must then acknowledge.

SNMPv3 adds security to SNMP and provides message integrity, authentication and encryption.

Early implementations of SNMP required the NMS to frequently use SNMP Get Requests to obtain copies of MIB counters at specified intervals for subsequent processing of performance data. This was a large processing and network overhead. RMON probes on LANs can now be used to collect and store similar performance information on a frequent basis. This information can then be uploaded to the NMS using SNMP GetBulk requests on a daily basis, which will enable the NMS to work much more efficiently.

Although SNMP is a standard, most suppliers have made proprietary extensions to the MIBs to create new objects or traps. These proprietary extensions make it much harder to implement open network management systems.

Activity 8.5

Use an on-line MIB Browser (one can currently be found at http://www.ibr.cs.tu-bs.de/cgi-bin/sbrowser.cgi) to examine the Ethernet MIB (1.3.6.1.2.1.35), the IP MIB (1.3.6.2.1.4), the TCP MIB (1.3.6.2.1.6), the UDP MIB (1.3.6.2.1.7) and the WWW MIB (1.3.6.1.2.1.65), or any other protocols we have studied, to see what counters and settable parameters are defined. If you cannot find an on-line MIB Browser, you can view similar information in the respective RFCs (3635, 2011, 2012, 2013, 2594).

8.8 Network management systems

NMSs usually run on powerful Unix workstations. They provide an integrated view of network status and network performance using graphical maps which can be hierarchical, so that network operators can zoom in to see more detail. They have powerful reporting facilities and can produce regular and ad hoc reports based on the performance data collected from agents. Some NMSs can also be used for device configuration.

In addition to the integrated NMS, other systems may be required to manage individual devices, particularly for configuration management, which is much harder to integrate than fault and performance management, as configuration data is much more device specific. Such systems are similar to the Element Management Systems in TMN.

Further management systems are often used for system management, to manage security functions, such as user profiles, work groups and permissions to use resources, and to manage storage devices, servers and their applications. All these functions can be combined with network management and Electronic Software Delivery in Enterprise Management Systems, such as HP OpenView and IBM's Tivoli, which incorporates NetView.

Other management systems may be required to manage specific applications, particularly with regard to setting up and changing user accounts, if there is an additional layer of security within the application. Business critical applications may well also do their own performance monitoring by measuring response times.

Activity 8.7

Using a search engine, find the web sites where Hewlett Packard and IBM describe their respective OpenView and Tivoli enterprise management system products. Compare the functions offered by each product.

Specimen examination question

(a) State whether each of the following statements is true or false and, if false, correct the statement:

i. Protocol analysers are able to record and analyse traffic on a LAN or WAN circuit and decode protocol headers at any layer.

ii. A virus is executable code that can exist on its own and can propagate itself to cause an unwanted event (harmless or destructive).

iii. Active attacks employ overt methods and hence are easier to detect than passive attacks.

iv. SNMPv2 added security features to SNMPv1, which transmitted community strings as plain text.

(b) Briefly describe four types of test equipment that can be used to diagnose faults.

(c) Describe the two methods used by accounting management to recover network costs from users and the situations in which both are normally used.

(d) Two routers, each with an availability of 99.9% are connected to each other by a private circuit which has an availability of 99.7%. The routers both have ISDN cards and are connected to ISDN lines. The availability of the ISDN service is 99.8%. What is the overall availability of the service between the LANs on each site which are connected to the routers?

(e) Describe the three main methods used to authenticate users.

Learning outcomes

At the end of this chapter, you should be able to:

- outline the main responsibilities of a network manager
- describe the main functions of fault, configuration, accounting performance and security management and contrast performance management with fault management
- outline the information that should be recorded in a trouble ticket.

- outline the test equipment that can be used to diagnose faults
- list the main causes of network faults
- describe, mathematically, how the various measurements associated with network reliability are related to each other and solve problems using these equations
- calculate overall availabilities for components connected in series and in parallel
- distinguish between threats, vulnerabilities and attacks
- outline the processes followed in risk management for controlling disruption, destruction and disaster and unauthorised access
- outline how TMN, CMIP and SNMP operate
- outline the main functions provided by Network Management.

Appendix A: Specimen examination paper

Answer two questions from this section.

Question 1

(a) State whether each of the following statements is true or false and, if false, write out a corrected version of the statement:

i. Selling a new product in a new market is called market development.

ii. Unlike USB, FireWire is a peer-to-peer protocol.

iii. 10G Ethernet does not support the CSMA/CD access method.

iv. Signalling System #7 (SS7) is an ITU-T defined common channel signalling system used by Public Packet Switched Data Networks.

