Internet delivery of LIMS via the application service provider model

Javier Tejero and Mark Fish

The delivery of software as a rented service over secure networks via the Internet, commonly known as ASP (Application Service Provision-Provider), is receiving a great deal of attention in the business press. Today, it is firmly established as the hot topic within the computing industry. While it will certainly have a profound effect on the way software suppliers do business, it appears that ASP will have a major impact on the way corporate applications are deployed in the future. In industries as highly regulated and security conscious as the pharmaceutical industry, many progressive organizations are either currently exploiting or investigating the benefits of ASP as a means of accessing applications such as LIMS, on which they place such reliance. The global and decentralized nature of many organizations may lend itself particularly to ASP software deployment.

Fundamentally, ASP is a means of obtaining access to software applications without the need to buy expensive licenses and hardware or employ high-cost support resources. The application itself is hosted on a third-party site with system maintenance, backup, and recovery provided by a third party. Products and services can instead be rented for a contracted period on a fixed cost per user/per month basis. This rental service fee replaces the initial IT capital expenditure that is usually associated with major projects, such as the implementation of a LIMS. Such an arrangement, combining capital retention and a predictable cost of ownership, is especially attractive to the small- to medium-sized organization. Such organizations may have previously been forced to accept second best in their selection of a LIMS.

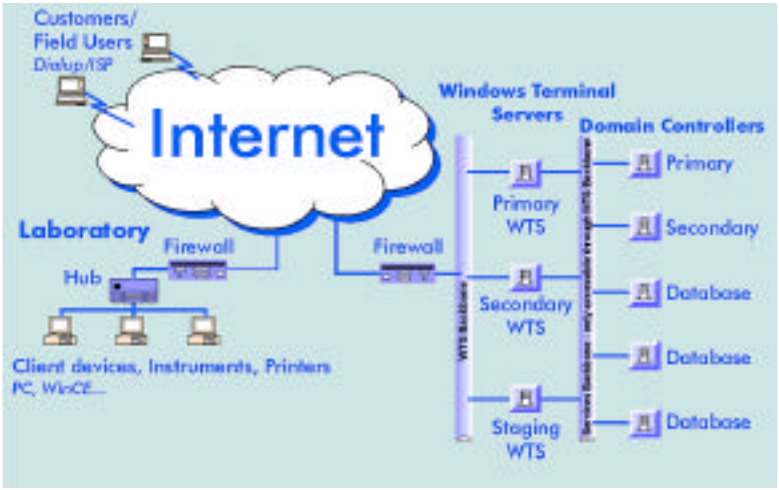

Figure 1 *LIMS via ASP-hosted installation.*

Many progressive organizations are either currently exploiting or investigating the benefits of ASP as a means of accessing applications such as LIMS.

To date, the great deal of hype surrounding the dawn of ASP has not been reflected by corresponding levels of adoption of LIMS implementations using the ASP model (see *Figure 1*). The IT industry can be held partly responsible due to a lack of clarity in what ASP offers. A high degree of cynicism has resulted, with serious doubts regarding the ability of ASP to meet corporate return on investment (ROI) goals. While little quantified data exist on the benefits of ASP, there are clear indications that it is here to stay. For example, in recently published research, spending on ASP in the health-care industry is predicted to increase from $125 million in 2000 to $599 by 2005 (**Gartner Group,** Stamford, CT).

The ASP industry has focused its communications on the savings to be made compared to a conventional local area network (LAN) deployment. *Table 1* highlights some of the hidden costs eliminated via an ASP software deployment.

Delivery of software via the ASP model is expected to benefit from the trend toward increased outsourcing of noncore activities. Over the last five years, in particular, both the chemical and pharmaceutical industries have seen major organizations outsource significant aspects of their operations, such as entire IT administration divisions and even strategic operations such as analytical services, as they focus

Table 1

Understanding total cost of ownership

Software as a product	**ASP: Eliminated hidden costs to the customer**
Licenses purchase (usually only 20–35% of total)	Hardware purchase and delivery
Application customization	Hardware installation and maintenance
Application training	Hardware upgrades
Software maintenance	Staff training in operating system, database, and application
	Tape handling and media costs
	Security tools, firewalls, physical server protection, operating system patch management

