Lucent Technologies
Bell Labs Innovations

Product information begins on page 2.

Lucent and Ascend have merged.

With the Lucent-Ascend merger, customers gain a broader and more powerful portfolio of next-generation data, voice, fax, and video services and products. To access up-to-the-minute information about our products, see page 2.

We also invite you to contact us with your questions directly at: info@ascend.com

Ascend

WHITE PAPER

Remote Networking Alternatives for the Enterprise

ASCEND

Table of Contents

1. Executive Summary

Driven by pressing business needs and shifting social trends, more and more workers are roaming further from their offices. You can find them everywhere – staffing small sales offices in far-off locations, laboring late at night on home computers, and working from hotels, convention halls, conference rooms and traffic jams.

All of these workers are part of a booming trend called remote access networking, or simply remote networking. Essentially, remote networking is a method of extending a company's resources to workers in the field using telecommunications technology. The "field" can be anywhere from across town or across the country to the other side of the world. The remote workers can be your company's branch office employees, full- or part-time telecommuters, traveling professionals, customers, suppliers or business partners.

Remote networking cuts across industry lines and international borders, affecting a growing number of workers that includes executives and engineers, secretaries and salesmen, doctors and delivery truck drivers. This diverse group has one thing in common: the need to communicate with colleagues and business associates in other locations and to access critical information housed on the corporate network. Today's sophisticated digital technologies and advanced communications services meet these needs – faster, easier and less expensive than ever before.

According to companies with remote networks already in place, the long list of benefits includes:

- Increased sales
- More effective customer support
- Faster response to customer needs
- Quicker project completion
- Increased job satisfaction
- Expanded presence in regional areas
- Improved corporate communications
- Better employee retention
- Faster product development cycles

Source: Infonetics Research, San Jose, California

Remote Networking Trends

Recent business, social and technological trends are helping to fuel the rapid growth of remote networking.

Business Trends **-** Over the last decade, changes in the economy, the workforce and the business environment have all increased the need for remote networking. In response to competitive pressures and the extensive travel demands of today's business world, companies are experimenting with telecommuting and sales force automation to increase productivity around the clock – and around the globe.

Social Trends **-** Changing attitudes about work and leisure time are placing increasing importance on flexibility in daily life. Telecommuting or working from branch offices closer to home lets employees enjoy less-structured lifestyles, live where they want or where housing is affordable, and accommodate child- or elder-care responsibilities.

Technology Trends **-** For years, analog phone lines and modem technology have limited the work employees could perform from remote sites. For workers with demanding requirements – service representatives, computer programmers, engineers or graphic artists, for example – sluggish modem speeds have limited productivity or made it impossible for them to work remotely, at all.

Telecommuting Facts

Telecommuting, or teleworking, is one of the fastest-growing segments of the remote networking phenomenon. Telecommuters include executives, managers, customer support representatives, sales professionals, editors, programmers and other information workers who access their enterprise network from home. Here are just a few of the facts about telecommuting:

- Telecommuting results in an average work time increase of two hours per day per worker (Gartner Group)
- Telecommuters at Pacific Bell exhibited 25 percent less absenteeism than other employees
- Companies save from $3,000 to $5,000 per year per telecommuter on facilities costs (Gartner Group)
- The number of telecommuters will continue to increase at the rate of more than 10 percent per year (Link Resources)

With the benefits and advantages, the main issue with remote networking today is not “if”, but “how”. The traditional analog modem bank is on the path to obsolescence with advances in technology and deregulation in the telecommunications industry. Organizations now have three far more capable and affordable options to the modem bank: private networks with digital access concentrators, “outsourced” wholesale access arrangements with network service providers, and the Internet-based virtual private networks (VPNs).

Each of the alternatives is highlighted in section 2. Section 3 compares and contrasts all three, indicating the best fit for each. In general, distance determines which alternative is the most cost-effective. Long-distance remote networking needs, especially for a company’s cross-country and international users, are best served by a VPN. Private networks and wholesale arrangements make more sense for local remote networking needs, such as telecommuting programs. Section 4 outlines the three fundamental building blocks of any remote network, and provides guidance for selecting the best services and equipment.

2. Remote Networking Implementation Alternatives

There are three fundamental ways to implement a remote networking solution: a private network, an outsourced “wholesale” network or a virtual private network (VPN). An enterprise-wide remote networking solution may involve only one or a combination of two or all three configurations.

The Private Network

A private network solution is the traditional form of remote access. Historically, the configuration involved a modem bank and remote access server at the central site; remote users dialed in directly via the Public Switched Telephone Network (PSTN). With this approach a complete solution needed not only the modem bank, of course, but also requires terminal adapters for Integrated Services Digital Network (ISDN) lines, channel and digital service units for leased lines and Frame Relay services, a multi-port terminal server, a router and lots of cables to interconnect everything. Managing such chaos—or even finding everything under all those cables—was an error-prone and expensive process.

Once the PSTN converted from analog to digital communications, the troublesome modem bank could be replaced with the more capable and affordable WAN access switch, also referred to as a digital access concentrator. The WAN access switch integrates all necessary technologies into a single, cohesive product, which is easier to install, operate and manage. The switch interfaces to the PSTN over high-speed T1/E1 or ISDN Primary Rate Interface (PRI) lines. Each line supplies 24 (T1) or 30 (E1) channels or “ports” that support the full spectrum of WAN technologies, including analog modems, ISDN Basic Rate Interface (BRI), Frame Relay and Switched 56 services. Consolidating these diverse forms of remote networking eliminates the headaches of piecemeal configurations, improves security, and lets a single dial-in telephone number serve all users.

