E-business infrastructure: Introduction, What is the internet?, How does it work? Internet standards, Focus on who controls the internet, Managing e-business infrastructure, Focus on web service and service and service-oriented, Focus on new access devices,

Introduction:

E-business infrastructure refers to the combination of hardware such as servers and client PCs in an organization, the network used to link this hardware and the software applications used to deliver services to workers within the e-business and also to its partners and customers.

Infrastructure also includes the architecture of the networks, hardware and software and where it is located. Finally, infrastructure can also be considered to include the methods for publishing data and documents accessed through e-business applications. A key decision with managing this infrastructure is which elements are located within the company and which are managed externally as third-party managed applications, data servers and networks.

It is also important that the e-business infrastructure and the process of reviewing new technology investments be flexible enough to support changes required by the business to compete effectively. For example, for the media there are many new technologies being developed which were described from 2005 onwards as Web 2.0 and IPTV (television delivered over the broadband Internet).We will look at these approaches later in this chapter, but for now look at the implications in the Real-world e-business experiences interview and consider the implications for the newspaper publishing industry. In a speech to the American Society of Newspaper Editors in April 2005, Rupert Murdoch of News Corporation said:

E-business infrastructure components

The different components of e-business architecture which need to be managed relate to each other. The different components can be conceived of as different layers with defined interfaces between each layer. The different layers can best be understood in relation to a typical task performed by a user of an e-business system.

A five-layer model of e-business infrastructure (Fig.3.1)

I **E-business services – applications layer**	CRM, supply chain management, data mining, content management systems
II **Systems software layer**	Web browser and server software and standards, networking software and database management systems
III **Transport or network layer**	Physical network and transport standards (transmission TCP/IP)
IV **Storage/physical layer**	Permanent magnetic storage on web servers or optical backup or temporary storage in memory (RAM)
V **Content and data layer**	Web content for intranet, extranet and Internet sites, customers’ data, transaction data, clickstream data

For example, **an employee who needs to book a holiday** will access a specific human resources application or program that has been created to enable the holiday to be booked (Level I in *Figure 3.1*). This application will enable a holiday request to be entered and will forward the application to their manager and human resources department for approval.

To access the application, the employee will use a web browser such as Microsoft Internet Explorer Mozilla Firefox or Google Chrome using an operating system such as Microsoft Windows XP or Apple OS X (Level II in *Figure 3.1*).

This systems software will then request **transfer of the information** about the holiday request across a network or transport layer (Level III in *Figure 3.1*).

The **information will then be stored** in computer memory (RAM) or in long-term magnetic storage on a web server (Level IV in *Figure 3.1*).

The information itself which makes up the web pages or content viewed by the employee and the data about their holiday request are shown as a separate layer (Level V in *Figure 3.1*), although it could be argued that this is the first or second level in an e-business architecture

Kampas (2000) describes an alternative five-level infrastructure model of what he refers to as 'the information system function chain':

1 *Storage/physical*.
Memory and disk hardware components (equivalent to Level IV in *Figure 3.1*).
2 *Processing*.
Computation and logic provided by the processor (processing occurs at Levels I and II in *Figure 3.1*).
3 *Infrastructure*.
This refers to the human and external interfaces and also the network, referred to as 'extrastructure'. (This is Level III in *Figure 3.1*, although the human or external interfaces are not shown there.)
4 *Application/content*.
This is the data processed by the application into information. (This is Level V in *Figure 3.1*.)
5 *Intelligence*.
Additional computer-based logic that transforms information to knowledge.
(This is also part of the application layer I in *Figure 3.1*.)

What is the internet:

INTRODUCTION

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals through computers irrespective of geographic locations.

DEFINITION OF INTERNET

The Internet is a global network of computers that allows people to send email, view web sites, download files such as mp3 and images, chat, post messages on newsgroups and forums and much more.

The Internet was created by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1960's and was first known as the ARPANet. At this stage the Internet's first computers were at academic and government institutions and were mainly used for accessing files and to send emails.

From 1983 onwards the Internet as we know it today started to form with the introduction of the communication protocol TCP/IP to ARPANet. Since 1983 the Internet has accommodated a lot of changes and continues to keep developing. The last two decades has seen the Internet accommodate such things as network LANs and ATM and frame switched services. The Internet continues to evolve with it becoming available on mobile phones and pagers and possibly on televisions in the future.

The actual term “Internet” was finally defined in 1995 by FNC (The Federal Networking Council). According to Federal Networking Council (FNC) **Internet refers to the global information system that**,

- is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons.
- is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols.
- provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Evolution of internet

ARPANET

In the mid-1960s, mainframe computers used in research organizations were unable to communicate with each other because of different manufacturers. The **Advanced Research Projects Agency (ARPA)** in the Department of Defence (DOD) was interested in finding the way the computers could connect to each other so that research work could be shared among researchers , thereby reducing costs and duplication of effort.

In 1967, at an Associate for Computing Machinery (ACM) meeting, ARPA presented its ideas for **ARPANET,** a small network of connected computers. The idea was that each host computer (not necessarily from same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of UTAH were connected via the IMPs to form a Network. Software called *Network Control Protocol* (NCP) provided communication between the hosts.

Birth of the Internet (Timeline)

In 1972, Vint Cerf and Bob Kahn, both of them who were part of core ARPANET group, collaborated on what they called *Internetting Project.* They wanted to link different networks together so that a host on one network can communicate with a host on a second different network. There were many problems to overcome: diverse packet sizes, diverse interfaces, and diverse transmission rates, as well as different reliability requirements. Cerf and Kahn devised the idea of a device called *gateway* to serve as the intermediary hardware to transfer packets from one network to another.

Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This was a new version of NCP (*network control protocol*). This paper on Transmission control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. A radical idea was the transfer of responsibility for error correction from IMP to the host Machine. Around this Time the responsibility of the ARPANET was handed over to the Defence Communication Agency (DCA).

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.

Shortly thereafter, the authorities made a decison to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internetworking Protocol (IP)**. IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCP/IP.

In 1981, under a DARBA contract, UC Berkely modified the UNIX operating system to include TCP/IP. this inclusion of network software along with a popular operating system did much to further the popularity of networking. The open (non-manufacturer-specific) implementation of Berkeley UNIX gave every manufacturer a working code base on which they could build their products.

In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

MILNET

In 1983, ARPANET was split into two networks: **MILNET** for military users and **ARPANET** for non military users.

CSNET

Another milestone in Internet History was the creation of CSNET in 1981. **CSNET** was a network sponsored by national science foundation (NSF). The network was coneived by universities that were ineligible to join ARPANET due to an absence of defense ties to DARPA. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower. It featured connections to ARPANET and Telnet, the first commercial packet data service.

By the middle, 1980s, most U.S. universities with computer science departments were part of CSNET. Other institutions and companies were also forming their own networks and using TCP/IP to interconnect. The term *Internet*, originally associated with government-funded connected networks, now referred to the connected networks using TCP/IP protocols.

NSFNET

With the success of CSNET, the NSF, in 1986, sponsored **NSFNET**, a backbone that connected five supercomputer centres located throughout the United States. Community networks were allowed access to this backbone, a T1 line with a 1.544 Mbps data rate, thus providing connectivity throughout the United States.

In 1990, ARPANET was officially retired and replaced by NSFNET. In 1995, NSFNET reverted back to its original concept of research network.

ANSNET

In 1991, the U.S government decided taht NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and MCI, filled the void by forming a nonprofit organization called Advanced Network and Services (ANS) to build a new, high-speed Internet backbone called **ANSNET**

The Internet today is not a simple architecture. It is made up of many wide and local area networks (WANs and LANs) joined by connecting devices and switching stations (*nodes*). The Internet is continuously evolving and many new users are added each day. today most end users who want Internet connection use the services of **Internet Service Providers (ISPs)**. There are International Service Providers, National Service Providers (SprintLink, PSINet, UUNet Technology, AGIS, and Internet MCI providing Internet at **network access points NAPs**), regional service providers and local service providers.

For your help here is the complete summary and list of important events of Internet History/Timeline

- **1969.** Four Node ARPANET established.
- 1970. ARPA hosts implement NCP.
- 1973. Development of TCP/IP suite begins.
- 1977. An Internet tested using TCP/IP.
- 1978. UNIX distributed to academic/research sites.
- 1981. CSNET established.
- 1983. TCP/IP becomes the official protocol for ARPANET.
- 1983. MILNET was Born.
- 1986. NSFNET established.
- 1990. ARPANET decommissioned and replaced by NSFNET.
- 1995. NSFNET goes back to being a research network.
- 1995. Companies known as **Internet Service Providers (ISPs)** started

Advantages of internet

There many advantages to using the internet such as:

E-mail Email is now an essential communication tool in business. It is also excellent for keeping in touch with family and friends. The advantage to email is that it is free (no charge per use) when compared to telephone, fax and postal services.

Information There is a huge amount of information available on the internet for just about every subject known to man, ranging from government law and services, trade fairs and conferences, market information, new ideas and technical support.

Services Many services are now provided on the internet such as online banking, job seeking and applications, and hotel reservations. Often these services are not available off-line or cost more.

Buy or sell products.

The internet is a very effective way to buy and sell products all over the world. ***Communities*** Communities of all types have sprung up on the internet. Its a great way to meet up with people of similar interest and discuss common issues.

A Leading-Edge Image

Presenting your company or organization as leading-edge shows your customers and prospective customers that you are financially strong, technologically savvy, and ready for the 21st century. And that you care enough about your customers to take advantage of new technologies for their benefit. And finally that you have the resources to support your clients in the most beneficial manner possible.

More and more advertisers on television, radio, magazines, and newspapers are including a Web address. Now is the time to avoid playing catch-up later.

Improved Customer Service

The companies are available to their customers 24 hours a day, 7 days a week. The Internet never sleeps. Whenever customer needs information about any company, products or services, they can access the company’s Web Page.

Market Expansion

The Internet is a global system. Latest estimates are that there are about 40 million people with access to the Internet, and this number is growing every day. By simply posting a Web Page you are also addressing International markets.

Low Cost Marketing

Imagine developing a full color brochure without having to incur the costs of proofs, printers, wasted paper, long lead times between revisions, and more. Then imagine a full color product or services brochure that is interactive and which incorporates text, graphics, audio, and/or video. One that can be immediately updated without incurring the usual costs of product material updates. For a minimal initial investment your company or organization is presented to millions of Internet users worldwide. It's like a virtual brochure in everyone's hand without the associated costs.

Low Cost Selling

Without the cost of direct selling potential customers can get detailed information about your products or services at any time. And they can easily order your products over the Internet, or request additional information be sent to them via a request form on your Web page.

Lower Communication Costs

Your time, and your employees time, is valuable. Most businesses and organizations spend time answering the same questions over and over again. With a Web page you can make the answers available to everyone immediately. You can also update your Wed page with new information quickly and easily.

Value Added Marketing

You can use your Web page to provide useful information about your particular industry, product or uses. Any type of information that you believe will be valuable to your customer base can be included in your web page to encourage visitors to your site. You can also provide easy links to other sites with information that would be of value to your customers.

How does it work?

We have introduced the general terms and concepts that describe the operation of the Internet and the World Wide Web. In this section we look briefly at the standards that you may encounter which have been adopted to enable information transfer. Knowledge of these terms is useful for anyone involved in the management of e-commerce since discussion with suppliers may involve them. The standards forming the technical infrastructure of the Internet are controlled by several bodies which are reviewed at the end of this chapter.

‘Internet’ refers to the global information system that – (i) is logically linked together by a

globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/ follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

TCP/IP

TCP/IP development was led by Robert Kahn and Vince Cerf in the late 1960s and early 1970s and, according to Leiner *et al*. (2000), four rules controlled Kahn's early work on this protocol. These four rules highlight the operation of the TCP/IP protocol:

1 Distinct networks would be able to communicate seamlessly with other networks.

2 Communications would be on a best-effort basis, that is, if a data packet did not reach the final destination, it would be retransmitted from the source until successful receipt.

3 Black boxes would be used to connect the networks; these are now known as 'gateways' and 'routers' and are produced by companies such as Cisco and 3Com. In order to keep them simple there would be no information retained by the 'gateways'.

4 There would be no global control of transmissions – these would be governed by the requester and sender of information.

It can be seen that simplicity, speed and independence from control were at the heart of the development of the TCP/IP standards.

The data transmissions standards of the Internet such as TCP/IP are part of a larger set of standards known as the Open Systems Interconnection (OSI) model. This defines a layered model that enables servers to communicate with other servers and clients. When implemented in software, the combined layers are referred to as a 'protocol stack'. The seven layers of the OSI model are:

□ □*Application.* The program such as a web browser that creates and receives messages.

□ □*Presentation*. These protocols are usually part of the operating system.

□ □*Session.* This includes data-transfer protocols such as SMTP, HTTP and FTP.

□ □*Transport.* This layer ensures the integrity of data transmitted. Examples include the Internet TCP and Novell SPX.

□ □*Network*. Defines protocols for opening and maintaining links between servers. The best known are the Internet protocol IP and Novell IPX.

□ □*Data link.* Defines the rules for sending and receiving information.

□ □*Physical.* Low-level description of physical transmission methods.

The postal service is a good analogy for the transmission of data around the Internet using the TCP/IP protocol. Before we send mail, we always need to add a destination address. Likewise, the IP acts as an addressed envelope that is used to address a message to the appropriate IP address of the receiver (*Figure 3.13*).

The Internet is a packet-switched network that uses TCP/IP as its protocol. This means that, as messages or packets of data are sent, there is no part of the network that is dedicated to them. This is like the fact that when your letters and parcels are sent by post they are mixed with letters and parcels from other people. The alternative type of network is the circuitswitched network such as phone systems where the line is dedicated to the user for the duration of the call. Taking the analogy further, the transmission media of the Internet such as telephone lines, satellite links and optical cables are the equivalent of the vans, trains and planes that are used to carry post. Transmission media for the Internet include analogue media such as phone lines and faster, digital media such as Integrated Service Digital Network technology (ISDN) and more recently the Asynchronous Digital Subscriber Line (ADSL).

In addition to the transmission media, components of the network are also required to direct or route the packets or messages via the most efficient route. On the Internet these are referred to as 'routers' or 'hubs', and are manufactured by companies such as Cisco and 3Com. The routers are the equivalent of postal sorting offices which decide the best route for mail to take. They do not plan the entire route of the message, but rather they direct it to the next router that seems most appropriate given the destination and current network traffic.

Some addressing information goes at the beginning of your message; this information gives the network enough information to deliver the packet of data. The **IP address** of a receiving server is usually in the form 207.68.156.58 (as shown in *Figure 3.8*) which is a numerical representation of a better-known form such as www.microsoft.com. Each IP address is unique to a given organization, server or client, in a similar way to postal codes referring to a small number of houses. The first number refers to the top-level domain in the network, in this case

.com. The remaining numbers are used to refer to a particular organization.

Once the Internet message is addressed, the postal analogy is not so apt since related information is not sent across the Internet in one large message. For reasons of efficiency, information sent across IP networks is broken up into separate parts called **packets**. The information within a packet is usually between 1 and 1,500 characters long. This helps to route information most efficiently and fairly with different packets sent by different people gaining equal priority. The transmission control protocol TCP performs the task of splitting up the original message into packets on dispatch and reassembling it on receipt. Combining TCP and IP, you can think of an addressed IP envelope containing a TCP envelope which in turn contains part of the original message that has been split into a packet (*Figure 3.13*).

The HTTP protocol

HTTP, the Hypertext Transfer Protocol is the standard used to allow web browsers and servers to transfer requests for delivery of web pages and their embedded graphics. When you click on a link while viewing a web site, your web browser will request information from the server computer hosting the web site using HTTP. Since this protocol is important for delivering the web pages, the letters http:// are used to prefix all web addresses. HTTP messages are divided into HTTP 'get' messages for requesting and web page and HTTP 'send' message as shown in *Figure 3.13*. The web pages and graphics transferred in this way are transferred as packets, which is why web pages do not usually download gradually but come in jumps as different groups of packets arrive.

The inventor of HTTP, Tim Berners-Lee, describes its purpose as follows (Berners-Lee, 1999):

HTTP rules define things like which computer speaks first, and how they speak in turn. When two computers agree they can talk, they have to find a common way to represent their data so they can share it.

Uniform resource locators (URLs)

Web addresses refer to particular pages on a web server which is hosted by a company or organization. The technical name for web address is **uniform (or universal) resource locator (URL)**. URLs can be thought of as a standard method of addressing, similar to postcodes or ZIP codes, that make it straightforward to find the name of a site.

Web addresses always start with 'http://', so references to web sites in this book and in most promotional material from companies omit this part of the URL. Indeed, when using modern versions of web browsers, it is not necessary to type this in as part of the web page location since it is added automatically by the web browser. Although the vast majority of sites start with 'www', this is not universal, so it is necessary to specify this.

Web addresses are structured in a standard way as follows:

http://www.domain-name.extension/filename.html

Domain names

The domain name refers to the name of the web server and is usually selected to be the same as the name of the company, and the extension will indicate its type. The extension is also commonly known as the generic top-level domain (gTLD). Note that gTLDs are currently under discussion and there are proposals for adding new types such as .store and .firm.

Common gTLDs are:

(i) .com represents an international or American company such as www.travelocity.com**.**

(ii) .org are not-for-profit organizations (e.g. www.greenpeace.org)

(iii) .mobi – introduced in 2006 for sites configured for mobile phones

(iv) .net is a network provider such as www.demon.net.

There are also specific country-code top-level domains (ccTLDs):

(v) .co.uk represents a company based in the UK such as www.thomascook.co.uk.

(vi) .au, .ca, .de, .es, fi, .fr, .it, nl, etc. represents other countries (the co.uk syntax is an anomaly!).

(vii) .ac.uk is a UK-based university or other higher education institution (e.g. www.cranfield.ac.uk).

(viii) .org.uk is for an organization focusing on a single country (e.g. www.mencap.org.uk).

The 'filename.html' part of the web address refers to an individual web page, for example 'products.html' for a web page summarizing a company's products.

When a web address is typed in without a filename, for example www.bt.com, the browser automatically assumes the user is looking for the home page, which by convention is referred to as index.html.When creating sites, it is therefore vital to name the home page index.html (or an equivalent such as index.asp or index.php).

The file index.html can also be placed in sub-directories to ease access to information.

For example, to access a support page a customer would type www.bt.com/support rather than www.bt.com/support/index.htm. It is important that companies define a URL strategy which will help customers or partners find relevant parts of the site containing references to specific products or campaigns when printed in offline communications such as adverts or brochures.

There is further terminology associated with a URL which will often be required when discussing site implementation or digital marketing campaigns, as shown in the box ‘What’s in a URL?’.

What’s in a URL?

A great example of different URL components is provided by Google engineer Matt Cutts (Cutts, 2007). He gives this example:

http://video.google.co.uk:80/videoplay?docid=-7246927612831078230&hl=
en#00h02m30s

Here are some of the components of the URL:

- The *protocol* is http. Other protocols include https, ftp, etc.
- The *host* or *hostname* is video.google.co.uk.
- The *subdomain* is video.
- The *domain name* is google.co.uk.
- The *top-level domain or TLD* is uk (also known as gTLD). The uk domain is also referred to as a country-code top-level domain or ccTLD. For google.com, the TLD would be com.
- The *second-level domain* (SLD) is co.uk.
- The *port* is 80, which is the default port for web servers (not usually used in URLs, when it is the default although all web servers broadcast on ports).
- The *path* is /videoplay. Path typically refers to a file or location on the web server, e.g. /directory/file.html.
- An example of the URL parameter is docid and the value of that parameter is -7246927612831078230. These are often called the name, value pair. URLs often have lots of parameters. Parameters start with a question mark (?) and are separated with an ampersand (&).
- The *anchor* or fragment is ‘#00h02m30s’.

Domain name registration

Most companies are likely to own several domains, perhaps for different product lines or countries or for specific marketing campaigns. Domain name disputes can arise when an individual or company has registered a domain name which another company claims they have the right to. This is sometimes referred to as ‘cybersquatting’.

One of the best-known cases was brought in 1998 by Marks and Spencer and other highstreet retailers, since another company, ‘One In a Million Limited’, had registered names such as marks&spencer.com, britishtelecom.net and sainsbury.com. It then tried to sell these names for a profit. The companies already had sites with more familiar addresses such as marksandspencers.co.uk, but had not taken the precaution of registering all related domains with different forms of spelling and different top-level domains such as .net. Unsurprisingly, an injunction was issued against One in a Million which as a result was no longer able to use these names. The problem of companies’ names being misappropriated was common during the 1990s, but companies still need to be sure to register all related domain names for each brand since new top-level domain names are created through time such as .biz and .eu.

Managers or agencies responsible for web sites need to check that domain names are automatically renewed by the hosting company (as most are today). For example, the .co.uk domain must be renewed every two years. Companies that don’t manage this process potentially risk losing their domain name since another company could potentially register it if the domain name lapsed. A further option with domain registration is to purchase generic domain names of established sites which may perform well in the search engines.

Web presentation and data exchange standards

The information, graphics and interactive elements that make up the web pages of a site are collectively referred to as **content**. Different standards exist for text, graphics and multimedia. The saying ‘content is king’ is often applied to theWorldWideWeb, since the content will determine the experience of the customer and whether he or she will return to a web site in future.

HTML (Hypertext Markup Language) – display of unstructured text content

Web-page text has many of the formatting options available in a word processor. These include applying fonts, emphasis (bold, italic, underline) and placing information in tables. Formatting is possible since the web browser applies these formats according to instructions that are contained in the file that makes up the web page. This is usually written in **HTML** or **Hypertext Markup Language**. HTML is an international standard established by the World Wide Web Consortium (and published at www.w3.org) intended to ensure that any web page authored according to the definitions in the standard will appear the same in any web browser. Content management systems (CMS, *Chapter 12*) are used to shield business content editors from the complexity of HTML.

A brief example of HTML is given for a simplified home page for an example B2B company in *Figure 3.14*. The HTML code used to construct pages has codes or instruction tags such as <TITLE>. to indicate to the browser what is displayed. The <TITLE>. tag indicates what appears at the top of the web browser window. Each starting tag has a corresponding end tag usually marked by a '/', for example, <B>plastics</B> to embolden 'plastics'.

The simplicity of HTML compared to traditional programming languages makes it possible for simple web pages to be developed by non-specialists such as marketing assistants, particularly if templates for more complex parts of the page are provided. Interactive forms and brochures and online sales are more complex and usually require some programming expertise, although tools are available to simplify these. See detailed information on creating HTML pages (*Chapter 12*).

XML (eXtensible Markup Language) – display and exchange of structured text and data

While HTML has proved powerful in providing a standard method of displaying information that was easy to learn, it is largely presentational. HTML only had a limited capability for describing the data on web pages. A capability for summarizing the content of pages is an example of **meta-data**. 'Meta' is part of the ancient Greek language, and in an information management context can be summarized as providing a description or definition about a topic or item.

HTML also has a limited capability for describing documents through **HTML meta-tags**. These are presented at the start of the document in the header area. As the example below shows they can be used to specify a document's author, last update and type of content. This uses only some examples of meta-tags; the full definition and an introduction to HTML are available from theWorldWideWeb Consortium at www.w3.org/MarkUp.

One application of meta-tags and an illustration of meta-data is that they are used by search engines to identify the content of documents. Early search engines such as AltaVista ranked documents higher in their listings which had meta-keywords that corresponded to the words typed into the search engine by its user. This led to abuse by companies that might include the name of their competitor or repeat keywords several times in the meta-tags, a process known as 'search engine spamming'. As a result, most search engines now attach limited importance to the keyword meta-tags – in fact Google does not use them at all for ranking purposes, but may use them to identify unique documents. However, most search engines including Google do attach relevance to the <TITLE> tag, so it is important that this does not just contain a company name. For example, easyJet.com used the following title tag which incorporates the main phrases potential visitors may type into a search engine.