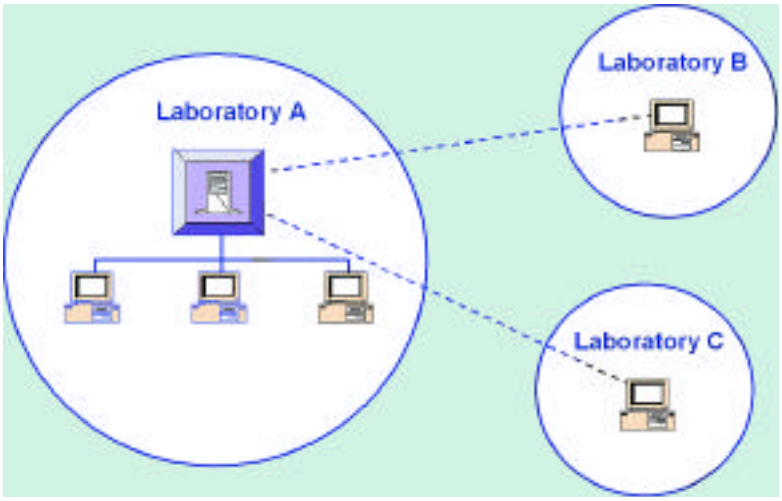

Figure 2 *Traditional LAN installation.*

on their core competencies. It appears that there are few, if any, business activities that are excluded in the trend to outsource; thus, the external hosting of LIMS applications will be part of this momentum. The contract research organization (CRO) industry has been considered the most likely early adopter for LIMS via ASP since it is more familiar with the outsourcing mode; indeed, its business is based on it. However, ASP requires more acceptance from its core markets, such as the large pharmaceutical companies, before there is serious commitment from CROs (see *Appendix*).

Under the ASP model, the human factors, in addition to many of the technical issues, surrounding LIMS selection and implementation still remain. By no means does ASP claim to be a solution for effortless LIMS implementation, but rather an alternative means of obtaining access to the application under a rented service agreement. Recruiting experienced specialists to handle project management, installation, and validation support is as important as in conventional implementations, as are issues such as obtaining user buy-in and management support for the project.

On the subject of system validation, ASP does raise some different considerations in demonstrating compliance during regulatory audits. In view of its recent focus on computerized systems, the U.S. FDA will likely scrutinize heavily, for example, measures to secure integrity in the data transfer from the customer to the third-party application host (issues related to data security are discussed in more detail below). As in conventional LIMS implementations, documented procedures need to be produced to cover the system's use and all system-related activities to ensure they satisfy regulatory requirements. Some forward-thinking LIMS vendors are now considering the specific validation support required by customers with ASP-hosted implementations.

Regarding regulatory compliance, since the introduction of 21 CFR Part 11 there has been much discussion as to whether an application delivered over the Internet can be defined in terms of an open or closed system. The Internet is by nature an open technology, and the instinctive response is that a system delivered over the Internet must be open. The increasing popularity and success of ecommerce applications such as Internet banking has helped change people's perceptions that the Internet can be made secure. An array of technology is available to effectively reduce the openness of the Internet, including the use of SSL and PKI encryption, complex authentication technology, dedicated routers and firewalls, and virtual private data networks that can make a traditional LAN look positively open in comparison. Irrespective of the open system issue, in pursuing the ASP concept in a regulated environment, some general recommendations can be made:

- Develop a strong technical agreement with the ASP partner clearly defining the responsibilities for compliance issues
- Develop a rigid audit process adapted specifically to the ASP market
- Be aware of the issues surrounding 21 CFR Part 11 and perform a critical technical analysis of the proposed solution.

Architecture options for implementation

There are essentially four main strategy options for a laboratory to consider in the implementation of a modern LIMS:

1. *Traditional LAN installation*. This is the standard client/server LAN setup (*Figure 2*). In a CRO operating multiple laboratories, the application would be hosted separately on a server at each site connected to PC clients, together with laboratory instrumentation and printers.

In this scenario, the LIMS is in-

stalled on both the clients and the server. System administration is required at each facility, including database maintenance and backups, installation and upgrades of client and server software, and user maintenance.

2. *Traditional WAN installation.* A WAN, or wide area network, is a computer network that uses telecommunications technology to span great distances, if necessary, and is usually adopted to connect disparate LANs together (*Figure 3*). In this configuration, the LIMS is installed on both the clients and a central server.