Another advantage of the WAN access switch is its integral digital modem technology. Digital modems:

- Deliver up to 56 Kbps throughput downstream to remote users (Conventional analog modem performance peaks at 33.6 Kbps.)
- Accommodate the full spectrum of analog and digital modem protocols
- Protect the investment in switch capacity with a software-based implementation that can keep pace with emerging and future modem standards

Typical Private Network

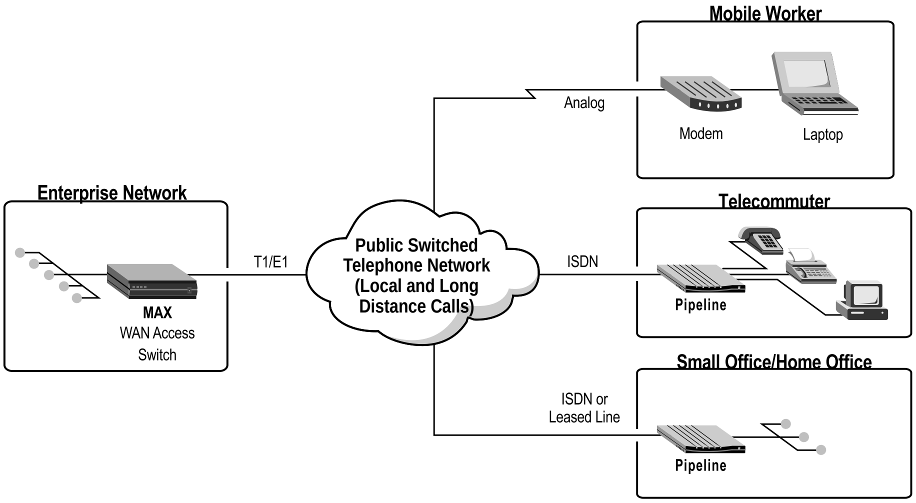

Figure 1 – The private network configuration for remote access, while often the most expensive solution, gives complete control to the enterprise.

The private network alternative has the advantage of being inherently secure, and gives complete management control to the enterprise. The main disadvantage is its relatively high cost of operation compared to that of a VPN or a wholesale arrangement.

Wholesale Remote Access

A wholesale arrangement essentially relocates the access ports from the enterprise premises to a network service provider's (NSP's) point of presence (POP). Remote users dial into the POP(s), where the traffic is routed to the enterprise over a high speed link.

The primary advantage of wholesaling is improved price/performance. Indeed, wholesale access takes economies of scale to the next level with *carrier-class* WAN access switches supporting thousands of ports and tens of thousands of users. Individually, very few organizations can justify such an expenditure. But collectively, through wholesaling arrangements with network service providers, enterprises can obtain a more feature-rich and cost-effective remote networking solution.

Typical Wholesale Network

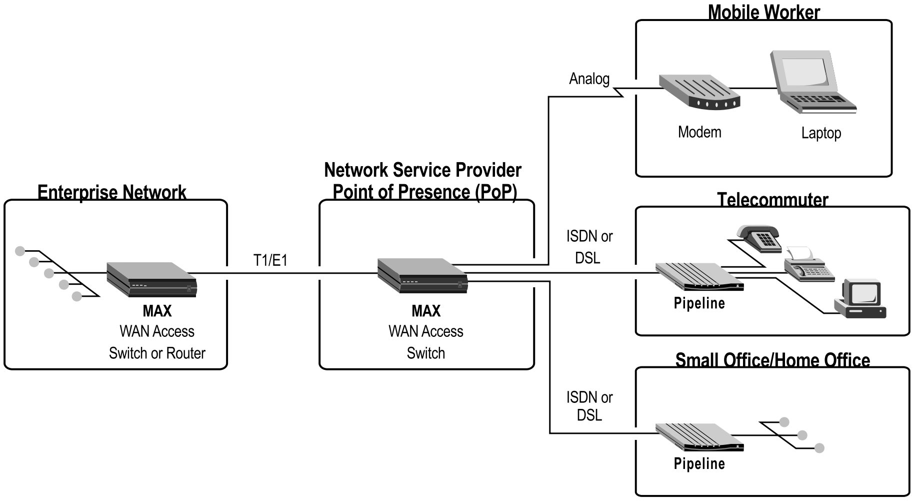

Figure 2 – A wholesale network arrangement can reduce costs while providing more powerful capabilities and improved availability.

Wholesale remote access affords numerous benefits:

- Saves money in several areas: staff, communications equipment, facilities, training and maintenance
- Improves connect success rates with carrier-class capacity and reliability
- Enables support for state-of-the-art capabilities, including 56K digital modems, Digital Subscriber Lines (DSL), Voice over IP, for "multimedia" applications and more
- Expands geographical coverage quickly and easily, all with *local* access anywhere in the service provider's service area
- Affords "pay per use" incremental expansion of access ports
- Permits use of a single telephone number for modem and ISDN users
- Operates transparently to the enterprise network, including user and domain names, password databases, e-mail addresses, and so on

The primary disadvantage of wholesale access is lack of availability. But the "presence" of wholesale access is expected to increase substantially over the next few years with regulatory reform permitting both new forms of carriers and increased competition among all carriers.

The Virtual Private Network

A virtual private network, or VPN, is a private network that utilizes the next-generation public network to carry all traffic in the WAN. The most widely available, least expensive and high-speed public network is the Internet. With its worldwide presence and unparalleled price/performance, the Internet is an excellent foundation for many enterprise networking needs, especially remote networking.

Perhaps the most compelling argument for VPNs is that, if users are already "on" the Internet, why not take full advantage of the connection for other applications? Over one-third of the organizations polled by Infonetics Research said their remote sites needed access to the Internet. Enterprise users likely need Internet access, too – to collaborate with clients or partners, scan professional journals or make travel arrangements. Users already on the Internet can be added to a remote access VPN easily and inexpensively.