[3 marks]

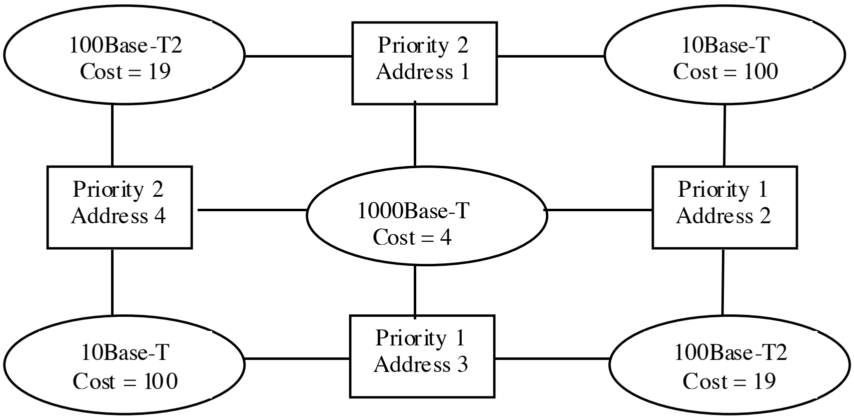
(b) Name the two main products of fixed network operators that are regarded as cash cows and describe how they are threatened. [3 marks]

How are the fixed network operators attempting to counter these threats? [3 marks]

(c) What factors have led to the popularity of using Metro Ethernet for LAN interconnection? [5 marks]

(d) Outline how a call is established through the Public Switched Telephone Network. [5 marks]

(e) Use the Spanning Tree Protocol to determine which bridge ports should be blocked in the following LAN topology. Show which bridge is elected as the root bridge and show the path costs from each bridge port to the root bridge. Mark all the root ports with an R and all the designated ports with an D and all the blocked ports with an X . Draw the spanning tree with thick lines. [6 marks]



Question 2

(a) State whether each of the following statements is true or false and, if false, write out a corrected version of the statement:

i. The Interior Gateway Routing Protocol is a proprietary distance vector routing protocol with a composite metric.

ii. The Internet Control Message Protocol is used by a device to indicate to a multicast router that it wants join a multicast group.

iii. Resource Reservation Protocol (RSVP) requests are made by the servers that transmit multicast messages.

iv. Multi-Protocol Label Switching provides a quality of service mechanism for the Internet that will work across multiple ISPs.

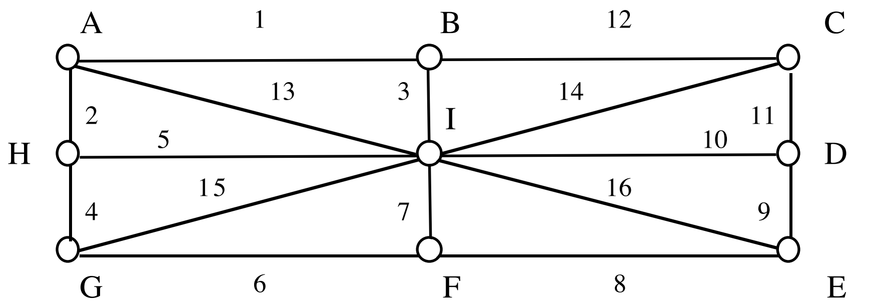
[3 marks]

(b) Describe four situations that may require bridges to be used between two LAN segments. [4 marks]

(c) List the six requirements for a routing algorithm and indicate between which pairs of requirements tradeoffs exist. [6 marks]

(d) Describe three techniques that can be used to minimise the effects of packet loss on multimedia communications. [6 marks]

(e) Use Dijkstra's algorithm to compute the shortest path between the points A and E using the metrics given in the diagram below. Draw the network in your answer book, showing all the node labels generated by the algorithm and indicating the shortest route with bold lines. [5 marks]



Question 3

(a) State whether each of the following statements is true or false and, if false, write out a corrected version of the statement:

i. Network design is a deterministic process that will result in a single optimal design.

ii. With Variable Length Subnet Masks, point to point circuits can be defined as /31 networks.

iii. The cost of internal networks is often charged to departments by means of an approximate cost apportionment method.

iv. A firewall router is placed at the boundary between a private and public network and it filters packets by examining addresses, port numbers or protocols. [3 marks]

(b) A new school is being planned and there is a requirement for a local area network to be implemented with access from every classroom. There are to be 100 PCs in the computer labs and another 50 dispersed in various rooms around the building, as well as 20 laptops which teachers will expect to be able to use in any room. It is expected that each PC will require no more than 50 kbit/s. Cost is to be the primary design consideration.

