RESOURCE GUIDE

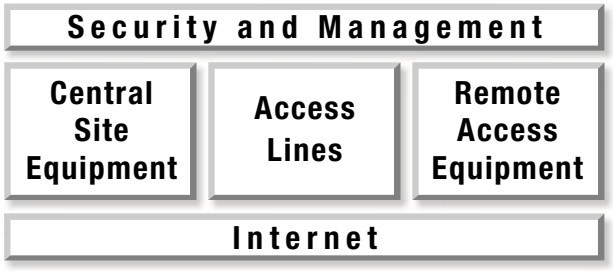
Ascend

RESOURCE GUIDE

Corporate Remote Access Guide

ASCEND

Corporate Remote Access Guide



A Resource Guide for Planners, Executives and Information Managers Worldwide

Table of Contents

TABLE OF DIAGRAMS

1. An Introduction To Remote Networking

What is Remote Networking?

Driven by pressing business needs and shifting social trends, more and more workers are roaming further from their corporate LAN. 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 networking. Simply put, remote networking is a method of extending a company's resources to workers in the field using telecommunications technology. The "field" can be anywhere — across town, across the country or on the other side of the world. The remote workers can be your company's branch office employees, teleworkers*, 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 LAN.

Today's sophisticated digital technologies and advanced communications services meet these needs — faster, easier and cheaper than ever before. Branch office employees access corporate data transparently, at lightening speeds. Traveling professionals conduct business globally, without time constraints. Teleworkers get more work done, with less stress.

** A "teleworker" or "telecommuter" is any employee who works from home, full-time or part-time, after hours or on weekends. The term "telecommuter" is commonly used in North America. "Teleworker" is used in other parts of the world and throughout this document.*

The Benefits of Remote Networking

The obvious benefits of anywhere, anytime connectivity have hundreds of companies pressing forward with plans to build remote access networks. Their plans are ambitious — with 40 percent of respondents to a recent Dataquest survey predicting that more than 20 percent of employees will have some form of remote access by 1998. Members of the business operations and services industry top the list of organizations with plans to install remote access networks. Following close behind are the transportation, communications, utilities, wholesale and retail, banking and finance and manufacturing industries.

Remote Networking:

A seamless and secure connection between mobile workers, telecommuters and remote offices on one hand, and the corporate backbone, the Internet and on-line services, on the other.

Companies can expect to reap substantial benefits from remote networking. According to companies with remote networks already in place, the long list of benefits includes:

- Increased sales
- More efficient customer support
- Faster response to customers' needs
- Quicker project completion
- Increased job satisfaction
- Increased presence in regional areas
- Improved corporate communications
- Employee retention
- Faster product development times

Source: Infonetics Research, San Jose, California

Remote Networking Applications

To get the most out of your remote network, make sure your branch offices, traveling professionals and teleworkers have access to critical applications on the corporate LAN and enough bandwidth to use them adequately. Remote users simply cannot do their jobs effectively without access to e-mail, groupware and the other applications their counterparts use in the home office.

Your users will need access to use some, or all, of the following applications. Most of them require high-bandwidth equipment and connections.

E-mail

Most of your remote workers need e-mail to keep in touch. To send intercompany messages, they will need dial-in access to your company's e-mail server. To send messages to clients, customers, business partners or others outside your company, they will need access to on-line services such as America Online, Microsoft Network and CompuServe or an account at an Internet Service Provider (ISP).

FTP

File Transfer Protocol (FTP) is a simple-to-use program that lets you download files from remote servers on the Internet or other TCP/IP environments. You will need FTP capabilities, for example, to download free software from bulletin board services, research papers from a university and product information from a vendor's web site.

Groupware

If your company uses groupware packages such as Lotus Notes, Microsoft Exchange, Claris Works or WordPerfect Office, giving your remote users access to their powerful capabilities is a must. Groupware includes centralized scheduling programs, bulletin boards, interactive conferencing and "whiteboards" that let groups of users work on a single document or image at the same time. Remote users usually need high-bandwidth to take full advantage of these powerful applications.

Remote Networking Popularity

If your company is implementing a remote access program or expanding an existing one, you're not alone — thousands of organizations have remote access networks in place and the number is more than doubling each year. According to a report by Infonetics Research, companies by 1998 will spend a total of $4.4 billion worldwide on remote access equipment. That's a six-fold increase over 1994 equipment expenditures of just $720 million.

Internet access

Over one-third of the organizations polled by Infonetics Research said their remote sites needed access to the Internet. Yours may need Internet access, too — to collaborate with clients or partners, scan professional journals or make airline reservations. Since most Internet services are inefficient at slow speeds, a growing trend is to give remote callers high-bandwidth connections and digital equipment.

Virtual Private Networks (VPNs)

These new offerings from Internet Service Providers let you set up a Virtual Private Network (VPN) over the Internet. VPNs, acting as Intranets, are a good way to connect your remote sites, teleworkers, customers or mobile users into a secure, private network without paying long distance charges or installing costly dedicated lines. They use tunneling techniques to protect your private data from hackers or other individuals you want to keep out of your network.

Remote Networking Trends

Recent business, social and technological trends are also fueling the rapid growth of remote networking.

Business Trends

Over the last decade, changes in the economy, the shifting makeup of the work force and increasing global competition have created a business environment ripe for remote networking. In response to competitive pressures and workers' demands for more flexibility and empowerment, companies are experimenting with alternative workstyles such as teleworking that increase productivity. In the United States more than half the work force are information workers who can use computers, telephone lines, faxes and express mail to perform their work from almost any geographic location.

Social Trends

Because of changing attitudes about work, leisure time and changes in the size, shape and nature of our families, people are placing increasing importance on flexibility in their work lives. 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 file-transfer 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

Teleworking is one of the fastest-growing segments of the remote access marketplace. Telecommuters include executives, managers, customer support representatives, sales professionals, editors, programmers and other information workers who access their corporate LAN from home.

- *Companies save from $3,000 to $5,000 per year/per telecommuter on facilities costs. (Gartner Group)*
- *Telecommuting results in an average work time increase of two hours per day/per teleworker. (Gartner Group)*
- *Telecommuters at Pacific Bell exhibited 25 percent less absenteeism than other employees.*
- *The number of telecommuters will continue to increase at the rate of more than 10 percent per year through 1998. (Link Resources)*

Thanks to recent advances in telecommunications technology, remote workers now have new options. High-speed, high-performance digital network services and sophisticated access equipment allow remote sites to connect to corporate networks at speeds of 128 Kbps and beyond. This means a wider range of employees, including those with intensive data communications requirements, can now work from the field effectively. Telecommuters, like their office counterparts, can use emerging high-bandwidth applications such as collaborative sessions, large file transfers, whiteboards and desktop video.

This good news is the result of several factors. Local and long distance phone companies have lowered tariffs on high-speed digital offerings such as ISDN and extended their service areas into suburbs and less-populated areas. New services such as Frame Relay and xDSL have come on the scene, tailor-made to fit the usage patterns and traffic requirements of many of today's remote workers. To support these services, a wide variety of digital access equipment is available, at affordable prices.

Network management and security methods have improved, too. Vendors have adopted de facto standards that ensure interoperability with other vendors' devices. Equipment is getting easier to set up and manage with standards-based platforms. New security solutions are available that minimize the increased risks associated with opening corporate networks to remote traffic.

The right time for your company to start remote networking is now. By the end of the century, remote networking will no longer be an option available to only a subset of the work force. It will be a necessity, utilized by companies who want to recruit and retain employees, contribute to a cleaner environment and remain competitive in the marketplace.

2. The Building Blocks of Remote Networking

The Bigger Picture

Technology is just one aspect of your company's overall remote networking strategy. When you look at the bigger picture, larger issues of human resources and business processes come into play.

A Gartner Group report says companies should consider the business issues involved in remote networking before making any technology decisions. Its recommendation: identify the business forces behind your remote networking program, determine the management issues involved and identify the business value of performing work out of the traditional office environment. Once these issues are resolved, proceed to the final step — choosing technology that supports your specific business processes.

This guide does not address these business planning or human resources issues. A variety of publications and videos available from bookstores, libraries and professional associations can help with these aspects of remote networking.

Setting up a successful remote access network involves making some difficult choices.

This guide is an educational tool that will help you make those choices. It explains the mechanics of remote access technologies, describes the pros and cons of different remote access equipment options and guides you through the complex process of building a remote access network. The information will be helpful to a variety of organizations with remote access needs ranging from simple to complex.

Whether you're the planner who devises your company's remote access plan, the executive who approves the plan, or the information manager responsible for implementing the plan and keeping it up and running — this guide helps you accomplish the task before you.

The guide is laid out in a modular fashion. If you're a newcomer to remote networking, you should read it from cover to cover for background on all aspects of the technology. If you're already familiar with basic remote access concepts, you can use it as a reference guide, skimming some chapters and reading others thoroughly for more detailed information.

When you've finished, turn to the three case studies in Appendix A, page 61. These are real-world examples of successful remote access networks. As you read through them, get a feel for the remote networking application that most closely resembles your company's remote access needs. Then complete the Remote Networking Requirements worksheet in Appendix C, page 71. From there, you should have most of the information you need to lay out your own remote networking plan.

The plan you implement now will form the foundation of your company's remote access program well into the next century. Make sure it can expand to accommodate more remote workers, handle high-bandwidth, multimedia applications and provide a smooth migration to an all-digital environment.

Remember, the right technology solution is the one that gives your remote workers the computing resources they need to work effectively. Choosing that solution now means the difference between a remote access program that may never quite get off the ground and one that improves corporate communications, operates within budget, keeps network resources secure and improves your company's bottom line.

Reevaluating Your Remote Access Strategy

Fax for More Information

If you would like assistance in determining your remote networking requirements, fax a copy of your completed Remote Networking Requirements Worksheet in Appendix C to an Ascend Communications PreSales Technical Consultant. Contact details are on the rear cover of this guide.

Chances are, you already have a few branch offices or teleworkers accessing your corporate network. If this is the case, take a close look at how your network infrastructure handles remote traffic now before taking steps to expand your remote access program.

Once you understand your existing remote access strategy, carefully consider your plan for adding new remote users. Are you starting a telecommuting program? Deploying sales staff to virtual offices? Extending connectivity to your business partners or major customers?

If the additions to your remote network are sizable, you should consolidate all of your remote traffic onto a single access line and a single remote access server. This consolidation will eliminate the separate access lines, terminal servers, modem banks and other devices you use now. It will also eliminate the management and support headaches you are experiencing, maintaining racks of equipment and a myriad of different access lines.

Expanding your remote access network may force you to reevaluate your whole remote access strategy. It's a lot of work, but in the long run, a new strategy will save money on access lines and equipment, improve management and support and increase network security. A more integrated approach also gives you the opportunity to plan ahead for the inevitable growth of your remote network in the years ahead.

The Building Blocks of Remote Networking

Setting up a remote networking program that meets your company's needs is a big job. You can make the job easier if you realize it's a step-by-step process that breaks down into five individual building blocks. Use these building blocks to construct your remote access network:

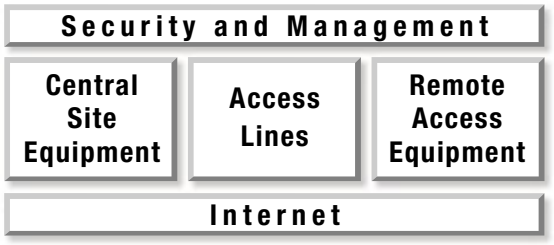


Figure 1

Carrier Services

These are the services that carry data traffic between your remote locations and your central site—such as analog, ISDN, Frame Relay and xDSL. They can be provided by telephone companies as well as Internet Service Providers, Competitive Access Providers and Local Exchange Carriers.

Remote Access Equipment

The equipment that your branch offices, teleworkers and mobile workers use to connect their LANs or workstations to the phone company's access lines is called remote site access equipment or customer premises equipment.

Central Site Access Equipment

Central site access equipment — the linchpin of your remote access network — is the hardware on your corporate LAN that answers incoming calls from remote workers.

Security & Management

Remote access computing exposes your network resources to thieves and hackers. Protect yourself against both internal and external security threats with next-generation security products that are on the market now.

Through network management tools, you can control your remote site equipment and access lines, without sending IS staffers into the field.

Internet Access

Access to the Internet has become a crucial piece of any remote network solution. As companies develop Virtual Private Networks (VPNs)—which allow users at one location to "tunnel" through the Internet to access resources at a different location—the Internet itself helps extend traditional functionality of the corporate LAN.

The following chapters of this guide discuss the building blocks of remote access networking in detail.

Chapter 3 — looks at different access line technologies and their suitability for remote networking applications.

Chapter 4 — discusses the advantages and disadvantages of various types of remote site access equipment.

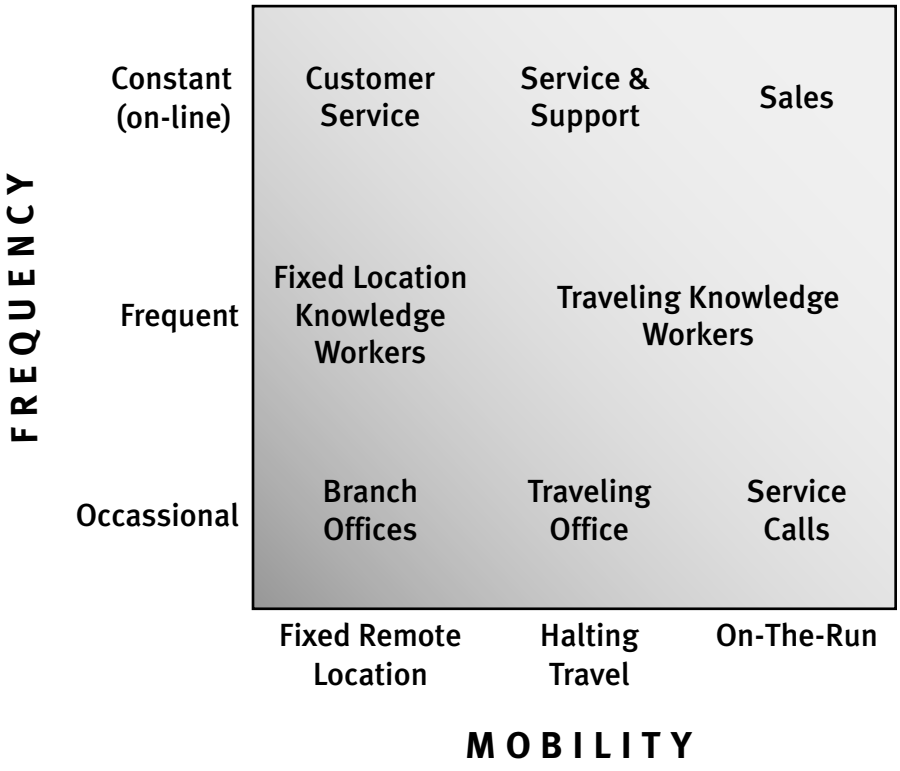
Chapter 5 — takes an in-depth look at central site access equipment and their features.

Chapter 6 — explains the importance of remote access security and the four fundamental elements of a total security solution.

Chapter 7 — describes the challenges of remote management and methods of managing, training and supporting remote users.

Chapter 8 — describes requirements for Internet access and for building VPNs.

Types of Remote Workers



Source: Gartner Group

Figure 2 – Remote workers can be classified by their mobility and by how frequently they access the corporate LAN.

3. Carrier Services: Making the Right Choices

Access lines are the pipes that send data into a carrier's network from an endpoint location such as a branch office, customer's site, telecommuter's home or corporate central site. These pipes connect your remote users with the important computing resources on their company's enterprise network and the Internet.

Setting up a remote access network requires two types of access lines: remote site access lines and central site access lines. Remote site access lines carry traffic from remote users' sites onto the telephone company's network. Central site access lines extend from the carrier's network to your corporate office, aggregating traffic from multiple remote sites onto the corporate LAN.

Consider remote site access lines first. Then decide the type of central site access line you need. The speed, type and number of access lines your remote workers use will determine which type of access line you should install at your central site.

Remote Site Access Lines

Each remote location needs an access line to link their LAN or workstation to your corporate LAN, the Internet or commercial on-line services. This access line must give them the speed and reliability to perform their jobs just as easily from remote sites as from the office.

Consider the following basic issues before you select access lines for your remote locations:

Usage Patterns

Consider your remote access traffic patterns. How often does a particular site need network access? What kind of tasks do users perform remotely? What type and size of files do they exchange over the network? What sort of response times do they need? (See Figure 3)

File Transfer Times

File Type	File Size	9.6 Kbps	28.8 Kbps	64 Kbps	128 Kbps	512 Kbps
Word Processing (20 pages)	**40 K**	33 sec.	11 sec.	5 sec.	2.5 sec.	.625 sec.
Spreadsheet	**100 K**	83 sec.	27 sec.	12.5 sec.	6.25 sec.	1.6 sec.
Black & White	**1 MB**	14 min.	4.5 min.	2 min.	1 min.	15 sec.
Presentation						
CAD/CAM	**2 MB**	29 min.	9 min.	4 min.	2 min.	30 sec.
Digitized Photograph	**4 MB**	56 min.	19 min.	8 min.	4 min.	1 min.
Color Presentation	**10 MB**	139 min.	46 min.	21 min.	10 min.	2.5 min.
X-ray Files	**100 MB**	23 hrs.	8 hrs.	3.5 hrs.	1.7 hrs.	26 min.

Figure 3 – File transfer times will vary considerably, depending on the speed of your remote workers' access lines and the size of the files they transmit.

Your answers to these questions will determine the type of access line you need. An analog line, for example, may be adequate for sales staff at a small remote office who access their corporate LAN twice daily to read e-mail and submit orders electronically. A dedicated Frame Relay connection, on the other hand, may be needed by a bank customer service representative, who works full-time from home and queries his company's database all day long.

Cost

To select the most cost-effective access lines, estimate how many hours per month each remote site will use its network link. Then determine how far away each site is located from the phone company's nearest serving office. With this information, you can determine the relative cost of different types of access lines. Also factor in the cost of the remote site access equipment you will need to support a particular access line type (see Chapter 4).

The Break-even Point: ISDN or Frame Relay

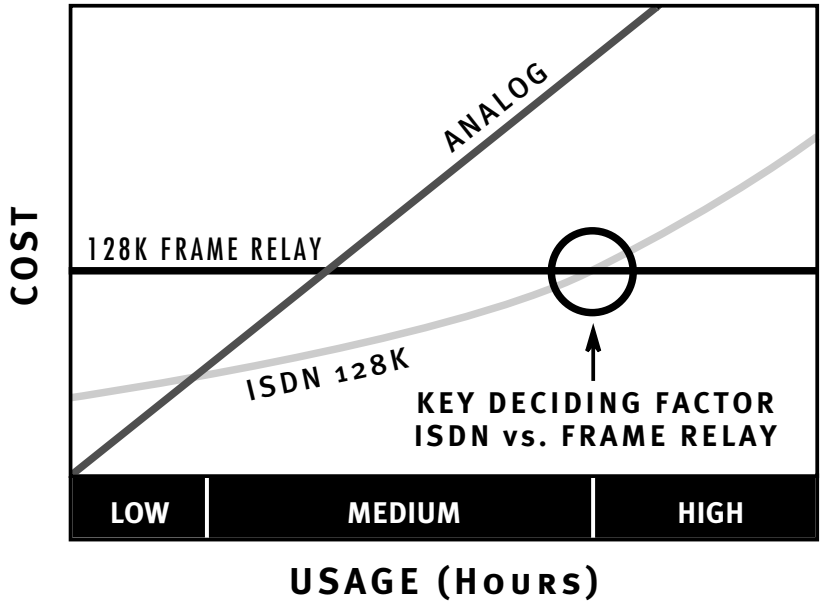


Figure 4 – ISDN will probably be less expensive than Frame Relay, unless your workers live outside your company's local calling area or connect to your LAN an average of more than three hours per day. Check your local carrier's tariffs to determine the exact break-even point.

Availability

Certain remote site access lines such as ISDN or Frame Relay may not be available in all of the geographic locations where your company does business. Find out in advance from your telephone company if you are limited to certain types of access lines in certain areas.

