In this chapter you will learn to:

- use applications to create and transmit messages
- establish a communications link and describe the steps that take place in its establishment
- identify and describe specified protocols at different stages of the communication
- identify client processing and server processing
- describe the advantages and disadvantages of client – server architecture

  use a communication system to transmit and receive audio, video and text data
- for given examples, identify the participants, information/data, information technology, need and purpose
- for given examples explain how data is transmitted and received
- for given examples, identify the advantages and disadvantages of the system
- compare and contrast traditional communication systems with current electronic methods
- represent a communication system diagrammatically
- predict developments in communication systems based on current trends
- simulate activities involved with communication in areas such as
  - e commerce
  - EFTPOS
  - Internet banking
- for a given scenario, choose and justify the most appropriate transmission media
- diagrammatically represent the topology
- describe the location and role of hardware components on the network
- compare the functions of different hardware components
- identify the main characteristics of network operating software
- compare and contrast the Internet, intranets and extranets
- distinguish between data in analog and digital form
- justify the need to encode and decode data
- identify where in a communication system signal conversion takes place
- describe the structure of a data packet
- describe methods to check the accuracy of data being transmitted
- detail the network management software in a given network
- describe the role of the network administrator and conduct network administration tasks
- demonstrate logon and logoff procedures, and justify their use
- adopt procedures to manage electronic mail
- describe and justify the need for ethical behaviour when using the Internet
- discuss the social and ethical issues that have arisen from use of the Internet, including:
  - the availability of material normally restricted
  - electronic commerce
  - domination of content and control of access to the Internet
  - the changing nature of social interactions
- identify the issues associated with the use of communication systems including:
  - teleconferencing systems
  - messaging systems
  - e commerce
  - EFTPOS
  - electronic banking
- design and implement a communication system to meet an individual need
- predict developments in communication systems based on current trends

Which will make you more able to:

- apply and explain an understanding of the nature and function of information technologies to a specific practical situation
- explain and justify the way in which information systems relate to information processes in a specific context
- analyse and describe a system in terms of the information processes involved
- develop solutions for an identified need which address all of the information processes
- evaluate and discuss the effect of information systems on the individual, society and the environment
- demonstrate and explain ethical practice in the use of information systems, technologies and processes
- propose and justify ways in which information systems will meet emerging needs
- justify the selection and use of appropriate resources and tools to effectively develop and manage projects
- assess the ethical implications of selecting and using specific resources and tools, recommends and justifies the choices
- analyse situations, identify a need and develop solutions
- select and apply a methodical approach to planning, designing or implementing a solution
- implement effective management techniques
- use methods to thoroughly document the development of individual or team projects

In this chapter you will learn about:

Characteristics of communication systems

- communication systems as being those systems which enable users to send and receive data and information
- the framework in which communication systems function, demonstrated by the *Fig 3.1* model
- the functions performed within the communication systems in passing messages between source and destination, including:
  - message creation
  - organisation of packets at the interface between source and transmitter
  - signal generation by the transmitter
  - transmission
  - synchronising the exchange
  - addressing and routing
  - error detection and correction
  - security and management
- the roles of protocols in communication
  - handshaking and its importance in a communications link
  - functions performed by protocols at different levels
- the client - server model
  - the role of the client and the server
  - thin clients and fat clients
  - examples of clients such as web browsers and mail clients
  - examples of servers such as print servers, mail servers and web server

Examples of communication systems

- teleconferencing systems
- messaging systems, including email, voice mail and voice over Internet protocol (VOIP)
- other systems dependent on communication technology such as:
  - e commerce
  - EFTPOS
  - electronic banking

Transmitting and receiving in communication systems

- transmission media including:
  - wired transmission, including twisted pair, coaxial cable and optic fibre
  - wireless transmission, including microwave, satellite, radio and infrared
- characteristics of media in terms of speed, capacity, cost and security
- communication protocols, including:
  - application level protocols, including http, smtp and SSL
  - communication control and addressing level protocols, including TCP and IP
  - transmission level protocols, including Ethernet and Token ring
- strategies for error detection and error correction
- network topologies, including star, bus, ring, hybrid and wireless networks
- the functions performed by hardware components in communication systems including
  - hubs and switches
  - routers
  - modems
  - bridges and gateways
  - network interface cards (NIC)
  - mobile phones
  - cable
  - wireless access points
  - Bluetooth devices
- characteristics of network operating software
- the similarities and differences between the Internet, intranets and extranets

Other information processes in communication systems

- collecting, such as
  - the phone as the collection device with voice mail
  - EFTPOS terminal as a collection device for electronic banking
- processing, including
  - encoding and decoding analog and digital signals
  - formation of data packets
  - routing
  - encryption and decryption
  - error checking
    - parity bit check
    - check sum
    - cycle redundancy check
- displaying, such as
  - the phone as the display device with voice mail
  - EFTPOS terminal as a display device for electronic banking

Managing communication systems

- network administration tasks, such as:
  - adding/removing users
  - assigning users to printers
  - giving users file access rights
  - installation of software and sharing with users
  - client installation and protocol assignment
  - logon and logoff procedures
  - network based applications

Issues related to communication systems

- security
- globalisation
- changing nature of work
- interpersonal relationships
- e crime
- legal
- virtual communities
- current and emerging trends in communications, including
  - blogs
  - wikis
  - RSS feeds
  - podcasts
  - online radio, TV and video on demand
  - 3G technologies for mobile communications

3

COMMUNICATION SYSTEMS

Communication systems enable people and systems to share and exchange data and information electronically. This communication occurs between transmitting and receiving hardware and software over a network – each device on a network is called a node. Consider the diagram in *Fig 3.1*. As each message leaves its source it is encoded into a form suitable for transmission along the communication medium, which could be a wired or wireless connection. During its travels, the message may follow a variety of different paths through many different networks and connection devices. Different types of connection device use different strategies to determine which path each message will follow – switches decide based on the MAC address, whilst routers use the IP address, for example. Eventually the message arrives at the receiver, who decodes the message as it arrives at its destination. The network could be a local area network (LAN), a wide area network (WAN), it could be the Internet, an intranet, extranet or any combination of network types.

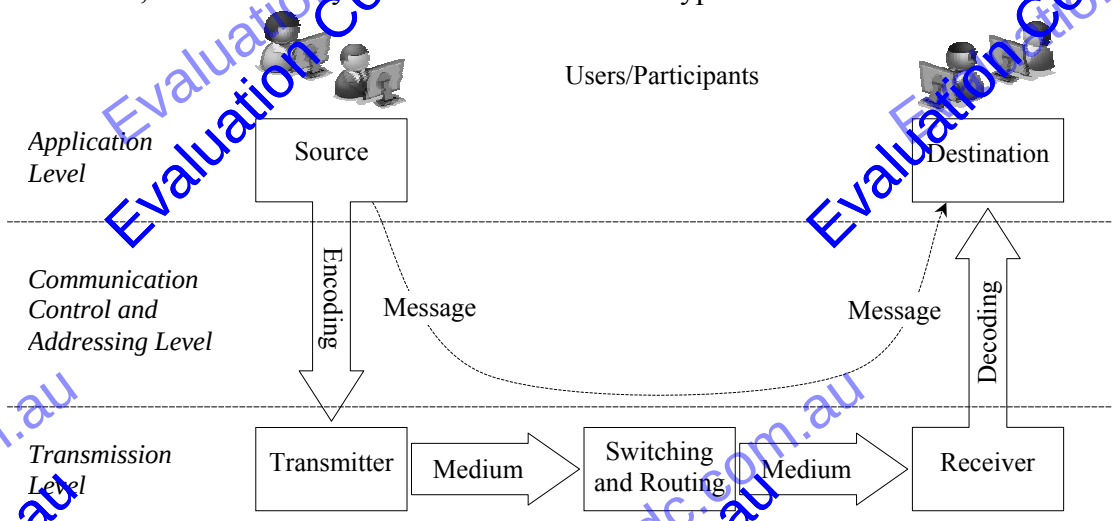


Fig 3.1
Communication system framework from NSW Board of Studies IPT syllabus (modified).

For communication to be successful requires components to agree on a set of rules known as protocols. Establishing and agreeing on which set of protocols will be used and the specific detail of each protocol must occur before any data can be transmitted or received – this process is known as handshaking. Protocols are classified according to the level or layer in which they operate. In the IPT course we classify protocols into three levels, namely; Application Level, Communication Control and Addressing Level, and Transmission Level (refer *Fig 3.1*). As messages pass through the interface between sender and transmitter they are encoded, meaning they descend the stack of protocols and are finally transmitted – each message is progressively encoded using the protocol (or protocols) operating at each level. Conversely, as messages are received they pass through the interface between receiver and destination – the original message is decoded by each protocol in turn as it ascends through each level of the protocol stack.

In the IPT syllabus three levels of protocols are defined; this framework provides a simplified view of the more detailed OSI (Open Systems Interconnection) model. The OSI model defines seven layers, where each layer can be further expanded into sub-

layers. Layers specified within the OSI model are combined to form the levels of the IPT model as shown in *Fig 3.2*. In IPT the OSI Presentation and Application layers (layer 6 and 7) are combined to form the IPT Application Level. OSI layers 3, 4 and 5, the network, transport and session layers are combined to form the IPT Communication Control and Addressing Level. Finally, protocols operating within the Physical and Data link layers (layer 1 and 2) of the OSI model are included in the IPT Transmission level. Throughout this chapter we focus on the IPT version with reference to the OSI model when appropriate.

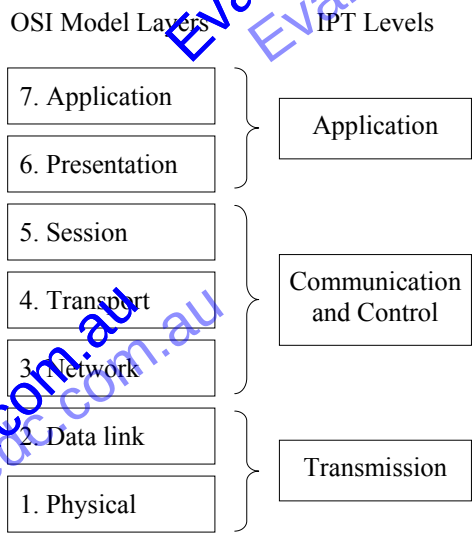


Fig 3.2
Comparison of the seven layers of the OSI model with the three levels used in IPT.

Note that in most cases communication occurs in both directions, even when the actual message only travels in one direction. The receiver transmits data back to the transmitter including data to acknowledge receipt, request more data or to ask for the data to be resent should it not be received correctly. The details of such exchanges are specific to the particular protocol being used.

In this chapter we consider:

- Characteristics of communication systems, including an overview of each protocol level based on the OSI model, details of how messages pass from source to destination, examples of protocols operating at each level, measurements of transmission speed and common error checking methods.
- Examples of communication systems including teleconferencing, messaging systems and financial systems.
- Network communication concepts including client-server architecture, network physical and logical topologies and methods for encoding and decoding digital and analog data.
- Network hardware including transmission media, network hardware devices such as hubs, switches and routers, and also servers such as file, print, email and web servers.
- Software to control networks including network operating software, network administration tasks and other network-based applications.
- Finally we consider issues related to communication systems and current and emerging trends in communication.

Consider the following examples of communication:

1. A conversation with a young child.
2. Sending a birthday card to your grandmother.
3. Watching television.
4. Ordering a meal in a restaurant.

GROUP TASK Discussion
For each example, identify the source, destination and medium over which messages are sent. Describe suitable communication rules (protocols).

CHARACTERISTICS OF COMMUNICATION SYSTEMS

Before we examine the details of particular examples of communication systems it is worthwhile understanding some communication concepts and terminology common to most communication system. The knowledge gained in this section underpins much of the work covered in the remainder of this chapter.

OVERVIEW OF PROTOCOL LEVELS

Software is used to control and direct the operation of hardware. The transmitter and the receiver must agree on how the hardware will be used to transfer messages. This is not a simple matter, a large variety of applications transfer data using a wide variety of operating systems, protocols, devices and transmission media. In 1978 a set of standards was first developed by the International Standards Organisation (ISO) to address such issues. These standards are known as the *Seven-Layer Model for Open Systems Interconnection* or more simply as the *OSI Model*. This seven-layer model has been largely accepted and used by network engineers when creating all types of transmission hardware and software.

The hardware actually used for transmission resides within the IPT Transmission Level, which includes the physical layer of the OSI Model. The physical layer includes NICs, hubs and the various different types of physical and wireless transmission media. These components actually move the data from the transmitter to the receiver. How they do this is determined by the higher software layers, each layer performs its functions with data from the layer above during transmitting and the layer below during receiving.

The seven layers of the OSI model are referred to as the OSI stack. Each packet of data must descend the stack, be transmitted and then ascend the stack on the receiving computer. A brief explanation of the general tasks performed at each of the OSI layers and IPT levels follows. To avoid confusion between IPT levels and OSI layers we will always refer to the IPT syllabus levels as "IPT… Level" and OSI layers as "OSI… Layer".

IPT Presentation Level

7. OSI Application Layer – The actual data to be transmitted is created by a software application, this data is organised in a format understood by the application that will receive the data.
6. OSI Presentation Layer – The data is reorganised into a form suitable for subsequent transmission. For example, compressing an image and then representing it as a sequence of ASCII characters suited to the operating system. The presentation layer is commonly part of the application or is executed directly by the application and is often related to the requirements of the operating system. Protocols operating at this level include HTTP, DNS, FTP, SMTP, POP, IMAP and SSL.

IPT Communication Control and Addressing Level

5 OSI Session Layer – This is where communication with the network is established, commences and is maintained. It determines when a communication session is started with a remote computer and also when it ends. For example, when performing an Internet banking transaction it is the session layer that ensures communication continues until the entire transaction is completed. Layer 5 also includes security to ensure a user has the appropriate access rights.

4. OSI Transport Layer – The transport layer manages the correct transmission of each packet of data. This layer ensures that packets failing to reach their

destination are retransmitted. For example, TCP (Transport Control Protocol) operates within layer 4. TCP is used on TCP/IP networks, such as the Internet, to ensure the correct delivery of each data packet actually occurs.

3. OSI Network Layer – This is where packets are directed to their destination. IP (Internet Protocol) operates here – its job is to address and forward packets to their destination. There is no attempt to check each packet actually arrives. Routers also operate at this layer by directing packets along the best path based on their IP address. Routers often have their software stored in flash memory and can be configured remotely from an attached computer.

PT Transmission Level

2. OSI Data Link Layer – This layer defines how the transmission media is actually shared. Device drivers that control the physical transmission hardware operate at this layer. They determine the final size of transmitted packets, the speed of transfer, and various other physical characteristics of the transfer. Switches and the Ethernet protocol operate at this level, directing messages based on their destination MAC (Media Access Controller) address. Other data link protocols include Token Ring, SONET and FDDI.

MAC Address
Media Access Controller Address hardwired into each device. A hardware address that uniquely identifies each node on a network.

1. OSI Physical Layer – This layer performs the actual physical transfer, hence it is composed solely of hardware. It converts the bits in each message into the signals that are transmitted down the transmission media. The transmission media could be twisted pair within a LAN, copper telephone cable in an ADSL connection, coaxial cable, optical fibre or even a wireless connection.

OVERVIEW OF HOW MESSAGES ARE PASSED BETWEEN SOURCE AND DESTINATION

In this section we explain the general processes occurring from when a message is first created at the source until it arrives at its final destination. Most of the points made here will be expanded and elaborated upon throughout the remainder of this chapter. The intention of this overview is to explain how all the different processes and information technology we will study fit together to form a logical operational communication system. It may be worthwhile rereading this overview as you work through this chapter to help explain where each new area of study fits within the overall communication process.

Message creation

The message is compiled at the source in preparation for sending. This takes place using some type of software application and perhaps involves the collection of message data from one of the system's users or participants.

Some examples of message creation include:

- A user writing an email using an email client such as Outlook.
- A web server retrieving requested HTML files from secondary storage in preparation for transmission to a web browser.
- A DBMS server extracting records from a database for transmission to a client application.
- Speaking during a VOIP (Voice Over Internet Protocol) phone conversation.
- Pressing the delete key to remove a file stored on a file server.

GROUP TASK Discussion
Brainstorm other examples where messages are created in preparation for transmission. In each case identify the software used to create the message.

Organisation of packets at the interface between source and transmitter

In general, when a message is being prepared for transmission it descends the stack of protocols from the Application Level down to where it is ready for physical transmission by the hardware operating at the Transmission Level. Each protocol wraps the data packet (or frame or segment – different names are used depending on the particular protocol) from the layer above with its own header and trailer. The header and trailer contain data relevant to the protocol operating at that layer. The protocol operating within the next lower layer considers each entire packet from the prior layer to be data and adds its own header and trailer (refer *Fig 3.3*). Hence the protocols within each layer are applied independently of the protocols operating in other layers. Some protocols include the address of the receiver within the header and many include some form of error detection code within their header or trailer.

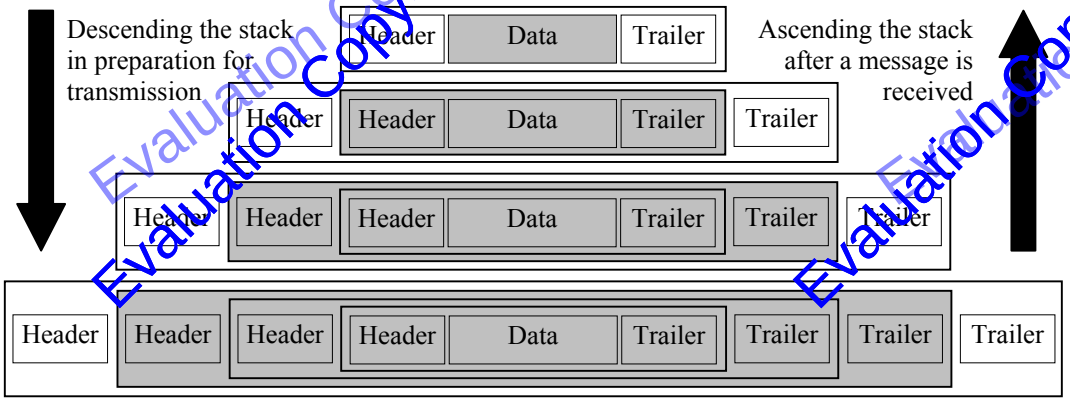


Fig 3.3
Descending and ascending the stack occurs during transmitting and receiving respectively.

Fig 3.3 implies each layer is creating a single data packet from the packet passed from the preceding layer. This need not be the case; usually multiple packets are created based on the requirements of the individual protocol being applied.

Let us work through a typical example. The software application, perhaps after direction from a user, first initiates the processes required to prepare the message for transmission. Essentially commands that include the message are issued to the protocol operating at the Application Level. For instance, to send an email message the email client software issues SMTP commands that include the recipient's email address and the content of the email message. To request a web page a web browser issues an HTTP command that includes the URL of the requested page. At this level we still have a single complete message. Furthermore the Application Level protocol is part of the software application; hence at this stage all processing has been performed by the same software that created the message.

Next the message is passed on to the Communication Control and Addressing Level. Commonly two or more protocols are involved, for example TCP in the OSI Transport Layer and then IP within the OSI Network Layer. Protocols operating at this level operate under the control of the operating system. They are not part of individual software applications, rather they are installed and managed by the operating system. The Communication Control and Addressing Level ensures packets reach their destination correctly. They include error checks, flow control and also the

source and destination address. Imagine the data packet has been passed to TCP. If the packet is longer than 536 bytes then TCP splits it into segments. The header within each segment includes a checksum and also information used by IP. TCP creates a connection between the source and destination that is used to control the flow and correct delivery of all segments within the total message. As each TCP segment is produced it is passed on to IP – TCP requires that IP be used. IP is the protocol that routes data across the network to its destination. IP packets are known as datagrams. During transmission routers determine where to send each datagram based on the destination IP address. The final Communication Control and Addressing protocol passes each packet to the Transmission Level protocol(s) that operates in conjunction with the physical transmission hardware.

At the receiving end the processes described above are essentially reversed – each protocol strips off its header and trailer, performs any error checks, and passes the data packet up to the next protocol. The specifics of different protocols are described in detail later in this chapter.

Consider the following:

TCP/IP is actually a collection of many protocols operating above layer 2 of the OSI model. As TCP/IP does not include data link (layer 2) and physical (layer 1) protocols it is able to operate across almost any type of communication hardware. This is the central reason why TCP/IP is so suited to the transfer of data and information over the Internet.

The suite of TCP/IP protocols does not precisely mirror the seven layers of the OSI model. Commonly layers 5, 6 and 7 are combined in TCP/IP references and are collectively called the application layer. Layer 4 remains as the transport layer and layer 3 is renamed as the Internet layer.

GROUP TASK Discussion
Explain why Transmission Level protocols (layer 1 and 2 of the OSI model) do not form part of the TCP/IP protocols. How does this assist TCP/IP to operate across almost any network?

GROUP TASK Research
Using the Internet, or otherwise, determine TCP/IP protocols operating within the application, transport and Internet layers mentioned above.

Signal generation by the transmitter

The transmitter is the physical hardware that generates or encodes the data onto the medium creating a signal. In most cases transmitters and receivers are contained within the same hardware device – receivers decode the signal on the medium. This hardware is controlled by protocols operating at the Transmission Level. The main task of the transmitter is to represent individual bits or patterns of bits as a wave – this wave is the signal that is actually transmitted through the medium. For instance, on copper wires bits are represented by altering voltage, on optical fibres light waves are altered, and for wireless mediums radio waves, infrared waves or microwaves are altered. In all cases characteristics of some type of wave is altered by the transmitter. The rules of the Transmission Level protocol determine precisely which characteristics are altered. Some rules determine how each pattern of bits is encoded, others determine the speed of transmission and others are used to control and

synchronise the exchange. Examples of devices that include a transmitter (and also a receiver) include NICs, switches, routers, ADSL and cable modems, and even mobile phones and Bluetooth devices.

Transmission

Transmission occurs as the signal travels or propagates through the medium. Each bit or often pattern of bits moves from transmitter to receiver as a particular waveform. The transmitter creates each waveform and maintains it on the medium for a small period of time. Consider a Transmission protocol transmitting at 5Msym/s. This means the transmitter generates 5 million distinct symbols (wave forms representing bit patterns) every second. And it also means each distinct symbol is maintained on the medium by the transmitter for a period of one five millionth of a second. If each symbol represents 8-bits (1-byte) of data then one megabyte of data could potentially be transferred in one fifth of a second – as 1 million bytes requires 1 million symbols, and 5 million symbols can be transferred in one second. One fifth of a second is the time required for the physical transmission of one megabyte of binary data if the transmission occurs as a continuous stream of symbols and the transmitter and receiver are physically close together. In reality, data is split into packets, which are not sent continuously, errors occur that need to be corrected and some mediums exist over enormous distances – such as up to satellites or across oceans. Furthermore some protocols wait for acknowledgement from the receiver before they send the next data packet. This in itself has the potential to double transmission times – flow control is used by protocols to help overcome this problem.

Synchronising the exchange

To accurately decode the signal requires the receiver to sample the incoming signal using precisely the same timing used by the transmitter during encoding. This synchronising process ensures each symbol or waveform is detected by the receiver. If both transmitter and receiver use a common clock then transmission can take place in the knowledge that sampling is almost perfectly synchronised with transmitting. This is the most obvious method of achieving synchronous communication, for example the system clock is used during synchronous communication between components on the motherboard. Unfortunately, the use of a common clock is rarely a practical possibility when communication occurs outside of a single computer. As a consequence, other techniques must be used in an attempt to bring the receiver into synch with the transmitter.

Today synchronous transmission systems have almost completely replaced older asynchronous links, which transferred individual bytes separately using start and stop bits. Synchronous communication does not transfer bytes individually; rather it transfers larger data packets usually called frames. Frames vary in size depending upon the individual implementation. 10baseT Ethernet networks use a frame size of up to 1500 bytes and frame sizes in excess of 4000 bytes are common on high-speed dedicated links.

There are two elements commonly used to assist the synchronising process. A preamble can be included at the start of each frame whose purpose is initial synchronisation of the receive and transmit clocks. The second element is included or embedded within the data and is used to ensure synchronisation is maintained throughout transmission of each frame. Let us consider each of these elements.

Firstly each frame commences with a preamble. The Ethernet Transmission Level protocol uses an 8 bytes (64 bits) long preamble, which is simply a sequence of alternating 1s and 0s that end with a terminating pattern (commonly 1 1) called a frame delimiter. The receiver uses the preamble to adjust its clock to the correct phase

as the transmitting clock (see *Fig 3.4*). A frame delimiter is needed at the end of the preamble because the receiver may lose some bits during clock adjustment so these delimiting bits act as a flag indicating the start of the actual data.

