Abstract

Why the ongoing surge in Internet popularity? The simplest explanation is that there is nothing else like it. Local area networks enable data exchange only with a select set of other users. The Internet is the largest wide area data network in existence—there are nearly 12 million hosts and over 250,000 web sites covering 83 countries. Currently there are around 40 million users which is expected to grow to 100 million by the year 2000. The Internet can now support storage, searching and transmission of full multimedia data including audio, video, formatted documents as well as conventional data. The Internet allows local and wide area users to communicate with more people, in more ways and provides access to the largest range of database servers in the world. The growth in demand for Internet access has been accompanied by the development of an ever-growing range of client–server tools and GUIs (graphical user interfaces). This tutorial paper discusses a number of the pertinent issues relating to the protocols, architecture, services and facilities of the Internet.

1. Introduction

The Internet is a global, cooperative collection of over 500,000 Internet domains spanning 83 countries and linking over 12 million host computers. Currently, there are over 40 million Internet users, with a growth rate of 10–15% per month. The Internet supports numerous services, including electronic mail, file transfer, fax messaging, conferencing, bulletin boards, remote computer access, search engines, electronic storefronts, electronic shopping, EDI and many more.

The information and services are distributed among the various individually managed networks comprising the Internet and are accessible from anywhere in the world to anyone with a valid Internet address and connection. Organizations join the Internet because it offers worldwide connectivity and access to useful information, and because it is cheaper than establishing and operating private networks.

The last 2 years have seen substantial changes in the availability of Internet services and facilities. Not only has commercial access to the Internet become available in many countries, but the range of these services has increased markedly. Significant changes have occurred in many countries of the world with a whole variety of organizations now offering access to the Internet in a variety of ways. Much of this change has resulted from a more liberal interpretation of the acceptable use policy (AUP) [1] by the National Science Foundation in the US with a resulting substantial increase in the availability of commercial access. Although commercial access to the Internet has been available for many years, companies were expected to connect only for research and educational purposes. Today, however, the AUP is being interpreted very liberally and organizations such as the Telecom Authorities as well as many other organizations in various countries have taken on the responsibility for providing access to the Internet. However, the range of these services as well as their performance and cost attributes varies enormously.

For users, the Internet provides a wealth of technical information, database and software services, usually at minimal cost. A number of books are now available which describe the many aspects of Internet’s operation and usage [2–5]. The Internet is in a unique position in that it is not owned by any one organization. All users in fact contribute to the overall Internet by making services available to other users on their own network. It is a unique example of cooperation in a competitive world which benefits everybody providing basic rules and courtesy are respected.

There really is no other network which provides such a comprehensive range of facilities and services. Private
networks enable users to communicate only with those in the same business. Networks such as Compuserve, Sprint, BIX and Reuters also provide a wide range of complementary information services while gateways between the Internet and these networks usually provide for e-mail transfer at least.

There still exists a fundamental difference in philosophy in the use of the Internet by its various user groups, although there is every sign that these differences can be accommodated. The academic and research institutions together with the Government agencies who pioneered the use of Internet made information freely available to the Internet community usually at no cost—all for the advancement of learning and research. Exchange of ideas and software was encouraged. Furthermore, little attention was given to the security of information—rather its widespread dissemination was to be encouraged. It was not until 1988 following a major security breach in Europe and the United States, as well as the release of the Internet worm,¹ that attention was directed to issues of security. These security issues are now of vital importance to the growing number of commercial Internet users.

Intranet has become a widely used term and refers to a private Internet based upon the same TCP/IP protocol suite as used in the Internet. Organizations are looking at using a private web-based Intranet as their primary information resource. Many of the hypertext ideas suitable for document storage and distribution that were piloted with the Internet have become readily accepted for Intranets as well. Interconnection of these private Intranets with the public Internet requires careful design and particular attention to security issues. This is further discussed in Section 6.

2. Internet's architecture and protocols

2.1. Early developments

The Internet traces its origins to the US Federal Government’s Defence Advanced Research Projects Agency (DARPA), the research and development arm of the Department of Defence (DOD). In 1969, the DOD started building a packet switched network called ARPANET for the support of various computer science and military research projects. The network grew to encompass many different types of computers at universities and research centres nationwide. In 1973, an internetworking project was initiated at Stanford University—later involving BBN and University College, London—to develop a suite of protocols for the network.

By 1978, four versions of the transmission control protocol (TCP) were developed and tested and by 1980 a stable protocol suite was established facilitating connectivity among ARPANET computers. In 1983, all ARPANET users were switched over to these new standard protocols, known collectively as transmission control protocol/Internet protocol (TCP/IP) [6–8] as shown in Fig. 1. ARPANET was retired in June 1990 and was replaced by a number of commercial and Government-operated backbones in the US, Europe and Asia–Pacific regions. Although ARPANET has since been supplanted by more advanced networks, the TCP/IP protocols continue to be used and enhanced.

The lowest layer of the TCP/IP protocol suite is called the link layer and contains specific protocols for LANs and other types of communications subnetworks including serial routing protocols such as SLIP² (serial line IP) and PPP³ (point-to-point protocol). The next layer is the Internet layer which provides routing and relaying between subnetworks in the Internet. The transport layer provides end-to-end communications links between systems—sometimes referred to as sockets or ports (sockets with addresses assigned to them). The application layer provides applications such as remote login, terminal emulation, file transfer and web browsers.