You should consider the following design options:

i. 802.11b Wireless LAN

ii. 10Base-T Ethernet using unshielded twisted pair wiring

iii. 10Base-F Ethernet using fibre optic cable

iv. Fibre Distributed Data Interface.

State which of the above design options best suits the customer requirements, giving your reasons for choosing this design and rejecting the other designs. [6 marks]

(c) Describe five factors that would influence the design of a WAN topology. [5 marks]

(d) List 10 potential causes of network faults. [5 marks]

(e) What does the acronym MTBF stand for and what, in one word, does it measure? [1 mark]

A router has an MTBF of 4 years and is maintained by a company that has a Mean Time to Diagnose of 1 hour, a Mean Time to Respond of 3 hours and a Mean Time to Fix of 2 hours. Calculate the availability of the router. [5 marks]

Notes

Appendix B: Model answers and hints

Chapter 2

(a) True or False

i. FALSE – a problem child has high market growth.

ii. TRUE.

iii. FALSE – it has done so in many countries by means of subsidiaries.

iv. TRUE.

(b) See bullet point list in Section 2.1.

(c) The main difference relates to the lack of an incumbent in mobile markets. This means that the markets are more dynamic, innovative and competitive. Because of the lack of competition, this fixed market is more heavily regulated than the mobile market. The fixed market is also much nearer being fully saturated, so high growth is harder to achieve than it is in the mobile market. The mobile market can appeal to a younger customer base than the fixed market. It is generally only householders who buy fixed network services, but mobile services can be bought by children, young people and students.

(d) See Section 2.2.4, first paragraph.

(e) See Section 2.2.5.

Chapter 3

(a) True or False

i. TRUE.

ii. FALSE – authentication is a service provided by the station.

iii. FALSE – it uses Differential Manchester encoding.

iv. TRUE.

(b) See Sections 3.1.1 and 3.1.2.

(c) See bullet point list in Section 3.3.1.2.

(d) See Section 3.3.2, first paragraph.

(e) See Section 3.3.5, third bullet point list.

Chapter 4

(a) True or False

i. TRUE.

ii. FALSE – the CSU/DSU is owned by the customer in North America.

iii. TRUE.

iv. FALSE – ATM cells have a fixed length of 53 bytes with a 5-byte header.

(b) See Sections 4.2.1.1 and 4.2.1.2.

(c) The main advantage is that satellite communications can take place from any point in the satellite's footprint and places with no fixed or mobile infrastructure can be served. The main disadvantage is the cost and the long propagation times.

(d) See Section 4.2.7.2 under the heading Network operation.

(e) See Sections 4.2.8 and 4.2.9.

Chapter 5

(a) True or False

i. TRUE.

ii. FALSE – Link State routing protocols flood the network with the status of links whenever the status changes.

iii. FALSE – the PSTN uses static routing, often over a fully meshed core network.

iv. TRUE.

(b) See bullet point list in Section 5.1.

(c) See bullet point list in Section 5.2.3

(d) See Section 5.6.6.1.

(e) See Chapter 5.6.3, first paragraph.

Chapter 6

(a) True or False

i. FALSE – JPEG is a lossy algorithmm.

ii. TRUE.

iii. FALSE – DiffServ redefines the Type of Service field.

iv. TRUE.

(b) See Section 6.2.1, 6.2.2, 6.2.3 and 6.2.4

(c) See Section 6.1.

(d) ATM was designed with multimedia in mind. It therefore has mechanisms designed to provide QoS. The Internet on the other hand, was designed to carry non real-time data and any QoS mechanisms have to be bolted onto it. ATM is a connection-oriented protocol where packets between a source and destination will always take the same route, and it is easy to reserve resources to guarantee QoS. The Internet uses a connectionless network layer and packets can take different routes through the network, so it is much more difficult to reserve any resources. ATM has a fixed length cell size while IP has a variable length packet size. This makes it harder to provide a consistent QoS on the Internet.

(e) See Sections 6.4.5, 6.4.6 and 6.4.8.

Chapter 7

(a) True or False

i. FALSE – they are fire-resistant not non-flammable.

ii. TRUE.

iii. FALSE – it should focus on the business advantages.

iv. TRUE.

(b) See appropriate columns in Table 7.2.