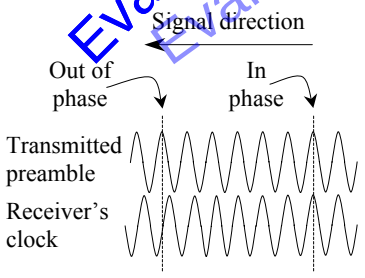


Fig 3.4
The preamble is used to synchronise the phase of the receiver's clock to match the transmitter's clock.

The preamble is followed by the data that needs to be received. The representation of the bits within the signal provides the second element used to maintain synchronisation. Commonly bits are represented not as high or low signals but using the transitions between these states. An example of such a system is Manchester Encoding used within 10baseT Ethernet networks. Using this system a low to high transition represents a 1 and a high to low transition represents a 0. As the clocks are initially synchronised then the location of the transitions representing the bits is known. The receiver detects each transition, if they are slightly out of synch then the receiving clock adjusts accordingly, hence Manchester Encoding is an example of a self-clocking code. As can be seen in *Fig 3.5*, two frequencies are needed to implement such a system; a base frequency and a frequency that is precisely double the base frequency. Data is transmitted at the same rate as the base frequency. For example 10baseT Ethernet transfers data at 10 megabits per second and therefore a base frequency of 10 mega hertz is used.

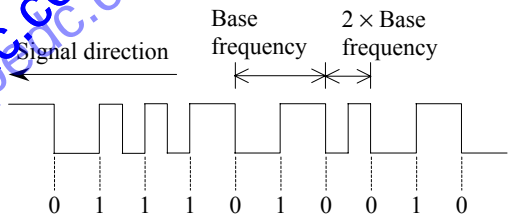


Fig 3.5
Manchester encoding uses the transitions between high and low to represent bits.

Other Transmission Level protocols use similar synchronisation strategies. For instance ADSL connections transmit superframes that contain many data frames. The header of the superframe contains synchronisation data much like the preamble of an Ethernet frame. Each data frame begins at equal and precisely spaced intervals.

Addressing and routing

During transmission data packets may pass through many different and varied links – particularly when the communication is over the Internet. Furthermore it is likely that packets forming part of a single file will travel over quite different paths from the transmitter to the receiver. Each new communication link will have its own protocol or set of protocols and hence each packet must ascend the protocol stack until it reaches the addressing or routing protocol and then descend the protocol stack as it is prepared for transmission down the next path.

Ethernet and other Transmission Level protocols use the receiver's MAC address to determine the path leading to the receiver. For instance an Ethernet switch maintains a table of all the MAC addresses of attached devices. Frames can therefore be directed down the precise connection that leads to the receiver. Most routers use the IP address within IP datagrams together with their own routing table to determine the next hop in a datagrams travels. The routing table is continually being updated to reflect the current state of attached networks and surrounding routers. Routers can therefore divert datagrams around faulty or poorly performing network connections.

GROUP TASK Research
Determine the protocols operating on either your own or your friend's home network. Explain how a message is sent using these protocols.

Error detection and correction

As messages descend the stack prior to transmission many protocols calculate checksums or CRC (Cyclic Redundancy Check) values and include them within their headers or footers. Once the message has been received it ascends the protocol stack, where each protocol examines its own received headers and trailers. If error detection is used by the protocol then the error check calculation is again performed to ensure the result matches the received checksum or CRC value. Whenever an error is detected virtually all protocols discard the entire packet and the sender will need to resend the packet to correct the problem. In general, CRC's are used within hardware operating within the Transmission Level, whilst checksums are used within many higher level protocols.

Clearly some strategy is needed so the sender can determine that an error was detected by the receiver and within which data packet the error occurred. Some protocols acknowledge only correct packets. This strategy is used by TCP and requires the sender to maintain a list of transmitted packets; as each acknowledgement arrives the associated packet is removed from the list. Packets remaining on the list for some specified period of time are resent. Within other protocols, such as Ethernet the receiver specifically requests packets to be resent each time an error is detected. There are specialised protocols that include self-correcting error detection codes – in this case some errors can be corrected at the destination without the need to resend the packet. Other protocols, such as IP, simply discard the message without any attempt to notify the sender.

GROUP TASK Discussion
Specialist systems, such as space probes, don't both with error correction; rather they send the whole message multiple times. Why is this strategy inappropriate for most communication systems? Discuss.

Security and management

Many protocols restrict messages based on user names and passwords, and others go a step further by encrypting messages during transmission. For example, POP (Post Office Protocol) operates on most mail servers. Top retrieve email messages from a POP server the user must first be authenticated – meaning a correct user name and password combination must be included. In this case the user name also identifies the mail box from which email messages are retrieved. SSL (or https) uses a public key encryption and decryption system to secure critical data transfers such as financial transactions. We explained encryption and decryption strategies in some detail within Chapter 2 and we will describe their implementation within the SSL protocol later in this chapter when we examine electronic banking.

GROUP TASK Discussion
Review the explanation of encryption and decryption in Chapter 2. Is encryption only used to secure messages during transmission? Discuss.

PROTOCOLS

There are literally thousands of different protocols that exist. Each protocol is designed to specify a particular set of rules and accomplish particular tasks. For example, Ethernet is the most widespread Transmission Level protocol for the transfer of data between nodes on local

Protocol
A formal set of rules and procedures that must be observed for two devices to transfer data efficiently and successfully.

area networks, however Ethernet is not suitable for communication over wide area networks (WANs) carrying enormous amounts of data over long distances. Commonly such networks use protocols such as ATM (Asynchronous Transfer Mode) or SONET (Synchronous Optical Network) – ATM is used on most ADSL connections and SONET for connections between network access points (NAPs) that connect different cities and even continents. Ethernet, ATM and SONET all operate at the Transmission Level (OSI layer 1 and 2).

Before two devices can communicate they must first agree on the protocol or series of protocols they will utilise. This process is known as 'handshaking'. Handshaking commences when one device asks to communicate with another; the devices then exchange messages until they have agreed upon the rules that will be used. Depending on the protocol being used handshaking may occur just after the devices are powered up or it may occur prior to each communication session occurring.

Handshaking
The process of negotiating and establishing the rules of communication between two or more devices.

In IPT we study three common examples of Application Level protocols, namely http, smtp and SSL – we examine HTTP in this section, smtp later as we discuss email and SSL during our discussion on electronic banking. Two Communication Control and Adressing protocols are required, namely TCP and IP. We describe each of these in this section and as they are common to most of today's networks we expand on this discussion throughout the text. At the Transmission Level we need to cover Ethernet and also the token ring protocol. We deal with Ethernet in this section and token ring later in the chapter as we discuss the operation of ring topologies.

HTTP, TCP, IP and usually Ethernet all contribute during the transfer of web pages – these four protocols are described in this section.

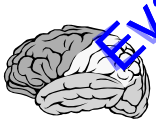
Hypertext Transfer Protocol (HTTP)

HTTP operates within the IPT Application Level and within layer 6 of the OSI model. HTTP is the primary protocol used by web browsers to communicate and retrieve web pages from web servers. A client-server connection is used where the browser is the client and the web server is the server. There are three primary HTTP commands (or methods) used by browsers – GET, HEAD and POST.

The HTTP GET method retrieves entire documents – the documents retrieved could be HTML files, image files, video files or any other type of file. The browser requests a document from a particular web server using a GET command together with the URL (Universal Resource Locator) of the document. The web server responds by transmitting the document to the browser. The header, which precedes the file data, indicates the nature of the data in the file – the browser reads this header data to determine how it should display the data in the file that follows. For example if it is an HTML file then the browser will interpret and display the file based on its HTML tags.

The HTTP HEAD method retrieves just the header information for the file. This is commonly used to check if the file has been updated since the browser last retrieved the file. If the file has not been updated then there is no need to retrieve the entire file, rather the existing version held in the browser's cache can be displayed.

The HTTP POST method is used to send data from the browser to a web server. Commonly the POST method is used to send all the data input by users within web-based forms. For example many web sites require users to create an account. The users details are sent back to the web server using the HTTP POST method.



Consider the following:

Using a Telnet client it is possible to execute HTTP methods (or commands) directly. The following steps outline how to accomplish this task using a machine running current versions of Microsoft's Windows operating system.

1. Start a DOS command prompt by entering `cmd` at the run command located on the start menu.
2. From the command prompt start Telnet with a connection to the required domain on port 80. Port 80 is the standard HTTP port on most web servers. For example `telnet www.microsoft.com 80` will initiate a connection to Microsoft.com.
3. Turn on local echo so you can see what you are typing. First type `Ctrl+]`, then type `set localecho` and press enter. Press enter again on a blank line.
4. Type your HTTP GET or HEAD command, including the host name and then hit enter twice. For example `GET /index.htm HTTP/1.1` then press enter, now type `Host: www.microsoft.com` and press enter twice. For GET commands the server will respond by sending the HTTP header followed by the document. For HEAD commands the server responds with just the HTTP header for the file. An example is shown below in *Fig 3.3*.

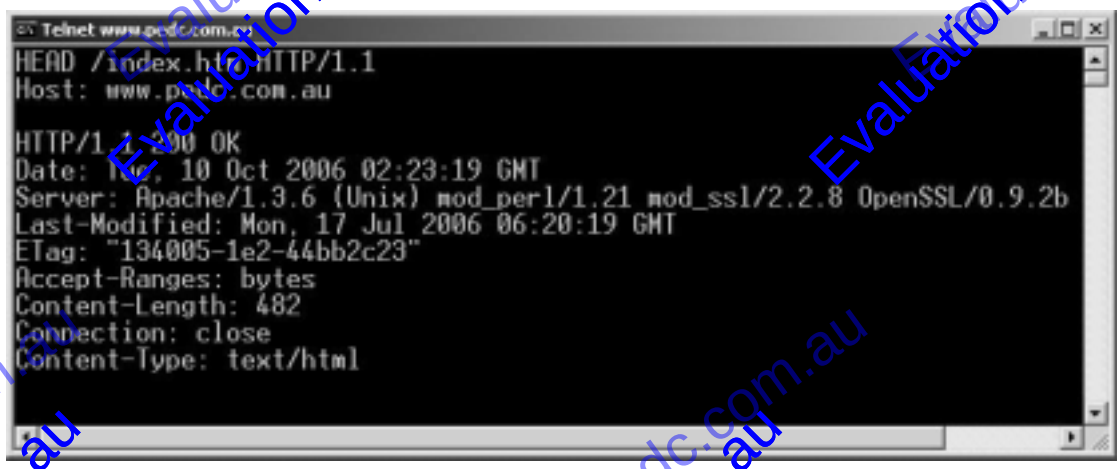


Fig 3.6
Screen dump of a Telnet session showing the HTTP HEAD method and the results for the file index.htm on the www.pedc.com.au domain.

GROUP TASK Practical Activity
Locate a simple web page using a web browser. Now use Telnet to retrieve the page using an HTTP GET command and then retrieve just the header using an HTTP HEAD command.

GROUP TASK Discussion
Discuss possible uses for the information contained within the HTTP headers returned by web servers.

Transmission Control Protocol (TCP)

TCP operates within the Communication Control and Addressing Level (Transport layer 4 of the OSI model). TCP, together with IP, are the protocols responsible for the transmission of most data across the Internet. The primary responsibility of transport layer protocols such as TCP is ensuring messages are actually delivered correctly.

Unlike most protocols that operate completely independently of their neighbouring protocols, TCP requires IP to be operating. TCP considers elements of the IP header – the reverse is not true, IP can operate without TCP, however for almost all implementations both TCP and IP are operating. This is why both TCP and IP are commonly referred to as TCP/IP.

In TCP terminology each packet is called a segment, where a segment includes a string of bytes forming part of the data to be sent. TCP includes checks for errors within each segment and also uses a system known as "sliding windows" to control the flow of data and ensure every byte of data is acknowledged once it has been successfully received. TCP is often called a "connection oriented" and "byte oriented" protocol as it maintains information about individual bytes transferred within a particular communication session.

Each TCP segment includes a header that includes the sequence of bytes contained within the segment and a checksum – we discuss the detail of checksums later in this section. The checksum is produced prior to the segment being sent. Upon arrival of each segment the checksum is recalculated to ensure it matches the checksum within the header. If it matches then the bytes received within the segment are acknowledged.

By default TCP segments contain a total of 576 bytes. This total includes 20 bytes for the TCP header and 20 bytes for the IP header, leaving 536 bytes for data. The sender in a TCP session continues sending segments of data up to the limit (window size) specified within acknowledgements from the receiver. Conceptually as subsequent segments are sent and received the window slides progressively along the length of the total message data, hence the name "sliding window". This flow control mechanism allows the receiver to adjust the rate of data it receives.

Consider the following:

Fig 3.7 below is a simplified conceptual view of the TCP sliding windows system at a particular point in time during a TCP communication session. In this diagram the "…cat sat on the mat…" text forms the complete message to be sent using multiple segments. Some data has been sent by the sender and acknowledged as correct by the receiver, some data has been sent but not yet acknowledged.

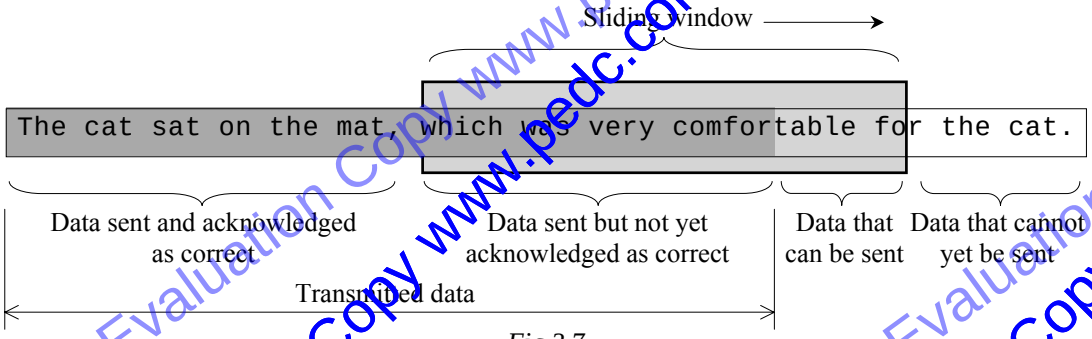


Fig 3.7
TCP uses a system known as "sliding windows" for flow control.

As the sender receives acknowledgements for transmitted segments the sliding window moves to the right. This movement enlarges the width of the "data that can be sent" region, hence the sender transmits more segments. Should segments fail to reach the receiver, contain errors or become delayed by network congestion then the window slides more slowly. When segments arrive quickly and without error the window slides more rapidly.

Pages 241 to 260

Not included in this Evaluation Copy

Intranet and Extranet

An intranet is a private network maintained by a company or government organisation and is based on the Internet protocol (IP). Many intranets include leased high-speed lines to connect their local area networks (LANs) into a private wide area network (WAN). The leased lines are dedicated to traffic on a specific private intranet. Such leased lines mean that the amount of data transferred is under the direct control of the intranet owner. This control becomes significant when real time synchronous applications are used. Some intranets connect LANs using the public Internet where all messages are encrypted during transmission to ensure privacy is maintained.

Extranets are an extension of an intranet to allow access to customers and other users outside the organisation. The interface between the extranet and the intranet must be secure – commonly firewalls, user names and passwords and also encryption is used. Extranets allow companies to share their services with other companies. For instance a large bank may provide online banking services to other smaller banks via its extranet.

Both intranets and extranets can also include virtual private networks (VPNs). VPNs use the infrastructure of the public Internet to provide secure and private connections to a company's internal network. A VPN allows employees to securely communicate with their company's network using any Internet connection. VPNs include tunnelling Transmission protocols, which not only encrypt and secure messages but also encrypt all internal network addresses. Examples of tunnelling protocols include Microsoft's Point to Point Tunnelling Protocol (PPTP), Cisco's Layer 2 Forwarding protocol (L2F) and the Layer 2 Tunnelling Protocol (L2TP) which is a standard that aims to combine the benefits and functions within both PPTP and L2F.

GROUP TASK Research
Explain why organisations may choose to set up an intranet in preference to simply using the public and less expensive infrastructure of the Internet.

TELECONFERENCING

Teleconference
A multi-location, multi-person conference where audio, video and/or other data is communicated in real time to all participants.

The term "teleconference" encompasses a wide variety of different real-time conference systems. From a simple three-way call using standard telephones to systems that share audio, video and other types of data between tens or even hundreds of participants. The essential feature of all teleconferencing systems is synchronous communication between many people in many different locations. Commonly many participants are present at one location whilst single participants are present at other locations. For example teleconferencing is routinely used for meetings between an organisation's head office and its branch offices. There are many participants present at head office and other participants at each branch office.

Historically the term "teleconference" referred to multi-person multi-location conferences sharing just audio over the PSTN - this audio only meaning is still used by many. Today such conferences routinely include video and various other types of data in addition to audio. Many references recommend using more descriptive terms, such as videoconference to describe systems that include video or e-conference when many data types are shared. In our discussion we shall use the more general meaning of teleconferencing that includes the real-time sharing of a variety of different data types.

We cannot hope to describe all the possible types of teleconferencing systems available. Rather we examine two particular examples of teleconferencing that utilise different information technology to achieve their purpose, namely:

1. Business meeting system, sharing audio over the PSTN.
2. Distance education system, sharing audio, video and other data using both the PSTN and the Internet.

For each teleconferencing system we identify the environment and boundaries, purpose, data/information, participants and information technology. We then discuss the information processes, in particular the essential transmitting and receiving processes used by the system. Finally we consider the advantages and disadvantages of teleconferencing within the context of the particular system.

GROUP TASK Research
Using the Internet, or otherwise, create a list of specific examples where teleconferencing is used.

1. BUSINESS MEETING SYSTEM, SHARING AUDIO OVER THE PSTN.

Environment / Boundaries

In this example we consider a medium sized business that has a head office in Sydney and five branch offices in country towns throughout NSW. At some stage during each Tuesday a teleconference is scheduled between the general manager, the four division managers and each of the branch mangers. The general manager and the division managers have offices within head office. Each of the division managers takes turns to chair and manage the weekly meeting.

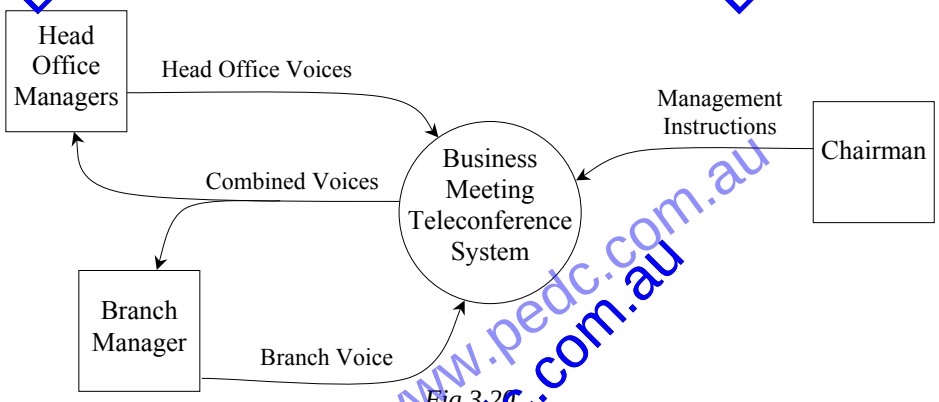


Fig 3.20

Initial context diagram for a business meeting teleconference system.

An initial context diagram describing this teleconferencing system is reproduced in *Fig 3.20* – the data flows and labels at this stage are incomplete. On this diagram just one of the branch managers is shown, in reality there are five branch managers. It makes sense to include the chairman as a separate entity as the inputs into the system from the chairman are different to their contributions as a member of the head office managers.

GROUP TASK Discussion
How does the initial context diagram in *Fig 3.20* assist to define the boundaries of the teleconferencing system?

Purpose

The needs that the weekly management meetings aim to fulfil include:

- Efficiently disseminating information to all managers throughout the organisation.
- Improving the efficiency of decision-making processes by managers – particularly with regard to including branch managers in the decision making process.
- Encouraging the sharing of ideas and strategies between members of the management team.
- Sharing of staff issues occurring at the local level with a view to more amicably and consistently resolving such issues across the entire organisation.
- Maintaining and enhancing interpersonal relationships between members of the management team.
- Inclusion of all managers, even if this means rescheduling the meeting at late notice.

Taking these needs and other more general business needs into account, the purpose of this business teleconferencing system is to:

- Provide the ability for all managers to contribute equally at weekly management meetings.
- Enable managers at remote locations to participate in all meetings without the need to travel.
- Output audio of sufficient quality such that all voices can be understood at all locations, including when multiple people are speaking at the same or different locations.
- Reduce costs through a reduction in the number of face-to-face management meetings required throughout the year.
- Be simple to setup, such that meetings can be rescheduled at late notice with minimal effort.
- Include only reliable, commonly available, well-tested technologies that provide a high quality of service without the need for onsite technical expertise during use.

GROUP TASK Discussion
Discuss how each of the above purpose statements assist in fulfilling one or more of the above needs.

Data / Information

The following table summarises the data/information used by the teleconference system. The table includes the audio input to and output from the system together with data required to access and manage the setup and operation of the system.

In this example system the meeting agenda and the minutes produced after the meeting are not included. Such data and information is outside the boundaries of the system that were defined on the initial context diagram.

Data/Information	*Data type*	*External Entity*	*Source OR Sink*	
Head Office Voices	Audio	Head Office Managers	✓	
Branch Voice	Audio	Branch Manager	✓	
Combined Voices	Audio	Head Office Managers /Branch Manager		✓
Management Commands	Numeric	Chairman	✓	
Start Date/Time	Numeric	Chairman	✓	

Host PIN	Numeric	Chairman	✓	
Guest PIN	Numeric	Branch Manager	✓	
Dial in Number	Numeric	Chairman /Branch Manager	✓	
Simulated Voice Response	Audio	Chairman /Branch Manager		✓

The details from the above table form the basis for completing the data flows on the initial context diagram – the final version is reproduced in *Fig 3.21*. Note that the chairman has the responsibility for setting up the technology including when the conference will take place prior to each conference. All non-audio inputs are numeric as they are entered via a telephone keypad.

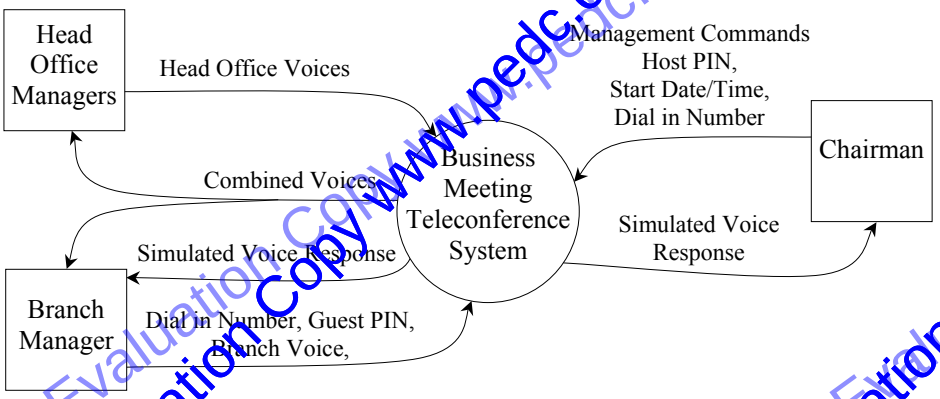


Fig 3.21
Final context diagram for a business meeting teleconference system

Participants

The general manager and the four division managers at head office, one of which acts as the chairman. The five branch managers located in different country towns throughout the NSW.

Information Technology

- Standard telephones used by each branch manager to dial into the system, enter their Guest PIN and also to speak and listen during the conference.
- Polycom Sound Station 2W^{TM} Wireless Conference phone used at head office (see *Fig 3.22*). The Polycom Sound Station 2W^{TM} includes three high quality microphones to collect head office participant's voices. It also includes a high quality speaker for displaying audio from branch managers. The conference phone is full-duplex to allow branch voices to be heard whilst head office participants are speaking.

Fig 3.22
Polycom Sound Station 2W conference phone.

- Teleconferencing server controlling a PABX (Private Automatic Branch Exchange) that connects the PSTN circuits originating from head office with each of the PSTN circuits originating from the branches (see *Fig 3.23*). This server is maintained by a teleconferencing company who charges for its service on a per/minute per connection basis for each conference.
- PSTN used to transmit and receive all data. The data is in analog form at each branch, at head office and also as it enters the PABX at the Teleconferencing Company.