The limited capability within HTML for meta-data and data exchange has been acknowledged and, in an effort coordinated by the World Wide Web Consortium, the first **XML** or **eXtensible Markup Language** was produced in February 1998. This is not strictly a replacement for HTML since HTML and XML can coexist – they are both markup languages. To help developers use HTML and XML together a new standard, confusingly known as XHTML, was adopted. XHTML and XML are based on Standardized General Markup Language (SGML). The key word describing XML is 'extensible'. This means that new markup tags can be created that facilitate the searching and exchange of information. For example, product information on a web page could use the XML tags <NAME>, <DESCRIPTION>, <COLOUR> and <PRICE>. Example of tags relevant to a product catalogue are shown below.

```
<META name="keywords" content="phone directory, address
book">
<META name="description" content="An online phone book">
<META name="date" content="2005-11-06T08:49:37+00:00">
```

```
</HEAD>
```

Chapter 3 E-business infrastructure

```
<title>easyJet.com – easyjet low cost airline, easy jet, flight,
air fares, cheap flights</title>
```

XML or eXtensible
Markup Language
Standard for transferring
structured data, unlike
HTML which is purely
presentational.

Example XML for online marketplace catalogue

This example is a standard for publishing catalogue data. It can be seen that specific tags are used to identify:

□ □ Product ID
□ □ Manufacturer
□ □ Long and short description
□ □ Attributes of product and associated picture.

There is no pricing information in this example.

```
<CatalogData>
<Product>
<Action Value5"Delete"/>
```

An XML implementation typically consists of three parts: the XML document, a document type definition (DTD) and a stylesheet (XSL), which are usually stored as separate files.We need a simple example to understand how these relate. Let’s take the example of a bookstore cataloguing different books. You will see from this example that it is equivalent to using a database such as Microsoft Access to define database fields about the books and then storing and displaying their details.

The XML document contains the data items, in this case the books, and it references the DTD and XSL files:

Networking standards

Internet standards are important in that they are at the heart of definitions of the Internet. According to Leiner *et al*. (2000), on 24 October 1995 the Federal Networking Council unanimously passed a resolution defining the term‘Internet’.

How the Internet Works

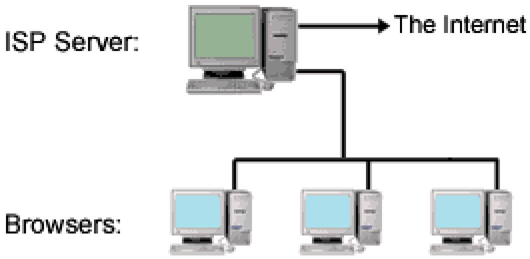
The internet is a world-wide network of computers linked together by telephone wires, satellite links and other means. For simplicity's sake we will say that all computers on the internet can be divided into two categories: *server*s and *browser*s.

Servers are where most of the information on the internet "lives". These are specialised computers which store information, share information with other servers, and make this information available to the general public.

Browsers are what people use to access the World Wide Web from any standard computer. Chances are, the browser you're using to view this page is either *Netscape Navigator/Communicator* or *Microsoft Internet Explorer*. These are by far the most popular browsers, but there are also a number of others in common use.

When you connect your computer to the internet, you are connecting to a special type of server which is provided and operated by your Internet Service Provider (ISP). The job of this "ISP Server" is to provide the link between your browser and the rest of the internet. A single ISP server handles the internet connections of many individual browsers - there may be thousands of other people connected to the same server that you are connected to right now.

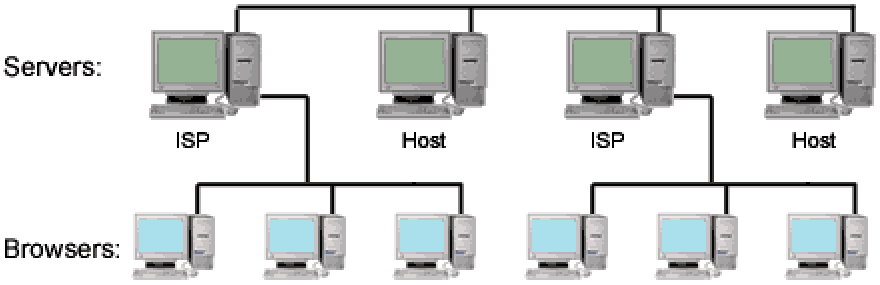
The following picture shows a small "slice" of the internet with several home computers connected to a server:



ISP servers receive requests from browsers to view webpages, check email, etc. Of course each server can't hold all the information from the entire internet, so in order to provide browsers with the pages and files they ask for, ISP servers must connect to other internet servers. This brings us to the next common type of server: the "Host Server".

Host servers are where websites "live". Every website in the world is located on a host server somewhere (for example, MediaCollege.Com is hosted on a server in Parsippany, New Jersy USA). The host server's job is to store information and make it available to other servers.

The picture below show a slightly larger slice of the internet:



To view a web page from your browser, the following sequence happens:

1. You either type an address (URL) into your "Address Bar" or click on a hyperlink.
2. Your browser sends a request to your ISP server asking for the page.
3. Your ISP server looks in a huge database of internet addresses and finds the exact host server which houses the website in question, then sends that host server a request for the page.
4. The host server sends the requested page to your ISP server.
5. Your ISP sends the page to your browser and you see it displayed on your screen.

Introduction

How does the Internet work? Good question! The Internet's growth has become explosive and it seems impossible to escape the bombardment of *www.com*'s seen constantly on television, heard on radio, and seen in magazines. Because the Internet has become such a large part of our lives, a good understanding is needed to use this new tool most effectively.

This whitepaper explains the underlying infrastructure and technologies that make the Internet work. It does not go into great depth, but covers enough of each area to give a basic understanding of the concepts involved. For any unanswered questions, a list of resources is provided at the end of the paper. Any comments, suggestions, questions, etc. are encouraged and may be directed to the author at the email address given above.

Where to Begin? Internet Addresses

Because the Internet is a global network of computers each computer connected to the Internet **must** have a unique address. Internet addresses are in the form **nnn.nnn.nnn.nnn** where nnn must be a number from 0 - 255. This address is known as an IP address. (IP stands for Internet Protocol; more on this later.)

The picture below illustrates two computers connected to the Internet; your computer with IP address 1.2.3.4 and another computer with IP address 5.6.7.8. The Internet is represented as an abstract object in-between. (As this paper progresses, the Internet portion of Diagram 1 will be explained and redrawn several times as the details of the Internet are exposed.)

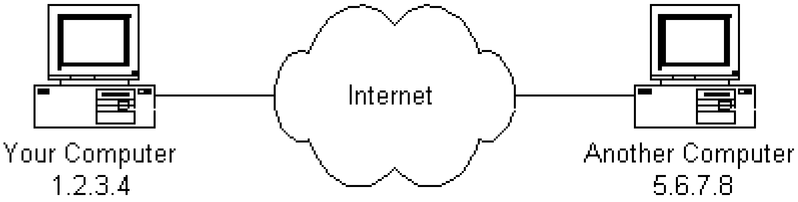


Diagram 1

If you connect to the Internet through an Internet Service Provider (ISP), you are usually assigned a temporary IP address for the duration of your dial-in session. If you connect to the Internet from a local area network (LAN) your computer might have a permanent IP address or it might obtain a temporary one from a DHCP (Dynamic Host Configuration Protocol) server. In any case, if you are connected to the Internet, your computer has a unique IP address.

Check It Out - The Ping Program

If you're using Microsoft Windows or a flavor of Unix and have a connection to the Internet, there is a handy program to see if a computer on the Internet is alive. It's called **ping**, probably after the sound made by older submarine sonar systems.[1] If you are using Windows, start a command prompt window. If you're using a flavor of Unix, get to a command prompt. Type `ping www.yahoo.com`. The ping program will send a 'ping' (actually an ICMP (Internet Control Message Protocol) echo request message) to the named computer. The pinged computer will respond with a reply. The ping program will count the time expired until the reply comes back (if it does). Also, if you enter a domain name (i.e. www.yahoo.com) instead of an IP address, ping will resolve the domain name and display the computer's IP address. More on domain names and address resolution later.

Protocol Stacks and Packets

So your computer is connected to the Internet and has a unique address. How does it 'talk' to other computers connected to the Internet? An example should serve here: Let's say your IP address is 1.2.3.4 and you want to send a message to the computer 5.6.7.8. The message you want to send is "Hello computer 5.6.7.8!". Obviously, the message must be transmitted over whatever kind of wire connects your computer to the Internet. Let's say you've dialed into your ISP from home and the message must be transmitted over the phone line. Therefore the message must be translated from alphabetic text into electronic signals, transmitted over the Internet, then translated back into alphabetic text. How is this accomplished? Through the use of a **protocol stack**. Every computer needs one to communicate on the Internet and it is usually built into the computer's operating system (i.e. Windows, Unix, etc.). The protocol stack used on the Internet is referred to as the TCP/IP protocol stack because of the two major communication protocols used. The TCP/IP stack looks like this:

Protocol Layer	**Comments**
Application Protocols Layer	Protocols specific to applications such as WWW, e-mail, FTP, etc.
Transmission Control Protocol Layer	TCP directs packets to a specific application on a computer using a port number.
Internet Protocol Layer	IP directs packets to a specific computer using an IP address.
Hardware Layer	Converts binary packet data to network signals and back. (E.g. ethernet network card, modem for phone lines, etc.)

If we were to follow the path that the message "Hello computer 5.6.7.8!" took from our computer to the computer with IP address 5.6.7.8, it would happen something like this:

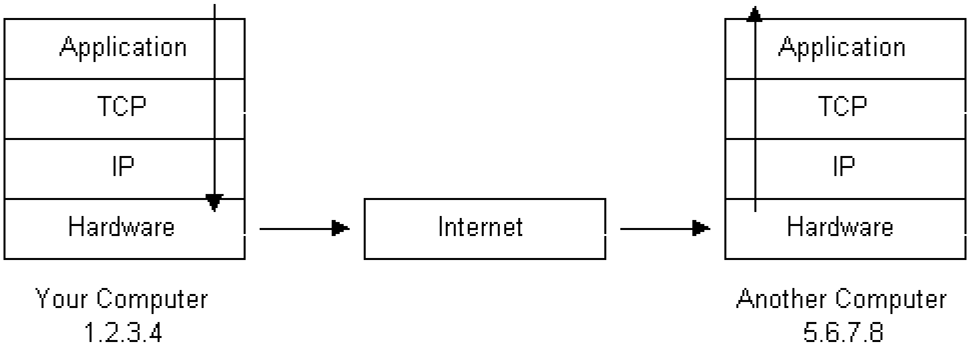


Diagram 2

1. The message would start at the top of the protocol stack on your computer and work it's way downward.
2. If the message to be sent is long, each stack layer that the message passes through may break the message up into smaller chunks of data. This is because data sent over the Internet (and most computer networks) are sent in manageable chunks. On the Internet, these chunks of data are known as **packets**.
3. The packets would go through the Application Layer and continue to the TCP layer. Each packet is assigned a **port number**. Ports will be explained later, but suffice to say that many programs may be using the TCP/IP stack and sending messages. We need to know which program on the

destination computer needs to receive the message because it will be listening on a specific port.

4. After going through the TCP layer, the packets proceed to the IP layer. This is where each packet receives it's destination address, 5.6.7.8.
5. Now that our message packets have a port number and an IP address, they are ready to be sent over the Internet. The hardware layer takes care of turning our packets containing the alphabetic text of our message into electronic signals and transmitting them over the phone line.
6. On the other end of the phone line your ISP has a direct connection to the Internet. The ISPs **router** examines the destination address in each packet and determines where to send it. Often, the packet's next stop is another router. More on routers and Internet infrastructure later.
7. Eventually, the packets reach computer 5.6.7.8. Here, the packets start at the bottom of the destination computer's TCP/IP stack and work upwards.
8. As the packets go upwards through the stack, all routing data that the sending computer's stack added (such as IP address and port number) is stripped from the packets.
9. When the data reaches the top of the stack, the packets have been re-assembled into their original form, "Hello computer 5.6.7.8!"

Networking Infrastructure

So now you know how packets travel from one computer to another over the Internet. But what's in-between? What actually makes up the Internet? Let's look at another diagram:

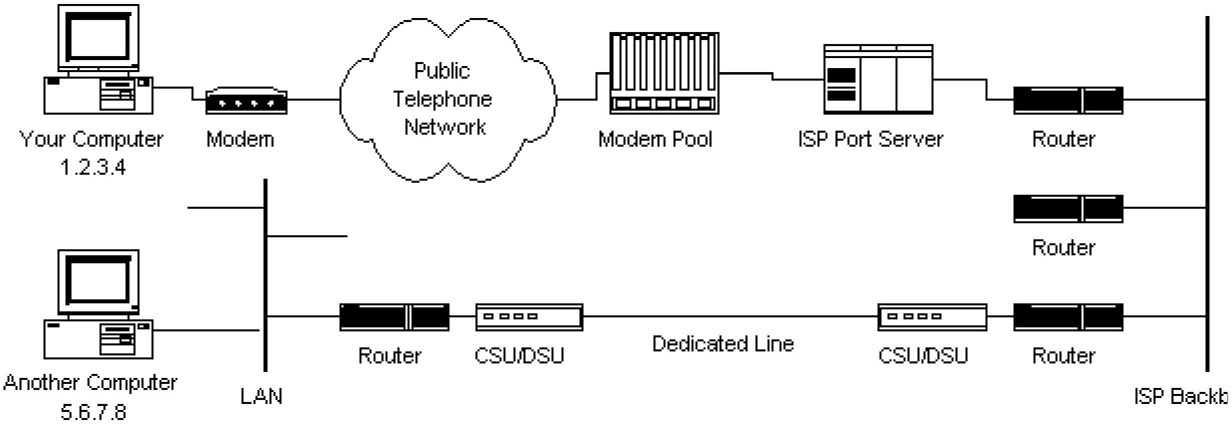


Diagram 3

Here we see Diagram 1 redrawn with more detail. The physical connection through the phone network to the Internet Service Provider might have been easy to guess, but beyond that might bear some explanation.

The ISP maintains a pool of modems for their dial-in customers. This is managed by some form of computer (usually a dedicated one) which controls data flow from the modem pool to a backbone or dedicated line router. This setup may be referred to as a port server, as it 'serves' access to the network. Billing and usage information is usually collected here as well.

After your packets traverse the phone network and your ISP's local equipment, they are routed onto the ISP's backbone or a backbone the ISP buys bandwidth from. From here the packets will usually journey through several routers and over several backbones, dedicated lines, and other networks until they find their destination, the computer with address 5.6.7.8. But wouldn't it would be nice if we knew the exact route our packets were taking over the Internet? As it turns out, there is a way...

Check It Out - The Traceroute Program

If you're using Microsoft Windows or a flavor of Unix and have a connection to the Internet, here is another handy Internet program. This one is called **traceroute** and it shows the path your packets are taking to a given Internet destination. Like ping, you must use traceroute from a command prompt. In Windows, use `tracert www.yahoo.com`. From a Unix prompt, type `traceroute www.yahoo.com`. Like ping, you may also enter IP addresses instead of domain names. Traceroute will print out a list of all the routers, computers, and any other Internet entities that your packets must travel through to get to their destination.

If you use traceroute, you'll notice that your packets must travel through many things to get to their destination. Most have long names such as sjc2-core1-h2-0-0.atlas.digex.net and fddi0-0.br4.SJC.globalcenter.net. These are Internet routers that decide where to send your packets. Several routers are shown in Diagram 3, but only a few. Diagram 3 is meant to show a simple network structure. The Internet is much more complex.

Internet Infrastructure

The Internet backbone is made up of many large networks which interconnect with each other. These large networks are known as **Network Service Providers** or **NSP**s. Some of the large NSPs are UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet, as well as others. These networks **peer** with each other to exchange packet traffic. Each NSP is required to connect to three **Network Access Points** or **NAP**s. At the NAPs, packet traffic may jump from one NSP's backbone to another NSP's backbone. NSPs also interconnect at **Metropolitan Area Exchanges** or **MAE**s. MAEs serve the same purpose as the NAPs but are privately owned. NAPs were the original Internet interconnect points. Both NAPs and MAEs are referred to as Internet Exchange Points or **IX**s. NSPs also sell bandwidth to smaller networks, such as ISPs and smaller bandwidth providers. Below is a picture showing this hierarchical infrastructure.

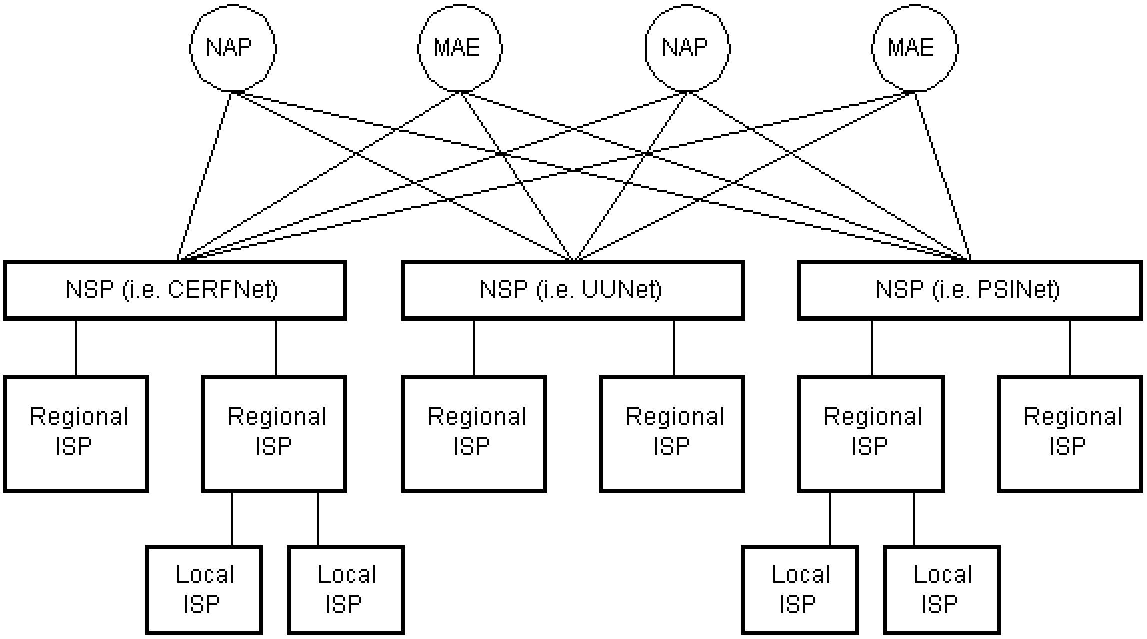


Diagram 4

This is not a true representation of an actual piece of the Internet. Diagram 4 is only meant to demonstrate how the NSPs could interconnect with each other and smaller ISPs. None of the physical network components are shown in Diagram 4 as they are in Diagram 3. This is because a single NSP's backbone infrastructure is a complex drawing by itself. Most NSPs publish maps of their network infrastructure on their web sites and can be found easily. To draw an actual map of the Internet would be nearly impossible due to it's size, complexity, and ever changing structure.

The Internet Routing Hierarchy

So how do packets find their way across the Internet? Does every computer connected to the Internet know where the other computers are? Do packets simply get 'broadcast' to every computer on the Internet? The answer to both the preceding questions is 'no'. No computer knows where any of the other computers are, and packets do not get sent to every computer. The information used to get packets to their destinations are contained in routing tables kept by each router connected to the Internet.

Routers are packet switches. A router is usually connected between networks to route packets between them. Each router knows about it's sub-networks and which IP addresses they use. The router usually doesn't know what IP addresses are 'above' it. Examine Diagram 5 below. The black boxes connecting the backbones are routers. The larger NSP backbones at the top are connected at a NAP. Under them are several sub-networks, and under them, more sub-networks. At the bottom are two local area networks with computers attached.

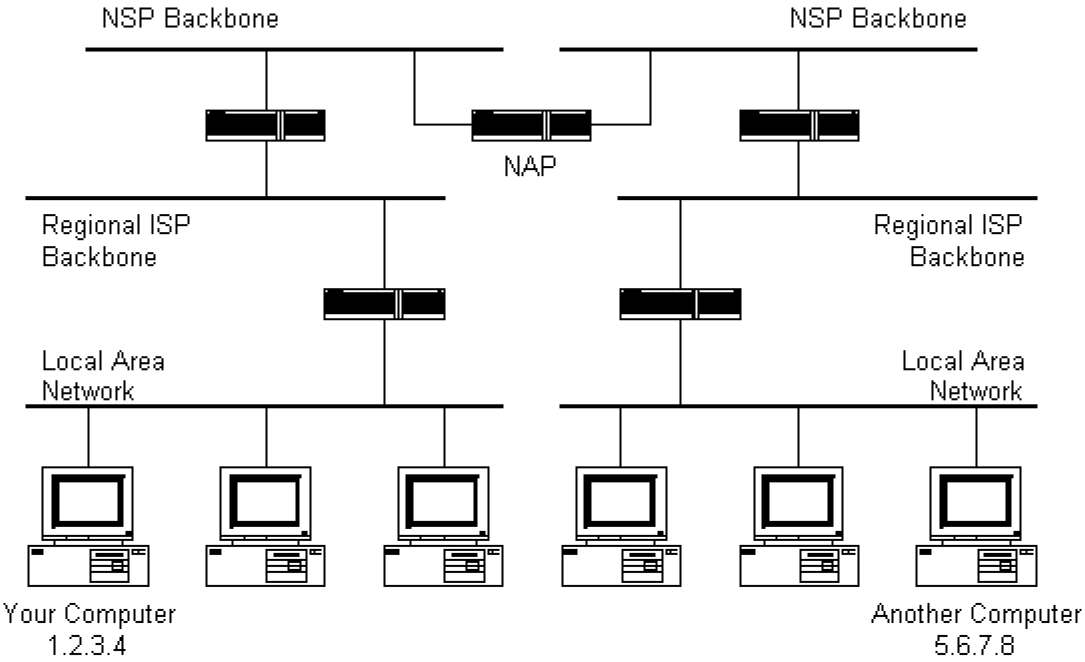


Diagram 5

When a packet arrives at a router, the router examines the IP address put there by the IP protocol layer on the originating computer. The router checks it's routing table. If the network containing the IP address is found, the packet is sent to that network. If the network containing the IP address is not found, then the router sends the packet on a default route, usually up the backbone hierarchy to the next router. Hopefully the next router will know where to send the packet. If it does not, again the packet is routed upwards until it reaches a NSP backbone. The routers connected to the NSP backbones hold the largest routing tables and here the packet will be routed to the correct backbone, where it will begin its journey 'downward' through smaller and smaller networks until it finds it's destination.

Domain Names and Address Resolution

But what if you don't know the IP address of the computer you want to connect to? What if the you need to access a web server referred to as *www.anothercomputer.com*? How does your web browser know where on the Internet this computer lives? The answer to all these questions is the **Domain Name Service** or **DNS**. The DNS is a distributed database which keeps track of computer's names and their corresponding IP addresses on the Internet.

Many computers connected to the Internet host part of the DNS database and the software that allows others to access it. These computers are known as DNS servers. No DNS server contains the entire database; they only contain a subset of it. If a DNS server does not contain the domain name requested by another computer, the DNS server re-directs the requesting computer to another DNS server.

