resource guide

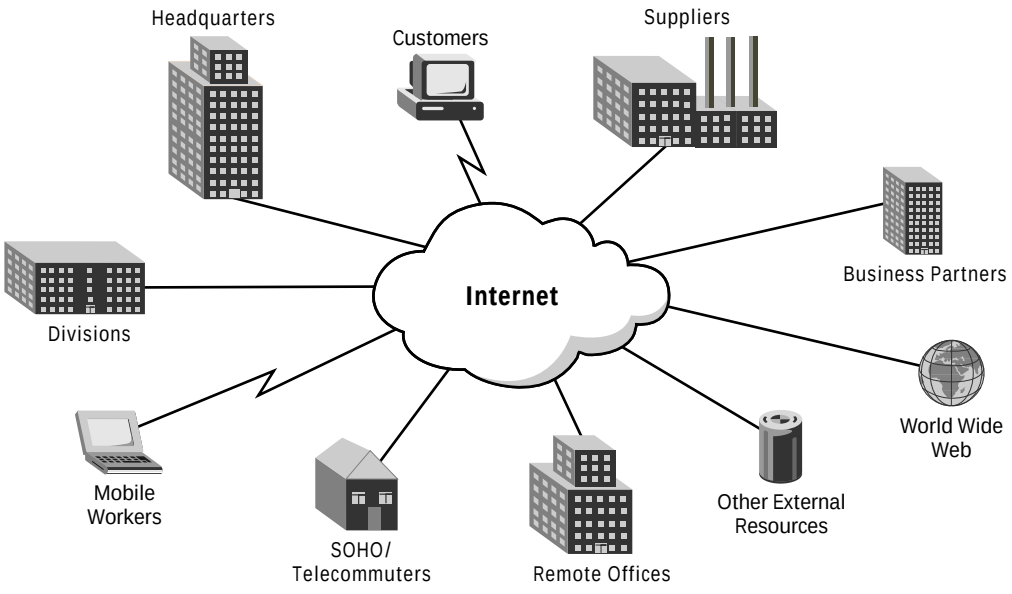
Ascend

resource guide

How To Extend the Power of Your Intranet

ASCEND

How to Extend the Power of Your Intranet



A Resource Guide for MIS Managers, Web Masters and Network Managers

ASCEND

Table of Contents

© 1997 Ascend Communications, Inc.

1. Executive Summary

Intranets use an IP-based network and its associated applications to conduct daily business activities. Examples include:

- *Web browsers and servers for "publishing" corporate information*
- *Electronic mail for inter- and intra-office communications*
- *FTP, the File Transfer Protocol, for sending and receiving files*
- *Telnet terminal emulation for accessing midrange and mainframe computers*
- *Usenet groups for delivering news and articles to "communities of interest"*
- *On-line "chat" and multicast applications for collaborative work and training*

Organizations today are struggling to meet the information explosion occurring both on the outside and from within. An *intranet* can help meet many, if not most, internal communications needs. Simply put, intranets use the Internet protocol and IP applications for internal communications. These inexpensive, proven and capable IP-based solutions—particularly the remarkably friendly and increasingly popular Web browser interface—make private data readily accessible by all workers.

The unprecedented success of the Internet, combined with the numerous applications for and advantages of intranets, are causing a near revolutionary trend in networking. Most analysts agree that intranets will grow at up to 10 times the breakneck pace of the Internet itself. By the year 2000, for example, intranets are expected to account for 90% of Web servers with over 250 million intranet clients (International Data Corporation). Some 25% of companies have already implemented an intranet, and nearly 70% likely will by the end of 1997 (Business Research Group and Zona Research).

This guide is intended for MIS managers, Web Masters and Network Managers. It explores four ways to extend the power of an intranet:

- ***Broadening its reach enterprise-wide to all remote employees and offices.*** Enterprise intranets afford a capable and cost-effective way to distribute, collect and manage internal information.
- ***Incorporating selective third parties, such as customers and suppliers***—an idea so popular it now has its own name: the extranet. Extranets employ tried and true industry standards to assure interoperability among organizations.
- ***Connecting an intranet to the Internet for seamless access to internal and external information resources.*** An integrated intranet/Internet solution leverages common software and network infrastructure for all communications needs.
- ***Replacing portions of the private network's WAN backbone with an Internet-based virtual private network, or VPN.*** VPNs offer a savings of up to 60% over equivalent private networks.

Two appendices are also included. The first provides checklists for selecting remote access equipment and network management solutions. The second offers an overview of Ascend's products used in Internet, intranet and extranet applications.

© 1997 Ascend Communications, Inc.