Types of Remote Site Access Lines

Choose access lines with capabilities that align with your remote users' traffic patterns. Four main types* of remote access lines are available:

- Analog, which utilizes circuit switching technology
- ISDN Basic Rate Interface (ISDN BRI), which utilizes circuit switching technology
- Switched 56, which utilizes circuit switching technology (North America only)
- Frame Relay, which utilizes fast-packet switching technology

Switched vs. Dedicated Services

Switched services such as ISDN and Switched 56 are usually more economical for remote networking because charges are determined by usage — you only pay for the bandwidth actually used.

In some countries and regions, depending on tariffing, Frame Relay is a cost-effective option for remote sites with usage requirements of more than three hours per day.

Analog

This is the same service you use at home for voice conversations. Analog lines use modems and Pulse Code Modulation (PCM), a digital representation of the analog wave form, to exchange data traffic over wide area links at speeds up to 36.6 Kbps. Support for up to 56K is possible as that technology becomes more widely implemented at the central site and end user site.

Advantages: *Ubiquitous; inexpensive.*

Other Considerations: *Too slow for heavy usage or high-bandwidth applications; lengthy call set-up time (up to 40 seconds); only 93 percent connect rate; often connect at slower speeds to accommodate noisy line conditions.*

Switched 56

Switched 56 is an end-to-end switched digital service available in North America that supports data transport over a carrier's network at 56 Kbps. Access equipment that performs inverse multiplexing lets you combine multiple Switched 56 lines to achieve a throughput of 112 Kbps or higher. In locations where ISDN is unavailable, Switched 56 is a good substitute.

Advantages: *Twice the speed of 28.8 Kbps modems; available in some areas where ISDN is not.*

Other Considerations: *Can be expensive if remote sites are located a long distance from the phone company's central office.*

** The latest in remote access, Digital Subscriber Line, is being rolled out for testing in some cities and offers high-speed access and file transferring capabilities over existing copper wire.*

Analog Lines: The Drawbacks

Analog phone lines, which were designed for voice communications, present significant limitations when transmitting data. Line noise, nearly imperceptible to the human ear during a phone conversation, frequently wreaks havoc on data transmissions, causing distortion, data errors and lost connections. The switching equipment at the phone company's serving office also creates line noise and data corruption.

Digital services, on the other hand, provide end-to-end digital connectivity from the local loop all the way across the phone company's backbone network. They also eliminate line noise and the time-consuming conversion from analog to digital, and back. As a result, digital connections such as ISDN and Frame Relay provide greater reliability, improved performance and increased throughput.

Transmitting Data Over Analog Lines

Figure 5 – Compared to digital technologies, the process of transmitting data over analog phone lines is slow and unreliable.

To transmit data from a PC over an analog phone line, a modem must first convert the PC's digital signal to analog. The resulting analog signal is then transmitted to the telephone company's central office over a local access line. There, switching equipment converts the analog signal into a 64 Kbps data stream using a technique called PCM. Next, the digital stream containing the digitized analog wave form is transmitted onto a long-distance carrier's digital backbone network.

The process is reversed at the other end of the transmission. Switching equipment restores the digitized PCM stream to its original analog wave form and then transmits it over a local access line to its destination. Finally, another modem restores the analog wave form back to a digital signal so the PC can process it.

ISDN & ISDN BRI

The terms ISDN and ISDN BRI are commonly used in the United States.

In many other countries the term "Microlink" is often used to describe ISDN BRI functionality.

ISDN BRI

ISDN BRI access lines consist of two 64 Kbps channels called B-channels that carry either voice or data, and a third D-channel used primarily for signaling.

In countries where ISDN BRI is available, it is offered as a switched service—also called a dial-up service. (A leased line refers to a connection between two predetermined locations such as a headquarters and a regional office; switched connections can be made to any location from any location.) In Australia, Germany, and Japan, ISDN is also available as a semipermanent service, which is essentially a leased line connection.

Some ISDN BRI access equipment includes a feature called inverse multiplexing that allows users to combine the two B-channels of an ISDN BRI line to achieve a total throughput of 128 Kbps. Used in conjunction with compression, this feature makes it possible to achieve very high data rates. See Some ISDN Basics on page 14 for more details.

Advantages: *Relatively high speed; cost effective; set-up time of less than a second; handles multiple devices, multiple phone numbers and both data and voice calls on a single pair of wires.*

Other Considerations: *Can be expensive in some areas; not available in all countries.*

Frame Relay

Frame Relay is a fast-packet switching technology which is popular in many corporate networks. It works by breaking data streams into variable length packets and routing them across a carrier's network over predetermined logical connections called Permanent Virtual Circuits (PVCs). Frame Relay requires a dedicated connection to the network.

Frame Relay pricing is usually based on some combination of the following:

- Fixed monthly access charges
- Committed Information Rate (CIR) is the minimum amount of bandwidth available to the network. Negotiated between the user and carrier.
- Number of PVCs
- Number of frames transmitted per billing cycle
- The amount and number of times your transmission rate exceeds your CIR

Frame Relay pricing is distance insensitive, making it a good choice for remote offices or teleworkers who would otherwise pay long distance rates to connect to the corporate LAN. It is also a good choice for locations that average more than three hours per day on-line.

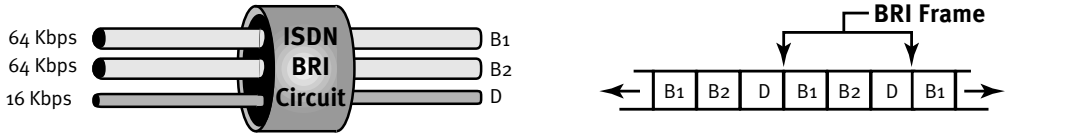
Advantages: *Economical in frequent-usage, high-bandwidth situations.*

Disadvantages: *Expensive if users must set up PVCs to a number of different locations; requires greater technical expertise to set up and manage.*

Some ISDN Basics

Integrated Services Digital Network, called ISDN for short, is an all-digital telecommunications technology that can simultaneously transmit voice conversations and data calls over the same pair of copper telephone wires. What's important about ISDN and what makes it different from the analog phone lines that your remote callers may use today is its flexibility and speed.

Inside An ISDN BRI Line



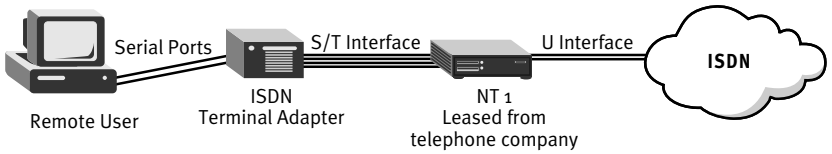
Data and voice traffic travels on the B-channels, B1 and B2. The D-channel is used for signaling information.

ISDN BRI uses a line encoding technique called 2B1Q. The line transmission rate is actually 192 Kbps. Two B-channels (128 Kbps) are available for user data.

Figure 6

Connecting to an ISDN Line

In Europe, The Pacific Rim, Latin America, and The Middle East



In North America

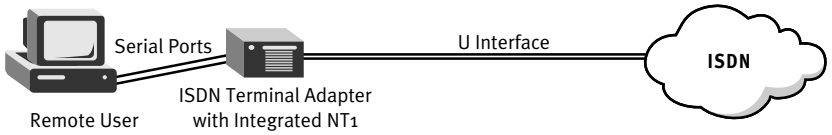


Figure 7 – A U interface connects a two-wire ISDN line to a terminating device called an NT1. In North America, the NT1 is purchased and installed by the customer, as a separate device or integrated into an ISDN access device. In other parts of the world, the NT1 is considered part of the telephone network and is leased to the customer by the telephone company. The four-wire S/T inter face allows up to eight devices to be installed on the same ISDN line.

How ISDN Works

ISDN BRI brings the speed, flexibility and reliability of digital communications right into your branch office or teleworker's home. It works by dividing the total bandwidth of a digital line into three separate channels. Two of the channels, called B-channels (Bearer channels), operate at 64 Kbps and are always used to carry voice or data traffic. A third channel, the D-channel (Delta channel), carries signaling information which tells the telephone network how to handle each of the B-channels.

The flexibility of ISDN comes from its ability to use each B-channel for separate voice or data applications. With ISDN you can download a document from your corporate network over one 64 Kbps B-channel. At the same time, you can browse the Internet or answer a phone call over the other B-channel.

Some ISDN Basics

You can squeeze even higher performance out of ISDN using inverse multiplexing, a standard feature of some remote site access equipment. Inverse multiplexing creates extra bandwidth by aggregating two B-channels of a ISDN BRI line into a single "virtual" channel of 128 Kbps or combining multiple BRI lines for even higher bandwidth.

The Advantages of ISDN BRI over Analog

Once you know how ISDN BRI works, it's easy to understand why it's better for remote access applications than analog lines.

Based on speed alone, ISDN BRI wins over analog hands down. Its top data rate of 128 Kbps is twice as fast as 56K modems, three times faster than the 33.6 Kbps modems, four times faster than 28.8 Kbps modems and nearly nine times faster than 14.4 Kbps modems, the most commonly used modems in the marketplace today.

ISDN beats analog when it comes to call setup time, too. With an analog line and a modem, it usually takes between eight and fifteen seconds to set up a call and sometimes as much as 40 seconds. With ISDN, calls are set up at lightning speeds of just 300 milliseconds. The difference is only a matter of seconds. But for remote users who must dial up network connections repeatedly during the day, seconds mean considerable savings in terms of connect time and aggravation.

Another advantage of ISDN is reliability. ISDN lines are virtually error-free, since they improve a signal along the length of its transmission and maintain full speed, all the way. Analog calls are subject to interference which may corrupt your data and cause modems to automatically degrade to slower speeds. Worse yet, line problems can cause modems to suddenly terminate your network connection.

ISDN BRI Versus Analog

	ISDN BRI	Analog
Speed	64 Kbps on each B-channel 5 times faster than analog	Up to 33.6 Kbps on dial-up modem[1]
	Call setup time: 300 milliseconds.	Call setup time: >8-26 seconds average.
Flexibility	Two simultaneous calls can be made over a single BRI	Only one call can be made at a time.
	Bandwidth expansion is possible through combining B-channels. Up to eight telephones, computers, or fax machines can be linked to a single BRI	A telephone, computer, and fax machine can share an analog line. Only one telephone number can be assigned to an analog line.
	B-channels can be used for voice and data.	
Cost	Faster speeds result in less usage and higher productivity.	Slower speeds result in higher usage and lower computer productivity.

[1]Does not include 56K technology

Figure 8

Last but not least, ISDN is cost-effective. ISDN provides much better speed and reliability. You can save even more money by installing an ISDN integrated access device that lets you run your computer, phone and fax over the same ISDN line.

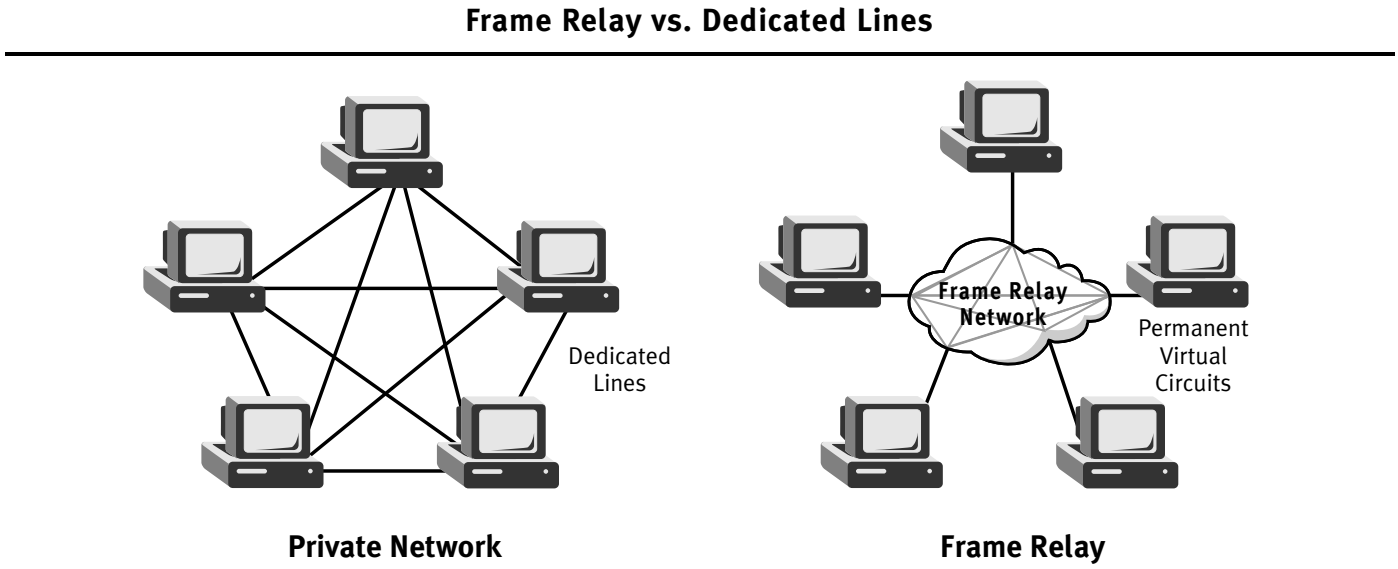


Figure 9 – The private network here requires costly dedicated lines between each site on the network for a total of 10 dedicated lines. A Frame Relay network requires only one connection into the network at each site, for a total of five lines.

Remote Site Access Lines: A Comparison

	Analog	ISDN BRI	Switched 56	Frame Relay (64K)
Speed				
Low	✓			
Medium		✓	✓	✓
High		✓		✓
Frequency				
Occasional	✓	✓	✓	
Frequent	✓	✓	✓	✓
Volume				
Low	✓			
Medium		✓	✓	✓
High		✓		✓
Installation Cost				
Low	✓	✓		
Medium		✓		
High			✓	✓
PROS	Low Cost Ubiquitous	High-speed Relatively Low Cost	Nearly Ubiquitous	Economical for Heavy Usage
CONS	Slow Error-prone	Not available in Some Areas	Can be Expensive	Expensive if Connecting to Multiple Locations

Figure 10 – The kind of access lines you need depends on your telecommuters' usage patterns and bandwidth requirements. Because of aggressive pricing and marketing by carriers and increasingly widespread availability over the last few years, ISDN is becoming the access line of choice for the majority of today's telecommuters.

Central Site Access Line Options

The ISDN Advantage

ISDN PRI lines are popular for central site access applications because they allocate bandwidth to either voice or data on a call-by-call basis.

Customers using PRI lines instead of regular T1 circuits have reported that they can reduce the number of channels they use by 25 percent, according to a recent U. S. study by Pacific Bell.

Now that you've chosen access lines for your remote sites, you're ready to select your central site access lines. These are the circuits that carry data traffic from your branch offices, customers and telecommuters/teleworkers onto your corporate network.

The process of choosing central site access lines consists of three basic steps:

Step 1: Estimate the amount of traffic your remote sites will generate. Base this estimate on the total number of remote users in your program, the combined bandwidth of their access lines and predicted usage patterns. Make allowances for peak traffic periods on certain days of the week or month or at certain times of the day. Then plot your results to determine how much total bandwidth you will need.

Step 2: Consider your new remote access needs in the context of any remote access program you have in place now. If you're already using a combination of separate analog, Frame Relay, ISDN or Switched 56 lines, think about combining traffic from existing remote users and traffic from new remote sites onto one access line. A single access line will save money on your phone bill and on equipment, management and support.

Step 3: Choose the central site access line best suited to your particular needs from the following options:

- Replace individual low-speed lines with a new T1 or ISDN PRI circuit. You will save money and your new high-speed pipe can handle traffic from both new and existing remote users.
- If you have extra bandwidth on an existing T1 or PRI access line, piggyback your remote access traffic onto the corporate LAN over this line.
- If you already transmit voice traffic from your PBX over an T1 or PRI line, reallocate a portion of its bandwidth to carry data traffic from your remote sites.

E1 or ISDN PRI?

T1/E1

In North America, the most widely used digital communications circuit is called T1. T1 circuits transmit voice and data at the speed of 1.544 Mbps over 24 channels of 56 Kbps, each.

In Europe, the Pacific Rim, the Middle East and Latin America, the most widely used digital communications system is called E1. E1s have a total capacity of 2.048 Mbps. Each E1 can be divided into 32 channels of 64 Kbps, each.

In Japan, Hong Kong, Korea, Taiwan and several other countries you may encounter both T1 and E1.

T1 is used throughout this document. Substitute E1 for T1 for your regional offices in Europe and other locations outside North America.

Whether you decide to install a new access line to handle remote traffic or consolidate traffic from a growing number of remote users onto an existing access line, there are two types of central site access lines available to you:

T1

A channelized 1.544 Mbps pipe that is divided into 24 channels. Each channel is capable of carrying a single 56 Kbps voice or data stream. Using T1 access equipment, users can preallocate certain channels on an T1 link to carry voice and others to support data traffic.

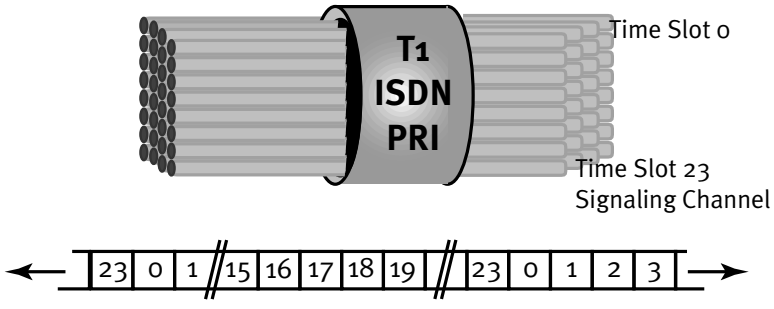
If you don't have enough remote traffic to justify a full T1 link, you may opt to install a fractional T1 access line instead. Fractional T1s are generally available in North America in speeds of N x 56 Kbps, in increments up to 1.544 Mbps.

ISDN PRI

ISDN Primary Rate Interface lines* are based on E1 lines, both physically and electrically, but are channelized differently. Each ISDN PRI line contains 24 64 Kbps channels. One channel is used for framing and signaling, leaving 23 for user traffic. Like T1 lines, ISDN PRIs can carry all different kinds of traffic, including Frame Relay, Switched 56 and voice traffic.

The major difference between T1 lines and ISDN PRI lines is their flexibility in handling calls. With T1 lines, channels must be preallocated to carry either voice or data traffic. With an ISDN PRI/T1 line, channels are allocated dynamically, on a call-by-call basis, as the mix of voice and data calls change.

Inside An ISDN PRI Line



User traffic travels on time slots 0 -22 and time slot 23 carries signaling information.

Figure 11

**In the United States the term PRI or ISDN PRI is commonly used. In many other countries the term Macrolink is used to describe ISDN PRI functionality.*

ISDN PRI, E1 and T1: A Features Comparison

	PRI T1	E1	T1
Speed	64 Kbps on each of 24 channels	64 Kbps on each of 32 channels	56 Kbps on each of 24 channels
		Channel 0 and 16 used for framing and signaling	8 Kbps of each channel is used framing and signaling
	Call setup time: 300 milliseconds	Call setup time: 3 to 5 seconds	Call setup time: 3 to 5 seconds
Flexibility	Any channel can be used for inbound calls, outbound calls, or 800 calls, on a call-by-call basis.	Channels are preassigned for type of calls, so some channels can sit idle while other channels ring busy.	Channels are pre-assigned for type of calls, so some channels can sit idle while other channels ring busy.
	Look-ahead routing feature does not allocate channel if destination number is busy.	Channel is allocated for the call while it checks to see if destination line is busy.	Channel is allocated for the call while it checks to see if destination line is busy.
	Allocate channels by time of day, e.g., more voice calls during day and high speed data transfer at night.	Voice and data channel assignments are fixed and can't borrow from each other.	Voice and data channel assignments are fixed and can't borrow from each other.
Cost	25% more efficient use of channels (avg.)	Need more channels to ensure no busy.	Need more channels to ensure no busy.

Figure 12

4. Remote Site Access Equipment: The Alternatives

Once you've decided which access lines fit your remote users' needs, your next step is to choose equipment that physically connects their LAN, laptop or desktop computer to these lines. Consider your choices carefully. The remote site access equipment you select will have a long-lasting effect on your recurring remote access costs, your network's security and the overall success of your remote access network.