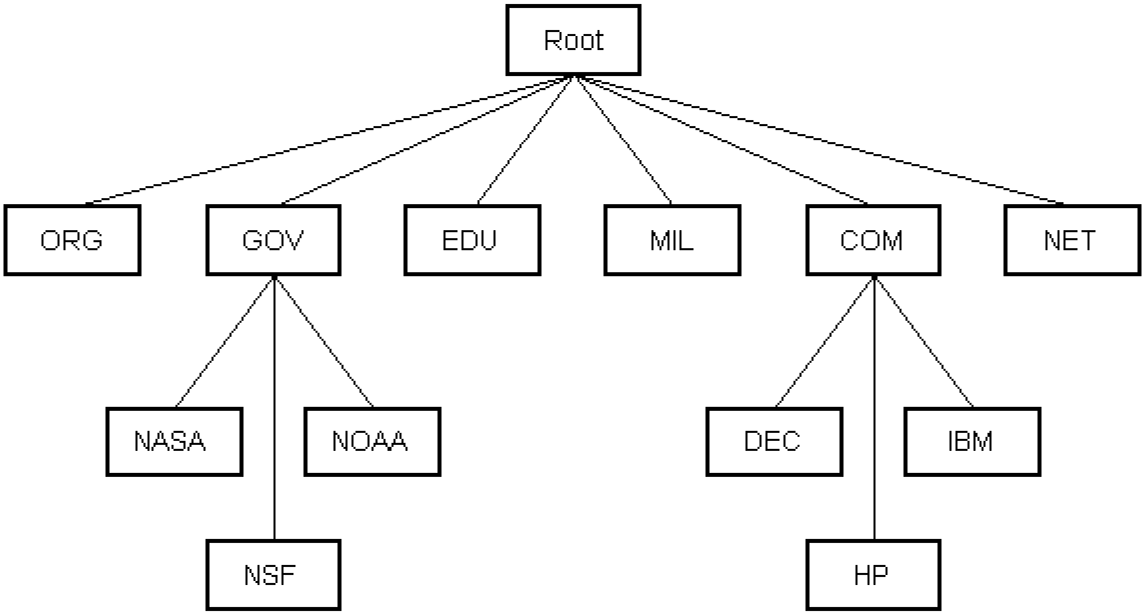


Diagram 6

The Domain Name Service is structured as a hierarchy similar to the IP routing hierarchy. The computer requesting a name resolution will be re-directed 'up' the hierarchy until a DNS server is found that can resolve the domain name in the request. Figure 6 illustrates a portion of the hierarchy. At the top of the tree are the domain roots. Some of the older, more common domains are seen near the top. What is not shown are the multitude of DNS servers around the world which form the rest of the hierarchy.

When an Internet connection is setup (e.g. for a LAN or Dial-Up Networking in Windows), one primary and one or more secondary DNS servers are usually specified as part of the installation. This way, any Internet applications that need domain name resolution will be able to function correctly. For example, when you enter a web address into your web browser, the browser first connects to your primary DNS server. After obtaining the IP address for the domain name you entered, the browser then connects to the target computer and requests the web page you wanted.

Check It Out - Disable DNS in Windows

If you're using Windows 95/NT and access the Internet, you may view your DNS server(s) and even disable them.

If you use Dial-Up Networking:
Open your Dial-Up Networking window (which can be found in Windows Explorer under your CD-ROM drive and above Network Neighborhood). Right click on your Internet connection and click Properties. Near the bottom of the connection properties window press the TCP/IP Settings... button.

If you have a permanent connection to the Internet:
Right click on Network Neighborhood and click Properties. Click TCP/IP Properties. Select the DNS Configuration tab at the top.

You should now be looking at your DNS servers' IP addresses. Here you may disable DNS or set your DNS servers to 0.0.0.0. (Write down your DNS servers' IP addresses first. You will probably have to restart Windows as well.) Now enter an address into your web browser. The browser won't be able to resolve the domain name and you will probably get a nasty dialog box explaining that a DNS server couldn't be found. However, if you enter the corresponding IP address instead of the domain name, the browser will be able to retrieve the desired web page. (Use ping to get the IP address prior to disabling DNS.) Other Microsoft operating systems are similar.

Internet Protocols Revisited

As hinted to earlier in the section about protocol stacks, one may surmise that there are many protocols that are used on the Internet. This is true; there are many communication protocols required for the Internet to function. These include the TCP and IP protocols, routing protocols, medium access control protocols, application level protocols, etc. The following sections describe some of the more important and commonly used protocols on the Internet. Higher level protocols are discussed first, followed by lower level protocols.

Application Protocols: HTTP and the World Wide Web

One of the most commonly used services on the Internet is the World Wide Web (WWW). The application protocol that makes the web work is **Hypertext Transfer Protocol** or **HTTP**. Do not confuse this with the Hypertext Markup Language (HTML). HTML is the language used to write web pages. HTTP is the protocol that web browsers and web servers use to communicate with each other over the Internet. It is an application level protocol because it sits on top of the TCP layer in the protocol stack and is used by specific applications to talk to one another. In this case the applications are web browsers and web servers.

HTTP is a connectionless text based protocol. Clients (web browsers) send requests to web servers for web elements such as web pages and images. After the request is serviced by a server, the connection between client and server across the Internet is disconnected. A new connection must be made for each request. Most protocols are connection oriented. This means that the two computers communicating with each other keep the connection open over the Internet. HTTP does not however. Before an HTTP request can be made by a client, a new connection must be made to the server.

When you type a URL into a web browser, this is what happens:

1. If the URL contains a domain name, the browser first connects to a domain name server and retrieves the corresponding IP address for the web server.
2. The web browser connects to the web server and sends an HTTP request (via the protocol stack) for the desired web page.
3. The web server receives the request and checks for the desired page. If the page exists, the web server sends it. If the server cannot find the requested page, it will send an HTTP 404 error message. (404 means 'Page Not Found' as anyone who has surfed the web probably knows.)
4. The web browser receives the page back and the connection is closed.
5. The browser then parses through the page and looks for other page elements it needs to complete the web page. These usually include images, applets, etc.
6. For each element needed, the browser makes additional connections and HTTP requests to the server for each element.
7. When the browser has finished loading all images, applets, etc. the page will be completely loaded in the browser window.

Check It Out - Use Your Telnet Client to Retrieve a Web Page Using HTTP

Telnet is a remote terminal service used on the Internet. It's use has declined lately, but it is a very useful tool to study the Internet. In Windows find the default telnet program. It may be located in the Windows directory named telnet.exe. When opened, pull down the Terminal menu and select Preferences. In the preferences window, check Local Echo. (This is so you can see your HTTP request when you type it.) Now pull down the Connection menu and select Remote System. Enter www.google.com for the Host Name and 80 for the Port. (Web servers usually listen on port 80 by default.) Press Connect. Now type

```
GET / HTTP/1.0
```

and press Enter twice. This is a simple HTTP request to a web server for it's root page. You should see a web page flash by and then a dialog box should pop up to tell you the connection was lost. If you'd like to save the retrieved page, turn on logging in the Telnet program. You may then browse through the web page and see the HTML that was used to write it.

Most Internet protocols are specified by Internet documents known as a **Request For Comments** or **RFC**s. RFCs may be found at several locations on the Internet. See the Resources section below for appropriate URL's. HTTP version 1.0 is specified by RFC 1945.

Application Protocols: SMTP and Electronic Mail

Another commonly used Internet service is electronic mail. E-mail uses an application level protocol called **Simple Mail Transfer Protocol** or **SMTP**. SMTP is also a text based protocol, but unlike HTTP, SMTP is connection oriented. SMTP is also more complicated than HTTP. There are many more commands and considerations in SMTP than there are in HTTP.

When you open your mail client to read your e-mail, this is what typically happens:

1. The mail client (Netscape Mail, Lotus Notes, Microsoft Outlook, etc.) opens a connection to it's default mail server. The mail server's IP address or domain name is typically setup when the mail client is installed.
2. The mail server will always transmit the first message to identify itself.
3. The client will send an SMTP HELO command to which the server will respond with a 250 OK message.

4. Depending on whether the client is checking mail, sending mail, etc. the appropriate SMTP commands will be sent to the server, which will respond accordingly.
5. This request/response transaction will continue until the client sends an SMTP QUIT command. The server will then say goodbye and the connection will be closed.

A simple 'conversation' between an SMTP client and SMTP server is shown below. **R:** denotes messages sent by the server (receiver) and **S:** denotes messages sent by the client (sender).

```
This SMTP example shows mail sent by Smith at host USC-ISIF, to
Jones, Green, and Brown at host BBN-UNIX.  Here we assume that
host USC-ISIF contacts host BBN-UNIX directly.  The mail is
accepted for Jones and Brown.  Green does not have a mailbox at
host BBN-UNIX.

-------------------------------------------------------------

   R: 220 BBN-UNIX.ARPA Simple Mail Transfer Service Ready
   S: HELO USC-ISIF.ARPA
   R: 250 BBN-UNIX.ARPA

   S: MAIL FROM:<Smith@USC-ISIF.ARPA>
   R: 250 OK

   S: RCPT TO:<Jones@BBN-UNIX.ARPA>
   R: 250 OK

   S: RCPT TO:<Green@BBN-UNIX.ARPA>
   R: 550 No such user here

   S: RCPT TO:<Brown@BBN-UNIX.ARPA>
   R: 250 OK

   S: DATA
   R: 354 Start mail input; end with <CRLF>.<CRLF>
   S: Blah blah blah...
   S: ...etc. etc. etc.
   S: .
   R: 250 OK

   S: QUIT
   R: 221 BBN-UNIX.ARPA Service closing transmission channel
```

This SMTP transaction is taken from RFC 821, which specifies SMTP.

Transmission Control Protocol

Under the application layer in the protocol stack is the TCP layer. When applications open a connection to another computer on the Internet, the messages they send (using a specific application layer protocol) get passed down the stack to the TCP layer. **TCP is responsible for routing application protocols to the correct application on the destination computer**. To accomplish this, port numbers are used. Ports can be thought of as separate channels on each computer. For example, you can surf the web while reading e-mail. This is because these two applications (the web browser and the mail client) used different port numbers. When a packet arrives at a computer and makes its way up the protocol stack, the TCP layer decides which application receives the packet based on a port number.

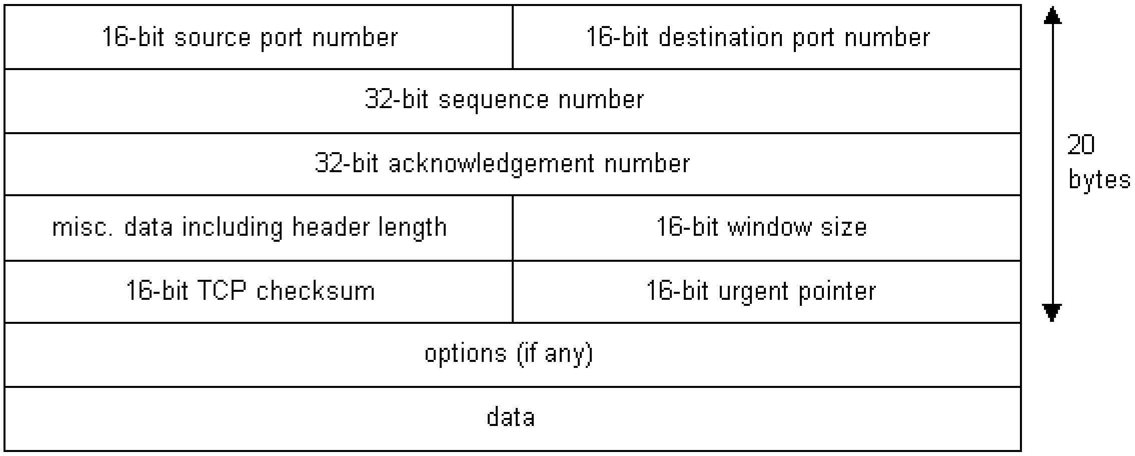
TCP works like this:

- When the TCP layer receives the application layer protocol data from above, it segments it into manageable 'chunks' and then adds a TCP header with specific TCP information to each 'chunk'. The information contained in the TCP header includes the port number of the application the data needs to be sent to.

- When the TCP layer receives a packet from the IP layer below it, the TCP layer strips the TCP header data from the packet, does some data reconstruction if necessary, and then sends the data to the correct application using the port number taken from the TCP header.

This is how TCP routes the data moving through the protocol stack to the correct application.

TCP is not a textual protocol. **TCP is a connection-oriented, reliable, byte stream service**. Connection-oriented means that two applications using TCP must first establish a connection before exchanging data. TCP is reliable because for each packet received, an acknowledgement is sent to the sender to confirm the delivery. TCP also includes a checksum in it's header for error-checking the received data. The TCP header looks like this:



16-bit source port number	16-bit destination port number
32-bit sequence number	
32-bit acknowledgement number	
misc. data including header length	16-bit window size
16-bit TCP checksum	16-bit urgent pointer
options (if any)	
data	

Diagram 7

Notice that there is no place for an IP address in the TCP header. This is because TCP doesn't know anything about IP addresses. TCP's job is to get application level data from application to application reliably. The task of getting data from computer to computer is the job of IP.

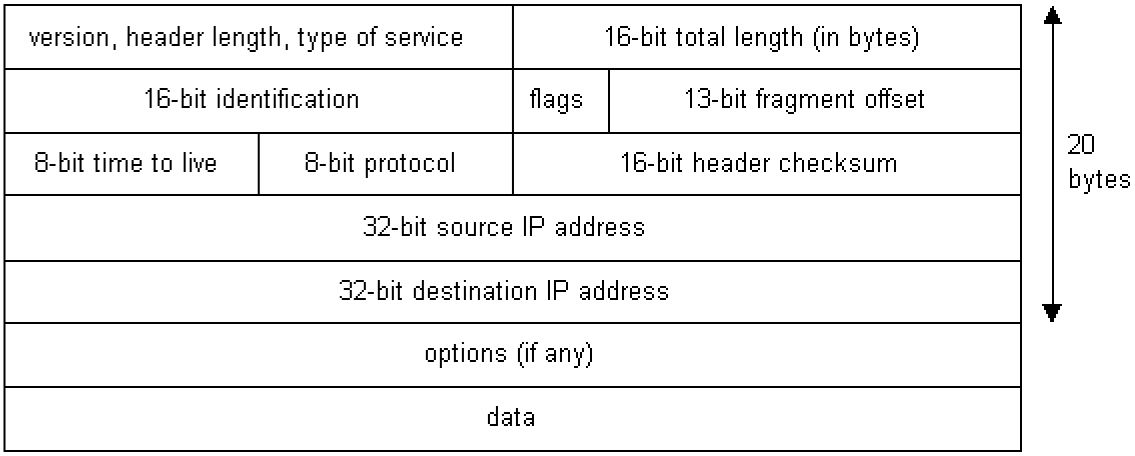
Check It Out - Well Known Internet Port Numbers

Listed below are the port numbers for some of the more commonly used Internet services.

FTP	20/21
Telnet	23
SMTP	25
HTTP	80
Quake III Arena	27960

Internet Protocol

Unlike TCP, **IP is an unreliable, connectionless protocol**. IP doesn't care whether a packet gets to it's destination or not. Nor does IP know about connections and port numbers. **IP's job is too send and route packets to other computers**. IP packets are independent entities and may arrive out of order or not at all. It is TCP's job to make sure packets arrive and are in the correct order. About the only thing IP has in common with TCP is the way it receives data and adds it's own IP header information to the TCP data. The IP header looks like this:



<table>
<tr><td colspan="2">version, header length, type of service</td><td colspan="2">16-bit total length (in bytes)</td></tr>
<tr><td colspan="2">16-bit identification</td><td>flags</td><td>13-bit fragment offset</td></tr>
<tr><td>8-bit time to live</td><td>8-bit protocol</td><td colspan="2">16-bit header checksum</td></tr>
<tr><td colspan="4">32-bit source IP address</td></tr>
<tr><td colspan="4">32-bit destination IP address</td></tr>
<tr><td colspan="4">options (if any)</td></tr>
<tr><td colspan="4">data</td></tr>
</table>

Diagram 8

Above we see the IP addresses of the sending and receiving computers in the IP header. Below is what a packet looks like after passing through the application layer, TCP layer, and IP layer. The application layer data is segmented in the TCP layer, the TCP header is added, the packet continues to the IP layer, the IP header is added, and then the packet is transmitted across the Internet.

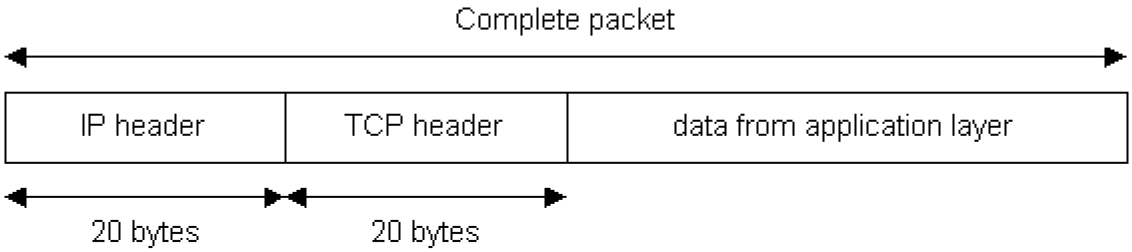


Diagram 9

Wrap Up

Now you know how the Internet works. But how long will it stay this way? The version of IP currently used on the Internet (version 4) only allows 2^{32} addresses. Eventually there won't be any free IP addresses left. Surprised? Don't worry. IP version 6 is being tested right now on a research backbone by a consortium of research institutions and corporations. And after that? Who knows. The Internet has come a long way since it's inception as a Defense Department research project. No one really knows what the Internet will become. One thing is sure, however. The Internet will unite the world like no other mechanism ever has. The Information Age is in full stride and I am glad to be a part of it.

REQUIREMENTS FOR INTERNET

The basic requirements for connecting the computer system to the internet can be classified into two categories:

- Hardware Requirement

- Software Requirement

Hardware Requirements Users can use any of the PC models coming today e.g. Intel Celeron, Intel P-I, Intel P-II , Intel P-III, Intel P-IV, AMD K6, CYRIX MII, etc. The CPU of 350 MHz and above gives a good performance.

Your computer should have atleast of 16 MB RAM to have good navigation on the net. The AGP card should have at least 4 MB RAM. This helps in watching the graphics/movies on the Internet effectively.

One should have a telephone line or ISDN (Integrated Services Digital Network) connection. ISDN connection has more bandwidth as compared to a single telephone line. A modem is also required. Modem stands for modulator / demodulator. The computer operates on digital signals, whereas the telephone lines operate on analog signals. So an additional piece of hardware, i.e., modem is connected between the computer and the telephone line. Modem converts the digital signals to analog and vice versa. Modems are inbuilt or they can be connected externally. The good modems available in the market are from the companies US ROBOTICS, D-Link etc. A modem can be an ordinary modem or a fax/voice modem. The fax/voice modem in addition to data, can also carry, voice on the net.

Software Requirements

We should have connecting software and web browser software. Internet can be called upon from any operating system e.g. Windows 98, Windows NT, Linux, Unix, etc. The two most widely used web browsers are Internet explorer and Netscape communicator.

After having the basic requirements the additional requirements that are required for smooth and quality service of internet, the following software are required:

- Anti-Virus

- Anti-Worm

- Firewall

- System Utilities

- Download Accelerator or Getright like software
- Compression and Uncompressing utilities

- Adobe Acrobat Reader

- Macromedia Flash

- E-mail configuring software like MS Outlook

- Web Messenger etc.

Internet standards:

Network Protocols and Standards, that is what I will be describing in this article. First we define *protocol*, which is synonymous with "rule". Then we discuss standards, which are agreed-upon rules.

Protocols

In computer networks, communication occurs between entities in different systems. An **entity** is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a **protocol.**

A **protocol** is a set of rules that governs data communication. A protocol defines what is communicated, how it is communicated and what is communicated. The Key elements of a protocol are syntax, semantics and timing.

- **Syntax.** Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to the address of the receiver, and the rest of the stream to the message itself.
- **Semantics**. Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** Timing refers to two characteristics: when data should be sent and how fast it can be sent. For example, if a sender produces data at 100 Megabits per second (Mbps) but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and also in guaranteeing national and international interoperability of data and telecommunications technology and processes. They provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication.
Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" and "by regulation").

- **De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.** De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology.
- **De jure. De jure standards** are those that have been legislated by an oficially recognized body.

Standards and Organizations

standards are developed through cooperation of standards creation committees, forums and government regulatory agencies. Some of the standards establishment Organizations are:

- International Standards Organisation (ISO) http://www.iso.org/
- International Telecommuniations Union-Telecommunication Standards Sector (ITU-T). http://www.itu.int/ITU-T
- American National Standard Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE). http://www.ieee.gov/
- Electronic Industries Association (EIA).

Forums

Telecommunications technology development is moving faster than the ability of standards committee to ratify standards. Standards committees are procedural bodies and by nature slow moving. to accommodate the need fro working models and agreements and to facilitate the standardization process, many special-interest groups have developed *forums* made up of representatives from interested corporations. The forums work with universities and users to test, evaluate and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following:

- **Frame Relay Forum.** The Frame Relay Forum was formed by digital equipment Corporation, Northern Telecom, Cisco, and StrataCom to promote the acceptance and implementation of frame relay. Today, it has around 40 members representing North America, Europe, and the Pacific rim. Issues under Review include flow control. encapsulation, translation, and multicasting. the forum's results are submitted to the ISO.
- **ATM Forum. http://www.atmforum.com/** The ATM Forum provides acceptance and use of Asynchronous Transfer Mode (ATM) technology. The ATM Forum is made up of Customer Premises Equipment (e.g., PBX systems) vendors and Central Office (e.g., telephone exchange) providers. It is concerned with the standardization of service to ensure interoperability.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as Federal Communication Commission in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.

- **Federal Communications Commission (FCC). http://www.fcc.gov/** The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications.

An **Internet Standard** is as thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC).** Each RFC is edited, assigned a number, and made available to all interested parties.

RFCs go through maturity levels and are categorized according to their requirement level.

Maturity Levels

An RFC, during its lifetime, falls into one of six **maturity levels:** proposed standard, draft standard, Internet standard, historic, experimental, and Informational.

- **Proposed Standard.** A proposed standard is a specification that is stable, well understood, and of sufficient interest to the internet community**.** At this level, the specification is usually tested and implemented by several different programs.
- **Draft Standard.** A proposed standard is elevated to draft standard status after atleast two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an internet standard.
- **Internet Standard.** A draft standard reaches Internet standard after demonstrations of successful implementation.
- **Historic.** The Historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an internet standard.
- **Experimental.** An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the internet. Such an RFC should not be implemented in any functional Internet service.
- **Informational.** An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.

RFC Requirement Levels

RFCs are classified into 5 Requirement Levels: required, recommended, elective, limited use and not recommended.

- **Required**. An RFC is labeled *required* if it must be implemented by all Internet systems to achieve minimum conformance. For example, IP and ICMP are required protocols.
- **Recommended**. An RFC labeled *recommended* is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET are recommended protocols.
- **Elective**. An RFC labeled *elective* is not required and not recommended. However, a system can use it for its own benefit.
- **Limited Use**. An RFC labeled *limited use* should be used only in limited situations. Most of the experimental RFCs fall under this category.
- **Not recommended**. An RFC labeled *not recommended* is inappropriate for general use. Normally a historic (obsolete) RFC may fall under this category.

Internet Standards

The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards. There are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards.

The Internet Standards Process described in this document is concerned with all protocols, procedures, and conventions that are used in or by the Internet, whether or not they are part of the TCP/IP protocol suite. In the case of protocols developed and/or standardized by non-Internet organizations, however, the Internet Standards Process normally applies to the application of the protocol or procedure in the Internet context, not to the specification of the protocol itself.

In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

The Internet Standards Process

In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body (see below), and is published.
In practice, the process is more complicated, due to
(1) the difficulty of creating specifications of high technical quality;
(2) the need to consider the interests of all of the affected parties;
(3) the importance of establishing widespread community consensus; and
(4) the difficulty of evaluating the utility of a particular specification for the Internet community.