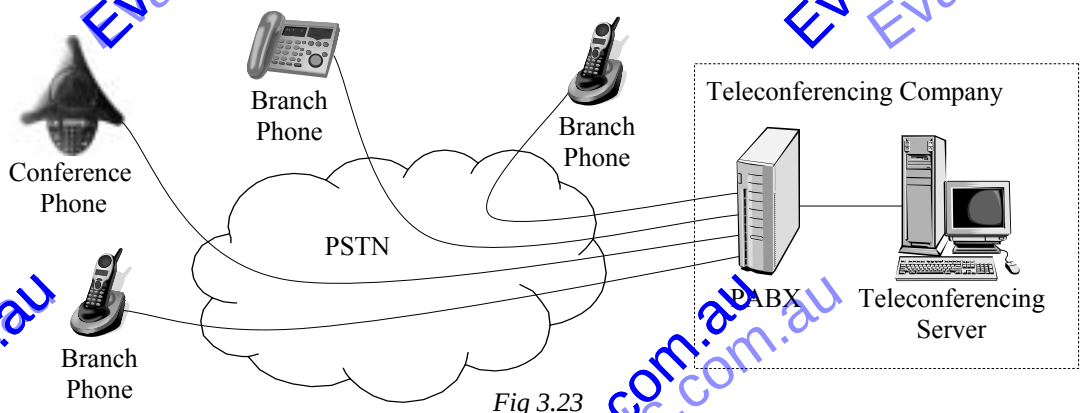


Fig 3.23
Network diagram including significant hardware within the business meeting system, sharing audio over the PSTN.

Information Processes

The following processes occur during a typical teleconference:

- Step 1. Setup by chairman

Prior to the teleconference the chairman rings the phone number of the teleconferencing server (Dial in Number). The chairman enters the Host PIN and is then prompted by the server to configure the conference. The server uses simulated voice prompts and the chairman responds by entering numbers through their phone keypad. The configuration includes the date and time of the conference together with the creation of a Guest PIN. The chairman provides the time and Guest PIN to each of the branch manager participants.

- Step 2. Participants enter conference

Just prior to the scheduled start time the chairman dials the teleconferencing server and enters the Host PIN using the conference phone. They follow the voice prompts to commence the conference. To join the conference each branch manager participant dials the "Dial in Number" and enters the Guest PIN. The teleconferencing server directs the PABX to connect the telephone line from each branch manager participant to the head office line. Once all branch managers have dialled in the conference can commence. The company pays a per minute charge for each connection used during a teleconference.

- Step 3. Conference takes place

During the teleconference all participants' voices are transmitted and received along the same single circuit. As is the case with any standard phone call, each local telephone only displays remote voices (and other audio). Prior to display local audio is filtered from the signal by the local phone.

- Step 4. Conference ends

The conference ends automatically when the conference phone hangs up. This occurs as soon as the teleconferencing server detects that the phone line that commenced the conference has been disconnected. The teleconferencing server then calculates the charge for the conference based on the total conference time and the number of participants.

GROUP TASK Activity
Create a step-by-step description of the steps required to setup and run one of the business teleconferences.

Advantages / Disadvantages

Advantages include:

- Reduction in costs associated with travel and accommodation. Furthermore branch managers are not absent from their offices as often and unproductive travel time can be used more productively.
- No additional hardware or software required apart from the conference phone at head office. There is no need for onsite technical help as the technical side of the conference has been outsourced to the teleconferencing company.
- Simple to setup and schedule conferences as required. Face to face meetings must be scheduled well in advance, whilst teleconferences can occur when and as required. This allows urgent decisions and issues to be resolved and information to be disseminated more efficiently.
- More regular communication between the complete management team results in better informed decisions and improved communication of these decisions. Furthermore issues occurring at the local level are better understood by head office, hence more appropriate solutions result.

Disadvantages include:

- Face to face communication includes body language and facial expressions – such communication is totally lost using a voice only system.
- Branch managers are not physically present, whilst division managers and the general manager are. This reduces the ability of branch managers to develop close inter-personal relationships with other members of management.
- It is difficult to maintain concentration during extended phone calls. From the branch manager perspective each teleconference is essentially an extended phone call.

GROUP TASK Discussion
The business described above has outsourced the technical side of its teleconferencing. Identify advantages and disadvantages of outsourcing in this situation.

2. DISTANCE EDUCATION SYSTEM, SHARING AUDIO, VIDEO AND OTHER DATA USING BOTH THE PSTN AND THE INTERNET.

Environment / Boundaries

In this example we consider a teleconferencing (or web conferencing) system used by ABC University. The system transmits audio over the PSTN using a system similar to the previous business meeting system. The system also transmits and receives live video and other digital data using IP over the Internet. Various University courses use the system so that students at remote sites can both observe and contribute to live presentations as they occur in front of local students.

The presenter and the local students are present within a purpose built teleconferencing room at ABC University. Each remote student connects to the conference via a standard telephone line for audio content and via a web browser running on a personal computer with a broadband Internet connection for video and other data.

Purpose

Students at ABC University are able to complete many degrees as either full-time on-campus students or as part-time off-campus students. The teleconferencing system aims to provide the off-campus students equal access to live presentations without the need for lecturers to duplicate or significantly modify their presentations.

The purpose of this teleconferencing system is to:

- Enable remote off-campus students to be equal participants in live presentations.
- Remove the need for lecturers to prepare different material for on and off campus students.
- Allow individual remote students to connect to teleconferences using their existing hardware and broadband Internet connections.
- Allow presenters to seamlessly operate the technology with minimal disruption to the local student's view of the presentation.

Data / Information

Data/Information	*Data type*	*Description*
Participant Audio	Audio	Audio from the teleconferencing room and remote students is added to a shared PSTN circuit.
Combined Audio	Audio	Mixed audio from all sites is present on the shared PSTN circuit.
Participant Video	Video	Video from the teleconferencing room and each remote student is transmitted using IP and the Internet to a remote chat and video conferencing server.
Video Stream	Video	Video from the chat and video server is transmitted using IP to participant's web browsers. A separate stream is used for each connection and is tailored to suit the actual speed of the individual connection..
Application Data	Various	Includes data to enable the sharing of documents, virtual whiteboard, desktops and other types of digital data. This includes the ability to concurrently edit the virtual whiteboard and single documents.
Chat Data	Text	The system includes an instant messenger chat feature. Chat data can be broadcast to all participants or between specific individuals. All chat data passes through the Chat and Video Conferencing Server.
Conference IP Address	Numeric	The IP address of the conference management server used by all participants to connect to the system.
Participant IP Address	Numeric	The IP address of each computer participating in the conference.
Dial in Number	Numeric	Used to connect voice via the PSTN to the remote telephone conferencing server.
Student PIN	Numeric	Used by students to verify their identity as they initiate telephone and web sessions.
Presenter PIN	Numeric	Used by the presenter to verify their identity as they initiate telephone and web sessions.

Participants

- Lecturers who present material from the purpose built teleconferencing room.
- Full-time students who are present within the teleconferencing room.
- Part-time students who connect to the teleconference presentation from their own home or office.

Information Technology

Fig 3.24
Purpose built audio/video/web teleconferencing room.

Fig 3.25
WebConference.com™ software within Internet Explorer.

Teleconferencing room:

- Personal computer with web browser, WebConference.com™ software and high-speed Internet connection.
- Three large monitors – one for displaying video of participants, another for other application data. The third monitor is used to display data to the presenter so they do not need to turn away from their audience.
- DLP data projector used by the presenter to display any data source to the local students using a remote control.
- Document camera for collecting images and video of paper documents as well as 3D objects.
- Video camera with pan, tilt and focussing functions as well as the ability to follow the current speaker's voice.

- DVD and video player – the output can replace the normal video camera.
- High quality microphones throughout the room. The main presenter wears a lapel microphone. The microphone system includes echo cancelling so that audio from the speakers is not retransmitted.
- High quality speaker system optimised for voice frequency output.

Remote Students:

- Personal computer with web browser connected to a broadband Internet connection.
- WebConference.com™ software which is downloaded and run automatically within the student's browser – an example screenshot is reproduced above in *Fig 3.25*.
- Web camera for collecting local video.
- Standard telephone, however a headset is recommended.

Teleconferencing Service Provider (in this example WebConference.com™):

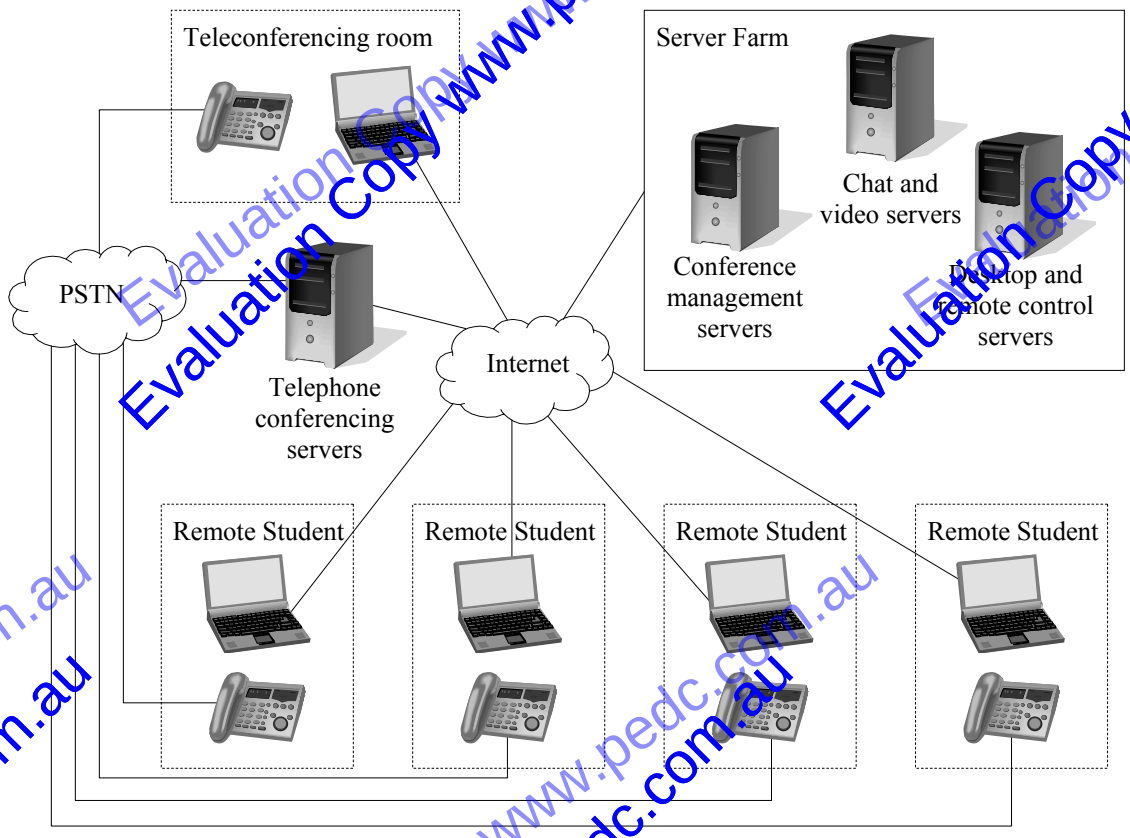


Fig 3.26

Network diagram including significant hardware within the WebConference.com™ system, sharing audio over the PSTN and IP data over the Internet.

- Multiple server farms (see *Fig 3.26*) that include collections of the following servers in a variety of different locations throughout the world.
- Conferencing management server used to control the setup and running of each conference. This includes directing connections to other servers and other server farms before and during the conference to ensure a continuous high quality of service.
- Chat and video server receives video and chat data from all participants and transmits this data out as required. The server creates and transmits suitable streams of video data to each participant's web browser based on the current speed of each participant's Internet connection.

- Desktop and remote control server used to receive and transmit application data. For example the presenter may share an open Word document on their local machine such that remote students can edit the document synchronously.
- Telephone conferencing server used to connect all PSTN lines from all participants to form a single shared circuit.

Information Processes

Some general collecting and displaying information processes occurring include:

- Collecting – audio using telephone and conference room microphones, video using cameras, text using keyboard, images using document camera.
- Displaying – audio using speakers in conference room and speaker in remote student's phones, video and other data types are displayed on monitors and using the DLP data projector.

Let us consider how video is transmitted and received in some detail. The data flow diagram in *Fig 3.27* describes this process for a single stream travelling from the teleconferencing room to a single remote student – clearly there are potentially numerous other streams travelling in all directions between all participants. The points that follow elaborate on the DFD:

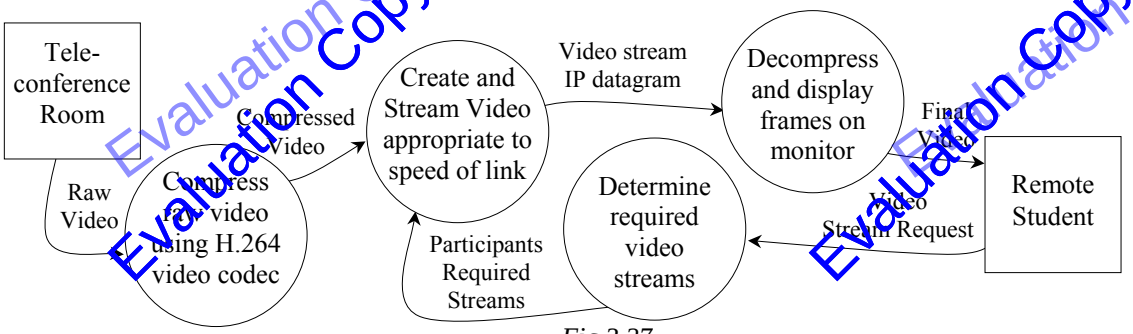


Fig 3.27
DFD describing the transmission of a single video stream.

- Raw video is collected as a sequence of images called frames by the video camera. For many applications the video camera includes a microphone and hence sound samples are also collected – within this example system no audio is collected by the video cameras. The raw frames from the conference room are collected at a far higher resolution than those collected from each remote student's web camera.
- The raw video frames are fed in real time through a software-based codec. In this example the MPEG-4 part 10 or H.264 codec is used. A codec is used to compress and decompress data prior to and after transmission. The codec compresses the video using an efficient block-based compression technique. We discussed block-based coding in some detail on page 59 and 60 of the related IPT Preliminary Text.
- The compressed video data is transmitted via the Internet to the Chat and Video server. This server determines which streams of video data each participant requires and prepares to transmit just those streams to the participant's web browser. For example typically a remote student will view video from the teleconference room and perhaps streams from two or three other remote students.
- Each chat and video server includes streaming video server software. This software is able to determine the optimum transmission speed for each participant's Internet link. The job of the streaming server is to adjust the resolution and frame rate of each video stream to maximise the quality of the video transmitted to each participant. For example a slower link will receive smaller and fewer frames than a faster link. Furthermore the quality of the video can be altered by the streaming server in real time should the speed of a link change during the conference.

- The stream of video is ultimately transmitted as a sequence of IP datagrams. Higher resolutions and frame rates require more IP datagrams per second than lower resolutions and frame rates.
- As the stream of IP datagrams are received the same H.264 codec is used by the receiver's computer to decompress the video. Finally the decompressed frames are displayed on the receiver's monitor.

Advantages / Disadvantages

For this example we restrict our advantages/disadvantages to those concerned with technical aspects of the system.

Technical advantages include:

- Remote students do not require any specialised or dedicated information technology apart from the free and automatically installed WebConference.com™ software operating within their browser.
- Video streams are automatically adjusted to suit the speed of each participant's Internet connection. This means slower speed connections receive a continuous video experience, albeit at reduced resolution and frame rates.
- The quality of audio is not affected by poor or congested Internet connections. The PSTN provides an audio signal of equal quality to all remote participants. Even if a student's Internet connection is lost the audio is still active.
- The system includes redundant servers and server farms so that failure of a single server or connection to a single server farm does not disrupt conferences.

Technical disadvantages include:

- Some remote students will experience poor quality video due to slower Internet connections. Most remote students are likely to receive video of somewhat lower quality compared to those students present within the teleconferencing room.
- Most remote students connect from their home. Therefore their home telephone is tied up for the duration of each conference.

GROUP TASK Discussion
Identify and describe more general advantages and disadvantages of the above system for each of the system's participants.

Consider the following:

During a conference the same video stream originating from the teleconferencing room is being sent multiple times as a separate stream to each remote student. This system is an example of a multipoint Unicast transfer. There are currently two types of multipoint transfer that can be used over an IP network – Unicast and Multicast. Unicast is a point-to-point system where each IP datagram travels to exactly one recipient – this is the normal method currently used to transfer virtually all IP datagrams across the Internet. Multicast is a one-to-many system where a single IP datagram is sent to many recipients.

The multicast system requires a multicast destination IP address within the IP datagram. During transmission of a multicast IP datagram each router examines the multicast destination address and may then decide to forward the datagram along more than one connection. The multicast system has the potential to significantly improve the speed of transfer for streamed video (and also audio) over the Internet. Although many current routers include support for the required multicast protocols there are many that do not and there are many other routers where multicasting is turned off – multicast IP datagrams arriving at such routers are simply discarded.

GROUP TASK Research
Using the Internet, or otherwise, identify and briefly describe the protocols used by routers to route multicast IP datagrams.

GROUP TASK Discussion
Explain how multicasting can significantly speed up the transfer of streamed audio and video.

HSC style question:

A company has won a contract to supply security infrastructure and personnel for the 2008 Beijing Olympics. The company has offices in Sydney, London, New York and now Beijing. Each week the senior management at all offices participate in a teleconference over the Internet that includes both audio and video.

(a) Compare and contrast the use of teleconferencing with traditional telephone and face-to-face communication in this situation.

(b) Identify and briefly describe the information technology required by this teleconferencing system.

(c) Describe how data is transmitted and received between offices during one of the weekly teleconferences.

Suggested solution

(a) Both teleconferencing and traditional methods allow people from different offices in different parts of the world to communicate effectively. This teleconferencing system includes video in addition to audio. Multiple participants can hear and see the other participants of the conference. For this company the participants are located in different offices across the world. Therefore the system requires high speed Internet links to transmit the video and audio data. The quality of the video and audio is dependent on these public Internet links.

Face-to-face communication can only occur between people in the same location. This means face-to-face meetings would need to be scheduled at one of the offices (Sydney, London, New York or Beijing) and there would be large expenses and work time lost in getting people from the other offices in for the meeting. Furthermore it would be impractical for such face-to-face meetings to occur on a regular basis.

Traditional telephone is audio communication between two people over the PSTN – or three people, if a three-way conference call is possible. The participants can only hear the other person's voice, there are no visuals and so body language plays no part in the conversation, hence business and personal relationships are harder to build. This teleconferencing system assists in this regard as it includes video and it supports synchronous communication between many more participants.

In this example the audio is transmitted over the Internet. Due to the packet-switched nature of IP transmissions the audio will be of lower quality than is possible using a normal circuit-switched telephone line. Also the company does not control the Internet, hence transmission speeds between participants will vary which will affect the quality of both the audio and video.

The significant advantage of teleconferencing for an international company is that none of their workers need to leave their home country to participate in the conference. The use of teleconferencing reduces expenses (no plane and accommodation costs) and maintains productivity (no wasted hours on plane trips). It also allows the company to have frequent meetings at short notice and at relatively minimal cost.

(b) The hardware required by each participant includes a video and audio capture device at each location. This is likely to be a simple webcam with microphone. Each location must also have a screen in which to display the images from each location as well as speakers to play the audio. Inside the computer there needs to be a sound and video card.

A high-speed network link to the Internet is needed so that the data (video and audio) can be transmitted and received in nearly real time. Faster links resulting in high resolution and smoother video together audio that is in sync with the video. This means that each office will require a fast broadband Internet connection.

Software is required that captures the video and audio and streams across the Internet to the teleconferencing server. In this case the video and audio would be combined (multiplexed) and sent together as a continuous stream of IP datagrams.

A teleconferencing server is needed with multiple high-speed Internet links. It receives the streams from each participant and sends out an individual video/audio stream to each participant. Multicasting is unlikely to be possible as the transmission is over the public Internet.

(c) At a teleconference each participant's analog data is captured as digital video frames and digital sound samples. This data is then multiplexed and compressed together using a codec such MPEG 4. The data is then streamed over the Internet to the teleconferencing server as a sequence of IP datagrams.

The teleconferencing server receives the video/audio streams from each participant. It also determines the particular streams requested by each participant and the current speed of their individual transmission links. The server then produces a suitable stream for each participant that will maximise the quality of his or her received video and audio. The stream sent is altered during the conference in response to changing transmission speeds.

At each participant location the received data is decompressed and then broken down into the audio and video components. Finally the audio samples are converted to analog and output through the speakers. As this occurs the video frames are displayed in sequence on the participant's screen.

Comments

- In an HSC or Trial examination this question would likely be worth nine marks – three marks for each part.
- A multicast system could be described, however at the time of writing there were few Internet connections that support IP multicasting between different countries.
- Presently most business teleconferencing systems use the PSTN for audio. In this case the question states that the Internet is used for both video and audio.
- A conference phone could be used at each office as it is likely that more than one participant is present at some locations.

SET 3C

1. During a telephone call over the PSTN, which of the following is TRUE?
   (A) Data can travel over a variety of different routes during a conversation.
   (B) A single connection is maintained for the duration of the call.
   (C) The data is split into packets that travel independently of each other.
   (D) The same circuit may be shared with IP and other voice data.

2. Which of the following terms best describes a private WAN connecting a company's various offices?
   (A) Intranet
   (B) Extranet
   (C) Internet
   (D) PSTN

3. The PSTN is currently used for audio in many teleconferences because:
   (A) voice quality is better on a connectionless network.
   (B) currently multicasting is not widely implemented on the Internet.
   (C) circuit switched networks provide higher levels of security.
   (D) voice quality is better on a connection-based network.

4. When participants are widely dispersed, which of the following is an advantage of teleconferencing systems compared to face-to-face meetings?
   (A) Ability to develop personal relationships is enhanced.
   (B) Specialised information technology is required.
   (C) Significant savings in terms of money and time.
   (D) All of the above.

5. Which of the following is TRUE for PSTN based audio conferences?
   (A) Each participant has a different circuit.
   (B) Audio from each participant is transferred as a sequence of packets.
   (C) All participants share a single circuit.
   (D) Each participant must use a dedicated conference phone.

6. The purpose of a streaming video server is:
   (A) to adjust the quality of the video stream sent to each participant based on their transmission speed.
   (B) to transmit identical streams of video to all conference participants.
   (C) to ensure a continuous connection between all participants is maintained.
   (D) to connect and disconnect participants as they enter and leave the conference.

7. With regard to the video received during a videoconference, which of the following is TRUE?
   (A) All participants in a video conference must receive video of identical quality.
   (B) The quality can never exceed that of the collected video.
   (C) The codec used by the sender can be different to the codec used by the receivers.
   (D) Video quality decreases as transmission rates increase.

8. When IP multicast is used, which of the following occurs?
   (A) Each participant receives the same stream.
   (B) Each participant receives their own stream.
   (C) A dedicated streaming server is definitely required.
   (D) Video cannot be sent from multiple locations.

9. Teleconferencing can best be described as:
   (A) synchronous and simplex.
   (B) asynchronous and full duplex.
   (C) asynchronous and simplex.
   (D) synchronous and full duplex.

10. Which list contains devices used to collect data during teleconferences?
    (A) Phone, monitor, keyboard, mouse.
    (B) Speakers, monitors, headsets, projectors.
    (C) Phone, video camera, document camera, keyboard, mouse.
    (D) Video camera, document camera, speakers, scanners.

11. Define each of the following terms:
    (a) Internet (b) PSTN (c) Intranet (d) Extranet (e) Teleconference

12. Compare and contrast IP unicasting with IP multicasting with regard to their use in teleconferencing systems over an intranet and over the Internet.

13. Explain the differences between packet switched connectionless networks and circuit switched connection-based networks.

14. Outline the processes performed by teleconferencing servers when:
    (a) sharing audio over the PSTN. (b) sharing video over the Internet.

15. Compare and contrast teleconferencing systems with face-to-face meetings.

MESSAGING SYSTEMS

In this section we first consider the basic operation of traditional phone and fax systems operating over the PSTN. We then consider enhancements to the traditional phone system to include voice mail and information services. We then consider VoIP, a system for making phone calls using the Internet. Finally we examine the characteristics of email and how it is transmitted and received.

1. TRADITIONAL PHONE AND FAX

Telephones

Telephones and the PSTN network connecting homes and organisations operate using similar principles as the original system first implemented over 100 years ago. Essentially all telephones have a microphone, a speaker, some sort of bell and a simple switch to connect the phone to the telephone network. A 100-year-old phone will still operate on most of today's phone lines. The only significant difference being the signals used to dial numbers – older phones use pulse dialling whereas current phones use tone dialling. When pulse dialling the phone switch is rapidly disconnected and connected the same number of times as the number being dialled – techniques included tapping the hook the required number of times or rotating a dial. Tone dialling transmits different frequencies to represent each number.

Fig 3.28
Rotary dial telephone in common use from 1940-1990.