The use of PPP or SLIP means that the user’s machine has full Internet connectivity permitting full client–server operation and GUI-based applications to be used with native access to all Internet services. They both support asynchronous dial-up and synchronous leased line operation. SLIP cannot support error detection or data compression (although one version—CSLIP—compresses the TCP/IP headers), but is easy to configure and is included in most UNIX system architectures. PPP also offers three-way handshaking and authentication features for dial-up connections.

TCP/IP operates on the assumption that a common Internet layer service can be provided to support applications. The Internet layer provides a connectionless (datagram) service to the transport layer and operates directly over connectionless media, such as IEEE802-series LANs. The Internet protocol (IP) provides routing and relaying between the various types of networks, whether they be connection-oriented, such as X.25 or Frame Relay, or connectionless, as in the case of LANs. IP always operates in conjunction with the Internet control message protocol (ICMP) which provides error reporting and congestion control facilities. One of the unique features of this architecture is its ability to be used over any conceivable transmission medium.

¹ A worm in the Internet brought large parts of the network to a standstill in 1988. The worm exploited problems in sendmail and finger programs running UNIX on Suns and VAXs.

² Serial line IP (SLIP) is a protocol for sending IP packets over point-to-point serial links. It has been around for several years, but can be slow and less flexible than its successor—PPP.

³ Point-to-point protocol (PPP) is now the standard for sending IP packets over point-to-point serial links.

---

1. The four layers of the TCP/IP model.
The transport layer consists of two protocols. The transmission control protocol (TCP) is connection-oriented and provides for reliable end-to-end transmission of long streams of bytes. The user datagram protocol (UDP) is connectionless and provides the ability to send short messages without the overhead of establishing an end-to-end connection. Several application layer protocols exist which use UDP and TCP to provide network services. Fig. 2 shows a typical range of these application protocols used on the Internet to support e-mail, file transfer, remote logins and network management.

2.2. Internet addressing

With several million users of the Internet, addressing can become quite complex. At the top of the address hierarchy is the domain, indicated by two- or three-character codes. Common three-character code domains include commercial (.com or.co), educational (.edu), governmental (.gov), and military (.mil). Nearly 50% of all registered domain names are commercial organizations.

Each level of the domain naming system has name assignment authority over the subdomains that it controls. Thus, the .co domain can give authority to IBM, for example. IBM, in turn, can give authority to its operating units, which ultimately have control over individual hosts. Two-character country codes are also in the domain list. Examples include .uk (United Kingdom), .sg (Singapore), .au (Australia), .nz (New Zealand). Names on the Internet are formatted according to the following hierarchy of domains and subdomains: machine.suborganization.organization.domain, for example server3.sales.telecom.hk.

The Internet’s domain name service (DNS) maps host names to addresses. Requests for translations of host names into Internet addresses are sent to a domain name server. The server can either respond with the complete translation, or with the name of another server to contact for that information. The Internet addresses are translated into physical addresses, which may use alphanumeric characters and have semantic content (as opposed to the 32 bit Internet address).

IP’s addressing scheme is integral to how IP datagrams are routed through a TCP/IP internetwork. An IP address is 32 bits long and is divided into an assigned network number portion and a host number portion. The host number portion can be further segmented into a subnet number portion and a host portion. Subnetting allows a network administrator to build multiple networks of hosts and yet localize each host’s traffic to specific subnets. IP addresses are expressed as four decimal numbers ranging from 0 to 255 with each number separated by a dot, for example 132.181.19.12.

IP addressing supports four unique network classes as shown in Fig. 3. The left-most bits of any IP address indicate its network class. IP network numbers are assigned by the network information centre (NIC) and will fall into one of the following classes based on the network size requirements:

- Class A networks are reserved for very large
organizations and for countries. The first octet is assigned by the NIC, and the remaining three octets are available for hosts and/or subnets. Class A networks have network numbers from 1 through 127 \((2^{24} - 1)\) each with 16 million \((2^{23})\) hosts. For example, 127.122.0.230 is a class A address because the first octet is in the range of 1 through 127.

- **Class B networks** allocate the first two octets to the network number, i.e. 16 384 \((2^{16})\) networks, leaving the two remaining octets for host and/or subnet assignment. Class B network numbers are very popular because up to \(2^{16} = 65536\) hosts and/or subnets can be assigned. A large proportion of the available class B network numbers have been assigned by the NIC and organizations requesting class B addresses must prove why a class B address is justified.

- **Class C networks** allocate the first three octets \((2^{24} - 1)\) to the network number, i.e. around 2 million, leaving the last octet—\(2^{8}\) hosts for hosts and/or subnets. Typically organizations request multiple class C addresses to ensure they have enough address space for future growth.

- **Class D addresses** are reserved for multicast groups.

Class A addresses are assigned to the largest networks such as NFSNET and MILNET, while Class C addresses are typically assigned to small business LANs. The NIC administers the network numbers only and once a site is assigned a network number (class A, B or C, depending on the expected number of hosts at the site), and it is then up to the site to determine how to allocate addresses to individual hosts.