The goals of the Internet Standards Process are:
o technical excellence;
o prior implementation and testing;
o clear, concise, and easily understood documentation;
o openness and fairness; and
o timeliness.

The following organizations are involved in the Internet standards process.

* IETF

The Internet Engineering Task Force (IETF) is a loosely self- organized group of people who make technical and other contributions to the engineering and evolution of the Internet and its technologies. It is the principal body engaged in the development of new Internet Standard specifications, although it is not itself a part of the Internet Society. The IETF is composed of individual Working Groups, which are grouped into Areas, each of which is coordinated by one or more Area Directors. Nominations to the Internet Architecture Board and the Internet Engineering Steering Group are made by a nominating committee selected at random from the ranks of regular IETF meeting attendees who have volunteered to serve as nominating committee members.

- ISOC

Internet standardization is an organized activity of the Internet Society (ISOC). The ISOC is a professional society that is concerned with the growth and evolution of the worldwide Internet, with the way in which the Internet is and can be used, and with the social, political, and technical issues that arise as a result. The ISOC Board of Trustees is responsible for approving appointments to the Internet Architecture Board from among the nominees submitted by the IETF nominating committee.

- IESG

The Internet Engineering Steering Group (IESG) is responsible for technical management of IETF activities and the Internet Standards process. As part of the Internet Society, it administers the Internet Standards process according to the rules and procedures given in this document, which have been accepted and ratified by the Internet Society Trustees. The IESG is directly responsible for the actions associated with entry into and movement along the "standards track", as described in section 3 of this document, including final approval of specifications as Internet Standards. The IESG is composed of the IETF Area Directors and the chairperson of the IETF, who also serves as the chairperson of the IESG.

- IAB

The Internet Architecture Board (IAB) is a technical advisory group of the Internet Society. It is chartered by the Internet Society Trustees to provide oversight of the architecture of the Internet and its protocols, and to serve in the context of the Internet Standards process as a body to which the decisions of the IESG may be appealed (as described in section 3.6 of this document). The IAB is responsible for approving appointments to the IESG from among the nominees submitted by the IETF nominating committee.

1.3 Standards-Related Publications

1.3.1 Requests for Comments (RFCs)

Each distinct version of a specification is published as part of the "Request for Comments" (RFC) document series. This archival series is the official publication channel for Internet standards documents and other publications of the IESG, IAB, and Internet community. RFCs are available for anonymous FTP from a number of Internet hosts.

The RFC series of documents on networking began in 1969 as part of the original ARPA wide-area networking (ARPANET) project to status memos about the Internet. RFC publication is the direct responsibility of the RFC Editor, under the general direction of the IAB.

Every RFC is available in ASCII text, but some RFCs are also available in PostScript. The PostScript version of an RFC may contain material (such as diagrams and figures) that is not present in the ASCII version, and it may be formatted differently.

```
*********************************************************
*  A stricter requirement applies to standards-track    *
*  specifications: the ASCII text version is the        *
*  definitive reference, and therefore it must be a     *
*  complete and accurate specification of the standard, *
*  including all necessary diagrams and illustrations.  *
*                                                       *
********************************************************
```

The status of Internet protocol and service specifications is summarized periodically in an RFC entitled "Internet Official Protocol Standards" [1]. This RFC shows the level of maturity and other helpful information for each Internet protocol or service specification.

Some RFCs document Internet standards. These RFCs form the 'STD' subseries of the RFC series . When a specification has been adopted as an Internet Standard, it is given the additional label "STDxxxx", but it keeps its RFC number and its place in the RFC series.

Not all specifications of protocols or services for the Internet should or will become Internet Standards. Such non- standards track specifications are not subject to the rules for Internet standardization. Generally, they will be published directly as RFCs at the discretion of the RFC editor and the IESG. These RFCs will be marked "Prototype", "Experimental" or "Informational" as appropriate.

```
*******************************************************
*   It is important to remember that not all RFCs     *
*   are standards track documents, and that not all   *
*   standards track documents reach the level of      *
*   Internet Standard.                                *
*******************************************************
```

Internet Drafts

During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF's "Internet Drafts" directory, which is replicated on a number of Internet hosts. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision.

An Internet Draft that is published as an RFC, or that has remained unchanged in the Internet Drafts directory for more than six months without being recommended by the IESG for publication as an RFC, is simply removed from the Internet Draft directory. At any time, an Internet Draft may be replaced by a more recent version of the same specification, restarting the six-month timeout period.

An Internet Draft is NOT a means of "publishing" a specification; specifications are published through the RFC mechanism described in the previous section. Internet Drafts have no formal status, are not part of the permanent archival record of Internet activity, and are subject to change or removal at any time.

```
*******************************************************
*   Under no circumstances should an Internet Draft    *
*   be referenced by any paper, report, or Request-for-*
*   Proposal, nor should a vendor claim compliance     *
*   with an Internet-Draft.                            *
*******************************************************
```

Note: It is acceptable to reference a standards-track specification that may reasonably be expected to be published as an RFC using the phrase "Work in Progress", without referencing an Internet Draft.

Internet Assigned Number Authority (IANA)

Many protocol specifications include numbers, keywords, and other parameters that must be uniquely assigned. Examples include version numbers, protocol numbers, port numbers, and MIB numbers. The IAB has delegated to the Internet Assigned Numbers Authority (IANA) the task of assigning such protocol parameters for the Internet. The IANA publishes tables of all currently assigned numbers and parameters in RFCs titled "Assigned Numbers".

Each category of assigned numbers typically arises from some protocol that is on the standards track or is an Internet Standard. For example, TCP port numbers are assigned because TCP is a Standard. A particular value within a category may be assigned in a variety of circumstances; the specification requiring the parameter may be in the standards track, it may be Experimental, or it may be private. Note that assignment of a number to a protocol is independent of, and does not imply, acceptance of that protocol as a standard.

NOMENCLATURE

The Internet Standards Track

Specifications that are destined to become Internet Standards evolve through a set of maturity levels known as the "standards track". These maturity levels -- "Proposed Standard", "Draft Standard", and "Standard"

Even after a specification has been adopted as an Internet Standard, further evolution often occurs based on experience an the recognition of new requirements. The nomenclature and procedures of Internet standardization provide for the replacement of old Internet Standards with new ones, and the assignment of descriptive labels to indicate the status of "retired" Internet Standards.

Types of Specifications

Specifications subject to the Internet standardization process fall into two categories: Technical Specifications (TS) and Applicability Statements (AS).

Technical Specification (TS)

A Technical Specification is any description of a protocol, service, procedure, convention, or format. It may completely describe all of the relevant aspects of its subject, or it may leave one or more parameters or options unspecified. A TS may be completely self-contained, or it may incorporate material from other specifications by reference to other documents (which may or may not be Internet Standards).

A TS shall include a statement of its scope and the general intent for its use (domain of applicability). Thus, a TS that is inherently specific to a particular context shall contain a statement to that effect. However, a TS does not specify requirements for its use within the Internet; these requirements, which depend on the particular context in which the TS is incorporated by different system configurations, is defined by an Applicability Statement.

Applicability Statement (AS)

An Applicability Statement specifies how, and under what circumstances, one or more TSs are to be applied to support a particular Internet capability. An AS may specify uses for TSs that are not Internet Standards.

An AS identifies the relevant TSs and the specific way in which they are to be combined, and may also specify particular values or ranges of TS parameters or subfunctions of a TS protocol that must be implemented. An AS also specifies the circumstances in which the use of a particular TS is required, recommended, or elective.

An AS may describe particular methods of using a TS in a restricted "domain of applicability", such as Internet routers, terminal servers, Internet systems that interface to Ethernets, or datagram-based database servers.

The broadest type of AS is a comprehensive conformance specification, commonly called a "requirements document", for a particular class of Internet systems, such as Internet routers or Internet hosts.

An AS may not have a higher maturity level in the standards track than any standards-track TS to which the AS applies. For example, a TS at Draft Standard level may be referenced by an AS at the Proposed Standard or Draft Standard level, but not by an AS at the Standard level.

An AS may refer to a TS that is either a standards-track specification or is "Informational", but not to a TS with a maturity level of "Prototype", "Experimental", or "Historic"

Although TSs and ASs are conceptually separate, in practice a standards-track document may combine an AS and one or more related TSs. For example, Technical Specifications that are developed specifically and exclusively for some particular domain of applicability, e.g., for mail server hosts, often contain within a single specification all of the relevant AS and TS information. In such cases, no useful purpose would be served by deliberately distributing the information among several documents just to preserve the formal AS/TS distinction. However, a TS that is likely to apply to more than one domain of applicability should be developed in a modular fashion, to facilitate its incorporation by multiple ASs.

Standards Track Maturity Levels

ASs and TSs go through stages of development, testing, and acceptance. Within the Internet standards process, these stages are formally labeled "maturity levels".

This section describes the maturity levels and the expected characteristics of specifications at each level.

Proposed Standard

The entry-level maturity for the standards track is "Proposed Standard". A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well-understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable. However, further experience might result in a change or even retraction of the specification before it advances.

Usually, neither implementation nor operational experience is required for the designation of a specification as a Proposed Standard. However, such experience is highly desirable, and will usually represent a strong argument in favor of a Proposed Standard designation.

The IESG may require implementation and/or operational experience prior to granting Proposed Standard status to a specification that materially affects the core Internet protocols or that specifies behavior that may have significant operational impact on the Internet. Typically, such a specification will be published initially with Experimental or Prototype status (see below), and moved to the standards track only after sufficient implementation or operational experience has been obtained.

A Proposed Standard should have no known technical omissions with respect to the requirements placed upon it. However, the IESG may recommend that this requirement be explicitly reduced in order to allow a protocol to advance into the Proposed Standard state, when a specification is considered to be useful and necessary (and timely), even absent the missing features.

Implementors should treat Proposed Standards as immature specifications. It is desirable to implement them in order to gain experience and to validate, test, and clarify the specification. However, since the content of Proposed Standards may be changed if problems are found or better solutions are identified, deploying implementations of such standards into a disruption-sensitive customer base is not normally advisable.

Draft Standard

A specification from which at least two independent and interoperable implementations have been developed, and for which sufficient successful operational experience has been obtained, may be elevated to the "Draft Standard" level. This is a major advance in status, indicating a strong belief that the specification is mature and will be useful.

A Draft Standard must be well-understood and known to be quite stable, both in its semantics and as a basis for developing an implementation. A Draft Standard may still require additional or more widespread field experience, since it is possible for implementations based on Draft Standard specifications to demonstrate unforeseen behavior when subjected to large-scale use in production environments.

Internet Standard

A specification for which significant implementation and successful operational experience has been obtained may be elevated to the Internet Standard level. An Internet Standard (which may simply be referred to as a Standard) is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

A Draft Standard is normally considered to be a final specification, and changes are likely to be made only to solve specific problems encountered. In most circumstances, it is reasonable for vendors to deploy implementations of draft standards into the customer base.

Non-Standards Track Maturity Levels

Not every TS or AS is on the standards track. A TS may not be intended to be an Internet Standard, or it may be intended for eventual standardization but not yet ready to enter the standards track. A TS or AS may have been superseded by more recent Internet Standards, or have otherwise fallen into disuse or disfavor.

Specifications not on the standards track are labeled with one of four off-track maturity levels: "Prototype, "Experimental", "Informational", and "Historic". There are no time limits associated with these non-standard track labels, and the documents bearing these labels are not Internet standards in any sense. As the Internet grows, there is a growing amount of credible technical work being submitted directly to the RFC Editor without having been gone through the IETF. It is possible that such outside submissions may overlap or even conflict with ongoing IETF activities. In order for the best technical result to emerge for the community, we believe that the such outside submissions should be given the opportunity to work within IETF to gain the broadest possible consensus.

It is also possible that supporters of a view different from the IETF may wish to publish their divergent view. For this reason, it is important that, ultimately, authors should have the opportunity to publish Informational and Experimental RFCs should they wish to. However, it is also possible that this could open a loophole in which developers could try to bypass the IETF consensus process completely by publishing an Informational RFC (and relying on the prestige of the RFC series to gain community support for their document).

For all these reasons, the IESG and the RFC Editor have agreed to the following policy for publishing Info and Exp RFCs:

1. The RFC Editor will bring to the attention of the IESG al Informational and Experimental submissions that the RFC Editor feels may be related to, or of interest to, the IETF community.

2. The IESG will review all such referrals within a fixed length of time and make a recommendation on whether to publish, or to suggest that the author bring their work within the IETF.
3. If the IESG recommends that the work be brought within the IETF, but the author declines the invitation, the IESG may add disclaimer text into the standard boilerplate material added by the RFC Editor (e.g., "Status of this memo").

Prototype

For new protocols which affect core services of the Internet or for which the interactions with existing protocols are too complex to fully assimilate from the written specification, the IESG may request that operational experience be obtained prior to advancement to Proposed Standard status. In these cases, the IESG will designate an otherwise complete specification as "Prototype". This status permits it to be published as an RFC before it is entered onto the standards track. In this respect, "Prototype" is similar to "Experimental", except that it indicates the protocol is specifically being developed to become a standard, while "Experimental" generally indicates a more exploratory phase of development.

Experimental

The "Experimental" designation on a TS typically denotes a specification that is part of some research or development effort. Such a specification is published for the general information of the Internet technical community and as an archival record of the work. An Experimental specification may be the output of an organized Internet research effort (e.g., a Research Group of the IRTF), or it may be an individual contribution.

Documents intended for Experimental status should be submitted directly to the RFC Editor for publication. The procedure is intended to expedite the publication of any responsible Experimental specification, subject only to editorial considerations, and to verification that there has been adequate coordination with the standards process.

Informational

An "Informational" specification is published for the general information of the Internet community, and does not represent an Internet community consensus or recommendation. The Informational designation is intended to provide for the timely publication of a very broad range of responsible informational documents from many sources, subject only to editorial considerations and to verification that there has been adequate coordination with the standards process.

Specifications that have been prepared outside of the Internet community and are not incorporated into the Internet standards process by any of the provisions of Section 4 may be published as Informational RFCs, with the permission of the owner.

Historic

A TS or AS that has been superseded by a more recent specification or is for any other reason considered to be obsolete is assigned to the "Historic" level. (Purists have suggested that the word should be "Historical"; however, at this point the use of "Historic" is historical.)

Requirement Levels

An AS may apply one of the following "requirement levels" to each of the TSs to which it refers:

(a) Required: Implementation of the referenced TS, as specified by the AS, is required to achieve minimal conformance. For example, IP and ICMP must be implemented by all Internet systems using the TCP/IP Protocol Suite.

(b) Recommended: Implementation of the referenced TS is not required for minimal conformance, but experience and/or generally accepted technical wisdom suggest its desirability in the domain of applicability of the AS. Vendors are strongly encouraged to include the functions, features, an protocols of Recommended TSs in their products, and should omit them only if the omission is justified by some special circumstance.

(c) Elective: Implementation of the referenced TS is optional within the domain of applicability of the AS; that is, the AS creates no explicit necessity to apply the TS. However, a particular vendor may decide to implement it, or a particular user may decide that it is a necessity in a specific environment.

(d) Limited Use: The TS is considered appropriate for use only in limited or unique circumstances. For example, the usage of a protocol with the "Experimental" designation should generally be limited to those actively involved with the experiment.

(e) Not Recommended: A TS that is considered to be inappropriate for general use is labeled "Not Recommended". This may be because of its limited functionality, specialized nature, or historic status.

The "Official Protocol Standards" RFC lists a general requirement level for each TS, using the nomenclature defined in this section. In many cases, more detailed descriptions of the requirement levels of particular protocols and of individual features of the protocols will be found in appropriate ASs.

THE INTERNET STANDARDS PROCESS

Review and Approval

A "standards action" -- entering a particular specification into, advancing it within, or removing it from, the standards track -- must be approved by the IESG.

- Initiation of Action

Typically, a standards action is initiated by a recommendation to the appropriate IETF Area Director by the individual or group that is responsible for the specification, usually an IETF Working Group.
After completion to the satisfaction of its author and the cognizant Working Group, a document that is expected to enter or advance in the Internet standardization process shall be made available as an Internet Draft. It shall remain as an Internet Draft for a period of time that permits useful community review, at least two weeks, before submission to the IESG with a recommendation for action.

- IESG Review and Approval

The IESG shall determine whether a specification satisfies the applicable criteria for the recommended action

The IESG shall determine if an independent technical review of the specification is required, and shall commission one when necessary. This may require creating a new Working Group, or an existing group may agree to take responsibility for reviewing the specification. When a specification is sufficiently important in terms of its potential impact on the Internet or on the suite of Internet protocols, the IESG shall form an independent technical review and analysis committee to prepare an evaluation of the specification. Such a committee is commissioned to provide an objective basis for agreement within the Internet community that the specification is ready for advancement.

The IESG shall communicate its findings to the IETF to permit a final review by the general Internet community. This "last-call" notification shall be via electronic mail to the IETF mailing list. In addition, for important specifications there shall be a presentation or statement by the appropriate Working Group or Area Director during an IETF plenary meeting. Any significant issues that have not been resolved satisfactorily during the development of the specification may be raised at this time for final resolution by the IESG.

In a timely fashion, but no sooner than two weeks after issuing the last-call notification to the IETF mailing list, the IESG shall make its final determination on whether or not to approve the standards action, and shall notify the IETF of its decision via email.

- Publication

Following IESG approval and any necessary editorial work, the RFC Editor shall publish the specification as an RFC. The specification shall then be removed from the Internet Drafts directory.

An official summary of standards actions completed and pending shall appear in each issue of the Internet Society Newsletter. This shall constitute the "journal of record" for Internet standards actions. In addition, the IESG shall publish a monthly summary of standards actions completed and pending in the Internet Monthly Report, which is distributed to all members of the IETF mailing list.

Finally, the IAB shall publish quarterly an "Internet Official Protocol Standards" RFC, summarizing the status of all Internet protocol and service specifications, both within and outside the standards track.

Entering the Standards Track

A specification that is potentially an Internet Standard may originate from:

(a) an ISOC-sponsored effort (typically an IETF Working Group),

(b) independent activity by individuals, or

(c) an external organization.

Case (a) accounts for the great majority of specifications that enter the standards track. In cases (b) and (c), the work might be tightly integrated with the work of an existing IETF Working Group, or it might be offered for standardization without prior IETF involvement. In most cases, a specification resulting from an effort that took place outside of an IETF Working Group will be submitted to an appropriate Working Group for evaluation and refinement. If necessary, an appropriate Working Group will be created.

For externally-developed specifications that are well-integrated with existing Working Group efforts, a Working Group is assumed to afford adequate community review of the accuracy and applicability of the specification. If a Working Group is unable to resolve all technical and usage questions, additional independent review may be necessary. Such reviews may be done within a Working Group context, or by an ad hoc review committee established specifically for that purpose. Ad hoc review committees may also be convened in other circumstances when the nature of review required is too small to require the formality of Working Group creation. It is the responsibility of the appropriate IETF Area Director to determine what, if any, review of an external specification is needed and how it shall be conducted.

Advancing in the Standards Track

A specification shall remain at the Proposed Standard level for at least six (6) months.

A specification shall remain at the Draft Standard level for at least four (4) months, or until at least one IETF meeting has occurred, whichever comes later.

These minimum periods are intended to ensure adequate opportunity for community review without severely impacting timeliness. These intervals shall be measured from the date of publication of the corresponding RFC(s), or, if the action does not result in RFC publication, the date of IESG approval of the action.

A specification may be (indeed, is likely to be) revised as it advances through the standards track. At each stage, the IESG shall determine the scope and significance of the revision to the specification, and, if necessary and appropriate, modify the recommended action. Minor revisions are expected, but a significant revision may require that the specification accumulate more experience at its current maturity level before progressing. Finally, if the specification has been changed very significantly, the IESG may recommend that the revision be treated as a new document, re-entering the standards track at the beginning.

Change of status shall result in republication of the specification as an RFC, except in the rare case that there have been no changes at all in the specification since the last publication. Generally, desired changes will be "batched" for incorporation at the next level in the standards track. However, deferral of changes to the next standards action on the specification will not always be possible or desirable; for example, an important typographical error, or a technical error that does not represent a change in overall function of the specification, may need to be corrected immediately. In such cases, the IESG or RFC Editor may be asked to republish the RFC with corrections, and this will not reset the minimum time-at- level clock.

When a standards-track specification has not reached the Internet Standard level but has remained at the same status level for twenty-four (24) months, and every twelve (12) months thereafter until the status is changed, the IESG shall review the viability of the standardization effort responsible for that specification.
Following each such review, the IESG shall approve termination or continuation of the development. This decision shall be communicated to the IETF via electronic mail to the IETF mailing list, to allow the Internet community an opportunity to comment.
This provision is not intended to threaten a legitimate and active Working Group effort, but rather to provide an administrative mechanism for terminating a moribund effort.

Revising a Standard

A new version of an established Internet Standard must progress through the full Internet standardization process as if it were a completely new specification. Once the new version has reached the Standard level, it will usually replace the previous version, which will move to Historic status. However, in some cases both versions may remain as Internet Standards to honor the requirements of an installed base. In this situation, the relationship between the previous and the new versions must be explicitly stated in the text of the new version or in another appropriate document

Retiring a Standard

As the technology changes and matures, it is possible for a new Standard specification to be so clearly superior technically that one or more existing Internet Standards for the same function should be retired. In this case, the IESG shall approve a change of status of the superseded specification(s) from Standard to Historic. This recommendation shall be issued with the same Last-Call and notification procedures used for any other standards action.

Conflict Resolution and Appeals

IETF Working Groups are generally able to reach consensus, which sometimes requires difficult compromises between differing technical solutions. However, there are times when even reasonable and knowledgeable people are unable to agree. To achieve the goals of openness and fairness, such conflicts must be resolved with a process of open review and discussion.
Participants in a Working Group may disagree with Working Group decisions, based either upon the belief that their own views are not being adequately considered or the belief that the Working Group made a technical choice which essentially will not work.
The first issue is a difficulty with Working Group process, and the latter is an assertion of technical error. These two kinds of disagreements may have different kinds of final outcome, but the resolution process is the same for both cases.

Working Group participants always should first attempt to discuss their concerns with the Working Group chair. If this proves unsatisfactory, they should raise their concerns with an IESG Area Director or other IESG member. In most cases, issues raised to the level of the IESG will receive consideration by the entire IESG, with the relevant Area Director or the IETF Chair being tasked with communicating results of the discussion.

For the general community as well as Working Group participants seeking a larger audience for their concerns, there are two opportunities for explicit comment.

(1) When appropriate, a specification that is being suggested for advancement along the standards track will be presented during an IETF plenary. At that time, IETF participants may choose to raise issues with the plenary or to pursue their issues privately, with any of the relevant IETF/IESG management personnel.
(2) Specifications that are to be considered by the IESG are publicly announced to the IETF mailing list, with a request for comments.

Finally, if a problem persists, the IAB may be asked to adjudicate the dispute.

* If a concern involves questions of adequate Working Group discussion, the IAB will attempt to determine the actual nature and extent of discussion that took place within the Working Group, based upon the Working Group's written record and upon comments of other Working Group participants.

* If a concern involves questions of technical adequacy, the IAB may convene an appropriate review panel, which may then recommend that the IESG and Working Group re-consider an alternate technical choice.

* If a concern involves a reasonable difference in technical approach, but does not substantiate a claim that the Working Group decision will fail to perform adequately, the Working Group participant may wish to pursue formation of a separate Working Group. The IESG and IAB encourage alternative points of view and the development of technical options, allowing the general Internet community to show preference by making its own choices, rather than by having legislated decisions.

EXTERNAL STANDARDS AND SPECIFICATIONS

Many standards groups other than the IETF create and publish standards documents for network protocols and services. When these external specifications play an important role in the Internet, it is desirable to reach common agreements on their usage -- i.e., to establish Internet Standards relating to these external specifications.