In a remote access VPN, the headquarters and every individual telecommuter and mobile worker has a *local* link to the Internet. The VPN supports IP-based applications, of course, and can also handle most non-IP applications via IP tunneling. Local connections to local NSPs – leased lines, Frame Relay or dial-up – eliminate all long-distance charges.

Virtual Private Network

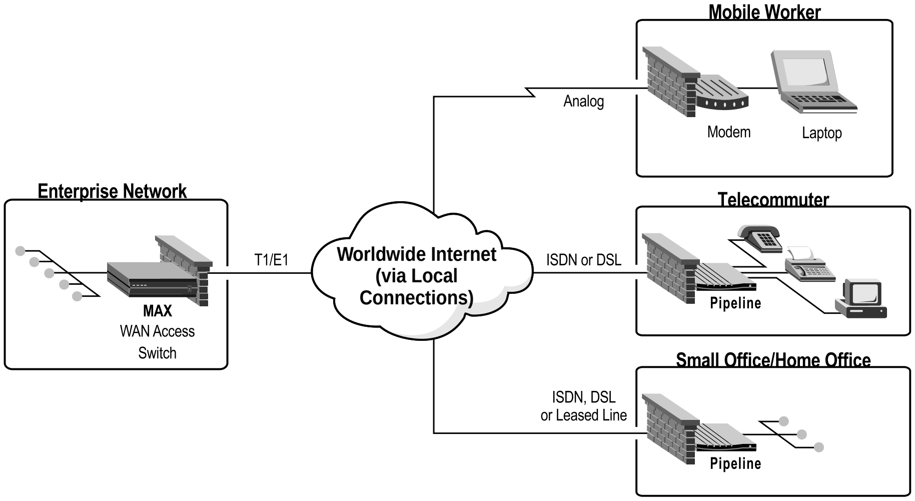

Figure 3 – Remote access is an ideal application for the many cost-saving advantages of an Internet-based virtual private network.

An Internet-based remote access VPN offers three compelling advantages:

A savings of up to 60% over equivalent private networks

- Eliminate long-distance switched calls (PSTN or ISDN)
- Pay only for actual usage with no idle lines or wasted Frame Relay commitments
- Use the same equipment for both Internet access and the VPN
- Minimize network design and management responsibilities

An ability to exploit the Internet infrastructure

- Low-cost public bandwidth
- Worldwide presence with ISPs in nearly every city
- Voice over IP and multicast for “multimedia” applications
- Mesh redundancy and fault tolerance
- User familiarity simplifies training and support

A way to enhance flexibility

- Add and delete connections instantly
- Provide periodic or temporary connectivity almost effortlessly
- Integrate third-party users easily, including customers, suppliers and business partners
- Select appropriate access rates from 28-128 Kbps and beyond with DSL

The cost-savings of VPNs over equivalent private networks are substantial – and real. Here are estimates by three leading industry analyst firms:

- *Infonetics Research* estimates a savings of 60-80% for remote access VPNs. Infonetics believes that, by 2001, one-third of US remote access applications will be implemented using VPNs.
- *Gartner Group* expects VPNs to offer a savings of at least 50% for remote access and, owing to this substantial savings, 70% of *Fortune 500* companies will use VPNs for remote access by 2003.
- *Forrester Research* found the following 60% savings when comparing private and virtual private solutions for a 2000-user remote LAN access network:

Network Expenses	Private Network	VPN
T1 Lines	$ 48,000	$ 68,400
Routers & Servers	208,000	44,800
Phone & ISP Charges	2,160,000	1,080,000
User Support	600,000	(Included) 0
TOTAL	$ 3,016,000	$ 1,193,200

Note the major savings in three distinct areas: equipment consolidation (“Routers & Servers”); elimination of long-distance services (“Phone & ISP Charges”); and management expenses (“User Support”). The only area where VPN costs are higher is the local access lines, which need to operate at a higher data rate with the consolidation to a single line for both the Internet and the remote access VPN.

Real-world experience confirms these estimated cost savings. One company achieved a 67% savings with a remote access VPN for 150 users. The private network had a monthly operating cost of $48,000 with an average usage of 2 hours per day per user. With the VPN, monthly operating costs decreased $30,000 to only $18,000 – a savings of $360,000 per year. Another company reported an annual savings of $252,000 for a 100-user remote access VPN. By taking advantage of $19.95/month unlimited Internet access, yet another organization was able to save a whopping 78%, primarily by eliminating long-distance charges. For companies that already provide such Internet access for employees, the user side of a remote access arrangement is effectively “free” with a VPN!

3. Choosing the Best Remote Networking Option

Affordability often determines the best option for a remote access network. But the most cost-effective alternative must still satisfy three general requirements: compatibility, security and availability.

Compatibility

Application compatibility is generally not an issue with private and wholesale remote access networks. The “raw” nature of the dial-up links accommodates any and all applications, including those with unusual protocols.

Remote access VPNs may require special provisions, however. Applications that use registered IP addresses can operate via the Internet “as is” with the addition of readily available security measures. To make non-IP or “private IP” applications compatible with the Internet, a company has three choices:

- Convert the application to IP – an endeavor that is usually easier said than done
- Make use of special gateways that convert other protocols to IP
- Employ tunneling or encapsulation techniques to package other protocols in IP for transit across the Internet

The best choice depends on what options are available for specific applications and the organization’s long-term networking objectives. But unless the application is so old or so unusual, chances are at least one of these three options will work. Normally the most straightforward choice is tunneling, which works with the widest variety of client/server and legacy applications. Some ISPs can now even offer a fully outsourced VPN solution, which requires no special customer premises equipment or other investment.