In many older homes the copper wires connecting the phone to the PSTN network have been in place for many more years than originally intended, it is what happens once the wires reach the local telephone exchange that has changed. In the past, actual mechanical switches were used to connect the copper wire from your home phone directly with the copper wires connected to the phone being called. Circuit switching creates a direct connection or circuit between the two phones. In the days of manual switchboards, operators would manually connect the wires running from your home with the wires running to the person's phone you wished to call. Although manual switching has now been completely replaced by electronic switching, the PSTN circuit switched network operates using this very same connection-based principle, that is, a direct connection is setup and maintained whilst each conversation takes place.

During a typical conversation we spend less than half the time listening, less than half the time speaking and the remaining time in relative silence. This is not such a concern between a phone and its local exchange, however over longer distances the inefficiencies are significant. Today, apart from the connection between telephones and their local exchange, the remainder of the PSTN is essentially digital. Digital networks make much more efficient use of the lines. By digitising the analog voice signals it becomes possible to compress the bits and also to combine (multiplex) many conversations on a single physical connection. This means many conversations share the same line simultaneously. Various different modulation schemes are used depending on the range of frequencies used and the physical attributes of the cable. For example time division multiplexing (TDM), used on tier 1 (T1) lines, samples each voice 8000 times per second and each of these samples is coded into 7-bits. A total of 24 voice channels are combined onto a single copper circuit. Most medium to large organisations do away with analog lines altogether, rather they have one or more T1 lines that directly enters their premises.

It is the digital nature of most of the PSTN that has allowed most phone companies to provide their customers with additional features, such as call waiting, caller id, three-

way calls, call diversion and voice mail. The processing required to implement these features occurs at the telephone exchange – the customer sends commands to access and control the feature using tones generated by their phone's keypad. Furthermore much of the PSTN's digital infrastructure is used to transmit IP data across the Internet.

GROUP TASK Discussion
Explain the difference between analog and digital voice signals. Why do you think analog signals are still used between most phones and their local telephone exchange? Discuss.

Facsimile (Fax)

Alexander Bain first patented the basic principle of the facsimile, or fax machine, in 1843. Incredibly this is some 33 years before the telephone was invented. It was some twenty years later that the first operational fax machines and transmissions commenced. Initially it seems odd that fax pre-dates telephones, however in fact it makes sense. At this time the telegraph system using Morse code was in operation. Morse code was transmitted by opening and closing a circuit, which is similar to the binary ones and zeros used by today's fax machines.

It wasn't until the late 1960s that fax machines became commercially viable; these machines adhered to the CCITT Group 1 standard, which used analog signals and took some 6 minutes to send each page. The message was sent as a series of tones, one for white and another for black, these tones were then converted to an image using heat sensitive paper. By the late 1970s the fax machine had become a standard inclusion in most offices. A new Group 2 standard was introduced; these Group 2 machines generated digital signals and used light sensors to read images on plain paper originals. Soon after machines were developed that used inkjet and laser printer technologies to print directly onto plain paper. The Group 3 standard was introduced in 1983; it contained various different resolutions together with methods of compressing the digital data.

Fig 3.29
Fax machines are standard items in almost all offices.

Today computers are routinely used to produce, send and receive faxes; in fact most dial-up modems have built in fax capabilities. There are even Internet sites that allow a single fax to be broadcast to many thousands of fax machines simultaneously. It is common today for a single device to integrate scanning, faxing and printing.

GROUP TASK Discussion
Brainstorm specific examples where fax has been used. For each example, discuss reasons why fax has been used in preference to phone, email or other messaging systems.

2. VOICE MAIL AND PHONE INFORMATION SERVICES

Voice mail, in its simplest form, is much like a digital version of a traditional answering machine. Calls that are not answered after a predefined number of rings are diverted to the voice mail system. The voice mail system answers the call and plays a pre-recorded outgoing message (OGM). The OGM welcomes the caller and provides instruction on how to leave a message – for residential phones the OGM may be as simple as "Hi, you've reached Sam, please leave a message after the tone and I'll get back to you ASAP." The voice mail system then digitally records the users voice and

stores it within the customers voice mailbox. At some later time the customer rings the voice mail system, verifies their identity using a numeric password and listens to the voice messages held in their voice mailbox. During message retrieval the customer uses their phone keypad to enter commands that control the voice mail system. No doubt we are all familiar with such systems.

GROUP TASK Activity
Create a DFD to describe the data flows, external entities and basic processes in the simple voice mail system described above. Include just two processes – "Leave Message" and "Retrieve Messages".

The familiar voice mail system described above is normally a service provided by the customer's local telephone service provider – Telstra, Optus, Orange, etc. The servers used to process messages are located and owned by the telephone company. More sophisticated voice mail systems are used by business and government organisations. These organisations maintain their own systems. Such systems include a multitude of features designed to meet the needs of the individual organisation and its customers. They do a lot more than maintaining voice mail for many users. Commonly such systems integrate with other messaging systems such as email and fax, and they provide automated information services and call forwarding functionality to customers. For our purposes we more accurately describe such systems as Phone Information Services.

The majority of phone information systems include a hierarchical audio menu whereby customers navigate down through the hierarchy of menus to locate information or be directed to specific personnel. The available options at each level of the hierarchy are read out as an OGM, the customer responds using their phone's keypad or using voice commands to progress to the next level.

Some of the features present within Phone Information Services include:

- Voice mail management for many users. Customers enter the extension number of the required person and if not answered the system records the message to the person's mailbox.
- Support for multiple incoming and outgoing lines of different types. Today large organisations will have many digital T1 lines connected directly to the PSTN and also VoIP (voice over IP) lines connected to the Internet via broadband connection.
- Fax on demand where customers navigate a menu system to locate and request particular documents to be faxed back.
- Call attendant functions where the menu system filters callers through to the correct department based on the caller's selections. Some systems can forward calls to other external lines.
- Text to speech (TTS) capabilities that allow text to be read to users over the phone. For example, TTS can be used to read emails and other text documents or more simply it is often used to read numbers and currency amounts back to customers to verify their data entry.
- Call logging to databases. For example records commonly include the caller id, time and length of call. This data is analysed to provide management information to the organisation.
- Provision of information to customers. The OGMs include information rather than just details of how to navigate the menu system. For example in Australia numbers with the prefix 1900 provide such information on a user pays basis.

- Automated ordering systems that allow customers to order and pay for products without the need for a human operator. Often includes collecting and verifying credit card payments.
- Automated surveys where answers to questions are stored within a linked database. Some commercial surveys use the 1900 system or the SMS system where the user is charged on their telephone bill for their contribution. The telephone company forwards the funds to the survey provider.
- Integration of voice mail with other messaging systems. For example voice mail messages are converted to email messages and appear in the recipients email inbox. The email can include the voice message as an audio attachment or the audio can be converted to text using voice recognition.

GROUP TASK Discussion
Brainstorm a list of phone information services members of your class have used. Identify and briefly describe features within these services.

GROUP TASK Research
Currently VoIP is becoming a popular alternative to standard PSTN lines. It is likely that by the time you read this it will be a routine method for making phone calls. Research VoIP and describe its essential differences compared to traditional telephone lines.

Consider the following:

ISO/IEC 13714 is the international standard for interactive voice response (IVR) systems. Recommendations within this standard include how each key on a standard telephone keypad should be used when designing menus for IVR systems. These recommendations include:

- # key – used to delimit data input or to stop recording and move to the next step. It can also be used as a decimal point. The preferred name for # is "hash".
- * key – used to stop the current action and return the caller back to the previous step. Often this means the last OGM will replay. When entering data the * key should clear the current entry. The preferred name for * is "star".
- 0 key – if possible the 0 key should be used to transfer the call to an operator or to provide help on the current feature or action. The preferred name for 0 is "zero".
- 9 key – used to hang-up the call where this is a suitable option.
- Yes/No responses – the 1 key should be used for Yes and the 2 key used for No.
- Alpha to numeric conversions – America and the rest of the world use slightly different mappings. To ensure IVR systems work on both systems the following mappings should be used:

1 – QZ	4 – GHI	7 – PQRS
2 – ABC	5 – JKL	8 – TUV
3 – DEF	6 – MNO	9 – WXYZ

  Note that 1 and 7 map to Q and that 1 and 9 map to Z.
- OGMs should refer to numbers on the telephone keypad not letters.
- OGMs should be phrased with the function first followed by the key to press. For example "To pay an invoice press 2".
- Menu OGMs should be in ascending numerical order with no gaps in numbering.

- Commonly used functions should be listed first. For example pressing 1 causes the most commonly used function to activate.
- In general menus should be limited to 4 commands (excluding help, operator transfer, back and hang-up commands).

GROUP TASK Discussion
In your experience, have these recommendations been implemented within phone information services you have used? Discuss reasons for the existence of the ISO/IEC 13714 standard.

Storyboarding and simulating an example IPT Phone Information Service

In this example we shall develop a phone information system to provide basic information about the IPT HSC course and each of its component topics. In addition the system will be able to record student's questions into a voice mailbox corresponding to the topic.

Consider the essentially hierarchical storyboard reproduced in *Fig 3.30*. Each rectangle on this storyboard corresponds to an OGM (outgoing message) – some OGMs are menus, others simply provide information and some do both. Think of an OGM as the audio version of a screen on a normal storyboard – both screens and OGMs display data. The lines between each OGM rectangle include the key used to navigate from OGM to OGM. Notice that a line exists from each topic to the voice mailboxes. In the final system a separate mailbox will be maintained for each topic. Each mailbox is linked to the email address of an expert on that topic. When a question is left by a student caller it is immediately emailed to the corresponding topic expert. The email includes the phone number (CallerID) of the student caller together with an audio file attachment and the topic name.

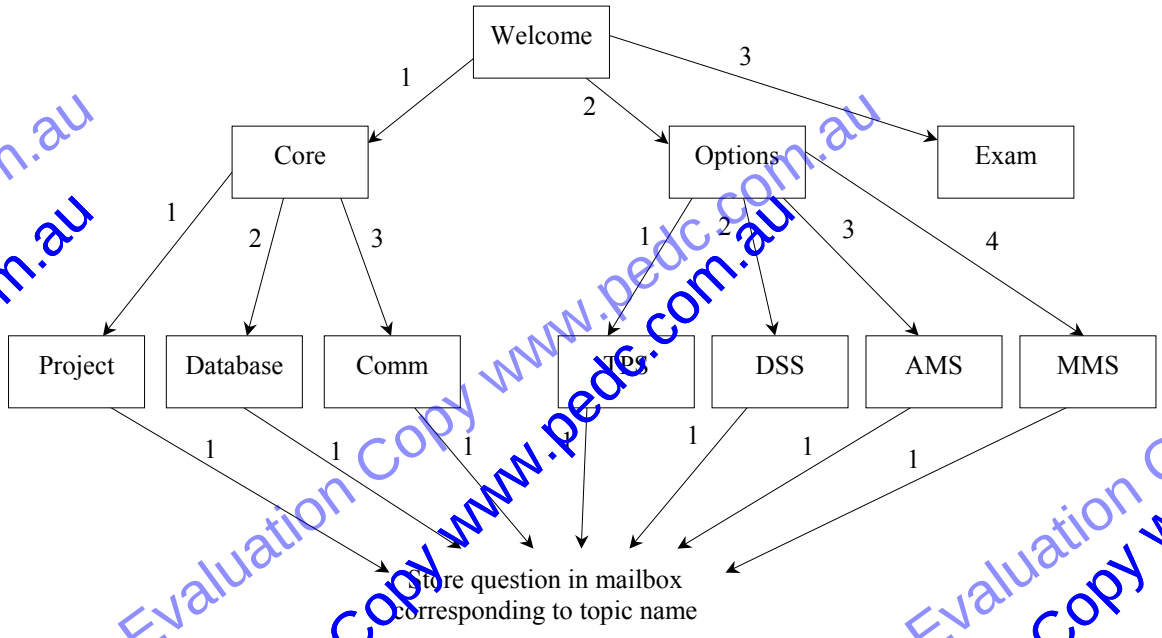


Fig 3.30
Storyboard showing the links between OGMs for the example IPT Phone Information Service.

When we create a storyboard for a user interface we also create designs for each individual screen. When designing OGMs we need simply design the text that will be spoken (or synthesised) for each OGM. The table in *Fig 3.31* details the text of each OGM together with actions performed in response to user key presses.

OGM Name	*Text*	*Action*
Welcome	Welcome to the IPT HSC command centre. We provide general information and answers to specific questions on all topics. For core topics please press 1. For option topics please press 2. For HSC examination details press 3.	1- go to Core OGM 2- go to Options OGM 3- go to Exam OGM *- repeat Welcome OGM 9- end call.
Core	There are 3 core topics each worth 20 percent. For project work press 1. For Information systems and databases press 2. For Communication Systems press 3.	1- go to Project OGM 2- go to Database OGM 3- go to Comm OGM *- go to Welcome OGM 9- end call.
Options	There are 4 options of which 2 must be completed. For Transaction Processing Systems press 1. For Decision Support Systems press 2. For Automated Manufacturing Systems press 3. For Multimedia systems press 4.	1- go to TPS OGM 2- go to DSS OGM 3- go to AMS OGM 4- go to MMS OGM *- go to Welcome OGM 9- end call.
Exam	The IPT HSC Examination is a 3 hour exam that contains 3 sections. Section 1 is worth 20 marks and is composed of 20 multiple choice questions based on the 3 core topics. Section 2 is worth 40 marks and is composed of 4 free response questions based on the 3 core topics. Section 3 is worth 40 marks and contains one 20 mark question for each option topic. You must complete 2 questions. To return to the previous menu press the star key.	*- go to Welcome OGM 9- end call.
Project	Project work involves planning, designing and implementing an information system that has a specific purpose. To leave a question about project work press 1.	1- leave message in Project mail box *- go to Core OGM 9- end call.
Database	Information systems and databases emphasises the organising, storing and retrieving processes within database systems and hypermedia. To leave a question about information systems and databases press 1.	1- leave message in Database mail box *- go to Core OGM 9- end call.
Comm	Communication systems support people by enabling the exchange of data and information electronically. This topic emphasises the transmitting and receiving processes. To leave a question about communication systems press 1.	1- leave message in Comm mail box *- go to Core OGM 9- end call.
TPS	Transaction processing systems meet record keeping and event tracking needs of organisations. To leave a question about transaction processing systems press 1. To go back to the previous menu press the star key.	1- leave message in TPS mail box *- go to Core OGM 9- end call.
DSS	Decision support systems use models, analytical tools, databases and automated processes to assist decision making. To leave a question about decision support systems press 1. To go back to the previous menu press the star key.	1- leave message in DSS mail box *- go to Core OGM 9- end call.
AMS	Automated manufacturing systems gather data through sensors, process this data and send signals to actuators that perform some mechanical task. To leave a question about automated manufacturing systems press 1. To go back to the previous menu press the star key.	1- leave message in AMS mail box *- go to Core OGM 9- end call.
MMS	Multimedia systems combine different types of data. To leave a question about multimedia systems press 1. To go back to the previous menu press the star key.	1- leave message in MMS mail box *- go to Core OGM 9- end call.

Fig 3.31
Details of each OGM in the example IPT HSC Phone Information system.

Pages 281 to 300

Not included in this Evaluation Copy

Suggested solution

(a) Impossible to perform cash deposits and withdrawals, also impossible to perform cheque deposits. Any services that cannot easily be described using a rigid procedure are difficult to perform using electronic banking. For example a farmer may default on a loan however they may well be expecting a large cheque at any moment. Such problems are easily explained to a local bank manager who understands the needs and operational realities of small business within his local area. Such understanding is near impossible to replicate electronically.

(b) Likely reasons for further job losses include.

- Local residents now travel to other towns to perform their banking. Therefore fewer customers are in town to spend money within local businesses.
- Banking is performed electronically hence no need for customers to go to town so local businesses suffer job losses.
- Local people no longer carry cash, so on-the-spot purchases are reduced. This results in lower turnover and consequential job losses.
- A spiralling effect occurs whereby one business closing causes more people to travel to larger centres, which further reduces the clientele for other businesses, and so on.
- Without access to a local bank manager, small business owners are less able to explain their needs in regard to financial problems. As a consequence it is difficult for them to access funds to continue operation.

(c) Possible education and training strategies that could be used include:

- Provision of onsite visits at minimal or no cost when people first apply for internet or telephone banking services.
- Free classes on the use of the Internet. Perhaps through the local school or TAFE college.
- Creation of a mentoring scheme, whereby current local users are encouraged to provide assistance to elderly or indigenous users.
- Instructional information brochures sent to all elderly or indigenous customers.
- Provide free access to electronic banking through council libraries and community centres. Provide trainers to assist people on a one-to-one basis.
- Free assistance via a 1800 number.

Comments

- Each part of this question would likely be worth 3 marks.
- In part (a) it is necessary to identify banking services that cannot physically be performed over the Internet as well as those that are difficult to perform successfully without face-to-face contact.
- In parts (b) and (c) it is necessary to identify multiple reasons/strategies. It is reasonable to expect that three solid reasons/strategies would need to be identified for full marks.

4. TRADING OVER THE INTERNET

Buying and selling goods over the Internet is booming. Individuals and small business are able to sell to worldwide markets with little initial setup costs. Buyers are able to compare products and prices easily from the comfort of their own home. Online auctions, such as eBay, provide a means for selling and purchasing. Furthermore processing payments for goods is simplified using sites such as PayPal.

Trading over the Internet has resulted in the creation of virtual businesses. These businesses do not require shop fronts and are able to set up operations across the globe without the need to invest in expensive office space. Such businesses are an example of a virtual organisation – other types of virtual organisation exist to complete specific projects, collaborate on new standards or simply to share common interests. For example a database application can be developed using a team of developers who each live in different countries.

Virtual Organisation
An organisation or business whose members are geographically separated. They work together using electronic communication to achieve common goals.

One of the most significant problems facing businesses that sell over the Internet is establishing customer trust and loyalty. Most people feel they are more likely to receive quality service and product support when they purchase from a traditional store. Traditional shopfronts have a permanence about them and furthermore customers are negotiating deals face-to-face. This is not the case when trading over the Internet. In general the only contact is via the website and email messages. Internet only businesses must provide exceptional customer service and support if they are to overcome these issues.

Another significant concern for Internet buyers is security of purchasing transactions. In particular security of account details such as credit card numbers and account numbers. Companies, such as PayPal, resolve this concern by acting as a "middleman" between buyer and seller. The buyer submits their financial details to the middleman who makes the payment to the seller on behalf of the buyer. The seller never receives the customer's credit card or account details. The funds are withdrawn from the buyer's account and deposited into the seller's account by the "middleman".

Consider PayPal:

Currently PayPal is the world's most popular online payment service. PayPal maintains accounts for each of its customers – both buyers and sellers. When making a purchase funds must first be deposited into your PayPal account. These funds are then transferred into the sellers PayPal account. Sellers are then able to transfer the funds from their PayPal account into any bank account throughout the world. All PayPal financial transactions are encrypted using the SSL protocol.

PayPal is currently owned by eBay and hence paying for eBay items using PayPal is the preferred method. PayPal provides their service to all types of online stores and services. Some sellers direct customers to the PayPal site as one payment option whilst others integrate the PayPal system within their site such that all payments are effectively made using PayPal. For sellers the use of PayPal removes the need for them to setup their own secure payment systems and to have them certified according to the legal requirements of their country. Furthermore PayPal can accept payments in almost any currency from people almost anywhere in the world.

Behind the scenes PayPal maintains communication links to banking systems and clearing houses throughout the world. These various systems charge fees to process transactions. PayPal does not charge buyers for a basic account, however they charge sellers a percentage on their sales in much the same way that merchants are charged by banks for credit card sales. PayPal also makes much of their money from interest earned on the money within PayPal accounts.

GROUP TASK Discussion
Identify reasons why buyers and sellers prefer to perform online financial transactions using services such as PayPal rather than more traditional credit card and direct deposit transaction systems.

GROUP TASK Discussion
PayPal is not a bank and therefore the laws and government safeguards with which banks must comply do not apply. Discuss possible implications for PayPal customers.

Consider eBay:

Currently eBay is the most popular online auction and Internet trading system. According to eBay their customers are buying and selling with confidence.

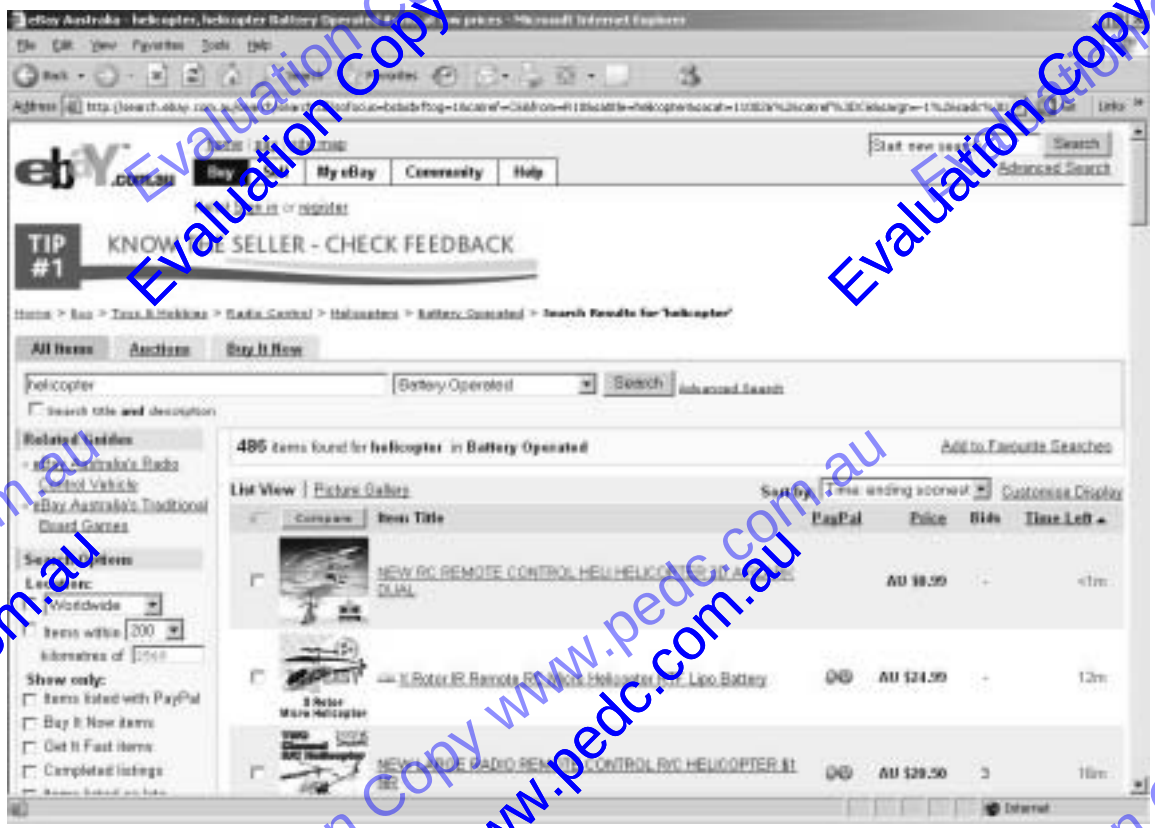


Fig 3.48
eBay's online auction search screen.

GROUP TASK Discussion
Identify and describe features within the eBay system that encourage honest trading between buyers and sellers.

GROUP TASK Discussion
Currently there are millions of people worldwide who earn the majority of their income from eBay sales. Compare and contrast eBay stores with traditional stores.

SET 3E

1. Examples of electronic commerce systems include:
   (A) Fax, telephone, teleconferencing.
   (B) EFTPOS, DBMS, Web servers.
   (C) ATMs, EFTPOS, Internet banking.
   (D) Banks, Building Societies, Credit Unions.

2. Display devices within ATMs include:
   (A) screen, speaker, cash dispenser, receipt printer.
   (B) keypad, touch screen.
   (C) screen, receipt printer, keypad, magnetic stripe reader.
   (D) magnetic stripe reader, barcode scanner, touch screen.

3. Which of the following is TRUE of EFTPOS transactions?
   (A) The customer's PIN is used to identify the customer's account.
   (B) Funds are not immediately credited to the merchant's account.
   (C) Funds are reserved prior to customers entering their PIN.
   (D) Funds leave customer's accounts during the evening following the purchase.

4. The most significant problem for businesses selling over the Internet is:
   (A) establishing customer trust and loyalty.
   (B) verifying customer payments.
   (C) complying with complex taxation laws that apply in different countries.
   (D) maintaining stock in different geographical locations.

5. Examples of "server side" systems include:
   (A) http, https.
   (B) Java and VB applets.
   (C) CGI, ISAPI.
   (D) SSL, TLS.

6. Virtual businesses:
   (A) can trade internationally.
   (B) require shop fronts.
   (C) must rent or buy office space.
   (D) require significant capital to setup.