Remote Site Equipment Options and Access Lines

Access Line	Access Equipment Options
Analog	Modem
ISDN BRI	ISDN Terminal Adapter
	Bridge
	Router
	Integrated Access Device
Frame Relay	Bridge
	Router
xDSL	Bridge
	Router
	ISDN Terminal Adapter (IDSL only)

Figure 13 – Your choice of access lines will determine your remote site equipment options.

Remote Site Access Equipment Options

Remote site access equipment has an interface on one side that connects it to the telephone company's access line. On the other side, it plugs directly into an interface on your remote LAN file server, PC workstation or laptop computer.

Your remote site access equipment options are determined by the type of access line you select. For example, a modem is your only choice of access equipment if you install an analog line. If you decide on an ISDN BRI circuit instead, you have three choices of access equipment — ISDN terminal adapters, ISDN bridges or routers or Integrated access devices.

Currently, there are six types of equipment available for remote access:

- **Modems**
- **DSU/CSUs**
- **Routers**
- **ISDN Terminal Adapters**
- **Bridges**
- **ISDN Integrated Access Devices**

Modems

Modems, the workhorses of the remote access world, are stand-alone units or cards that fit inside a PC and connect to an analog phone line. The maximum throughput for most modems today is 33.6 Kbps (newer modems may get as much as 56 Kbps under the right set of conditions)—an adequate speed for many remote applications. Modems are still a must in hotel rooms, customer's sites, or other locations where only analog lines are available.

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

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

Access Line: *Analog*

DSU/CSU — Data Service Unit/Channel Service Unit (North America Only)

The digital equivalent of analog modems, DSU/CSUs are used to terminate Switched 56 or fractional T1 (FT1) access lines. They work by converting data signals generated by digital devices into digital transmission signals for transport over wide area networks. DSU/CSUs can be purchased as stand-alone units that connect to the serial or Ethernet port of a PC or LAN file server. They also come built into larger equipment such as routers.

Advantages: *Inexpensive compared to other digital access equipment*

Other Considerations: *Contains no intelligence; cannot bond channels together to achieve higher throughput.*

Access Lines: *Switched 56 or FT1 leased lines.*

ISDN Terminal Adapters (ISDN TAs)

These simple devices plug into the serial port of a PC or laptop. They work by translating data into ISDN-compatible data using a method called rate adaption, and performing signaling and call setup. Most ISDN TAs cannot automatically bond B-channels of an ISDN line into a single channel. Further, the serial port of a PC limits external TAs to a total of 112 Kbps throughput. Some internal TA cards can get as much as 122 Kbps, still shy of the 128 Kbps maximum throughput available from an ISDN line. With ISDN DSL (IDSL), an Ascend innovation, users can potentially achieve 128 Kbps over an IDSL line.

Advantages: *Less expensive than ISDN bridges or routers; faster than modems.*

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

Access Line: *ISDN; IDSL*

Bridges

Bridges transmit data across wide area networks to other devices on the same LAN segment. Unlike routers, which send packets to specific network addresses over the best route, bridges simply broadcast packets over the entire network. Since they are protocol independent, bridges can be used to connect LANs running different protocols.

Advantages: *Easier to set up and manage than routers or ISDN integrated access devices.*

Other Considerations: *More expensive than ISDN TAs, DSU/CSUs or modems; their inefficient use of bandwidth can result in "broad-cast storms" and network congestion.*

Access Lines: *ISDN; Switched 56; Frame Relay; xDSL; dedicated.*

Routers

These intelligent devices connect remote users to corporate networks over ISDN, Switched 56, dedicated or Frame Relay access lines. Routers select the optimal path for sending data through a network based on routing tables that contain information on all the addresses in the network and the best pathways to each one.

Because routers are protocol dependent, they can only route traffic between LANs running the same protocols but can bridge other protocols. Routers are particularly efficient for linking multiple segments and subnetworks of large corporate LANs.

Advantages: *Operate over multiple networks; make efficient use of network bandwidth.*

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

Access Lines: *ISDN; Switched 56; Frame Relay; xDSL; dedicated*

ISDN Integrated Access Devices

This is a type of access equipment designed specifically for small offices or home offices. ISDN integrated access devices come with an ISDN port and either one or two analog ports, so you can transmit both analog and digital calls over the same ISDN BRI line. They can be configured to function as either bridges or routers.

Advantages: *Handle ISDN and analog devices at the same time; can multiplex both B-channels to achieve 128 Kbps throughput*

Other Considerations: *More complex to set up and provision than other access equipment.*

Access Line: *ISDN*

Remote Site Access Equipment: A Features Comparison

	Modems	ISDN TA	Bridge/Router	Integrated Access Device
Access Line	Analog	2 B-channels	2 B-channels	ISDN and analog
Advantage	• Low cost • Easy	• Low-cost ISDN	• High performance • Secure • Remotely manageable	• Solves SOHO wiring limitations • Analog support • Lower cost line charges • Multiplex voice & data traffic • Secure • Remotely manageable
Disadvantage	• Slow	• Not the full 128 Kbps	• Cost	• Slightly longer installation for analog & ISDN connections
Cost	$100 - $300	$350 - $600	$595 - $2,000	$595 - $3,000

Figure 14 – Integrated access devices let remote workers plug their computer and one or two analog devices into the same ISDN line.

Setting Up The Home Office

Executives, managers or teleworkers who frequently work at home need a full range of equipment in their home offices in order to perform their jobs effectively.

That means duplicating most of the functionality of their corporate workspace in a home office setting. To do that, most home workers will need the following equipment:

- Computer with a built-in modem
- Printer
- Fax capabilities (fax software or stand-alone fax machine)
- Telephone
- Answering machine

Connecting all of this equipment typically requires three separate analog telephone lines: one for data, one for voice calls and one for fax transmissions. The result: three hefty installation fees and three monthly phone bills.

The ISDN Solution

Using an ISDN BRI circuit eliminates the need for three separate access lines. Since ISDN handles both analog and digital traffic, workers can carry on voice conversations, send and receive faxes and transmit data onto their corporate network over a single ISDN line. That increases performance, saves money on phone charges and cuts down on the number of phone lines that must be installed at an employee's home.

To take full advantage of ISDN, your home workers will need an ISDN integrated access device with an ISDN port and either one or two analog ports. With an ISDN BRI line and an ISDN integrated access device, small and home offices can:

- Transmit data at 128 Kbps using both ISDN B-channels.
- Automatically allocate channels for incoming or outgoing calls and faxes.
- Handle two calls simultaneously (two digital, two analog or one analog and one digital).
- Set up a call in about 300 milliseconds.
- Supports multiple pieces equipment on a single line (phones, fax machines, answering machines, etc).

Integrated access devices let users connect both analog and digital equipment, including a computer, analog phone, fax machine and answering machine, to the same ISDN line. The equipment your workers connect to the line can be located anywhere in their home and plugged into standard inside phone wiring. ISDN IADs can be configured to meet specific country requirements, incorporating the NT1 functionality where permitted or providing an S/T interface when required.

The Small Office/Home Office: Before and After ISDN

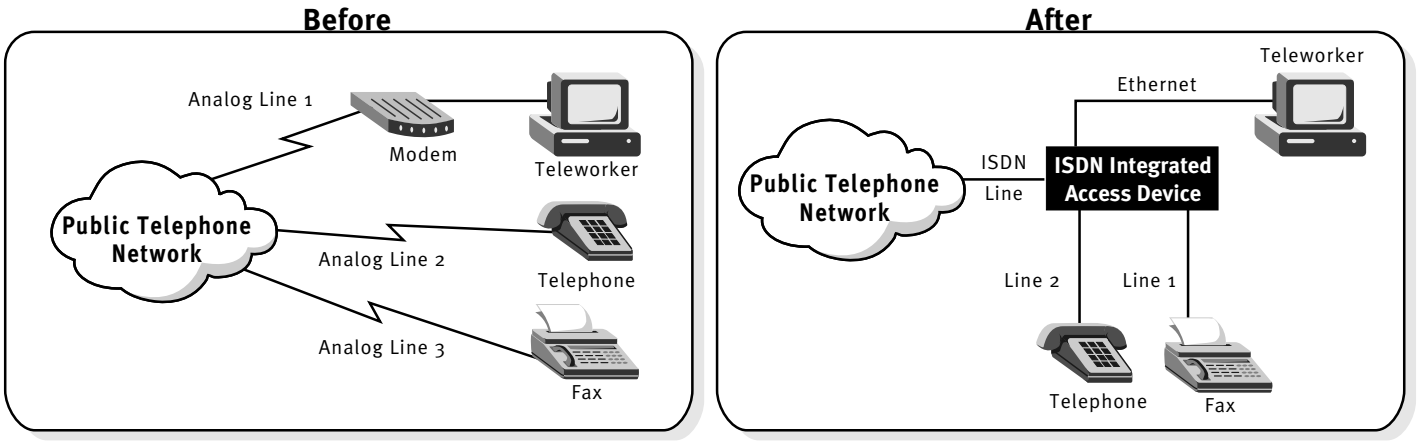


Figure 15 – Many small office/home office users decide they need three phone lines — one for voice, one for fax modems and a third for connecting to the company LAN or the Internet. But the third line often requires new wiring running from the street through the walls of their house — at great expense. An integrated access device eliminates the need for this extra phone line, allowing two lines to function as three and using existing wiring.

Creating more bandwidth

Some access equipment contains special features that give remote workers more bandwidth. That means you save money on access charges and your users can perform their jobs more effectively. Look for these bandwidth management features when you shop for remote site access equipment.

Inverse multiplexing

For applications with fluctuating bandwidth requirements such as large file transfers or videoconferencing, inverse multiplexing gives remote users the speed they need, when they need it. It works by combining multiple Switched 56K channels or 64K ISDN channels into a temporary high-speed data stream, providing N X 56/64 Kbps bandwidth of 112/128 Kbps, 384 Kbps, 512 Kbps, etc. Inverse multiplexers are available as stand-alone units or as features of other access equipment.

Dynamic Bandwidth Allocation™ (DBA), Multilink Protocol Plus™ (MP+)

An important set of features for access equipment, DBA and MP+ work together to add or subtract bandwidth from an ISDN or Switched 56 connection to accommodate changes in the data flow from an end user application. DBA monitors channel capacity and MP+ automatically adds or removes channels from the connection as needed. For instance, ISDN provides two B-channels, which are typically billed as two lines. When users initiate a large file transfer, DBA and MP+ work together to handle the increased traffic by transparently adding bandwidth—the second B-channel—to the connection. When the file transfer is completed, the feature automatically drops one of the B-channels, saving money on transmission charges.

Compression

Compression, a feature built into most access equipment, is another method of creating more throughput for your remote callers. By squeezing large files into smaller chunks by as much as four-to-one, compression reduces the bandwidth required to transmit a block of information. Situations using compression with DBA can, for example, provide 512 Kbps throughput over a 128 Kbps line. With compression activated, that throughput represents a tenfold increase over most modems. (Note: If the source file has been previously compressed, additional compression may prolongate transfer times.)

5. Central Site Remote Networking Equipment

At your central site, you'll need new access equipment to handle the increased flow of traffic from your remote sites. The equipment acts as a gatekeeper between your LAN resources and callers in the field, performing critical functions which include answering incoming calls, checking user passwords, rejecting unauthorized users and routing traffic onto the LAN. On the wide area network side, it connects to the FT1/T1, T1/E1, ISDN PRI/T1 or Frame Relay access line that you are using to carry remote site traffic. On the other side, it connects to your local area network file server.

Remote Access Servers: A Definition

Your best choice of central site access equipment is a remote access server. Remote access servers let any number of users at remote locations dial in over a wide area network link, establish a connection to the corporate LAN as if they were locally attached and terminate the connection once they complete their work. Many remote access servers combine a number of diverse technologies into a single cohesive product, under a single advanced management package.

Today, remote access servers are widely used by organizations faced with exploding remote access requirements. They are rapidly replacing terminal emulation and remote control, older methods of connecting remote users that have been used for the last decade. Both of these older methods have serious drawbacks in today's demanding remote access environment. Terminal emulation treats a remote user's workstation like a dumb terminal, so it cannot support client/server applications. Remote control requires a dedicated PC on the corporate LAN for each remote client and uses proprietary technologies between client and server.

Features of Remote Access Servers

To keep up with the boom in remote access computing, remote access server technology has matured considerably over the last several years. Next-generation remote access servers available now support huge remote access networks with thousands of users, small operations with a handful of teleworkers, and everything in between. They also come with a wide range of price tags and a variety of features and functionality.

Your choice of remote access server depends on the number of remote users you're supporting, the type of access lines you install, your network protocols and your network management and security needs.

- Basic units support just a few users, connect to external analog or digital access devices and target a single wide area network service such as analog or ISDN BRI.
- Mid-range remote access servers typically support several different LAN connections or protocols, come with access devices integrated into the unit itself and handle between 16 and 32 users.
- High-end units are distinguished by a broad range of features that include support for a breadth of WAN interfaces such as ISDN BRI and PRI, T1/E1, Frame Relay and Switched 56, modular design, support for hundreds of remote clients, integrated remote management, routing and terminal server capabilities, digital modems, inverse multiplexing and firewall security capabilities.

Too Much Equipment, Too Many Lines

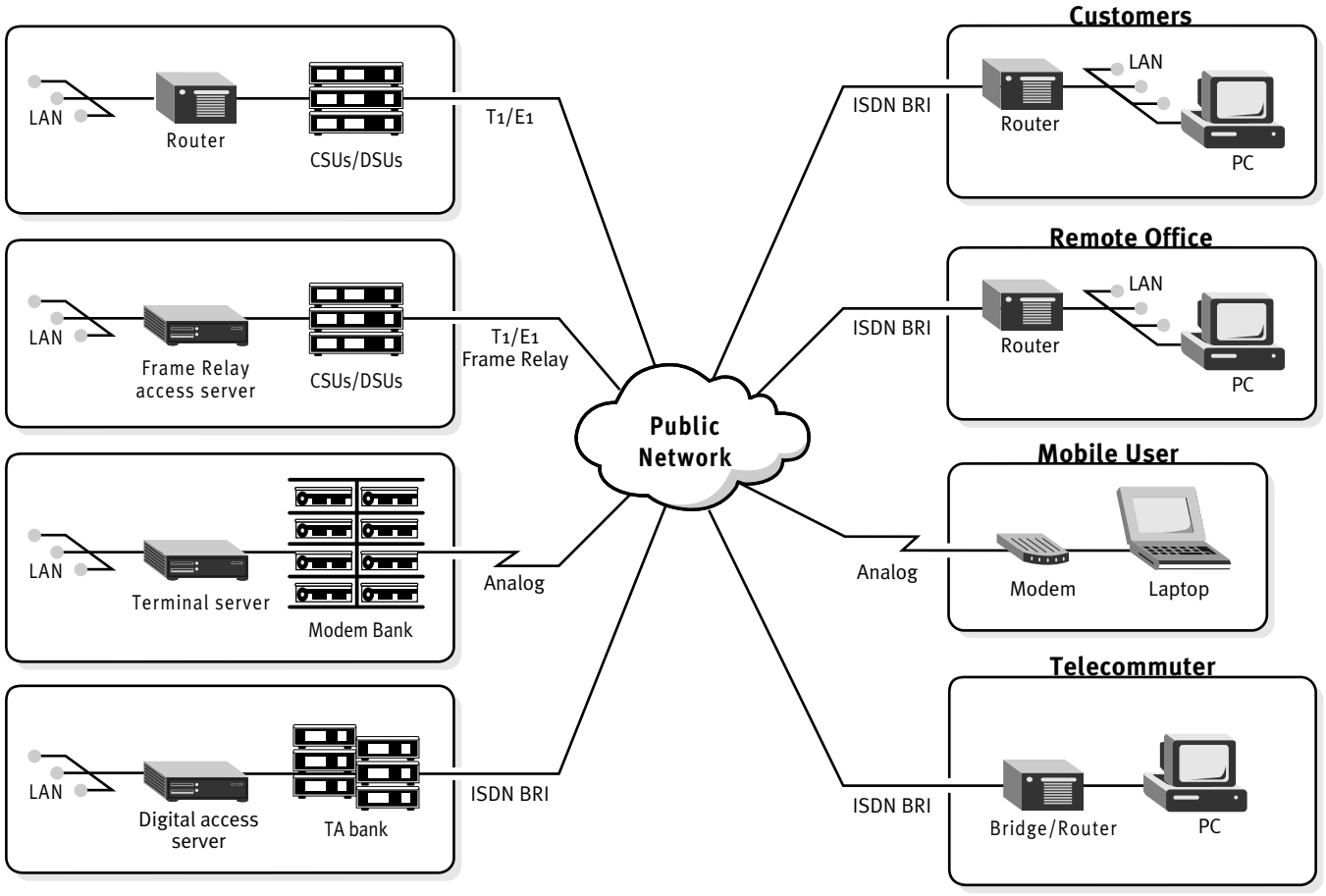


Figure 16 – Using stand-alone equipment for each type of network service can create a complex, difficult to manage network that lacks the necessary security provisions.

In general, avoid low-end solutions that use external modems or other external access devices. They are difficult to manage and force you to allocate a fixed number of channels to either analog or digital traffic. Instead, look for a solution that is flexible, features integrated digital modems for combined analog-digital connectivity, firewall capabilities and scales so you can add more users and access lines quickly.

Remote Access Servers: An Integrated Solution

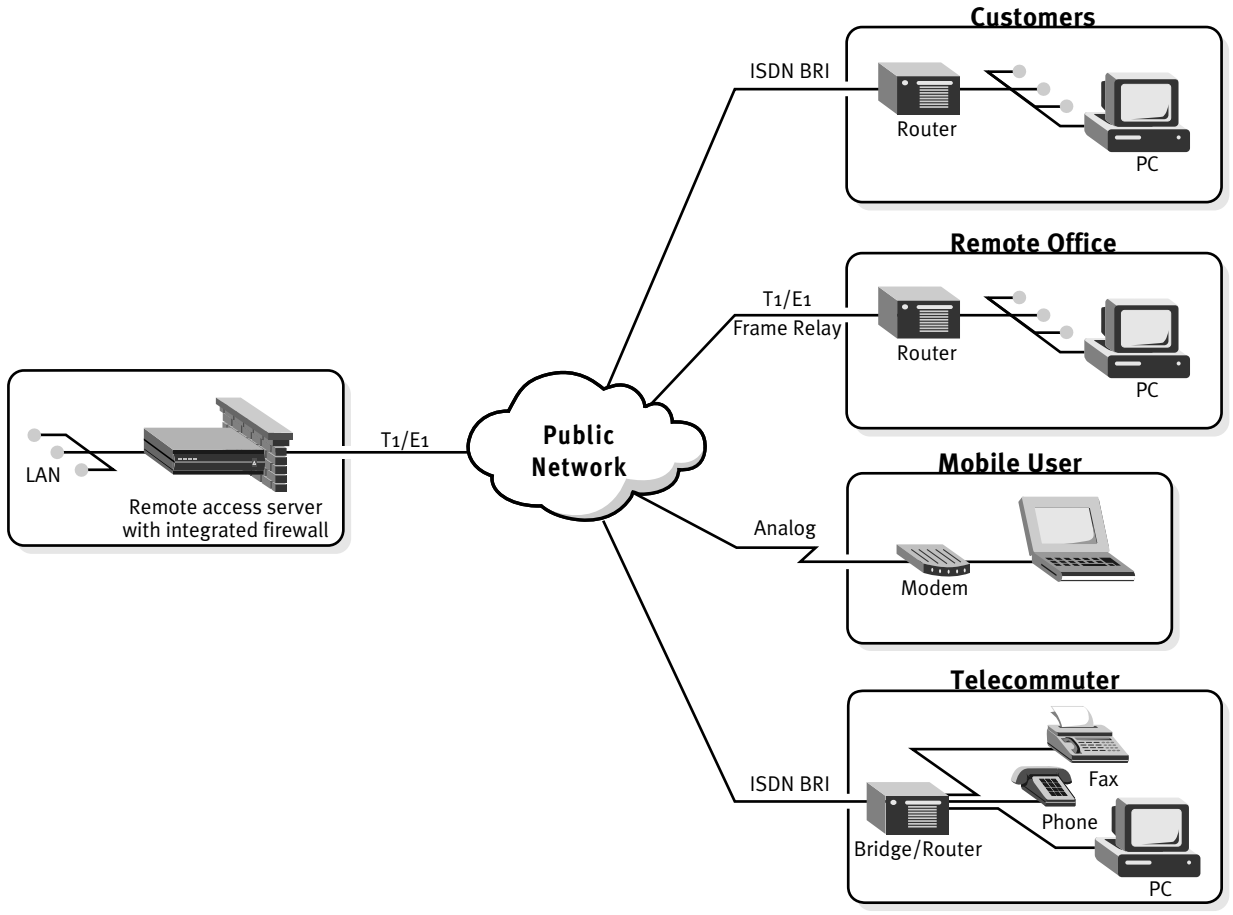


Figure 17 – An integrated remote access server provides a highly efficient, centrally managed solution that has firewall protection built into the equipment itself.

