Corporate Remote Access Alternatives

iPass White Paper

Table of Contents

Executive Summary

Organizations requiring widespread remote access will find significant savings in Internet and VPN solutions using iPass Corporate Access versus traditional in-house modem pools. iPass Corporate Access adds global coverage and improved quality of service to Internet access solutions.

Overview

A growing number of organizations are interested in providing easy, cost-effective remote network access for their employees to improve availability to applications such as electronic mail, database and sales force automation applications, and intranets. Factors driving this interest include an increasing appreciation of the role of information management as a source of competitive information, the rise of technology that makes remote network access simple and practical, and organizational and workforce changes.

To implement remote network access (referred to as remote access), companies have a number of options available to them, each with their own set of advantages and disadvantages. Some of the most commonly examined options for providing corporate remote access include the following:

- **Public switched telephone network (PSTN)-based solutions** -- These include modem banks, telephone lines, 800 numbers and remote access servers.
- **Integrated services data networks (ISDN)** -- This is a digital upgrade to PSTN, offering up to 128Kbps of channel capacity on a single basic rate interface (BRI) line.
- **Asymmetric digital subscriber line (ADSL) and cable modems** -- These are two emerging technologies designed to leverage the existing telephone and cable television infrastructure to provide high-bandwidth data access.
- **Wireless data networks** -- These use wireless technology to provide continuous untethered access to corporate data and applications.
- **Internet access and virtual private network (VPN) technologies** -- These leverage the global, public Internet to provide secure, remote access.

For companies that need to provide access to the corporate network from a wide variety of locations, PSTN and Internet-based solutions with VPN technologies are the only practical solutions. While setting up a simple modem-based solution for corporate access has a low entry cost, expenses rapidly escalate as the volume of users and their geographic mobility increases. Corporate remote access solutions based on Internet and VPN technologies are highly cost-effective. (Appendix A shows a sample savings calculation for iPass Corporate Access versus modem banks and phone lines, with average savings of 75%.)

For an Internet-based strategy to be effective, however, companies need to carefully consider the capabilities of their Internet access provider, weighing issues such as service coverage, interoperability, security, quality of service, and ease of deployment and use. For reasons of service coverage alone, a single service provider may not be able to meet all of these criteria. Some ISPs have sought to address this by entering into "alliances" with other ISPs. These solutions are fraught with problems of security, accounting and scalability. The iPass Corporate Access solution, which provides remote network access through a number of top-tier ISPs and carriers, emerges as the premier solution for telecommuting and roaming users.

Business Case for Remote Access

The market for remote access products and services is one of the fastest growing markets in the technology sector. Remote access describes the technology and services used to establish and maintain a temporary connection to a corporate network for the purposes of exchanging information and running applications. These applications may include the following:

- Electronic mail
- Database applications
- Sales force automation (SFA)
- File/data replication
- Intranet office productivity

Providers in the remote access market include hardware vendors of remote access switches and modems; software vendors of operating systems, virtual private network (VPN) solutions; and service providers vendors of private, wide-area networking (WAN) and value-added networking (VAN) services. With the proliferation of the Internet, and the availability of security products that ensure data privacy over public networks, regional and national ISPs are increasingly seeking opportunities for growth by providing remote access solutions to the corporate market. According to Dataquest, the total remote access market is projected to grow from $2.6 billion in 1995 to $12 billion in 2000.

Business Drivers

Before examining the various options available for remote access, it is useful to consider some of the business requirements behind it. Primary among these are competition, technology, and changes in organizations and workforces.

Information as a Source of Competitive Advantage

Companies are becoming increasingly aware of the role of information as a source of competitive advantage. For example, companies can leverage information and develop new products and services that create superior value for their customers. In many organizations today, product development teams are cross-functional, cross-divisional, and even cross-company. With the trend toward "virtual enterprises," companies are partnering with others. Remote access technology is used to allow people to work together effectively using electronic mail, calendaring/scheduling software and other groupware products, often from geographically diverse locations and across different time zones.

Another way companies leverage information for a competitive advantage is by allowing their employees to learn more about customers and their needs, and therefore allowing them to deliver superior customer service. SFA and customer service applications are among the fastest growing segments in the package application market. In this case, remote access allows a salesperson working out of a field sales office, a home office, a customer site or a hotel room, to gather information about customer behavior. This enables the company to respond more quickly and efficiently to customer needs

Technology

Business adoption of new technologies is also driving the need for remote access. One prime example is the rise in popularity and use of the Internet - which has accelerated the need for remote access. The Internet, along with its host of service providers, forms a vast, global remote access network. Organizations and vendors, appreciating the value of having a ready-made public infrastructure for communication, have rushed to find ways to employ it for private communication in a secure fashion. In response, vendors have

introduced products designed to bring about "virtual private networks" (VPNs), where data is accessed and transported over the public Internet in a safe, reliable and secure fashion.