2. Enterprise Intranets: Extending the Reach to All Employees

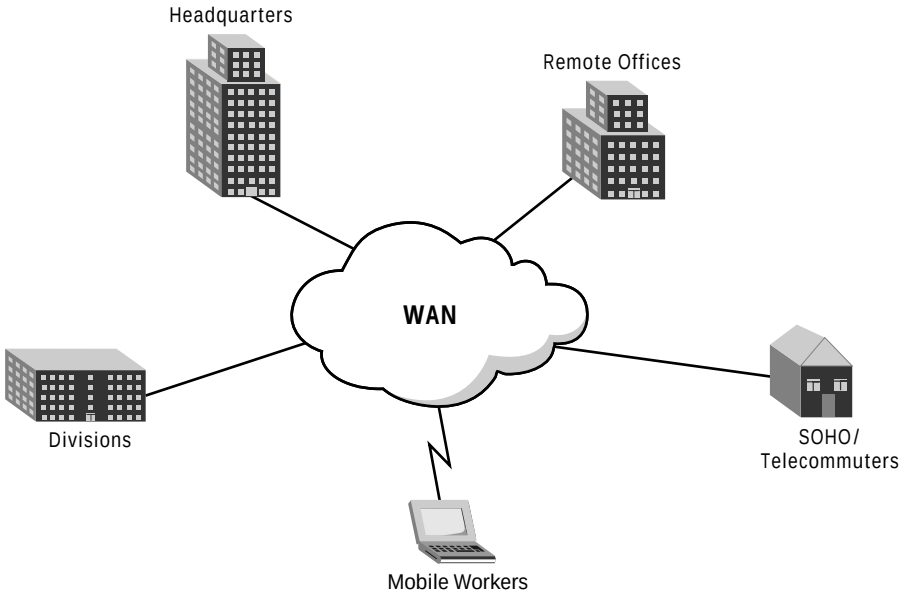


Figure 1 — An enterprise intranet facilitates communication across the entire organization.

An enterprise-wide intranet involves linking all of an organization's remote sites and users with an IP-based private network as shown in the diagram.

Intranets are popular because they afford a capable, user-friendly and cost-effective way to distribute, collect and manage internal information (Figure 1). The organization achieves the maximum benefit when the intranet extends enterprise-wide.

No organization is too small or too large to take advantage of the proven capability and scalability of the world's largest network, the Internet, to implement an intranet for all of its employees. Whether the company has two or two thousand offices, the two basic requirements of an enterprise intranet are the same:

- Equip each site and user with a suitable system for remote access
- Provide leased line and/or dial-up services for all locations to form the Wide Area Network (WAN) backbone

© 1997 Ascend Communications, Inc.

WAN Security Options

An enterprise intranet or any other private wide area network that uses the Public Switched Telephone Network (PSTN) should have adequate security provisions to prevent unwanted access. Organizations can choose from the following list of WAN security options (relevant standards, where applicable, are listed):

- ***Password Identification** affords the minimum level of protection (Password Authentication Protocol).*
- ***User Authentication** is superior because it positively and securely identifies legitimate remote users (Challenge Handshake Authentication Protocol).*
- ***Token Cards** offer virtually "bullet-proof" authentication with single-use passwords.*
- ***Calling Line ID (CLID) and callback** help ensure that only authorized users are dialing into the intranet.*
- ***Authorization** grants authenticated users permitted access only.*
- ***Firewall** protection is a must when the intranet is connected to any other network, particularly the Internet (refer to Connecting an Intranet to the Internet). Firewalls isolate private resources from the organization's public ones, such as a World-Wide Web server. Integrating the firewall with the remote access equipment is the most easily managed and cost-effective approach. Dynamic firewall technology affords the best protection because it more explicitly allows in and out of the network.*

For managing security provisions, the industry-standard Remote Authentication Dial-In User Service (RADIUS) database maintains user profiles that contain passwords (authentication) and access privileges (authorization). RADIUS also provides an accounting of usage for billback and other purposes.

Different types of sites need different types of remote access equipment. Appendix A provides checklists for equipment needed in the central site, remote offices and divisions, and the small office/home office (SOHO) environment.

For the intranet's WAN backbone, an organization has three options:

- Create it as a totally separate network, in parallel with an existing non-IP private network (not normally the most cost-effective alternative)
- Use multiprotocol routing to merge both the IP-based intranet and the current non-IP networks onto a common WAN infrastructure
- Make the backbone exclusively IP through means of tunneling, encapsulation and/or gateways to carry the traffic of all other protocols

Choosing the best backbone must take into account both the existing WAN provisions and the organization's long-term networking objectives. Multiprotocol routing usually makes the most sense for organizations that expect to have a fairly even mix of both IP and non-IP traffic for the foreseeable future. Organizations that have made a commitment to IP as the strategic protocol of choice are likely best served by a backbone that uses IP switching or is in some other way optimized for IP.

© 1997 Ascend Communications, Inc.

3. Extranets: Adding Customers, Suppliers and Business Partners

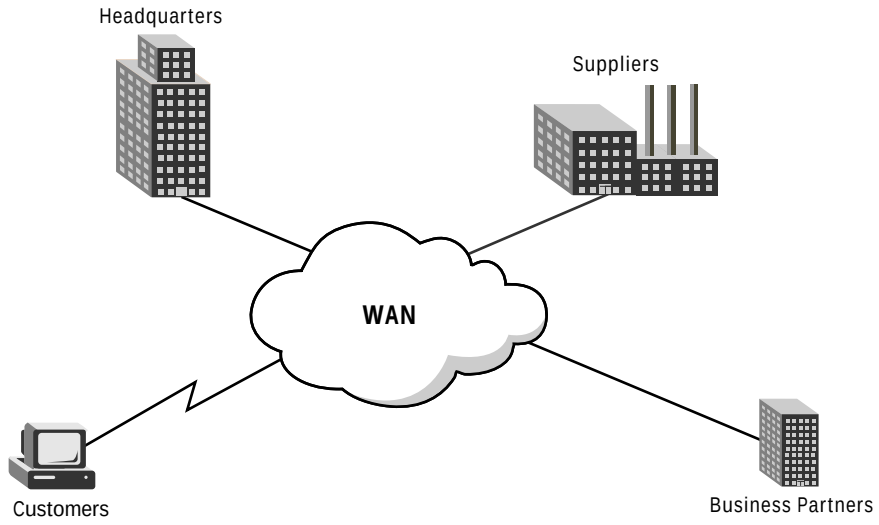


Figure 2 — An extranet extends the intranet to outside organizations, such as customers, suppliers and business partners.