Tunneling: Making the Virtual Paths in Virtual Private Networks

Tunneling applies proven technology to Internet-based VPNs. A tunnel is a special IP “envelope” that makes non-IP and private IP applications compatible with the Internet, and is unnecessary for clients and servers with registered IP addresses. The tunneling process occurs at both ends of the connection: encapsulation at the source places the original packet in a special IP packet; decapsulation at the destination removes the special IP packet, leaving the original intact. Here is a list of the most popular tunneling and encapsulation protocols:

- The *Point-to-Point Tunneling Protocol* (PPTP), created by Microsoft and Ascend Communications, is an extension to the Point-to-Point Protocol (PPP) for Windows NT and NetWare client/server environments
- The *Layer-2 Tunneling Protocol* (L2TP) is a proposed industry standard that will combine the best features of PPTP and Layer-2 Forwarding (L2F) to accommodate IP, IPX, AppleTalk, NetBIOS, NetBEUI and other PPP-supported protocols
- The *Ascend Tunnel Management Protocol* (ATMP), supporting both PPTP and GRE (Generic Routing Encapsulation as defined in RFCs 1701/1702) can be used for “private IP”, IPX and NetBIOS/NetBEUI applications
- *Data Link Switching* (DLSw), originally defined by IBM and now an industry standard, encapsulates SNA traffic (the LU 6.2 protocol) in IP.
- *IP Security* (IPSec), which adds packet encryption and authentication to other tunneling protocols, also has a Tunnel Mode of operation to provide basic tunneling on its own.

Security

There are three P's that, together, constitute total network security:

- Protection of resources through a dynamic firewall defense
- Proof of identity through both user and packet authentication
- Privacy of information through snoop-proof packet encryption

All three P's are equally important in any enterprise networking application, including remote access. Exclusively private networks may use only simple passwords for proof of identity, and take for granted both protection of resources and privacy of information. But any time a private network interfaces to a public network, such as the Internet, none of the three P's can be taken for granted. So in any wholesale arrangement or VPN, a firewall should exist at every interface to the public network, every user should be fully authenticated, and encryption should be available as needed on an application-by-application basis.

Protection of Resources

Firewalls are essential any time a private network interfaces to a public network. A firewall passes only authorized traffic for all trusted users, and blocks everything else. In other words, all attempts at access by unknown or untrusted users are stopped, and the two-way traffic of trusted users is screened to ensure it is expressly permitted.

This important form of protection must be provided for *every* user and site. Why? Because *if you don't have security everywhere, you don't have security anywhere*. Just as a chain is only as strong as its weakest link, so too is a network security system. Any "unlocked door" makes resources throughout the enterprise vulnerable.

The biggest single limitation of most firewalls is that securing every single connection becomes cost-prohibitive, thus negating the cost-saving advantages of a wholesale arrangement or VPN. The ideal firewall solution, therefore, should meet all of the following criteria:

- It should be integrated with the remote networking equipment to make the protection both effective and affordable.
- A low-cost, software-only version should be available for individual users with ordinary analog modems.
- The firewall should strictly enforce a policy of "that which is not expressly permitted is denied."
- The design should employ state-of-the-art *dynamic* stateful inspection for maximum protection.
- The offering must be certified by the International Computer Security Association (ICSA).
- An optional unprotected "de-militarized zone" (DMZ) LAN interface should be available, on the Internet side of the firewall, for Web and other public servers.

Proof of Identity

Various forms of authentication are available to establish proof of identity. The most basic form of authentication involves entering a simple password during logon, such as with the Password Authentication Protocol (PAP). The Challenge Handshake Authentication Protocol (CHAP) is a little more sophisticated, but still fairly easy to circumvent. Even for private networks, such rudimentary methods are increasingly insufficient. Token cards, by contrast, offer virtually "bulletproof" authentication with single-use passwords.

Private networks can take advantage of calling line ID (CLID) and callback for telecommuters, where each user is associated with a permanent telephone number. CLID requires the local carrier to provide calling line information, but is transparent to the user. With callback sessions, the user's initial logon is terminated, and the session is reestablished *from* the central site. Some ISPs may offer this advanced form of authentication for wholesale arrangements and VPNs.

The ultimate form of authentication validates each and every packet with a digital signature. Packet authentication validates source addresses and provides integrity by ensuring that data has not been altered during transmission (see discussion of IPSec's Authentication Header below).

Privacy of Information

IP Security, or simply IPSec, is outlined in a series of standards (RFCs 1825-1829) that add data authentication, integrity and confidentiality to any IP-based network, especially VPNs. There are two aspects to IPSec's protection: the Authentication Header (AH) and the Encapsulating Security Payload (ESP), which can be employed individually or in combination.

An AH adds a digital signature to the header using the Message Digest (MD) or the Secure Hash Algorithm (SHA). The header's digital signature authenticates the packet with a keyed code that assures data integrity by enabling detection of any alteration during transmission.

The ESP portion of IPSec encrypts and decrypts either the entire packet (Tunnel Mode) or just the data (Transport Mode) using the Data Encryption Standard (DES) or Triple DES (3DES). Encrypted ESP packets keep transmitted data strictly confidential, and can provide adequate user authentication and data integrity for most applications.

Availability

Availability has three equally critical dimensions – uptime, throughput and latency – and both private networks and wholesale arrangements offer inherent assurances for all three. For VPNs, uptime assurances are generally covered by a Service Level Agreement (SLA), while throughput and latency are normally elements of Quality of Service (QoS) provisions. SLAs guarantee that network uptime will exceed 99 percent, for example, with money-back guarantees when the service provider fails to deliver. Meeting such stringent service levels with a private network or wholesale arrangement is relatively straightforward; the Internet, however, presents a different situation for VPNs.