Organizational and Workforce Changes

Finally, recent years have seen a dramatic change in the nature of corporate organizations and workforces. Organizations are typically less hierarchical, and much of the work is done by cross-functional teams. Team members working on a project may be located on different floors of the same building, different company locations, or even different countries.

In addition, typical workers are much more mobile today with respect to their careers and employers. Companies have come to appreciate the need to identify and recruit top talent wherever they find it. This means accommodating workers preferences for domicile, working hours and telecommuting. In light of these organizational and workforce changes, remote access technology has become part of the essential "glue" that holds work teams together.

Remote Access Alternatives

When it comes to remote access, organizations have a number of different options available to them. These vary considerably in cost, service coverage, throughput and suitability for various applications. We briefly review some of the more popular options available for use in corporate environments. These include the following:

- Public switched telephone networks (PSTN)
- Integrated services data networks (ISDN)
- ADSL and cable modems
- Wireless data networks
- Internet and VPN technologies

Below, we describe each option and its relative advantages and disadvantages.

Public Switched Telephone Networks (PSTN)

The PSTN approach is a typical in-house remote access solution, consisting of a modem bank, telephone lines and a remote access server (Figure 1, next page). Additionally, sites might elect to deploy a toll-free "800" number to provide remote access to domestic roaming users.

PSTN's primary advantage is that the entry cost for a small-scale deployment can be very low. For the lowest entry point, all that is needed is a Windows NT server, modem and a telephone line (Windows NT has remote access service built into the server). However supporting larger numbers of users quickly becomes a problem, requiring a support staff plus the purchase and deployment of dedicated remote access servers, modem banks and multiple telephone lines. In addition, most of the costs associated with this solution are "fixed" with respect to the number of users. Accommodating additional numbers of users during peak usage hours involves expanding the capacity of the modems, whether that capacity is needed all the time or not. Connection costs for users whom roam across national boundaries becomes problematic as toll charges mount. Furthermore, dependency on the telephone infrastructure for reliable data transport can cause problems in many areas of the world where quality toll connections are not available.
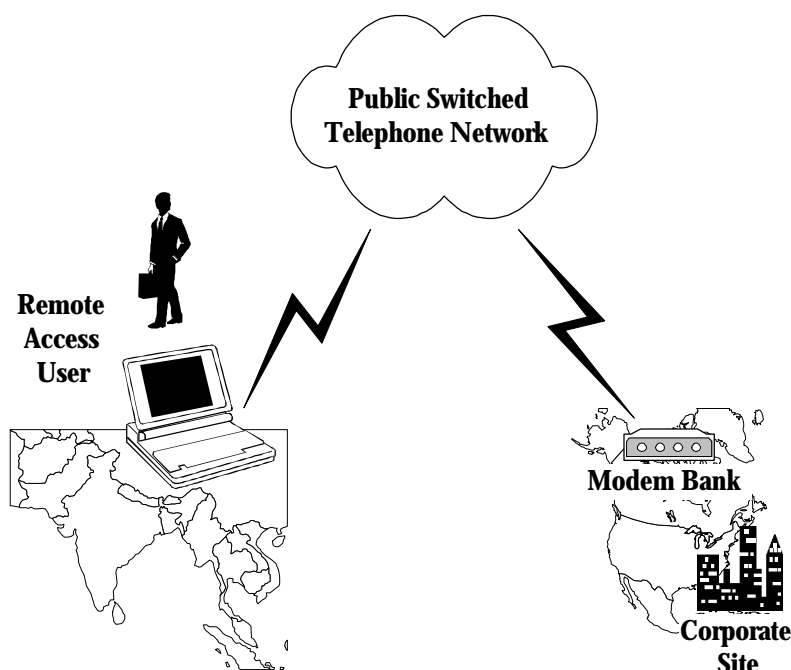
Figure 1: Traditional in-house PSTN remote access solution

Integrated Services Data Networks (ISDN)

ISDN technology has been available since the early 1980s, and represents an end-to-end digital upgrade to PSTN. A typical solution involves lines and equipment provided by an ISDN service provider, a remote access server with ISDN support and an ISDN bridge/router. Like PSTN, ISDN users are only charged for the duration of their connection.

ISDN's primary advantage is its improved bandwidth over PSTN. A BRI can reliably carry data at 128 Kbps without the use of data compression technology (as opposed to a maximum of 56 Kbps for PSTN solutions). With the use of data compression technology, throughput can be even higher. However, ISDN has many of the same cost disadvantages as PSTN solutions for remote access. Organizations must purchase and administer phone lines and remote access equipment. Plus, adding capacity to service additional users can be expensive. In addition, ISDN is not available in all areas and cannot be used reliably across provider boundaries. Therefore, ISDN can provide a satisfactory solution for telecommuters living in an ISDN service area with high bandwidth needs, but is not suitable for the roaming user.

Asymmetric Digital Subscriber Line (ADSL) and Cable Modems

ASDL and cable modems are two emerging technologies that take advantage of existing copper wire infrastructure. Both technologies make use of an "asymmetric" channel, meaning that downstream and upstream access may be at different rates.