Whereas the intranet is for internal communications, the extranet uses the same IP-based solutions to establish external communications with other organizations.

Extranets employ tried and true industry standards and applications to ensure compatibility between organizations. Perhaps the most significant extranet application is the powerful Web browser/server combination. Web technology gives a homogeneous appearance to heterogeneous data resources, which is particularly important across organizational lines. Web browsers, available for every workstation, are utterly simple to use. Web servers and/or gateways are also available on a full spectrum of platforms ranging from PCs and UNIX hosts to midrange and mainframe computers. Indeed, Web technology is perfectly suited to the extranet.

Establishing an extranet involves providing customers, suppliers and business partners access to internal resources beyond those available to the public on the organization's World Wide Web server (Figure 2). For example: customers may want to check order status; suppliers may need access to the master production schedule; and business partners may be members of internal teams that use groupware for project management.

© 1997 Ascend Communications, Inc.

The remote access equipment used in extranets is identical to that used in intranets. The same network access switch at the central site that accepts dial-in calls from intranet users also handles all extranet calls. Similarly, remote access routers and SOHO routers, like those used in intranets, meet the needs of a wide variety of extranet sites. (Checklist requirements for different types of equipment are provided in Appendix A.)

Security becomes especially important when letting "outsiders" access internal information resources. Fortunately, the security tools needed for extranets are also identical to those used for intranet/Internet access. Popular options for extranet security include password identification, authentication, Calling Line ID (CLID), authorization and firewalls. User authentication combined with a dynamic firewall—both integral to the network access equipment—affords excellent security for most extranets.

The only real difference between intranet and extranet security is substantially more restrictive access privileges defined for all outsiders. Individual security profiles should be defined for each and every supplier and business partner in the extranet. For the multitude of customers, however, defining individual profiles might be too much of a burden. The task can be simplified by creating a "generic" profile for use by all customers. Any customer that requires access to the order processing database, for example, is given the generic account name and password.

© 1997 Ascend Communications, Inc.

4. Connecting an Intranet to the Internet

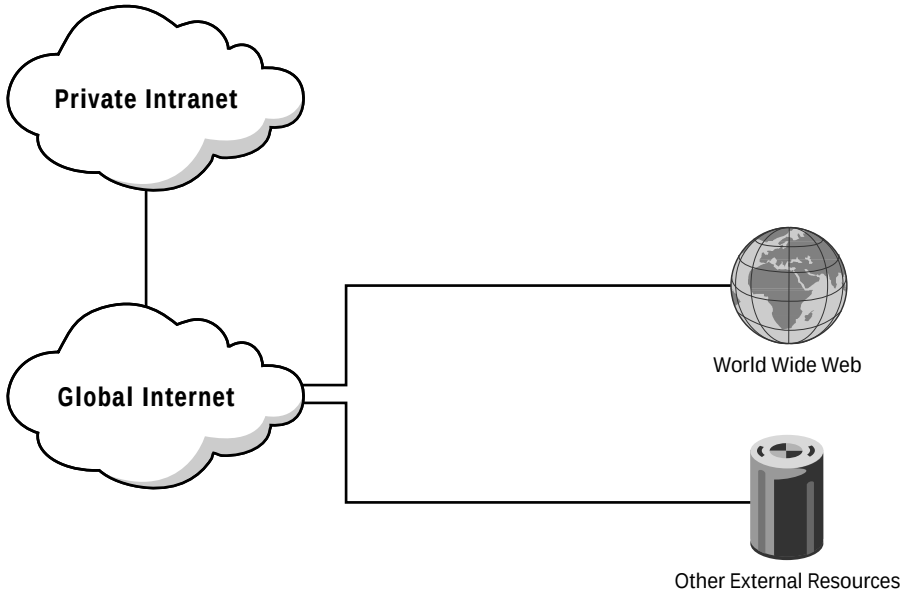


Figure 3 — Internet-intranet integration gives users transparent access to a world of information.

A natural and logical extension for any intranet is seamless integration with the Internet. An integrated intranet/Internet solution leverages common software and network infrastructure for all communications needs. From a single Web browser interface, for example, users can have access to both private and public information resources, and a single e-mail application can serve all internal and external communications needs (Figure 3).

Granting Internet access to intranet users has three requirements:

- A connection to the Internet
- Use of “official” Internet addresses
- Firewall protection to isolate internal resources

© 1997 Ascend Communications, Inc.