7. Cash is only dispensed from an ATM after:
   (A) the customer's PIN is verified as correct.
   (B) sufficient funds are available in the customer's account.
   (C) funds are transferred into the financial institution operating the ATM's account.
   (D) All of the above.

8. At the time this text was written the country who used EFTPOS the most was:
   (A) Australia.
   (B) USA
   (C) New Zealand.
   (D) Sweden.

9. Which of the following is TRUE when using SSL or TLS?
   (A) The URL commences with http and public key encryption is used.
   (B) The URL commences with https and public key encryption is used.
   (C) The URL commences with https and private key encryption is used.
   (D) The URL commences with http and private key encryption is used.

10. An organisation where members are geographically separated but work together via electronic communication is known as a(n):
    (A) online business.
    (B) e-commerce site.
    (C) virtual organisation.
    (D) internet community.

11. Identify and briefly describe the operation of collection and display devices within:
    (a) ATMs
    (b) EFTPOS terminals

12. Explain the processes that occur when making a withdrawal from an ATM.

13. Explain the processes that occur when making an EFTPOS purchase.

14. Research and describe TWO examples where illegal electronic access has been gained to bank accounts.

15. Online auctions sites such as eBay have an enormous following.
    (a) Explain how such sites build trust between buyers and sellers.
    (b) Identify different payment options available on auction sites and assess the security of each option.

NETWORK COMMUNICATION CONCEPTS

In this section we introduce concepts required to understand the design and operation of networks. We shall examine client-server architecture and distinguish between thin and fat clients. We then consider network topologies that describe how network devices are physically and logically connected. Finally we describe different encoding and decoding methods used to represent data as signals suitable for transmission.

CLIENT-SERVER ARCHITECTURE

Client-Server Architecture
Servers provide specific processing services for clients. Clients request a service, and wait for a response while the server processes the request.

As the name client-server suggests, there are two different types of computer present on the network, namely servers and clients. The server provides particular processing resources and services to each client machine. For example, web servers retrieve and transmit web pages, and database servers retrieve and transmit records. The client machines, which are commonly personal computers, also perform their own local processing. For example, web browsers, email clients and database applications. Each server provides processing services to multiple clients.

Client-server processing is a form of distributed processing where different computers are used to perform the specific information processes necessary to achieve the systems purpose. Client-server processing occurs sequentially, this means that for each particular client-server operation just one CPU is ever processing data at a particular time. Many operations may well be occurring simultaneously however each particular operation is processed sequentially.

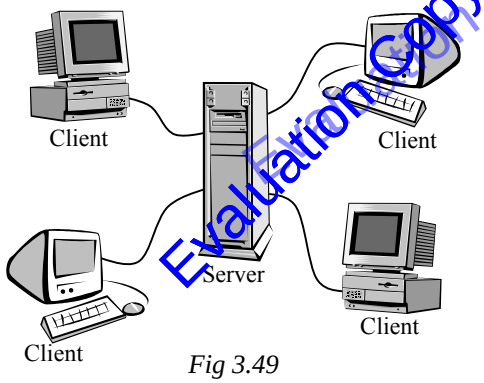


Fig 3.49
Each server provides services to multiple clients.

When a particular operation is being performed either the client is processing or the server is processing, but not both at the same time. Consider *Fig 3.50*, the client machine performs processing and then when it requires the resources of the server it sends a request, the client waits for a response from the server before it continues processing. Between the request being sent and the response being received the server is performing the requested processes.

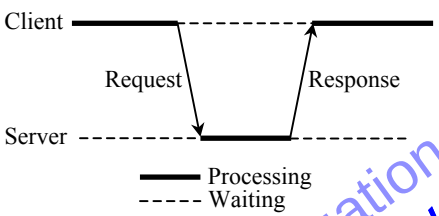


Fig 3.50
Client-Server processing is performed sequentially.

Notice that the client machines do not need to understand the detail of the server's processes and the server does not need to understand the detail of the processes occurring on the clients. Rather the two machines merely agree on the organisation of requests and responses. Hence a single server can provide processing resources to a variety of different clients running quite different software. For example, a single web server is able to provide resources to client computers of various types running a variety of different web browsers. Similarly a single database server can provide data to a variety of different client applications. As long as the request is legitimate, the server will perform the required processes and generate and transmit a response.

Our discussion so far implies that servers are quite separate computers dedicated solely to server tasks; for large systems with many clients this is often the case,

however it is not a requirement. Consider a small office or even home local area network (LAN). One machine is likely to be connected to the Internet and hence is an Internet server for all other computers on the LAN. Another computer on the LAN is connected to and controls the operation of a shared printer; hence it is a print server. Both these computers are servers, yet they are also clients to each other and even to themselves. In effect a computer can be a server for some tasks and a client for others.

In general client applications provide the user interface, hence they manage all interactions with end-users. This includes collecting and displaying information processes. In many cases the user is unaware of the server's role – indeed many users maybe unaware of the servers very existence. From the user's perspective interactions between client and server are transparent. For example when performing an Internet banking transaction a web browser is the client application that requests data from the banks web server. The banks web server then acts as a client to the banks DBMS server. Users need not be aware of the servers involved and almost certainly are unaware of the specifics of the client-server processes occurring.

Authentication
The process of determining if someone, or something, is who they claim to be.

On larger local area networks (LANs) it is common for all network tasks to be performed by one or more servers using client-server architecture. These servers commonly run a network operating system (NOS) such as versions of Linux, Novell Netware or Windows Server. These network servers control authentication of users to ensure security. Authentication processes aim to determine if users, and other devices, are who they claim to be. Commonly users must log into the network server before they are able to perform any processing. In most cases a logon password is used, however digital certificates and biometric data such as fingerprints are becoming popular methods of authenticating users. NOSs also provide file server, print server and numerous other services to users. We examine NOSs and their capabilities in more detail later in this chapter.

GROUP TASK Discussion
Simple passwords are often compromised. Identify techniques and strategies for maximising the security of passwords.

In our above discussion, the client machine has applications installed that are executed by the CPU within the machine. Such clients are known as "fat clients" or "thick clients". Another strategy that is gaining in popularity is the use of thin clients. A thin client is similar in many ways to the old terminals that once connected to centralised mainframe computers. These terminals only performed basic processing tasks, such as receiving data, displaying it on the screen and also transmitting input back to the mainframe. Thin clients can be implemented in a number of ways. They can be very basic low specification personal computers, often without any secondary storage. These thin clients rely on servers to perform all the real processing. Other thin client implementations are software based. For instance, the RDP (Remote Desktop Protocol) can be used to connect and execute any application running on a remote server. Essentially RDP simply sends the screen display from the remote computer to the thin client. The user at the thin client can therefore log into and operate the remote computer as if they were actually there. This technique is popular with IT staff as it allows them to manage servers from remote locations, such as from home. It is also routinely used to allow employees to access their work network from home or other locations via the Internet. RDP and other thin client protocols also provide a simple technique for making applications available over the Internet.

NETWORK TOPOLOGIES

The topology of a network describes the way in which the devices (nodes) are connected. A node is any device that is connected to the network, including computers, printers, hubs, switches and routers. All nodes must be able to communicate using the suite of protocols defined for the particular network. In general all nodes are able to both receive and transmit using the defined network protocols. Nodes are connected to each other via transmission media, either wired cable or wireless.

Physical Topology
The physical layout of devices on a network and how the cables and wires connect these devices.

The topology of a network describes these connections in terms of their physical layout and also in terms of how data is logically transferred between nodes. The physical connections between devices determine the physical topology. The logical topology describes how nodes communicate with each other rather than how they are physically connected.

Logical Topology
How data is transmitted and received between devices on a network regardless of their physical connections.

There are three basic topologies – bus, star and ring. In addition two other topologies, hybrid and mesh, are common on larger networks. Each of these topologies can describe the physical or the logical topology of a network. Often the logical topology is different to the physical topology. For example a physical star topology has all nodes on the LAN connected by individual cables back to a central node – often a hub or switch. This same network can have a different logical topology, either a logical bus or perhaps a logical ring topology.

Physical Topologies

- **Physical Bus Topology**

All nodes are connected to a single backbone – also known as a trunk or bus. The backbone is a single cable that carries data packets to all nodes. Each node attaches and listens for data present on the backbone via a T-connector or vampire connector. As the two ends of the backbone cable are not joined it is necessary to install terminators at each end. The function of the terminators is to prevent reflection of the data signal back down the cable. On electrical networks, as opposed to fibre optic networks, terminators are resistors that completely stop the flow of electricity by converting it into heat.

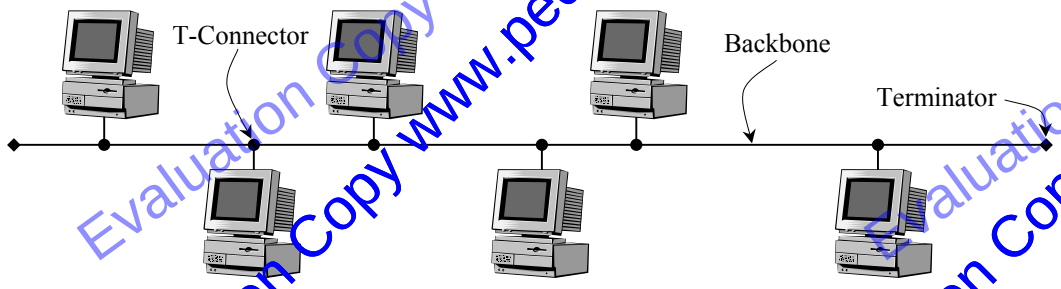


Fig 3.51
Physical bus topologies use a single backbone to which all nodes connect

In the past physical bus topologies were used for most LANs – in particular Thicknet and Thinnet Ethernet LANs that use coaxial cable as the transmission media. Although these networks require less cable than current star wired topologies they are unable to accommodate the large number of nodes present on many of today's LANs.

Furthermore a single break in the backbone disables the entire network. Today physical bus topologies are used for some high-speed backbones (often using fibre optic cable) and other long distance connections within commercial and government WANs. These high-speed applications have few attached nodes, in many cases just one at each end of the backbone to link two buildings. Where quality of service is critical it is common to install a secondary backbone to provide a redundant connection. If the primary backbone fails for any reasons then the network automatically switches to the secondary backbone.

- **Physical Star Topology**

All nodes connect to a central node via their own dedicated cable. Today the physical star topology is used on almost all LANs, including wireless LANs. In most cases the central node is a switch that includes multiple ports. In the past the central node was likely to have been a hub, multistation access unit (MAU) or even a central computer. We consider the operation of hubs and switches later in this chapter. MAUs are used in token ring networks so that a physical star topology can be used with token ring's logical ring topology. For wireless LANs a WAP (Wireless Access Point) is used as the central node. In terms of physical star topologies the central node is the device that connects all outlying nodes such that they can transmit and receive packets to and from each other node.

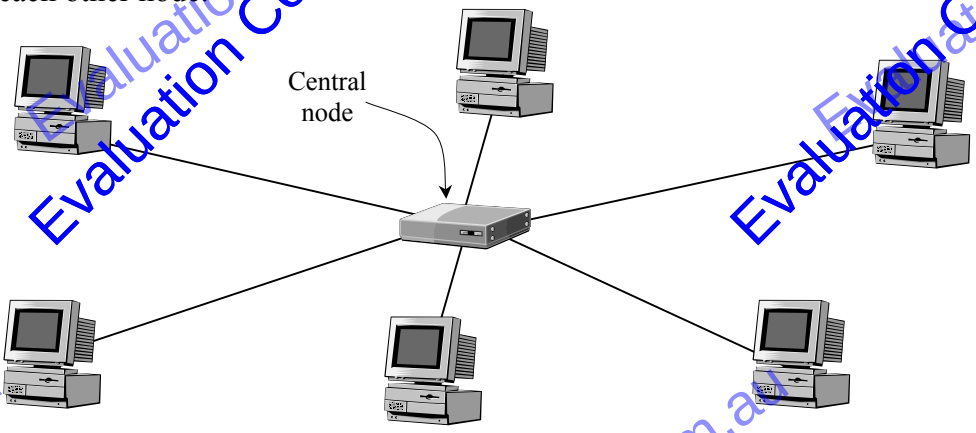


Fig 3.52
In a physical star topology all nodes connect to a central node using their own dedicated cable.

Physical star topologies have a number of advantages over physical bus and ring topologies. This is particularly true for LANs where nodes are physically close – such as within the same room or building. Firstly each node has its own cable and hence can be connected and disconnected without affecting any other nodes. Secondly new nodes can easily be added without first disabling the network. Finally identifying faults is simplified as single nodes can simply be disconnected from the central node in turn until the problem is resolved.

There are however some disadvantages of physical stars. Significantly more cabling is required, however this cable is generally less expensive as it must only support transmission speeds sufficient for a single node. Today UTP (Unprotected Twisted Pair) is the most common transmission media. Also if a fault occurs in the central node then all connected nodes are also disabled.

GROUP TASK Practical Activity
Consider one of your school's computer rooms. Estimate the length of cable required to connect all computers (and other nodes) using a physical bus topology and then using a physical star topology.

- **Physical Ring Topology**

In a physical ring each node connects to exactly two other nodes. As a consequence the cable forms a complete ring. In general data packets circulate the ring in just one direction. This means each node receives data from one node and transmits to the other. If the cable is broken at any point then the entire network is disabled. Therefore removing a node or adding a new node requires the network to be stopped. Furthermore in most implementations each data packet is received and then retransmitted by each node, hence all nodes must be powered at all times if the network is to operate. For these reasons physical ring topologies are seldom used for LANs today.

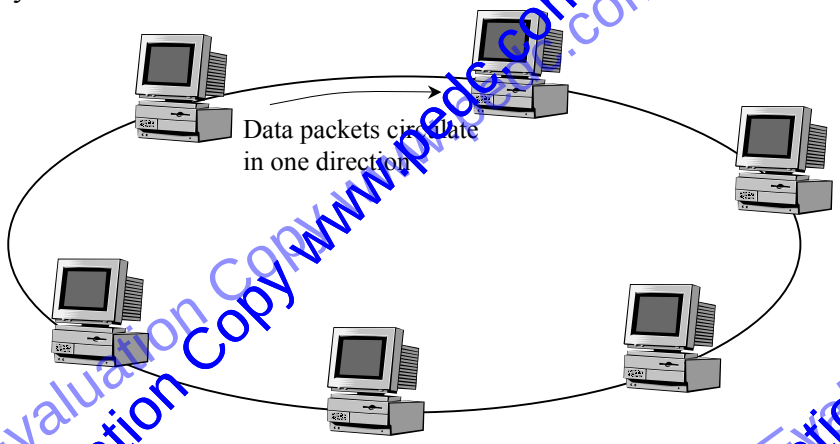


Fig 3.53
In physical ring topologies data packets pass through each node as they circulate the ring.

FDDI (Fibre Distributed Data Interface) and SONET (Synchronous Optical Network) networks are usually configured as physical rings and always operate as logical rings. FDDI can be used for LANs however it is more commonly used for longer distance high-speed connections. As the names suggest FDDI and SONET use optical fibre as the transmission media. FDDI is commonly used to connect an organisation's buildings whilst SONET is used for much greater distances. Both protocols use two physical rings with data circulating in different directions on each ring. Distances between FDDI nodes should not exceed 30km while distances in excess of 100km are common for SONET. For long distance applications the second ring is maintained solely as a backup should a fault occur in the primary ring. In such cases it is preferable to physically route the cabling of each ring separately. The aim being to improve fault tolerance should a cable be broken at any single location. If the cables for both rings are within close proximity (like within the same trench) then chances are that both cables will be broken together. When FDDI is used within a building then both rings can be used for data transmission, which effectively doubles the speed of data transfer.

- **Physical Hybrid Topology**

Hybrid or tree topologies use a combination of connected bus, star and ring topologies. Commonly a physical bus topology forms the backbone, with multiple physical star topologies branching off this backbone (see *Fig 3.54*). The backbone is installed through each building (or room) with a star topology used to branch out to the final workstations – the topology resembles the trunk and branches of a tree.

All hybrid topologies have a single transmission path between any two nodes. This is one reason the name 'tree' is used; consider the leaves on a tree, there is one and only one path from one leaf to another – the same is true for nodes in a physical hybrid or tree network.

Hybrid topologies are the primary topology of most organisations' networks. They allow for expansion – new branches can be added by simply connecting central nodes and branching out to the new workstations. It is common practice to install cabling that supports two or more times the anticipated transmission speed so that future expansion can easily and economically be accomplished. The extra cost of better quality higher-speed cabling being relatively insignificant compared to the installation costs. Consider the tree topology in *Fig 3.54*. It makes sense to install cabling that supports much higher data transfer speeds for the main backbone, whilst the cabling in each of the stars and rings is less critical.

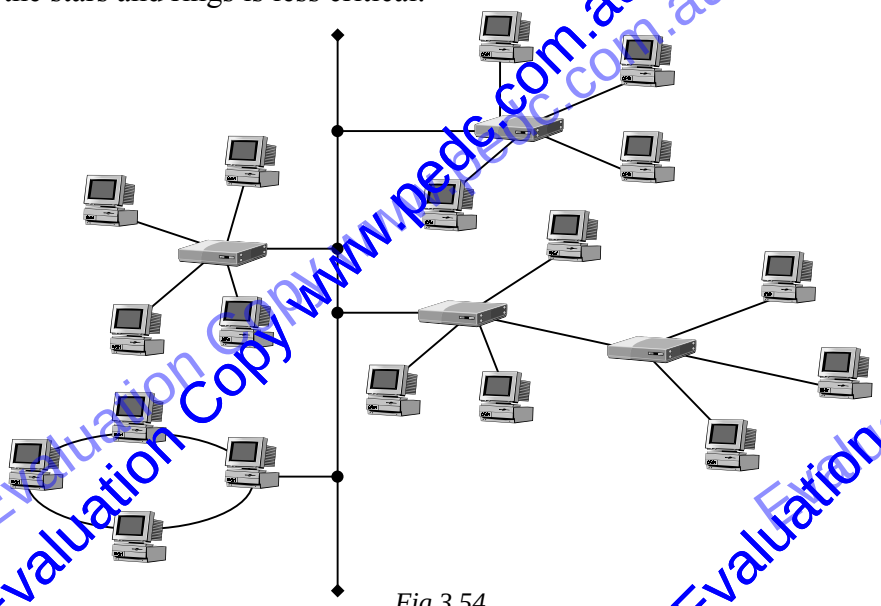


Fig 3.54
Physical tree topologies connect multiple bus, star and/or ring topologies such that a single path exists between each node.

GROUP TASK Practical Activity
Consider your school's physical network. Construct a diagram to describe the physical topology.

GROUP TASK Discussion
Discuss problems that could occur if there is more than one physical path between two nodes on a network.

- **Physical Mesh Topology**

Mesh topologies include more than one physical path between pairs of nodes. This is the primary topology of the Internet, where IP datagrams can travel different paths from the transmitter to the receiver. Mesh topologies require routers to direct each packet over a particular path. Without routers data packets can loop endlessly or they can be reproduced such that two or more copies arrive at the final destination.

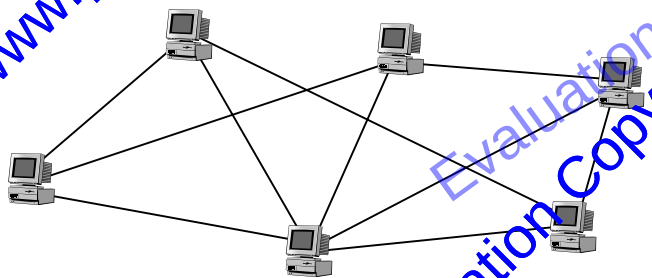


Fig 3.55
Mesh topologies include more than one path between individual nodes.

Commonly the nodes on a mesh network are all routers, and each router connects to further routers or a LAN. Mesh networks provide excellent fault tolerance, as packets are automatically routed around faults. A full mesh topology exists when all nodes are connected to all other nodes. Full mesh topologies are used in high-speed long distance connections where there are relatively few nodes and network performance and quality of service is absolutely critical. When a full mesh is used messages can be rerouted along any other path and hence fault tolerance is maximised.

Logical Topologies

The logical topology of a network describes how data is transmitted and received on a network, regardless of the physical connections. In some references the term "signal topology" is used in preference to the term "logical topology". In many ways this is a more descriptive term as the logical topology describes how signals are transferred between nodes on a network.

It is important to note that both electrical and light signals travel along transmission media at close to the speed of light. This is so fast that when a signal is placed on a wire or fibre it is almost immediately present at all points along the media. The speed of transmission is determined by the rate at which the sender alters the signal – in comparison the time taken for the signal to actually travel down the wire is relatively insignificant.

On an individual LAN the logical topology is in the majority of cases determined at the Transmission Level – the data link layer of the OSI model. The data link layer (layer 2) controls and defines how data is organised and directed across the network. This includes the format and size of frames as well as the speed of transmission. Commonly the unique MAC address of each node is used to direct messages to their destination. In essence the data link layer controls the hardware present at the physical layer (layer 1 of the OSI model).

Multiple LANs are commonly connected to form a WAN at the network layer. In an IP network routers direct messages in the form of IP datagrams to the next hop based on their IP address. Each hop in a datagram's journey may use different data link and physical layer protocols. The logical paths that datagrams follow describe the logical topology of WANs – commonly a logical mesh topology. We restrict our discussion to logical topologies operating within individual LANs.

In this section we discuss bus, ring and star (or switching) logical topologies at the datal link level. For each logical topology we identify common physical topologies upon which the logical signalling operates and we consider the media access controls used to deal with multiple nodes wishing to transmit at the same time.

- **Logical Bus Topology**

A logical bus topology simply means that all transmissions are broadcast simultaneously in all directions to all attached nodes. In effect all nodes share the same transmission media, that is, they are all on the same network segment. All nodes on the same network segment receive all frames – they simply ignore frames whose destination MAC address does not match their own. This presents problems when two or more nodes attempt to send at the same time. When this occurs the frames are said to collide – in effect they are corrupted such that they cannot be received correctly. A method of media access control (MAC) is needed to either prevent collisions or deal with collisions after they occur.

Prior to about 2004 logical bus topologies were by far the most popular – at the time a logical bus was the topology used by all the Ethernet standards. Furthermore switch

technology, which permits more efficient logical star topologies was expensive or simply not available. Currently switches are inexpensive and are required for the current full-duplex Gigabit and faster Ethernet standards.

Ethernet when operating over a logical bus topology uses CSMA/CD as its method of media access control (MAC). CSMA/CD is commonly associated with Ethernet, however in reality it is a MAC technique that is used by a variety of other albeit less popular low-level protocols. CSMA/CD is an acronym for "Carrier Sense Multiple Access with Collision Detection - quite a mouthful, however the general idea is relatively simple to understand.

The "Multiple Access" part of CSMA/CD simply refers to the ability of nodes to transmit at any time on the shared transmission media, as long as they are not currently receiving a frame. Remember that all nodes receive all frames at virtually the same time on a logical bus. If no frame is being received then the transmission media is not being used, therefore nodes are free to send. In *Fig 3.56* the transmission media is free after Node A completes transmission of a frame. This is the "Carrier Sense" part of CSMA/CD – in essence nodes must wait until only the carrier signal is present before sending. Say a node is not receiving and therefore it transmits a frame. Now it is possible that one or more other nodes have also transmitted a frame at the same time – they too were not receiving. If, or when, this occurs a collision takes place on the shared transmission media and all frames are garbled. In *Fig 3.56* a collision occurs when both Nodes B and C transmit at the same time. All nodes are able to detect these collisions and in response a jamming signal is transmitted – this is the "Collision Detection" part of CSMA/CD. In response all sending nodes wait a random amount of time and then retransmit their frames. In *Fig 3.56* Node C waits a shorter time than Node B, hence Node C transmits it's frame prior to Node B.

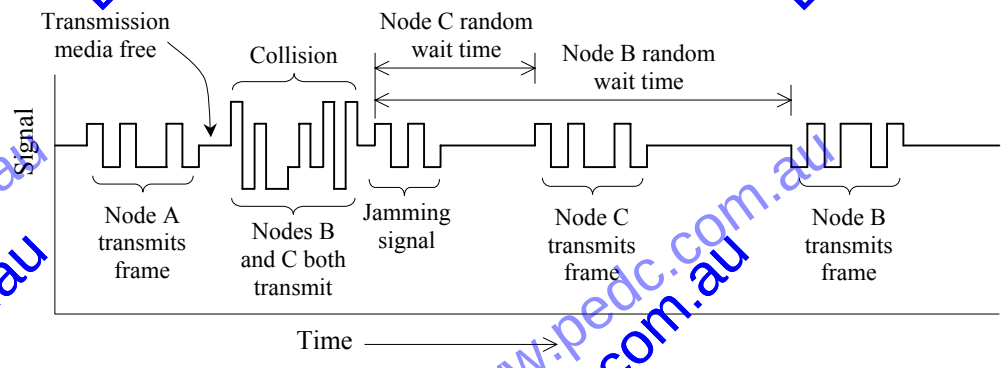


Fig 3.56

CSMA/CD strategy where node B and node C are waiting to transmit after node A has finished.