(c) An integrated TDM solution (iii) best meets the requirement as it allows voice and data to share the same communications circuits which with four offices can be configured into a very resilient full mesh. 1.5 Mbit/s or 2 Mbit/s circuits could carry the load even under failure conditions. Any capacity less than this would not be able to carry all the traffic if one of the other circuits failed. A private circuit solution can also deliver low and constant delays for the real-time application.

A managed PSTN solution for voice and frame relay solution for data (i) would be very expensive, as there would be no integration between the voice and the data and the voice would be charged per minute on the PSTN, which would work out much more expensive than a private circuit. This design is also unlikely to meet the reliability requirement unless each of the dual access circuits were provided which would make the design even more expensive.

An Internet-based solution with dual access from each site to an ISP (ii) must be ruled out as one of the applications is real time and requires low and constant delays which cannot be achieved using the Internet. The design is also likely to be expensive as the cost of a dual access circuit to an ISP from each site will be quite high.

Although an ATM solution (iv) will meet the requirements of the real time application and will support voice and data integration, it will be prohibitively expensive. The lowest access speed for ATM is 155 Mbit/s which is a hundred times more than needed. In addition dual access circuits would be required to meet the reliability requirement which will make the solution yet more expensive.

(d)

4th Byte	Subnetwork Address
000XXXXX	200.3.4.0/27
001XXXXX	200.3.4.32/27
010XXXXX	200.3.4.64/27
011XXXXX	200.3.4.96/27
1000XXXX	200.3.4.128/28
1001XXXX	200.3.4.144/28
1010XXXX	200.3.4.160/28
1011XXXX	200.3.4.176/28
1100XXXX	200.3.4.192/28
1101XXXX	200.3.4.208/28
111000XX	200.3.4.224/30
111001XX	200.3.4.228/30
111010XX	200.3.4.232/30
111011XX	200.3.4.236/30
111100XX	200.3.4.240/30
111101XX	200.3.4.244/30
111110XX	200.3.4.248/30
111111XX	200.3.4.252/30

(e) See bullet point list in Section 7.2.7.

Chapter 8

(a) True or False

i. TRUE.

ii. FALSE – a virus must be part of another program, a boot sector on a disk or a macro in a document.

iii. TRUE.

iv. FALSE – SNMPv3 added security features to SNMPv2 which transmitted community strings as plain text.

(b) See first bullet point list in Section 8.2.3.

(c) See Section 8.4.

(d) Overall availability of circuit plus ISDN backup:

= 1 – (1 – 0.997) x (1 – 0.998)
= 1 – 0.002 x 0.002
= 1 – 0.000006
= 0.999994

Overall availability of service = 0.9992 x 0.999994

In the exam, it is possible that calculators will not be allowed, in which case this would be the answer in its simplest form.

The numerical answer is 0.997995 or 99.8%.

(e) See Section 8.6.4.2 first paragraph.

Appendix A: Specimen examination paper

Question 1

(a)

i. FALSE – it is called diversification

ii. TRUE

iii. TRUE

iv. FALSE – it is used by the Public Switched Telephone Network

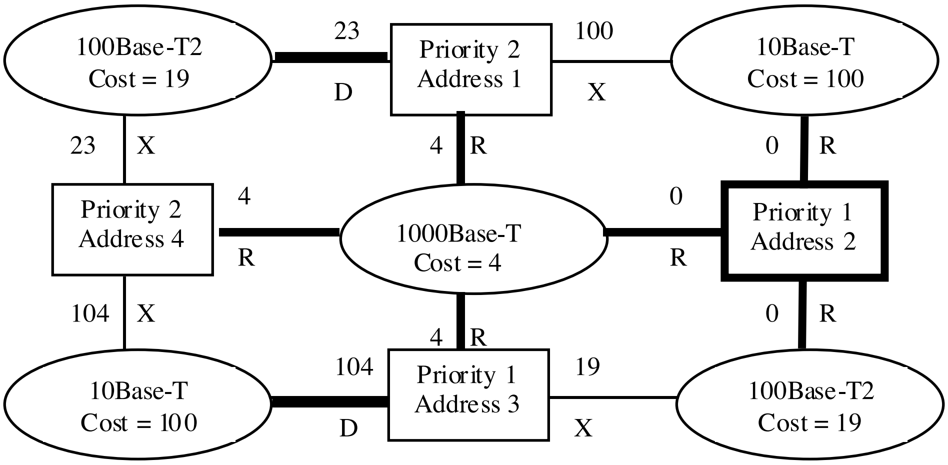
(b) The two main cash cow products of the fixed network operators are the PSTN and private circuits. The PSTN is threatened by mobile telephony and Voice over IP and private circuits are threatened by managed services such as IP VPNs accessed via Digital Subscriber Line technologies.