There are two basic ways to connect an organization to the Internet. For companies with enterprise-wide leased line private WANs, a single high-speed link from the central site's network access switch can serve all users. For all other companies, the best solution normally is to establish a local Internet Service Provider (ISP) account for each site/user. To access both the intranet and the Internet simultaneously, the remote sites should use multi-channel Integrated Services Digital Network (ISDN) equipment that allows available channels to be used individually or in combination on demand. Whichever option is chosen, the equipment used should be compatible with any advanced features offered by the ISP's Point of Presence (POP) equipment.

Intranets that use "official" IP addresses already meet the second requirement. Intranets with "private" IP addresses have two options. The first is to obtain a block of Internet address sufficient to convert *all* clients and servers. The second is to use a smaller pool of Internet addresses that are "leased" to users from a Dynamic Host Configuration Protocol (DHCP) server, a Network Address Translation (NAT) server or an IP gateway.

A firewall, the third requirement, is needed to isolate private resources while granting outside Internet users access to the organization's public resources, such as a Web server. There are four options, presented in order of increasing effectiveness:

- Use the network access switch's integral firewall to restrict access to public resources with a special profile for all "anonymous" users
- Physically segregate all public resources on a separate LAN segment, commonly referred to as the demilitarized zone (DMZ), connected to its own LAN port on the network access switch
- Totally quarantine the DMZ LAN with a separate network access switch on a separate link to the ISP
- Fully outsource all public servers to the ISP

© 1997 Ascend Communications, Inc.

5. Virtual Private Networks: The Future of Intranets and Extranets

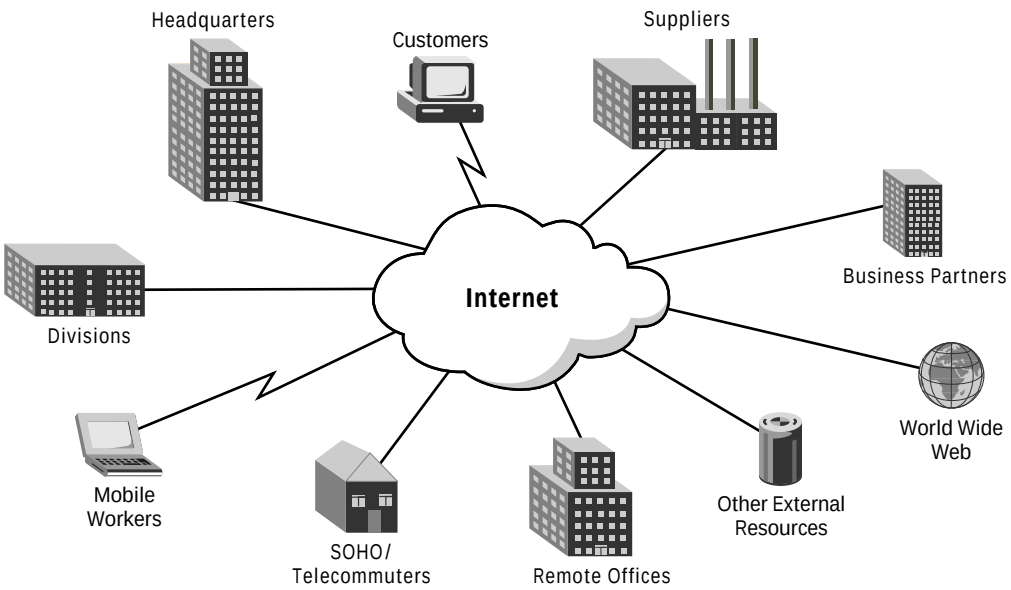


Figure 4 — An Internet-based VPN can provide the long-distance communications for both extranets and enterprise intranets.

Rather than just connect their intranet to the Internet, some organizations may prefer to use the Internet as a "public data network" backbone to transport private data worldwide. Such an arrangement is called a Virtual Private Network, or VPN.

A VPN takes advantage of the Internet's global presence to interconnect all locations in the intranet/extranet (Figure 4). In a VPN, every location has a *local* connection to the Internet through a local ISP. The Internet itself then serves as the wide area backbone carrying all intranet and extranet traffic. By replacing private WANs, VPNs offer a savings of up to 60% over equivalent private networks, according to Forrester Research.

While a VPN costs substantially less to operate than a private network, it cannot deliver the same level of performance. However, the overall price/performance and other advantages, including enhanced flexibility and reduced management responsibilities, should make VPNs quite popular in the future. VPNs are worth considering now for the extranet, and should be ready in a few years for the more traffic-intense intranet.

© 1997 Ascend Communications, Inc.

An Internet-based VPN can employ the same equipment used in a private remote network, provided it meets these two additional requirements:

- Internet compatibility
- Enhanced security provisions

Internet compatibility is achieved—in addition to the same methods available for connecting an intranet to the Internet—with one other option: tunneling techniques. Tunneling encapsulates private intranet/extranet and non-IP packets within public Internet packets. Popular standards include Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Mobile IP, Ascend Tunnel Management Protocol (ATMP) and/or other tunneling protocols based on Generic Routing Encapsulation (GRE).

Security enhancements involve more rigorous control of user authentication and authorization, along with encryption to assure strict confidentiality of all private information that traverses the public Internet. IPsec, which employs the Data Encryption Standard (DES and Triple DES), is the dominant choice for Internet-compatible encryption. For managing the keys that "lock" and "unlock" the encrypted packets, IPsec uses a combination of the Internet Security Association Key Management Protocol (ISAKMP) and the Oakley Key Determination Protocol.