ADSL uses standard twisted-wire telephone lines to provide high-speed connectivity to the Internet (through a participating Internet service provider) and/or corporate LANs. ADSL generally provides downstream data rates from 1.544 Mbps to 9 Mbps. Upstream rates are 16 Kbps-640 Kbps. An example of an ADSL service is Pacific Bell's FasTrack DSL service, which provides customers in limited service areas with 1.544Mbps downstream and 384Kbps upstream. To connect directly to the corporate LAN, businesses must connect to Pacific Bell's switched data network.

Cable Modems are another "asymmetric" technology used to provide high-speed access to the Internet through the existing cable television infrastructure. Because of the nature of the cable television network,

cable modem services provide variable downstream performance, typically in the 1.5 - 3Mbps range, depending on how much traffic is on the network. This can be used in conjunction with VPN technology to provide a secure corporate remote access solution. A typical example of a current service using cable modem technology is the Cox@Home service offered by Cox Cable. Cox Cable is currently available in a number of markets throughout the United States.

ADSL and cable modems are promising as a cost-effective means of providing high speed corporate remote access to telecommuters and day-extenders, who are in fixed and known locations. However, both solutions require special lines and equipment at the remote site and are very limited in terms of service area. As a result, these solutions do not represent a viable solution for roaming corporate users.

Wireless Data Networks

Wireless data networks allow roaming users, connecting with laptop computers, WindowsCE machines or PDAs, to have continuous untethered access to messages and corporate data. To implement a wireless corporate remote access solution, a corporate customer connects to a wireless network service provider through a leased line. The end-user device must be equipped with a wireless modem, which allows it to send and receive data over the wireless network.

The primary advantage of wireless solutions is the high degree of mobility they provide. Users can connect anywhere, even where no telephone lines are available. However, this mobility comes at a rather steep cost.

There are three primary disadvantages to corporate access via wireless networks:

- **Data Rate** - Data rates are typically much lower than those supported by wireline solutions. For example, one major service provider, ARDIS, supports only 4800 bps in most of its coverage area. Another service, RAM, supports 9000 bps.

- **Coverage and Reliability** -- Coverage and reliability for wireless solutions can be rather spotty. For example, ARDIS offers service coverage for the top 400 metropolitan areas in the United States. In general, the ability to roam across national boundaries with these services is very limited. Also, being wireless, the robustness of the connection can be effected by buildings and other obstructions. Applications used with wireless services must be able to tolerate frequent dropouts and data errors.

- **Cost** - Cost for wireless solutions are higher than wireline solutions. This expense includes the cost of the service itself, as well as the cost of the end-user equipment required. For example, hardware costs for ARDIS or RAM Mobile Data Services can run $500 - $700/user.

As a result, wireless remote access solutions tend to be suitable for specialized users and applications. They are not suitable for broad groups of telecommuters or day extenders, people who have to travel across national borders, or applications with high bandwidth requirements (such as file transfer and database transactions).

Internet and VPN Technologies

The proliferation of the Internet has led many companies and vendors to investigate using it as a means of low-cost, reliable and secure remote access to the corporate network. Typically, all that is required at the company site is connectivity to the Internet (which almost all companies already have) and the appropriate access control technology. In addition, the optional deployment of virtual private network (VPN) solutions allows companies to ensure privacy of the data that travels through the public infrastructure (Figure 2).
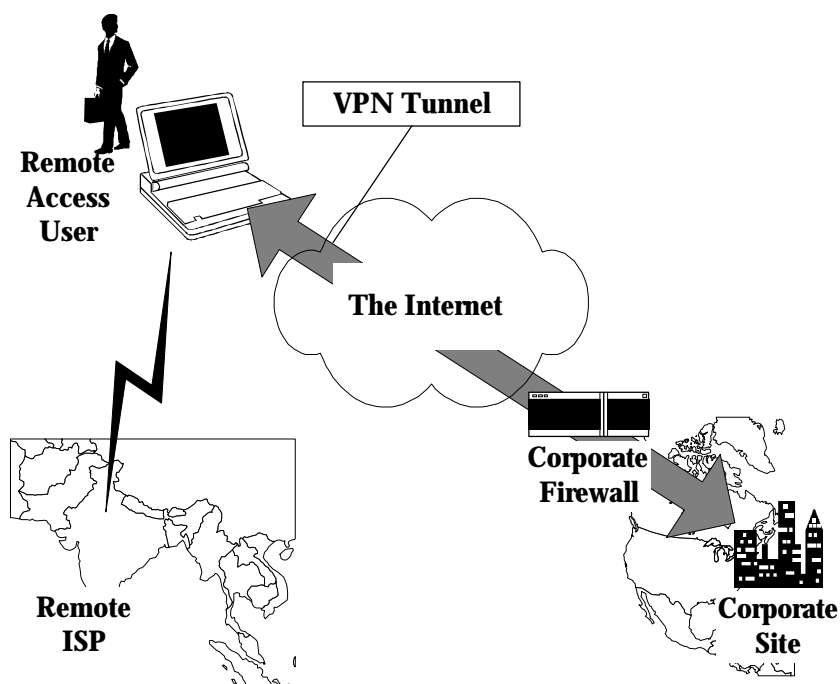