Digital Modems

Digital modems allow a remote access server to support both analog and digital callers over the same digital access line. They work by taking the PCM digital data stream sent by a modem, converting it back to an analog wave form and then performing the necessary demodulation. Digital modems also convert outgoing analog signals from modems on a LAN to digitized analog wave forms and then into PCM data streams, allowing transport over digital facilities.

To protect your equipment investment, make sure your remote access server has digital modem capabilities. If it does, you can switch from analog to digital services simply by replacing the digital modems with new digital interface cards.

Inside A Digital Modem

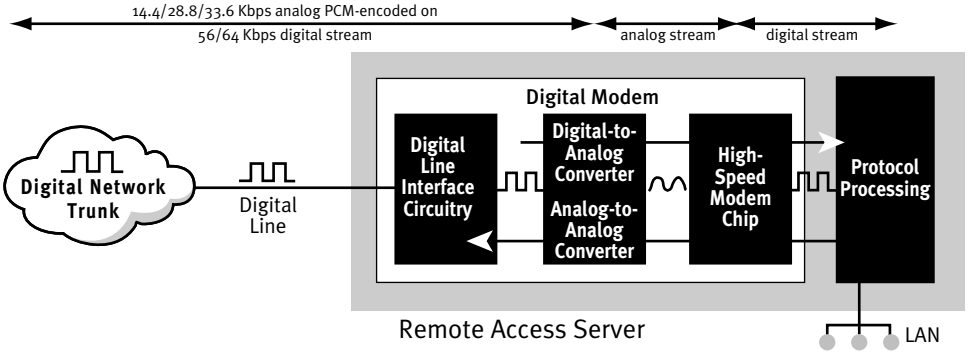


Figure 18 – Integrated digital modems let users with analog lines access the LAN over a digital connection. Users on the LAN can also use the digital modems to dial out.

Five Benefits of Remote Access Servers

Remote access servers are experiencing widespread popularity because they save users time, money and management headaches. Specific benefits of remote access servers include their ability to:

1. Consolidate access lines

A remote access server consolidates incoming traffic from multiple remote locations onto a single access line. This eliminates the need for separate analog, dedicated and digital dial-up lines at your central site. It also cuts down on access line, management and support costs.

2. Replace digital access devices

One remote access server replaces dozens of terminal adapters, DSU/CSUs, routers and other access devices that clutter equipment rooms and wiring closets at central sites.

3. Eliminate modem banks

A remote access server with digital modem capabilities can handle traffic from both analog and digital callers, eliminating the need for separate analog modem banks and digital equipment.

4. Reduce network management costs

Getting rid of extraneous access lines and multiple access devices at your central site reduces the time you spend managing and troubleshooting your network and the cost of network management.

5. Improve network security

Individual modems and terminal adapters are difficult to secure because they create multiple entry points into your network where hackers can enter. Remote access servers can offer increased security by reducing the number of network entry points to just one. They also come with a variety of built-in security features that range from PAP and CHAP to dynamic password authentication to integrated firewall technology. Displacing previously inordinately expensive stand alone firewall devices.

Remote Access Servers: Evaluation Criteria	
LAN interfaces	Ethernet, Token Ring, FDDI, LocalTalk
WAN interfaces	Analog; Switched 56; Frame Relay; ISDN BRI; ISDN PRI; T1/E1; xDSL
Protocols supported	TCP/IP; Netware IPX; AppleTalk; DECnet; SNA.
Number of simultaneous sessions	Ranges from 1 to over 700. Average is 16 to 48.
Compression	Products with hardware compression can support full throughput of four ISDN PRI/T1 or E1 circuits. Products with software compression cannot support more than two.
Video integration	The ability to support video protocols and dynamically allocate 64 Kbps channels to videoconferencing sessions.
PBX integration	The ability to allocate a fixed number of 64 Kbps channels to handle voice traffic from an attached PBX.
Digital Modems	Allows support for both analog and digital callers over a single digital access line (see below).
Terminal Server Capability	Converts incoming serial traffic from modem users into IP traffic for transmission over WAN or LAN interfaces.
Remote Access Routing	Dynamic IP addressing; filtering; remote node support; broadcast suppression.
Special Features	Dynamic Bandwidth Allocation; inverse multiplexing; compression; error correction; spoofing.
Internet gateway	IP routing; filtering by address, protocol and port; PPP support.
Management	Simple Network Management Protocol (SNMP); Telnet; proprietary.
Security	Restricted address; incoming call ID; callback; PAP; CHAP; dynamic password authentication servers, encryption; and integrated dynamic firewalls.
User Authentication	Support for industry-standard RADIUS and the older TACACS systems is required.
Scalability	Modular architecture; expands to accommodate new interfaces; compatibility between product models.
Global certification	Essential if central sites or remote locations are located in countries throughout Europe and the Pacific Rim.

Figure 19

6. Remote Access Security: Issues and Solutions

The statistics you read about computer crimes are alarming. Each year, reported incidents of confidential business information theft are rising exponentially and dollar losses from hacking total in the billions. Crimes run the gamut, from direct theft of a company's bank assets or trade secrets to acts of vandalism that plant fraudulent records on corporate systems or destroy valuable database files.

Adding to the problem is the explosive growth of remote access and Internet access. Although remote computing will provide your company with substantial benefits in productivity, it also poses a serious threat to the safety of your network's resources.

That's why it's more important than ever before to implement strict security mechanisms in your network. In fact, security may be the most important issue to consider when you draw up your remote networking plan.

Define A Security Policy

If your company already has security policies and procedures in place, re-evaluate them in the context of the increased risks of remote access. The measures you already use on your corporate network to identify users and safeguard sensitive data maybe inadequate in a remote access environment. You will need new measures, such as one-time passwords and perimeter firewalls, to thwart clever hackers who now can invade your network by attaching their illegitimate traffic onto legitimate traffic from branch offices, mobile workers or customers.

Before you outline your new security plan or decide what security equipment to purchase, take a close look at your company's unique security requirements. Different organizations will need different levels of security and different security policies. Only your own organization can define your security policy. What impact would the theft of sensitive files or destruction of your billing database have on your organization.

How remote users access your network will also help define your company's security stance, since certain remote access methods carry more risk than others. Do top executives call into your network from home or the road, accessing sensitive information over unprotected phone lines? Do sales staff use wireless modems? Remote users like these will warrant stricter security measures than low-risk users. By simply surfing the net, you are opening the door to hackers who can "steal" valuable corporate resources.

Hacker Facts

- *In another recent survey, 24.2 percent of a group of 898 organizations, both public and private, experienced some verifiable computer crime in the last six months.*
- *One out of five Internet sites has suffered a security breach, according to a survey of Fortune 500 corporations, government agencies and universities.*
- *A 73 percent rise in Internet security incidents occurred from 1992 to 1993.*
- *The number of computer viruses rose from one in 1986 to 5,000 in 1994.*
- *According to the U.S. Department of Defense of 8,932 computers attacked, 7,860 were broken into, 390 detected the attack, but only 19 reported the attack.*

Source: Computer Security Institute, San Francisco, CA

Before you start drawing up your security policy, take the following steps:

Decide what resources need protecting. Your network is a combination of equipment — file servers, LAN segments and workstations; and critical business data — confidential records, customer databases, strategic plans and other types of files. Decide specifically what equipment and data will be exposed to attack when you open your network to remote users. Equipment housing highly sensitive data will undoubtedly require more security.

Perform a risk assessment. An organization can be especially vulnerable to risks if it is growing rapidly, operates in a highly-competitive industry, owns proprietary information or intellectual property that other companies want or works with a large numbers of contractors, consultants or vendors. You may also be vulnerable to theft or vandalism from users inside your own organization. To find out the likelihood of network security breaches, perform a risk assessment or consult a computer security specialist.

Determine how critical your network resources are to your business operations. Ultimately, the amount of security you need will be determined by the value your company assigns to their computing resources and the chance that these resources will be compromised. Could a competitor break into your network and steal your marketing plans, customer database or other confidential information? It is surprising how frequently this occurs. If they did, how much would your company lose in sales revenues?

Decide how much you are willing to spend on security. Implementing iron-clad security can be expensive. There's the initial cost of purchasing and installing security equipment, in addition to ongoing costs of support and maintenance. Make sure the cost of your security measures are commensurate with the value of the resources you're trying to protect and the risk that they will be stolen or compromised.

Once you've taken these steps, determine your security needs and define your organization's position on security. First, define your security position in general terms. Then get specific. Pinpoint what data and systems you need to protect, what levels of protection are appropriate and what security hardware and software you will need to secure your network.

Basic Security Requirements

There are several basic requirements that every successful security solution should meet, whether your company is local or multinational, public or private, large or small. The solution you choose should be:

Integrated. A firewall that is built into your remote access device is easier to manage and prevents hackers from attacking the device itself.

Very Secure. Your solution should use the latest, state-of-the-art technologies and provide the highest possible level of security.

Transparent to users. It's human nature — users will go to great lengths to undermine security methods that are difficult to use. Make sure that doesn't happen in your organization by choosing security that makes logging on from a remote site or home office as easy as logging on from a workstation connected directly to the corporate LAN.

Easy to administer. The system you choose should make it easy to add and change users' security profiles, add and delete users and administer from a central location. It should also let users access multiple servers or subnets without being added to the system multiple times and use the same password to access resources anywhere in the network.

Flexible. As your company's business needs expand, its remote access program will grow, too. Pick a security system that will be flexible enough to grow along with it. Security systems should be able to accommodate changes in platforms, protocols and operating systems without compromising security or impacting network performance.

Deployable enterprise-wide. For end-to-end security, you need to secure both the corporate LAN as well as remote sites. Your solution should be cost-effective enough for end-to-end implementation.

The Elements of Security

To eliminate the increased risks of setting up a remote access network, you need security solutions designed to handle these risks. Security vendors today are building more and more sophisticated security products that address the specific risks inherent in remote access and Internet access.

The security solution you choose should include these four fundamental elements:

- Authentication
- Authorization
- Encryption
- Perimeter Firewalls

Your individual security needs will determine how you combine these elements into a total security solution.

The Elements of a Security Solution

Security Elements	Method
Authentication	Smart Card
	CHAP/PAP
	One-time Passwords
	Simple Passwords
	Token-based Security Cards (RADIUS)
Authorization	RADIUS
	TACACS
	TACACS+
	Access Control
Encryption	Network Level
	Application Level
Perimeter Firewall	Static Packet Filtering
	Dynamic Firewall

Figure 20

Authentication Methods

Authentication is the process of forcing users to prove their identity before they can gain access to a network's resources. Methods range from simple password exchanges to sophisticated dynamic password authentication systems that use one-time passwords and separate hardware and software at the user's site and the central site.

In many remote access environments today, traditional reusable passwords used alone do not provide adequate security. Passwords are simply too easy to guess, and hackers with electronic "sniffers" can steal them as they move over a network. If you do allow reusable passwords, insist that users choose strong passwords containing a mixture of letters and numbers, not obvious ones such as social security numbers or names of family members or pets. Also be sure to limit the number of log in attempts with bad passwords.

Most authentication mechanisms are available as built-in features of remote site and central site equipment. As you perform evaluations of remote access equipment, look for these features and test their performance. Commercially available software packages that provide authentication include: RADIUS, Ascend's Access Control™ (an enhanced version of RADIUS), TACACS, and TACACS+.

Following are descriptions of the most commonly used authentication methods, listed in order from the least secure to the most secure. Dynamic password authentication systems, used in conjunction with other security methods, provide the highest level of security available today.

Restricted Address

This is a first line of defense that keeps unauthorized users from accidentally gaining access to your network. It works by programming your central site server with a list of remote node addresses that can dial into the network. Only incoming calls from addresses on the list are accepted; all other calls are rejected.

Advantages: *Protects against accidental access by users dialing an incorrect phone number.*

Other Considerations: *Authenticates the equipment, not the user, so stolen equipment can be used to gain network access.*

Incoming Call ID

When a remote caller initiates an access attempt, this security method checks the caller's authorized phone number against the phone number provided by the telephone company's network switch. If the numbers match, the user is allowed access to the system. Incoming call ID is a special service provided by the phone company. To use it, your central site equipment must also support incoming call ID. Incoming Caller ID is also called Calling Line Identification or CLID.

Advantages: *Very secure, since defeating it requires tampering with the phone company's central office switch.*

Other Considerations: *Can't be used by mobile workers; service is not available in all areas.*

Callback

With callback, a remote user dialing into central site must identify himself with a password or identification number. The central site server then automatically terminates the connection and calls back the user at a telephone number that has been preprogrammed into the server.

Advantages: *Reliable for verifying a call from a particular site, such as a customer's location or a teleworker's home.*

Other Considerations: *Doesn't work for mobile workers calling in from locations such as client sites or hotel rooms; adds a delay to the process of establishing a network connection; can be bypassed using call forwarding; does not protect against the unauthorized use of a computer at an authorized location.*

PAP

Password Authorization Protocol (PAP), a simple password protocol that is part of the IETF suite of protocols, transmits a user's name and password across a phone line to a central server for authentication. PAP's password database on the server is encrypted; a user's password as it travels across the network link is not.

Advantages: *Password database is encrypted.*

Other Considerations: *Password is transmitted in the clear, making it very easy to electronically eavesdrop the line and pick up passwords.*

CHAP

When a remote user calls a server that uses Challenge Handshake Authorization Protocol, the server sends back a random challenge (key) to the modem, bridge or router that initiated the call. Using the key, the remote access equipment encrypts the password and returns it to the server. Password snooping is very difficult with CHAP, since the password is encrypted before it is transmitted over the network.

Advantages: *Secure against eavesdroppers.*

Other Considerations: *Since CHAP's password database is in plain text form it is vulnerable to snooping.*

Dynamic Password Authentication Systems

These are third-party products that consist of software running on a UNIX machine and two-factor password generators that generate dynamically-changing passwords. Password generators are software-based or hardware-based "tokens" the size of credit cards that remote users carry with them. Both types of password generators use two-factor authentication, a method that requires a user to provide something he knows (a password or personal identification number) and something he has (the software password generator or token).

There are two types of two-factor authentication systems: time-based and challenge-response. Time-based authentication systems generate a password every 60 seconds that is valid for one minute. A user must send the password over the network within that time period in order to gain access to the system. Challenge-response systems generate an encrypted password good for a single use, only.

Advantages: *Harder to defeat than other security methods since passwords are used once only; good for traveling workers who are not statically located and may use different computer equipment.*

Other Considerations: *Third party products may cause compatibility problems in multivendor environments unless used with the RADIUS security server (see a more detailed explanation of RADIUS and third party products in "Authorization Methods.").*

Security Tips for Corporate Networks

Password security: In computing environments that allow reusable passwords, ensure that strong passwords are chosen. Insist that passwords contain an alphanumeric mix and are at least six to eight characters long. If appropriate, use third party software to enforce password composition rules and forced password changes. Alternately, consider implementing one-time passwords or tokens for authentication and authorization.

Anti-virus defense: Install anti-virus software at both the network server and workstation levels. Keep up with current versions and do not allow users to disable software. Use both a scanner to detect existing viruses and an activity trapdoor to look for viruses unreported by the users.

Network communications: Use encryption to protect sensitive data over networks.

Remote access: For secure dial-in access, implement unique user IDs and passwords, limited access terms and limited connection durations. Consider token cards and dial-back modems.

Internet access: Do not allow Internet access without ensuring that firewalls and other integral components of information security are in place. Use firewalls, but not as your sole means of defense.

Mobile computers: To secure mobile computers, install access control programs and physical security devices. Consider encryption and token cards.

Buy smart: Before purchase, evaluate products for security features. After purchase, disable default accounts and change default passwords. Turn on all appropriate audit and security features.

Audit: Conduct regular and frequent reviews of security logs and audit trails. Institute an incident report procedure.

Identify risks: Conduct a thorough risk analysis of your computing environment. If you don't have the expertise in-house, look for outside help.

Enforce policies: Develop comprehensive policies and procedures for all aspects of information security and make sure they are enforced.

Educate your users: Raise the security awareness of your users with an enterprise-wide educational campaign. User-oriented computer security newsletters, videos and posters can also be effective tools. Tell them why security controls are necessary and teach them how to use them.

Educate yourself: There is a wide range of training, conferences, books, periodicals and newsletters on computer security.

Source: Computer Security Institute

Authorization Methods

Once a user is authenticated, another security mechanism called authorization takes over. Authorization, also called access control, is a method of establishing access privileges for users or groups of users. Access can be granted to all of a network's resources, or restricted to specific LANs, LAN segments, network servers, devices or applications.

The authorization function is performed by special software running on a dedicated server. The server's database maintains a unique security profile on each user in the network. It also keeps accounting records on each caller that managers can use to track usage patterns and charge back departments within their organization.

Authorization systems support call, data and generic filtering, a feature which manages and controls the type of applications and resources a caller can access, such as telnet, WWW and FTP. For increased network security, filtering can be performed based on source/destination IP addresses, protocols and port numbers. Generic filtering provides similar filtering capabilities for other protocols such as IPX and NetBIOS.

Authentication Methods

Data Sensitivity		Security Solution		Result
Non-sensitive data	→	No Security	→	Requires no security
Limited security	→	Restricted access and PAP	→	Prevents accidental access
Mid-range security	→	CHAP	→	Defeats snooping on a line
High security for users at predetermined location	→	Incoming Call ID and Callback	→	Requires tampering with telephone system to defeat
High security with one-time authentication and restricted access	→	Dynamic password authentication servers	→	Defeats snooping, unauthorized user at authorized work site or theft of remote access equipment

Figure 21

Authorization systems are designed to control the access of individual users and user groups, only. If you decide to block access to certain resources on a company-wide basis, use a perimeter firewall to do it (see Perimeter Firewalls section, page 44). Perimeter firewalls are useful for restricting access to a certain Internet destination, for example, or use of a particular protocol.

The four commercially available software packages that handle authentication also authorization support: RADIUS, TACACS, TACACS+ and Ascend's Access Control (an enhanced version of RADIUS).

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is the security administration standard that is widely used by large and small companies, ISPs and carriers. It provides authorization, identification, authentication and management services to distributed networks. Currently in the process of being approved as a standard by the Internet Engineering Task Force (IETF), RADIUS is already the de facto industry standard for security authorization and authentication.

RADIUS functions as an information clearinghouse, storing complete security profiles on all of a network's users, including access restrictions, destination-specific routing, packet filtering and accounting information. 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 security profiles for thousands of users.

How RADIUS (Remote Authentication Dial-in User Service) Works

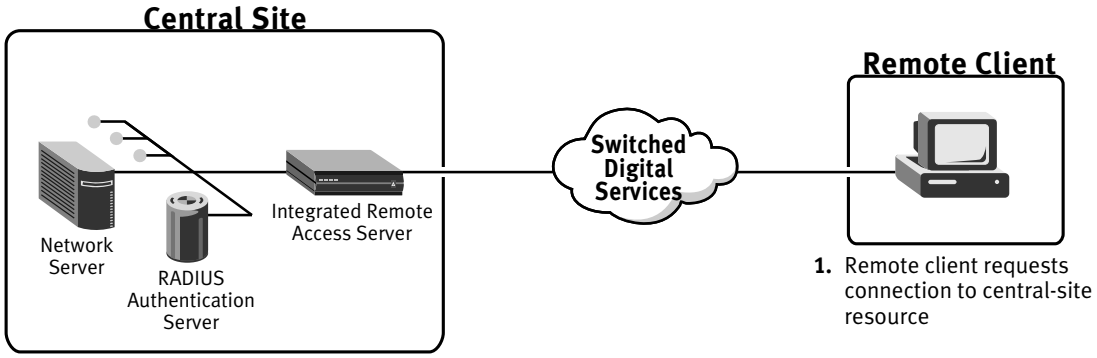


Figure 22

Here's how RADIUS works. When remote callers with modems, ISDN TAs, bridges or routers request access to a RADIUS-managed network, a remote access server answers the call. The server obtains the caller's user name and password and forward it to RADIUS for authentication. Then, the server requests the user's authorization information from RADIUS. RADIUS looks up the user's security profile in its database and passes it back to the server. Finally, the server grants the user network access according to the access privileges contained in his RADIUS security profile.