The fixed network operators attempt to counter these threats by offering these new products (such as VoIP and xDSL broadband Internet access) in competition to their cash cow products and by diversifying into providing business solutions and outsourcing rather than just communications products.

(c) Metro Ethernet has become popular, as it can prove LAN speed connections, at reasonable costs, between sites using the same protocols as are used on the LANs. Metro Ethernet thus maintains simplicity, as no protocol translation is required, and allows the use of cheap interface cards, which have been mass produced for PCs.

(d) See Section 4.2.4, paragraphs 2 and 4.

(e)



Question 2

(a)

i. TRUE.

ii. FALSE – It is the Internet Group Message Protocol.

iii. FALSE – RSVP Requests are made by the receivers.

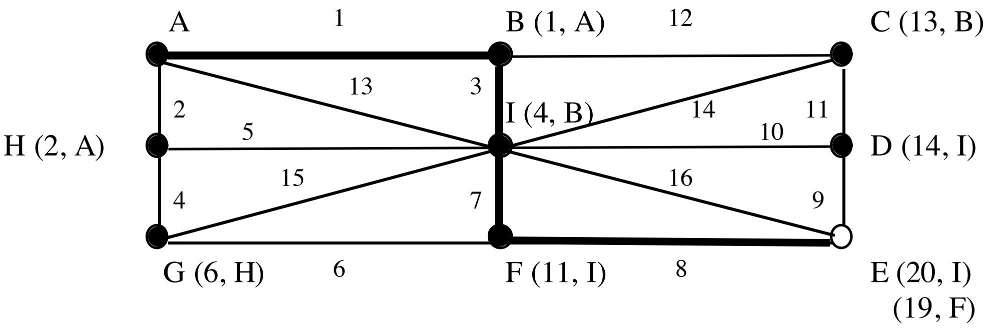
iv. TRUE.

(b) See bullet point list in Section 5.2.

(c) See Section 5.3.2, fourth paragraph.

(d) See Section 6.4.2.

(e)



Question 3

(a)

i. FALSE – It is a heuristic process that will result in a number of potential designs.

ii. FALSE – Point-to-Point circuits can be defined as /30 networks.

iii. TRUE.

iv. TRUE.

(b) A 10Base-T Ethernet using UTP (ii) would be the best solution to meet the school's requirements as it will do so at minimal cost because UTP cable is the cheapest of all the options. Hubs can be installed in each lab to connect up all the PCs in the labs and two cables could be run to each classroom to support a PC in the classroom and a teacher's laptop.

A Wireless LAN solution (i) would be ideal in many ways, as no cabling would be needed and any device (including the laptops) could be moved without them having to be plugged into the network. But the Wireless LAN equipment would be expensive to purchase as compared to the cost of 10-Base-T. The cost of Wireless LAN cards for PCs and the base stations would outweigh the cost of UTP cabling and Ethernet network cards, both of which are extremely cheap.

A 10-Base-F solution (iii) is not necessary as the overall capacity requirements point to a 10 Mbit/s LAN which can easily be supported using UTP which is much cheaper than fibre. There are no other factors in a school environment such as risk of electromagnetic interference or security reasons to justify the purchase of fibre.

Again the capacity requirement would not justify FDDI (iv) as a solution as it runs at 100 Mbit/s. There is no stated requirement for resilience that would justify the choice of a ring topology. This solution would be too expensive for the school's requirements.

(c) See Section 7.2.4, third bullet point.

(d) See Section 8.2.3, second bullet point list.

(e) MTBF stands for Mean Time Between Failures. It is a measure of reliability.

$$\begin{aligned} \text{MTTR} &= \text{MTTD} + \text{MTTResp} + \text{MTTF} \\ &= 1 + 3 + 2 \\ &= 6 \text{ hours} \end{aligned}$$

$$\begin{aligned} \text{MTBF} &= 4 \text{ years} \\ &= 4 \text{ x } 365.25 \text{ x } 24 \text{ hours} \\ &= 35{,}064 \text{ hours} \end{aligned}$$

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

$$= \frac{35064}{35064 + 6}$$

$$= \frac{35064}{35070}$$

(This is the answer in its simplest form, if a calculator is not used).