Each host on an IP Internet has a globally unique IP address. This IP address is typically configured into the operating system of the host by a network administrator. Class B addresses are very common and might appear as 132.181.30.3 where the first two numbers represent the network number in a country, the second number might be one of a range (e.g. 30–35) which represents a specific host in a domain such as a department or workgroup and the 3 might represent a user in that domain.

If a locally administered network is not connected to the Internet, the address can be arbitrary. However, the use of arbitrary addresses is not recommended, since it can cause problems with later connections to the Internet. When the network manager wants to connect to other IP-based systems, all local addresses have to be assigned by the NIC.

### 2.3. Address expansion

The Internet protocol’s 32 bit address space cannot support for long the explosive growth of the Internet. The current IP routing and addressing scheme can support only about 2 million network addresses, which are expected to run out by 1998. This means the Internet protocol must be modified to support more network addresses and more sophisticated services.

The current version of IP, Version 4, can handle Internet growth well into the next century, thanks to classless inter-domain routing (CIDR). This is a scheme for assigning and grouping addresses in a way that more flexibly defines network and host addresses, which essentially allows more address definitions in the same amount of address space. While CIDR can extend the life of IPv4 to about the year 2008, it solves only one problem. Internet users have begun demanding services not easily handled by IPv4, such as:

- security;
- multicasting;
- autoconfiguration;
- mobility;
- resource reservation; and
- policy-based routing.

After 3 years of deliberations, in 1994 the Internet engineering task force (IETF) selected the next generation of Internet protocol. IPv6 [9] is essentially a version of the simple internet protocol plus (SIPP) proposal, which extends the 32 bit address space to 64 bits by deleting unrequired data in the IP header, thereby supporting more levels of the addressing hierarchy and many more addressable nodes. IPv6 also provides more features, including easier router configuration and better security. The drawback to IPv6 is that large corporate and institutional Internet users will have to upgrade their entire router installations. They have two implementation choices:

- run both old and new IP stacks together in routers; or
- install gateways to translate between the old and the new protocols. Eventually, the new version of IP will require changes to end-systems and applications as well.

### 3. Internet’s client–server systems

The Internet provides a range of tools for both communication and information retrieval as shown in Fig. 4. Because of the vast size and scope of this network important tools have and are still being developed to aid in the access to this information. These tools go beyond the conventional e-mail, news, bulletin board and directory services and include powerful client–server and GUIs, discussed below.

#### 3.1. Electronic mail (e-mail)

The most popular Internet application is electronic mail. For business, this means an unparalleled degree of communication with staff in the field, with suppliers, and most important of all, with customers and potential customers.

The format of an Internet e-mail address follows the form user@organization.domain, where the organization name
could be the name of a company, of a Government agency, or of an educational institution. Larger organizations often add names of particular servers or smaller subdivisions, or departmental names to this part of the address. Additionally, for networks outside the US, two-letter country designators are appended on the end of the address, for example:

- .hk—Hong Kong;
- .sg—Singapore;
- .uk—United Kingdom;
- .nz—New Zealand.

Domain types fall into a few different categories usually connected with the operation of the Internet in some way:

- com for commercial organizations;
- edu for educational institution;
- gov for government agencies;
- mil for military installations;
- net for network access providers;
- org for non-profit organizations.

### 3.1.1. SMTP (simple mail transport protocol)

SMTP is the messaging protocol governing electronic mail transmissions and receptions over TCP/IP-based networks, and the Internet in particular. SMTP enables users of any PC-based e-mail product that supports MHS (message handling system) to exchange messages with users who have SMTP-based e-mail. MHS is a store-and-forward technology upon which most popular e-mail systems for PC LANs are based. The POP (post office protocol) mail system obviates the necessity to be permanently connected to the mail server and, for example, allows timed and automated connection for uploading and downloading e-mail.

### 3.1.2. MIME (multipurpose Internet mail extension)

MIME is an extension to SMTP that allows users to attach different types of documents to their e-mail messages. Before MIME, the only way to append files to other files for transfer over the TCP/IP-based Internet was to decode a message and include it in the body of another message. Today, the combination of MIME and GUIs makes it easy to add binary file attachments such as:

- sound;
- video;
- text;
- programs;
- graphics;
- spreadsheets.

### 3.2. Network news

Network News, often called USENET News, is a large collection of around 10 000 special interest bulletin boards. Over 4000 of these are devoted to particular geographic areas and location-specific newsgroups exist for nearly all major metropolitan areas in the Internet-connected world.

Not every provider carries every metropolitan newsgroup—most smaller providers carry only newsgroups specific to their own location for example. Newsgroups are divided into several broad categories and a useable ordering of content is achieved by following a hierarchical pattern.

The 'comp' newsgroup category, short for 'computer', contains over 500 groups devoted to specific areas of computer technology. For example, the hardware category includes specific types of machines and the software category includes specific application types, as well as specific product offerings from major manufacturers.
Other newsgroup categories include:

- sci—for physical sciences such as physics, chemistry and biology;
- soc—for the discussion of religious and political social issues;
- rec—for recreation, provides for the discussion of mainstream hobbies and sports;
- alt—for alternative, is the largest and most unrestrained newsgroup category (topics of discussion among the alt newsgroups range from the amusing to the ridiculous).