© 1997 Ascend Communications, Inc.

Appendix A: Checklists for Selecting Remote Access Equipment and Management Solutions

There are three basic types of sites in the typical intranet/extranet:

- The central site, usually the headquarters
- Remote offices and divisions with dozens or hundreds of employees, including third party facilities
- The small office/home office (SOHO) for both telecommuters and sales/service outposts, along with individual third party users

Checklists of equipment capabilities needed in all three situations—network access switches, remote access routers and SOHO routers, respectively—can be found in this appendix. Enterprise intranet/extranet network management requirements are provided in a separate checklist.

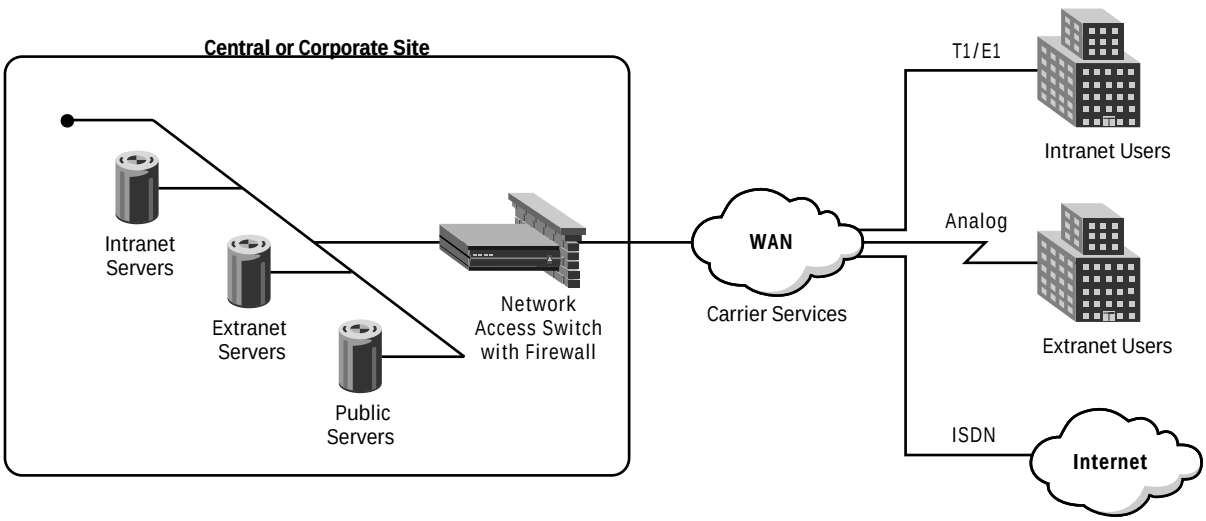


Figure 5 — When setting up an intranet solution, you should consider the types of equipment needed to handle different volumes of traffic and types of applications for each of the basic sites converting to your headquarters.

© 1997 Ascend Communications, Inc.

The Network Access Switch for the Central Site

The network access switch, or WAN access switch, is the heart of an intranet/extranet. Remote sites connect to the switch using leased lines or dial-up WAN services. A capable network access switch also supports high-speed Internet connections and can be used to implement an Internet-based VPN.

Here is a checklist of desirable features for the network access switch:

- ✓ Multi-port WAN capabilities supporting a wide range of services, including T1/E1, ISDN PRI/BRI, Digital Subscriber Lines (xDSL), DS-3, analog modems, cellular, Frame Relay and X.25
- ✓ High-speed channelized PSTN trunk lines to consolidate traffic from numerous remote locations, which likely use different WAN services
- ✓ Digital modem technology for peak performance and compatibility with a broad assortment of analog modems, including new asymmetric 56 Kbps modems
- ✓ A suitable LAN interface such as Ethernet, Fast Ethernet and the Fiber Distributed Data Interface (FDDI)
- ✓ Strong security provisions, especially authentication and authorization
- ✓ Optional dynamic firewall protection that is integrated with the switch's other security provisions
- ✓ Support for VPNs through standard tunneling and IPsec encryption
- ✓ Built-in compression to maximize throughput
- ✓ Dynamic bandwidth management for enhanced performance
- ✓ Ability to handle IP multicast applications
- ✓ Robust local and remote management to maximize uptime at minimal cost
- ✓ Call detail reporting (CDR) to track usage by all intranet users
- ✓ RADIUS database support for administering security and accounting
- ✓ Resiliency with dual power supplies and hot-swapable interface cards
- ✓ Sufficient capacity (WAN ports and overall throughput) to support the anticipated number of sites/users and traffic volume
- ✓ Compatible family of scalable products to keep pace with network growth
- ✓ Certification for operation with local carrier services

© 1997 Ascend Communications, Inc.

Remote Access Routers for Offices, Divisions and Third Party Organizations

The remote access router, sometimes called a WAN router, provides a cost-effective solution for multi-user offices and divisions, along with third party organizations. Depending on the number of users and expected traffic patterns, most remote access routers will use Frame Relay, ISDN, xDSL or leased lines for throughput ranging from 56 Kbps to 7 Mbps. Because ISDN works with bandwidth on demand, it is often the preferred choice for most sites needing intranet, extranet, Internet or VPN access (Figure 6).