$$= 99.98\%$$

Notes

Appendix C: List of acronyms

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACL	Asynchronous Connection-Less
ADM	Add-Drop Multiplexer
ADPCM	Adaptive Differential Pulse Code Modulation
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding (PHB)
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
AOL	America On-Line
AP	Access Point
ARQ	Automatic Repeat Request
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASM	Any-Source Multicasting
ASN.1	Abstract Syntax Notation 1
ATM	Asynchronous Transfer Mode
AT&T	American Telephone and Telegraph
AUI	Attachment User Interface
AuC	Authorisation Centre
bit	binary digit
bit/s	bits per second
BA	British Airways
BERT	Bit Error Rate Tester
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BNC	Bayonet Neill Concelman
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSC	Base Station Controller
BSS	Base Station System
BSS	Basic Service Set
BT	British Telecommunications plc (no longer expanded as an acronym)
BTS	Base Transceiver Station
cHTML	Compact Hyper-Text Mark-up Language
CBR	Constant Bit Rate

CCITT	Comité Consultatif International Téléphonique et Télégraphique
CD	Compact Disc
CD/ROM	CD Read Only Memory
CDDI	Copper Distributed Data Interface
CEO	Chief Executive Officer
CERT	Computer Emergency Readiness Team (no longer expanded as an acronym)
CIDR	Classless Internet Domain Routing
CIR	Commited Information Rate
CIX	Commercial Internet Exchange
CL	Connection-less
CLEC	Competitive Local Exchange Carrier
CLNP	Connectionless Network Layer Protocol
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMTS	Cable Modem Termination System
CO	Connection-orientated
CPE	Customer Premises Equipment
CRC	Cyclical Redundancy Check
CRS	Computerised Reservation System
CR-LDP	Constraint-based Routing Label Distribution Protocol
CS	Convergence Sub-layer
CSI/DSU	Channel Service Unit / Data Service Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
CUG	Closed User Group
C&W	Cable & Wireless
DBS	Direct Broadcasting by Satellite
DCE	Data Communications Equipment / Data Circuit-terminating Equipment
DCF	Distributed Coordination Function
DE	Default (PHB)
DIX	Digital, Intel and Xerox consortium
DLCI	Data Link Connection Identifier
DMTF	Dual-Tone Multiple Frequency
DMZ	De-Militarised Zone
DNIC	Data Network Identification Code
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification

DQDB	Distributed Queue Dual Bus
DS	Data-Strobe
DS	Distribution System
DS	Differentiated Services
DSAP	Destination Service Access Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
DUAL	Diffusing Update Algorithm
DV	Distance Vector
DVD	Digital Versatile Disk
DVMRP	Distance Vector Multicast Routing Protocol
DWDM	Dense Wave Division Multiplexing
DXI	Data eXchange Interface
EDGE	Enhanced Data rates for Global Evolution
EF	Expedited Forwarding (PHB)
EFM	Ethernet in the First Mile
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EIR	Equipment Identity Register
EMS	Element Management System
ES	End System
ESD	Electronic Software Delivery
ESS	Extended Service Set
FDDI	Fibre Data Distributed Interface
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FEC	Forward Equivalence Class/ Forward Error Correction
FECN	Forward Explicit Congestion Notification
FHSS	Frequency Hopping Spread Spectrum
FRAD	Frame Relay Access Device
FSK	Frequency Shift Keying
GDS	Global Distribution System
GEO	Geosynchronous Earth Orbit
GFR	Guaranteed Frame Rate
GIF	Graphics Interchange Format
GMSC	Gateway Mobile Switching Centre

GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GTE	General Telephone and Electronics Corporation (now owned by Verizon)
GbE	Gigabit Ethernet
HDLC	High-level Data Link Control
HEC	Header Error Control
HLR	Home Location Register
HP	Hewlett Packard
HR-DSSS	High Rate DSSS
HSCSD	High Speed Circuit-Swicthed Data
HTML	Hyper-Text Mark-up Language
HTTP	Hyper-Text Transfer Protocol
Hz	Hertz
IBM	International Business Machines Corporation
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
ILEC	Incumbent Local Exchange Carrier
IMAP	Internet Mail Access Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IS-IS	Intermediate System to Intermediate System
ITU-R	International Telecommunications Union – Radio communications Sector
ITU-T	International Telecommunications Union – Telecommunications Standardization Sector
IrDA	Infra-red Data Association
IrLAP	Infra-red Link Access Protocol
IrMP	Infra-red Management Protocol
JPEG	Joint Photographic Expert Group