Figure 2: VPN remote access solution

The primary advantages of Internet remote access solutions, coupled with VPN technology, are cost effectiveness, superior coverage and scalability. One potential problem, however, involves user administration. Typically, assignment of user names and passwords must be coordinated with an ISP. In addition, local ISPs specialize by geographic area, causing gaps in their service coverage. In order to get sufficient global coverage the company or remote user might require arrangements with multiple ISPs, further complicating matters. iPass Corporate Access addresses the coverage, user authentication and cost problems raised by local ISPs.

Comparing the Alternatives

Below is a table comparing the remote access alternatives described above based on costs, performance, coverage and suitability for various user applications.

As the table illustrates, corporate remote access alternatives differ considerably in a number of key factors. Some meet the high bandwidth needs of developers and other "power" users, while others are targeted for applications that require continuous connectivity while roaming within a defined service area. For a company requiring remote access for telecommuters, day extenders and internationally roaming users, the only viable alternatives today are PSTN-based solutions involving phone lines and modem banks, or using the Internet with VPN technology.

Criteria	PSTN (Phone lines and modem banks)	ISDN	ADSL	Wireless Data Networks	Internet Access (VPN)
Typical fixed costs	Modems, remote access servers, phone line installation; inexpensive modem at remote site	ISDN line and equipment, remote access server, ISDN bridge/router; ISDN line and equipment at remote site	Corporate connectivity to provider's ATM cell relay service; ADSL modem and line at remote site	Leased line to wireless network service provider; wireless modems on end-user equipment	If not through existing ISP, requires network connectivity and Internet router; standard phone line and modem at remote site
Typical variable (usage-related) costs	Connect time	Connect time	None (charges based on capacity)	Data transferred	Connect time
Maximum throughput	56Kbps	128Kbps and above	384Kbps upstream, 1.544Mbps downstream (typical)	4.8 Kbps to 19.2 Kbps (typical)	56Kbps
Coverage	Geographically limited; national with 800 number	Limited to service areas	Limited to service areas	National, in major metropolitan areas	Local to global, depending on service provider
Suitable for telecommuter or day-extender use?	Yes	Yes	Yes	No	Yes
Portability for roaming users?	Yes	No	No	Yes	Yes

Solutions based on the Internet and VPN technology offer a number of advantages over in-house, PSTN-based solutions. Principal among these is cost. The cost of deploying and maintaining an Internet-based remote access solution is generally much less than that for an equivalent in-house modem solution. As an example, Forrester Research provides the following table of cost comparisons for companies who support a population of 1,000 remote users per year.

	PSTN-based solutions	Internet-based solutions
Phone/ISP charges	$1.08M	$.54M
User support	$.30M	$0 (included in user access costs)
Capital expenses	$.1M	$.02M
T1 lines	$.02M	$.03M
Total	**$1.5M**	**$.59M**

The value of an Internet-based remote access solution is even greater when users roam extensively. An Internet access provider with a global presence can save companies a considerable amount of money in toll charges when users connect from overseas and remote corners of the world.

What to Look for in an Internet Access Provider

Clearly, using the Internet and VPN technologies is a compelling alternative for companies looking to provide remote network access for their roaming and telecommuting users. One key to making a remote access VPN pay off is careful selection of the Internet access provider. Highlights of a few of the major considerations are shown below:

- **Coverage** - The Internet access provider should have points of presence (POPs) in every location where users may need to connect.

- **Interoperability** - A remote access solution should be interoperable with a large variety of authentication platforms, firewall and secure VPN solutions. This minimizes integration requirements and allows businesses to select the security solutions that best meet their remote access and networking needs.

- **Security** - There are several security concerns for companies implementing an Internet-remote access solutions that should be examined. With regards to the Internet access provider, a major concern is preventing fraud by users who gain access to public networks (such as the Internet) through compromised user credentials. User IDs and credentials should be managed locally, if possible, and a security infrastructure should be in place to protect these from compromise if they travel over the public network.

- **Quality of Service** - This can mean a number of things: availability, throughput and reliability (to name a few). When selecting a corporate remote access solution considerable thought should be given to quality of service issues such as these. Users want to connect with enough speed to quickly send and retrieve email and other information. They do not want to get busy signals or discover the network is down when trying to dial in. To ensure reliability there must be redundancy in every component of the solution, particularly at the point of dial-up access. Remote access solutions should also scale gracefully to accommodate a large number of users at times of peak usage.

- **Ease of Deployment and Use** - Regardless of the remote access solution selected, it must be easy to deploy, support and maintain. The solution must be simple for non-technical mobile workers and telecommuters to ensure they can connect easily and to minimize support requirements.