GROUP TASK Discussion

It is possible for short Ethernet frames to collide after they have been successfully sent. This is more likely where there are large physical distances between the sending nodes. Why is this so? Discuss.

Clearly a physical bus topology supports a logical bus topology. Examples include the earlier Ethernet standards that use coaxial cable, such as 10Base2 (also known as Thinnet) and the earlier 10Base5 standard (also known as Thicknet). There are also Ethernet standards using optical fibre that utilise physical and logical bus topologies. We will examine many of the commonly used Ethernet standards later in this chapter when we consider transmission media and cabling standards in some detail.

Most current Ethernet networks are wired with UTP (Unprotected Twisted Pair) cable into a physical star topology. When connected via a hub a logical bus topology is

being used. Hubs simply repeat all received signals out to all connected nodes; therefore all nodes share a common transmission medium and exist on the same network segment. We examine the operation of hubs in more detail later in this chapter. In terms of logical topologies, conceptually we can think of a hub containing a mini backbone shared by all nodes. 10BaseT and 100BaseT are common Ethernet standards that are wired into a physical star, but use a logical bus topology when the central node is a hub.

Current wireless LANs (WLANs) based on the IEEE 802.11 standard use a logical bus topology. The 802.11 standard specifies two "physical" types of WLAN, those with a central node in the form of a wireless access point (WAP) and "ad-hoc" WLANs where nodes connect directly to each other. Those with a central WAP utilise a physical star topology. Essentially a WAP amplifies and repeats signals much like a wired hub – all nodes hear all messages from the WAP. Ad-hoc WLANs use a physical mesh-like topology that changes dynamically as nodes connect and disconnect.

GROUP TASK Research and Discussion
Why do you think "ad-hoc" wireless LANs have been described as having a physical "mesh-like" topology? Research and discuss.

On all current (2007) 802.11 WLANs all nodes transmit and receive using a single wireless channel – hence a logical bus topology is being used. The characteristics of wireless transmission make CSMA/CD an inappropriate media access control strategy. Wireless nodes are effectively half-duplex as they are unable to reliably listen to a signal whilst they are transmitting – the wireless signal being drowned by their transmission. As a consequence detecting collisions during transmission is difficult. To overcome this issue 802.11 WLANs use CSMA/CA as their media access control strategy rather than CSMA/CD. CSMA/CA is an acronym for "Carrier Sense Multiple Access with Collision Avoidance". As the name implies, CSMA/CA attempts to prevent data collisions occurring rather than dealing with collisions once they have occurred. The CSMA/CA strategy is not new; it was integral to the operation of AppleTalk networks used by early Apple Macintosh computers.

So how does CSMA/CA avoid collisions? Like CSMA/CD each node must first wait for the transmission media to be free. Unlike collision detection nodes must then wait a random amount of time before commencing transmission. In *Fig 3.57* Node C has generated a shorter wait time than Node B so no collision occurs. This simple strategy avoids most of the collisions that occur on CSMA/CD networks. Using CSMA/CD numerous nodes are likely to be waiting for a clear transmission media and as soon as the line is clear they all commence transmission together resulting in collisions such as the one detailed in *Fig 3.56* above. Using CSMA/CA waiting nodes will rarely commence transmitting simultaneously.

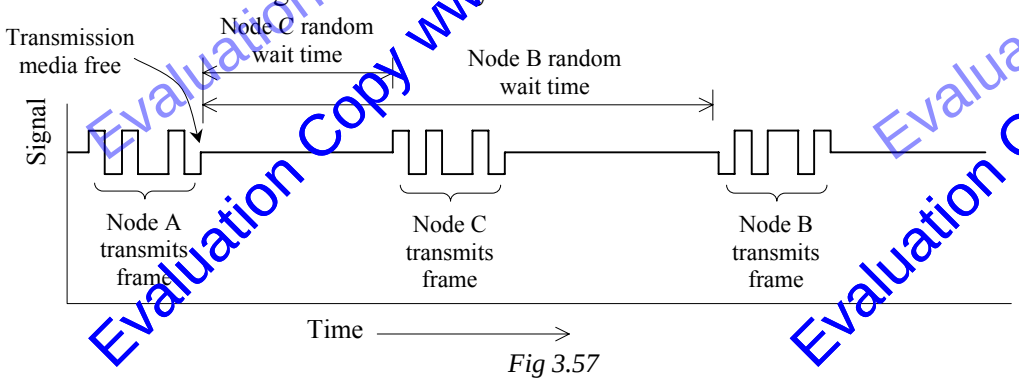


Fig 3.57

CSMA/CA strategy where node B and node C are waiting to transmit after node A has finished.

Further collision avoidance strategies are optionally employed on 802.11 WLANs. One system, known as RTS/CTS, allows nodes to reserve the transmission media in advance. The system can be turned completely off or on, or more commonly the system is used for frames exceeding a preset byte length. Using the RTS/CTS system a node waiting to transmit first sends an RTS (Request To Send) frame. This RTS frame contains a duration ID field that specifies the time the sending node will require the transmission media. In response a CTS (Clear To Send) frame that also contains a duration field is returned. Nodes only send data frames after they have received a CTS frame. Other nodes also receive the CTS frame so that they do not commence sending until sufficient time has elapsed.

GROUP TASK Practical Activity
Examine the configuration screens for a WAP (wireless access points are also included within devices commonly known as "wireless routers"). Identify and describe the purpose of any RTS/CTS settings.

No collision detection or avoidance scheme is 100% perfect – some collisions will not be detected whilst other frames will continue to collide on subsequent transmission attempts. All OSI layer 2 protocols specify some limit to the number of retries that can occur for individual frames. Eventually some frames are simply dropped. Dealing with such failures is left up to the higher OSI layer protocols where definite positive acknowledgement of transmission is required.

There exists media access control (MAC) strategies used over shared transmission media that avoid the possibility of collisions completely. TDMA (time division multiplexing) is used on some fixed and mobile phone networks whilst polling is used for some data networks. The 802.11 WLAN standard includes the option to include polling functionality. Essentially polling gives total control of media access to one node. This node then asks each node in turn if it wishes to transmit.

GROUP TASK Research
Using the Internet, or otherwise, research the essential features and differences between TDMA and polling MAC strategies.

- **Logical Ring Topology**

When a logical ring topology is used each node receives frames from one and only one node and transmits frames to one and only one node. As a consequence all frames circulate a logical ring. Each node receives and transmits each frame so that all frames circulate around the entire ring. The destination or recipient node takes a copy prior to transmitting the frame. Collisions are simply impossible on logical ring topologies.

IBM's original "token ring" protocol was once the most common LAN protocol – Ethernet has largely replaced "token ring". However, the general operation of token ring networks is also implemented within long-distance high-speed networks including FDDI and SONET protocols.

In most logical ring implementations a single frame (known as a token) circulates the ring continuously. When a node wishes to send it must wait for the token. It then attaches its data to the token and sends it on its way. The frame containing the data continues around the ring being received and transmitted in turn by each node until it reaches the recipient. The recipient takes a copy of the data and also sends the frame on to the next node. Eventually the data frame returns to the original sender. The sender then removes the data frame and sends out the token. The token continues to circulate until the next node wishes to send.

Early IBM Token Ring networks were wired into a physical ring topology (see *Fig 3.58*). Later implementations used a physical star topology where the central node was a Multistation Access Unit (MAU) as shown in *Fig 3.59*. Conceptually a MAU can be thought of as containing a miniature ring. MAUs are able to automatically sense when a node is either not attached or is not powered and close the ring accordingly.

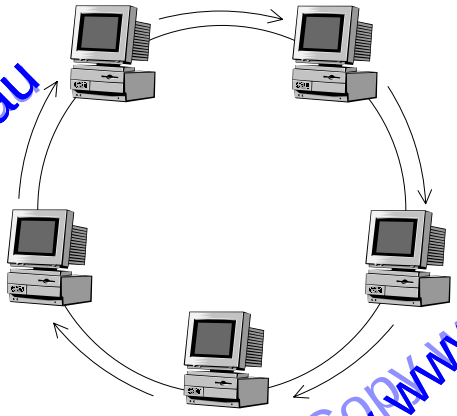


Fig 3.58
IBM Token Ring with physical and logical ring topology.

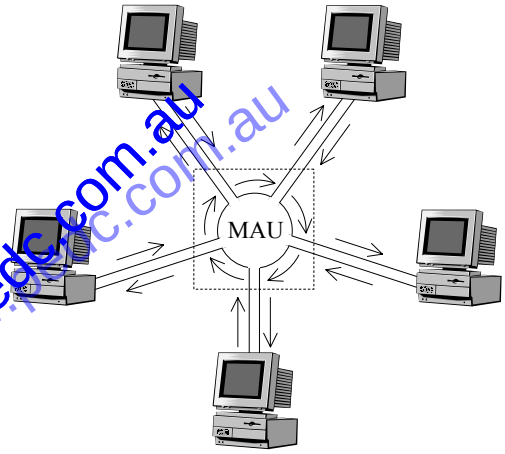


Fig 3.59
IBM Token Ring with physical star topology and logical ring topology.

GROUP TASK Research
Using the Internet, or otherwise, research the data transfer speeds achieved using IBM's Token Ring networks.

FDDI and SONET are both used for long distance communication. In these cases the nodes are routers rather than computers. These routers include connections to other networks not just to adjacent nodes in the ring. In most examples a physical ring topology is used in conjunction with logical ring topologies. Common FDDI and SONET networks are operated by large business, government or telecommunication companies using fibre optic cable. Currently data transfer rates of 40Gbps are achieved using SONET.

GROUP TASK Research
SONET speeds are based on STS levels and Optical Carrier (OC) specifications. Use the Internet to research the speed of SONET based networks based on different STS levels and OC specifications.

SONET rings provide many of the major Internet and PSTN links between major cities. As a consequence such networks must ensure quality of service at all costs. A single physical ring is unsuitable for such networks as a single break in a cable disables the entire network. To solve this problem FDDI and SONET use multiple connected rings. Most FDDI implementation use dual rings – the second existing as a redundant backup should the first fail. Many SONET networks utilise many more than two rings. These multi-ring networks are known as "self-healing rings" and are able to divert data packets around problem areas in a virtual instant. For our discussion we will consider a typical dual-ring FDDI or SONET ring configuration.

When dual rings are used the tokens on each ring rotate in different directions. Say, clockwise for the primary ring and anti-clockwise on the secondary (or standby) ring. Note that under normal conditions the secondary ring is not being used. Imagine a fault occurs in the primary ring – the secondary ring can then become the active ring

whilst the fault is corrected. Now imagine both rings are cut, perhaps by a backhoe physically cutting through the cable. This situation is illustrated in *Fig 3.60* where the cable connecting Node B and Node C has been cut. The new transmission path is shown using dotted arrows. Notice that data still travels in the original direction on both the primary and secondary rings.

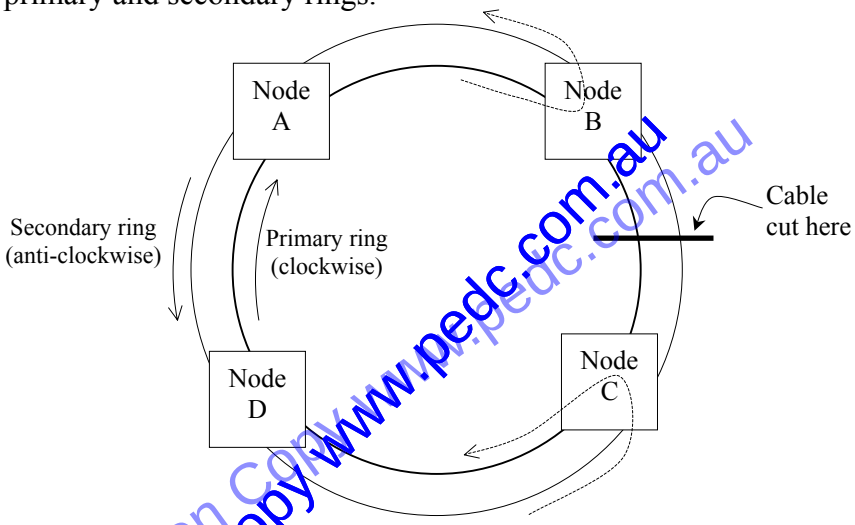


Fig 3.60

Dual ring topology where a cable has been cut causing a new logical ring to be automatically created.

More rings can be added to further improve the fault tolerance or "self-healing" ability of critical ring networks. Note that many complex implementations that more closely resemble a physical mesh topology are used; yet all maintain a logical ring topology.

GROUP TASK Discussion
Identify possible points of failure for each of the physical topologies shown in *Figures 3.58, 3.59* and *3.60*. Suggest how the possibility of such failures could be avoided.

- **Logical Star Topology**

In a logical star topology each node has its own connection to a switch that is the central node. In many references logical star topologies are known as logical switch topologies. Currently all logical star topologies also use a physical star topology.

On a logical star every node exists on its own network segment with the switch. Switches are OSI data link layer 2 devices. In current configurations this connection is full duplex, as it includes two distinct transmission channels – one for sending and one for receiving. Most Ethernet networks use a twisted pair of copper wires (UTP) for each of these channels. Collisions are impossible on logical stars. Frames on each channel always travel in a single direction – either a frame is travelling from node to switch or it is on the other channel travelling from switch to node. Situations where two or more frames exist on a single channel can never occur.

When a node sends a frame the switch detects the destination MAC address and transmits the frame only to the node with that MAC address. Switches are able to process multiple frames simultaneously that are addressed to different nodes. We consider the operation of switches in more detail later in this chapter.

GROUP TASK Discussion
Compare and contrast examples of physical star topologies that use logical bus, logical ring and logical star topologies.

HSC style question:

Luke's Limos is a used car business comprised of three car yards located in adjoining suburbs of Sydney. Currently each car yard has its own Ethernet network that includes a central switch, laser printer and a cable broadband connection to the Internet.

Each of the four salesmen at each car yard has a computer in their office where they record information in regard to their contacts with customers. Currently each salesman is free to record this information in a way they feel best meets their needs.

All computers at each car yard are able to access detailed information in regard to the vehicles for sale at their particular site. This information is stored in a simple flat file database located on the sales manager's computer at each car yard.

All cars currently for sale at all three yards are advertised on a website that is maintained by a web design company. When a car is being prepared for sale an email is sent to the web designer. The email includes the basic details, sale price and an attached photo of the vehicle. When a car is sold the web designer is again emailed so that the vehicle can be removed from the website.

(a) (i) Draw a diagram to represent the physical network topology at one of the car yards.

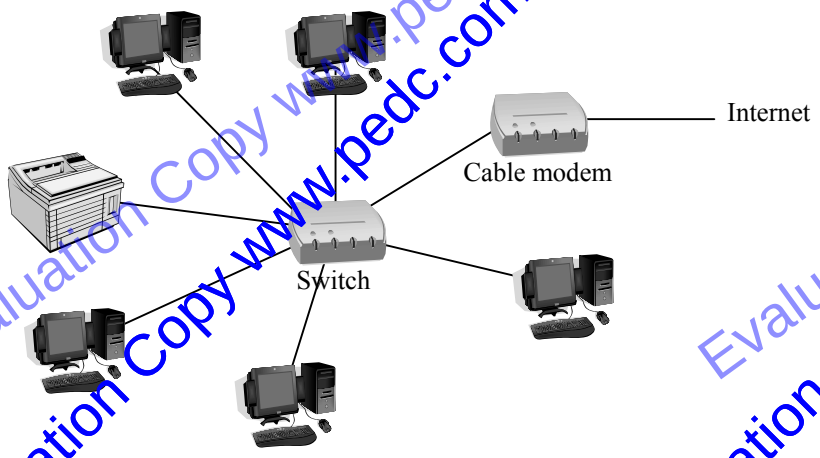
(ii) Explain how data collisions are detected (or avoided) within each car yard's network.

(b) The owner is considering opening a further two car yards within the next year and wishes to explore ways of improving the information flow throughout the business. The owner intends to implement a team approach to selling cars. This requires that all salesmen are able to view the details of all vehicles and all customer contacts within the business.

Discuss suitable modifications and/or additions to the current information system to assist the owner achieve this objective.

Suggested Solution

(a) (i)



(ii) Switches set up a dedicated circuit between sender and receiver. This means it is impossible for collisions to occur. In essence every combination of every pair of nodes is in its own network segment.

(b) Possible modification/additions that could include:

- Use of a single relational database to hold full details of all cars and edited directly by Luke's Limos salesmen.
- The relational database of all car details is held or at least accessed from a web server. Web pages describing each car are produced dynamically using data from the new relational database.
- The web designer sets up and maintains the webpage generation process for the general public. The web pages being generated from the database when requested by a browser.
- Customer contacts could also be included within the database accessed by the web server.
- A replicated database could be used for customer contacts. New contacts being entered at each car yard and then distributed to other yards automatically during the replication process.
- A distributed database could be used for customer contacts where local contacts are physically stored at each individual car yard. However the data from all car yards is still available to all other car yards.
- The customer contact database should include a system where all salesman who have had dealings with a customer are informed of any new contacts with that customer. Perhaps a simple automated email could be sent to all salesman who have had previous contact with a customer whenever a new customer contact occurs.

Comments

- In (a) (i) a star physical topology should be drawn that includes all the devices mentioned in the question.
- In (a) (ii) mention could be made of a star/switched logical topology hence no possibility of collisions occurring.
- Although incorrect, it is likely that some portion of the marks in (a) (ii) would be allocated if CSMA/CD or CSMA/CA was described correctly.
- In part (b) there are many other possible modifications and additions that could be discussed. It is important that each modification/addition is related directly back to the requirements of the new system that are outlined in the question.
- Note that part (b) combines aspects of the database and communication topics.
- Part (b) is an extended response question that would likely be worth 4 to 6 marks in a real examination. Therefore a number of points should be made and explored in some depth. The suggested answer includes many points, however each point could well be explored in greater detail.

SET 3F

1. Which of the following is TRUE of client-server systems?
   (A) Clients must understand the detail of server processes.
   (B) Servers process client requests.
   (C) Clients provide services to servers.
   (D) Servers are always dedicated machines.

2. An employee uses their laptop at home to connect to a server at their work using a thin client RDP Internet connection. Which of the following is TRUE?
   (A) Applications run on the client.
   (B) Applications run on the server.
   (C) The laptop has no hard disk.
   (D) No data is transmitted to the server.

3. The physical topology of a network:
   (A) determines how data is transferred between devices.
   (B) can change when different protocols are installed.
   (C) describes and determines how nodes communicate with each other.
   (D) describes how devices are physically connected to each other.

4. A break in a single cable is more significant when using a:
   (A) physical bus or star topology.
   (B) physical ring or star topology.
   (C) physical ring or bus topology.
   (D) physical mesh topology.

5. Multiple paths between nodes is a feature of:
   (A) physical mesh topologies.
   (B) physical bus topologies.
   (C) physical star topologies.
   (D) physical tree topologies.

6. On an Ethernet LAN each node is connected via UTP to a central hub. Which topology is being used?
   (A) Physical star, logical bus.
   (B) Physical star, logical star.
   (C) Physical bus, logical bus.
   (D) Physical bus, logical star.

7. In regard to topologies and the OSI model, which of the following is generally TRUE?
   (A) Logical topologies for WANs are determined at the data link layer and for LANs at the network layer.
   (B) Logical topologies for LANs are determined at the data link layer and for WANs at the network layer.
   (C) Physical topologies for LANs are determined at the data link layer and for WANs at the network layer.
   (D) Physical topologies for WANs are determined at the data link layer and for LANs at the network layer.

8. All nodes receive all transmissions at virtually the same time when using which logical topology?
   (A) Ring
   (B) Star
   (C) Switched
   (D) Bus

9. What is a data collision?
   (A) Corruption when a nodes starts receiving whilst it is still transmitting.
   (B) A procedure used to ensure transmissions arrive at their destination on logical bus topologies.
   (C) Corruption of messages due to multiple nodes transmitting simultaneously on the same communication channel.
   (D) A fault in the logical topology such that multiple nodes are able to transmit at the same time.

10. Critical ring networks are said to be "self healing", what does this mean?
    (A) Cables are able to repair themselves when broken.
    (B) Each node contains redundant components that take over should the primary component fail.
    (C) Data traffic can be automatically diverted around faults.
    (D) Two or more physical rings are installed.

11. Define each of the following terms and provide an example:
    (a) Client-server architecture (b) Physical topology (c) Logical topology

12. Construct a table of advantages and disadvantages of:
    (a) Physical bus, star and ring topologies. (b) Logical bus, star and ring topologies.

13. Explain how data collisions are prevented, avoided or detected on each of the following networks:
    (a) Ethernet over a logical bus topology.
    (b) IEEE 802.11 wireless LAN.
    (c) IBM Token Ring network.

14. Distinguish between thin clients and fat clients using examples.

15. Maximising fault tolerance of critical networks is a major priority. Describe at least THREE techniques that improve a network's fault tolerance.

ENCODING AND DECODING ANALOG AND DIGITAL SIGNALS

For communication to take place both transmitting and receiving must occur successfully. Transmitting involves the sender encoding the message and transmitting it over the medium. Receiving involves the receiver understanding the organisation of the encoded message – based on the protocols agreed upon during handshaking with the transmitter. The receiver can then decode the message based on the rules of the agreed protocols. In essence both encoding and decoding are organising information processes. Encoding organises the data into a form suitable for transmission along the communication medium. Decoding changes the organisation of the received data into a form suitable for subsequent information processes.

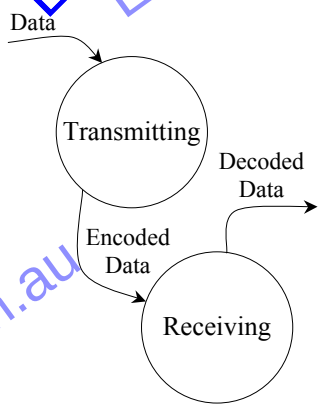


Fig 3.61
Transmitting encodes data and receiving decodes data.

Prior to transmission data is encoded into a signal according to the rules of the transmission protocols being used and suited to the transmission media along which the message will travel. When messages reach their destination the receiver reverses this process by decoding the signal and transforming it back into data.

Data that originates or is stored on a computer is always in binary digital form. Digital data is all data that is represented (or could be represented) using whole distinct numbers – in the case of computers a binary representation is used. Continuous data that usually originates from the real world is analog. Both analog and digital data can be encoded and transmitted on electromagnetic waves. Note that in reality all waves are continuous hence they are analog. For our purpose, it is how we choose to interpret the data carried on these analog waves that we shall use to distinguish between digital signals and analog signals. A digital signal is being used when digital data is encoded onto an analog wave. An analog signal is being used when analog data is encoded onto an analog wave.

To encode analog data into a digital signal requires that the data first be converted into digital using an analog to digital converter (ADC). Similarly to encode digital data into an analog signal the data must be converted to analog data using a digital to analog converter (DAC).

GROUP TASK Discussion
Discuss and develop definitions for the terms "digital data" and "analog data".

Analog Data to Analog Signal

When the data is analog the waveform varies continuously in parallel with the changes in the original analog data. For example microphones collect analog sound waves and encode them as an infinitely variable electromagnetic wave (see *Fig 3.62*). The voltage transmitted from the microphone varies continuously in parallel with the sound waves entering the microphone. An analog signal is produced as the entire analog wave represents the original analog data. All points on the analog wave have significance – this is not true of digital signals.

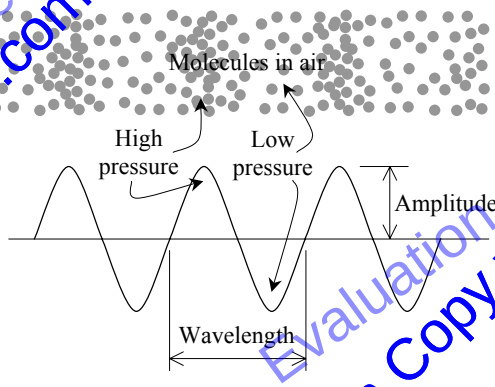


Fig 3.62
Microphones convert analog sound waves into analog signals carried on analog waves.

Pages 321 to 340

Not included in this Evaluation Copy

gateway address for all local nodes wishing to access the Internet. The gateway hides the local IP addresses from the Internet, instead IP datagrams are all sent using the gateway's WAN or Internet IP address. The gateway keeps track of the local IP addresses so that IP traffic from the Internet can be directed to the correct local node.

If a LAN includes a gateway that provides a connection to the Internet then the gateway's LAN IP address must be known to all nodes – in most operating systems this IP address is specified as the default gateway – in *Fig 3.87* 10.0.0.138 is the local IP address of the ADSL router that links to the Internet.