KLM	Koninklijke Luftvaartmaatschappij NV (Royal Dutch Airlines)
kHz	kiloHertz (thousand Hertz)
kbit/s	kilobit (thousand bits) per second
L2CAP	Logical Link Control Adaptation Protocol
LAPB	Link Access Protocol Balanced
LAPD	Link Access Protocol Digital
LAN	Local Area Network
LANE	LAN Emulation
LASER	Light Amplification by Stimulated Emission of Radiation
LDP	Label Distribution Protocol
LED	Light-Emitting Diode
LEO	Low Earth Orbit
LLC	Logical Link Control
LS	Link State
LSR	Label Switch Router
LTP	Lightweight Transport Protocol
LZW	Lempel Ziv Welch (algorithm)
L2TP	Layer 2 Tunnelling Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Multi-Station Access Unit
MBone	Multicast Backbone
MCI	Microwave Communications Incorporated
MCL	Mercury Communications Ltd
MEO	Medium Earth Orbit
MFS	Metropolitan Fibre Systems (now owned by MCI)
MHz	MegaHertz (million Hertz)
MIB	Management Information Base
MLT-3	Multi-Line Transmission 3-level
MMF	Multi-Mode Fibre
MMS	Multimedia Messaging Service
MMS	Microsoft Media Server
MOSPF	Multicast Open Shortest Path First
MPEG	Motion Picture Expert Group
MPLS	Multi-Protocol Label Switching
MP3	MPEG 1 Level 3
MSC	Mobile Switching Centre
MSN	Microsoft Network
MTBF	Mean Time Between Failures
MTSO	Mobile Telecommunications Switching Office (N. America)

MTTD	Mean Time to Diagnose
MTTF	Mean Time to Fix
MTTR	Mean Time to Repair
MTTResp	Mean Time to Respond
Mbit/s	Megabits (million bits) per second
ms	milliseconds (thousandth of a second)

NAT	Network Address Translation
NE	Network Element
NEC	Nippon Electric Company (no longer expanded as an acronym)
NIC	Network Interface Card
NMC	Network Management Centre
NMS	Network Management System
NNI	Network-to-Network Interface
NRZ	Non-Return to Zero
NRZ-I	Non-Return to Zero - Invert
NSAP	Network Service Access Point
NSFNET	National Science Foundation Network
NTL	National Transcommunications Ltd (no longer expanded as an acronym)
NTT	Nippon Telephone & Telegraph (no longer expanded as an acronym)
NTU	Network Terminating Unit
nrt-VBR	Non-real-time Variable Bit Rate

OC	Optical Carrier
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PABX	Private Automatic Branch Exchange
PAD	Packet Assembler Disassembler
PAM	Pulse Amplitude Modulation
PAN	Personal Area Network
PARC	Palo Alto Research Center
PARS	Programmable Airline Reservation System
PC	Personal Computer
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PEST	Political, Economic, Socio-cultural and Technological factors

PHB	Per Hop Behaviour
PIM	Protocol Independent Multicasting
PIN	Personal Identification Number
PMUX	Primary Multiplexer
PNA	Progressive Network Audio
PNG	Portable Network Graphics
PNM	Progressive Network Media
PON	Passive Optical Network
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPSDN	Public Packet Switched Data Network
PPT	Post, Telegraphs and Telephones
PPTP	Point-to-Point Tunnelling Protocol
PRI	Primary Rate Interface
PSI	Performance Systems International
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RBOC	Regional Bell Operating Company
RCH	Regional Cable Head
RFC	Request For Comment
RFCOMM	Radio Frequency Communications
RFP	Request for Proposal
RIP	Routing Information Protocol
RMON	Remote Monitor
RPOA	Recognised Private Operating Agency
RPF	Reverse Path Forwarding/Flooding
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RTT	Round Trip Time
RZ	Return to Zero
rt-VBR	Real-time Variable Bit Rate
SABRE	Semi-Automated Business Research Environment
SAN	Storage Area Network
SAP	Service Advertising Protocol