A centralized server helps reduce administration workload and offers the benefit of storing all of the CRO's LIMS data in a single, searchable repository.

3. *Centrally hosted thin client installation.* Again, using a multisite example, all system administration is managed at a corporate center, where the system is hosted and distributed to each site via a WAN or the Internet using a VPN (virtual private network) (*Figure 4*). This is often called an internally hosted ASP.

Thin client technology is not a new concept; the pharmaceutical industry has been exploiting its benefits for several years. The concept of the thin client is central to the delivery of LIMS via ASP. Essentially, it is an architecture in which all application processing is carried out on the server. Since the application is installed and runs entirely on the server, there is minimal processing footprint and disk space capacity required on the client.

Thin client technology removes the need to install complex applications on the clients. This reduces the overhead in terms of maintenance and hardware requirements. Modern applications of thin client technology enable complex applications to be run on client PCs using little more than an Internet browser. Windows Terminal Server (**Microsoft Corp.,** Redmond, WA) has become the industry standard technology for providing users with access to 32-bit applications via a browser.

In this scenario, each laboratory is free to focus on its core business and competencies. IT resources can be centralized and the expensive specialized skills, such as those possessed by a database administrator, are no longer required at each site.

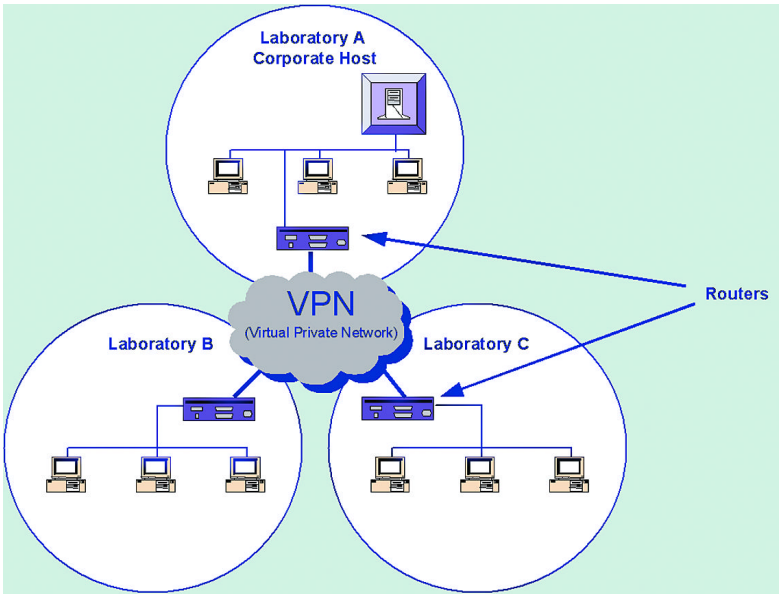

Figure 3 *Traditional WAN installation.*

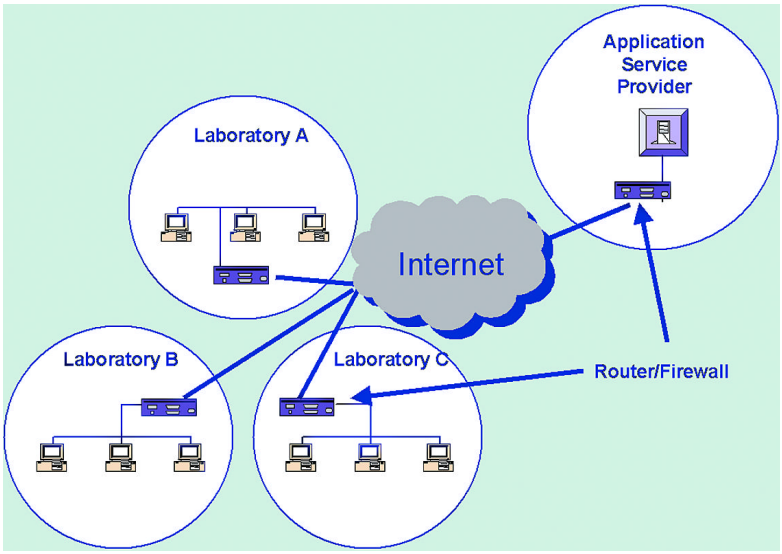

Figure 4 *Centrally hosted thin client installation.*

4. *ASP-hosted installation.* Using the true ASP model, a LIMS is hosted on a centrally managed server farm (directly connected to the Internet) and maintained by third-party IT specialists (*Figure 5*). Users access the LIMS using any Internet-connected desktop device with a standard Web browser. There is no requirement for application installation, maintenance, and technical support.