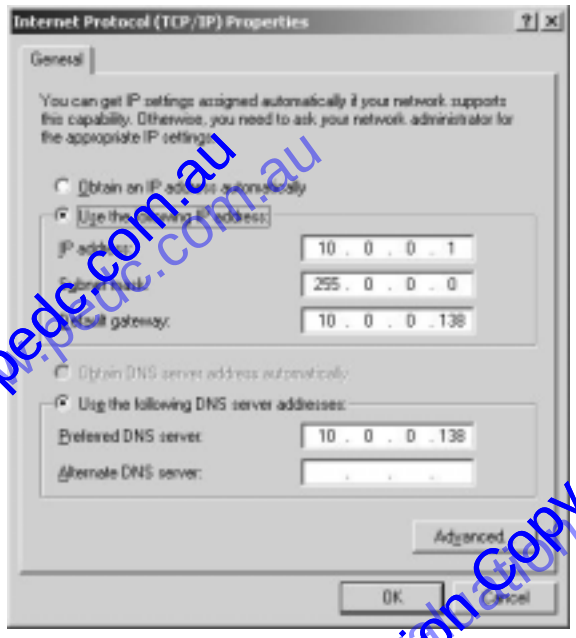


Fig 3.87
The default gateway setting specifies the node acting as the gateway to the Internet.

Like many technology related terms the meaning of the word "gateway" is used differently in different contexts. In general usage the word "gateway" is used to refer to devices that connect a LAN directly to the Internet. However, routers commonly include one or more gateways. As a consequence the general public often use the words router and gateway interchangeably.

- **Wireless Access Point**

Wireless access points (WAPs) or simply access points (APs) are the central nodes on wireless LANs. Access points broadcast to all wireless nodes within the coverage area. On 802.11 WLANs the access point does not direct packets to specific nodes or control the order in which nodes can transmit, rather they simply repeat all packets received. Conceptually an access point performs much like a hub on a wired LAN.

Fig 3.88
Linksys WAP54G wireless access point.

A significant issue with WLANs is security – any user within the coverage range can potentially access the network. To counteract this possibility access points include security in the form of WEP (Wired Equivalent Privacy) and WPA (WiFi Protected Access). WEP uses a single shared key encryption system whilst WPA generates new encryption keys at regular intervals. The WEP system can and has been infiltrated so currently WPA is the recommended system.

No encryption system can work if it is not turned on. This is a major issue for both home and business WLANs. Furthermore the simplicity of creating a WLAN and the ability to access WLANs from outside make security a signifcant issue. Hackers need only to connect a wireless access point to an existing Ethernet connection point and they then have complete access without the need to work around complex firewalls and proxy servers.

- **Modem**

The term modem is a shortened form of the terms modulation and demodulation, these are the primary processes performed by all modems. Today most modems are used to connect a computer to a local Internet Service Provider (ISP); the ISP supplying a high-speed ADSL or cable connection to the Internet. Dial-up modems were once the primary device for connecting users to the Internet. Currently dial-up modems are more often used to send faxes from computers over the PSTN – virtually all dial-up modems are able to both send and receive fax transmissions.

We discussed modulation in some detail earlier in this chapter. Basically modems modulate digital signals by altering the phase, amplitude and/or frequency of electromagnetic waves. That is, modulation is the process of encoding digital data onto an analog waveform. Demodulation is the reverse of the modulation process. Demodulation decodes analog signals back into their original digital form. Clearly both sender and receiver must agree on the method of modulation used if communication is to be successful.

Modulation
The process of encoding digital information onto an analog wave by changing its amplitude, frequency or phase.

Demodulation
The process of decoding a modulated analog wave back into its original digital signal. The opposite of modulation.

Modems are commonly connected to a computer via a USB port or an Ethernet network connection. These interfaces are considered digital links; they do use electromagnetic waves however the data is represented using different voltages. The electronic circuits within the computer can use these voltage changes directly. In contrast modulated analog waves, such as those transmitted down telephone lines or coaxial cables, are not suitable for direct use by the circuits within the computer. Hence the primary role of modems is to provide an interface between the modulated analog waves used for long distance transfer and the digital data suitable for use by computers.

- **ADSL modems**

Asymmetrical digital subscriber lines (ADSL) use existing copper telephone lines to transfer broadband signals. Although these copper wires were originally designed to support voice frequencies from 200 to 3400Hz, they are physically capable of supporting a much wider range of frequencies. It is the various switching and filtering hardware devices within the standard telephone network that prevent the transfer of frequencies above about 3400Hz. To solve this problem requires dedicated hardware to be installed where each copper line enters the local telephone exchange.

ADSL signal strength deteriorates as distances increase, the signal cannot be maintained at all for distances greater than about 5400 metres. Voice lines much greater than 5400 metres are possible using amplifiers. Unfortunately these amplifiers boost only the lower frequencies required for voice, hence ADSL is not currently available in many remote rural areas. Even when distances are short and the copper runs directly into the exchange problems can occur as a consequence of interference. In general phone lines within a building and out to the street are not shielded against interference, this interference is rarely significant enough that a connection cannot be established, however it often reduces the speed of such connections.

So how does ADSL transfer data between an ADSL modem and the local telephone exchange? Using a modulation standard known as Discrete MultiTone (DMT). DMT operates using frequencies from about 8kHz to around 1.5MHz. This bandwidth is split into some 247 individual 4kHz wide channels as shown in *Fig 3.89*. Each channel is modulated using QAM. DMT's task is to specify the channels that are used for actual data transfer. If interference is present on a particular 4kHz channel then DMT will shut down that channel and assign a new channel. This channel switching occurs in real time and is completely transparent to the user. In a sense ADSL is like having 247 dial-up modems all working together, each modem using QAM and DMT ensuring they all work together efficiently. The ADSL modem and the DSL hardware at the telephone exchange communicate to agree on the channels currently being used.

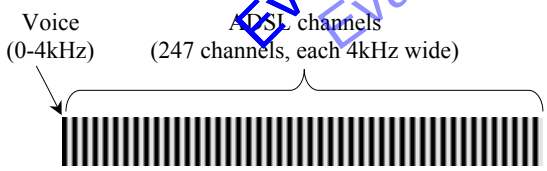


Fig 3.89
ADSL splits higher frequencies into 247 channels, each 4kHz wide.

At the local telephone exchange all the copper wires from the neighbourhood are connected to a splitter (see *Fig 3.90*). This splitter directs the 0-4kHz frequencies to the normal telephone network and the higher ADSL frequencies to a DSL Access Multiplexor (DSLAM). The DSLAM (see *Fig 3.90*) performs all the DMT negotiations with individual ADSL modems and directs data to and from ISPs, where it heads onto the Internet. The term *multiplexor* simply refers to the DSLAM's task of combining multiple signals from customers onto a single line and extracting individual customer signals from this single line.

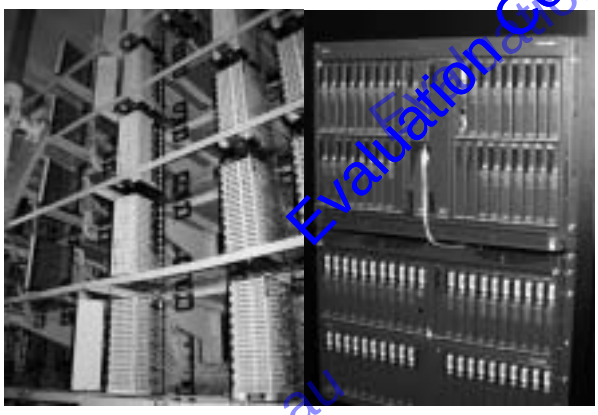


Fig 3.90
A splitter (left) and DSLAM (right).

In most ADSL systems the lower bandwidth ADSL channels are used for upstream data (from modem to exchange) and higher frequency channels are used for downstream data (exchange to modem). Some channels are able to transfer data in both directions. ADSL is one example of a DSL technology, the A stands for asymmetrical, meaning transmitting and receiving occur at different speeds.

GROUP TASK Research
Research, using the Internet, the upstream and downstream speeds that are achieved using current ADSL connections.

Consider the following

When first installing an ADSL connection it is necessary to install one or more low-pass (LP) filters. Sometimes a single filter is installed where the phone line enters the premises. In this case a qualified technician is required to install a dedicated ADSL line from the LP filter to the location of the ADSL modem. In other cases, the user installs a separate LP filter, like the one shown in *Fig 3.91*, between each telephone and wall socket.

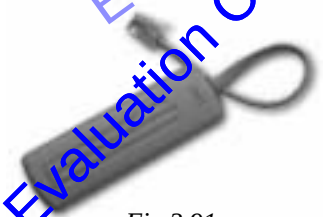


Fig 3.91
Inline LP filter.

GROUP TASK Discussion
What is the function of an LP filter? Describe how the two LP filter installation methods described above achieve the same outcome?

- **Cable modems**

Cable modems connect to the Internet via coaxial cables; usually the same cable that transmits cable TV stations. *Fig 3.92* describes how the bandwidth within the cable is split into channels. A single 6MHz bandwidth channel is used for downstream data – 6MHz is the width of a single cable TV station. This 6MHz wide channel is assigned within the range 88 to 860 megahertz. A narrower bandwidth channel is used for upstream; commonly 1.6MHz wide however various other bandwidths are supported ranging from 200kHz to 3.2MHz. The upstream channel is assigned within the range 5 to 42 megahertz. The particular frequencies used for both channels are determined by the cable Internet provider and cannot be altered by individual users.

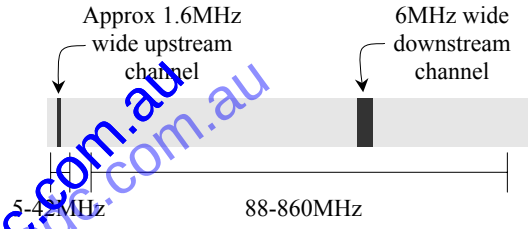


Fig 3.92
Cable modems share a bandwidth of 6MHz downstream and a lower bandwidth upstream.

The bandwidth used in a cable system is significantly larger than that used for ADSL. Therefore, one would assume the rate of data transfer would be much larger. In reality cable connections achieve speeds similar to ADSL connections; why is this? Cable connections are shared amongst multiple users. A single 6MHz downstream channel is likely to be shared by hundreds of users. In a sense all the cable modems sharing a particular channel form a local area network. Every cable modem within the network receives all messages; they just ignore messages addressed to other modems. Consequently when only a few users are downloading then higher speeds are possible than when many users are downloading. Clearly the same situation occurs when uploading. This is why cable Internet companies include statements within their conditions stating that speeds quoted are not guaranteed.

Consider the following

Cable modems connect using coaxial cable whilst ADSL systems use standard copper telephone wires. Coaxial cable is shielded to exclude outside interference and also to ensure the integrity of the signal.

GROUP TASK Discussion
ADSL uses DMT and many small bandwidth channels, whilst cable uses QAM and two relatively large bandwidth channels. Discuss reasons for these differences in terms of the transmission media used by each system.

Currently both ADSL and cable Internet providers reduce speeds when an agreed download limit has been exceeded. For cable connections only the upstream speed is reduced whilst both up and downstream speeds are reduced for most ADSL connections.

GROUP TASK Discussion
How can ADSL and cable Internet providers alter speeds? And why don't cable Internet providers reduce downstream speeds? Discuss.

- **Router**

Routers specialise in directing messages over the most efficient path to their destination. Today the large majority of routers operate at the network layer of the OSI model using the IP protocol. Therefore routing decisions are based on each datagram's destination IP address. Routers usually include the functionality of a gateway. They are able to communicate with networks that use different protocols and even completely different methods and media for communication. Many routers also include a variety of different security features. They are able to block messages based on the sender's IP address, block access to specific web sites and even restrict communication to certain high level protocols.

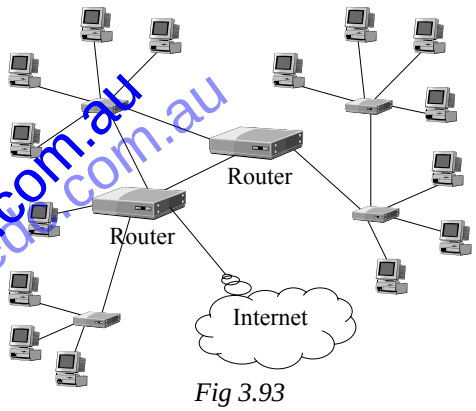


Fig 3.93
Routers forward messages over the most efficient path and can alter this path as needed.

Home or small business routers connect a single LAN to the Internet. For these systems the decision is relatively simple – either the IP datagram is addressed to a local node or it is not. Local datagrams are left alone whilst all others are sent out to the Internet. The routing table maintained by these routers is relatively small and rarely changes. Home and small business routers are commonly integrated devices that commonly include a router, an Ethernet switch and also a wireless access point – these integrated devices are what the general public call routers.

Routers out on the larger Internet connect to many other routers. For these routers deciding on the best path for each IP datagram is considerably more complex. Such routers communicate with other adjoining routers to continually update their internal routing table. The routing table is examined to determine the most efficient route for each IP datagram. However, should any connections within the most efficient path fail then routers automatically direct the message over an alternate path. On larger wide area networks, and in particular the Internet, thousands of routers work together to pass messages to their final destination.

Consider the following

Earlier in this chapter we discussed the operation of the Internet Protocol (IP). During our discussion we learnt that each IP address is composed of a network ID and a host ID. Routers use the network ID as the basis for directing IP datagrams. Network IDs effectively splits the Internet into a hierarchy of sub-networks or subnets. You may have heard the term subnet mask or seen this setting on your own computer. Subnet masks when combined with IP addresses enabled the network ID (and also the host ID) within an IP address to be determined. Routers perform this process on every destination IP address in every datagram to determine the datagrams next hop. The Network IDs and subnet masks are stored in the router's internal routing table.

A routing table is essentially a table that includes records for each Network ID the router knows about. Each record includes a field for the network's IP addresses, the networks subnet mask, the gateway IP address and a metric field. The network IP address and subnet mask are compared with the destination IP address within the current datagram. If the destination IP address is determined to be part of that network then the datagram is sent on the interface with the corresponding gateway IP address.

All routers have multiple IP addresses, one for each gateway. Each gateway provides an interface connecting to another router. The metric field is used to rank records that correspond to the same network ID – higher ranked records being used first.

GROUP TASK Practical Activity
On a Windows machine open a command prompt (type cmd at the run command on the start menu) and type the command ROUTE PRINT. This causes the current routing table to be displayed. Identify each of the fields mentioned above.

GROUP TASK Practical Activity
On a Windows machine open a command prompt (type cmd at the run command on the start menu) and type the command TRACERT followed by a web address, e.g. TRACERT www.microsoft.com. This causes a table showing each hop in a datagrams journey to be displayed. Determine and describe the significance of the fields and records displayed.

SERVERS

Servers provide specific processing services to other nodes (clients). We discussed the general operation of client/server architectures earlier in this chapter. In this section we briefly consider some of the more common services performed by servers. Note that this section is included under the general heading of "Network Hardware"; servers are often distinct computers designed with hardware suited to the services they provide, however what makes them servers is actually the installed software. On large networks dedicated servers are common whilst on smaller networks a server may well perform many tasks including the execution of end-user applications.

Most servers run a network operating system (NOS) to manage user access to the services the server provides. We discuss features of network operating systems in the next section. Most network operating systems include file server and print server functionality as these are the core services that require user authentication and user access rights.

There are numerous different services that servers provide. Examples of servers includes file servers, print servers, database servers, mail servers, web servers and proxy servers. In this section we restrict our discussion to a brief overview of each of these services.

File Servers

A file server manages storage and retrieval of files and also application software in response to client requests. In hardware terms dedicated file servers do not require extremely fast processors, their main requirement being large amounts of fast secondary storage and a sufficiently fast connection to the network.

Fault Tolerance
The ability of a system to continue operating despite the failure of one or more of its components.

Commonly file servers include multiple hard disks connected together into an array – RAID (Redundant Array of Independent Disks). Users are often unaware that multiple disks are being used. RAID uses different combinations of striping and mirroring to both improve data access speeds and also to improve the fault tolerance of the system. Striping stores single files across a number of physical disks and mirroring stores the same data on more than one disk. On larger RAID systems it is possible to replace faulty drives without halting the system – this is

known as hot swapping. To further improve fault tolerance many file servers include various other redundant components including extra power supplies, cooling fans and in some cases the complete server is replicated.

File servers must be able to process multiple file access requests from many users. Consequently the network connection to a file server often operates at a higher speed than for other workstation nodes. For each client request the file server, in combination with the NOS, checks the user's access rights or permissions before retrieving the file. The file server in combination with the NOS ensures the file is retrieved and transmitted according to the user's assigned access rights.

GROUP TASK Discussion
No doubt your school has one or more file servers. Determine the hardware specifications of these machines. Do these machines include any redundant components? Discuss.

Print Servers

A print server controls access to one or more printers for many clients. The print server receives all print requests and places them into an ordered print queue. As the printer completes jobs the next job in the print queue is progressively sent to the printer. Most print servers allow the order or priority of jobs to be changed and they also allow jobs to cancelled. When sharing smaller printers connected directly to a workstation the print server is a software service included within the operating system. In larger networks a dedicated printer server is used.

Dedicated print servers include more advanced functionality. Examples of such functionality includes:

- Ability to prioritise users based on their username. Jobs from higher priority users are placed higher in the print queue.
- Broadcast printing where a single job is printed on many printers.
- Fault tolerance or fall over protection where jobs that fail to print on one printer are automatically directed to some other printer.
- Job balancing where print jobs are spread evenly across many printers.
- Reservation systems where a user can reserve a printer with specific capabilities.
- Ability to reprint documents without the need for the client to resubmit the job. This is particularly useful in commercial environments when a printer jams or has some technical problem.
- Adding banner pages to print jobs. Banners are like cover pages – they commonly include the username, file name and time the job was started. Banners are useful for high volume systems where determining where one job ends and another starts would otherwise be difficult.
- Support for different operating systems and printing protocols. The print server converts client jobs from different operating systems so they will print correctly on a single printer.

GROUP TASK Discussion
No doubt your school has many printers in different locations throughout the school and most users only have access to specific printers. Discuss how printers in your school are shared.

Database Servers

Database servers run database management system (DBMS) software. We discussed the role DBMSs in some detail in chapter 2. Briefly a database server executes SQL statements on behalf of client applications. This can involve retrieving records, performing record updates, deletions and additions. The DBMS provides the connection to the database and ensures the rules defined for the database are maintained. For example ensuring relationships are maintained and performing data validation prior to records being stored.

Mail Servers

We discussed the detailed operation of email earlier in this chapter. Email uses two different application/presentation layer protocols SMTP and either POP or IMAP. These protocols run on SMTP, POP and IMAP servers. It is not unusual for all three protocols to run on a single server machine.

Email client applications, such as Microsoft Outlook, must be able to communicate using these protocols. SMTP (Simple Mail Transfer Protocol) is used to send email messages from an email SMTP client application to an SMTP server. Emails are received by an email client application from a POP (Post Office Protocol) server or IMAP (Internet Message Access Protocol) server.

Web Servers

We discussed the operation of web servers when discussing the HTTP protocol earlier in this chapter. Essentially a web server provides services to web browsers – they retrieve web pages and transmit them back to the requesting client web browser.

Web servers must also include services that allow web pages to be uploaded, edited and deleted. Such services require users to first be authenticated by the web server. Many web servers, particularly those operated by ISPs, host many different web sites. These servers require high speed links to the Internet together with fast access to the files they host.

Proxy Servers

A proxy server sits between clients and real servers. The proxy server tries to perform the request itself without bothering the real server. In essence the proxy server performs requests on behalf of a server. This relieves pressure on the real server and also reduces the amount of data that needs to be transmitted and received. Proxy servers speed up access times when the same request is made by many clients. The proxy server keeps a record of recent requests and responses within its large cache.

Perhaps the most common type of proxy server are those that operate between client browsers and web servers. The proxy server receives all web requests from all clients. If the files are found in the proxy server's cache then there is no need to retrieve it from the original remote web server. Proxy servers that operate between clients and the Internet are also gateways – they provide connectivity between the LAN and the Internet. These proxy servers are also used to censor and filter web content. For example many proxy servers can be set to block access to particular websites or restrict access to particular websites. Most proxy servers can also filter incoming pages to remove pornography and other undesirable content.

GROUP TASK Discussion

It is likely that Internet access at your school is via a proxy server – either within the school or operated by the school system. Determine if this is the case and describe the processes this server performs.

NETWORK SOFTWARE

Network software includes the Network Operating System (NOS) and also network based applications such as those running on the various servers within the network. Most operating systems include network capabilities, however a NOS has many more advanced network management and security features. Network operating systems allow networks to be centrally controlled by network administrators. The ability to centrally control networks improves the security and efficiency of access to the network's various resources. Furthermore it greatly simplifies the tasks performed by network administrators.

In this section we restrict our discussion to an overview of network operating systems and some of the common tasks performed by network administrators.

NETWORK OPERATING SYSTEM (NOS)

Network operating systems operate at the network and above layers of the OSI model. The NOS is installed on one or more servers where it provides various services to secure and support the network's resources and users – one vital NOS service being the authentication of users based on their user names and passwords. Once authenticated the NOS provides the user with access to the network's resources based on their pre-assigned privileges and profiles. Network resources include a variety of hardware and software such as servers, workstations, printers, applications, directories and files. A profile commonly includes details of the desktop configuration, language, colours, fonts, available applications, start menu items and location of user documents. Privileges define the services, directories and files a user (or workstation) can access together with details of how these resources can be used – including file access rights or permissions. Other servers on the network trust the NOS to authenticate users, hence a single login is required.

The NOS allows network administrators to create policies. A policy is used to assign particular resources to groups of users and/or groups of workstations (or clients) with common needs. For example in Windows Server 2003 group policies are created that include profile and privilege details common to groups of users or workstations. Users in a sales department all use similar applications and settings hence the same group policy can be assigned to all users in the sales department. Similarly a group policy can be created for groups of client machines (or workstations), for example workstations in one area may all connect to a particular printer and may connect to the Internet via a particular gateway. Policies greatly simplify the administrative tasks performed by network administrators.

GROUP TASK Research
Using the Internet, or otherwise, find examples of different network operating systems in common use. Research the techniques and tools used to share resources using each of theses NOSs.

NETWORK ADMINISTRATION TASKS

Network administrators are the personnel responsible for the ongoing maintenance of network hardware and software. This includes installation and configuration of switches, routers and other active hardware devices. However on a day-to-day basis network administrators spend much of their time providing support to new and existing users. This includes configuring new workstations (clients) and controlling and monitoring access to network resources as needs change.

Maintaining a LAN is a complex and specialised task performed by professional network administrators. In IPT we can only hope to grasp a general overview of the processes performed by a network administrator. The detail of how each task is accomplished will be different depending on the NOS used. Therefore we restrict our discussion to an overview of some of the more common network administration tasks.

Adding/Removing Users

Each new user has an individual account created that includes their username and password together with details of any assigned policies and privileges. Obviously a user's account is removed or made inactive when a user is removed.

The policies and privileges assigned to a user may be inherited from other existing group policies. Commonly a new user will require access to similar network resources as other groups of existing users, hence the new user is added to one or more existing groups. For example a new salesman requires the same access as existing salespersons. Therefore they are added to the "Sales Group"; as a consequence the new user has access to the same set of network resources as the existing salespersons. When adding a new user they are commonly given a standard password that must be changed when they first log onto the network.

If the network is configured such that users can logon at a number of workstations then their individual profile is configured to be stored on a server. During logon the user is first authenticated and then their individual profile is copied from the server to the local workstation. When they logoff any profile changes, such as desktop settings, are written back to the server.

GROUP TASK Research

Microsoft Windows Server NOSs use domains, domain controllers and active directories. Research and discuss the meaning of these terms and briefly explain the purpose of each.

Assigning printers

Printers can be assigned to specific workstations or to specific users. As printers are physical devices that are installed in specific locations it often makes sense to assign printers to workstations rather than users. This means users will have access to a printer that is physically close to the workstation where they are currently logged on.

Assigning file access rights

File access rights are also known as permissions. On many systems file access rights are a type of privilege. File access rights determine the processes a user can perform on a file or directory at the file level. On most systems the access rights applied to a directory also apply to any files or sub-directories contained within that directory.

Commonly groups of users that perform similar tasks require similar file access rights, which can form part of an assigned group policy. The majority of users will also require full access to a particular directory or folder where their own files and documents are stored.

Typically file access rights are stored by network operating systems within an access control list (ACL). An ACL specifies the user who owns (created) the directory or file, groups who have permissions to access the file and also the access rights assigned to these users. Let us consider typical permissions (access rights) that can be specified for directories (or folders) and also for individual files. The details below relate specifically to systems that use the NT file system (NTFS), which includes all current versions of Microsoft Windows. Other operating systems will have a similar set of permissions.