In addition to its authorization and authentication capabilities, RADIUS performs two important functions. Its central database can manage authentication for all users on a network, regardless of their location, simplifying security administration. RADIUS also allows remote access products to interoperate with third-party security systems from different vendors on the same network.

Encryption Methods

Encryption, the art of writing in secret code, disguises the contents of a message as it travels over a network, making it unintelligible to hackers and eavesdroppers who may monitor or copy it. Encryption uses a mathematical algorithm and a digital key based on the algorithm to code a message at one end of a transmission and then decode it at the other end. Only a user who possesses the key can unlock and read an encrypted message.

Encryption can protect just part of a transmission, such as a user password or a credit card number, or entire files. Encryption is most commonly used for securing passwords as they travel across wide area links. Less common is full data encryption, which encodes and decodes large blocks of data, such as sensitive files. Full data encryption is usually cumbersome and costly because it takes lots of computing resources and processing time.

Encryption can take place at two different stages of a network transmission. End-to-end encryption, a method of safeguarding data over both a user's internal network and a public network link, is performed by the client workstations at either end of the transmission. Network encryption, which encrypts data traveling between routers or integrated remote access servers over wide area links, is performed at the firewall level.

The new standard, IPSEC, an Internet standard for securing IP traffic, permits authentication of every IP datagram and at the same time allows encryption at the network level or application level selectively.

Types of Encryption

Used in conjunction with other security mechanisms, encryption should play a critical role in your network's security scheme. Encryption systems in use today consist of two types — private-key encryption and public-key encryption.

Private-Key Encryption

With private-key encryption, a single unique key is used to encrypt and decrypt data. Private-key encryption is an effective method for encrypting small amounts of data such as passwords, and transmitting them between a single device such as an integrated remote access server and a large group of users.

Data Encryption Standard (DES), an encryption scheme developed and maintained by the Institute for Computer Science and Technology for the National Bureau of Standards, has become the nonproprietary industry standard for private-key encryption.

Public-Key Encryption

Public-key encryption uses two different keys for performing encryption. One is a private key that individual users use to encrypt their own messages. The other is a public key that users distribute to the recipients of their messages. The public key will only decode messages sent by the user holding the corresponding private key.

Public-key encryption is typically implemented in electronic mail systems to protect messages as they are sent over wide area communications links.

End-to-End Encryption

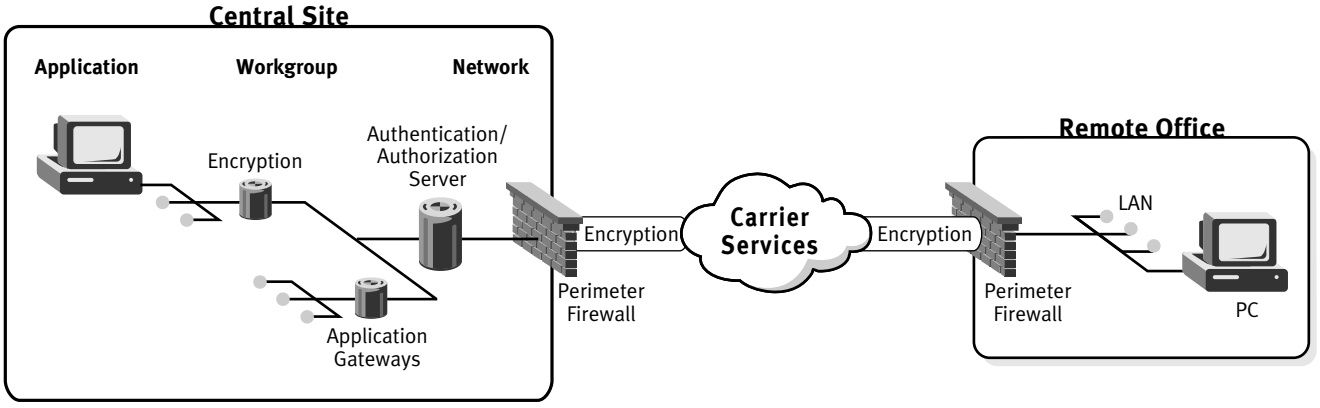


Figure 23 – End-to-end encryption safeguards data over both a user's internal network and a public network link. Network encryption safeguards data traveling over wide area links.

Perimeter Firewalls

With Internet usage soaring at the rate of 1.5 million users a month, the number (see Hacker Facts, page 34) of hackers staging attacks from the Internet is soaring along with it. Your company needs firewall protection if your network has links to the Internet or to any remote network. Firewalls are the only mechanism that can adequately protect your computing resources against thieves and vandals.

Perimeter firewalls are barricades that you erect at the edge of your company's network to keep intruders from entering. Think of a firewall as a giant door blocking the only entrance into your castle. Friend and foe, alike, must knock on this door to request admittance. When foes knock, the door recognizes them as intruders and repels them immediately before they ever set foot inside the castle. But when friends request entry, the door opens and admits them at once. To friends, the door into the castle is invisible.

Perimeter firewalls can be implemented at the network level, as stand-alone devices, or as fully integrated firewalls built into routers or integrated remote access devices. They can also be implemented at the application level, using proxy gateways and servers.

Stand-alone Firewalls

Most commercial firewall products are stand-alone, or managed component, firewall applications. These systems usually require the following elements:

- Specialized firewall software
- Firewall configuration and management software
- Dedicated hardware to run the applications
- A router to establish a connection to the Internet or other remote network

Stand-alone Firewalls

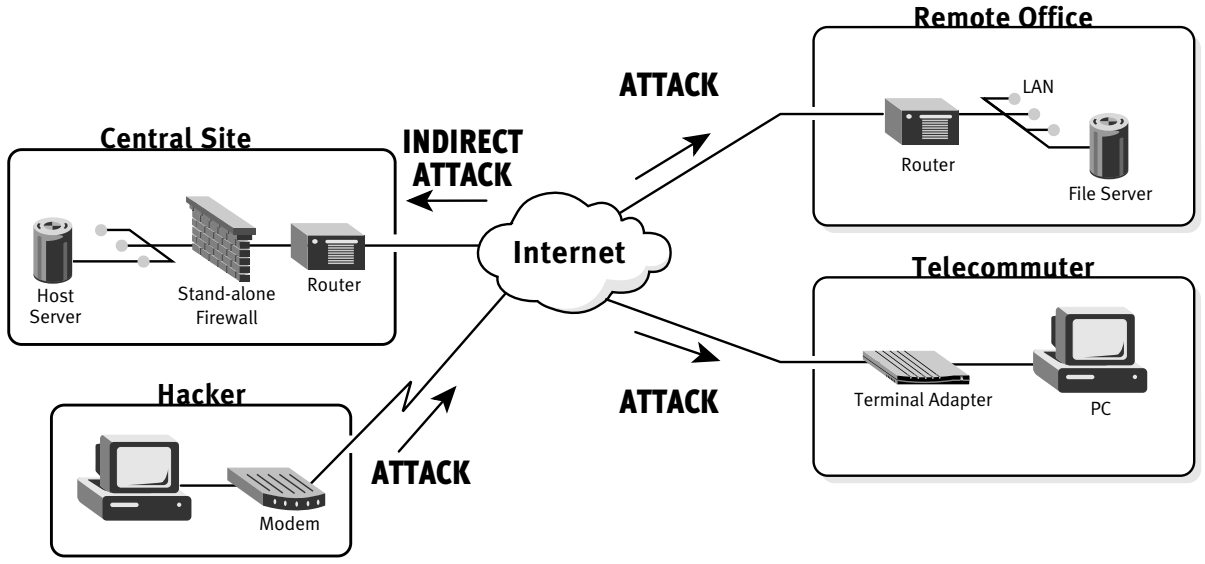


Figure 24 – Stand-alone firewalls are expensive hardware/software solutions that require a great deal of tinkering and adjustment to both the firewall and the router to provide maximum security. Since stand-alone firewalls are installed behind the router, the router itself is exposed to hacker attacks.

The cost of purchasing a stand-alone firewall solution can amount to as much as $40,000 or more. Because of this high price tag, stand-alone firewalls make deployment throughout the enterprise too expensive for most companies, leaving remote sites vulnerable to hacker attacks. Since stand-alone firewalls are installed behind the router itself, they also leave your router exposed to attacks.

Integrated Firewalls

Integrated firewalls are available at a fraction of the cost of stand-alone solutions, so you can afford one in front of every entry point into your network that may be vulnerable, including branch office routers and telecommuters with stand-alone systems.

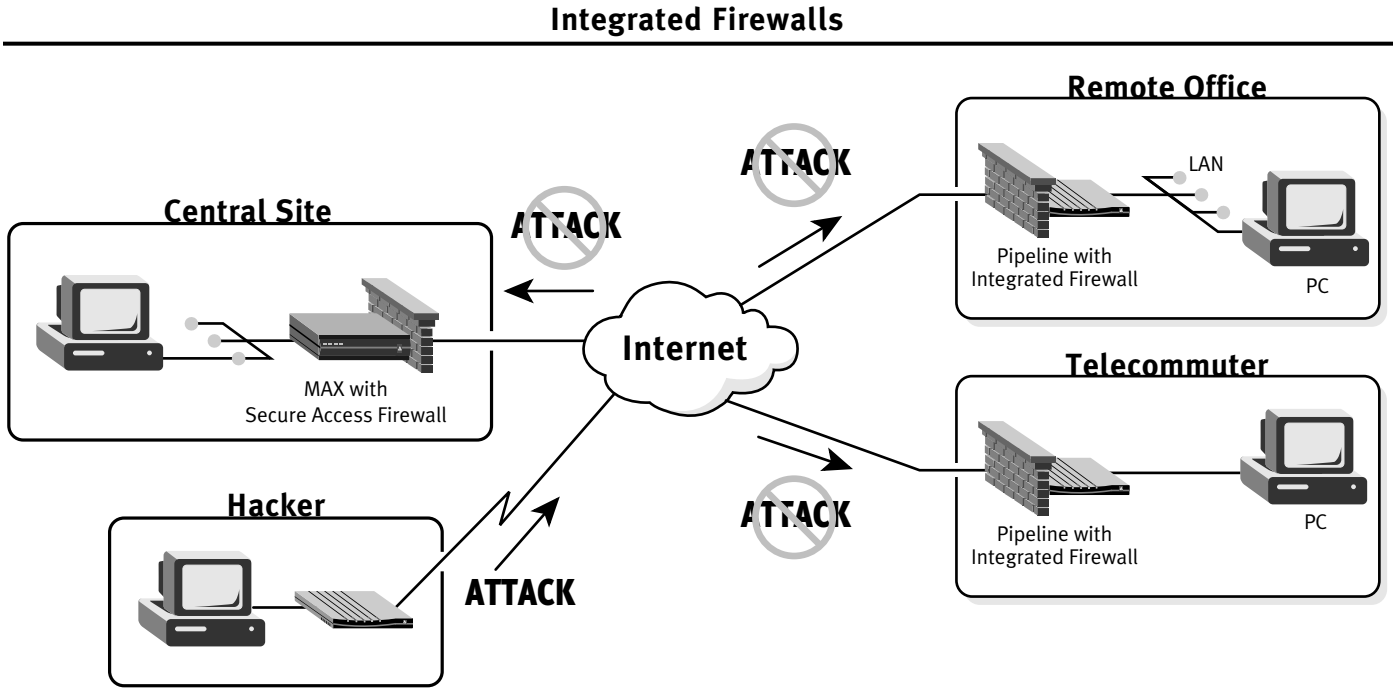


Figure 25 – Integrated firewalls are a superior alternative to stand-alone firewalls. They are also inexpensive, so you can afford to install them to protect every remote site in your network.

Other benefits of integrated firewalls can be summarized as follows:

- Because the firewall is embedded in the router, both network and system router are protected against attacks.
- Integrated solutions run on unique operating systems, eliminating security "holes" and bugs inherent to common operating systems, which can be exploited by hackers to circumvent a stand-alone firewall.
- The router/firewall solution offers an economical package with a low initial investment since users do not need a dedicated workstation, custom software and separate router.
- Integrated solutions provide a lower cost of ownership since maintenance costs such as operating system upgrades and user training are eliminated or significantly reduced.
- A single-vendor solution reduces interoperability problems, reduces support costs and lightens the load on internal help desk resources.
- A single solution simplifies system management and configuration.

Perimeter Firewall Technologies

Basic Firewall Design Issues

- *Is your firewall stance open (everything is allowed that is not expressly prohibited) or closed (everything is prohibited that is not expressly allowed)?*
- *Does the firewall present any inconvenience to legitimate users?*
- *Does the firewall log attempted security breaches for potential action by administrators?*
- *If a hacker does break through the firewall, is the network wide open once he gets inside?*
- *Is it easy to detect if the firewall is compromised?*

There are two types of firewall technologies available today: static packet filtering and dynamic firewalls. Static packet filtering and dynamic firewalls can be implemented as either stand-alone devices or integrated into routers or remote access servers.

Static Packet Filtering

Static packet filters examine every packet passing through the network interface to see if it meets pre-established requirements about source and destination IP addresses. However, static packet filters do not monitor the "session state" — the real-time events involved in sending and receiving data during a TCP session.

Because they do not perform session state monitoring, static packet filtering limits your control and potentially places your network at risk. During an FTP session — since static packet filters don't know which port number a remote caller and an FTP server have negotiated for a file transfer — they keep open all the high-numbered ports from 1,024 to 65,535. This makes thousands of ports vulnerable to probing attacks from unauthorized users for the duration of the FTP session. If all the ports are open, intruders can break into your network. If all the ports are closed, even authorized users are prevented from entering the network.

Dynamic Firewalls

Dynamic firewalls are an intelligent, next-generation firewall technology that provides a more secure solution than static packet filters.

Dynamic firewalls give you more granular control over users entering the network because they use state-of-the-art technology to create dynamic rules and adapt them to changing network traffic in real time. These rules can be modified to accept or reject conditions depending on specifications such as applications, protocols, network addresses, session state or direction. Once a session has been initiated, dynamic firewalls monitor requests to open ports between terminating points. They open only designated ports and keep all other ports closed. When the session has ended, the ports are immediately closed, eliminating the potential for hackers to infiltrate the network and your company's sensitive data.

7. Management: Supporting Your Remote Access Network

A network management system keeps track of the activities on your network and keeps the components of your network in proper working order. It also can reduce downtime, improve user services and facilitate cost controls.

Remote networking introduces a new level of complexity to your network management task. With phone lines, users and equipment scattered hundreds or even thousands of kilometers away, there are more things that can go wrong. To make your job easier, use the same tools and procedures to manage your remote sites that you're already using to manage the network equipment and workstations at your central site.

How smoothly your remote network operates will depend primarily on how well you integrate your remote equipment into your existing network management system. It also depends on how well you train your remote users and how you plan to support them. The bulk of this chapter looks at how network management systems work and gives you some ideas about how to manage remote workers. A brief discussion of training and support issues follows.

Monitoring and Control

A network management system performs two main functions: monitoring and control.

Monitoring collects information about a network and its components —servers, routers, bridges, gateways, workstations and cables — and displays the information on a centralized network management system. Specific monitoring functions include:

- Fault monitoring, which identifies abnormal network conditions that require repair.
- Accounting monitoring, which tracks the use of network resources to determine how efficiently they are being used, and to charge back costs to different projects or departments.
- Performance monitoring, which pinpoints network congestion and collects such statistics as throughput, error levels response times and CPU utilization.

Control functions let managers modify network parameters and take specific action on different network components. Control functions include:

- Configuration management, which deals with such issues as configuring new hardware, updating drivers, setting and modifying attribute values, shutting down parts of the network, distributing software and performing database updates.
- Security management, which provides encryption exchanges within the network management system itself and distributes encryption algorithms for devices on the network.

Network Management System Components

Together, the set of tools that perform these monitoring and control functions is called a "network management system." The tools are actually software programs that work together, collecting and compiling management information, displaying it and allowing IS staff to interpret it. All of the programs in a network management system should operate under a single, user-friendly interface, so staff can view the network as a unified architecture and perform management tasks from one central location.

There are five main components of a network management system: the system administrator, network managers, managed devices, agents and a management information base (MIB). Here's how they interoperate.

System administrator

A host-based or UNIX-based system that collects and compiles management information from different network managers and presents it on a single platform. The most commonly used system administrator packages are OpenView Management System from Hewlett-Packard, SystemView from IBM and SunNet Manager from Sun Microsystems, Inc.

Network managers

Software that communicates with agents in managed devices to gather information about their operation. The information is stored in a Management Information Base (MIB). Network managers can be vendor-specific, gathering detailed information about particular devices, or generic software that gathers information about multiple vendors' devices.

Management Information Base (MIB)

A database of information about all the manageable devices on the network. Information on each device is contained in what is called a "managed object" within the MIB. Information about managed objects include network protocol information, routes and other factors that relate to how a particular kind of device functions.

Managed devices

Devices on the network that are capable of being managed, such as routers, remote access servers, computers, hubs and switches.

Agents

Software modules implemented in network devices that require managing. Agents collect information about events that occur within the device such as the number of packets transmitted, and communicate that information to network managers. The information is stored in the MIB.

What Is SNMP?

The most commonly used protocol for network management (SNMP) is Simple Network Management Protocol, a standard that got its start within the Internet community in the late 1980s. Today, SNMP is in widespread use and is supported by almost every network device manufacturer in the industry.

SNMP links the device that is being managed with the network manager that is managing it. Here's how: Devices that are SNMP compatible contain agents that collect management information about the device and send that information to a MIB by means of the SNMP protocol. Network managers use the information in the MIB to report the status of the device to the system administrator. A system administrator collects management information from a number of vendors' network managers and presents it for viewing on a single management console.

If your remote access equipment vendor offers their own SNMP-compatible network manager, use it. It will give you a much greater degree of control over their remote access equipment than using a generic network manager designed to manage equipment from different vendors.

The SNMP Environment

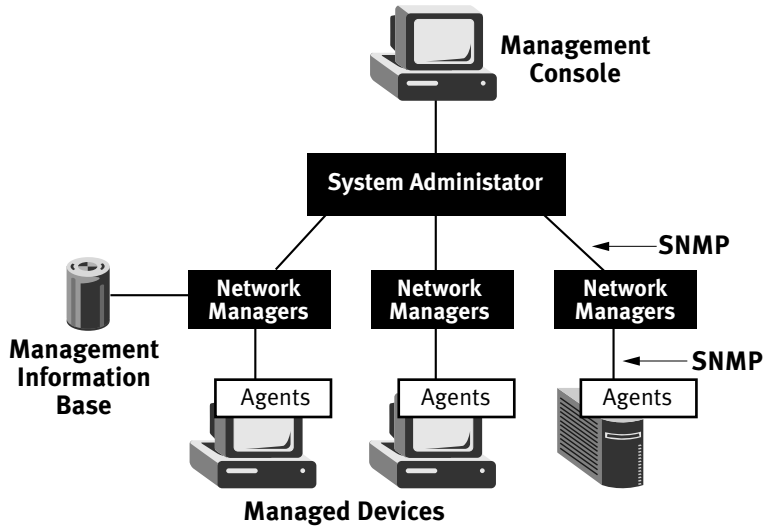


Figure 26 – Using SNMP, network managers collect information about managed devices and report their status to the system administrator

Management Features of Remote Access Equipment

Some remote access equipment contains special management features that give you greater control over the equipment. Check for these useful features before you make a buying decision.

Telnet

Part of the TCP/IP protocol, Telnet is a straightforward tool you can use in conjunction with your network management system to troubleshoot remote connections. Telnet works by establishing a "virtual terminal" session with remote site equipment over a wide area link. This allows you to remotely perform configuration, diagnostics and other control functions that otherwise would be performed by a locally attached terminal.