### 3.3. FTP (file transfer protocol)

FTP allows users to transfer files from machine to machine on the Internet. Access to files posted to the Internet such as directories, catalogues and bibliographies are examples of research-related applications of FTP. It is possible to transfer files in various formats, allowing the user to retrieve software programs, graphic images and other files which are not necessarily in ASCII text. Also available via FTP are the contents of a variety of electronic journals as well as copies of selected software packages.

The Internet is a network of thousands of machines, and many of these provide public access via anonymous FTP. This means that the TCP/IP software and FTP can be used to log into a remote machine with the userID of anonymous. This restricted access to remote machines grants access to vast numbers of files that can be transferred back to a local Internet machine. Text files, computer programs and graphics are just a few of the types of files available through anonymous FTP. There exists an excellent FTP search tool\(^4\) on the Internet which provides access to many remote servers that permit FTP access.

### 3.4. Telnet (a simple remote terminal protocol)

Telnet is the virtual terminal protocol which enables a user to simulate a direct connection from a terminal to a remote host on the Internet by way of a virtual terminal standard. Telnet is a program which is widely distributed throughout the Internet system. Telnet is a powerful facility which can be used to provide outside access to parts of a system. Furthermore, Telnet is used by a number of more complex client–server systems to be discussed below.

Telnet has two operating modes: input and command mode. Input mode is used most often as it is rarely necessary to reconfigure Telnet’s parameters. The command mode enables a user to communicate asynchronously/synchronously, determine status, set various arguments, open and close host ports as well as specify a variety of variations of these basic actions.

### 3.5. Archie (an archive of archives)

Archie is a search engine or a collection of resource discovery tools that together provide an electronic directory service for locating information on the Internet. Originally created to track the contents of anonymous FTP archive sites, the Archie service was subsequently developed to include a variety of other on-line directories and resource listings. Thus having become aware of the enormous volume of information and software which can be obtained via FTP on the Internet, the challenge was then how to find the item or file when required.

Archie’s primary use was to locate specific files on the Internet which are available via anonymous FTP. There is a limit to the number of FTP sites that can be included in Archie’s database; however, the database is extensive and indexes many of the most popular anonymous FTP locations. The heart of the Archie service is a database of the file systems of the many thousands of anonymous FTP sites. Each server maintains its own database and special resource discovery software regularly updates this database.

Archie is a good example of a client–server system in action where the local workstation runs the Archie client software which in turn communicates with the Archie server in a remote location to accomplish the search. Access is also possible to Archie via Telnet or e-mail. Today Archie services are hidden from users behind modern web systems.

### 3.6. Gopher

Gopher is an extension to Archie and links together a variety of systems on the Internet. Gopher was designed as a CWIS (campus wide information system) and document delivery system, but it has been expanded greatly over time. It is menu-driven and these menu items can include documents, menus, FTP sites, Archie searches, Telnets, WAIS (wide area information service), or other kinds of information on the Internet. The Gopher client is a multipurpose browser running on a local workstation which provides connection to a Gopher server. Today Gopher services are hidden from users behind modern web systems.

Archie provides a method for searching for basic files and programs while Gopher is a more elaborate worldwide client–server information retrieval tool. Although originally designed to be used to retrieve text-based titles, it has evolved into a full multimedia information retrieval tool and Gopher services offer the ability to retrieve plain text, formatted text images, sounds and full motion video.

### 3.7. WAIS (wide area information server)

The wide area information server (WAIS) attempts to harness the vast data resources of the Internet by making it easy to search for and retrieve information from remote databases which are called sources in WAIS terminology.

\(^4\) http://ftpsearch.ntnu.no/search-info/search.html.
WAIS servers not only help the user to find the right source, they also handle access to it.

Like Gopher, WAIS systems use the client–server model to facilitate the navigation of these data resources. Unlike Gopher, WAIS does the searching for the user. A WAIS client (run either on the user’s workstation or on a remote system through Telnet) communicates with a WAIS server and requests it to perform a search using an information retrieval language similar to SQL (structured query language).

After a search to identify any documents, a list of hits, or ranked document titles will be returned. The WAIS server ranks these hits from the most-to-least relevant document and ranks them by the number of search words that occur in the document.

As with Archie and Gopher, WAIS formed the building blocks for modern web systems, thus many of its facilities are available through modern web servers.

3.8. WWW (world wide web)

The most recent and fastest growing addition to the family of Internet tools is the world wide web server hypermedia project, designed and prototyped at CERN (European Laboratory for Particle Physics) in Switzerland and known as CERN 3.0 HTTP (hypertext transport protocol [10,11]). WWW takes Internet usage a step forward by linking information globally via hypertext, alongside the ability to link with FTP sites, Gopher and news servers.

WWW is similar to Gopher, but is hypertext based rather than menu-driven and is a better platform for multimedia documents than Gopher. Like Gopher, WWW can act as a front-end for just about any piece of information on the Internet.

The WWW is an attempt to unify the vast amount of information available via the global networks, and to do this using a simple client–server system. WWW can be seen as part of the move towards unifying network tools, negating the need to run several different pieces of software to make best use of network resources.