There are two categories of external specifications:

(1) Open Standards

Accredited national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-TS, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards.

(2) Vendor Specifications

A vendor-proprietary specification that has come to be widely used in the Internet may be treated by the Internet community as if it were a "standard". Such a specification is not generally developed in an open fashion, is typically proprietary, and is controlled by the vendor or vendors that produced it.

To avoid conflict between competing versions of a specification, the Internet community will not standardize a TS or AS that is simply an "Internet version" of an existing external specification unless an explicit cooperative arrangement to do so has been made. However, there are several ways in which an external specification that is important for the operation and/or evolution of the Internet may be adopted for Internet use.

(a) Incorporation of an Open Standard

An Internet Standard TS or AS may incorporate an open external standard by reference. The reference must be to a specific version of the external standard, e.g., by publication date or by edition number, according to the prevailing convention of the organization that is responsible for the specification.

For example, many Internet Standards incorporate by reference the ANSI standard character set "ASCII" [2]. Whenever possible, the referenced specification shall be made available online.

(b) Incorporation of a Vendor Specification

Vendor-proprietary specifications may be incorporated by reference to a specific version of the vendor standard. If the vendor-proprietary specification is not widely and readily available, the IESG may request that it be published as an Informational RFC.

For a vendor-proprietary specification to be incorporated within the Internet standards process, the proprietor must meet the requirements of section 5 below, and in general the specification shall be made available online.

The IESG shall not favor a particular vendor's proprietary specification over the technically equivalent and competing specifications of other vendors by making it "required" or "recommended".

(c) Assumption

An IETF Working Group may start from an external specification and develop it into an Internet TS or AS. This is acceptable if (1) the specification is provided to the Working Group in compliance with the requirements of section 5 below, and (2) change control has been conveyed to IETF by the original developer of the specification. Continued participation in the IETF work by the original owner is likely to be valuable, and is encouraged.

The following sample text illustrates how a vendor might convey change control to the Internet Society:

"XXXX Organization asserts that it has the right to transfer to the Internet Society responsibility for further evolution of the YYYY protocol documented in References (1-n) below. XXXX Organization hereby transfers to the Internet Society responsibility for all future modification and development of the YYYY protocol, without reservation or condition."

Focus on who controls the internet,

Nobody owns Internet. The Internet, with its roots primarily in the research domain, has evolved and gained a broader user base with significant commercial activity. Various groups taht coordinate Internet issues have guided this growth and development.

- **Internet Society (ISOC). http://www.isoc.org/** The Internet Society is an international, non profit organization formed in 1992 to provide support for the Internet standards process. ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as IAB, IETF, IRTF, and IANA. ISOC also promotes research and other scholarly activities relating to the Internet.
- **Internet Architecture Board (IAB). http://www.iab.org/** The Internet Architecture Board is the technical advisor ISOC. The main purposes of the IAB are to oversee the continuous development of the TCP/IP Protocol Suite and to serve in technical advisory capacity to research members of the Internet community. IAB accomplishes this through its two primary components, the Internet Engineering Task Force (IETF) and the Internet Research Task force (IRTF). Another responsibility of the IAB is the editorial management of the RFCs. IAB is also the external liaison between the Internet and other standards organizations and forums.
- **Internet Engineering Task Force (IETF)**. http://www.ietf.org/ The **Internet Engineering Task Force** is a forum of working groups managed by the Internet Engineering Steering Group (IESG). IETF is responsible for identifying operational problems and proposing solutions to these problems. IETF also develops and reviews specifications intended as Internet standards. The working groups are collected into areas, and each area concentrates on a specific topic. Currently nine areas have been defined, although this is by no means hard and fast number. The areas are: Applications, Internet Protocols, Routing, Operations, User Services, Network Management, Transport, Internet protocol next generation (IPng), and Security
- **Internet Research Task Force (IRTF). http://www.irtf.org/** The **Internet Research Task Force (IRTF)** is a forum of working groups managed by the Internet Research Steering Group (IRSG). IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.
- **Internet Assigned Numbers Authority (IANA) and Internet Corporation for Assigned Names and Numbers (ICANN). http://www.icann.org/** The Internet Assigned Numbers Authority (IANA), supported by the U.S. government, was responsible for the management of Internet domain names and addresses until October 1998. At that time the Internet Corporation for Assigned Names and Numbers (ICANN), aprivate nonprofit corporation managed by an international board, assumed IANA operations.
- **Network Information Center (NIC).** The NIC is responsible for collecting and distributing information about TCP/IP protocols.

Above were the main organisations that administers Internet.

Who controls this web, this cloud, this network of networks? Well, no one, really. The Internet seems to be both institutional and anti-institutional at the same time, massive and intimate, organized and chaotic. In a sense the Internet is an international cooperative endeavor, with its member networks kicking in money, hardware, maintenance, and technical expertise.

The U.S. government has had a big influence on the federally funded parts of the Internet. The National Science Foundation (NSF) initiated the NSFNET in the mid 1980s, a nationwide backbone in the United States that connected many mid-level networks, which in turn connected universities and other organizations. At the time of this writing, the NSFNET production backbone is being phased out and connectivity will be offered by other providers, including commercial networks, in the near future. But you may still hear people refer to the NSF and its influence on the Internet. The NSF funds an experimental high-speed network and will continue to provide funding for a short time to assist universities and schools in getting Internet connections.

Names and Addresses

If you've ever traveled in a country where you couldn't read the street signs or figure out how they numbered the houses, you'll understand the wisdom of learning the Internet's name and address system. Most computers on the Internet can be identified in two ways. Each computer, or **host**, has a name and a numerical address (both unique), just as most of us can be located by our names or numerically by our phone numbers. It's easier to remember a name than a phone number, and it's the same on the Internet. An Internet computer name is usually several words separated by periods, such as yahoo.com. An Internet address—technically an **IP address**—is four numbers also separated by periods, for example, 161.44.128.70.

When you're saying these names and addresses out loud, you should substitute "dot" for "period" to sound as though you belong.

The idea is for people to use the computers' names when accessing resources, and to let the computers and routers work with the IP addresses. Each Internet-connected organization keeps a database of the names and addresses of all the computers connected to its own networks. Because there are so many computers on the Internet and there is no real central authority, name assignment is best left to the local networks.

Domain Name System. There's actually a method to these names and addresses—a naming system known as the Domain Name System, or DNS. The DNS is also the worldwide system of distributed databases of names and addresses. These databases provide the "translation" from names to numbers and vice versa, a sort of international *Who's Who* of computers. DNS names are constructed in a hierarchical naming fashion, which you can think of as a worldwide organization chart. At the top of this chart are top-level specifications, such as EDU (educational), COM (commercial), GOV (government), MIL (military), ORG (organizations), and NET (networks), and also two-letter country codes, such as US for the United States and CH for Switzerland.

An organization can register for a **domain name**, selecting one of the top-level specifications mentioned above that describes it best, and then preceding it with a recognizable version of its name. For example, the ABC Software Systems company will have a domain name like *abc.com*. From there, it can divide itself into subdomains, extending the organization chart to department levels, or it can just give all of its computers names in the *abc.com* domain.

Once you understand how this naming system works, you can remember names more easily, and you can also tell things about a computer, such as to what organization it belongs. The names do not, however, always indicate geographical location.

Many U.S. organizations and companies use the three-letter designations mentioned above (for example, EDU, COM, and ORG). However, most countries have stipulated that organizations use their two-letter country codes for top-level domains. For example, an actual computer name, *quake.think.com*, refers to a commercial (COM) enterprise: the computer's name is *quake* and it belongs to Thinking Machines Corporation (*think*), a supercomputer manufacturer in the United States. Another example is *fujitsu.co.jp*, a computer at the Fujitsu Company in Japan (*jp* is the two-letter country code for Japan).

Managing e-business infrastructure:

The key management issues of e-Business infrastructure are as follows:

1. **Which type of e-Business applications do we develop?**

   Various applications of e-commerce are continually affecting trends and prospects for business over the Internet. This issue basically indicate the purpose of e-Business applications. E.g. Supply Chain Management, e- procurement, secure online ordering, customer relationship management.

2. **Which technologies do we use?**

   E-Business Technology provides professional services that help the business take full advantage of Internet advances. These technologies can improve the business processes in a cost-effective manner. E.g. email, web based ordering vs. EDI

3. **How do we achieve quality of service in applications?**

   An important aspect in business-to-business e-commerce scenarios is how to meet response time and throughput requirements of applications in spite of execution taking place across corporate boundaries and, in the future, via the Internet instead of using leased lines. Given the unpredictable variations of available bandwidth in today’s Internet, providing Application Quality of Service guarantees for these requirements is a complex task. Some of the requirements to achieve the quality of service are business fit, security speed, availability and errors.

4. **Where do we host applications?**

   It basically includes the internal or the external sourcing.

5. **Application Integration**

   This particular issue deals with the integration of the e-business solutions with:

   a) Legacy Systems

   b) Partner Systems

   c) B2B exchanges and intermediaries

6. **Which access platforms do we support? Which development technologies and standards do we use?**

   This may include the mobile access, interactive digital TV, etc.

   E.g. CGI, Perl, Cold Fusion, ActiveX

7. **How do we manage content and quality?**

   In e-Business scenarios, the evaluation of the quality of exchanged data is essential for developing the service based applications and correctly performing cooperative activities. This issue focuses on how the content and data are updated so that they are up to date, accurate, easy to find and easy to interpret.

8. **How do we manage employee access to internet?**

   Monitoring the employee's usage of internet in an organization is crucial for any organization. Since staff can potentially waste time using the internet or can act illegally.

9. **How do we secure data?**

   Consumer trust in the security of sensitive information is more critical than ever .Many security issues can arise such as deletion of the content and data in error or maliciously. Such security issues much be dealt effectively.

As explained at the start of the chapter, **e-business infrastructure** comprises the hardware, software, content and data used to deliver e-business services to employees, customers and partners. In this part of the chapter we look at the management of e-business infrastructure by reviewing different perspectives on the infrastructure. These are:

1 *Hardware and systems software infrastructure*. This refers mainly to the hardware and network infrastructure discussed in the previous sections. It includes the provision of clients, servers, network services and also systems software such as operating systems and browsers (Layers II, III and IV in *Figure 3.1*).

2 *Applications infrastructure*. This refers to the applications software used to deliver services to employees, customers and other partners (Layer I in *Figure 3.1*).

A further perspective is the management of data and content (Layer V in *Figure 3.1*) which is reviewed in more detail in the third part of this book.

To illustrate the importance and challenges of maintaining an adequate infrastructure, read the mini case study about the **microblogging** service Twitter. Twitter is a fascinating case of the challenges of monetizing an online service and delivering adequate services levels with a limited budget and a small team. This case study shows some of the successes and challenges for the start-up e-business.

Managing hardware and systems software infrastructure

Management of the technology infrastructure requires decisions on Layers II, III and IV in *Figure 3.1.*

Layer II – Systems software

The key management decision is standardization throughout the organization. Standardization leads to reduced numbers of contacts for support and maintenance and can reduce purchase prices through multi-user licences. Systems software choices occur for the client, server and network. On the client computers, the decision will be which browser software to standardize on, for example Microsoft Explorer or an open-source alternative. Standardized plug-ins such as Adobe Acrobat to access .pdf files should also be installed across the organization. The systems software for the client will also be decided on; this will probably be a variant of Microsoft Windows, but open-source alternatives such as Linux may also be considered. When considering systems software for the server, it should be remembered that there may be many servers in the global organization, both for the Internet and intranets. Using standardized web-server software such as Apache will help maintenance. Networking software will also be decided on; this could be Microsoft-sourced or from other suppliers such as Sun Microsystems or Novell.

Layer III – Transport or network

Decisions on the network will be based on the internal company network, which for the e-business will be an intranet, and for the external network either an extranet or VPN (*p. 177*) or links to the public Internet. The main management decision is whether internal or external network management will be performed by the company or outsourced to a third party. Outsourcing of network management is common. Standardized hardware is also needed to connect clients to the Internet, for example, a modem card or external modem in home PCs or a network interface card (NIC) to connect to the company (local-area) network for business computers.

Layer IV – Storage

The decision on storage is similar to that for the transport layer. Storage can be managed internally or externally. This is not an either–or choice. For example, intranet and extranet are commonly managed internally while Internet storage such as the corporate web site is commonly managed externally or at an application service provider (*p. 168*). However, intranets and extranets can also be managed externally.

We will now consider decisions involving third-party service providers of the hardware and systems software infrastructure.

Managing Internet service and hosting providers

Service providers who provide access to the Internet for consumers or businesses are usually referred to as 'ISPs' or 'Internet service providers'. ISPs may also host the web sites which publish a company's web site content. But many organizations will turn to a separate hosting provider to manage the company's web site and other e-business services accessed by customers and partners such as extranets, so it is important to select an appropriate hosting provider.

ISP connection methods

Figure 3.2 shows the way in which companies or home users connect to the Internet. The diagram is greatly simplified in that there are several tiers of ISPs. A user may connect to one ISP which will then transfer the request to another ISP which is connected to the main Internet backbone.

High-speed broadband is now the dominant home access method rather than the previously popular **dial-up connection**.

However, companies should remember that there are significant numbers of Internet users who have the slower dial-up access which they support through their web sites. Ofcom (2008) reported that the proportion of homes taking broadband services grew to 58% by Q1 2008, a rise of six percentage points on a year earlier. However, the rate of growth is slowing, following increases of 11% and 10% in the previous two years.

Broadband uses a technology known as ADSL or asymmetric digital subscriber line, which means that the traditional phone line can be used for digital data transfer. It is asym- metric since download speeds are typically higher than upload speeds. Small and medium businesses can also benefit from faster continuous access than was previously possible.

The higher speeds available through broadband together with a continuous 'always on' connection that has already transformed use of the Internet. Information access is more rapid and it becomes more practical to access richer content such as digital video. The increased speed increases usage of the Internet.

Issues in management of ISP and hosting relationships

The primary issue for businesses in managing ISPs and hosting providers is to ensure a satisfactory service quality at a reasonable price. As the customers and partners of organizations become more dependent on their web services, it is important that downtime be minimized. But surprisingly in 2008 severe problems of downtime can occur as shown in *Box 3.5* and the consequences of these need to be avoided or managed.

Speed of access

A site or e-business service fails if it fails to deliver an acceptable download speed for users.

In the broadband world this is still important as e-business applications become more complex and sites integrate more rich media such as audio and video. But what is acceptable? Research supported by Akamai (2006) suggested that content needs to load within 4 seconds, otherwise site experience suffers. The research also showed, however, that high product price and shipping costs and problems with shipping were considered more important than speed. However, for sites perceived to have poor performance, many shoppers said they would be be likely to visit the site again (64%) or buy from the e-retailer (62%).

Speed of access of a customer, employee or partner to services on an e-business server is determined by both the speed of server and the speed of the network connection to the server. The speed of the site governs how fast the response is to a request for information from the end-user. This will be dependent on the speed of the server machine on which the web site is hosted and how quickly the server processes the information. If there are only a small number of users accessing information on the server, then there will not be a noticeable delay on requests for pages. If, however, there are thousands of users requesting information at the same time then there may be a delay and it is important that the combination of web server software and hardware can cope. Web server software will not greatly affect the speed at which requests are answered. The speed of the server is mainly controlled by the amount of primary storage (for example, 1024 Mb RAM is faster than 512 Mb RAM) and the speed of the magnetic storage (hard disk). Many of the search-engine web sites now store all their index data in RAM since this is faster than reading data from the hard disk. Companies will pay ISPs according to the capabilities of the server.

As an indication of the factors that affect performance, the DaveChaffey.com website has a shared plan from the hosting provider which offers:

- 2400 GB bandwidth
- 200 MB application memory
- 60 GB disk space (this is the hosting capacity which doesn't affect performance).

An important aspect of hosting selection is whether the server is **dedicated** or shared (colocated). Clearly, if content on a server is shared with other sites hosted on the same server then performance and downtime will be affected by demand loads on these other sites. But a dedicated server package can cost 5 to 10 times the amount of a shared plan, so many small and medium businesses are better advised to adopt a shared plan, but take steps to minimize the risks with other sites going down.

For high-traffic sites, servers may be located across several computers with many processors to spread the demand load. New distributed methods of hosting content, summarized by Spinrad (1999), have been introduced to improve the speed of serving web pages for very large corporate sites. These methods involve distributing content on servers around the globe, and the most widely used service is Akamai (www.akamai.com). These are used by companies such as Yahoo!, Apple and other 'hot-spot' sites likely to receive many hits.

The speed is also governed by the speed of the network connection, commonly referred to as the network '**bandwidth**'. The bandwidth of a web site's connection to the Internet and the bandwidth of the customer's connection to the Internet will affect the speed with which web pages and associated graphics load onto the customer's PC. The term is so called because of the width of range of electromagnetic frequencies an analogue or digital signal occupies for a given transmission medium.

As described in *Box 3.7*, bandwidth gives an indication of the speed at which data can be transferred from a web server along a particular medium such as a network cable or phone line. In simple terms bandwidth can be thought of as the size of a pipe along which information flows. The higher the bandwidth, the greater the diameter of the pipe, and the faster information is delivered to the user. Many ISPs have bandwidth caps, even on 'unlimited' Internet access plans for users who consume high volumes of bandwidth for video streams for example.

Table 3.5 shows that the top five sites with the lowest download speeds tend to have a much lower page size or 'weight' compared with the slower sites from 95 to 100. This shows that the performance of a site is not simply dependent on the hosting with the ISP, but depends on how the site is designed. Such a system is known as a content management system (CMS). As explained in more detail in *Chapter 12*, a CMS is a means of managing the updating and publication of information on any web site, whether intranet, extranet or Internet.

The CMS used can also make a big difference. However, viewing these slower sites over a broadband connection shows that this is perhaps less of an issue than in the days when the majority, rather than the minority, were dial-up Internet users.

A major factor for a company to consider when choosing an ISP is whether the server is *dedicated* to one company or whether content from several companies is located on the same server. A dedicated server is best, but it will attract a premium price.

Availability

The availability of a web site is an indication of how easy it is for a user to connect to it. In theory this figure should be 100 per cent, but sometimes, for technical reasons such as failures in the server hardware or upgrades to software, the figure can drop substantially below this. *Box 3.8* illustrates some of the potential problems and how companies can evaluate and address them.

Service-level agreements

To ensure the best speed and availability a company should check the **service-level agreements (SLAs)** carefully when outsourcing web site hosting services. The SLA will define confirmed standards of availability and performance measured in terms of the *latency* or network delay when information is passed from one point to the next (such as London to New York). The SLA also includes notification to the customer detailing when the web service becomes unavailable with reasons why and estimates of when the service will be restored. Further information on SLAs is available at www.uk.uu.net/support/sla/.

Security

Security is another important issue in service quality. How to control security was referred to in the earlier section on firewalls and is considered in detail in the Focus on security design (*Chapter 11*, p. 652).

Managing employee access to the Internet and e-mail

This is covered in *Chapter 11* in the *Focus on e-business security* section.

Security is a prime concern of e-business managers. The principal concern is the security of information: both about customers and internal company data about finance, logistics, marketing and employees. Indeed, we saw in *Chapter 4* that securing customer information is a legal requirement under data protection laws in many countries. These risks apply to all companies, large and small. Larger companies tend to be more at risk from targeted attacks which are directed at disrupting services. Information used within e-business systems must be safeguarded from a range of hazards. The range of risks faced by organizations are summarized in *Box 11.3*.

Given the extent of the security risks described in *Figure 11.19*, many organizations now implement a formal **information security management system**.

The information management strategy will mandate that there is an **information security policy**. This may be a policy developed in-house, or adoption of a security standard such as British Standard BS 7799 which has now been upgraded and ratified as international standard ISO/IEC 17799.

I have based the coverage in this edition of *E-Business and E-Commerce Management* on ISO 17799 since this has comprehensive coverage of different risks and approaches to management of security. It recommends the following processes:

1 *Plan* – perform business risk analysis
2 *Do* – internal controls to manage the applicable risks
3 *Check* – a management review to verify effectiveness
4 *Act* – action changes required as part of the review as necessary.

ISO 17799/BS 7799 provides an international standard which helps give a framework by which to manage the risks to the information evident from *Figure 11.19*. It requires the following areas of information security management to be defined:

- *Section 1: Security policy*. Describes the organization's requirements and scope of security for different business areas and sites. It also should demonstrate the support of senior management in controlling and owning security.
- *Section 2: Organizational security*. Describes how the company manages security including different staff responsibilities for security, how security incidents are reported, actioned and reviewed as a standard business activity to improve security.
- *Section 3: Asset classification and control*. This is similar to completing an inventory of physical assets such as computers, printers, machinery, vehicles, etc. It requires an information audit asking questions such as 'Howmuch does it cost to obtain?Howmuch would it cost to replace? What is the extent of damage done to the organization if it was disclosed to the public or a competitor?'. Through answering these questions and developing an inventory for different types of information assets, appropriate safeguards can be put in place. BS 7799 recommends that an **information asset register (IAR)** be created, detailing every information asset within the organization such as databases, personnel records, contracts, software licences, publicity material. For each asset, responsibility is defined. The value of each asset can then be determined to ensure appropriate security is in place.
- *Section 4*: *Personnel security*. This ensures there is clarity within job definitions and employment contracts, to reduce the risk of human error leading to information loss and to ensure that staff understand what their rights and responsibilities are concerning information

security. Staff training is also important to achieve this. An example of education material which is publicly available for the Massachusetts Institute of Technology is: http://web.mit.edu/ist/topics/security/ .

- *Section 5: Physical and environmental security*. This defines physical access to buildings. It also considers how information can be protected from threats such as fire and flood.
- *Section 6: Communications and operations management*. Guidelines on the day-to-day operation of information systems is the largest section of BS 7799. It covers acceptance criteria for new or updated systems, virus defence software, e-mail and web-site usage, network access and backup and restore systems.
- *Section 7: Access control*. This defines how to protect access to information systems through access control mechanisms (username and password procedures with different security clearance for different applications and types of information).
- *Section 8: System development and maintenance*. This specifies how new systems must be designed and procured with security in mind.
- *Section 9: Business continuity management*. **Business continuity management or disaster recovery** specifies how the organization will be able to continue to function in the event of a major event such as a fire or flood or other damage to information systems. Use of off-site backups and alternative systems is key to this.
- *Section 10: Compliance*. This specifies how an organization will comply with the relevant UK and EU law related to information security management including Health and Safety legislation – The Data Protection Act, The ComputerMisuse Act, The Designs, Copyrights and Patents Act, The Human Rights Act. Implementing BS 7799 is a good way of helping ensure that a business does comply with these requirements. Regular audit and review needs to occur to ensure the organization remains compliant.

We will now cover some of the main threats to security in the e-business which need to be managed.

Managing computer viruses

Computer viruses are a significant threat to company and personal information since it is estimated that there are now over 100,000 of them.

Types of virus

There are many different mechanisms by which computer viruses spread from one machine to another. All use some technique for the virus to reproduce itself or ‘self-replicate’ and then pass on to another machine. We will now briefly review the main different types of computer virus companies need to protect against.

1 *Boot-sector virus*. **Boot-sector viruses** were most important when floppy disks were widely used.

2 *Worms*. A **worm** is a small computer program that replicates itself and then transfers itself from one machine to the next. Since no human interaction is required, worms can spread very rapidly. For example, the ‘Code Red’ worm replicated itself over 250,000 times in just nine hours on 19 July 2001. In 2003, the ‘Slammer’ worm exploited a security loophole in the Microsoft SQL server database product and rapidly infected 75,000 machines. Each infected machine sent out so much traffic that many other servers failed also. This was one of the fastest spreading viruses of all time, as *Figure 11.20* shows. In future it seems such worms will bring the Internet to a complete standstill.