Ownership of the software licenses remains with the application vendor, while the data are owned by customers and held securely on their behalf at the server farm. Ownership of data should be one of the greatest concerns for organizations considering ASP deployment. It is crucial that the ASP agreement details how regular access to data is to be provided

and in what format the data are to be supplied to enable them to be utilized in conjunction with other applications should the ASP agreement be terminated. Such an agreement means that the client is protected if the vendor and/or ASP partner cease to trade. A further measure that the client can take to minimize risk is to insist on the provision of backup data (in a specified format and storage media) on a periodic basis.

Independent computing architecture

The use of client-independent architecture, such as that offered by Independent Computing Architecture (ICA) (**Citrix Systems Inc.,** Fort Lauderdale, FL) enhances Windows Terminal Server to provide more efficient performance and more flexibility in the use of client machines. The company also offers improved system management tools and local RS232 port, printer, and drive mapping.

A client-independent approach can result in very low cost of application ownership. Since applications reside and execute on the server, the time and costs of installing, configuring, and deploying applications to users is greatly reduced. Also, since only the graphical user interface (GUI) of the application is distributed to the client, virtually any device can access even the most sophisticated applications. This client-independent approach can distribute applications over any network to virtually any client device in any location and deliver performance similar to that experienced by users operating on a WAN. Performance is not dependent on the power or type of client workstations, whether they are high-end PCs, legacy (386, 486) PCs, Unix workstations, Macintosh systems (**Apple Computer,** Cupertino, CA), or network- and Windows-based terminals.

While server-based computing is usually perceived to drive up network usage costs, this is not the case with the ICA model. Only keystrokes, mouse movements, and screen updates are distributed to the client; thus high performance is possible even over low-speed connections. This approach not only reduces network traffic, but can improve performance and productivity for a WAN, Internet-connected, and remote dial-up users by as much as 10 times while using existing network infrastructure. Users can avoid the significant costs of network infrastructure upgrades for additional bandwidth and significantly reduce ongoing data communications service costs.

A further benefit is that users of the system receive the normal application GUI as opposed to an alternate Web view. This means they can take advantage of the full, rich user interface of an application.

Benefits of ASP

The benefits of obtaining LIMS via an externally hosted ASP delivery mechanism fall into two broad categories. First, the technology acquisition costs are stretched out rather than compressed into the front end of the transaction. Second, resources required to subsequently manage the solution are outsourced, so that the user need not invest in expensive in-house support skills and can focus more resources and capital on strategic business issues.

Business operations

1. The application can be up and running on a new machine within very short time periods, and customers can realize the benefits of their investment sooner. Additionally, ASP means that configuring machines for a new workgroup is not required.

2. The LIMS can be delivered precisely where and when it is required. This includes rapid installation in a new laboratory several hundred kilometers away. With ASP rental agreements, price barriers are lower and market-leading LIMS applications become more affordable for smaller organizations. Also, the significant burdens that can be imposed by configuring hardware and operating systems are eliminated.

3. Users can transfer business focus from IT issues to laboratory objectives.

Total cost of ownership

1. There are minimal up-front costs for hardware and software, with better capital retention. Second, because processing requirements for running ASP are smaller, overall hardware costs are lower. ASP performance does not deteriorate if a lower-specification desktop is used to access the LIMS. With all the processing being performed centrally, there is no requirement for a powerful computer to ensure good performance. As little as a 386 Pentium 90 PC (**Intel Corp.,** Santa Clara, CA) with less than 100 MB of space is sufficient.

2. Payment is only for the number of users needed, when they are needed, thereby eliminating unnecessary software licensing.

3. IT costs become much easier for the customer to predict, with no unexpected hardware or software upgrade costs. This is a particularly popular aspect of ASP delivery with IT departments.

4. Nonstrategic IT staff costs are reduced, and in-house IT staff are able to focus on business development and new services instead of system and application maintenance. This can also alleviate recruitment problems and have a positive effect on staff retention.