Call Detail Recording

This feature lets you record statistics about every call a device makes so you can pinpoint network bottlenecks and allocate costs to departments for billing purposes. With Call Detail Recording you can log statistics such as the date, time and duration of a call, the number called, and whether the call was incoming or outgoing.

Ping

A common way to identify an end-to-end connection is to send a "ping" packet from a management workstation at one end of a wide area link to a workstation at the other end. If the equipment and the network link are operational, the destination workstation will send back a "ping" to the originating workstation. "Pinging" is a particularly useful feature in remote networks, where traveling to a remote location to troubleshoot equipment may be impractical or nearly impossible.

Spoofing

Spoofing fools remote site and central site equipment into thinking a network connection is active even when it's not. It works by allowing equipment on each side of the connection to issue and respond to keep-alive messages without constantly keeping the network connection active to poll them. This eliminates the aggravation of re-establishing network connections constantly and saves money by establishing connections only when needed.

Training Your Remote Users

The importance of proper training for your remote users may seem obvious, but is frequently overlooked. According to "The Real Costs of Remote Access", a recent study by Infonetics Research, most remote users receive little or no formal training. Instead, they're left to learn by themselves through trial and error, or get quick, informal training in the basics from a co-worker — how to plug in a modem and use remote access client software.

Companies that provide little or no training to remote workers may incur large hidden costs. Self-learning is time consuming and learning from a coworker involves two people's time. Without adequate training, simple problems like an improper password sequence or missing printer driver may cause hours or even days of missed work.

Don't make the mistake of letting your remote workers train themselves. Provide training classes with an expert trainer that will get them up to speed on the hardware and software they need to use in the field. Then encourage them to call your help desk, where trained help desk personnel can provide quick response and expert advise about products. Finally, arrange for service contractors in the area where your remote sites are located. When your help desk can't solve a problem over the phone, local service contractors give your users someone to turn to for help.

Supporting Your Remote Users

Providing technical support to your remote users is just as important as training them.

At the start, budget plenty of IS staff time for setting up your branch offices, mobile workers and teleworkers. The majority of this time will be spent helping workers set up and configure their equipment. Allow some time for actually traveling to remote locations, in cases where there are a large number of remote users or where users experience problems that can't be solved over the phone.

Also budget staff time for setting up access equipment at your central site. Your new remote access server will need to be configured and tested, and new accounts, passwords and security files must be set up for your new users.

Ongoing support of your remote sites will take about 15 percent of your staff's time, according to figures compiled by Infonetics Research. A sizable portion of that time — 33 percent — will be spent installing and configuring equipment; another 46 percent will be spent troubleshooting and fixing problems.

Make sure that's enough. According to the Infonetics Research study, remote workers, themselves, spend three to seven hours on average a month of their own time, installing, configuring and problem solving their software and hardware. In the same month, IS staff only spend between 20 and 50 minutes supporting each teleworker or mobile user.

One way to cut down on support time — and expense — is to select equipment that is easy to set up and trouble-free to operate. When you're evaluating remote access equipment, check to make sure set up and configuration procedures are simple and that important functions are transparent to the user. Easy-to-use equipment will save time for your remote workers, and your staff, too.

Finally, expect to restructure your support program somewhat to accommodate your new remote access network. Extend your help desk hours, if you need to, or reschedule personnel to support users working after hours or in different time zones. Train your staff thoroughly on the new access equipment remote users are installing and set up procedures for supporting remote users. Also consider what new support issues you might encounter, such as traveling professionals in hotel rooms who must to access your network through different types of PBX equipment.

8. Leveraging the Internet

Is your company using the Internet only for web-based marketing? If so, consider just a few of the Internet's other potential corporate uses:

- *supporting customers via the web*
- *exchanging internal and external e-mail*
- *sending faxes long-distance with local calls*
- *performing market and engineering research*
- *receiving news and other timely information*
- *training and distance learning with IP multicast*
- *buying and selling products with electronic commerce*
- *collaborating with strategic partners and outside project teams*
- *implementing an Internet-based virtual private network*

The Internet may be the only network your organization will ever need. While this might appear at first to be somewhat of an exaggeration, industry analysts are touting the Internet as a solution for all wide area communications. And many companies are indeed beginning to use the Internet for an expanding array of applications. Its strategic importance is why the Internet is considered one of the fundamental building blocks of corporate remote networking.

Most organizations already recognize the unprecedented marketing potential of the Internet's World Wide Web. It seems that every company, government agency, library, university, TV and radio station, magazine–virtually every institution–now has a web site on the Internet. But the Internet is much more than just a backbone for the web, and few organizations have yet to utilize its full potential or the value-added capabilities of Network Service Providers (NSPs)—companies that provide Internet access such as local and national carriers, Internet Service Providers, Competitive Local Exchange Carriers and Competitive Access Providers.

The Internet and NSPs are becoming strategic for most businesses. Over time, a growing percentage of private applications will leverage the Internet's ever-expanding capacity and reach, and NSPs will play more of a critical role in commercial accounts.

There is certain to be a broader role in your organization for the Internet and your NSP. In the not too distant future many companies will achieve the ultimate use of the Internet: an enterprise-wide Virtual Private Network (VPN). When the majority of an organization's users are connected to the Internet, a full-fledged VPN is within reach.

Virtual Private Networks: The Ultimate Corporate Internet Application

A VPN is a private network that uses a public network, in this case the Internet, as the infrastructure for all communications. It is "virtual" because the VPN appears to the user organization as a genuine private network, with exclusive use of resources, even though all traffic is traversing public facilities. Why use the Internet? It is the most widely available, least expensive "public data network" in the world. There are currently some 30 million users, and its global presence is growing at a whopping 15% per month.

The forces driving this inevitable migration to VPNs include the:

- High cost of operating private networks
- Increasingly mobile and disperse workforce
- Need to interact "on-line" with customers and suppliers
- Desire to consolidate and simplify the user interface to networked applications

Virtual Private Networking: In Concept

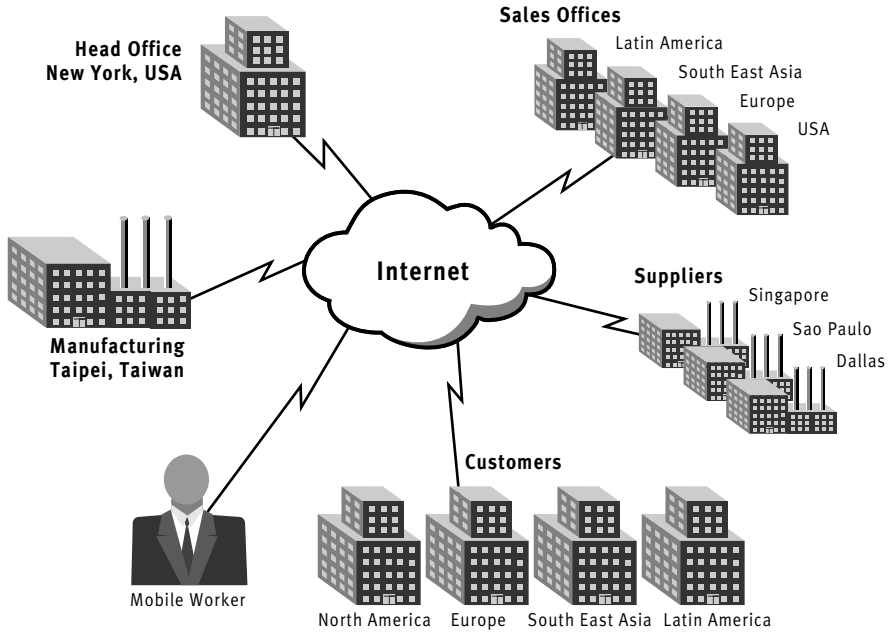


Figure 27 – An Internet-based VPN can be a cost-effective complement to the private network for many internal communications needs.

VPNs Offer Many Benefits

Companies report savings of up to 60% by using Internet-based VPNs in place of private networks. The Internet's two key advantages for enterprise networks are its low cost and worldwide presence. Add to this its flexibility and dependability, and the Internet becomes eminently qualified for mission-critical applications.

Internet-based virtual private networks can:

- Replace all or part of an existing private network
- Supplement the private network by meeting backup/overflow needs, or by offloading certain applications to free bandwidth
- Add new locations, especially international sites, to the existing enterprise network
- Handle new applications without disturbing the existing private network

VPNs Requirements

Virtual private networks based on the Internet have several fundamental requirements, including:

- Support for the Internet Protocol (IP) and IPX gateways
- Dynamic firewall protection
- Tunneling capabilities
- Support for encryption
- A user and security management system

An Internet-based VPN offers three compelling advantages:

A savings of up to 60% over equivalent private networks

- *Eliminate long-distance leased lines (including alternate "mesh" paths)*
- *Eliminate long-distance switched calls (PSTN or ISDN)*
- *Pay only for actual usage with no idle lines or wasted Frame Relay commitments*
- *Use less equipment with the same 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 NSPs in nearly every city*
- *Mesh redundancy and fault tolerance*
- *User familiarity*

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 28.8 Kbps to T1/E1 speeds and beyond*

Applications that use registered IP addresses can operate via the Internet, as is, with the addition adequate security measures. For non-IP or "private IP" applications, a company has three choices:

a. convert the application to IP, an endeavor that is usually easier said than done

b. make use of special gateways that convert other protocols to IP

c. 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 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 best choice is tunneling, which works with the widest variety of client/server and legacy applications. Many NSPs can now even offer a fully outsourced VPN solution, which requires no special customer premises equipment or other investment.

Security, the other requirement for VPNs, puts the private in virtual private networks. The Internet itself is a public network with minimal security provisions. So there is legitimate concern that private information could be accessed while in transit or directly from servers/hosts.

Fortunately, security measures are readily available to keep transmitted data strictly confidential and to prevent unauthorized access of sensitive information. Confidentiality is added through one of many encryption techniques. Individual users can be screened with a variety of authentication and authorization protocols. And network-attached resources are protected by firewalls. Together, encryption, authentication, authorization and firewalls make VPNs truly private for mission-critical internal communications.

VPNs Are Suitable for Many Applications

Applications that make good VPN candidates meet at least one of the following three criteria; the best meet all three:

- high number of users and/or sites
- widespread locations involving long distances, nationally or internationally
- relatively modest bandwidth and latency requirements

Here is a list of applications that often make sense for a VPN:

- local, regional or nationwide remote access and telecommuting programs
- communications with field sales/support personnel
- a comprehensive internetwork of branch and regional offices
- distribution of software/data updates, or performing backups at remote locations
- collaborative work using Internet Relay Chat or shared whiteboard applications
- distance learning, training and other "broadcast" applications using multicast
- extending a local intranet nationwide or worldwide
- adding new remote users and/or applications

Tunneling: Making the Virtual Paths in Virtual Private Networks

- *Proven technology that is now being applied to Internet-based VPNs*
- *Unnecessary for VPNs with registered IP addresses*
- *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*
- *Generic Routing Encapsulation (GRE) as defined in RFCs 1701/1702 supports a wide variety of popular protocols*
- *The Point-to-Point Tunneling Protocol (PPTP) works with Windows NT and NetWare servers*
- *The Layer 2 Tunneling Protocol (L2TP) will add certain PPTP features to Layer 2 Forwarding (L2F) in a new standard*
- *The Ascend Tunnel Management Protocol (ATMP), supporting both GRE and PPTP, can be used for "private IP" (unregistered addresses), IPX and NetBIOS/NetBEUI applications*
- *Mobile IP can be used to tunnel IP within IP for mobile workers*
- *Data Link Switching (DLSw) can be used to encapsulate SNA protocols*

There is no longer any reason to postpone the inevitable. The future of enterprise networks is here today with VPNs.

Internet Access for the Entire Corporation

The equipment used for accessing the Internet is often identical to that used for all other corporate remote networking applications. The reason is that most NSPs use the very same public wide area network and similar systems to support their subscribers. Sometimes the only difference between a private corporate remote access network and an NSP network is the applications software.

Nevertheless, there are certain product features that may be relevant or more important when accessing the Internet via an NSP. Selecting the optimal equipment for the entire corporation requires considering at least three separate situations: the individual user, the remote office and the major facility.

Individual Users

Individual users embody mobile workers and telecommuters. Mobile workers generally use analog or cellular modems to have access anywhere in the world via the public switched telephone network (PSTN). Telecommuters are "tethered" at home offices and, therefore, are better served by digital equipment and services (see Chapter 4 for a detailed discussion of the home office integrated access device, which provides a complete data, voice and fax communications solution on a single line).

To access the Internet, individual users need a TCP/IP protocol stack and certain applications, such as an e-mail package and a web browser. Suites of such software are bundled with Windows and other workstation operating systems; alternatives are available from a number of vendors. For accessing the Internet, most NSPs use a password to prevent "free" or otherwise unauthorized access. If your organization is using the Internet for a VPN, be certain to have your NSP(s) enforce strict user authentication, and select user access equipment with integral firewall protection.

Remote Offices

Remote offices typically involve relatively small workgroups, and there are a number of equipment alternatives for Internet access. The two traditional approaches involve individual analog modems at each user's desk, or a shared modem bank, which is often integrated with the local server. The problem with both of these approaches is the analog modem: modems are expensive, provide marginal performance, require separate phone lines, pose security risks and are difficult, if not impossible, to manage remotely.

Analog modem problems and limitations are causing many organizations to turn to the Integrated Services Digital Network (ISDN). Because ISDN is digital, it offers higher throughput and instantaneous connections, both of which are major advantages for remote office Internet access. ISDN equipment comes in two basic flavors: a terminal adapter or a remote access router. Many ISDN terminal adapters are network interface cards (NICs) that plug directly into the local server. The solution is often quite inexpensive and easy to support, which are beneficial when numerous remote offices are involved.

VPNs and the Enterprise

In any enterprise VPN, the headquarters, each division, all branch and regional offices, and every individual telecommuter and mobile worker has a link to a local NSP. Everyone can communicate with everyone else, whether in a true intranet, which uses IP-based applications such as web servers and browsers, or with other applications using IP tunneling. Local connections to local NSPs–leased lines, Frame Relay or dial-up–eliminate all long-distance charges. Why load up the private network with intranet traffic, for example, when the Internet will serve just as well, if not better? Indeed, a unified intranet/Internet may be the ultimate corporate network from a user's perspective.

VPNs are normally used to complement private networks, either by adding new sites or applications, or by replacing a portion of the private network. A particularly expensive or troublesome segment of an existing private network is an ideal candidate for a VPN pilot. If part of your network is causing most of your headaches, you have little to lose by at least discussing the options with your NSP. The NSP's rich experience with Internet technology make it an excellent resource for implementing VPNs, including intranets.

For slightly more money, the remote access router provides much more robust capabilities in an easy to install and manage standalone box that attaches to the remote office LAN. Because it does not depend on the local server, the ISDN remote access router eliminates configuration complexities, consumes no server resources and can be managed remotely because it is always on-line. One of the most desirable features in a remote access router is integrate dynamic firewall protection. Dynamic firewalls isolate all resources on the enterprise-wide network from unauthorized access by hackers.

To get the most from ISDN's Basic Rate Interface (BRI) service, select a terminal adapter or remote access router with bandwidth on demand and data compression. These two features combine to deliver the needed performance, from 64 Kbps to 512 Kbps, while minimizing connect times and service fees.

A new alternative to ISDN for remote offices is the ISDN Digital Subscriber Line (IDSL). IDSL, an Ascend innovation, offers the same 128 Kbps throughput (512 Kbps with compression), and is compatible with existing ISDN terminal adapters and remote access routers. The major difference is that IDSL provides a constant connection, much like a leased line, rather than a dial-up link. As a result, IDSL may be less expensive than ISDN. Check with your NSP for availability and pricing.

For software, each user must have a TCP/IP protocol stack, along with an e-mail interface and a web browser. Alternatively, a special gateway application can be added to the remote office server. The gateway converts the server's Network Operating System (NOS) protocol–such as IPX or NetBEUI–to IP. The gateway normally includes Internet-compatible applications that run on the server or on the individual clients.

Major Facilities

Major facilities include the headquarters and all divisions. Each has a large number of users, and some may be web sites. As such, Internet access should be considered mission-critical. Employees need passage to the wealth of Internet resources; telecommuters and mobile workers want remote access via the Internet-based VPN; and your web site is visited 24 hours a day by customers and prospects around the globe.

Businesses with steady inbound/outbound Internet traffic can benefit by having a dedicated line to the NSP's point-of-presence (POP). A full T1/E1 line, operating at 1.5 Mbps, can support several dozen concurrent Internet sessions in most organizations–which translates to hundreds of users. Even a fractional T1 line, or a Frame Relay link operating at 56 Kbps or higher, can keep access to the web server open around the clock.

But a single line, regardless of its speed, is risky. Dedicated lines, while ideal for mission-critical applications, regularly become overloaded and can go out of service at any time. Supplemental dial-up bandwidth can handle either situation. A single dial-up ISDN BRI line with compression provides 512 Kbps throughput–enough to handle an overload situation or maintain Internet access until the primary link comes back on-line.

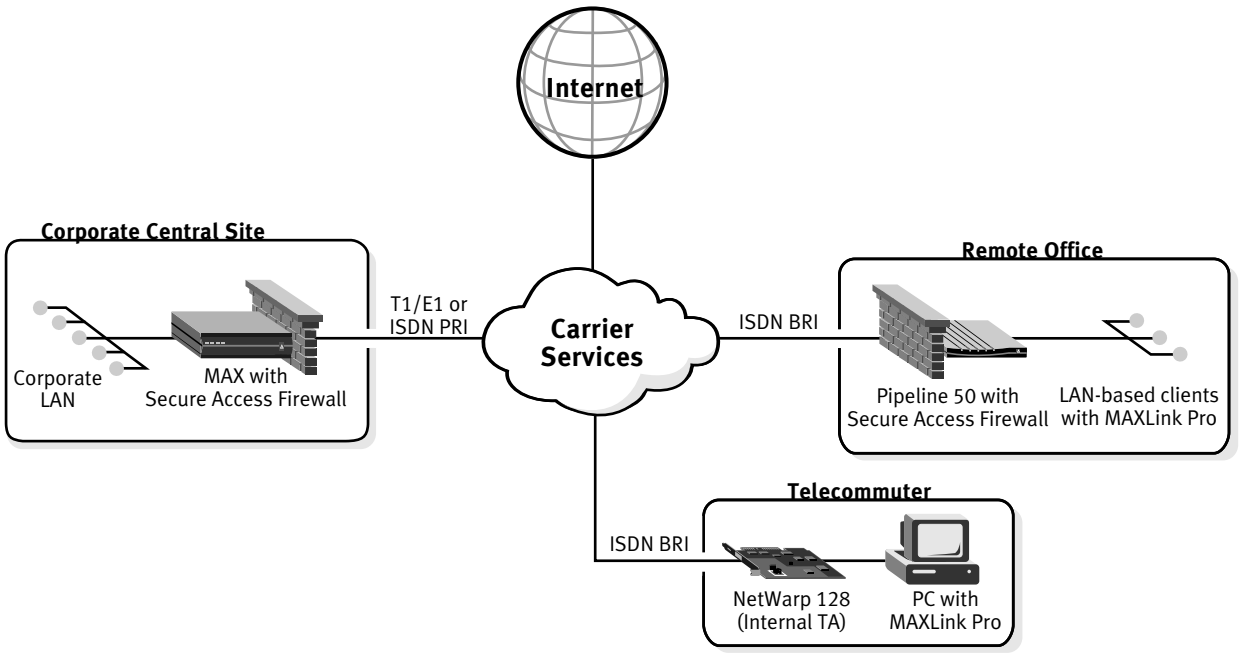


Figure 28 – ISDN provides an effective and high speed method for remote offices to access the Internet.