3 *Macro-viruses*. Macro-viruses are piggybacked on documents created by office applications such asMicrosoftWord and Excel. Office software such as this has a macro-facility to help users record common actions such as formatting or to develop more complex applications in Visual Basic for Applications (VBA).One of the best-known macro-viruses is ‘Melissa’. This struck in March 1999 and it marked a new trend as it combined a macro virus with one that accessed the address book of Microsoft Outlook to e-mail itself to new victims. This was one of the fastest spreading viruses in history and it is estimated that it affected over a million PCs. In 2002, the author of the ‘Melissa’ virus, David L. Smith, was sentenced to 20 months in prison in the US.

4 *E-mail attachment viruses*. These viruses are activated when a user of an e-mail program opens an attachment. ‘Melissa’ is an example of such a virus. The ‘Love Bug’ virus contains the subject line ‘I love you’, while the message contains the text ‘kindly check the attached LOVELETTER from me’ which is an attached file called LOVE-LETTER-FORYOU. TXT.VBS. The virus deleted image and audio files and accessed Internet servers to send out different versions of itself.According to ClickZ (2003) it was estimated that nearly $9 billion damage was done through this virus. Much of the costs is not the loss of data, but the cost of hiring specialists to rectify the problem or staff time lost.

5 *Trojan viruses*. A **trojan** is a virus that masquerades as a bona fide application. They are named after the Greek myth of the giant wooden horse used by attackers to gain access to Troy in order to attack it. Examples include utilities such as a file-sharing program, a screen saver, upgrades to some system components and even imitation anti-virus programs. The advantage for virus writers is that the programs can be much larger. One of the most famous trojans is ‘Back Orifice’, reputedly developed by a hacking group known as ‘Cult of the Dead Cow’. This could be attached to other larger files and gave complete access to a machine for a hacker.

6 *Hoax e-mail viruses*. These are warnings about viruses which are not real viruses which ask the recipient to send the warning on to their friends. They are usually malicious, but can contain instructions on how to remove the virus by deleting files which could cause damage. They cause disruption through time lost.

Protecting computer systems against viruses

All organizations and individuals require a policy to combat the potential impact of viruses given the frequency with which new, damaging viruses are released. Even individual computer users at home should think through the steps they can take to counter viruses. There are two approaches that can be combined to counter viruses. These are using the right tools and educating staff to change practices.

Anti-virus software is well known as a tool to protect systems from viruses. Many businesses and homes now use products such as McAfee Virus Scan and Symantec Norton Anti-Virus to protect themselves against the threat of viruses. Unfortunately, a lot more action is required than initial purchase for the anti-virus software to be effective. We have seen above that new viruses are continually released. It is therefore essential that regular updates be obtained and this often doesn’t happen since a process has to be in place to trigger updates such as a monthly update.

Companies also need to decide on the frequency of scanning memory and computer files, since a full-scan on start-up can take a long time. Most anti-virus software now seeks to identify viruses when they first arrive (real-time scanning). A further issue is how good the anti-virus tool is at identifying e-mail and macro-viruses, since it is less straightforward for these types of virus to be identified.

Another approach to countering e-mail viruses is to use an external **managed e-mail service** which scans e-mails before they arrive in the organization and then scans e-mails for viruses when they are sent. For example, Messagelabs **(**www.messagelabs.com**)** scans 2.7billion e-mails a day for 7,500 companies worldwide. In August 2008 it reported that:

- 78% of messages were spam
- 1 in 88 contained a virus
- 1 in 522 was a phishing attempt.

Managed e-mail services are likely to be more effective than using internal anti-virus software since the service providers are experts in this field. They will also be able to identify and respond to e-mail worm attacks more rapidly.

To summarize, organizations need a policy to be developed for use of anti-virus software. This should specify:

1 The preferred anti-virus software to be used on all machines.
2 The frequency and mechanism for updating anti-virus software.
3 The frequency with which the whole end-user PC is system-scanned for viruses.
4 Organizational blocking of attachments with uncommon extensions.
5 Organizational disabling of macros in office applications.
6 Scanning to be performed on mail servers when e-mails are first received and before viruses are sent.
7 Recommendations on use of spam-filtering software.
8 Backup and recovery mechanisms.

Education of staff in identifying and then acting upon the different types of virus can also limit the impact of viruses. Apart from Internet worms which execute automatically, some steps can be taken to reduce the risks from all the types of viruses identified above. Some general instructions can then be developed as part of a policy to reduce the risk of virus infection and transmission.Many of these apply also to home machines:

1 Do not switch off machines when the floppy disk is still in the drive (reduces transmission of boot-sector drives). PCs can also be configured so that they do not boot off the floppy drive.
2 Do not open attachments to e-mails from people you don’t know (reduce transmission of e-mail attachment viruses). Since some viruses will be sent from trusted sources, only open attachments which look legitimate, for exampleWord documents with relevant names. Some viruses use file extensions that are not commonly used such as .pif, .scr or .vbs.Viewing documents rather than opening them for editing can also reduce the risk of transmission.
3 Download software only from the official source, and always check for viruses before installing the software (reduces risk of trojan horse viruses).
4 Disable or turn off macros inWord or Excel unless you use them regularly (reduces risk of macro-viruses).
5 Back-up important files daily if this function is not performed by a system administrator.

Controlling information service usage

Issues in controlling information service typically involve one of two problems from the employer’s perspective. First, hardware and software resources provided for work purposes are used for personal purposes, thus reducing productivity. Secondly, monitoring the use of information introduces legal issues of surveillance. Monitoring of information service usage includes checking for:

- Use of e-mail for personal purposes.
- Inappropriate use of e-mail, possibly leading to legal action against the company.
- Use of Internet or web sites for personal use.

The problems in e-mail usage are covered in the later section on e-mail management. The extent of these issues, particularly in larger organizations is apparent from *Figure 11.21*.

Monitoring of electronic communications

Employee communications monitoring or surveillance is used by organizations to reduce productivity losses through time wasting. Time can be wasted when a member of staff spends time when they are paid to work checking personal e-mail messages or accessing the Internet for personal interests.

Simple calculations highlight the wastage when staff time is spent on non-productive work. If an employee earning £25,000 per year, spends 30 minutes each day of a 5-day week answering personal e-mails or visiting non-work-related web sites, this will cost the company over £1,500 per year. For a company with 100 employees, where the average employee works 46 weeks per year, this amounts to over £150,000 per year or the cost of several new employees! Activities such as using streaming media to view the news or download audio clips can also place strain on the company networks if they are common.

A typical example of alleged time wasting where the company dismissed the employee involved Lois Franxhi, a 28-year-old IT manager who was sacked in July 1998 for making nearly 150 searches over four days in office hours for a holiday. She claimed unfair dismissal – she was pregnant at the time of the dismissal. As with many unfair dismissals, the case was not clear-cut, with Mrs Franxhi claiming the company sacked her because of sex discrimination. The tribunal dismissed these claims, finding that the employee had lied about the use of the Internet, saying she had only used it for one lunchtime when in fact records showed she had used it over four days.

More recently DTI (2006) reported on a member of staff at a small services company who accessed adult web sites at work. He used someone else's computer to conceal his activity. In another case, a lovesick employee at a medium-sized manufacturer spent up to six hours a day on a dating agency web site! The survey reports that

> *What hurts companies is the number of these incidents they suffer, more than one a day on average. While the median was only a few incidents a year, some small companies reported hundreds of e-mail abuses every day.*

Communications monitoring of employees may also be warranted if it is felt they are sending or receiving e-mails or accessing web sites which contain content the organization deems unacceptable. Typical examples of such content are pornography or racist material. However, some organizations even block access to news, sports or web-based e-mail sites because of the amount of time staff spend in accessing them. To define permissible content, many organizations now have acceptable-use policies. For example, many universities, at log-in, or in computer labs and libraries have notices about '**acceptable-use policy**'. This will describe the types of material it is not acceptable to access and is also a means of explaining monitoring procedures.

Scanning and filtering are the two most common form of monitoring. **Scanning software** identifies the content of e-mails sent or received and web pages accessed. Tools such as WebSense or MailMarshal SMTP from Marshal orWeb Marshal will look for the occurrence of particular words or images – pornography is indicated by skin colour tones for example. Rules will also be set up, for example to ban e-mail attachments over a particular size or containing swearing as indicated by *Figure 11.22*. Such tools can also give a picture of the most popular types of site or content. This might show, for example, how much time is being wasted accessing news and sports sites.

Such software usually also has blocking or filtering capabilities. **Filtering software** such asWebsense (www.websense.com) can detect and block other activities such as:

- Peer-to-peer (P2P) file sharing, for example of MP3 audio files
- Instant messaging using Yahoo! Messenger or Microsoft Instant Messenger
- The use of streaming media (e.g. audio and video) and other high-bandwidth applications
- Accessing specified sites, e.g. sadly some companies block all access to social networks or news sites such as www.bbc.co.uk or www.msn.co.uk since analysis has shown that staff spend so much time using them. Access to personal e-mail programs such as Yahoo! Mail or Hotmail may also be blocked. This would not be popular at universities!
- Spyware which seeks to send out information collected from computers
- Adware programs which place adverts or pop-ups
- Employee hacking.

Websense and similar products can block sites in different categories, for different types of staff, according to the acceptable-use policy of the organization using a database (www.

websense.com/products/about/database/categories.cfm) that contains over 1.5 million web sites in many categories of which we list just some to illustrate the degree of control available to the employer. Example of the categories include:

- Abortion or Pro-Choice or Pro-Life
- Adult Material
- Parent category that contains the categories: Adult Content, Lingerie and Swimsuit,Nudity, Sex, Sex Education
- Adult Content
- Advocacy Groups
- Business and Economy
- Financial Data and Services
- Drugs
- Education
- Entertainment
- Gambling
- Games
- Government
- Military – sites sponsored by branches or agencies of the armed services
- Political Organizations – sites sponsored by or providing information about political parties and interest groups focused on elections or legislation
- Health
- Information Technology
- Search Engines and Portals – for example, sites that support searching the web, newspapers and social networks
- Web-based E-mail – sites that host web-based e-mail
- Job Search
- Militancy and Extremist
- News and Media
- Racism and Hate
- Religion
- Shopping
- Professional andWorker Organizations
- Society and Lifestyles
- Hobbies
- Personals and Dating
- Sports
- Travel
- Vehicles
- Violence
- Weapons.

Consider how many of those listed above you may visit when studying, at business or at home. It will be apparent that if an employer wishes, they can block virtually every site. I know of some organizations in the UK that block access to all news sites and have worked in an organization that even blocked access to search engines such as Google and web mail such as Hotmail and Yahoo! Mail. When search engines are blocked, management-grade employees are likely to be restricted in their understanding of the business environment and are restricted from self-development! Employees are likely to view negatively an employer who does not trust them to use their time judiciously.

The popularity of different methods of monitoring and blocking are shown in *Figure 11.23*.

Employee monitoring legislation

Although employee monitoring falls within the remit of European data protection law, the Data Protection Act was not originally devised to cover employee monitoring. To help clarify the law on employee monitoring in the UK, in June 2003, the Office of the Information Commissioner published ‘Monitoring at Work’, the third part of the Employment Practices Data Protection Code. The code provides practical guidance for employers on how they should approach monitoring of employees in the workplace. These guidelines seek to achieve a balance between employees’ wishes for privacy and the need for employers to run their businesses efficiently. The code does not prevent monitoring, but is based on the concept of proportionality. Proportionality means that any adverse impacts from monitoring must be justified by the benefits to the employer and others. This addresses an apparent anomaly in that data protection law refers to individual consent for processing of personal data being ‘freely given’ and it is not normal for employees to give this consent. The code makes it clear that individual consent is not required provided that an organization has undertaken an ‘**impact assessment**’ of monitoring activities.

According to the code, an impact assessment involves:

- *identifying clearly the* ***purpose(s)*** *behind the monitoring arrangement and the benefits it is* *likely to deliver*

- *identifying any likely **adverse impact** of the monitoring arrangement*
- *considering **alternatives** to monitoring or different ways in which it might be carried out*
- *taking into account the **obligations** that arise from monitoring*
- *judging whether monitoring is **justified**.*

The code does not make specific recommendations about monitoring of e-mails or web traffic, but it does refer to them as typical monitoring activities which it suggests may be acceptable if staff are informed of them and an impact assessment has been conducted. The code does ask employers to consider whether alternatives may be better than systematic monitoring. Alternatives may include training or clear communication from managers and analysis of stored e-mails where it is thought an infringement has taken place rather than continuous monitoring. For example, automated monitoring is preferred to IT staff viewing personal e-mails of staff. The code also makes clear that the company should not undertake any **covert monitoring**; so it should be open about all the types of monitoring that occur. In universities, as mentioned above, at log-in, or in computer labs and libraries there is often a notice about 'acceptable-use policy'. This will describe the types of material it is not acceptable to access and is also a means of explaining monitoring procedures. It does appear, that if an employee was disciplined or dismissed for sending too many personal e-mails for instance, they would have legitimate grounds to appeal if they had not been informed that monitoring was occurring and their managers had not made it clear that this was acceptable practice.

Other European countries have different laws on monitoring. Some such as Germany are much more restrictive than the UK in terms of the level of monitoring that organizations are able to perform. Organizations opening offices abroad clearly need to be aware of local variations in legal constraints on employee monitoring and data protection.

E-mail management

E-mail is now an essential business communication tool and is also widely used for personal use. The popularity of e-mail as a communication tool has resulted in billions of messages being sent each day. For the individual, managing these communications in their e-mail inbox is rapidly becoming impossible! For the information services manager and indeed any business manager, there are three main controls that need to be considered to reduce the amount of time effectively wasted by staff reading e-mail. Controls can be introduced as part of an e-mail management policy to minimize the volume of:

1 Spam (unsolicited e-mail).

2 Internal business e-mail.

3 External business e-mail.

4 Personal e-mail (friends and family).

Despite the potential time loss through e-mail misuse an AMA (2003) survey suggested that only 34% of employers had a written e-mail retention and deletion policy in place. Furthermore, there are issues of legal liability about what employees say in their e-mail which also need to be considered.We will look at the risk and controls of each e-mail risk in turn.

1 Minimizing spam (unsolicited e-mail)

Spam is now a potential problem for every company and individual using the Internet. At the time of writing over 75% of e-mails were spam or virus-related in some countries and individuals whose inboxes are unprotected can receive hundreds of spam e-mails each day. The spammers rely on sending out millions of e-mails often from **botnets** of infected PCs in the hope that even if there is only a 0.01% response they may make some money, if not necessarily get rich.

Legal measures to combat spam have had limited success. So, many information services managers are now using a range of methods to control spam. *Figure 11.24* summarizes alternative techniques to combat spam. *Figure 11.24(a)* is the original situation where all mail is allowed into an inbox. *Figure 11.23(b)* uses different techniques to reduce the volume of e-mail through identification and blocking of spam. *Figure 11.24(c)* is a closed inbox where only known, trusted e-mails are allowed into an organization.

The full range of techniques that can be used in combination to combat spam include:

1 *Avoid harvesting of addresses*. Spammers harvest e-mails from e-mail addresses published on web pages and even the program code used to convert online form content to an e-mail to a company. By reducing the number of e-mail addresses published, or changing their format, the number of e-mail addresses can be reduced.

2 *Educate staff not to reply to spam*. The worst thing an individual can do on receiving spam is to reply to it to complain or to attempt to unsubscribe. This merely confirms to the spammer that the address is valid and they are likely to send more junk e-mail and sell your address on to other spammers. In Microsoft Outlook images are not enabled since downloading images in an HTML e-mail is a sign to spammers that yours is a valid address.

3 *Use filters*. Filtering software can identify spam from key words and phrases such as 'For Free', 'Sex' or 'Viagra' contained in the subject line, from address and body copy of the e-mail. **E-mail filters** are provided for users of web-based e-mail such as Hotmail and

Yahoo! Mail with e-mails placed in a junk mail folder. Microsoft Outlook Express has its own filter. Filtering software such asMailwasher (www.mailwasher.net),Mcaffee Spamkiller (www.mcaffee.com) can also be installed. Unfortunately, many spammers know how to avoid the keywords in the filters. The problem with filters and other services is that there can be ‘false positives’ or valid e-mails that are classified as junk. Additionally, spammers find ways to work around filters by putting ‘gobbeldy gook’ in the footer of their messages that is not recognized by the filters or using variants of words such as V1agra, or Via-gra. Review of these may still be necessary. This technique is represented by *Figure 11.24(b)*.

4 *Use ‘peer-to-peer’ blocking services*. These take advantage of humans being good at identifying spam and then notifying a central server which keeps an index of all spam. CloudMark (www.cloudmark.com), a peer-to-peer solution, requires users to identify spam by pressing a ‘Block’ button in Outlook Express which then updates a central server, so when others download the same message at a later time, it is automatically identified as spam. This technique is represented by *Figure 11.24(b)*.

5 *Use blacklist services*. **Blacklists** are lists of known spammers such as those reported to Spamhaus Project (www.spamhaus.com) or SpamCop (www.spamcop.net). They are often used in conjunction with filters to block e-mails. One of the most widely used systems developed by Brightmail (www.brightmail.com) uses a global network of e-mail addresses set up to trap and identify spam. Brightmail is increasingly used by ISPs such as BT OpenWorld to block spam, but it is not a cheap service, costing $5 to $15 per year. This price could easily be justified by the time staff save over the year. This technique is also represented by *Figure 11.24(b)*.

6 *Use whitelist services*. The **whitelist** approach has not been adopted widely since it is difficult to set up, but it probably offers the best opportunity for the future. An increasing problem for companies using e-mail for marketing is ‘false positives’ – where filters identify their legitimate e-mail as spam.Whitelist services are one solution to this. A whitelist gives a list of bona fide e-mail addresses that are likely to want to contact people within an organization. It will include all employees, partners, customers and suppliers who have obtained opt-in from employees to receive e-mail. E-mail from anyone not on the list will be blocked. However, maintaining such as list will require new software and new procedures for keeping it up-to-date. One approach that has been developed in the US is the concept of a ‘bonded sender’ developed by Ironport (www.bondedsender.com). Senders of opt-in e-mail post a financial bond to prove they are a reputable company. Another service rapidly gaining acceptance is Habeas (www.habeas.com) where special text (a ‘warrant mark’) is sent in outbound mail, which allows filtering systems to identify the e-mail as ‘not spam’. This technique is represented by *Figure 11.24(c)*.

Providers such as Sendmail (www.sendmail.com), GoodMail (www.goodmail.com) and the Yahoo!-sponsored DomainKeys and Microsoft-sponsored Sender Policy Framework have developed ‘sender authentication technology’which allows organizations to verify the source of a message before accepting it by automatically checking if it came from where it claims it did.

A further approach is **challenge/respond**. Here, if a message is received from a person who is not on the whitelist, a message is sent to that person requesting that they click on a link to verify that they are a genuine person and not a spammer (spammers would not have time to verify all addresses since it cannot be done automatically). Of course, this presents a problem for legitimate commercial e-mail marketers.

7 *Ensure anti-virus software and blocking is effective*. E-mail viruses are increasingly perpetrated by spammers since they are a method of harvesting e-mail addresses. Virus protection needs to be updated daily with new signatures if addresses are not to be captured through viruses.

2 Minimizing internal business e-mail

The ease and low cost of sending e-mails to a distribution list or copying people in on a message can lead to each person in an organization receiving many messages each day from colleagues within the organization. This problem tends to be worse in large organizations, simply because each individual has a larger address book of colleagues.

A press release from the British Computer Society summarizing research conducted by the Henley Management College released on 20 December 2002 suggested that a lot of time is wasted by managers when processing irrelevant e-mails. It suggested that ‘UK management is now suffering acute stress from “Information Overload”’ with executives, ‘complaining of being deluged by e-mail that demands a daily average of two hours of executive time’; particularly frustrating is that nearly a third of e-mail received is deemed to be irrelevant and much is rated of poor quality. Further findings included:

- Of seven common management tasks, meetings took up 2.8 hours on average, dealing with e-mail came second with an average of 1.7 hours and accessing information from the Internet accounted for a further 0.75 hour.
- Respondents reported receiving on average 52 e-mails per day while 7 per cent received

100 e-mails per day or more.

- Managers reported that less than half of e-mails (42 per cent) warranted a response, 35 per cent were read for information only and nearly a quarter were deleted immediately. On average only 30 per cent of e-mails were classified as essential, 37 per cent as important and 33 per cent as irrelevant or unnecessary.
- Despite the reservations about the quality and volume of e-mails received the majority of respondents (81 per cent) regarded e-mail as the communications technology which has had the most positive impact on the way they carried out their job, alongside the Internet and the mobile phone.

To overcome this type of business e-mail overuse, companies are starting to develop e-mail policies which explain best practice. For example, considering the way that the authors of Chaffey andWood (2005) use their e-mail, we quickly devised these guidelines:

- Only send the e-mail to employees for which it is essential to inform or act upon;
- Banning certain types of e-mails, such as the classic 'e-mail to the person who sits next to you' or individuals in the same office (although there are strong arguments for this since e-mail is an asynchronous medium and colleagues are not always available or don't wish to be disturbed);
- Avoid 'flaming' – these are aggressive e-mails which often put voice to feelings that wouldn't be said face-to-face. If you receive an annoying e-mail it is best to wait 10 minutes to cool down rather than 'flaming' the sender;
- Avoid 'trolls' – these are a species of e-mail closely related to flame-mails. They are postings to a newsgroup deliberately posted to 'wind up' the recipient. They are best ignored;
- Combine items from separate e-mails during the day or week into a single e-mail for the day/week;
- Write clear subject lines;
- Structure e-mails so that they can be scanned quickly using sub-heads and numbered and bulleted lists;
- Make follow-up actions clear;
- When reading e-mail, use folders to categorize e-mails according to content and priority;
- Perform e-mail reading and checking in batches, e.g. once per morning or afternoon rather than being alerted to and opening every e-mail that arrives;
- Delete e-mails which are not required for future reference (large volumes are taken up on servers through staff not deleting e-mails and their attachments);
- And so on – all common-sense guidelines, but often common sense isn't common!

3 Minimizing external business e-mail

As well as spam which is unsolicited and usually untargeted, people within an organization can also receive many e-mails from legitimate suppliers. For example, an IT manager might receive e-mails from hardware and software manufacturers, service providers, event or conference organizers and e-newsletters from magazines. These sources of e-mail are not usually controlled through company e-mail policies; it is usually left to the judgement of the individual employee to select appropriate e-newsletters. The technologies to block e-mails, such as spam filters, will not usually block such messages, but primitive filters may, if they block words such as 'Offer' or 'Free' which also appear in legitimate business e-mails. The challenge/respond system will still enable such e-mails to be received. Additionally, technology described in *Chapter 12* is available to block access to certain web sites such as news or entertainment sites, and this software renders e-newsletters less effective since images are not downloaded from blocked sites. An approach used by many individuals to help control information from these sources is to use a separate e-mail address from the main inbox when opting in. This could be a Hotmail or Yahoo! Mail address and this form of e-newsletter can be read at the office or at home and is also available when the individual changes jobs.

4 Minimizing personal e-mail (friends and family)

Although there are many surveys about the volume of spam and amount of time spent processing e-mail at work, there is relatively little data published on the amount of time spent writing personal e-mails. Most of it is not independent; it is commissioned by vendors of software for monitoring e-mail use. However, using e-mail for personal use is going to occur if there are no measures to stop it.

To minimize this problem and some of the problems of over-using e-mail for business use, the following steps can be taken:

1 Create written guidelines defining the policy on acceptable e-mail use and disciplinary procedures for when guidelines are breached;

2 Use increasing levels of control or sanctions for breaches including performance reviews, verbal warnings, removal of e-mail privileges, termination and legal action;

3 Providing training for staff on acceptable and efficient e-mail use;

4 Monitor e-mails for signatures of personal use and any breaches of the policy, e.g. swearing, and take action accordingly.