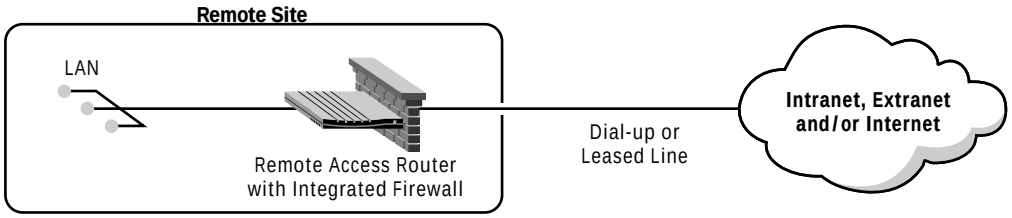


Figure 6 — Through an integrated access router, users on a LAN can access public and private resources as if they had a dedicated line.

Here is a checklist of desirable features for a remote access router:

- ✓ Either a leased line (DDS56, T1/Fractional T1, Frame Relay or xDSL) or dial-up (ISDN BRI) WAN interface for the desired performance
- ✓ A dual WAN unit provides both a primary leased line and a secondary high-speed dial-up link for backup and overflow needs
- ✓ Integral CSU/DSU and/or NT-1 line adapters (required by the carrier) simplify installation and management
- ✓ Ethernet LAN connectivity to assure application interoperability
- ✓ Sufficient capacity or scalability to support all users
- ✓ Standards-based security that supports authentication, integral dynamic firewall protection and IPsec encryption for VPNs
- ✓ Built-in compression to maximize throughput and lower the cost of ownership
- ✓ Dynamic bandwidth management for enhanced performance
- ✓ Ease of installation and simplicity of operation
- ✓ Call detail reporting (CDR) to track each worker's network usage
- ✓ Remote manageability and downloading of software upgrades via the WAN to eliminate the need for an on-site technician
- ✓ A compatible family of products to handle the wide diversity of remote office needs and circumstances
- ✓ Certification for operation with local carrier services

© 1997 Ascend Communications, Inc.

SOHO Routers for Small Offices, Home Offices and Individual Users

The SOHO router, often called an Integrated Access Device or IAD, offers a total solution for data, voice and fax communications—making it ideal for offices with one or a few users (Figure 7). Advanced bandwidth management techniques let users access the intranet, extranet, Internet and/or VPN on both ISDN BRI channels (at up to 512 Kbps with compression) and still receive incoming voice and fax calls—all on a single line. An alternative to ISDN is the Rate Adaptive Asymmetric Digital Subscriber Line (RADSL), which offers a single analog phone line on the same pair of wiring with a digital data line. For maximum productivity at an affordable price, there is no better solution than the SOHO router.

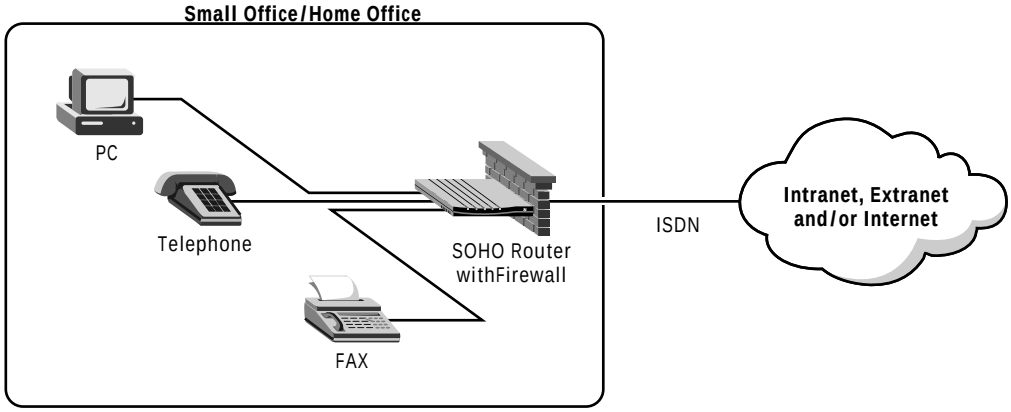


Figure 7 — An integrated access device allows users to perform multiple tasks over a single ISDN line.

Here is a checklist of desirable features for a SOHO router:

- ✓ A single ISDN BRI line that handles all data, voice and fax communications
- ✓ An integral NT-1 interface to eliminate the need for an external adapter
- ✓ Ethernet LAN connectivity for highest performance and greatest flexibility
- ✓ Two POTS ports for connecting the telephone (plus optional answering machine) and a fax machine
- ✓ Standards-based security that supports authentication, integral dynamic firewall protection and IPsec encryption for VPNs
- ✓ Built-in compression to maximize throughput and lower the cost of ownership
- ✓ Support for advanced dynamic bandwidth management to optimize user productivity by handling data, voice and fax concurrently and interchangeably
- ✓ Tamper-proof security that is almost effortless to use
- ✓ Ease of installation and simplicity of operation
- ✓ Remote manageability to facilitate centralized support
- ✓ Certification for operation with local carriers

© 1997 Ascend Communications, Inc.