Anonymous FTP is still a very useful Internet facility. It provided the original archive facility, making files available at a multitude of sites around the world. The addition of a search engine, Archie, made it possible to find named files. However, Archie only informs the user about sites where a desired file resides—it is still necessary to use an FTP client to obtain a copy. Gopher went some way to remedying this by providing on-line viewing and retrieval facilities within the client package while WAIS brought out the power of full text search and querying of resources. Although these tools enable Internet searching and the retrieval of information resources, they exist generally independently of each other.

Fig. 5 shows some of the properties and relationships between these client–server systems used in the aid of information retrieval on the Internet.

Gopher implemented the concept of bookmarks, which allowed the marking of desirable sites or documents for future reference. WWW, on the other hand, is built on the concept of links. The underlying language is powerful yet extremely simple: within any WWW document there can be links to other documents, links to points within the same document and links to other resources such as FTP sites, Gopher, WAIS servers and news groups.

In the WWW pointers can be created to specify the location of a target which can be a text file, an image, a Gopher server, FTP site or various other types of information. The work of locating and displaying the target information is done within the client application—all that is transferred across the network is the information that is displayed according to the built-in rules of the client browser. All formatting and layout of information is constructed locally according to the software and preference settings. For this reason, WWW information can be constructed according to standard rules and WWW browsers permit navigation of the Internet, but return different results depending on their sophistication. The user’s view of the WWW depends

Fig. 5. Client–server systems used for Internet access.
very much on what client software is used. WWW browsers will return information from FTP sites and Gophers, but they are of real benefit when used in conjunction with the hypertext markup language (HTML) and the hypertext transport protocol (HTTP) servers—WWW’s own server software [11].

3.9. WWW browsers

Mosaic [12] was the name of a software tool originally developed by NCSA (National Centre for Supercomputing Applications) and was the most widely used GUI front-end client software. However, a new company called Advanced Mosaic Communications continued the development of Mosaic, but then changed its name to Netscape. Now the world market in Internet browsers is dominated by both Netscape’s browser and Microsoft’s Internet Explorer.

Web server software provides sophisticated graphical facilities which have the ability to display:
- text in bold and italic;
- layout elements such as paragraphs, bulleted lists and quoted paragraphs;
- electronic text in a variety of fonts;
- hypertext and hypermedia documents;
- sound and playback;
- freeze frame and full motion video images.

The capability to support hypermedia—sounds, movies, extended character sets and interactive graphics—is fundamental to many multimedia browsers and is generally achieved by the use of third-party products such as Quicktime, Adobe Acrobat, MPEG Play and others.

Web browsers typically keep track of where the user has been, offering a list of visits which enables quick backtracking—a very useful feature when the user has moved a long way down a branch and found a dead end. A browser also offers caching: it keeps a copy of pages that have been visited so that if a backtrack is necessary, information downloads do not necessarily have to be repeated.

A web browser is an interface to the WWW distributed information system. Like Gopher, WWW is functionally split into two parts, the server and the client. The server manages the data and answers requests from client applications. On the Internet, multiple servers and clients can run simultaneously. This arrangement enables the data to be distributed among many machines, and also allows many users to access a particular server at the same time. The user works with the client application, which connects to appropriate servers, gathers the desired information, and presents it in a useful format. There are other web client applications, but a browser is distinguished by its support for multiple hardware platforms and the advanced features of the WWW hypertext markup language (HTML) to be discussed in the following section.

Various browsers have some useful features that are common among each platform-specific version. For example, documents can be annotated for future reference and the annotations appear at the bottom of the document and can be viewed and edited along with the original document. Future versions of these web browsers will allow annotations to be shared publicly or within a local group of users. Recent pages can be saved in the cache which makes backing up much faster (and less costly) than reloading an entire document over the Internet. Finally, the list of documents that have been visited is saved on a hot list for rapid future reference.

4. Web servers, search engines and development tools

4.1. Client–server development tools

The two most popular web development platforms are Sun Microsystems’s Java and Microsoft’s ActiveX. Java was the first significant web server development system which simplified many of the difficulties encountered with C++. ActiveX is an umbrella term for a set of new technologies, including the WinInet APIs (which are wrappers for HTTP, FTP, Gopher and other Internet standards) and ActiveX controls.

Both of these platforms have suffered from security problems, although recent patches seem to have rectified these problems. They are both potentially insecure by nature as running on-line programs, such as those that Java and ActiveX enable, client systems cannot check for those programs’ compliance with local security requirements.

HTML has been remarkably successful in enabling text formatting, embedded pictures and hypertext links both within and between documents. HTML is based on SGML (standardized generalized markup language), which is used in many industries to create documentation in a device independent format. An SGML document contains the text information along with tags that specify character formatting (bold face, underline, etc.) and layout formatting (document title, section heading, bulleted lists, etc.).

One limitation of HTML lay in its lack of ability to initiate an executable program from within an HTML document; to overcome this problem CGI (common gateway interface) scripts were written. These could be executable programs written in C, UNIX shell scripts or equivalent which initiate programs to run on a server. CGI scripts are often used to create web forms, which let the user enter information after a question and send it back to the web server. These items are becoming standard on web pages, but building and maintaining them can be time-consuming. Subsequently Java introduced the concept of applets—executable programs which could run on the client [although subsequently ‘saplets’ (server applets) were created which are executable programs which can run on the server].