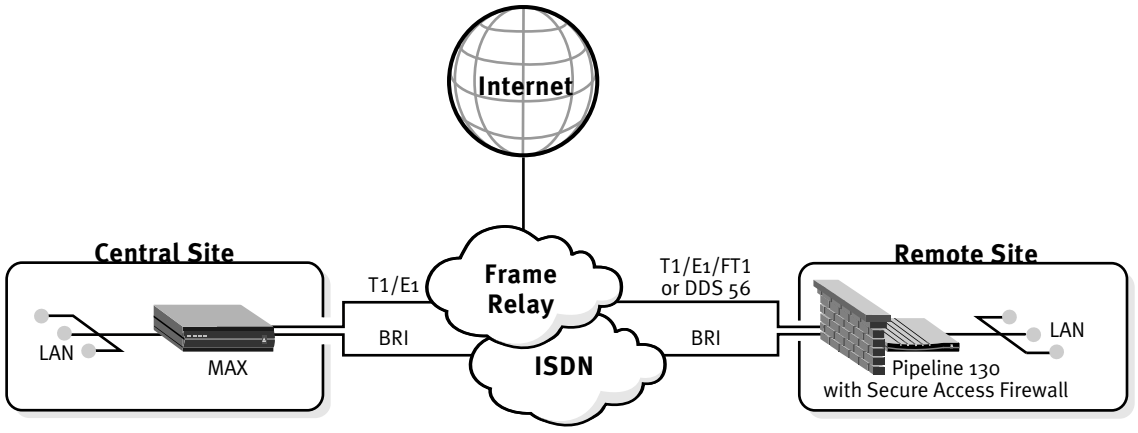


Figure 29 – The dual-WAN remote access router offers the high throughput and availability needed by major facilities.

Here is a checklist of basic requirements that should be included in your Internet access equipment:

- ✓ *capability and capacity to handle all Internet and VPN needs*
- ✓ *bandwidth on demand and data compression to minimize service fees and lower the cost of ownership*
- ✓ *Ethernet LAN connectivity or plug-in NIC for simple integration and seamless application interoperability*
- ✓ *ability of all office users to share available bandwidth automatically and transparently*
- ✓ *compatibility with the local NSP's equipment for optimum performance*
- ✓ *standards-based management (local and remote) and accounting*
- ✓ *integral dynamic firewall security to prevent unauthorized access and protect all network-attached resources*
- ✓ *built-in CSU/DSU or ISDN NT-1 adapter, as required by the carrier, eliminates the need to purchase and install separate units*

The best solution is a LAN-attached remote access router with both primary and secondary WAN ports. The dual-WAN router should automatically and transparently add the supplemental dial-up ISDN bandwidth when the dedicated primary link is saturated or goes down. The router should also automatically terminate the ISDN call when, in either situation, the supplemental bandwidth is no longer needed. No on-duty attendant should be required once the system has been configured for the desired operation.

If your organization does *not* have a VPN for remote office internetworking and remote access by telecommuters and mobile workers, then the major facility should be considered a "central site" and equipped with a more capable WAN access switch. The multi-port WAN access switch has ample capacity to provide the dial-up bandwidth for web site or other backup and overflow needs. Whether a major facility with a remote access router or a central site with a WAN access switch, be certain to select equipment with integrated dynamic firewall protection.

Software requirements for the major facility are identical to that of the remote office, albeit on a much larger scale. The only difference may be that the server is actually a midrange or mainframe host computer.

Selecting a Network Service Provider

Selecting a Network Service Provider (NSP) is the most critical Internet-related decision. Whether your organization wants to use a national NSP or multiple local ones, consider each to be a strategic partner. Here is a checklist of considerations for selecting the best possible NSP(s). It is a rather long list, and some points may be relatively unimportant or irrelevant, but be sure to evaluate thoroughly all NSP candidates.

Considerations for choosing an NSP include:

- support for the full spectrum of WAN options (analog modems, cellular, ISDN, Frame Relay, SW56, T1/E1/PRI, X.25 and DSL)
- Multilink Protocol Plus™ (MP+) advanced dynamic bandwidth management (for backup and overflow needs, along with 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 and lower the cost of ownership)
- digital modem technology for improved link reliability and support of an open architecture for the latest in 56 Kbps analog modem technology
- standards-based tunneling for VPNs
- adequate security provisions, including encryption and authentication for VPNs
- support for Internet Group Management Protocol (IGMP) for multicast
- fax distribution capabilities
- call detail reporting to track usage by all users
- high-speed backhaul links to the Internet backbone for good performance
- redundancy to assure adequate up-time for mission-critical needs
- ability to help support remote users/offices directly
- web outsourcing of the server itself and/or content design
- POP locations everywhere needed to assure local access calls
- pricing structure, including monthly fees and additional usage charges

Outsourcing to Your NSP

Many organizations outsource their web presence to an NSP. The NSP achieves many economies of scale that make web outsourcing a less expensive alternative for businesses, for the same or better results. By having your NSP handle web content design, about the only thing you will need to do is download the "raw" material. And you even get to control your web page style by instructing the NSP how you want it to look and work. Designing user-friendly web pages takes special talent. That talent is expensive for a single organization to maintain.

But most NSPs offer much more than just web-related services. Many NSPs offer assistance managing the Internet connection, including equipment at your central and/or remote sites. Your NSP may be able to handle any or all of the following tasks: equipment installation, configuration and upgrades; IP address administration; firewall and other security management; network monitoring, troubleshooting and performance tuning; usage accounting; user help desk; carrier relationships; etc.

Most NSPs can provide valuable consulting services for Internet or intranet applications. NSPs can help select the most appropriate client/server software, recommend suitable access equipment that optimizes your connections to their equipment, prescribe gateways to interface legacy applications to the Internet, integrate an intranet with the private network, resolve IP addressing issues, offer advice on improving performance, train users, etc. Your NSP may have the answers to many of your perplexing problems.

An increasingly popular option is to outsource substantial portions of a remote access or virtual private network, including all user equipment, to NSPs. Under an outsourcing arrangement, a capable NSP can literally handle everything, end-to-end, for one monthly fee. There is only one call to place to add a new node, report a problem or change subscription options. Considering the cost of maintaining in-house expertise and the relentless changes in technology, outsourcing is often less expensive in the long haul.

And who better to handle the task than your existing Internet partner, your NSP.

Appendix A: Real-World Remote Networking: Case Studies

Application

- *Sales staff and engineers need access to computer resources from hotel rooms and home offices*

Current Approach

- *A few engineers with home offices use modems to connect to the corporate LAN*

The Need

- *High-speed connections for engineers*
- *High-level security features that protect corporate resources*
- *Platform that supports both analog and digital users*
- *Equipment that can be deployed in countries throughout Europe*

By now, you have all the information you need to start drawing up your remote networking plan. You've learned about access lines, discovered the pros and cons of certain types of remote access equipment, and understand the need for building strict, standards-based security and management mechanisms into your new remote network.

Before you proceed with your plan, take a few minutes to read through the following case studies. They describe actual remote access networks that are in operation today and the thinking that went into building them. The examples range from a simple remote network with 20 telecommuters to a very large-scale implementation that handles calls from thousands of remote users each day. Each case study uses products from Ascend Communications, the worldwide leader in remote networking solutions.

Case Study Number 1: *Computer Workstation Manufacturer Extends Network Resources To Traveling Sales Staff and Teleworkers*

Case Study Number 2: *Australian VAN Supplier Reduces Call Center Costs Through Teleworking*

Case Study Number 3: *Internet Service Provider Supports Analog and Digital Callers*

Case Study Number 1 Computer Workstation Manufacturer Extends Network Resources to Traveling Sales Staff and Teleworkers

Ascend Equipment

- *Pipeline 75 products in engineers' home offices*
- *A MAX product at the company's central site handles all telecommuting traffic*

The Benefits

- *Support for both analog and ISDN now; open architecture makes migration to an all-digital environment easy*
- *Remote access equipment can be integrated into the existing network management platform; remote management capabilities save time and expense*
- *Pipeline 75 products provide superior high-speed performance and eliminate hefty installation fees and monthly access charges*
- *Perimeter firewalls integrated into the MAX 200Plus and the Pipeline 75 thwart hacking attempts at the very edge of the network*

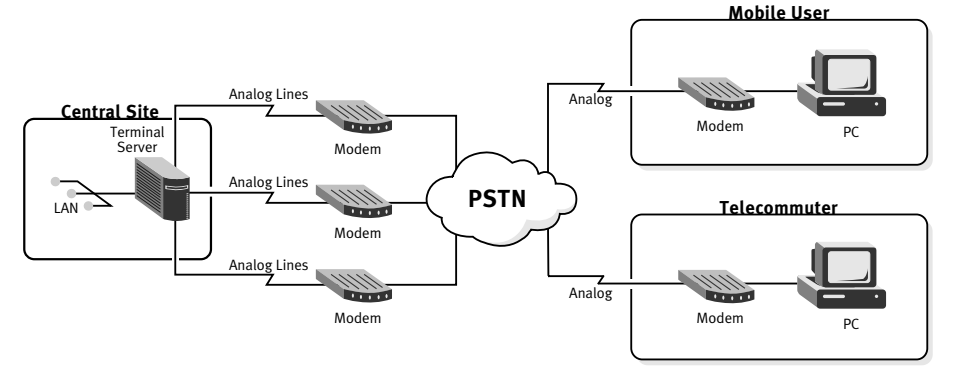
Background

In an effort to improve productivity and cut costs, managers at this multinational computer workstation manufacturer decide to implement a teleworking program at one of their small European offices. The new program must give traveling salesmen access to corporate resources from home and the road. It also must give engineers around-the-clock access to the network so they can work evenings and weekends from home offices.

Laptop computers with V.34 modems provide adequate performance to most members of the sales force, who mainly use the network to download e-mail and sales orders, and frequently need network access from hotel rooms over analog lines.

Engineers, who use powerful UNIX workstations at home, decide they need high-performance ISDN connections to quickly download large CAD/CAM files and manipulate other bandwidth-intensive applications.

Before



The Solution

To accommodate the needs of both its sales and engineering staff, the company needs a remote access solution that supports both analog and ISDN callers on a single platform. The solution must provide high-level security and offer remote management via SNMP.

Application:

- *A value-added network supplier maintains a 1-800 customer support number and a staff of trained customer service representatives (CSRs).*

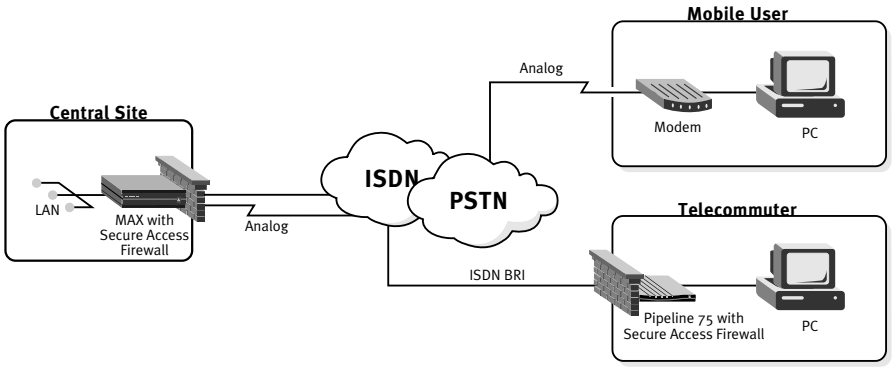
Current Approach:

- *The company hires enough full-time CSRs so that callers never have to wait too long on hold, even during peak calling periods.*

The Need:

- *Telecommuting platform that can extend customers' 1-800 calls over wide area network phone lines to CSRs working at home*
- *High-speed, end-to-end solution that is secure and manageable*
- *Home office equipment that is easy to use without on-site IS support*

The Ascend Solution



How It Works

The workstation manufacturer selects a MAX 200Plus as its remote access server. The decision is based on the flexibility of the platform, as well its security features and standards-based management capabilities.

The MAX 200Plus can handle up to eight simultaneous calls over four ISDN BRI access lines. A combination of low-cost, off-the-shelf PCMCIA modem cards and PCMCIA ISDN cards allow the MAX 200Plus to answer calls from both sales staff with modems and engineers with Pipeline 75 products. Since the unit is based on an open architecture, it can easily accommodate a shift in the number of analog and digital callers simply by swapping out PCMCIA cards.

The company decides to install Pipeline 75 routers at its engineers' homes. Pipeline 75 products save money on access line charges because they let engineers share the bandwidth of a single ISDN BRI line with a computer and any two analog devices such as phones, fax machines or modems. It also provides them with lightening-fast connections to the corporate LAN at speeds up to 512 Kbps, with compression. Built-in remote management features of the Pipeline 75 let network managers set up, configure and manage the unit directly from the central site.

To maintain network security, the company equips its MAX 200Plus with Secure Access™ Firewall, dynamic firewall software that keeps unauthorized users from gaining access to the network. The company also installs Secure Access Firewall software on its Pipeline 75 products so that hackers can't invade engineers' UNIX workstations and piggyback onto their traffic.

As teleworking expands to other offices, the same equipment configuration can be used. All of Ascend's equipment conforms to North American, European and Asian standards, supporting deployment worldwide.

Case Study Number 2 Australian VAN Supplier Reduces Call Center Costs Through Teleworking

Ascend Equipment

- *A MAX product at the downtown call center supports data calls from telecommuters over an ISDN PRI circuit*
- *Pipeline products allow telecommuters to receive 1-800 calls and access the company's customer database over the same ISDN BRI line*

The Benefits

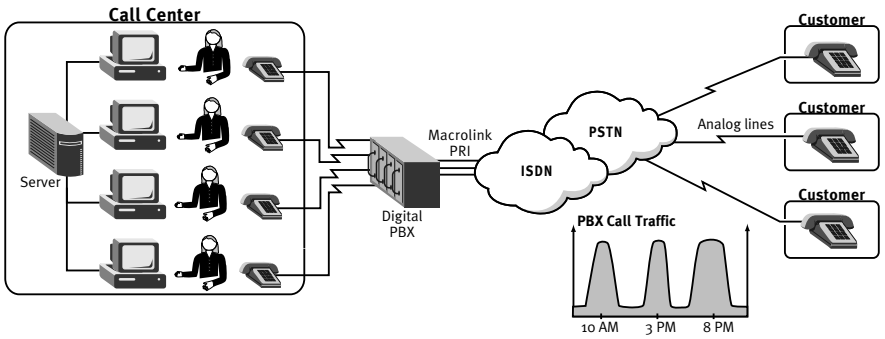
- *Provides an end-to-end digital solution that is manageable and secure*
- *Saves money on access lines, since the Pipeline products handle both analog and digital calls*
- *Gives CSRs nearly the same database response time they experience in the call center*
- *Eliminates the need for CSRs to use costly digital handsets*

Background

A value-added network supplier employs 50 customer service representatives (CSRs) in a downtown call center to answer 1-800 calls from customers. An Automatic Call Distributor (ACD), special software that is part of the company's PBX (also called a PABX in Europe and some Pacific Rim countries), places the calls on hold until a CSR becomes free and evenly distributes calls among available CSRs.

The call center receives the majority of its calls at three peak periods of the day. During these peaks, all 50 of the company's CSRs are continually busy answering calls and customers may be on hold for up to a minute. Throughout the rest of the day, the volume of calls drops dramatically and CSRs may sit for several minutes without receiving a single phone call.

Before



The Solution

Paying full-time CSRs to sit idle time during part of their shift is putting a strain on the call center's budget. So managers devise a plan that cuts back full-time staff at the call center to 30, a level sufficient to handle calls during off-peak hours. During peak hours, an additional 20 CSRs are hired to work split shifts from offices in their homes.

To implement the new plan, the company needs equipment that lets CSRs at home answer the 1-800 number and query the customer database, at the same time. The equipment also has to:

- Give CSRs database response times close to the response times they experience when working in the call center.
- Work with regular analog phones, instead of the costly digital headsets used in the call center.
- Keep charges for the CSRs' business lines completely separate from the charges for their personal phone line.
- Provide trouble free set up and operation, so that CSRs can use the equipment without on-site help from IS staff.

Application

- *Support analog, ISDN, leased access to Internet*

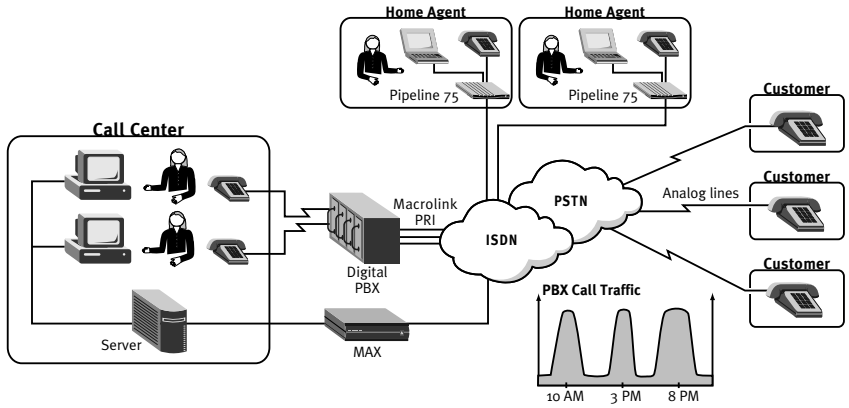
Current Approach

- *Modem pools, terminal adapters, routers, terminal servers*
- *Multiple authentication schemes*

The Need

- *Access server with security features that accepts calls over analog, ISDN and leased services*
- *Equipment for unmanned POPs managed with SNMP*

The Ascend Solution



How It Works

The company chooses an end-to-end digital remote networking equipment solution from Ascend because it meets all of these requirements, and then some.

The solution is based on the MAX 2000, remote access servers powerful enough to handle traffic from 20 teleworking CSRs who are on-line to the corporate LAN almost continuously during their shifts. A MAX 2000 can support 24 simultaneous calls from analog, ISDN and Frame Relay users over a single ISDN PRI line.

At each CSR's home, Pipeline 75 products let users set up simultaneous voice and data connections over a single ISDN BRI connection.

The Pipeline 75 is ideally suited to the company's teleworking application. It cuts down on monthly line charges and provides a single point of contact for management and security. Also it is extremely easy to use. CSRs simply plug their regular analog phone into one of analog ports on the Pipeline 75 and their computer into the unit's Ethernet port — and they're ready to answer customer calls.

One B-channel of the ISDN line handles the voice conversation between the CSR and the customer. The other B-channel connects the CSR at 64 Kbps to the customer's database record on the corporate LAN. The whole operation is transparent to both the ACD managing the call and to the caller, who can't tell if a CSR in the call center or at home.

The telecommuting program is a real success. The company has reduced its payroll expenses, while maintaining a high level of customer service. Employees benefit from telecommuting, too. CSRs are saved the stress of commuting downtown and enjoy flexible work hours that accommodate childcare responsibilities or part-time school schedules.

Case Study Number 3

Internet Service Provider Supports Analog and Digital Callers

Ascend Equipment

- *MAX supports analog, ISDN, T1/E1-R2, Frame Relay, and xDSL services for Internet access*
- *RADIUS authentication and accounting protocol*

The Benefits

- *Digital modems support analog subscribers; allow for smooth migration as users move to ISDN*
- *Channelized T1/E1 capability supports leased line connections*
- *Connects to both Ethernet and Frame Relay backbones*
- *RADIUS lets ISPs maintain centralized security profiles for thousands of users across large networks*

Background

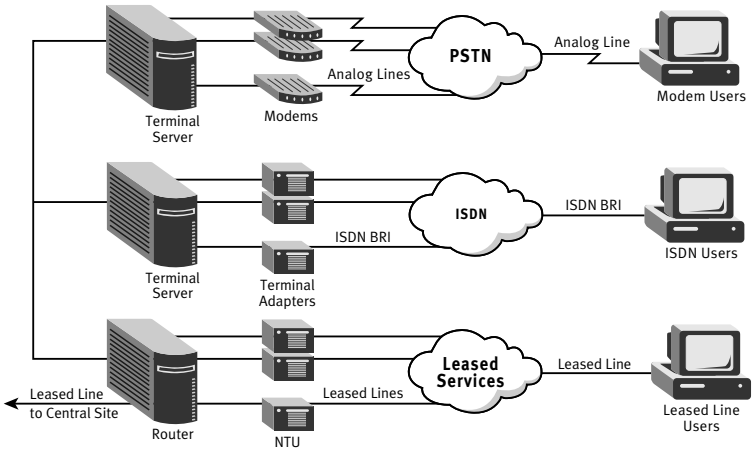
To keep up with the Internet's exploding popularity and accommodate thousands of new users each month that are jamming the information super highway, Internet Service Providers (ISPs) are expanding their service offerings and beefing up their network infrastructures.

As part of their expansion plans, ISPs are constructing new network access points in large metropolitan areas across the country that let subscribers connect to the Internet with a local phone call.

The access points, called Points of Presence (POPs), must accommodate subscribers with a variety of different Internet access methods. The most widely used access methods are still analog modems and 64 Kbps leased lines. With corporate customers, Frame Relay and ISDN Internet access are also becoming increasingly popular.