Enterprise Intranet Management Capabilities

Managing through and across the wide area network or the Internet requires a network-oriented approach rather than the traditional device-oriented management associated with local area networks. In other words, when managing in the WAN environment, it is important to "see the forest and not just the trees." This higher level perspective allows the entire wide area network to be viewed logically in its entirety.

The capabilities needed to manage WANs effectively include:

- Auto-discovery and dynamic mapping of the end-to-end network topology
- Capacity planning and performance trending through collection and analysis of traffic statistics
- User accounting that shows both the level and the patterns of usage by individuals and multi-user sites
- Real-time network monitoring with alert/alarm generation based on user-defined thresholds
- Traffic monitoring should also provide a way to assess actual throughput of dial-up and dedicated WAN lines
- Configuration management for bringing new locations on-line, and coordinating network-wide updates and changes
- A means of comparing actual vs. intended equipment configurations
- A trace function that tracks traffic through the network to help isolate bottlenecks and other problems
- Traditional device-oriented fault monitoring and diagnostics for pinpointing and troubleshooting specific equipment problems
- RADIUS database to handle security and accounting administration

© 1997 Ascend Communications, Inc.

Appendix B: Internet, Intranet and Extranet Solutions from Ascend Communications

Ascend Communications specializes exclusively in remote networking solutions. This dedicated focus enables the company to offer the industry's most advanced and broadest assortment of capable, flexible and affordable systems for enterprise intranets, extranets and Internet access. Different product families address the different needs end-to-end, all the way from the central site to individual SOHO workers (Figure 8). Ascend also offers robust support for mobile workers using ordinary analog modems.

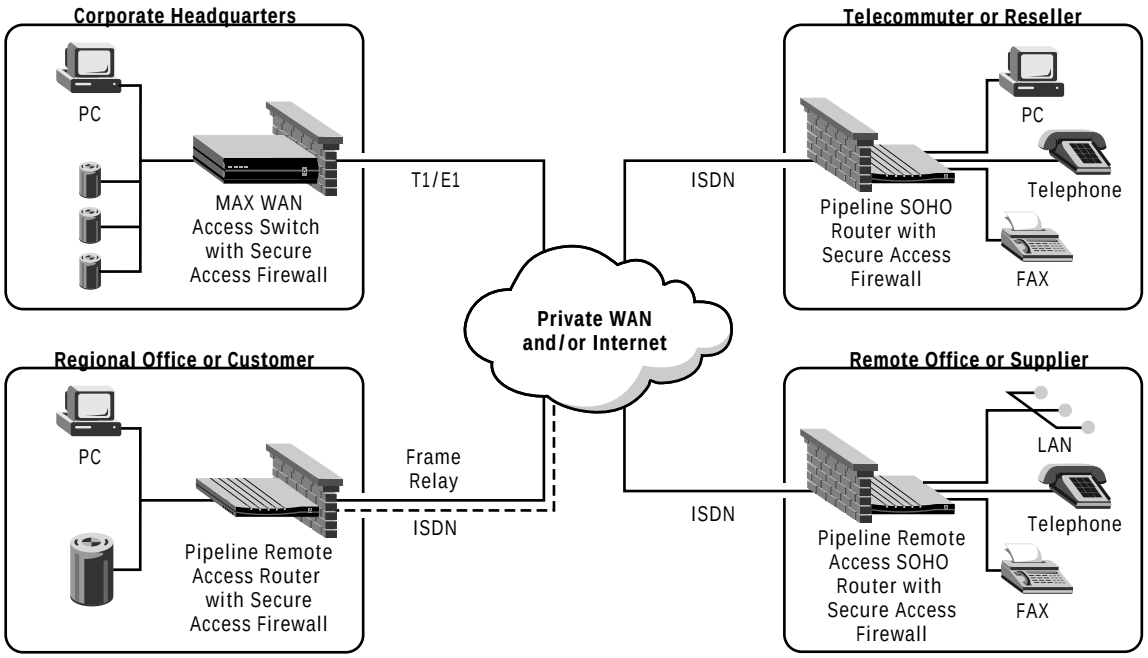


Figure 8 — Ascend offers a complete end-to-end solution for enterprise intranets, extranets and Internet access.

The MAX Dominates Internet Access Worldwide

Ascend's MAX WAN access switches are used by the vast majority of leading ISPs around the globe. In fact, 28 of the 30 largest ISPs use the MAX. In total, over 1,000 ISPs have installed the MAX in over 6,000 points of presence. MAX systems handle some 8,000,000 Internet sessions each and every day. No other solution is more capable—or more proven—for Internet access.

MAX WAN Access Switches

The MAX™ family of WAN access switches is the industry's most advanced network access solution for the central site and other major facilities. Versions of the MAX can support as few as two to over 2,000 concurrent sessions cost-effectively. Every member of the MAX family offers the same proven and robust feature set that has made the MAX the number one choice for Internet access (see sidebar).

Pipeline Remote Access and SOHO Routers

Ascend's Pipeline® family remote access routers and bridges handles everything from single-user home offices to multi-user offices of virtually any size. The SOHO routers afford a complete data/voice/fax communications solution, which is ideal for the home office telecommuter. Ascend's flagship SOHO router is the Pipeline 75, which offers the industry's most extensive feature set. The Pipeline 25-Px provides a less expensive alternative for individuals with less sophisticated needs.

