Internet: A Technical Primer

By Alexander Kogan, Ph.D., Ephraim F. Sudit, Ph.D., MBA, and Miklos A. Vasarhelyi, Ph.D.

Editor’s Note:
In its continuing coverage of the Internet, the IS Audit & Control Journal has initiated this three-part article documenting the history of the Net and the control and security issues associated with it. Part One, published here, presents an overview of the Internet, including its development and inherent control and security risks. Part Two, which will be published in the next issue, will focus on Internet services and services, while Part Three will cover in greater detail what threats the Internet poses to corporate computer facilities and recommendations for protecting information.

The Internet is a superstructure interconnecting diverse computer networks worldwide and is rapidly becoming an essential communication infrastructure of modern civilization. The users of the Internet have access to a variety of services ranging from traditional electronic mail, remote login and file transfer, to the World Wide Web (WWW).

The WWW or “Web” is the most sophisticated modern information system distributed over the Internet and its development is mostly responsible for the recent explosive growth in Internet usage and popularity. One of the most important features of the Web is its friendly graphical user interface.

The growth of the Internet has been formidable. The number of Internet hosts (a computer site with its own Internet protocol number providing Internet function to other sites on the Net) has been increasing exponentially as shown in Figure 1. It shows number of sites (in thousands) versus time scale.

Background
The seed money for the development of what has become the Internet was provided by the US government for the purpose of creating an independent computer network capable of sustaining its function after a massive nuclear attack. Designed to connect many heterogeneous networks, this network of networks evolved into a self-managing global computer super-network.

For a long time the major Internet backbone in the US was supported by the National Science Foundation. This government support was phased out and, starting in May 1995, the US part of the Internet has been privately owned and operated. As a result, a new Internet structure has evolved in the US.

The base of this new architecture is anchored to four all-purpose Network Access Points (NAPs). These NAPs are located in the vicinity of San Francisco, Chicago, New York and Washington DC, and are operated respectively by Pacific Bell, Ameritech, Sprint and MFS Datanet.

The NAPs allow various computer networks within the Internet to interconnect and exchange traffic. At the top of the Internet service provider hierarchy are the Network Service Providers (NSPs). The NSPs (e.g. MCI, Sprint, ANS, AlterNet, PSI) maintain their own large-scale wide-area networks, and, by the National Science Foundation rules, must connect to at least three of the NAPs. NSPs may also interconnect their networks directly (see Figure 2). Most of the NSPs implement their backbone networks using high-speed lines (i.e. T-3 lines with the speed of about 45 MB per second).

Regional Network Providers (RNP’s) comprise the second tier of Internet service. The RNP’s usually connect to the Internet through NSPs, but may also have direct connections to NAPs.

Larger organizations usually connect to the Internet through RNP’s while individual customers or small organizations typically connect to the Internet through intermediaries, the so-called Internet Access Providers (IAPs).
Every day in the U.S., over 25,000 new social security numbers are issued, an additional 7,500 are invalidated due to death. Veris+DF is a PC based software support service created to audit large files of social security numbers and report those that may be problematic. Incorporated within the system is the entire data base of social security numbers no longer valid due to death of the original assignee. This feature provides an excellent tool for auditing pension funds or other benefit plans to identify payments to persons no longer living.

One state agency recently used Veris+ to audit a pension file. They learned that pension checks were still being sent to many persons who had died.

A second state agency learned they were paying welfare benefits to persons who had submitted social security numbers that had never been issued or could otherwise not belong to them. Also identified were several recipients claiming social security numbers of persons who were no longer living.

Veris is excellent to use in "know your customer" due diligence programs.

COST: $1,200 per year. Updates available monthly or quarterly at additional cost.

SYSTEM REQUIREMENTS: PC compatible with 100MB hard drive or CD-Rom drive, and DOS 5.0.

VERIS SOFTWARE: Mini tape cartridge or CD-Rom disk.

OPTIONAL SERVICE: Send us your file on tape or diskette and we will process it for you the same day we receive it. Cost is $0.01 per each number checked with a minimum service charge of $100 for deceased file checking and $500 minimum for full validation check.

Security Software Solutions

Veris™

Timothy J. Rollins, President
P.O. Box 583 • Burlington, VT 05402
Phone: 802-660-8033 • Fax: 802-862-8792
Packets are basic information units consisting of a header and a body. The header contains source and destination information, while the body contains a portion of transmitted data. Typically, Internet packets range from a few bytes to more than a thousand bytes. Whenever a message is transmitted over the Internet, it is first partitioned into packets of appropriate size. Packets of each message may traverse the Internet following different routes to be reassembled at their destination point. The paths of packets are determined by routers which read packet headers and direct them in accordance with certain algorithms.

**Internet Access and Security**

The Internet backbone links the NAPs which provide access to the retail Internet Access Providers (IAPs), which in turn give access to consumers through typically narrow channels (called PPP or SLIP and ranging in speed from 2.4 kbps to 28.8 kbps). IAPs provide wider channels to organizations generally ranging from 56 kbps lines to 1.5 mbs (T1) lines.