Hacking

‘**Hacking**’ refers to the process of gaining unauthorized access to computer systems, typically across a network. Hacking can take different forms. Hacking for monetary gain is usually aimed at identity theft where personal details and credit card details are accessed for the purpose of fraud. Hacking could also occur with malicious intent. For example, a former employee might gain access to a network with a view to deleting files or passing information on to a competitor. Some of the notorious hackers who have been prosecuted, but often seem to have ultimately gained from their misdemeanours, are:

- *Robert Morris* – The son of the chief scientist at the US National Computer Security Center, this graduate student created a destructive Internet worm in 1988 which took advantage of a security flaw in the Unix operating system.When unleashed it caused thousands of computers to crash. The disruption was partly accidental and he released instructions to system administrators on how to resolve the problem. He was sentenced to three years of probation, 400 hours of community service and a fine of $10,050. He is now an assistant professor at MIT, where he originally released his worm to disguise its creation at Cornell University.
- *Kevin Poulsen* – In 1990 Poulsen took over all telephone lines into the Los Angeles radio station KIIS-FM, assuring that he would be the 102nd caller. Poulsen won a Porsche 944 S2. This was one of many hacks conducted while he worked for hi-tech company SRI International by day and hacked at night. He was eventually traced and, in June 1994, he pleaded guilty to seven counts of mail, wire and computer fraud, money laundering and obstruction of justice, and was sentenced to 51 months in prison and ordered to pay $56,000 in restitution. It was the longest sentence ever given for hacking. He is now a computer security journalist.
- *KevinMitnick* – The first hacker to be featured on an FBI ‘Most wanted’ poster,Mitnick was arrested in 1995. He later pleaded guilty to four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication.He admitted that he broke into computer systems and stole proprietary software belonging toMotorola, Novell, Fujitsu, Sun Microsystems and other companies. He was sentenced to 46 months. Following his sentence he became a security consultant and is now a leading commentator on security and has made many TV appearances and written books and articles.
- *Vladimir Levin* – A graduate mathematician who was part of a Russian gang that reputedly masterminded a $10 million fraud of Citibank. Arrested by Interpol at London’s Heathrow Airport in 1995.
- *Alexey Ivanov* – A June 2001 indictment against Ivanov alleged that he gained unauthorized access into CTS Network Services, a San Diego-based Internet service provider. Ivanov allegedly used a stolen credit card number to open an account with CTS, and once inside the company’s computers hacked the systems to gain control of the computers. He then used CTS computers to launch a series of computer attacks against e-commerce companies, including two credit card processors – Sterling Microsystems of Anaheim and Transmark of Rancho Cucamonga – and NaraBank of Los Angeles. Ivanov allegedly stole customer financial information, such as credit card and bank account numbers, leading to fraud of $25 million. A prison sentence of three years was given.

Hacking may not be directly related to theft or damage, but gaining access to a system may be perceived by the hacker as a technical challenge. The term‘hacking’ traditionally refers to the process of creating program code, another form of technical challenge. This can almost be considered as a pastime, albeit an unethical one.While not as popular as watching sports, hacking appears to be more than one or two people in each country. BBC (2003) reports that TruSecure, a US hacking monitoring organization, currently tracks more than 11,000 individuals in about 900 different hacking groups and gangs.

Three main forms of gaining unauthorized access to computer systems can be identified. First, the normal entry points to systems through usernames and passwords can be used. For example, many system log-ins have a username of ‘administrator’ by default. Sometimes the password will be the same. Other common passwords are days of the week or children’s names. Tools are available to try different alternative log-ins, although most modern systems will refuse access after several attempts. Hacking can be combined with identity theft to gain an idea of the passwords used.

The second form of hacking exploits known vulnerabilities in systems. Although these vulnerabilities in operating systems such as Windows or Linux or web browsers such as Internet Explorer are publicly known and will be posted on the vendor’s web site and specialist security web sites, there will be many system administrators who have not updated their systems with the latest security update or ‘patch’. This is partly because there are so many security vulnerabilities, with new ones being announced every week.

Thirdly, Kevin Mitnick refers to ‘**social engineering**’ which typically involves impersonating employees of an organization to access security details. One example of this, given in Mitnick and Simon (2002), is when the attacker contacts a new employee and advises them of the need to comply with security policies. The attacker then asks the user for their password to check it is in line with the policy of choosing a difficult-to-guess password. Once the user reveals their password, the caller makes recommendations to construct future passwords in such a way that the attacker will be able to guess them.

Protecting computer systems against hackers

Protecting computer systems against hackers involves creating counter-measures to the three main types of hacking outlined above. For gaining access to systems via passwords, policies can be developed to reduce the risk of access. One simple approach is to mandate that new passwords are required every month and that they contain at least one number and a mix of upper and lower case. This prevents users using simple passwords which are easily guessed. Education is required to reduce the risk of passwords falsely obtained through 'social engineering', but this will never completely remove the threat.

Computer systems can also be protected by limiting access at the point the external network enters the company. **Firewalls** are essential to prevent outside access to confidential company information, particularly where an extranet has been set up. Firewalls are usually created as software mounted on a separate server at the point where the company is connected to the Internet. Firewall software can then be configured to only accept links from trusted domains representing other offices in the company.

Measures must also be put in place to stop access to systems through published security vulnerabilities. BBC (2003) reported that in 2003 there were 5,500 security vulnerabilities that could be used. A policy on updating operating systems and other software with the latest versions is also required. It is not practical to make all updates, but new vulnerabilities must be monitored and patches applied to the highest-risk categories. This is a specialist task and is often outsourced. TruSecure **(**www.trusecure.com**)** is an example of a specialist company that monitors security vulnerabilities and advises organizations on prevention. TruSecure estimates that only 80 or 90 per cent of vulnerabilities are being used regularly, so patches should prioritize on these. TruSecure provides a service for hundreds of organizations to see whether they possess these vulnerabilities. They also employ a team of people who attempt to infiltrate hacker groups to determine the latest techniques. TruSecure gave the FBI over 200 documents about the 'Melissa' virus author. Although they did not know his real name, they knew his three aliases and had built a detailed profile of him.

A further approach organizations use to check their defences against hacking is to employ '**ethical hackers**'. These are former hackers who now apply their skills to test the vulnerabilities of existing systems.

Although all of the examples of hacking above involve computer network, sometimes 'low-tech' techniques can be used too. *Guardian* (2003) reported cases where criminals had impersonated call-centre staff in order to gain access to customer accounts!

Secure e-commerce transactions

For e-businesses offering online sales there are also additional security risks from the customer or merchant perspective:

(a) Transaction or credit card details stolen in transit.

(b) Customer's credit card details stolen from merchant's server.

(c) Merchant or customer is not who they claim to be.

In this section we assess the measures that can be taken to reduce the risk of these breaches of e-commerce security. We start by reviewing some of the theory of online security and then review the techniques used.

Principles of secure systems

Before we look at the principle of secure systems, it is worth reviewing the standard terminology for the different parties involved in the transaction:

♉ *Purchasers*. These are the consumers buying the goods.

♉ *Merchants*. These are the retailers.

♉ *Certification authority (CA)*. This is a body that issues digital certificates that confirm the identity of purchasers and merchants.

♉ *Banks*. These are traditional banks.

♉ *Electronic token issuer*. A virtual bank that issues digital currency.

The basic requirements for security systems from these different parties to the transaction are as follows:

1 *Authentication* – are parties to the transaction who they claim to be (risk (c) above)?

2 *Privacy and confidentiality* – are transaction data protected? The consumer may want to make an anonymous purchase. Are all non-essential traces of a transaction removed from the public network and all intermediary records eliminated (risks (b) and (c) above)?

3 *Integrity* – checks that the message sent is complete, i.e. that it is not corrupted.

4 *Non-repudiability* – ensures sender cannot deny sending message.

5 *Availability* – how can threats to the continuity and performance of the systembe eliminated?

Kesh *et al*. (2002) explore the security requirements for e-commerce in more detail.

Approaches to developing secure systems

Digital certificates

There are two main methods of encryption using **digital certificates**.

1 Secret-key (symmetric) encryption

Symmetric encryption involves both parties having an identical (shared) key that is known only to them. Only this key can be used to encrypt and decrypt messages. The secret key has to be passed from one party to the other before use in much the same way as a copy of a secure attaché case key would have to be sent to a receiver of information. This approach has traditionally been used to achieve security between two separate parties, such as major companies conducting EDI. Here the private key is sent out electronically or by courier to ensure it is not copied.

This method is not practical for general e-commerce, as it would not be safe for a purchaser to give a secret key to a merchant since control of it would be lost and it could not then be used for other purposes. A merchant would also have to manage many customer keys.

2 Public-key (asymmetric) encryption

Asymmetric encryption is so called since the keys used by the sender and receiver of information are different. The two keys are related by a numerical code, so only the pair of keys can be used in combination to encrypt and decrypt information. *Figure 11.25* shows how public-key encryption works in an e-commerce context. A customer can place an order with a merchant by automatically looking up the public key of the merchant and then using this key to encrypt the message containing their order. The scrambled message is then sent across the Internet and on receipt by the merchant is read using the merchant's private key. In this way only the merchant who has the only copy of the private key can read the order. In the reverse case the merchant could confirm the customer's identity by reading identity information such as a digital signature encrypted with the private key of the customer using their public key.

Pretty Good Privacy (PGP) is a public-key encryption system used to encrypt e-mail messages.

Digital signatures

Digital signatures can be used to create commercial systems by using public key encryption to achieve authentication: the merchant and purchaser can prove they are genuine. The purchaser's digital signature is encrypted before sending a message using their private key and, on receipt, the public key of the purchaser is used to decrypt the digital signature. This proves the customer is genuine. Digital signatures are not widely used currently due to the difficulty of setting up transactions, but they will become more widespread as the public-key infrastructure (PKI) stabilizes and use of certificate authorities increases.

The public-key infrastructure (PKI) and certificate authorities (CAs)

In order for digital signatures and public-key encryption to be effective it is necessary to be sure that the public key intended for decryption of a document actually belongs to the person you believe is sending you the document. The developing solution to this problem is the issuance by a trusted third party (TTP) of a message containing owner identification information and a copy of the public key of that person. The TTPs are usually referred to as '**certificate authorities**' **(CAs)**, and various bodies such as banks and the Post Office are likely to fulfil this role. That message is called a '**certificate**'. In reality, as asymmetric encryption is rather slow, it is often only a sample of the message that is encrypted and used as the representative digital signature.

Example certificate information could include:

- user identification data;
- issuing authority identification and digital signature;
- user's public key;
- expiry date of this certificate;
- class of certificate;
- digital identification code of this certificate.

It is proposed that different classes of certificates would exist according to the type of information contained. For example:

- name, e-mail address
- driver's licence, national insurance number, date of birth
- credit check
- organization-specific security clearance data.

Virtual private networks

A **virtual private network (VPN)** is a private wide-area network that runs over the public network, rather than a more expensive private network. The technique by which VPN operates is sometimes referred to as 'tunnelling', and involves encrypting both packet headers and content using a secure form of the Internet Protocol known as IPSec. As explained in *Chapter 3*, VPNs enable the global organization to conduct its business securely, but using the public Internet rather than more expensive proprietary systems.

Current approaches to e-commerce security

In this section we review the approaches used by e-commerce sites to achieve security using the techniques described above.

Secure Sockets Layer Protocol (SSL)

SSL is a security protocol, originally developed by Netscape, but now supported by all browsers such as Microsoft Internet Explorer. SSL is used in the majority of B2C e-commerce transactions since it is easy for the customer to use without the need to download additional software or a certificate.

When a customer enters a secure checkout area of an e-commerce site SSL is used and the customer is prompted that ‘you are about to view information over a secure connection’ and a key symbol is used to denote this security.When encryption is occurring they will see that the web address prefix in the browser changes from ‘http://’ to ‘https://’ and a padlock appears at the bottom of the browser window.

How does SSL relate to the different security concepts described above? The main facilities it provides are security and confidentiality. SSL enables a private link to be set up between customer and merchant. Encryption is used to scramble the details of an e-commerce transaction as it is passed between sender and receiver and also when the details are held on the computers at each end. It would require a determined attempt to intercept such a message and decrypt it. SSL is more widely used than the rival S-HTTP method.

The detailed stages of SSL are as follows:

1 Client browser sends request for a secure connection.

2 Server responds with a digital certificate which is sent for authentication.

3 Client and server negotiate session keys, which are symmetrical keys used only for the duration of the transaction.

Since, with enough computing power, time and motivation, it is possible to decrypt messages encrypted using SSL,much effort is being put into finding more secure methods of encryption such as **SET**. From a merchant’s point of view there is also the problem that authentication of the customer is not possible without resorting to other methods such as credit checks.

Certificate authorities (CAs)

For secure e-commerce, there is a requirement for the management of the vast number of public keys. This management involves procedures and protocols necesssary throughout the lifetime of a key – generation, dissemination, revocation and change – together with the administrative functions of time/date stamping and archiving. The successful establishment of a CA is an immense challenge of trust building and complex management. There are two opposing views on how that challenge should be met:

- *Decentralized*: market-driven, creating brand-name-based ‘islands of trust’ such as the Consumers Association. There is a practical need for a local physical office to present certificates of attestable value, e.g. passports, drivers’ licences. Banks and the Post Office have a huge advantage.
- *Centralized*: in the UK, the Department of Trade and Industry (DTI) has proposed a hierarchical tree leading ultimately to the government.

The best-known commercial CA is Verisign (www.verisign.com) and this is commonly used for merchant verification. For example, the Avon site uses Verisign to prove to its customers that it is the genuine site. Post Offices and telecommunications suppliers are also acting as CAs. Examples in the UK include BT (TrustWise) and the Post Office (ViaCode).

Reassuring the customer

Once the security measures are in place, content on the merchant’s site can be used to reassure the customer, for example Amazon (www.amazon.com) takes customer fears about security seriously, judging by the prominence and amount of content it devotes to this issue. Some of the approaches used indicate good practice in allaying customers’ fears. These include:

- use of customer guarantee to safeguard purchase;
- clear explanation of SSL security measures used;
- highlighting the rarity of fraud (‘ten million customers have shopped safely without credit card fraud’);
- the use of alternative ordering mechanisms such as phone or fax;
- the prominence of information to allay fears – the guarantee is one of themainmenu options.

Companies can also use independent third parties that set guidelines for online privacy and security. The best-known international bodies are TRUSTe **(**www.truste.org**)** and Verisign for payment authentication **(**www.verisign.com**)**.Within particular countries there may be other bodies such as, in the UK, ISIS or Internet Shopping is Safe scheme (http://isis.imrg.org)

Managing e-business applications infrastructure

Management of the **e-business applications infrastructure** concerns delivering the right applications to all users of e-business services. The issue involved is one that has long been a concern of IS managers, namely to deliver access to integrated applications and data that are available across the whole company. Traditionally businesses have developed applications silos or islands of information, as depicted in *Figure 3.17(a)*. This shows that these silos may develop at three different levels: (1) there may be different technology architectures used in different functional areas, giving rise to the problems discussed in the previous section, (2) there will also be different applications and separate databases in different areas and (3) processes or activities followed in the different functional areas may also be different.

These applications silos are often a result of decentralization or poorly controlled investment in information systems, with different departmental managers selecting different systems from different vendors. This is inefficient in that it will often cost more to purchase applications from separate vendors, and also it will be more costly to support and upgrade. Even worse is that such a fragmented approach stifles decision making and leads to isolation between functional units. An operational example of the problems this may cause is if a customer phones a B2B company for the status of a bespoke item they have ordered, where the person in customer support may have access to their personal details but not the status of their job, which is stored on a separate information system in the manufacturing unit. Problems can also occur at tactical and strategic levels. For example, if a company is trying to analyse the financial contribution of customers, perhaps to calculate lifetime values, some information about customers' purchases may be stored in a marketing information system, while the payments data will be stored in a separate system within the finance department. It may prove difficult or impossible to reconcile these different data sets.

To avoid the problems of a fragmented applications infrastructure, companies attempted throughout the 1990s to achieve the more integrated position shown in *Figure 3.17(b)*. Here the technology architecture, applications, data architecture and process architecture are uniform and integrated across the organization. To achieve this many companies turned to **enterprise resource planning (ERP)** vendors such as SAP, Baan, PeopleSoft and Oracle.

The approach of integrating different applications through ERP is entirely consistent with the principle of e-business, since e-business applications must facilitate the integration of the whole *supply chain* and *value chain*. It is noteworthy that many of the ERP vendors such as SAP have repositioned themselves as suppliers of e-business solutions! The difficulty for those managing e-business infrastructure is that there is not, and probably never can be, a single solution of components from a single supplier. For example, to gain competitive edge, companies may need to turn to solutions from innovators who, for example, support new channels such as WAP, or provide knowledge management solutions or sales management solutions. If these are not available from their favoured current supplier, do they wait until these components become available or do they attempt to integrate new software into the application? Thus managers are faced with a precarious balancing act between standardization or core product and integrating innovative systems where applicable. *Figure 3.18* (illustrates this dilemma. It shows how different types of applications tend to have strengths in different areas. ERP systems were originally focused on achieving integration at the operational level of an organization. Solutions for other applications such as business intelligence in the form of data warehousing and data mining tended to focus on tactical decision making based on accessing the operational data from within ERP systems. Knowledge management software (*Chapter 10*) also tends to cut across different levels of management. *Figure 3.18* only shows some types of applications, but it shows the trial of strength between the monolithic ERP applications and more specialist applications looking to provide the same functionality.

In this section we have introduced some of the issues of managing e-business infrastructure. These are examined in more detail later in the book. *Figure 3.19* summarizes some of these management issues and is based on the layered architecture introduced at the start of this section with applications infrastructure at the top and technology infrastructure towards the bottom.

Focus on web service and service and service-oriented,

'**Web services**' or 'software as a service (SaaS)' refers to a highly significant model for managing software and data within the e-business age. The web services model involves managing and performing all types of business processes and activities through accessing web-based services rather than running a traditional executable application on the processor of your local computer.

Benefits of web services or SaaS

SaaS are usually paid for on a subscription basis, so can potentially be switched on and off or payments paid according to usage, hence they are also known as 'on demand'. The main business benefit of these systems is that installation and maintenance costs such as upgrades are effectively outsourced. Cost savings are made on both the server and client sides, since the server software and databases are hosted externally and client applications software is usually delivered through a web browser or a simple application that is downloaded via the web.

In research conducted in the US and Canada by Computer Economics (2006), 91% of companies showed a first-year return on investment (ROI) from SaaS. Of these, 57% of the total had economic benefits which exceeded the SaaS costs and 37% broke even in year one. The same survey showed that in 80% of cases, the total cost of ownership (TCO) came in either on budget or lower. There would be few cases of traditional applications where these figures can be equalled.

Challenges of deploying SaaS

Although the cost reduction arguments of SaaS are persuasive, what are the disadvantages of this approach? The pros and cons are similar to the 'make or buy' decision discussed in *Chapter 12*. SaaS will obviously have less capability for tailoring to exact business needs than a bespoke system.

The most obvious disadvantage of using SaaS is dependence on a third party to deliver services over the web, which has these potential problems:

- Downtime or poor availability if the network connection or server hosting the application or server fails.
- Lower performance than a local database. You know from using Gmail or Hotmail that although responsive, they cannot be as responsive as using a local e-mail package like Outlook.
- Reduce data security since traditionally data would be backed up locally by in-house IT staff (ideally also off-site). Since failures in the system are inevitable, companies using SaaS need to be clear how backup and restores are managed and the support that is available for handling problems which is defined within the SLA.
- Data protection – since customer data may be stored in a different location it is essential that it is sufficiently secure consistent with the data protection and privacy laws discussed in *Chapter 4*.

You can see that there are several potential problems which need to be evaluated on a caseby-case basis when selecting SaaS providers. Disaster recovery procedures are particularly important since many SaaS applications such as customer relationship management and supply chain management are mission-critical.Managers need to question service levels since often services are delivered to multiple customers from a single server in a **multi-tenancy** arrangement rather than a **single-tenancy** arrangement. This is similar to the situation with the shared server or dedicated server we discussed earlier for web hosting. An example of this in practice is shown in *Box 3.9*.

An example of a consumer SaaS, word processing, would involve visiting a web site which hosts the application rather than running a word processor such as Microsoft Word on your local computer through starting 'Word.exe'. The best-known consumer service for online word processing and spreadsheet use is Google Docs (http://docs.google.com) which was launched following the purchase in 2006 by Google of start-up Writely (www.writely.com). Google Docs also enables users to view and edit documents offline, through Google Gears, an open source browser extension. 'Microsoft Office Live' is a similar initiative from Microsoft.

As an indication of the transformations possible through web services see *Figure 3.20* which shows how Google's mission to 'manage the World's information' also applies to supporting organizational processes. Google Apps enables organizations to manage many of their activities. The basic service is free with the Premier Edition which includes more storage space and security being $50 per user account per year.

A related concept to web services is **utility computing**. Utility computing involves treating all aspects of IT as a commodity service such as water, gas or electricity where payment is according to usage. A subscription is usually charged per month according to the number of features, number of users, volume of data storage or bandwidth consumed. Discounts will be given for longer-term contracts. This includes not only software which may be used on a pay-per-use basis, but also using hardware, for example for hosting. An earlier term is **'applications service providers' (ASP)** which is less widely used now.

Figure 3.21 shows one of the largest SaaS or utility providers Salesforce.com where customers pay from £5 to £50 per user per month according to the facilities used. The service is delivered from the Salesforce.com servers to over 50,000 customers in 15 local languages.

In descriptions of web services you may hear confusingly, that they access ‘the cloud’ or the term ‘**cloud computing**’, where the cloud referred to is the Internet (networks are often denoted as clouds on diagrams of network topology). So for example, if you are accessing your Google Docs then they will be stored somewhere ‘in the cloud’ without any knowledge of where it is or how it is managed since Google stores data on many servers. And of course you can access the document from any location. But there are issues to consider about data stored and served from the cloud: ‘is it secure, is it backed up, is it always available?’. The size of Google’s cloud is indicated by Pandia (2007) which estimated that Google has over 1 million servers running the open-source Linux software.

Think of examples of web services that you or businesses use, and you will soon see how important they are for both personal and business applications. Examples include:

- Web mail readers
- E-commerce account and purchasing management facilities such as Amazon.com
- Many services from Google such as Google Maps, GMail, Picasa and Google Analytics
- Customer relationship management applications from Salesforce.com and Siebel/Oracle
- Supply chain management solutions from SAP, Oracle and Covisint
- E-mail and web security management from companies like MessageLabs.

From the point of view of managing IT infrastructure these changes are dramatic since traditionally companies have employed their own information systems support staff to manage different types of business applications such as e-mail. A web service provider offers an alternative where the application is hosted remotely or off-site on a server operated by an ASP. Costs associated with upgrading and configuring new software on users’ client computers and servers are dramatically decreased.

Virtualization

Virtualization is another approach to managing IT resource more effectively. However, it is mainly deployed within an organization. VMware was one of the forerunners offering virtualization services which it explains as follows (VMware, 2008):

> *The VMware approach to virtualization inserts a thin layer of software directly on the computer hardware or on a host operating system. This software layer creates virtual machines and contains a virtual machine monitor or ‘hypervisor’ that allocates hardware resources dynamically and transparently so that multiple operating systems can run concurrently on a single physical computer without even knowing it.*
>
> *However, virtualizing a single physical computer is just the beginning. VMware offers a robust virtualization platform that can scale across hundreds of interconnected physical computers and storage devices to form an entire virtual infrastructure.*

They go on to explain that virtualization essentially lets one computer do the job of multiple computers, by sharing the resources of a single computer across multiple environments. Virtual servers and virtual desktops let you host multiple operating systems and multiple applications.