Developing out of HTML are tools for creating and maintaining web site content. The contenders here are
Microsoft’s FrontPage and Netscape’s LiveWire, although the two products are aimed at different users and address site construction quite differently. Both packages help deal with the everyday tasks of creating useful web content and keeping it up to date. Both provide hypertext markup language (HTML) authoring tools, check for broken links, and offer wizard-style functions to help create a complete web site. Both can also create interactive content—FrontPage with its WebBot add-ons and LiveWire through its JavaScript support. WebBots permit the automatic loading of web objects such as those created by CGI scripts and thus add more complex features to web pages.

As Microsoft tightens integration with the rest of the Office suite, its FrontPage looks attractive for people who want to use a Web server to store and distribute corporate documents on an Intranet, although it is not intended to handle a large and complex site. LiveWire can handle any site, but is substantially more complex than FrontPage. In general the characteristics of these two can be summarized as follows:

**Microsoft FrontPage**

*Advantages:*
- excellent HTML editor;
- good price/performance.

*Disadvantages:*
- limited programmability;
- requires server extension.

**Netscape LiveWire**

*Advantages:*
- powerful server scripting;
- can manage large web sites.

*Disadvantages:*
- steep learning curve;
- Netscape servers only.

### 4.2. Netscape Navigator and Microsoft’s Internet Explorer

Netscape and Microsoft have developed remarkably similar web browsers. Choice has more to do with packaging and marketing than with technical characteristics. They can both be used over dedicated or dialup (SLIP or PPP) Internet connections available from an ISP. They both permit the user to browse through pages of menus which are hyperlinked to data stored on servers in any location in the world and without having to be aware of the location of the network address of that information.

By use of point-and-click, these browsers use hypertext links to navigate and browse the web, and allows users to view graphics and hear embedded sounds without first having to download the files. Commercial versions are available for PC Windows, Macintosh and X-terminal UNIX-based systems. These versions include a toolbar and other aids to provide users with easy access to a variety of navigational shortcuts.

### 4.3. Search engines

Search engines have become a vital tool to aid with information retrieval by taking user queries and matching them with indexes of web sites. They are proliferating to the point that they have become commodity items that essentially deliver the same thing. However, because of differences among the search engines, there is little interoperability among them. For example, the language used to enter search queries frequently differs amongst sites. Several research projects are underway which aim to develop a standard search query language.

Some web servers feature integrated indexing and search engines to help users locate needed data quickly. Indexing components are used to organize information stored at the web site, while search engines track down stored data.

The competitive push to be the best and brightest Internet directory or service has segmented the web into dozens of proprietary directories that each exclude portions of the web. Some directories only include sites or people who voluntarily register with them. Along with the search engines are Internet directories and services, which incorporate search engines but also try to add value by evaluating web sites—either by putting them into categories or reviewing their content.

Examples of commonly used search engines include:

- DejaNews offers a tool for searching a 4 GB database of USENET newsgroup postings (www.dejanews.com).
- Ecola’s Tech Directory is an extensive directory of web sites of technology corporations and includes a list of on-line technology periodicals (www.ecola.com/tech-corp).
- Excite is a free service that offers both web-site searches and reviews (www.excite.com).
- Lycos is also a free service covering a wide range of computer-related topics (www.lycos.com).
- IBM has developed a subscription-based site called InfoMarket which is used for searching proprietary directories. (www.infomkt.ibm.com).
- InfoSeek provides a free service with searches and reviews of web content. It also has an enhanced, subscription-based service that can search various resources, including computer magazines, USENET newsgroups, news services and analyst reports (http://www2.infoseek.com).
- Inktomi is a parallel-processing global web site search tool developed at the University of California at Berkeley (http://www.inktomi.berkeley.edu).
- The-Inter.net offers pointers to search tools, hot lists and
a directory of home pages (http://the-inter.net/www/future21).
• NYNEX has developed an on-line yellow pages for US businesses (www.niyp.com/enterbusiness.html).
• World Yellow Pages has put together a global directory of on-line businesses, but registration is required (http://wyp.net).
• Yahoo is a searchable Internet directory that registers web sites by content. It also provides search tools and content reviews (www.yahoo.com).
• SavySearch (http://guaraldi.cs.colostate.edu:2000/form) and Quarterdeck’s Web Compass (www.quarterdeck.com) send queries to many search engines, returning abstracts that describe query results.

4.4. Internet service providers (ISP)

There are several types of Internet Service Providers—service companies that provide Internet connections and servers to individuals and organizations. Some resemble the traditional dialup bulletin boards, and many of the smallest providers have added Internet as an afterthought to their existing operations. Other small-scale providers started in business for the express purpose of providing Internet connectivity and a large number of these small have sprung up in deregulated environments. However, in the longer term they may not be able to offer robust or dependable enough connectivity for any but the smallest of businesses.

On a somewhat larger scale, the regional providers whose high-speed backbones once made up the major portion of the entire Internet, connecting universities and research centres into large subnets, are now willing and able to take on commercial customers. They have the depth of expertise and the physical infrastructure to do it. Finally, at the high end of the spectrum are the large commercial providers that include the telecommunication carriers and other computer industry giants such as IBM, Sprint and Compuserve.