Improved reliability, scalability, and flexibility

1. Predictable service levels are supported by service level agreements. Network up time and security are improved by putting the service into a formal, managed framework.

2. Third-party ASP architecture IT experts provide best practice management of systems, with continual review and updates as the business requires, in line with the most recent IT developments. The customer relinquishes responsibility for capacity, upgrades, and backups.

3. ASP has the ability to expand facilities to meet peaks in user demand, without having to upgrade server systems. The ASP "pay as you go" approach means that

more users can be added as and when required.

4. ASP is inherently scalable, and will meet any demand that might arise without a quantum change in applications or infrastructure.

Validation in required environments

1. The application is installed on the server in a controlled environment, eliminating the possibility of configuration being compromised through end users introducing incorrect DLL files or viruses.

2. Actual ASP installation is managed by ASP specialists, meaning less training records for the laboratory to administer.

3. Installation qualification is not required for client devices since no LIMS-specific software is installed.

4. Client devices can be of minimal footprint, with no need for hard disks, diskettes, etc.

5. With data being physically off-site under the control of an independent organization, the possibility of incidences such as malicious employees tampering with results is minimized.

Critical success factor

Data security and protection

In research conducted by **Datamonitor** (London, U.K.), the greatest single concern over ASP among end users was data integrity and security (more than 80% of respondents raised it as a major concern). Especially in regulated industries, this concern is even greater. As they travel over the network, data acquired on the LIMS can be secured using 128-bit encryption (such as SSL [secure socket layer]) (see Appendix) technology, which is considered the highest available. All reputable ASP hosting companies operate extensive physical security measures, including round-the-clock guards, at their data centers. The levels of security provided can exceed those found at a typical pharmaceutical R&D or manufacturing location.

Security in an ASP environment is critical and should be thought of in terms of an end-to-end process. One can think of the delivery of an Internet application in terms of delivering other high-value goods.

1. *Perimeter security.* Firewalls, intrusion detection, operating system patches, and virus protection in addition to actual physical security measures are used to ensure that a client's data are securely hosted.

2. *Access security.* Password policies and controls for the application and database, audit trails, backup policies and processes, and disaster recovery plans for the application and hardware can all help ensure that access to data is secured.

3. *Security in transit.* Network security, private data networks, SSL encryption, and virtual private data networks (VPDN) can all help ensure the security of data in transit. These technologies are like the armored cars of the Internet world.

Firewalls

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. A company that provides Internet connections for its workers will install a firewall to prevent outsiders from accessing its own private data resources and for controlling access to outside resources among its own users. Firewalls work closely with a router program, examining network packets to determine whether they should be allowed to pass or be blocked. A firewall also includes, or works with, a proxy server that makes network requests on behalf of workstation users based on a set of rules. For mobile users, firewalls allow remote access to the private network by the use of secure log-on procedures and authentication certificates. A case in point is the use of Clinical Trials Management Systems by remote Clinical Research Associates over the Internet. This has been accepted practice for a number of years and arguably manages some of the industry's most sensitive regulatory data.

System performance

Between the application hosted on the central server and the clients (user desktops), the only network traffic is screen pixel changes, mouse clicks, and keystrokes. Therefore, the loading is minimal, and with powerful servers, users of applications delivered by the ASP model can experience improved system performance in comparison to conventionally implemented applications.

The software vendor and ASP partner

Without a high degree of confidence in both application vendors and their ASP partners, the concept of hosting mission-critical IT applications off-site is not something that would be welcomed in the industry.

Since the inception of the ASP model, the track record of specialist IT application vendors (e.g., LIMS vendors) has been generally disappointing. This can be partly attributed to the newly emerging, and therefore unproven, technology with which they have been working. However, a more common factor in this lack of success has been the challenges posed by offering ASP as a total in-house hosted service themselves. Hosting applications using the ASP model requires an entirely different set of skills than those possessed by a specialist software developer. To address this, a booming ASP hosting industry has emerged with the necessary specialist skills, facilities, and security to deliver applications successfully over the Internet. In addition, the economies of scale and IT industry best practice that the ASP hosting company can provide benefit to both the end-user customer and the application vendor. Some of the world's biggest corporate names in both computing and telecommunications have made significant investment in the area of ASP. The adoption of such organizations as ASP partners by LIMS vendors should help alleviate end-user concern over picking

up the pieces after an ASP partner goes out of business.