QoS comes in three levels or classes: best effort, relative and absolute. *Best effort* is, essentially, the absence of QoS; neither throughput nor latency is assured. Most users of the Internet today receive best effort service, which is often adequate for remote networking needs. *Relative* QoS prioritizes traffic using the Type of Service (ToS) field in the IP header. The Internet's ability to deliver on such a request depends on two factors: the current network load and the percentage of traffic requesting prioritization. Hence the reason this service is relative. And even when higher priority is granted, relative QoS has no provision for minimizing latency. *Absolute* QoS guarantees delivery of both sufficient bandwidth and a not-to-exceed latency with no ifs, ands or buts—in other words: absolutely. Unfortunately, Absolute QoS is not available in the Internet today.

Class of Service	Throughput Assurance	Latency Assurance
Best Effort	No	No
Relative	Maybe	No
Absolute	Yes	Yes

The table summarizes all three classes of service. "Best effort" is adequate for most remote networking needs. "Absolute" may be necessary for multimedia applications such as videoconferencing and certain host/terminal applications because it is the only class of service that offers minimal latency.

Performance of any remote network, whether private, wholesale or virtually private, can be improved by employing compression, utilizing ISDN bandwidth on demand techniques like the Multilink Protocol Plus™ (MP+), and taking advantage of even higher bandwidth "on ramps" via Digital Subscriber Lines (DSL).

Distance Decides

Despite the various tradeoffs outlined above for compatibility, security and availability, affordability often dictates the solution. And it is *distance* that makes the most profound difference in cost of all three alternatives. For local remote networking applications, especially for telecommuters, the private network or wholesale arrangement are comparable in cost. As the distance between remote users and the central site increases, as is the case with traveling workers, the VPN alternative becomes more attractive. As the number of distant users increases, the advantages of the VPN become quite compelling.

The reason distance is often the primary decision criteria lies in the cost breakdown of a typical remote network. The initial equipment expenditure and implementation constitute only about 20% of the total three-year cost of ownership. Surprisingly, this capital expense is similar for all three alternatives. In fact, equipment for remote users is often identical with all three. The central site requires either a WAN access switch, for the private network, or a router for both the wholesale arrangement and the VPN. But because a “bare bones” WAN access switch is actually a router with special remote networking features, it is normally the most capable and flexible choice for all three alternatives.

With VPNs looming as an inevitable element of enterprise networking, the WAN access switch lets organizations build “VPN ready” private networks or enter into “VPN ready” wholesale arrangements with complete investment protection. When ready to migrate in whole or in part to a remote access VPN – now or in the near-term future – the switch’s VPN-specific options, such as a firewall, tunneling and IPSec provisions, can be added through software and memory upgrades to the router.

The on-going operating expenses of the remote network are what constitute the remaining 80% of the total cost of ownership. The two major on-going expenses are WAN services and network management.

Local WAN access charges, at both the central site and for all remote users, are almost identical among the three alternatives. The real difference is in the distance. Private networks incur long-distance charges for any call originating from beyond the central site’s local calling area. The “local” reach of wholesale configurations can be as large as an entire metropolitan area, depending on the service provider’s infrastructure. VPNs, with local connections for all users and sites, eliminate all long distance charges.

On-going management costs are typically higher with the private network configuration. With wholesale and VPN solutions, service providers are responsible for most of the infrastructure, and even handle some of the user support – especially the potentially troublesome basic network connection.

4. Remote Networking Building Blocks

There are three fundamental building blocks in any remote network: network services, access equipment and a management system. This section discusses the considerations for each as required by all three configuration alternatives.

Access Equipment
Network Services
Management System

Figure 4 – Every remote network is composed of these three basic building blocks.

Network Services

Network services include local access for all sites and users, along with long-distance services for a private network solution, and network/Internet service providers for wholesale and VPN solutions.

Local access services are required for all sites and users. The traditional provider of such services is the Regional Bell Operating Company (RBOC) or Incumbent Local Exchange Carrier (ILEC). Deregulation has created a new entrant to this market called the Competitive Local Exchange Carrier or CLEC (pronounced *See-Leck*). Both ILECs and CLECs offer essentially two broad choices for local access:

- Dial-up services, such as analog modems and ISDN, which are best for traveling employees and telecommuters, respectively
- Continuous forms of access, such as that provided by leased lines or Digital Subscriber Lines (DSL), which are required for the central site and may be cost-effective for “power” users or multi-user small office/home office (SOHO) environments

Beyond these two fundamental options, choosing the best alternative is really only a matter of speed: how much throughput does the user or site need? While most local access services incur a fixed monthly fee, some may have a variable usage charge, such as per-minute fees for ISDN. Sometimes a fixed rate leased or digital subscriber line is less expensive than the combined fixed and variable charge of a dial-up service, especially for full-time telecommuters.

Digital Subscriber Lines

DSL technology increases the throughput of ordinary twisted pair wiring in the local loop. Voice telephone services use this same wiring, but employ analog signaling methods that severely limit bandwidth. DSL technologies achieve higher transmission speeds – up to 7 Mbps – by utilizing advanced digital signal processing techniques, similar to those used for ISDN and T1/E1 today. A DSL link, in effect, creates a high-speed "leased line" between the central office and the user site, which is ideal for full-time telecommuters and other "power" users. Of the numerous DSL technologies available, these three most effectively utilize existing twisted pair wiring to deliver both voice and data services:

- *ISDN Digital Subscriber Line* (IDSL), pioneered by Ascend, delivers 128 Kbps performance and offers compatibility with existing ISDN access equipment.
- *Symmetric Digital Subscriber Line* (SDSL) furnishes 768 Kbps of throughput as a cost-effective alternative to leased lines.
- *Rate-adaptive Asymmetric Digital Subscriber Line* (RADSL) integrates lifeline analog voice (to power the telephone) with high-speed digital data for a total communications solution on a single pair of wiring. RADSL is available in Carrier Amplitude/Phase (CAP) and Discrete Multi-Tone (DMT) options that provide 64-640 Kbps in the upstream direction (from the subscriber) and 1.54-6.14 Mbps in the downstream direction, where bandwidth is needed the most.