While the geographic description of the setup (Figure 4) gives a feeling for the basic structure of the Internet, it is important to emphasize several factors:

- Each node of the Net typically is responsible for three costs: 1) the cost of its computer facilities, 2) communications costs to the access provider, and 3) access fees paid to their IAP.
- Internet access is not free but is often paid by an organization (i.e. a university or a corporation) rather than by individual users.
- In the Internet world, any node can be either a user of the Net (i.e. client) or a content/service provider (i.e. server), to the world.
- Typically, any Internet site which has content will tend to be a constantly connected node with its own Internet address (IP address). These numbers are translated to what is called “domain names” for access and contact by other nodes; and
- Traditionally “online services” (e.g. America Online,Prodigy and Compuserve) were distinct service providers, with their own content structure and access communication lines. During 1994 and 1995, online services became a more integral part of the Internet by providing gateways and access to the Internet (consequently acting as IAPs). Many predict that in the future online services will become a nearly indistinguishable part of the Net.

Large organizations will use “firewalls” to monitor, manage and limit access to their facilities as well as to increase the security of their installations. Firewalls act as computer gateways which allow employee remote sign-on. They also permit the passage of legitimate messages and connections from the outside world (see Figure 3).

A PPP/SLIP access typically means that when a client (user) accesses its provider, it is assigned a temporary IP for the duration of that session. Each site will typically have a

---

**Figure 3**

**Router**

Department LAN

---

**Figure 4**

**Internet Access and Security**

The Internet backbone links the NAPs which provide access to the retail Internet Access Providers (IAPs), which in turn give access to consumers through typically narrow channels (called PPP or SLIP and ranging in speed from 2.4 kbps to 28.8 kbps). IAPs provide wider channels to organizations generally ranging from 56 kbps lines to 1.5 mbs (T1) lines.

While the geographic description of the setup (Figure 4) gives a feeling for the basic structure of the Internet, it is important to emphasize several factors:

- Each node of the Net typically is responsible for three costs: 1) the cost of its computer facilities, 2) communications costs to the access provider, and 3) access fees paid to their IAP.
- Internet access is not free but is often paid by an organization (i.e. a university or a corporation) rather than by individual users.
- In the Internet world, any node can be either a user of the Net (i.e. client) or a content/service provider (i.e. server), to the world.
- Typically, any Internet site which has content will tend to be a constantly connected node with its own Internet address (IP address). These numbers are translated to what is called “domain names” for access and contact by other nodes; and
- Traditionally “online services” (e.g. America Online,Prodigy and Compuserve) were distinct service providers, with their own content structure and access communication lines. During 1994 and 1995, online services became a more integral part of the Internet by providing gateways and access to the Internet (consequently acting as IAPs). Many predict that in the future online services will become a nearly indistinguishable part of the Net.

Large organizations will use “firewalls” to monitor, manage and limit access to their facilities as well as to increase the security of their installations. Firewalls act as computer gateways which allow employee remote sign-on. They also permit the passage of legitimate messages and connections from the outside world (see Figure 3).

A PPP/SLIP access typically means that when a client (user) accesses its provider, it is assigned a temporary IP for the duration of that session. Each site will typically have a

---

**The upcoming advent of US$500 Internet computers and improved bandwidth access to the home will further increase computer user populations.**
definition of the type of services it provides ranging from basic e-mail to WWW services. Some sites can specialize in providing audio services, technical information through FTP, etc.

Audit and Control Issues

Figure 6 displays several concepts related to the Internet “hierarchy.” The Internet is purposefully anarchic. Its only central organization deals with standards, protocols and the establishment of domain names. Much of the administration is delegated progressively to lower and lower levels of the hierarchy.

While this architecture and relative absence of controls allows for nearly unlimited Internet growth, it can also cause problems associated with network congestion, lack of content control, limited standardization of nomenclature, security weaknesses, capacity planning, etc.

A Net server (that has context) will typically have a layer of software on top of its operating system for Net connectivity. The typical PC connected to the Internet, as described in Figure 7, will use a communications layer to connect Windows to a transport layer (say regular telephone twisted pair) and a browser/manager software (say Netscape) to interpret and present the data (files) obtained in the network. A more basic setup would be DOS-oriented using e-mail, telnet and lynx (a character mode browser).

Watch the Journal

Along with the opportunities, the Internet also added a major layer of risk to corporate information systems. While firewalls and careful monitoring of Internet access may somewhat mitigate corporate risks, anonymous access to corporate computer facilities greatly increase corporate risk. These risks and the IS control professional’s role will be discussed in a forthcoming article of this series to be published in the IS Audit & Control Journal.

Endnotes and Sources

4. A byte is a unit of information that consists of eight binary (0 or 1) digits.

Alexander Kogan, Ph.D.
is assistant professor of Accounting and Information Systems at Rutgers University in New Jersey, USA.

Ephraim F. Sudit, Ph.D., MBA
is professor of Accounting and Information Systems at the Rutgers University Graduate School of Management.

Miklos A. Vasarhelyi, Ph.D.
is a KPMG Peat Marwick Professor of Accounting at the Rutgers University Graduate School of Management.