© 1997 Ascend Communications, Inc.

Ascend remote networking solutions provide:

- *Full integration to eliminate the complexity of piecemeal configurations*
- *Multiservice platforms that support a wide variety of network services*
- *Industry-standard features for maximum compatibility and interoperability*
- *Software-based implementations upgradable to conform with future standards*
- *Advanced bandwidth management for the lowest possible cost of ownership*
- *Reliability and high performance to deliver peak productivity*
- *Extensive and easy-to-use network management capabilities*
- *Robust security provisions, including built-in dynamic firewall protection*
- *Certification with PSTN switches, carriers and WAN services around the world*
- *Comprehensive and responsive customer support services*

Data-only versions of Pipeline remote access routers are available in switched (ISDN or SW56) and leased line (T1/Fractional T1 or DDS56) versions. One model, the Pipeline 130, offers both leased line and switched WAN ports for mission-critical situations that require dial-up bandwidth on demand for backup and overflow needs. The award-winning Pipeline 50 is Ascend's most popular ISDN remote access router.

Network Management and Security

Network management begins with the installation and configuration of equipment—a chore that is particularly challenging at remote sites. To simplify the task, Ascend offers a Java-based Pipeline Configurator that automates the installation and configuration process. It allows a novice user to connect with a working configuration in about 15 minutes. Other utilities allow a network manager to optimize the configuration *remotely.*

Once the network is up and running, network managers can use Ascend's NetClarity™ to monitor the entire network. Ascend's NetClarity provides support for auto-discovery and dynamic mapping of the end-to-end topology, capacity planning and performance trending, real-time network monitoring and alert/alarm generation, configuration file management, and a trace function that tracks traffic through the network. Traditional diagnostic utilities for pinpointing and troubleshooting specific equipment problems are also included.

Ascend's Secure Access™ Firewall drives down the cost of security by integrating state-of-the-art firewall technology into the remote access equipment. Having the firewall at the perimeter of the WAN affords better security and eliminates the expense of separate hardware. Secure Access is a dynamic firewall that adapts continuously to changing traffic patterns. To assure maximum protection, the operation adheres to the policy that all access which is not expressly permitted is denied. Secure Access is certified by the National Computer Security Association (NCSA) and is available on all MAX and most Pipeline products.

Ascend's Access Control™ adds some 100 enhancements to industry-standard RADIUS for security and accounting administration. The implementation is the easiest to use and most feature-rich RADIUS-based solution available. The security provisions allow detailed access profiles to be created for both internal and external users. The user accounting shows both the level and the patterns of usage by individuals and multi-user sites. Best of all, Ascend Access Control allows security and accounting functions to be fully distributed and still be managed centrally.

© 1997 Ascend Communications, Inc.

Applications for Ascend Products

	Enterprise Intranets	Extranets	Integrated Intranet/Internet	Virtual Private Network
MAX WAN Access Switches	Central Site	Central Site	Central Site	Central Site and Other Large Sites
Pipeline Remote Access Routers	Remote & SOHO Offices	Third Party Facilities	Remote & SOHO Offices	Remote Offices, SOHO & Telecommuters
Secure Access Firewall	All Sites	All Sites	All Sites	All Sites
Ascend Access Control (extended RADIUS)	Central Site	Central Site	Central Site	Central Site

Ascend: the Remote Networking Industry Leader

- The preferred choice of Internet Service Providers (ISPs) worldwide
- The broadest, most feature-rich remote networking product line available
- The ISDN remote access router marketshare leader (Dell'Oro Group)
- Pioneer in advanced digital communications technologies, including digital modems, dynamic bandwidth management, Digital Subscriber Lines, tunneling and WAN management
- Recognition as the remote networking leader by major industry publications
  - — "MVP Award for Best Networking Hardware" from *PC Computing* magazine
  - — NetGuide Editors' Choice for remote access devices
  - — The "Editor's Choice Award" from *Network Computing* magazine
  - — The largest installed base of WAN access concentrators (Dell'Oro Group)
  - — Network Computing Well-connected award
  - — DataComm Hot Products award

© 1997 Ascend Communications, Inc.

How to Extend the Power of Your Intranet

Fax this Form For Additional Information

To: **ASCEND COMMUNICATIONS INC.**
Worldwide Headquarters
Attn: Pre-Sales Technical Consulting
Phone: 800-621-9578, option 4
Fax: 510-337-2668

From:
Name: _____
Title: _____
Company: _____
Address: _____
City: _____
State/Zip: _____ / _____
Country: _____
Telephone/Fax: _____ / _____
E-mail: _____

❑ Please send information on the following products:

❑ Pipeline ❑ MAX ❑ xDSL ❑ Security

❑ Please have an Ascend sales representative call.

ASCEND Remote Networking Solutions That Work.™

Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502-3002, USA
Tel: 510-769-6001
Fax: 510-747-2300
Toll Free: 800-621-9578
FAX Server: 415.688.4343
E-mail: info@ascend.com
Web Site: http://www.ascend.com

©Copyright 1997, Ascend Communications, Inc.

ASCEND

Remote Networking
Solutions That Work.™

06-10
06-97