Long-distance services are required for private networks, and may be needed for extending the reach of wholesale arrangements to remote metropolitan areas. Inter-eXchange Carriers (IXCs) were the only option for long-distance services until recently, with regulatory reform opening up this market to ILECs and CLECs, especially for intra-state needs.

Network/Internet services include both wholesale access providers, which are generally CLECs, and Internet service providers (ISPs). They are covered together here as providers of primarily *data* services. Many ILECs and IXCs are also ISPs, and some may even offer wholesale access in select markets.

Selecting a Network Service Provider

Selecting the right network service provider is critical to the success of the remote networking solution. Whether your organization wants to use a national provider or multiple local ones, consider each to be a strategic partner. Here is a checklist of considerations for selecting the best possible service provider(s). It is a rather long list, and some points may be irrelevant or relatively unimportant in your situation, but be sure to evaluate all candidates thoroughly.

- Support for the full spectrum of WAN options (analog modems, cellular, ISDN, Frame Relay, Switched 56, T1/E1/PRI, X.25 and DSL)
- Digital modem technology for improved link reliability and support of an open architecture for the latest in 56 Kbps analog modem technology
- Multilink Protocol Plus (MP+) advanced dynamic bandwidth management to accommodate telecommuter integrated access devices
- Standards-based compression (bandwidth on demand and compression work together to deliver optimal throughput as needed, and only as needed, to minimize service fees)
- Comprehensive security provisions, especially Proxy RADIUS and IPSec, and a reputation for administering security
- Support for L2TP, PPTP, ATMP and IPSec tunneling to accommodate existing protocols and applications
- High-speed backhaul links to the Internet backbone for good performance
- Redundancy to assure adequate uptime for mission-critical needs
- Service Level Agreement (SLA) uptime guarantees and confirmation reporting
- Tiered Quality of Service (QoS) options ranging from “best effort” to an “absolute” guarantee of throughput and latency
- End-to-end monitoring, operating and troubleshooting capabilities
- Value-added features, such as Voice over IP (VoIP), IP multicast and IP faxing
- Value-added services, including consulting, network design, systems integration, on-going support, user help desk, extranet management, data backup, Web hosting, electronic commerce, etc.
- POP locations near all users and sites, or national/international “roaming” agreements with other service providers, to minimize or entirely eliminate long-distance fees
- Call Detail Reporting (CDR) to track usage by all users
- Central site or distributed pricing and billing arrangements, including bundled and managed service offerings
- Long-term financial stability and viability

Access Equipment

Remote network access equipment comes in two categories: the WAN access switch for the central site; and systems for all remote users and sites.

The ***WAN access switch*** is the heart of any remote network. While an ordinary router may be suitable for wholesale arrangements or VPNs, the slight additional cost of a software-upgradeable WAN access switch (with built-in routing) provides excellent investment protection. Make sure your switch has the following features, as appropriate for your particular solution:

- Support for the most cost-effective WAN option desired, such as T1/E1, ISDN PRI/BRI, DSL, Frame Relay and ATM
- Digital modem technology, with support for asymmetric 56K, for direct dial-in calls from analog modem users
- Routing/bridging to handle all network protocols
- User authentication via PAP, CHAP, CLID, Callback and token cards
- RADIUS and Proxy RADIUS capabilities for administering security
- Support for L2TP, PPTP and ATMP tunneling protocols
- IPSec provisions for adding packet encryption and authentication to the tunneling protocols, and optionally, for its own direct tunneling capabilities
- Integrated and certified dynamic firewall for protection of local resources
- Built-in compression to maximize throughput
- Dynamic bandwidth management for maximum performance at minimal cost
- Ability to accommodate IP multicast and Voice over IP, Frame Relay or ATM
- Resiliency with redundant power supplies and hot-swapable interface cards for reliable operation
- Automatic supplemental dial-up bandwidth for backup and overflow needs
- Compatibility with any advanced capabilities offered by the service provider(s)
- Robust local and remote management to maximize uptime at minimal cost
- Modular architecture to accommodate new interfaces and configurations
- Adequate capacity to support anticipated traffic volumes
- Certification for operation with local carriers and services

Remote user/site systems vary tremendously to meet the different need of different users, but there is little variation required for the three remote networking alternatives. In other words, a system that meets a user's needs for a private network, will also be suitable for a wholesale arrangement or a VPN.

In general, individual users come in two types: mobile and stationary. Mobile workers have little choice but to use analog modems for the foreseeable future. The analog modem is the only remote access device compatible with the Plain Old Telephone System (POTS), and POTS is the only universally available service. Fortunately, for the daily access needs of those on the go, the modem's modest performance is normally adequate.

For the full- or part-time telecommuter, however, the better the performance, the better the productivity. ISDN at 128 kbps and DSL from 128 kbps to over 7 Mbps both offer excellent price/performance for the "power" telecommuter or home office environment. But a limitation in most homes adds an interesting twist. Many telecommuters need at least three lines: the home line, a business voice line, a data line and, maybe, a separate fax line. The problem is that many homes and apartments are wired for only one or two lines. In these situations the integrated access device (IAD), provides an optimal solution. The IAD uses the two BRI channels as needed to handle all data/voice/fax communications on a single line. Some versions of DSL also provide an integrated voice/data solution on a single pair of wiring (see the DSL sidebar in the Network Services section above for more details).