The iPass Corporate Access Solution

iPass Corporate Access provides an ideal Internet-based remote access solution for organizations and it is interoperable with all VPN and security solutions. The iPass service is easy to install and deploy, it generates a single, consolidated billing statement, and it provides users with immediate access to more than 3,000 dial-up POPs over 150 countries.

iPass Corporate Access represents a new model for providing Internet access to corporate users. Though iPass' industry-leading settlement and clearinghouse platform, iPass is able to aggregate many different top-tier Internet access provider networks into a single, multi-service provider solution.

Some ISPs have tried to address the service coverage issue by entering into a series of bilateral relationships with other ISPs agreeing to carry each other's customers and traffic. However, there are at least three issues that cause difficulty with such an arrangement: security, accounting and scalability. Technical integration between service providers to provide secure authentication and transport across a publicly accessible network can be extremely difficult. Accounting mechanisms to share costs can also be complex. The problem is complicated further as the provider seeks global coverage and must enter into relationships with not just one or two other providers, but hundreds of other providers. This scenario does not scale well, and the complexity of managing these relationships significantly increases each time a new ISP is added to the equation.

The iPass trusted, third-party clearinghouse service solves these problems by providing a robust, global platform for third-party authentication, authorization and settlement of Internet use. This transaction model has been proven in many other industries. For example, the banking industry has developed ATM networks, such as Cirrus, Plus or the Star System, for individuals to maintain one banking relationship and still get access to funds from other banks. iPass Corporate Access works the same way, transparently enabling Internet access through multiple, top-tier service providers and carriers throughout the world. When used in conjunction with VPN technology, this solution provides reliable, secure corporate remote access from virtually anywhere.

Service Features

iPass Corporate Access has a number of features that make it the ideal choice for Internet-based corporate remote access. Some of these are described below.

Coverage

The global Internet, with all its service providers, provides a reliable, low-cost infrastructure for connecting to a corporate network through the PSTN. However, even "global" Internet service providers have difficulty providing POPs in every location users want them. By contrast, the iPass Corporate Access solution provides access to more than 3,000 network POPs in over 150 different countries. This ensures roaming users are able to connect with a local telephone call from all over the world.

Interoperability

iPass Corporate Access can be used to supplement an existing remote access solution, or can provide a complete replacement for a company's existing remote access infrastructure. It was designed with completely open system architecture and is interoperable with all-common firewall and VPN solutions to ensure end-to-end data integrity and security. Companies benefit from the partnerships iPass has with many leading hardware and software companies. These companies include Microsoft, Ascend, Cisco, Check Point, Compaq/DIGITAL, Lucent/Livingston, Portal, RADGUARD, VPNet, V-ONE, RedCreek, Aventail, i-Planet, Secure Computing and many others. Through some of these partnerships, the iPass technology is integrated into other networking and security products so they are "iPass Ready", making it even easier for an organization to implement iPass if it is already using one of these products.

Security

iPass Corporate Access provides comprehensive access control through compatibility with industry-standard access control solutions such as RADIUS, TACACS+ and firewalls. Users can authenticate themselves through either "simple" authentication using a username and password, or by the use of hard-token credentials. Either way, user credentials are protected by 128-bit key secure socket layer (SSL) encryption as they travel through the Internet to the corporate server. Furthermore, a third-party Transaction Center participates in all service transactions, enabling the detection of fraud or unusual service usage patterns that indicate compromise of these credentials.

In the fall of 1997, the Roaming Operations Working Group (ROAMOPS) of the Internet Engineering Task Force (IETF) asked iPass to submit its secure authentication model for roaming as the basis for a secure roaming standard. This model was presented at the December 1997 IETF meeting and has gained widespread support from other industry leading equipment and service vendors. Other solutions, using authentication via proxy RADIUS servers and RADIUS shared secrets, have been judged inadequate because they involve sending a clear-text message over the Internet, providing a significant possible point of security failure. By securing all message exchanges using SSL, iPass offers the most secure and flexible roaming implementation in use today.

Quality of Service

The ISPs and telcos that provide access to the iPass network are top-tier providers from each region of the world and must meet stringent performance criteria in order to participate. Companies providing the Internet access for the iPass network include UUNet Technologies (Worldcom), CompuServe Network Services (Worldcom) GTE Internetworking, EQUANT, Hong Kong Telecom, NEC, NTT PC, and other top-tier regional providers. Redundant coverage in many cities worldwide by multiple participant service providers allows customers to find available access points even if one provider has a busy POP or suffers a temporary network outage.

iPass helps ensure reliability of the overall network by operating dual-redundant Transaction Centers around the world in secure sites with 24 x 7 system monitoring. Each iPass Transaction Center has a primary and secondary server, and each POP has a primary and backup Transaction Center for the routing of authentication requests and accounting detail. In addition, iPass runs continuous random testing of the entire network to monitor quality of service.