4.5. Network access

Users who run TCP/IP on their own computers can execute Telnet, FTP and other IP applications directly, instead of having to dial up the ISP to obtain access to these services. Because this method of access provides users with a full IP connection, multiple sessions can run concurrently. For example, it is possible to run multiple FTP and Telnet sessions with each session appearing in its own window.

Another way to obtain an IP connection is through a public dial-up provider. In addition to supporting TCP/IP, the computer must then also support an underlying link layer protocol such as SLIP and PPP for communicating over the telephone line.

Depending on the volume of traffic anticipated, dedicated 64 Kbps switched (ISDN) or permanent high-speed lines like 64 Kbps switched or 1.544/2.048 Mbps dedicated T1/E1 connections are necessary. They are essential for...
businesses that expect to establish an Internet point-of-presence for access by customers.

Delivering Internet services over a LAN will also mean running a TCP/IP stack side-by-side with the native network operating system. For example for Novell Netware this will require the loading of both the IP and IPX stacks at the workstation. If the network is already supplying some large-scale client–server applications such as a relational database, the choice of Internet applications software could be somewhat circumscribed by the TCP/IP stack already in place.

If the organization desires full-time, full-function access to the Internet via leased-line connections from its LAN or corporate backbone then ISPs can provide this on a regional, national or international basis.

5. Internet as a business tool

The statistics relating to the Internet are phenomenal. Most demonstrate exponential growth as can be seen in the following graphs. The number of users are growing at a rate between 10 and 15% per month, with the business sector being the fastest growing segment of the Internet. Figs. 6–8 show the growth in the number of connected Internet hosts, domains and web sites, respectively. These figures are available from the Internet and are constantly updated [13]. Fig. 9 indicates the projected number of users of the Internet to be 100 million by the end of this decade [14].

The largest growth segment of the Internet is the business sector. Based upon statistics gathered by NSF [15], the number of commercial addresses comprise 51% of Internet network registrations. This percentage does not include companies that registered under some research-related functions. By contrast, defence is 7%, government is 9% and education is just 4%.

Fig. 10 shows the distribution of Internet users by their top level domain name: commercial (.com, 42%), education (.edu, 27%), government (.gov, 5%), defence (.mil, 6%), organizations (.org, 4%) and networks (.net, 16%). Clearly there is some overlap between these groupings. The organizations grouping is intended to include non-profit groups such as IETF (Internet Engineering Task Force), Network Management Forum (NMF), Desktop Management Task Force (DMTF) and the International Standards Organization (ISO). The networks grouping includes non-profit network operators such as International Airline Transport Association (IATA), Society for Worldwide International Funds Transfer (SWIFT) and Usenet News Groups.

6. Firewalls and Internet security

Performance and security have been the two key factors
limiting widespread commercial use of the Internet in recent years. One of the key factors affecting the performance as seen by the users is dictated by the capacity of the access links to the interface router and the Internet backbone [16]. To a considerable degree the performance issue is being resolved as more backbone bandwidth is introduced and ISPs provide faster dial-up speeds as well as ISDN and leased line options. However, as more bandwidth is introduced the applications which require this bandwidth become more demanding and multimedia services including Internet telephony and video services necessitate particularly high capacity.

Security has been more difficult to resolve. The complexity of the various development platforms and operating systems (Java, ActiveX, Windows NT and UNIX in particular) as well as the stringent requirements for secure electronic transactions has meant that solutions have taken time to develop.

There are many stories in the literature describing how the Internet was used either directly or indirectly to break into remote hosts [17,18]. Thus attention needs to be directed to security issues at the network interface between the untrusted (Internet) and trusted (private) networks. Security issues also become of significant importance as organizations interconnect their Intranets with the Internet.

There are many different interpretations of the term firewall and this can be a source of confusion. One basis for defining a firewall is the OSI 7-layer model (see Fig. 11) which provides a clearer picture than does the TCP/IP model.

It can be seen that firewall architecture consists of two levels:

- Packet level firewalls which operate at the network (IP) and transport (TCP) layers—these are commonly referred to as screening routers or packet filters and block transmission of certain classes of traffic.
- Application level firewalls which operate at the session, presentation and application layers. They are usually implemented using dedicated hosts running specialized software and can also be referred to as bastion hosts or proxy servers usually running under UNIX or Windows NT.

An adequate level of security can be achieved by combining knowledge of computer security issues, the security features that a vendor can provide, public domain security software and adequate user education. Fig. 12 shows the relationship between various security scenarios in terms of cost and value. Some of these will be discussed below.

6.1. Packet filter/screening routers

One of the simplest protection methods is to ensure that the boundary router supports filtering. This then permits the specification of who can perform outbound remote logins or inbound file transfers. These routers are often called screening routers. Each data packet carries a description of the
source, destination, and service type (e.g., login, mail), which enables selective screening to be carried out.

Routers can be configured to prohibit traffic going from the Internet to an internal host or internal subnet. Routers also can be configured to prohibit traffic that participates in dangerous services such as TFTP (trivial file transfer protocol without passwords) and remote printing.

Filters can be set up to only allow e-mail to reach a single host on a LAN. From there this specifically allocated host can distribute the mail internally, thus reducing the number of hosts that have e-mail contact with the Internet. The famous Internet worm exploited a bug in sendmail and used it to gain access to many hosts throughout the Internet.\(^5\)

An example of a packet filter/screening router is shown in Fig. 13.