Where the LIMS vendor offers ASP delivery via a hosting company, the end-user customer requires reassurance regarding who has responsibility for servicing and supporting the LIMS. A single point of contact is required for efficient resolution of problems. Ideally, the responsibility for managing the delivery of the complete solution via ASP should rest with the LIMS vendor, whose agreement with the hosting company should be imperceptible to the end-user.

Reliability; proven methodologies and best practices; service organization and industry expertise; use of modern, proven technologies; a stable and functionally comprehensive solution; and worldwide integrated support structure are as applicable for selecting a vendor and LIMS solution for delivery using ASP and are in themselves critical to the success of a project.

Conclusion

The practice of outsourcing noncore business operations is a trend with a great deal of momentum. However, in the pharmaceutical industry, there has been an understandably cautious approach to outsourcing the hosting of mission-critical IT applications and data handling in general. Nevertheless, deployments of internally hosted LIMS via ASP in the pharmaceutical industry are common, suggesting that organizations are testing the waters as regards technology to support externally hosted LIMS via ASP.

From the customer's perspective, the benefits of obtaining an application via an externally hosted ASP delivery mechanism fall into two broad categories. First, the technology acquisition costs are stretched out rather than compressed into the front end of the transaction. Second, resources required to subsequently manage the solution can be outsourced. Certainly, the technology to ensure data security is now available, and highly configurable LIMS applications exist that lend themselves well to secure delivery over the Internet. Whether organizations considering ASP delivery of LIMS choose to adopt it or not, the significant business benefits of ASP can be extremely difficult to ignore.

Mr. Tejero is Director, and Mr. Fish is Business Development Manager, Pathfinder Global Services Group, ***Thermo LabSystems,*** *St. Georges Ct., Hanover Business Park, Altrincham, Cheshire WA14 5TP, U.K.; tel.: +44 (0) 161 942 3000; fax: +44 (0) 161 942 3001; e-mail: mark.fish@thermolabsystems.com.*

Appendix

Explanation of terms

1. *LIMS.* A LIMS is a laboratory data and information management system consisting of computing software and hardware to manage the daily operation of a laboratory, allowing laboratory management better control and allocation of resources. A LIMS offers a flexible technological solution to suit different laboratory, and industry requirements, and assists both the R&D and manufacturing QC functions to meet the regulatory requirements with audited data. Laboratory managers are better able to control testing procedures while keeping track of information, in addition to being provided with the tools to report data and results in a format that satisfies the rest of the organization.

The Nautilus LIMS (**Thermo LabSystems,** Cheshire, U.K.) is offered for delivery as an ASP service over secure networks using Internet technology. It offers an alternative to up-front capital purchase of software licenses and computing hardware. By making the LIMS available as a hired service delivered over the Internet, even the smallest laboratories can benefit from an acclaimed LIMS solution running on highly scaleable, reliable, and secure IT infrastructures.

A single monthly fee covers: rental of the LIMS software licenses; hosting of the application and data; management of the computing infrastructure, including networking and servers; software, including operating system, databases, and the application; and backups, upgrades, and help access. The total cost of ownership of LIMS is reduced since customers only pay for software as they use it. **Thermo LabSystems** and its partners provide all system management functions as part of the ongoing monthly usage charge.

Users access Nautilus LIMS using any Internet-connected desktop device, with a standard Web browser. There is no need for local application installation, maintenance, and technical support beyond the simple ICA client.

2. *SSL.* SSL, or secure socket layer, is a commonly used protocol for managing the security of a message transmission on the Internet. SSL is included as part of both the **Microsoft** and **Netscape** browsers (Mountain View, CA) and most Web server products. Developed by **Netscape,** SSL has also gained the support of **Microsoft** and other Internet client/server developers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

3. *VPN.* A virtual private network (VPN) sometimes referred to as a virtual private data network (VPDN), can be thought of in terms of delivering the same security and capabilities of a private LAN or WAN used by one company, through the public telecommunication infrastructure, at much lower cost. Privacy is maintained through the use of tunneling protocols and security procedures. Use of a VPN involves encrypting data before sending them through the public network and decrypting them at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Many VPN network use Point-to-Point Tunneling Protocol (PPTP) developed by **Microsoft, 3COM Corp.** (Santa Clara, CA), and others.