Ease of Installation and Use

The iPass RoamServer software can be installed in just a few hours. Once the software is set up and tested, virtually no maintenance is required. In addition, end-user deployment is simple. The iPass client solutions - Dial Wizard for Windows 95/98 and Macintosh, or Microsoft Connection Manager for Windows 95/98/NT - can be quickly installed by a remote access user by launching a simple point-and-click install program. After that, remote access users use a point-and-click interface to select a location and phone number to dial.

How iPass Corporate Access Works

The iPass Corporate Access solution consists of three major components:

- The iPass network
- The iPass RoamServer
- The iPass connection software

We describe each of these components below, and then describe how they work together to provide a global Internet access solution.

The iPass Network

Corporate customers connect to the iPass Network through their current Internet connectivity solution. The iPass Corporate Access service is composed of a group of top-tier ISPs and network service providers. Based on TCP/IP, as of October 1998, the network has more than 3,000 dial-up access points, in over 150 different countries throughout the world. In a fashion transparent to the user, the iPass network records each user session, passes logon credentials to the appropriate corporate remote access server, and performs settlement between the various service providers involved.

The iPass RoamServer

The iPass RoamServer is a software application approximately 1.6 Mbytes in size that can run on the same system as the company's authentication server, or on a separate system. The RoamServer responds to connection requests from roaming users and allows organizations to manage their own user lists and control their user access to the system through the authentication system of their choice. The RoamServer supports Microsoft Windows NT, Sun Solaris, Sun SunOS, IBM AIX, SGI IRIX, DIGITAL UNIX, HP-UX, BSDI, FreeBSD and Linux.

The RoamServer decrypts user credentials and checks their validity against the corporate remote access authentication server. This might be RADIUS, TACACS+, Windows NT domains, or any of the other authentication systems that integrates with these solutions. This may be a "simple" authentication based on username and password, or a system based on hard tokens. Token-based authentication refers to the use of special one-time passwords generated by a security server. Token-based authentication systems are generally considered to be more secure than password-based systems. A user is typically required to have a "token" in their possession when logging on to the corporate network, as well as a password or PIN. Token cards for a typical token-based authentication system, the SecurityDynamics ACE server, is shown in Figure 3. The iPass RoamServer interfaces with a variety of token-based authentication systems, such as the Security Dynamics ACE Server, through RADIUS and TACACS+ authentication servers.

Figure 3: Token cards for the Security Dynamics ACE Server

The iPass Connection Software

The iPass connection software is how the remote users connect to the iPass Network. Since the iPass Corporate Access solution involves connecting to the Internet though multiple ISPs worldwide, it is important users have an easy-to-use client software tool that can store multiple phone numbers from different ISPs with potentially different set up and dial-up scripting information. iPass has two such tools available:

- The iPass Dial Wizard for Windows 95/98 and Macintosh
- The Microsoft Connection Manager (MCM) for Windows 95/98/NT

The iPass Dial Wizard

The iPass Dial Wizard is a client application that provides users with an easy way to remotely connect to the iPass network (Figure 4). Using the iPass Dial Wizard, a user can easily locate any of the more than 3,000 POPs in the network by country, state or region, and city. The iPass Dial Wizard for Windows 95/98 automatically generates a Dial-Up Networking connection icon, with the proper telephone number and connection scripts, in the Dial-Up Networking folder. The user clicks the icon to connect through the given POP.

The iPass Dial Wizard is easily customizable by authorized iPass Solution Providers through a web-based application maintained on the iPass web site. This application allows iPass Partners to customize the connection software with their own logo, to add/delete POPs from the iPass phonebook, and to add pricing information to POPs. Future versions of the iPass Dial Wizard will support Windows NT.
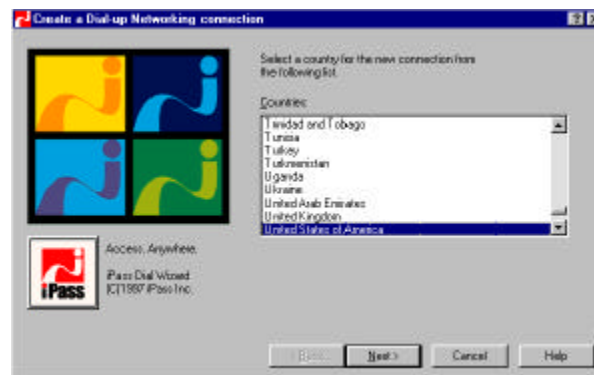

Figure 4: The iPass Dial Wizard user interface

Microsoft Connection Manager (MCM) for Windows 95/98/NT

MCM is a new versatile client dialer for connecting to network resources on either a public network or securely connecting to private networks over the Internet (Figure 5, next page). The MCM is available as part of Internet Connection Services for Microsoft RAS, which also includes the Connection Manager Administration Kit (CMAK), Internet Authentication Services (IAS), and Connection Point Services (CPS).