There are, essentially, four types of systems available for remote network users and sites:

- Modems
- Small Office/Home Office (SOHO) Routers
- ISDN Terminal Adapters
- ISDN Integrated Access Devices

Modems

Modems, the traditional workhorses of the remote networking world, are stand-alone units or cards that fit inside a PC and connect to an analog phone line. The typical throughput of most modems today ranges from 33.6 kbps to 56 kbps–adequate performance for many remote applications. Modems are still a must in hotel rooms, customer sites or other locations where only analog or PBX lines are available. PC software-based firewalls are used for security in wholesale and VPN arrangements. Ideally, the firewall should integrate IPSec and other tunneling protocols.

Access Line: *Analog*

Advantages: *Inexpensive; familiar; easy to use.*

Other Considerations: *Low speed; prone to errors; unsuitable for multimedia and large files; line noise often causes lost connections.*

SOHO Routers

These intelligent devices connect remote sites/users over ISDN, Switched 56, DSL, Frame Relay or leased lines. Feature-rich SOHO routers have a built-in dynamic firewall protection, IPSec authentication and encryption, tunneling support, compression, dynamic bandwidth management, and more. The SOHO router is ideal for small, multi-user offices and is suitable for many individual "power" users.

Access Lines: *ISDN; Switched 56; Frame Relay; DSL; Leased Line*

Advantages: *Built-in features improve performance by minimizing demands on the PC.*

Other Considerations: *More expensive than other access equipment; more complex to set up and manage than modems.*

ISDN Terminal Adapters (ISDN TAs)

These simple devices connect to the serial port of a PC or laptop, or plug directly into a card slot, offering higher data rates than even the fastest modems. They operate with either ISDN BRI or IDSL, both at 128 Kbps. But an ISDN TA normally requires that security and tunneling provisions operate in the host PC, which adversely impacts performance. In addition, the throughput of external ISDN TAs is limited by the COMport and its inability to support advanced bandwidth management techniques.

Access Line: *ISDN; IDSL*

Advantages: *Less expensive than SOHO routers or IADs; faster than modems.*

Other Considerations: *Contain no intelligence; limited throughput capability.*

ISDN Integrated Access Devices

Integrated Access Devices, or IADs, are designed specifically to maximize communications efficiency and productivity in the home office. IADs have an ISDN BRI line on the WAN side, and an Ethernet port and one or two POTS ports for interfacing home office equipment. The Ethernet port attaches to the user's PC or home office LAN; the POTS ports connect the telephone, answering machine and/or fax machine. For data communications, the IAD can be configured to function as a router or a bridge, and has built-in firewall, IPSec and tunneling features. Voice and fax communications operate just as they would with ordinary analog phone lines. The "value-add" of the IAD is that all communications—data, voice and fax—take place interchangeably, simultaneously and automatically over the two channels in the ISDN line.

Access Line: *ISDN*

Advantages: *Provides an integral and complete data/voice/fax solution.*

Other Considerations: *Somewhat complex to install and configure.*

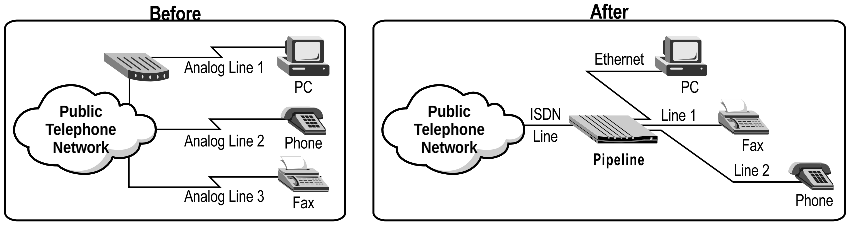

Figure 5 – The ISDN integrated access device provides a complete data/voice/fax communications solution on a single telephone line.

Remote Networking Management System

Remote networking management involves two systems: one for managing the equipment; the other for administering network usage. Every vendor has its own system for managing its own equipment. Fortunately, a standard solution, dubbed RADIUS, is available to insure network-wide integrity and interoperability for administering usage.

Managing equipment is ideally a centralized function in a remote network. Remote users normally lack the technical skills to troubleshoot problems, and prefer not to be bothered by routine system maintenance and upgrades. Normally, the management system is provided by the vendor of the remote access systems, and should have most of the following features:

- Auto-discovery and dynamic mapping of the end-to-end network topology with both physical and logical groupings of all equipment and links
- Real-time network monitoring of physical and logical WAN links, as well as traffic conditions, with fault alert/alarm generation based on user-defined thresholds
- Monitoring also offers a way to assess actual throughput on WAN lines, and helps control delivery of contracted SLA and QoS guarantees
- Capacity planning and performance trending through collection and analysis of traffic statistics that show both the level and patterns of usage by all users/sites
- Base-lining of normal operating conditions to help determine overall network "health" and for capacity planning needs
- Integrated, statistical accounting to track network traffic by user/department/site for bill-back or other purposes
- Remote configuration management for bringing new locations on-line, as well as coordinating network-wide updates and changes

- A means of comparing actual vs. intended equipment configurations
- Device-oriented fault detection and diagnostics for pinpointing and troubleshooting specific equipment problems
- A trace function that tracks traffic through the network, end-to-end, to help isolate bottlenecks and other problems
- A way to examine the WAN's Physical and Data Link layers, as well as assess actual throughput of dial-up and dedicated WAN links
- Compatibility with industry standards, like the Simple Network Management Protocol (SNMP)
- Support for RADIUS, TACACS or TACACS+ database for administering network usage

RADIUS (Remote Authentication Dial-In User Service) is the most widely used remote networking administration system. RADIUS is popular with enterprises and service providers alike because it handles all three A's of remote networking: authentication, authorization and accounting.