SAR	Segmentation and Reassembly
SBC	Southwestern Bell Corporation (no longer expanded as an acronym)
SCO	Synchronous Connection-Orientated
SCP	Service Control Point
SCSI	Small Computer Systems Interface
SDH	Synchronous Digital Hierarchy
SEAL	Simple and Efficient Adaptation Layer
SHDSL	Symmetric High-bit-rate Digital Subscriber Line
SIM	Subscriber Identity Module
SIP	SMDS Interface Protocol
SIP	Session Initiation Protocol
SMDS	Switched Multi-megabit Data Service
SMF	Single-Mode Fibre
SMIL	Synchronised Multimedia Integration Language
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SNAP	Sub-Network Access Protocol
SONET	Synchronous Optical NETwork
SPrings	Shared Protection Rings
SPF	Shortest Path First
SSAP	Source Service Access Point
SSM	Source-Specific Multicasting
SS7	Signalling System Number 7
STM	Synchronous Transport Mode
STP	Shielded Twisted Pair
STS	Synchronous Transport Signal
SVC	Switched Virtual Circuits
SWOT	Strength, Weaknesses, Opportunities and Threats
TA	Terminal Adaptor
TACS	Total Access Communication System
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TE	Traffic Engineering
TL	Twisted Pair Long Reach
TMN	Telecommunications Management Network
TTL	Time To Live

TV	Television
TWA	TransWorld Airlines (no longer exists)
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Telecommunications System
UNI	User-to-Network Interface
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
USO	Universal Service Obligation
USSD	Unstructured Supplementary Data Service
US-CERT	US Computer Emergency Readiness Team
UTP	Unshielded Twisted Pair
UUNet	Unix to Unix Network (no longer expanded as an acronym)
VCI	Virtual Channel Identifier
VCR	Video Cassette Recorder
VDSL	Very-high-speed Digital Subscriber Line
VLAN	Virtual LAN
VLR	Visitor Location Register
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VoATM	Voice over ATM
VoD	Video on Demand
VoFR	Voice over Frame Relay
VoIP	Voice over IP
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WDM	Wavelength Division Multiplexing
WML	Wireless Mark-up Language
WLAN	Wireless LAN
WPAN	Wireless PAN
WWN	WorldWide Names
WWW	World-Wide Web
XML	Extensible Mark-up Language
XOR	Exclusive OR
xDSL	any Digital Subscriber Line

Notes

Notes

Notes

Notes

Notes

Correction

Data communications and enterprise networking – volume 2

BSc in Computing and Information Systems

2005 2910222

August 2007, first correction

Chapter 2 – Network markets

p.12: Fixed network operators

Since the subject guide was written, there has been further consolidation amongst the US and UK fixed network operators.

Verizon successfully acquired MCI in 2005 and briefly became the largest US telecommunications company until later in the same year when SBC acquired AT&T, retaining the AT&T name for the merged company.

Energis was acquired by Cable & Wireless in 2005.

The two remaining UK cable TV companies (NTL and Telewest) finally merged in 2006 and branded the new company as Virgin Media. NTL having previously set up the ISP virgin.net with the Virgin Group and then bought it out and Telewest having acquired the Virgin Mobile virtual network operator, with a 30 year agreement to be able to use the Virgin brand. The Virgin Group, via a subsidiary, is a major share holder of Virgin Media. The merger of the ISP operations of NTL (virgin.net) and Telewest (Blueyonder) has created the UK's second largest broadband supplier (Virgin Broadband) and the UK's first 'quadruple play' (TV, Broadband, Mobile and Fixed Telephone) operator.

p.16: Internet Service Providers

Since the subject guide was written, France Telecom have rebranded their Wanadoo ISP business as Orange to gain leverage from their successful mobile phone brand. MCI, as discussed under Fixed Network Operators, has been acquired by Verizon and its ISP and IP businesses have been rebranded as Verizon Business.

Chapter 5 – Network integration (internetworking)

p.79: Figure 5.3: Example of Djikstra's Algorithm

The label for Node D should contain (16, C) rather than (16, B).

Appendices – Appendix B: Model answers and hints

P.156: Chapter 4 – Question (e)

The references to Sections 4.2.8 and 4.2.9 should have been to Sections 4.2.7 and 4.2.8.

P.156: Chapter 5 – Question (d)

The reference to Section 5.6.6.1 should have been to Section 5.6.1.1.

Comment form

We welcome any comments you may have on the materials which are sent to you as part of your study pack. Such feedback from students helps us in our effort to improve the materials produced for the International Programmes.

If you have any comments about this guide, either general or specific (including corrections, nonavailability of essential texts, etc.), please take the time to complete and return this form.

Title of this **subject guide** ....

....

Name ....

....

Address ....

....

....

....

Email ....

Student number ....

For which qualification are you studying?...

....

Comments

....

....

....

....

....

....

....

....

....

....

....

....

....

....

Please continue on additional sheets if necessary.

Date ....

Please send your comments on this form (or a photocopy of it) to:

Publishing Manager, International Programmes, University of London, Stewart House
32 Russell Square, London WC1B 5DN, UK.