Microsoft Connection Manager incorporates a number of new features designed to make it easier to deploy and administer a remote access environment. These include the following:

- **Transparent support for PPTP** -- Provides easy connectivity to virtual private networks (VPNs) over the Internet.
- **Dual password support** -- Includes support for both an Internet logon password as well as a private network password.
- **Auto re-dial and disconnect support** -- Includes the ability to transparently switchover to a backup telephone number.
- **Easy modification through the CMAK** - A wizard that allows iPass Partners and customers to customize their dialer application.
- **Support for automatic phone book updates through the phone book service** -- A component of the Internet Information Server that compares a client's resident connection configuration with the most recent files available on the server and downloads the appropriate phone book updates if necessary.

The Microsoft Connection Manager client is available for Windows95/98/NT. The Phone Book Service is a core Windows NT Server-networking service running on the Internet Information Server.

Figure 5: Microsoft Connection Manager user interface

iPass "Step-by-Step"

Having introduced the three components of the iPass remote access solution, let us examine how they work together to enable worldwide roaming. An overview is shown in Figure 6.
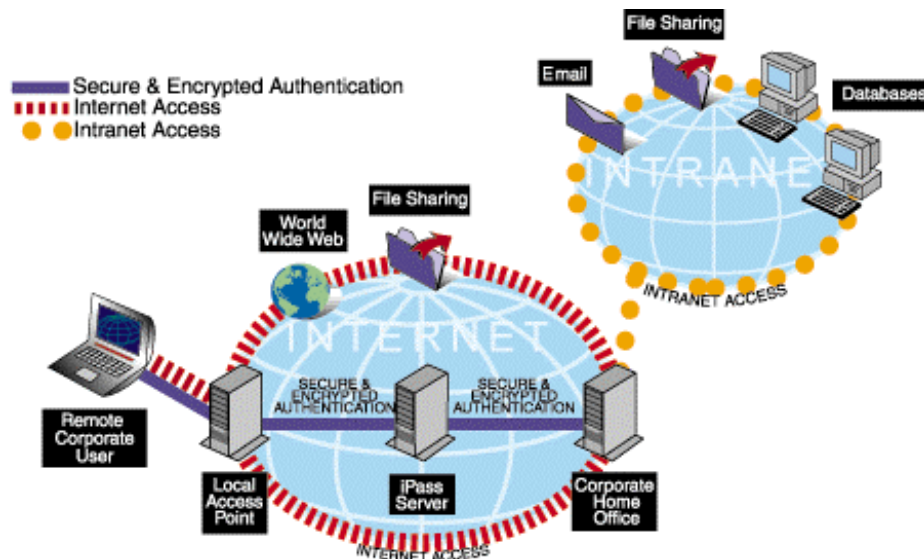

Figure 6: Overview of iPass Corporate Access

When a remote user connects to a local ISP which is part of the iPass network, the user inputs the same user name used when connecting to the company network, appending an @ sign and the company domain name to the end of the user name. For example, if the remote user normally uses "david" as a user name when

connecting to his company (whose domain name is "company.com.hk" in Hong Kong), he would "david@company.com.hk" in the iPass Dial Wizard or Microsoft Connection Manager. The addition of an @ sign to the regular user name identifies the user as a "visiting user" requiring remote authentication. iPass supplies enabling software to its ISP participants, called the iPass NetServer, to allow recognition of this information as a remote user authentication request.

The iPass NetServer software scans the authentication information provided by the user and determines if there is a roaming domain name after the user name. If a domain name is present, the user's login information is encrypted using SSL and sent to an iPass-managed server at an iPass Transaction Center. There are five such centers maintained in secure facilities throughout the world. If an iPass NetServer fails to communicate with a server at the nearest Transaction Center, it automatically fails over to a backup server. The login information is decrypted and the domain name is translated into an IP address for further routing to the company's iPass RoamServer. This system provides security and redundancy. The use of SSL encryption protects the user's identification and password from interception as it passes through the public Internet.

After the iPass Transaction Center has determined the IP address of the company's iPass RoamServer, the authentication request is once again encrypted, this time using information contained in an SSL certificate associated with the company, and sent to the iPass RoamServer software residing at the company network. The iPass RoamServer decrypts the authentication request and submits it to the company's standard authentication server as if it were a terminal server or network access device controlled by the company. The company authentication server responds to the request normally, providing an "access permitted" or a "access denied" response based on the validity of the user name and password. Interfacing with corporate authentication servers allows companies considerable flexibility in how they make the iPass service available to their employees. For example, a company could limit use to a specific subset of their employees, or limit use to certain times of the day.

Regardless, the response from the company's authentication server - positive or negative - is received by the iPass RoamServer, encrypted using the company's SSL certificate, and sent back to the iPass Transaction Center. The iPass Transaction Center receives the encrypted response, identifies the destination ISP (the local ISP where the roaming user signed on), encrypts the response using the destination ISP's SSL certificate, and returns the authorization message to the destination ISP. Based on the response received and decrypted by the visited ISP, the user is allowed to proceed, or is denied access.