6.2. Application level gateways and bastion hosts

Packet filtering routers have limitations and are frequently difficult to configure and update. Configuration rules are complex to specify and usually no formal testing facility exists for verifying their correctness. Some routers do not provide any audit capability, so that if a router’s rules still let through dangerous packets, this may remain undetected until a break-in has occurred.

Exceptions to rules will often need to be made to allow certain types of access that normally would be blocked, but exceptions to packet filtering rules can make the filtering rules so complex as to be unmanageable. For example, it is relatively straightforward to specify a rule to block all inbound connections to port 23 (the Telnet server). If exceptions are made and certain systems need to accept Telnet connections directly, then a rule for each system may need to be added (some packet filtering systems allow the sequential order of the filter rules to be significant). Sometimes the addition of certain rules may complicate the entire filtering scheme and can open up holes in the filtering scheme.

Advantages of application level firewalls or gateways include:

- Information hiding, in which the names of internal systems need not necessarily be made known via the DNS to outside systems. The application firewall may be the only host whose name must be made known to outside systems.
- Robust authentication and logging, in which the application traffic can be pre-authenticated before it reaches internal hosts and can be audited more effectively.
- Cost-effectiveness, since third-party software or hardware for authentication or auditing need be located only at the application gateway.
- Less-complex filtering rules, in which the rules at a packet filtering router will be less complex than they would if the router needed to filter application traffic and direct it to a number of specific systems.

Application firewalls also act as important filters for other protocols such as SMTP, FTP, X-Windows and a variety of other services. For example, some application firewalls provide the capability to deny FTP get and put commands which prevents the uploading of a file to an anonymous FTP server and thus provides a higher degree of assurance rather than just relying on correct file setting permissions at the anonymous FTP server.

Some Internet firewalls use a combination of a packet-filter screening computer or a hardware-router for controlling the lower layers of communication, and application gateways for the enabled applications. In general packet filters/screening routers and application gateways can

\(^5\)The Internet worm, which took advantage of bugs in certain sendmail and finger software, shut down large parts of the Internet in 1988.
form a powerful combination. Packet filtering via the router controls the lower architectural layers, while application gateways enable fine-tuned controls appropriate for the applications. Fig. 14 shows an example of a screened subnet application level gateway where a separate subnet is created between the trusted and untrusted networks.

6.3. Secure transactions on the Internet

Security was never a key design parameter of the original Internet. TCP/IP solves many problems in a remarkable way, but it was not designed to offer secure communication services. Because TCP/IP was not designed with security in mind, additional technology and policies must be introduced to solve typical security problems such as:

- How can users be authenticated to make sure they are who they claim to be? Standard Web protocols such as TCP/IP and HTTP make impersonating a person or an organization relatively simple.
- How can authentication be performed without sending usernames and passwords across the network in cleartext?
- How can a single-user login service be provided to avoid costly account maintenance for all the servers (web, proxy, directory, mail, news, etc) across the organization?
- How can privacy of communications be enforced for both realtime (e.g. data flowing between a Web client and server) and those with store-and-forward applications such as e-mail?
- How is it possible to ensure that messages have not been tampered with between the sender and the recipient?
- How can the confidential documents be safeguarded to ensure that only authorized individuals have access to them?

There are a number of technologies available which provide the foundation for a wide variety of security services, including encryption, message integrity, verification, authentication and digital signatures, all of which are based upon cryptography. A variety of authentication and encryption techniques have become available in recent times to provide secure Intranet operation out of basic Internet services.

These techniques include encrypted tunnelling [19], IP next generation (IPng) [9], point-to-point tunnelling protocol (PPTP) [20], secure sockets layer (SSL) [21], secure electronic transactions (SET) [22] and secure multipart Internet mail encoding (S/MIME) [23], which can all be seen in the protocol stack in Fig. 15.

6.4. Public domain security software

There is a variety of security software available on the Internet. Some of these are in the public domain while others are proprietary. Most were designed for TCP/IP UNIX based systems; however, other platforms are also supported. This critical area, under constant change, may
be kept up with by reading on the Internet under topics such as ‘Internet security’ [24] and ‘electronic commerce’ [25], both of which provide excellent information.

7. Summary

The next few years will see the Internet growing in significance as a strategic resource for many sectors of our society. In addition, as more and more organizations base their information resources on Intranets and then require connectivity with the Internet many new security issues will need to be resolved. This Internet/Intranet combination is very likely to form an electronic-commerce framework for business transactions, advertising and merchandising for many organizations in the future. This may well result in radical restructuring of the way in which business is carried out.

The demand for access to the Internet is growing at a phenomenal rate and the range of tools associated with the use of the Internet is changing extremely rapidly. Many new services based upon multimedia applications, such as voice and video, are likely to be seen in widespread use within 5 years and this will again stretch the performance parameters of the backbone systems, ISP access systems and the web servers themselves.

A new range of connectivity services are also emerging with such technologies as ADSL, FTTC, FITL, cable modems, etc. These will provide integrated services to both businesses and homes.

Furthermore, the rapid development of object-orientated web development tools means that organizations’ data structural and retrieval services will be entirely based upon a hypertext infrastructure.

References