RADIUS functions as an information clearinghouse, storing complete profiles on all of a network's users. The profiles contain passwords, access restrictions, destination-specific routing, packet filtering, accounting information and more. Used in conjunction with PAP, CHAP or other third-party authentication servers, a single RADIUS database server can administer multiple security systems across complex networks and maintain profiles for thousands of users.

RADIUS employs a client/server architecture with WAN access switches as the clients, and the RADIUS database as the server. Proxy RADIUS capability lets a server at the service provider's POP query the organization's server to access user profiles for wholesale arrangements and VPNs. In this way the organization maintains complete control over access to its resources, while allowing the security provisions to be enforced at the service provider POPs. This ability to handle distributed management with centralized control makes RADIUS ideal for remote networks of any configuration.

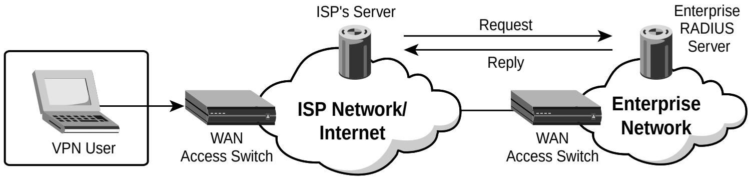

Figure 6 – A common use of Proxy RADIUS is for a server at the service provider's POP to access user profiles on a server at the organization's site.

Directory Enabled Networks

The Directory Enabled Network (DEN) initiative is an effort to standardize how network directory information is acquired, disseminated, stored and used. DEN affords a fully distributed directory architecture that is compatible with the Lightweight Directory Access Protocol (LDAP), Novell Directory Services (NDS), X.500, RADIUS and other popular directory services.

DEN takes a policy-based approach to all aspects of networking, including user profiles, networked applications, security, service provisioning and accounting. The standard is expected to become the preferred way to control network resources and user access capabilities. When available, DEN will afford a powerful yet simple way to establish and maintain remote networks.

5. Appendix: Ascend Product Information

Ascend has long been a leader in remote networking solutions, and continues its commitment to leadership with innovations in next-generation technologies. This appendix offers a high-level introduction to the Ascend remote networking product line. Details on these and other products are available at the Ascend Web site (www.ascend.com).

The award-winning Ascend ***Pipeline*** family provides the industry's widest assortment of VPN-ready solutions for individual users and SOHO environments alike. Any remote network benefits substantially from the Pipeline's superb price/performance and low cost of ownership.

The Ascend Pipeline family includes several models to fit applications ranging from single-user home offices to multi-user branch offices of virtually any size. Most models are complete data/voice/fax communications solutions with two analog POTS ports to connect telephones, answering machines and fax machines. The Ascend flagship model is the Pipeline 75, which offers the industry's most extensive feature set. The Pipeline 85 adds a 4-port Ethernet hub. The Pipeline 15 provide a less expensive alternative for individuals with less demanding needs.

Data-only models of the Pipeline are available in switched (ISDN or Switched 56) and leased line (T1/Fractional T1, DDS56 or xDSL) versions, each with support for Frame Relay. The Pipeline 130 offers both leased line and switched WAN ports for situations that require dial-up bandwidth on demand for backup and overflow needs. The Pipeline 220 adds a second Ethernet LAN port on the Internet side of the optional SecureConnect firewall. The award-winning Pipeline 50, ideal for smaller branch offices, is Ascend's most popular ISDN remote access router.

For the central site, the Ascend ***MAX WAN Access Switch*** affords the capability, scalability and flexibility required by today's sophisticated remote networks. MAX systems comes in a variety of fully-integrated models to fit any need—from two to over 2,000 concurrent sessions—all with support for private networks, wholesale arrangements and VPNs. The most popular enterprise version is the MAX 6000. Each MAX 6000 provides up to 384 ports; multiple systems can be integrated seamlessly with MAX Stack. Available WAN options include T1/E1, ISDN PRI/BRI, DSL, DS-3, Frame Relay, ATM, digital modems, cellular and X.25. For mission-critical facilities, the MAX 6000 offers both primary and backup/overflow bandwidth, as well as resiliency with dual power supplies and hot-swapable interface cards. Bandwidth on demand, Quality of Service (QoS) and Voice over IP (VoIP) features empower the MAX to meet the most demanding of applications.

Security for remote networks is the primary responsibility of the Ascend ***SecureConnect*** offering. SecureConnect combines an ICSA-certified dynamic firewall with IPSec's packet encryption (DES/3DES) and authentication (MD-5/SHA-1). The combination is an integrated option for The Ascend Pipeline and MAX systems, and is also available in a software-only Personal Edition for PCs with ordinary modems.

Management of remote networks is handled by the Ascend ***Navis*** network management system. Navis applications cover the installation, configuration and operation of Pipeline and MAX systems throughout the network. Remote sites and users can be managed fully, including network-wide upgrades, from the central site. Navis also includes Ascend's enhanced implementation of RADIUS, which supports Proxy RADIUS for enterprise control of security enforced at service provider POPs. The powerful capabilities and intuitive ease of use lets network managers maximize the benefits of remote networking with minimal training and effort.

ASCEND

Where Network
Solutions Never End™

Worldwide and North American Headquarters
Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
TEL: 510.769.6001
FAX: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 650.688.4343
Web Page: http://www.ascend.com

European Headquarters
Rudolph-Diesel-Strasse 16
D-64331 Weiterstadt
Germany
Tel: +49.6150.1094.10
Fax: +49.6150.1094.94

Asia-Pacific Headquarters
Suite 1908
Bank of America Tower
12 Harcourt Road
Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
TEL: 510.769.6001
FAX: 510.747.2300