So virtualization has these benefits:

- Lower hardware costs through consolidation of servers (see mini case below)
- Lower maintenance and support costs
- Lower energy costs
- Scalability to add more resource more easily
- Standardized, peronalized desktops can be accessed fromany location, so users are not tied to an individual physical computer
- Improved business continuity.

The mini case study gives an example of these benefits.

Service-oriented architecture (SOA)

The technical architecture used to build web services is formally known as a ‘**serviceoriented architecture**’. This is an arrangement of software processes or agents which communicate with each other to deliver the business requirements.

The main role of a service within SOA is to provide functionality. This is provided by three characteristics:

1 An interface with the service which is platform-independent (not dependent on a particular type of software or hardware). The interface is accessible through applications development approaches such asMicrosoft .Net or Java and accessed through protocols such as SOAP (Simple Object Access Protocol) which is used for XML-formatted messages, i.e. instructions and returned results to be exchanged between services.

2 The service can be dynamically located and invoked. One service can query for the existence of another service through a service directory – for example an e-commerce service could query for the existence of a credit card authorization service.

3 The service is self-contained. That is, the service cannot be influenced by other services; rather it will return a required result to a request from another service, but will not change state. Within web services, messages and data are typically exchanged between services using XML.

Mini Case Study 3.5

The Association of Teachers and Lecturers (ATL) is using virtualization to not only cut hardware costs, but also to recover quickly from systems failures and maintain business continuity. The Association of Teachers and Lecturers is an independent, registered trade union and professional association representing approximately 160,000 teachers, lecturers and support staff in maintained and independent nurseries, schools, sixth forms, and tertiary and further education colleges in the UK.

Ann Raimondo, head of information technology at ATL, is responsible for managing the IT infrastructure for the ever-expanding organization, including deploying equipment, IT support and training for its 150 employees. In addition to offices in London, Belfast and Cardiff, the ATL has a large volunteer base of remote workers throughout the UK who require IT systems and support. In her role, Raimondo was faced with the following challenges:

- Fifty per cent of the available server storage space was not utilized
- Seventy-two per cent of the storage space purchased was not being used
- Storage space could not be reallocated to other systems in need of additional storage
- Data were physically bound to a server, so if corruption occurred to the operating system or applications, the data on physical drives could not be reattached easily to another server and would need to be restored from backup.

The implementation resulted in the following benefits:

- **Server consolidation**. ATL consolidated from 22 servers to 11, reducing hardware requirements and costs by 50 per cent.
- **Flexibility and responsiveness**. Prior to bringing in ESX Server, deploying a new server would require approximately three weeks for sourcing, ordering and implementing hardware. With VMware virtual infrastructure, this same process takes less than one hour.
- **Lowered the cost of disaster recovery**. The hardware independence of VMware virtual infrastructure helps mitigate failures caused by hardware and enables recovery from a disaster in a matter of minutes, matching and improving on user downtime expectations.

Source: VMware (2007)

Virtualization cuts costs and improves

The examples of web services we have given above all imply a user interacting with the web service. But with the correct business rules and models to follow, there is no need for human intervention and different applications and databases can communicate with each other in real time. A web service such as Kelkoo.com which was discussed in *Chapter 2* exchanges information with all participating merchants through XML using an SOA. The concept of the semantic web mentioned above and business applications of web services such as CRM, SCM and ebXML are also based on an SOA approach. In another e-business application example provided by the World Wide Web Consortium at www.w3.org/TR/soap12-part0/, a company travel booking system uses SOAP to communicate with a travel company to book a holiday.

EDI

Transactional e-commerce predates the World Wide Web and service-oriented architecture by some margin. In the 1960s, **electronic data interchange (EDI)**, **financial EDI** and **electronic funds transfer (EFT)** over secure private networks became established modes of intra- and inter-company transaction. In this section, we briefly cover EDI to give a historical context. The idea of standardized document exchange can be traced back to the 1948 Berlin Airlift, where a standard form was required for efficient management of items flown to Berlin from many locations. This was followed by electronic transmission in the 1960s in the US transport industries. The EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) standard was later produced by a joint United Nations/European committee to enable international trading. There is also a similar X12 EDI standard developed by the ANSI Accredited Standards Committee.

Clarke (1998) considers that EDI is best understood as the replacement of paper-based purchase orders with electronic equivalents, but its applications are wider than this. The types of documents exchanged by EDI include business transactions such as orders, invoices, delivery advice and payment instructions as part of EFT. There may also be pure information transactions such as a product specification, for example engineering drawings or price lists.

Clarke (1998) defines EDI as:

the exchange of documents in standardised electronic form, between organisations, in an automated manner, directly from a computer application in one organisation to an application in another.

DTI (2000) describes EDI as follows:

Electronic data interchange (EDI) is the computer-to-computer exchange of structured data, sent in a form that allows for automatic processing with no manual intervention. This is usually carried out over specialist EDI networks.

It is apparent from these definitions that EDI is one form, or a subset of, electronic commerce. A key point is that direct communication occurs between applications (rather than between computers). This requires information systems to achieve the data processing and data management associated with EDI and integration with associated information systems such as sales order processing and inventory control systems.

According to IDC (1999), revenues for EDI network services were already at $1.1 billion in 1999 and forecast to reach over $2 billion by 2003. EDI is developing through new standards and integration with Internet technologies to achieve **Internet EDI**. IDC (1999) predicted that Internet EDI's share of EDI revenues would climb from 12 per cent to 41 per cent over the same period.

Internet EDI enables EDI to be implemented at lower costs since, rather than using proprietary, so-called **value-added networks (VANs)**, it uses the same EDI standard documents, but using lower-cost transmission techniques through **virtual private networks (VPNs)** or the public Internet. Reported cost savings are up to 90 per cent (*EDI Insider*, 1996). *EDI Insider* estimated that this cost differential would cause an increase from the 80,000 companies in the United States using EDI in 1996 to hundreds of thousands. Internet EDI also includes EDIstructured documents being exchanged by e-mail or in a more automated form using FTP.

It is apparent that there is now a wide choice of technologies for managing electronic transactions between businesses. The Yankee Group (2002) refers to these as 'transaction management (TXM)' technologies which are used to automate machine-to-machine information exchange between organizations. These include:

document and data translation, transformation, routing, process management, Electronic data interchange (EDI), eXtensible Mark-up Language (XML), Web services ... Valueadded networks, electronic trading networks, and other hosted solutions are also tracked in the TXM market segment.

INTERNET SERVICE PROVIDER

An ISP (Internet Service Provider) is a company which provides internet access to other companies or individuals. An ISP maintains connections to other networks and ISPs, acting as a router for internet traffic between a customer's computer and any other machine also connected to the internet anywhere else in the world.

3.6 TYPES OF INTERNET SERVICE PROVIDER

Internet Service Provider is a company that you dial up to get on the Internet. There are basically four different kinds:

- National Companies That Offer Services through out the country.
  - Providers:
    - o BSNL
  - Pros:
    - o If you travel or move, most likely you will be able to access the Internet at your new location.
    - o The extra services like chat rooms can be an added bonus.
  - Cons:
    - o Technical support may be hard to reach or long distance.
    - o Sometimes you get busy signals when trying to access them.
    - o If you don't use the services, if there is an additional charge, it is a waste of money.
    - o Although you buy an unlimited account, some will send you notices if you have been online too much.
- Specialized Companies That Offer A Service Like Filtering
  - Providers:

o Reliance

o Airtel

o Dishnet DSL

o Satyam Infoways

o HCL Infinet

• Pros:

o You don't have to install additional software to get pornography out of your computer.

o You will not have to update your filtering software.

• Cons:

o In some cases roaming facility of account is not available.

o Technical support may be limited.

• **Local ISPs (Small companies that offer Internet service to a small area)**

• Providers:

o Check in your telephone directory or yellow pages under Internet Services.

• Pros:

o Less error prone

o Less disconnections

o Offers a local dial up number if you are in a rural area that doesn't have local dial up numbers for the major providers.

• Cons:

• They may be limited in their equipment to offer a good, fast internet speed.

• They may be limited in offering any web guidance.

• **Free ISPs**

• Providers:

o Call Tiger

- Pros:

  o Free and no commitment

  o Cons:

  o Technical support may be limited, long distance, or not available.

  o May not offer reliable service.

  o Advertising banner can take up a lot of space on your screen.

  o Some charge very high set up fees (stay away from these)

3.7 TYPES OF INTERNET SERVICE PROVIDER ACCOUNTS

There are many types of connections USER can get on the internet depending on the type of use and the amount of resources (money) available. The different types of connections, their advantages and limitations have been discussed below:

No matter what type of connection you go in for, it should be reliable, fast, easily available, and economical. There is no such thins as a free connection to the Internet. Someone, somewhere has to pay for the equipment, software, telephone lines, and electricity.

Basically there are four types of connections to the Internet:

1. Dial-up Connection

2. ISDN Connection

3. Leased Line Connection

4. Cable Modem

5. DSL

6. Broadband

7. V-SAT

The most popular type of connection for an individual is the broadband connection as it is easily available and economical.

1. Dial-Up Connection

As the name suggests, dial-up link means you have to dial into a modem over a telephone line before you can get connected to the internet. A modem (modulator demodulator) is a device which converts digital signals emitting from the computer into analog signals so that the data is easily transmitted over analog telephone lines. At the receiving end, there is another modem which converts these transmitted analog signals back to the digital form which are received by the target computer.

For this type of connection you require:

A computer whose configuration could be 80486 but the best is Pentium-IV or above. Communication software, like dialer which the Internet connection provider will give and a telephone line.

A modem (optimal speed is 36.6 Kbps). These days we use modems of speeds up to 56 Kbps. Software like a browser, e-mail programme, FTP software, Newsgroup reader, Eudora, Outlook Express, etc. Outlook Express is one of the software which helps to read news and mail offline once they have been collected online.

There are 3 major ways by which you can get linked to the Internet using a dial-up connection, namely;

A. Host terminal connection

B. Individual computer

C. Dial-Up or on demand through the LAN.

A. Host Terminal Connection (Terminal Emulation)

In case of host terminal connection, a PC is connected to some Internet host via modem and a terminal emulation programme is run. Your terminal now acts like a vt-100 terminal . In other words, you are connected to a large computer which is connected to the Internet. Thus if want to download a file, the file is downloaded to the host and not your computer. To download a file from their host to your computer you need to have some specific software. In this type of connection you can download only text but not graphics. Hence, a host terminal connection is also referred to as a shell account. This account is best suitable for :

1. Students whose budget is low and their requirement is limited to text.

2. Users who connect via Telnet programmes.

3. Users whose frequency to use the Internet is low.

4. Users who want to use the Internet to access the network of their workplace from their home place (personal account). Such users could connect via Telnet.

5. Jobs where multi-tasking is not required. This connection permits only one task at a time, e.g., the user cannot read the news as well as download a file.

This type of a connection offers three different types of accounts depending on your distance from the ISP and the nature of work for which you want the connection.

1. Local dial.

2. Use of public data networks.

3. Restricted access.

1. Local Dial: Local dial is the cheapest type and is only possible if the host is at a local telephone call distance away.

2. Public Data Network: If the host is not in the vicinity, then long distance calls have to be made over public data networks. If the speed of such networks is slow then data transmission speed will also be slow and so the connection will prove to be more expensive.

3. Restricted Access Account: Suppose you want to access only E-mail or newsgroups. In such situations, restricted access account is best for you. There are certain sites which provide inexpensive E-mail accounts, local bulletin board services, etc. you just have to registered pay only for the services you want to use.

B. Individual Computer

Here your computer can work as an Internet Host, i.e., direct downloading of files and mails can be done when connected to the internet. This kind of link is a little more costly than the host terminal connection as you have to pay a monthly fees to the service provider or sometimes even a flat charge for a fixed period of time. Here you can have one or both the following account ;

1. Serial Line Internet Protocol (SLIP)

2. Point to Point Protocol (PPP)

1. Serial Line Internet Protocol (SLIP) . In case of SLIP data is sent in packets under speeds of 9600 bps on telephone lines using data compression protocols.

2. Point-to-Point Protocol (PPP). In case of PPP data is sent over telephone lines via modem. Double checking is done at the destination to see if data packets have arrived intact. This is better than SLIP as it allows authentification of users. These days PPP connections are more common. Again, speed of data transfer in PPP is faster than in SLIP.

This type of connection is good for people who:

1. Use Graphics.

2. Download files often.

3. Use direct e-mail or any other online service.

4. Use Internet regularly though for limited hours.

The limitations are few, such as , people may not be able to access the Internet easily if the disk space is limited or if the line is slow (i.e., speeds below 28.8 Kbps will not be accessible by other people).

C. **Dial-Up or On-Demand through the LAN**

In this case there is a dial up link from the LAN to which you are connected to. This type of connection is favourable for small business houses and educational institutes. Here the server, on demand, dials up for a connection and once the connection is established everybody logged on to the LAN can access the Internet. In such a situation if there is any file downloaded from the Internet then like any other file, this file will be accessible to all LAN clients. The only problem here is that the more the number of users logged onto the LAN and working on the Internet, the slower will be the Internet connect6ion. However, this is successful if you have a very fast server software along with a very fast line. Again extra software like proxy servers are also required to serve the needs of various individual LAN users with one Internet connection.

2. Integrated Services Digital Network Connection (ISDN)

This is a very high speed connection to the Internet over normal telephone line. It combines both voice and digital information in a single medium, making it possible to provide the customers with digital as well as voice connections. In ISDN connection, the information which is sent from your computer to the Internet is digital. Here we do not use a normal modem. As no conversion from analog to digital or vice versa is required, so we use an ISDN modem which is merely a terminal adapter. Another differences lies in the fact that the ISDN lines, in order to work, require power from outside. When there is a power shutdown, ISDN lines will not work. ISDN service has many variations but we follow Basic Rate Interface (BRI) Service. Here the ISDN line is divided into three logical channels, namely :

1. Two 64 Kbps B (bearer) channels.

2. One 16 Kbps D (Data) channel.

Thus ISDN is commonly referred to as 2B+D.

Over bearer channels you can send data. If only data is sent then it could be sent at a speed of 64+64=128 Kbps but if both data and voice is to travel then one B channel is dedicated to voice and the other to data. The data or D channel is used to send signaling information for routing data which is being sent over B channels. Those telephone companies which do not have the ability to use D channels remove 8 Kbps from each B channel. Therefore, only 56 Kbps of data can go over each of these B channels.

Apart from voice, many value added services are also being offered like:

1. Telephones will soon have the facility to display name, address, and telephone number of the caller while the telephone rings.

2. When the telephone gets connected to the computer, the caller's database record is displayed on the computer.

3. Call forwarding facility

4. Remote electricity meter reading services.

5. Smoke alarms that automatically call up the hospital, fire station or police station.

Advantages of using ISDN:

1. Allows high speed access, i.e., 128 Kbps.

2. No special laying down of wires. The existing copper telephone cables work fine.

3. Can be used for voice, data, graphics, full motion video as data transfer speed is high.

The only disadvantage of using ISDN is that it proves to be an expensive affair as special equipment is required for it and the tariff is also high.

3. Leased Line Connection (Dedicated Connection)

As the name suggests, a leased line connection is a permanent connection laid down between you and a modem. As it is permanently lined, you have a 24 hour access to the Internet, seven days in a week. A leased line connection is very useful especially when frequent information has to be accessed from the Internet and also when the volume of data transfer is high. It is also useful if the Internet is to be used for more than 12 hours a day.

This type of connection is the most reliable and has high speed. The only issue behind this connection is its cost.

The cost includes :

1. One time installation (laying down of physical line upto your site).

2. Yearly/periodically maintenance charge.

3. Annual tariff.

4. The necessary one time hardware, software and set up charges.

4. Cable Modem

In case of cable modem the Internet can be accessed through the normal coaxial television cables with the help of cable modems. Speed of cable modems is 10 to 100 times faster than normal dial-up connection modems. The only catch is that the local cable operator should have the capability to access the Internet over cable TV wires and that cable modems are slightly more expensive than normal modems. One advantage of cable modem connection is that you need not have a telephone line if you want this type of connection to the Internet.

Before giving approximate tariff rates for the different types of connections, let us discuss the role of Videsh Sanchar Nigam Limited (VSNL). VSNL is the gateway to Internet in India. It is also an Internet Service Provider (ISP) so that the user can acquire a connection from it. Until recently, VSNL was the only gateway of the Internet in India but now we have another private gateway, namely, Now Convergence. This organization also has some very good offers like faster downloads. Let us now discuss the role of an ISP.

5. DSL

DSL or Digital Subscriber Line service is provided through the existing telephone line, but it works differently than regular analog modem dial-up access. DSL operates over normal telephone lines and it can be used simultaneously with the telephone. DSL can increase the connection speed by as much as ten-fold from a standard dial-up modem.

6. Broadband

This type of access is good for remote locations, where ISDN, cable or DSL are not available. It gives a decent download speed, but to upload the data, the user still needs a regular analog modem to dial in, via a telephone line. Satellite connection can be either a two way service or a one way service. In case of two-way satellite service, the data is transmitted via satellite to a dish antenna at the user’s house. In one-way system, the user needs a conventional modem and a telephone link to an ISP. Satellite connection is expensive but sometimes is the only fast option for the people who are beyond the service area of cable and DSL providers.

7. Very Small Aperture Terminals (VSATs)

The two ground stations that communicate with one another via the satellite need not be the same size or transmit data with the same amount of power. Many satellite networks use a large number of small dishes, called VSATs (very small aperture terminals), for the outlying nodes and one central hub with a big dish that can transmit very powerful signals and is very sensitive to incoming ones. This system minimizes the cost of the majority of the ground stations at the expense of maintaining one big one, which can be shared by several users, However, this approach can cause additional delays, because the VSATs aren’t powerful enough to talk to one another directly through the satellite; messages must pass through the hub and make two trips into space before reaching their final destination, incurring a double delay.

VSATs are typically used by organizations, such as oil companies, that require data or voice communications between sites distributed over a wide geographical area. Terrestrial links are economical over short distances; their cost climbs quickly as the distance between locations increases. In addition, terrestrial data and voice links, while readily available in cities, are often difficult, if not impossible, to obtain in smaller urban 'and remote local areas using these links.

3.8 HOW TO SELECT INTERNET SERVICE PROVIDER

Before choosing an ISP, it is important to assess your company's business and marketing goals. In other words, you should determine what your organization will be using the

Internet for. Once you've determined this, you can contact ISPs that serve your geographic area and ask them about their services.

Here are some questions that user may wish to ask when choosing an ISP for Internet connection:

General

- What types of connections are available in your geographic area? (dial-up, ADSL, cable, etc...)
- What equipment (hardware) is necessary to establish a connection? (dial-up modem, cable modem, etc...)
- Does the ISP provide installation software?
- What kind of technical support can you expect?
- What additional perks are offered with each package? (Web space, additional e-mail accounts, etc.)

Connection

- Is the dial-up number billed as a local call?
- Does the ISP provide alternate local dial-up numbers? How many?
- Is remote service available? (regional, national, international)
- What type of connection speed can you expect?
- How often can you expect busy signals?
- What is the service's expected uptime?

Cost

- What payment options are available?
- Is there an initial connection fee?
- Can the type of connection be changed without penalty?
- How will your connection time be charged?

  - metered

  - flat rate

  - bandwidth use

  - combination of the above

- Are annual subscriptions offered at discounted prices? (as opposed to monthly charges)

- Are there any other possible charges?

Many of these questions can only be answered while trying for the services. You may want to request a trial period from an ISP so that you can evaluate its performance before signing on with them.

Web Hosting

Most companies that offer Web hosting services will offer basic packages which can be modified to accommodate your specific needs. Requesting and comparing this information is a good place to start when looking for Web hosting services. The following list outlines some important questions that should be answered before you make a decision:

General

- How much bandwidth is available for upload and download? (data transfer)

- How much storage space is available? Can additional space be added at a later date? (data storage)

- Does the ISP allow for commercial Web sites?

- What is the site's expected uptime? What is the company's policy with regards to this?

- Which operating systems do they support? (Microsoft, Unix, Linux...)

Services

- Does the ISP provide shopping cart and other e-commerce technologies and services?
- Are Web-based tools available for site maintenance and configuration?
- Which Web technologies are supported? (databases, programming environments, etc...)
- What kind of technical support can you expect?
- How many e-mail addresses (aliases) are provided per account?
- Are mailing list services available?

Costs

- What is the cost for domain name registration?
- What will be the total monthly cost of your company's desired Web hosting solution?
- Is there a service fee for adding or removing features?
- What is the cost of each additional feature? (databases, additional e-mail addresses, etc...)

Be wary of relatively low advertised prices when choosing a company to host your Web site. These low prices are usually offset by additional costs for basic services, or are indicative of poor performance. You may also want to visit some sites that are hosted by the company to see how they perform.

3.9 ISP IN INDIA

The current ISP scene is witnessing a roller coaster ride. The beginning of the year saw the presence of 25 brands and license for about 256 ISPs granted. The market was crowded, with not enough room for all of them to survive. It was also found that lavish advertising spends with everybody wanting to gain the early mover advantage. Every one focusing on price war, brand building took a pillion seat. Brands that did not build strong brand equity began to find the going tough. As a result, many leading brands too folded

up. The market finally settled with 3 to 5 players, with the future becoming a limited game.
Government issues three kinds of licenses to set up business:

- ISPs that want to operate at a national level will have to apply for category ‘A’ license. Bank guarantee of Rs.20 million.

- Category ‘B’ license will cover the four major cities and metros of the country in addition to 20 telecom circles. Bank guarantee of Rs.2 million.

- Category 'C' for smaller areas. Bank guarantee of Rs. 3 lakhs.

There is no limit on the number of players in an area and a company can apply for as many licenses as he/she wishes to apply. Private ISPs can establish their own gateways after obtaining security clearances. They have the option to use Videsh Sanchar Nigam Limited (VSNLs) gateways. ISPs can also interconnect among themselves and provide services to V-SAT substations. With the mushrooming of ISPs, the differentiator would be service standards, bandwidth to the Internet, uptime, customer education, training and support.
It is essential in India, that ISPs have to provide not only access and make money from that, but also:

- Provide additional businesses like hosting,

- Creating homepages and websites,

- Marketing the necessary equipment and

- Software the customer needs to set up business like modems, PCs, web browsers and authoring packages.

It is very unlikely that process would fall below the current levels. When the number of players are less, the price would stabilize Price cuts have not worked and when the market matures, the discerning users will increase, according to few experts. Some of the ISPs have already formed a castle in the north to arrest further price fall. This would happen even at other places. Free ISPs (FISPs) also made their presence last year. They

however, have a price not just in terms of the overall viewing area, that will be taken up by advertising banners, but in the type and extent of personnel information required to be provided. Before getting free access, most ISPs require demographic information at the time of sign-up. During the beginning of the year, the free ISPs did affect the market. Today, with most of the FISPs shutting shop, the market is growing. Free service providers will not be able to provide quality surfing experience, according to some people. The free ISPs target revenue out of sponsorships and advertisements. Many a times, customers know that using FISP is not economical enough as the download is supposed to be slower than a paid ISR resulting in longer time taken to browse and with added telephone cost.
While choosing a FISR it is imperative to consider:

(i) Whether the service is available in the area (local dial-up number)

(ii) The ISP has sufficient resources,

(iii) The size of the banners

(iv) Extent of personal information needed and

(v) Case of software set up.

Free ISPs and their Services

Name	**Banners**	**Speed**	**E-mail**	**Support**
caltiger.com	Yes	56 K	Pop	E-mail, FAQ, Tel.
bharat connect	Yes	56 K	Web Pop	-
cheecoo.com	Yes	-	-	E-mail, FAQ
freedialin	Yes	56 K	Web	E-mail, FAQ, Tel.
Logfree.com	-	56 K	-	-

Focus on new access devices,