At each point during the authentication, authorization and accounting process, all transactions are logged by the iPass Transaction Center. This entire process normally adds only 6-10 seconds to a direct login.

Once the user is connected, iPass does not handle packets during the actual session. The user accesses the Internet as a full IP peer, allowing any type of client-server encryption to be used during the session. As a result, companies may deploy any of a variety of client-server secure VPN solutions to ensure end-to-end security and integrity of data transport during the session.

Conclusion: The Complete Remote Access Solution

iPass Corporate Access offers a comprehensive solution for organizations seeking to give their application users easy, remote access to the corporate network. iPass Corporate Access can be deployed as a single remote access solution for telecommuters, day-extenders and roaming users, or it may be integrated with other remote access solutions to greatly extend their capabilities. Primary benefits of the iPass Corporate Access solution are listed below:

- **Low Cost** -- All that is required for an organization to start using iPass Corporate Access is installation of the iPass RoamServer software and distribution of the iPass connection software. Users then access the corporate network through the existing Internet network connections using

existing Internet access control solutions. Since there is no special hardware or phone lines to maintain, costs are driven solely by usage. These costs are often significantly less then those of 800 number or long distance telephone solutions.

- **Global Coverage** -- With more than 3,000 POPs in over 150 different countries, iPass Corporate Access provides superior geographic coverage compared to single network ISPs.

- **High Quality of Service** -- In each region of the world, iPass maintains partnerships with top-tier Internet and network service providers. With its highly-scalable, redundant settlement architecture, iPass ensures a high level of network availability and performance for end users.

- **Interoperability** -- The iPass solution can be used to supplement an existing remote access solution, or can provide a complete replacement for a company's existing remote access infrastructure.

- **Secure Authentication and Data Transport** - iPass Corporate Access provides complete security of user names and passwords during user authentication through the use of SSL encryption. iPass' system architecture eliminates security problems resulting from direct communication between the user's corporate site and the visited ISPs, removing possibilities for security breaches caused by inadequate security controls. Additionally, iPass supports standards-based strong key authentication and integrates well with all common firewall and secure VPN solutions, to ensure end-to-end security of data transfer between the client and company server.

- **Ease of Use** -- The iPass RoamServer software can be installed and running in just a few hours. Once the software is set up and tested, virtually no maintenance is required. End-user deployment is also simple. A remote user can quickly install the iPass client software - Dial Wizard for Windows 95/98 and Macintosh, or Microsoft Connection Manager for Windows 95/98/NT - by launching a simple point-and-click install program. After that, remote access users use a point-and-click interface to select a location and phone number to dial.

Summary

Organizations requiring widespread remote access will find significant savings in Internet and VPN solutions using iPass Corporate Access versus traditional in-house modem pools. iPass Corporate Access adds global coverage and improved quality of service to Internet access solutions.

About iPass Inc.

The iPass services allow business travelers and telecommuters to access the Internet, email and their corporate network with a local call from anywhere in the world. Through established relationships with the largest and most respected ISPs and telecommunications companies worldwide, iPass provides businesses with reliable access to the Internet through high-quality connections from even the most remote locations. With iPass, companies can eliminate internal modem banks, costly long-distance charges and toll-free calls. Today, more than 500Internet service providers (ISPs), telecommunication carriers, VARs and system integrators around the globe offer the iPass services. To learn more about iPass Corporate Access visit our web site at http://www.ipass.com/services/corporate-access/.

Appendix A - Comparing iPass to Modem Pools

Modem Pool Model
Remote users	100 users
Modems required	15
Access charge, modem costs	$130 per modem
Monthly equipment and lines	$1,950 per month
Support effort (hours/day)	1 hour per day
Support Cost	$7,500 per month
Total fixed costs/month	$9,450
Domestic calls (US/CDN)	6.0 hours/month at $0.10 per minute
International calls	0.5 hours/month at $1.80 per minute
Total Phone Charges	$9,000 per month
Total Cost with Modem Pool	$18,450 per month

iPass Corporate Access Model
Remote users	100 users
Support Staffing	$1,875 (1/4th of modem support)
Add'l bandwidth, set-up fees	$500
Fixed costs per month	$2,375
Domestic calls (US/CDN)	6.0 hours/month at $0.05 per minute
International calls	0.5 hours/month at.. $0.17 per minute
iPass usage charges	$2,310 per month
Total Cost with iPass	$4,685 per month

Net Savings	**$13,765 per month**
% Savings	**75%**
Payback	**3 weeks**

Bibliography

Bhawan, Chander, Remote Access Networks, McGraw-Hill (New York, NY)), 1998.

Check Point Software Technologies, Redefining the Virtual Private Network [Online], www.checkpoint.com/, March 4, 1998

Forrester, The Forrester Report – Telecom Strategies, Forrester Research, Inc (Cambridge, MA)., 1998

Scott, Charlie, Paul Wolfe and Mike Erwin, Virtual Private Networks, O'Reilly & Associates (Sebastopol, CA), 1998.