- **Directory (or folder) Permissions**
  - Full control – Users with full control can change the permissions for the folder, take ownership of the folder and delete any sub-folders and files within the folder. Full control also includes all of the permissions below.
  - Modify – Users can delete the folder and also perform processes permitted by write and read and execute permissions.
  - Read and Execute – Users can navigate through the folder to reach other folders and files. Includes read permission and list folder contents permission.
  - List folder contents – See the names of sub-folders and files within the folder.
  - Read – Users can see the name of sub-folders and files and view who owns the folder. Furthermore users can view all the permissions assigned to the folder but cannot alter these permissions. Users can also view attributes of the folder such as read-only, hidden, archive and system attributes.
  - Write – Users can create new files and sub-folders within the folder. They can change attributes of the folder. Users with write access can view, but not modify folder ownership and permissions.

Fig 3.94
Setting NTFS folder permissions.

- **File Permissions**
  - Full control – Users with full control can change the permissions for the file, take ownership of the file. Full control also includes all of the permissions below.
  - Modify – Alter and delete the file and also perform processes permitted by write and read and execute permissions.
  - Read and Execute – Users can run executable files and also read permission processes.
  - Read – Open and display the file. Furthermore users can view all the permissions assigned to the file but cannot alter these permissions. Users can also view attributes of the file.
  - Write – Overwrite the file with a new version. They can change attributes of the file. Users with write access can view, but not modify file ownership and permissions.

GROUP TASK Research
All current operating systems include some form of "file system". Determine the file system used by your school or home computer's operating system. Research available access rights and how they are inherited within this operating system.

Installation of software and sharing with users

Network operating systems are able to automate the installation of software to multiple users. This saves considerable time for network administrators, as they do not need to manually start the installation on numerous client workstations. On large networks where numerous software applications are being used by a wide variety of users in different combinations the automation of software installations is essential.

Software applications can be installed on individual client workstations where they are available for use by any user that logs onto the workstation. In this case the software installs next time the computer starts. This is an appropriate strategy when the software application is widely used – such as a word processor or email client. More specialised applications can be installed for particular users or groups of users. In this case the software installs when the user next logs on.

GROUP TASK Discussion

Think about software applications available for use on your school network. Some are available to all users whilst some are available to just some users. Explain how an upgrade of each of these applications could best be deployed to users.

Client installation and protocol assignment

Every network will have a different specific set of steps for installing new clients. Some require client applications to be installed manually, others automate this process. Some networks require a particular version of the operating system be installed over the network – in these cases it is common for the network settings to also be configured remotely and automatically. Commonly the network administrator or a technician performs these installation steps. Typical steps required to install a new client onto a network include:

1. Ensure the new machine has a compatible NIC (network interface card) installed that supports the data link and physical layer protocols used by the LAN. In most cases new NICs are able to automatically sense the correct speed and protocols being used.
2. Ensure the operating system on the client is compatible with the NOS. Most LANs now use TCP/IP therefore it will be necessary to obtain IP addresses and other parameters needed to configure the connection.
3. Physically connect the NIC to the network using a patch cable. Today this is usually a UTP path cable that connects to an existing network point on the wall. If the point has not been used then the network administrator may need to install a patch cable at the other end to complete the connection from patch panel to switch.
4. The network administrator needs to create the machine within the NOS and assign any profiles – which may include software to be installed. If a new user will use the client then they too will require a user account.
5. After booting the client machine it is necessary to enter a legitimate username and password. A domain or server is also specified. This is used to determine the location of the server used to authenticate the user name and password.

Fig 3.95
Windows Server 2003 logon screen.

HSC style question:

Jack is the network administrator for a company that employs some 50 staff. Each staff member has their own computer connected to the company's LAN. Each staff member has Internet and email access via the company's web and mail servers.

(a) What is a server, and in particular, what are the functions of web and mail servers?

(b) One of Jack's tasks is to assign file access rights to users. What does this task involve? Discuss.

(c) A number of staff are experiencing poor performance when using the LAN. Jack discovers that all these users are directly connected to a single hub and on this hub the data collision light is virtually always on.

Identify the network topology used for this part of the LAN and discuss possible reasons the data collision light is virtually always on.

Suggested Solution

(a) A server is usually a machine on a network that is dedicated to performing a specific task. However what makes these machines servers is the software they execute – hence any machine can be a server. Servers respond to requests from multiple clients. They specialise in performing specific tasks or services.

A web server responds to requests for web pages from clients (usually web browsers). The web server retrieves the requested page and transmits it back to the client (usually over the Internet using HTTP and TCP/IP).

Mail servers store email for each account and are used to set-up these accounts. Mail servers store incoming mail into each user's mail box. The post office protocol (POP) is used by email clients to retrieve mail from mail servers. The Simple Mail Transport Protocol (SMTP) is used to send mail to mail servers and between mail servers. The SMTP mail server checks the email address of all outgoing mail and directs it to the appropriate receiving mail server on the net.

(b) To assign file access rights requires that each user be assigned a user name and password. The user name can be grouped according to access required by different groups of users. Users or groups of users are then given rights to particular directories. These rights could allow them to merely read files or to create, modify and/or delete files within the directories they can access.

(c) As the users are connected to a hub a physical star topology and a logical bus topology is being used. As a consequence all nodes connected to the hub are sharing the same communication channel.

Because collisions are occurring it appears that CSMA/CD is being used. This means that two or more nodes can transmit at the same time resulting in the collisions indicated by the collision light. Reasons for so many collisions include excessive network traffic, which could be caused by a data intensive application, particularly one transferring video, image or audio to many nodes. Perhaps the hub itself is faulty or one node's NIC has a fault such that it is continually trying to send.

SET 3H

1. Which device converts data from a computer into a form suitable for transmission across a LAN?
   (A) NIC
   (B) Repeater
   (C) Switch
   (D) Router

2. Which device extends the range of transmission media?
   (A) Modem
   (B) Repeater
   (C) Bridge
   (D) Gateway

3. Routers direct messages based on which of the following?
   (A) Gateway Addresses
   (B) Collision Domains
   (C) MAC Addresses
   (D) IP Addresses

4. Redundant components in a server:
   (A) cause duplicate data.
   (B) reduce fault tolerance.
   (C) improve fault tolerance.
   (D) increase data access speeds.

5. A central node that repeats messages to all attached nodes is called a:
   (A) repeater.
   (B) switch.
   (C) router.
   (D) hub.

6. Which network device has at least two IP addresses?
   (A) Switch
   (B) NIC
   (C) Router
   (D) WAP

7. A server that operates between clients and real servers is called a:
   (A) mail server.
   (B) proxy server.
   (C) web server.
   (D) file server.

8. A server running SMTP, POP and IMAP is probably a:
   (A) mail server.
   (B) web server.
   (C) file server.
   (D) proxy server.

9. File access rights in many NOSs are known as:
   (A) permissions.
   (B) policies.
   (C) profiles.
   (D) privileges.

10. Policies are used by network administrators:
    (A) to simplify tasks.
    (B) to assign the same rights to many users.
    (C) to assign the same services to many clients.
    (D) All of the above.

11. Outline the processes performed by each of the following devices.
    (a) NIC
    (b) Repeater
    (c) Hub
    (d) Bridge
    (e) Switch
    (f) Gateway
    (g) WAP
    (h) Modem
    (i) Router

12. Outline the services provided by each of the following.
    (a) File server
    (b) Print server
    (c) Database server
    (d) Mail server
    (e) Web server
    (f) Proxy server

13. A device marketed as an "ADSL Modem" also includes four Ethernet ports and a wireless antenna. Identify and briefly describe the devices integrated within this "ADSL Modem".

14. Outline the steps performed by a network administrator to complete the following tasks.
    (a) Add a new user.
    (b) Install a new client machine.

15. A home network includes three PCs with Ethernet NICS, a laptop with an 802.11 wireless interface, an Ethernet switch, a WAP and an ADSL modem.
    (a) Construct a diagram to explain how these components would best be connected.
    (b) Identify and describe the processes occurring, and the software and hardware used as the laptop browses the web.

ISSUES RELATED TO COMMUNICATION SYSTEMS

Throughout much of this chapter we have concentrated on the technical detail of how data is transferred; in this section we are concerned with the sharing of information and knowledge. After all this is the central purpose of all communication systems.

When communication is face-to-face one's physical appearance, cultural background, gender and physical location are all on display. These factors greatly influence the communication that takes place. When communicating electronically such factors remain largely unknown. In cyberspace relationships can be built on common interests and needs. Information and knowledge is shared between people who may never physically meet. People who would not (or could not) normally communicate face-to-face can freely express and share their ideas and knowledge online. These people are free to converse without prejudice. However all is not perfect, this freedom can easily be abused by the unscrupulous.

Electronic communication systems, and in particular the Internet, allow information to be shared quickly and relatively anonymously. The identity of the author can be hidden or obscured which makes it difficult for readers to verify the source and quality of the information. Unscrupulous persons are able to masquerade as trusted others in order to fraudulently obtain personal information such as credit card or banking details.

Most people presume their email messages to be private; in reality network administrators and others with suitable access rights are able to view and monitor emails. Those in control of networks are able to restrict and monitor the activities of users. Such power relationships are often legitimate, however as is the case with all such relationships power can be abused.

The Internet has removed national and international boundaries. We are free to communicate and trade internationally. Individual governments have little control over international trade and furthermore enforcing international laws is expensive and often ineffective in cyberspace. For example sending spam (mass electronic junk mail) is illegal within Australia, however Australian law has no control over spam sent from off shore locations.

To cover all possible issues arising when using communication systems is clearly not possible. Rather in this section we describe general areas for further discussion and then outline some current and emerging trends in communication.

INTERNET FRAUD

Fraud is a criminal offence in virtually all countries, however Internet fraud when detected rarely results in a conviction. Fraud involves some kind of deception that includes false statements that intentionally aims to cause another person to suffer loss. Unfortunately fraudulent activity using the Internet is the most common form of e-crime. Examples of Internet fraud include:

- Some spam messages try to convince users to purchase goods at discount prices. Users then enter their banking or credit card details, which are later used to make fraudulent withdrawals or purchases. In most cases prices that are "too good to be true" probably are!
- Identity theft is a form of fraud where someone assumes the identity of someone else. Commonly the criminal obtains various personal details about the person so that they can convince organisations that they are that person. This enables the criminal to take out loans, purchase goods and withdraw money from the person's bank accounts. Identity fraud even when discovered can have long term

consequences as the person must restore their reputations with many different organisations.

- Phishing is a form of spam where the email contains a message that purports to be from a trusted source. One common phishing scam uses mass emails purporting to be from a particular organisation and asking recipients to update their details by clicking on a hyperlink. The hyperlink takes them to a site masquerading as the real organisation's login screen. The fraudulent screen collects the user name and password and then forwards the user to the real site. Often users are unaware they are a victim of a scam as the criminals do not use the log in details for some time.

GROUP TASK Research
Using the Internet, or otherwise, research particular examples of Internet fraud. For each example determine if the perpetrators where actually convicted.

GROUP TASK Discussion
Many Internet fraud scams involve banks and other financial institutions. Despite this fact it is rare for such organisations to publicly disclose the extent of such fraudulent activities. Discuss.

POWER AND CONTROL

Those who control access to information are placed in a position of power over the users whose access they control. Not only can access to information be restricted and censored but the activities of users can also be monitored. Often users do not understand the extent to which their online activities can be monitored. Some issues to consider include:

- Parents install Internet filtering software to restrict their children's access to pornography and other inappropriate online information. Essentially parents are acting as censors for their children.
- Employers are able to monitor or even remotely watch and listen into their employee's online sessions and telephone calls. From the employer's perspective they are legitimately monitoring the quality of service provided. Many employees feel such systems imply a lack of trust and infringe upon their right to privacy.
- Email messages, unless securely encrypted, can be freely read by anyone with administrator rights to a mail server through which the messages pass. Many businesses claim they have a right to view messages sent and received on behalf of their company. However there are many cases where this has occurred without the knowledge of the employees.
- Backup copies of messages and web sites can and are stored for extended periods of time. Deleting a message from an email client or a file from a web server is not sufficient. Server archives have been used during investigations and have led to prosecutions.
- Organisations, including most schools, restrict and censor Internet access allowing only "approved" web sites and applications. In theory legitimate reasons exist and in most instances new sites and applications can be added to the approved list upon application. In practice many users find such controls oppressive and react with attempts to circumvent such restrictions.

GROUP TASK Discussion
Consider restrictions placed on Internet access at your school, work or home. Do these restrictions give power to those who administer and control Internet access? Discuss.

REMOVAL OF PHYSICAL BOUNDARIES

In cyberspace one's physical location is of little or no relevance. Individuals and organisations can trade across the globe. This globalisation has many advantages. For instance virtual communities can be created without regard to geographical location. However, there are also legal implications in terms of criminal activity and also in terms of taxation law. Information can be obtained from international sources as easily as from local sources.

- It is difficult to determine the real nature and location of online businesses. A single person can setup a website that appears to represent a large corporation. Such businesses can be setup quickly and they can be dissolved just as quickly. The legal safeguards available in Australia are not present in many other countries. In general Australian law does not apply to international transactions.
- Virtual organisations and communities are created as needs arise. Some are based on common areas of interest, to collaborate on a particular project or to form relationships. Participants in such organisations are largely honest and genuine, however in many cases ethical behaviour cannot practically be enforced.
- Most people speak just one language. As a consequence we seldom communicate with those who speak a different language. This greatly restricts our ability to understand and empathise with other cultures despite the removal of physical boundaries.

GROUP TASK Discussion
Identify particular examples of communication systems you have used that traverse international boundaries. Discuss issues you experienced during such communications.

INTERPERSONAL ISSUES

Electronic communication systems have changed the way many form relationships. Ideas delivered electronically can often appear less forceful and caring when compared to face-to-face communication. During face-to-face communication we continually receive and send non-verbal feedback to confirm understanding and to build relationships. Chat, teleconferencing and other real time communication systems are an attempt to address this issue, however non-verbal clues are not present, which can restrict one's ability to form meaningful personal relationships.

- Online dating sites enable people to present a particular well thought out view of themselves, initial personal contact being made via email. On the surface people feel they have much in common – similar background, culture, job, etc. However when face-to-face meetings subsequently occur people often find there is little or no real attraction.
- Ideas and comments from amateur individuals can appear as legitimate as those from professionals and large trusted organisations. On the Internet uninformed individuals can make their views appear as forceful and influential as experts. This is difficult and rarely occurs with more traditional forms of communication.

- Text based messages delivered via email or chat can easily be misinterpreted. It takes time to receive feedback and even when received it lacks the body language, tone of voice and facial expressions present when communicating in person.
- All are equal when communicating electronically. We need not even be aware that we are communicating with someone with a disability. For example most people have difficulty communicating face-to-face with someone who has a profound hearing disability. On the Internet we may not be aware of such a disability.

GROUP TASK Discussion
Many of us regularly communicate electronically with people we have never met face-to-face. Compare and contrast such relationships with more traditional face-to-face relationships.

WORK AND EMPLOYMENT ISSUES

Electronic communication systems have changed the way many people work and where they complete their work. For many jobs the ability to use electronic communication systems is required. Communication systems have provided the means for many people to work from home or from virtually any other location. They can vary their work hours and they can be contacted anywhere. This is certainly positive for employers and clients, however too often it has led to an expectation that employees are always available.

- Work teams can be setup where team members never or rarely physically meet. Rather they communicate and collaborate electronically using email, forums, teleconferencing and other electronic communication systems.
- Traditional employment is largely based on hours worked. When employees work from home they may well work unusual hours interspersed with other home and personal activities. This presents problems for employers who require reassurance that work is completed. It also presents problems for employees who must balance their intertwined work and personal lives.
- Most research indicates that those who work from home actually work longer hours and are more productive compared to those who travel to a specific work place. Some of the efficiency is due to the travel time saved, however the remainder is largely due to employees having more control and responsibility for the work they do.
- Many employees are provided with mobile phones and laptops that mean they are contactable in various ways 24 hours a day from almost any location. Today many expect to speak directly with people at any time of the day or at least that a response to messages will be made within an hour or so.
- Traditional retail stores are experiencing strong competition form online retailers. Potential customers often view goods in a physical store and then negotiate a better deal with an online retailer. Online retailers have significantly lower operating costs.

GROUP TASK Discussion
Do you know people who work substantially from home? Compare and contrast the nature of work for these people compared to those who travel to a specific workplace.

CURRENT AND EMERGING TRENDS IN COMMUNICATION

Blogs

Blog is short for web log, which is essentially a journal that is made public by placing it on the web. Individuals regularly update their blog to express their personal views and opinions or simply to detail their day-to-day activities. Most blogs are arranged in date order with the most recent entry at the top. It is common for people to include a blog on their personal website – for instance, many people maintain a personal MySpace.com webpage. MySpace.com includes software tools that automate the creation of blogs.

Wikis

A wiki is a website where users are able to freely add new content and edit existing content. Apparently the term "wiki" originated from the Hawaiian phrase "wiki wiki", which means "super fast"; the implication being that the amount of content grows rapidly due to the large number of authors. Probably the most well-known and largest wiki is Wikipedia; an online encyclopaedia created and edited by members of the public. Because the information within a wiki is produced by the general public it should never be accepted on face value; rather alternative sources should be used to verify the accuracy of the information.

GROUP TASK Discussion

Some organisations, including some schools, have blocked access to Wikipedia, whilst others embrace and encourage its use. Discuss and debate both sides of this issue.

RSS Feeds

RSS is an acronym for Really Simple Syndication. Syndication is a process that has been used by journalists and other content creators for many years. When content, such as a news story or TV show, is syndicated it is published in many different places. For instance, a TV show such as Neighbours is produced in Australia but is syndicated and shown in many other countries. RSS feeds implement this syndication process over the Internet. The author offers some content they have created as an RSS feed. Other people can then choose to take up the author's offer of syndication and subscribe to the feed. With RSS feeds the subscription is usually anonymous – the author has no idea of the identity of the people who have subscribed to their RSS feed.

Podcasts are distributed as RSS feeds, however any type of online content can be distributed using this technique, including blogs, wikis, news and even updates to web sites. The feed can contain any combination of audio, video, image and text. In addition, feeds need not contain the complete content; rather a partial feed can be used that includes links to the complete content.

To subscribe to RSS feeds requires newsreader software. The newsreader stores details of each RSS feed you subscribe to. The newsreader then checks each subscribed feed at regular intervals and downloads any updates it detects to your computer. This means the content is sitting on your computer waiting to be read – there is no need to download anything at this time, in fact the computer can be offline.

RSS feeds have become popular largely as a consequence of the excessive quantity of junk mail people receive. Many people are reluctant to enter their email address into web forms out of fear they may receive masses of unwanted email messages. No identifying information, including email addresses, is required to subscribe to an RSS feed.

GROUP TASK Research
RSS feeds are in many ways an extension of newsgroups, which have been around as long as the Internet. Research how newsgroups work.

Podcasts

Podcasting puts users in control of what they listen to, when they listen to it, how they listen and where they listen. Essentially a podcast is an audio RSS feed that is automatically downloaded to your computer and copied to your MP3 player. Aggregator software, such as Apple's iTunes, manages and automates the entire process – from the user's perspective content simply appears on their MP3 player.

The term "podcast" is a play on the words iPod and broadcast, however any MP3 player can be used, not just Apple iPods – a podcast is simply a collection of MP3 files. Podcasters are the people who create the "radio like" audio content, often on a regular basis or as a series of programs. Typically each podcast is a sequence of MP3 files created over time. Commercial media and other organisations are also embracing podcasting as an alternative to more traditional information delivery systems.

GROUP TASK Research
Blogs, wikis and podcasts are often referred to as part of "Web 2.0". Research and discuss the meaning of the term "Web 2.0".

Online Radio, TV and Video on Demand (VOD)

Online radio and TV programs are streamed over the Internet and displayed in real time using a streaming media player. Many traditional radio and TV stations now provide their programs online. Some stations provide a live digital feed, however it is the ability to watch past programs that distinguishes online delivery from traditional broadcasts – users can watch the programs they want, when they want.

Video on demand (VOD) systems are used to distribute video content directly to users over a communication link – much like an online video/DVD store. The aim of all VOD systems is to provide users with high quality video immediately in real time. Unfortunately current (2007) transmissions speeds and compression technologies are insufficient for this aim to be achieved. As a consequence VOD implementations compromise either quality, range of titles or the immediacy of delivery. Streaming systems compromise quality whilst largely achieving the range of titles and real time aims. Cable and satellite pay TV offer a limited range of high quality titles where each title commences at regular intervals – not quite real time. Online VOD stores deliver a large range of high quality movies. However movies must be downloaded prior to viewing – typical downloads take more than an hour.

3G mobile networks

The term 3G refers to third generation mobile communication networks. Essentially 3G networks provide higher data transfer rates than older GSM and CDMA mobile phone networks. As a consequence, access to much richer content is possible. 3G networks support video calls, web browsing and virtually all other Internet applications. Although 3G mobile phones are the primary device used on 3G networks, it is also common to use 3G networks to connect computers to the Internet. Currently high speed 3G coverage is limited to major cities and surrounding areas.

GROUP TASK Research
Research current 3G network speeds, the speed required for high quality VOD and predictions of future mobile network speeds. When will high quality VOD be possible over mobile networks? Discuss.

CHAPTER 3 REVIEW

1. Which list contains ONLY network hardware?
   (A) SMTP server, NOS, DBMS server.
   (B) UTP cables, switch, NIC.
   (C) Router, proxy server, codec
   (D) Ethernet, TCP/IP, HTTP.

2. In regard to error checking, which of the following is TRUE?
   (A) Messages containing errors are discarded.
   (B) Messages without errors are acknowledged.
   (C) Messages with errors are resent.
   (D) All answers – it depends on the protocol.

3. A 16-bit checksum is being used. For an error to NOT be detected what must occur?
   (A) The corruption must be the result of a data collision.
   (B) The sender or receiver has incorrectly calculated the checksum.
   (C) The message is corrupted such that the checksum is still correct.
   (D) The sender and receiver are not synchronised or are using different protocols.

4. The essential difference between the Internet and the PSTN is:
   (A) Internet is packet switched, PSTN is circuit switched.
   (B) Internet is circuit switched, PSTN is packet switched.
   (C) Internet is connection-based, PSTN is connectionless.
   (D) Internet is digital, PSTN is analog.

5. A switch is called a multipoint bridge because:
   (A) it separates a network into different segments.
   (B) it converts between two or more protocols.
   (C) It maintains a send and receive channel for each node.
   (D) it uses a physical and logical star topology.

6. An email includes email addresses within its To and Bcc fields. Which of the following is TRUE?
   (A) The To recipients are unaware of any of the other recipients.
   (B) The Bcc recipients are unaware of any of the other recipients.
   (C) Recipients in the Bcc field will be unaware of the To recipients.
   (D) Recipients in the To field will be unaware of the Bcc recipients.

7. Client-server architecture is best described by which of the following?
   (A) A central server performs all processing on behalf of all clients or workstations.
   (B) A network wired as a physical star where the central node is a server and other nodes are clients.
   (C) Clients request a service, and then the server performs the operation and responds back to the client.
   (D) A system where particular machines known as servers control access to all network resources for client workstations.

8. Networks where all messages are broadcast to all attached nodes utilise which topology?
   (A) Logical bus topology.
   (B) Physical bus topology.
   (C) Logical star topology.
   (D) Physical star topology.

9. A self-clocking code where high to low and low to high transitions represent bits is known as:
   (A) CSMA/CD
   (B) CSMA/CA
   (C) Manchester encoding.
   (D) Ethernet.

10. The ability to stream video of different quality to many participants is commonly implemented over the Internet as:
    (A) multipoint multicast.
    (B) multipoint unicast.
    (C) single-point, unicast.
    (D) single-point, multicast.

11. Compare and contrast:
    (a) MAC addresses with IP addresses.
    (b) ADSL and cable modems.
    (c) Checksums with CRCs.
    (d) Odd parity with even parity.
    (e) Packet switched networks with circuit switched networks.
    (f) Analog data with digital data.
    (g) Wired media with wireless media.
    (h) CSMA/CD with token passing.
    (i) Blogs and wikis.
    (j) Online radio and TV with traditional radio and TV.
12. Outline the operation of:
    (a) Video conferences over the Internet.
    (b) Electronic mail.
    (c) EFTPOS.
    (d) Self-healing dual ring topologies.
    (e) Routers.
    (f) modems
    (g) HTTP.
    (h) RSS feeds
    (i) VOD
13. Explain how messages are transferred over Ethernet networks where a physical star topology is used and the central node is a:
    (a) hub.
    (b) switch
14. Explain how digital data is encoded using:
    (a) Manchester encoding.
    (b) 256 QAM.
15. Outline the processes performed by SSL, HTTP, TCP and IP as a private message passes from source to destination over the Internet.