To support these different access methods, many POPs are crowded with a mixture of hard-to-manage access equipment and separate access lines. Analog access requires dozens of terminal servers and hundreds of analog lines and modems. ISDN access involves multiple ISDN BRI access lines and terminal servers and different types of terminal adapters. Leased lines require another solution — dedicated ports on large routers, which are connected to the ISP's network over FT1/T1 lines.

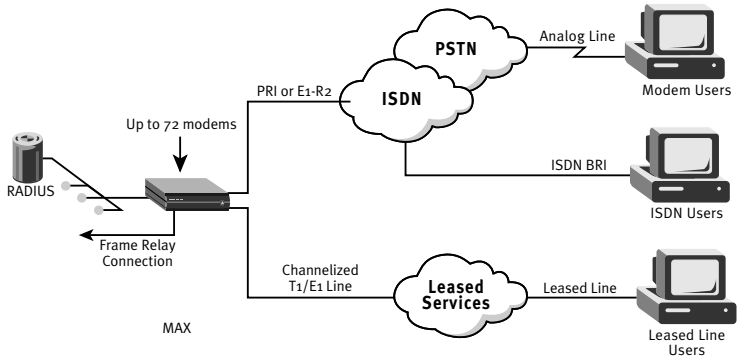
Before



The Solution

To simplify support for the growing number of subscribers and types of access methods, leading ISPs worldwide are installing MAX products in their POPs. The MAX supports analog, ISDN, Frame Relay, leased line and now the latest xDSL services in a single box that only occupies a small amount of rack space. This eliminates the need for separate modem banks, DSUs and ISDN terminal adapters, and the management headaches that go along with them.

The Ascend Solution



How It Works

The MAX 4002 and 4004 (MAX 4000 outside North America) provide an ideal solution for Internet access. Digital modems in the MAX can handle calls from analog callers at speeds up to 33.6 Kbps. Support for ISDN, Frame Relay, leased lines and xDSL also comes built into the equipment.

The MAX connects to a router on the ISP's network through an Ethernet port or over a high-speed serial interface that allows the MAX to send traffic over a Frame Relay backbone network at speeds up to 8 Mbps.

The MAX also supports RADIUS authentication servers, allowing ISPs to customize security methods to fit their own service needs and standardize them across their entire network.

Appendix B: Ascend's Remote Networking Products

Ascend Communications is a leading, worldwide provider of remote networking solutions for corporate central sites, Internet service providers, remote offices, mobile workers and telecommuters. Over 75 percent of remote networks around the world use Ascend's award-winning remote networking products to link branch offices, telecommute, surf the Internet, transmit video and perform hundreds of other remote networking tasks.

Ascend's product families – GRF, MAX including the MAX TNT, Pipeline, Multiband, NetWarp and security products including Secure Access Firewall and Access Control – provide a rock-solid, end-to-end foundation for remote networking, at the same time addressing your urgent needs for scalability, manageability and security.

The GRF Product Family

The GRF™ family of high-performance IP switches are cost-effective Layer-3 switches designed especially for demanding Points of Presence and backbone networking environments. The GRF's unique architecture combines switching with IP Forwarding Media Cards to deliver scalable performance up to 10 million packets per second. Depending on the system, the GRF can hold up to 16 media cards providing as much as 16 Gb/s of bandwidth for high-powered NAP, backbone and MegaPOP™ applications.

GRF 400 – provides 4 Gb/s to process 2.8 million pps and support as many as four IP Forwarding Media Cards.

GRF 1600 – supports up to 16 IP Forwarding Media Cards with 16 Gb/s of bandwidth and forwards up to 10 million pps.

The MAX Product Family

Ascend's MAX products are powerful remote access servers that let corporations build remote networks of any size, from any combination of analog and digital carrier services. MAX products combine the functionality of a WAN concentrator, a LAN access server, a router and a terminal server in a single box.

MAX TNT – integrates analog, ISDN PRI, BRI, T3, switched services, dedicated lines and Frame Relay; supports up to 150 T1/FT1/E1/FE1 Frame Relay connections and handles up to 672 simultaneous calls

MAX 4000 (outside North America only) – integrates support for analog, ISDN PRI, BRI, switched services, dedicated lines and Frame Relay over 4 E1/ISDN PRI access lines; supports up to 120 simultaneous calls

MAX 4002/4004 (North America only) – integrates support for analog, ISDN PRI, BRI, switched services, dedicated lines and Frame Relay over 4 T1/ISDN PRI access lines; supports up to 96 simultaneous calls

MAX 2000 – supports up to 24 analog/digital calls over a single T1/E1/ISDN PRI access line

MAX 1800 – supports up to 16 analog/digital calls over eight ISDN BRI lines

MAX 200Plus – uses PCMCIA technology; supports up to eight analog/ISDN calls over four ISDN BRI lines

The Pipeline Product Family

The Pipeline product family offers a full range of remote site access equipment including bridge/routers and ISDN integrated access devices. Pipeline products offer multiprotocol bridging and routing, inverse multiplexing and Dynamic Bandwidth Allocation.

Pipeline 25-*Fx* – a multiprotocol bridge which supports a small LAN with up to four computers over a single ISDN BRI line; contains one Ethernet port and two analog ports.

Pipeline 25-*Px* – an IP-only router for individual users that need ISDN BRI connectivity; uses a temporary IP addressing scheme.

Pipeline 50 – supports small offices and remote office LANs with multiple users over a single ISDN BRI line.

Pipeline 75 – supports small offices and remote office LANs with multiple users, contains an Ethernet port and two analog ports.

Pipeline 130 – dual-port, multiprotocol router that supports ISDN BRI, dedicated lines and Frame Relay at speeds ranging from 56 Kbps to T1.

The MultiDSL Family

Ascend's MultiDSL™ products offer the first integrated solution that lets service providers and corporations offer multiple xDSL services at speeds ranging from 128 Kbps to 6 Mbps. This turnkey solution includes both the Central Office Equipment (COE) and the Customer Premises Equipment (CPE) required for implementing DSL technologies immediately in a network. MultiDSL technologies use the existing copper telephone lines to support high-bandwidth applications such as remote access, Internet access and telecommuting.

ISDN DSL (IDSL) – modular cards that offer end-to-end IDSL solutions that let users transmit full duplex data at 128 Kbps and at distances up to 18,000 feet.

Symmetric DSL (SDSL) – modular cards that provide everything needed to transmit full duplex data to and from a central site or the Internet at speeds up to 768 Kbps and at distances up to 12,000 feet.

The Asymmetric DSL (ADSL) – modular cards that support for both Carrierless-Amplitude Phase (CAP) and Discrete Multi Tone (DMT); depending on the application and the type of ADSL, users can transmit data at speeds up to 640 Kbps on the downstream portion of the call and up to 6.14 Mbps on the upstream portion of the call.

The Netwarp Product Family

The Netwarp family of easy-to-use, high performance ISDN BRI terminal adapters gives telecommuters and remote users an affordable solution for connecting their stand-alone PC to high-speed ISDN services. Standard Plug-and-Play, as well as automatic switch protocol and line speed detection features, let users access the central site or the Internet in no time at all. When combined, these features allow even a novice PC user to complete installation quickly and easily without the frustration of manually entering protocol parameters.

NetWarp 128 – an ISA bus card that provides a cost-effective and easy to use solution for high speed, ISDN access to the Internet or a central site.

NetWarp Pro – an ISA bus card that lets telecommuters and small office/home office users integrate data, voice and fax communications over a single ISDN BRI line.

The Multiband Product Family

Multiband bandwidth-on-demand controllers are used for videoconferencing and other applications with fluctuating bandwidth needs such as backup and disaster recovery, distance learning and telemedicine. At their core is Ascend's industry-leading inverse multiplexing technology, a method of combining multiple switched channels into a single high-bandwidth data stream for speed as needed.

Multiband VSX BRI – a scalable inverse multiplexer that supports a single application over one to four ISDN BRI lines.

Multiband VSX T1 – a scalable inverse multiplexer that supports a single application at speeds ranging from 128 Kbps to T1/PRI.

Multiband Plus – an inverse multiplexer that supports multiple applications over two T1/PRI.

Multiband MAX – offers the most powerful Multiband solution and includes an inverse multiplexing card, SNMP management and the option to upgrade into a full MAX WAN access switch with support for extensive remote networking capabilities. The Multiband MAX family includes the 1800, 2000, 4002 and 4004.

Ascend's Security Architecture

Ascend's state-of-the-art, software-based security products work hand-in-hand with Ascend's MAX and Pipeline products to provide you with the most integrated, bullet-proof security solution the industry has to offer.

Secure Access Firewall – dynamic firewall technology available as a software option for the Pipeline 50, 75, 130 and the MAX family of products.

Secure Access Manager – a point-and-click Windows-based graphical user interface for configuring Secure Access Firewall, locally or remotely.

Access Control – a comprehensive authentication and authorization server based on industry-standard RADIUS that lets network administrators manage, control and secure analog as well as digital connections.

Appendix C: Remote Access Requirements Worksheet

Name: _____

Company: _____

Telephone Number: _____

The purpose of this worksheet is to help you determine your remote users' equipment needs. When you've finished filling out the worksheet you will be able to determine what central site and remote site access lines and equipment you will need to support your telecommuting program.

If you would like assistance setting up your remote networking program, fax a copy of this completed form to Ascend Communications, attn: PreSales Technical Consulting at 510-337-2668. Or call Ascend directly 800-621-9578, option 4. One of our remote networking experts will call you back to discuss the results of the worksheet with you and help you determine the access lines and equipment you'll need.

Remote Users

1. Mobile workers

a. How many mobile workers dial in over analog connections? Today _____ Planned _____

2. Telecommuters

a. How many analog telecommuters do you have? Today _____ Planned _____

b. How many ISDN telecommuters do you have? Today _____ Planned _____

c. How many Switched 56 telecommuters do you have? Today _____ Planned _____

d. How many Frame Relay telecommuters do you have? Today _____ Planned _____

3. Branch offices/support to the central site

a. How many analog lines? Today _____ Planned _____

b. How many ISDN lines? Today _____ Planned _____

c. How many Switched 56 lines? Today _____ Planned _____

d. How many Frame Relay circuits? Today _____ Planned _____

Note: Leased line connections are not supported in this analysis.

Central Site Circuit Requirements

4. Analog Lines

a. Total number of analog users to support
(answers from questions 1a, 2a, 3a): _____

b. What percentage of analog users (mobile workers, telecommuters, customers and suppliers) will dial into the network at the same time? _____%

c. Number of analog lines needed
(multiply number of users by percentage): _____

5. ISDN Lines

a. Total number of ISDN users to support
(answers from questions 2b, 3b): _____

b. What percentage of ISDN users (telecommuters, branch offices, customers and suppliers) will dial into the network at the same time? _____%

c. Number of ISDN lines needed
(multiply number of users by percentage): _____

6. Switched 56/Other Types of Lines

a. Total number of Switched 56 users to support
(answers from questions 2c, 3c): _____

b. What percentage of Switched 56 users (telecommuters, customers and suppliers) will dial into the network at the same time? _____%

c. Number of Switched 56 lines needed
(multiply number of users by percentage): _____

7. Frame Relay Lines

a. Total number of Frame Relay users to support
(answers from questions 2d, 3d): _____

b. What percentage of Frame Relay users (telecommuters, customers and suppliers) will dial into the network at the same time? _____%

c. Number of Frame Relay lines needed
(multiply number of users by percentage): _____

8. Central Site Line Requirements

a. Analog lines needed (from 4c): _____

b. ISDN lines (from 5c): _____

c. Switched 56 lines (from 6c): _____

d. Frame Relay lines (from 7c): _____

e. Total _____

f. Divide total by number of circuits (30 for E1, 24 for T1, 23 for ISDN PRI) _____ divide by 30, 24 or 23

g. Total number of T1/E1 or ISDN PRI lines required: _____

9. Central Site Equipment Requirements

a. Divide the total from 4c by 12.
This will give you the total number of digital modem cards _____

b. Divide the total from 4c by 72.
This will give you the total number of Ascend MAX 4004 products. _____

Appendix D: Glossary

Access Equipment
A device specifically designed to connect remote LANs or workstations to the corporate LAN.

Access Lines, Remote Site
Telephone circuits which connect access equipment at a remote site with the a carrier's network.

Access Lines, Central Site
Circuits which connect a company's central site with the carrier's network. They are used to route incoming data from remote workers onto a corporate LAN.

Authentication
Any one of a number of security measures that can be used to verify the identity of a remote caller.

Authorization
A system of establishing access privileges for users or groups of users.

Bridge
A protocol-independent access device that transfers data packets between LANs or LAN segments over wide area network connections.

Challenge Handshake Authorization Protocol (CHAP)
A security method that challenges and verifies a user's identification. CHAP encrypts a password as it travels over the network.

Call Detail Recording
A management function which collects and records information about outgoing calls.

Callback
A security mechanism that verifies callers by checking their password, terminating their connection, and then calling them back at a number that has been preprogrammed in a user database.

Calling Line ID (Incoming call ID)
A security method which checks a remote worker's authorized phone number against the number provided by the phone company's switching equipment.

Central Site
A centralized location, such as a company's corporate headquarters or regional office, which acts as a data collection point for branch offices, mobile workers, telecommuters and other remote callers.

Central Site Equipment
Remote networking equipment that connects telecommuters and other remote users to the corporate LAN.

Channel
A transmission path between two points. Usually refers to the smallest subdivision of a circuit or access line.

Circuit Switching
A communications method that dedicates an entire circuit to each call.

Compression
A feature of some access equipment that reduces the quantity of bandwidth required to transmit a block of information.

Customer Premises Equipment (CPE)
Access equipment or other termination equipment owned by a company that is physically located on a their property and used to connect to the telephone network.

DSU/CSU
Equipment used to terminate a Switched 56 line and convert a PC's digital data signal into a digital transmission signal.

Digital Modem
A system component which allows modem users to communicate over digital access facilities. They work by converting the PCM-encoded digital data streams sent by analog modem users into their original analog waveform.

Digital Subscriber Line
High-speed network service with speeds from 128 Kbps to 6 Mbps over existing copper telephone lines.

Dynamic Bandwidth Allocation (DBA)
A process that optimizes overall network efficiency by automatically increasing or decreasing the bandwidth of a channel to accommodate changes in data flow from end-user equipment.

Dynamic Password Authentication Servers
Products consisting of server software that generates constantly changing passwords and two-factor, software- or hardware-based password generators that telecommuters carry with them.

E1
A digital transmission link with a total capacity of 2.048 Mbps that is divided into 32 channels, each capable of carrying a 64 Kbps voice or data stream. Used outside of North America.

Encryption
A method of transmitting a message in secret code so that the contents of the message remain unintelligible to anyone that might monitor or copy it.

Fractional T1
A carrier service that offers data rates between 56 Kbps and 1.544 Mbps (T1) in increments of 56 Kbps.

Frame Relay
A fast-packet switching technology that divides data into variable-length packets for high-speed transmission over a shared digital communications channel.

File Transfer Protocol (FTP)
A program for transferring files over the Internet or other TCP/IP environments.

Internet
A global system of interconnected computers and computer networks used by millions of users.

Internet Access
The method by which users connect to the Internet.

ISDN BRI
A digital access line that is divided into three channels. Two of the channels, called B-channels, operate at 64 Kbps and are always used for data or voice. The third D channel is used for signaling at 16 Kbps.

ISDN PRI (E1)
Based physically and electrically on an E1 circuit, but channelized so that two channels are used for signaling and 30 channels are allocated for user traffic.

ISDN PRI (T1)
Based physically and electrically on an E1 circuit, but channelized so that one channel (24) is used for signaling and framing information. The other 23 channels are available for user voice and data traffic.

ISDN Terminal Adapters
Simple devices that provide ISDN compatibility by connecting an ISDN line to the serial port of a personal computer.

ISDN Integrated Access Bridge/Router
A remote access device that connects your computer to an ISDN line, performs bridging and/or routing and supports analog devices such as phones or faxes.

Inverse Multiplexing
A method of combining individually dialed low-speed circuits into a single high-speed data stream.

Local Area Network (LAN)
A data communications network connecting computers in workgroups, departments or buildings.

Modem
A remote access device that connects to PCs and converts digital data into analog signals.

NT1
A device used to connect terminal adapters and other terminal equipment such as ISDN telephones to an ISDN line. In North America, NT1 functionality is often integrated into an access device. In other areas of the world, the NT1 is a separate device that must be leased from the local telephone company.

Packet Switching
A data transmission method that divides data into individual packets for transmission over shared network facilities.

Password Authentication Protocol (PAP)
A simple password protocol that transmits a user name and password across the network, unencrypted.

Perimeter Firewall
There are two types of perimeter firewalls: static packet filtering and dynamic firewalls. Both work at the IP address level, selectively passing or blocking data packets. Static packet filters are less flexible than dynamic firewalls.

Ping
A command that sends an echo request from a management workstation to an end-user device to determine if the equipment and network link are operational.

R2
A series of ITU-T specifications which refer to analog and digital trunk signaling, using compelled handshaking on every Multiple Frequency signaling digit.

Private network
A network made up of dedicated lines leased from carriers, and switching equipment located on a customer's premises.

Remote Authentication Dial-In User Service (RADIUS)
A security administration standard that functions as an information clearinghouse, storing authentication information about users and administering multiple security systems across complex networks.

Remote Access
The process of allowing remote workers to access a corporate LAN over analog or digital telephone lines.

Remote Access Server
Access equipment at a central site that connects remote users with corporate LAN resources.

Remote Network
The access equipment and telephone lines that connect remote users at multiple locations to the corporate LAN.

Restricted Access
A security measure which admits or rejects callers by checking them against a list of remote node addresses programmed into a central site server.

Robbed Bit Signaling
RBS uses the eighth bit in each time slot of a T1 frame. Over a period of several time slots the stolen bit produces a signal, which is used by the T1 equipment. The bits are known as A and B bits.

Router
An intelligent access device that interconnects LANs of the same type and routes data according to parameters such as destination and route availability.

SNMP (Simple Network Management Protocol)
A defacto standard for managing devices on a network

S/T Interface (ISDN BRI)
A four-wire interface between an NT1 device and a terminal adapter. Outside North America, the local carrier usually provides the NT1 and the end user has the option to buy or lease a TA.

Spoofing
A method of fooling access equipment into thinking a network connection is active even when it's not.

Switched 56
An end-to-end digital service offered in North America that transmits data over wide area networks at 56 Kbps.

T1
A data communications link with a total capacity of 1.544 Mbps that is divided into 24 channels, each capable of carrying a 56 Kbps data stream. Used in North America.

Terminal Access Controller Access System (TACACS)
A system of authorizing users developed in the late 1970s by the Defense Data Network community to control access to its dial-in locations.

TACACS+
A proprietary enhancement to the older TACACS system. TACACS+ incorporates a number of the enhanced features found in RADIUS. TACACS+ is supported by Ascend products.

Teleworker/Telecommuter
A work-at-home computer user who connects to the corporate LAN using remote access technologies.

Teleworking/Telecommuting
The use of remote access technology to establish a useful office away from the traditional workplace.

Telnet
A management tool that establishes a virtual terminal session with a teleworker's computer over wide area links. Used to perform remote configuration, diagnostics and other control functions.

U Interface (ISDN BRI)
The two-wire interface that connects to the NT1 on a user's premises. In North America it can be integrated into the customer premises equipment. In other countries, it is typically supplied by the local carrier.

Virtual Private Network (VPN)

A method of connecting geographically dispersed locations over secure connections using the public telephone network or the Internet.

Wide Area Network (WAN)

A communications network that connects geographically remote LANs over local and/or long distance telephone lines.

World Wide Web (WWW)

An Internet service that uses a graphical, hypertext information system to create links between information resources.

Ascend Corporate Remote Access Guide

Fax this Form For Additional Information

To: **ASCEND COMMUNICATIONS INC.**
Worldwide Headquarters
Attn.: PreSales 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:

❑ NetWarp ❑ Pipeline ❑ MAX ❑ Multiband ❑ 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: 510-814-2300
Toll Free: 800-621-9578
FAX Server: 415.688.4343
E-mail: info@ascend.com
Web Site: http://www.ascend.com

ASCEND

Remote Networking
Solutions That Work.™