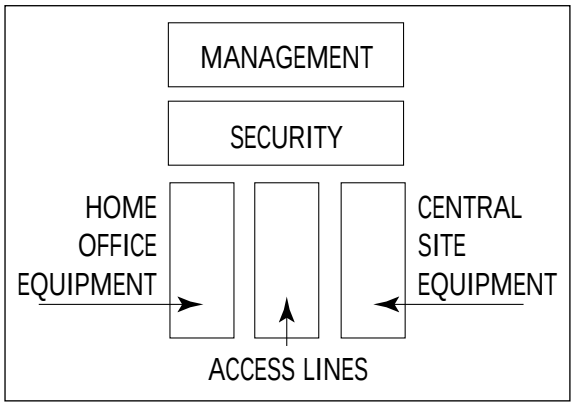
Telecommuting Network Planning Guide

A Resource Guide for
Planners, Executives and
Information Managers



ASCEND

Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502
800-621-9578
510-769-6001

Table of Contents

1. An Introduction To Telecommuting
   - Why Telecommute?
   - Telecommuting Benefits
   - Telecommuting Trends

2. Getting Started
   - How To Use This Guide
   - The Big Picture
   - Assessing Your Remote Access Strategy
   - Starting Small: Setting Up A Telecommuting Pilot
   - The Building Blocks of Telecommuting

3. Network Services: Making The Right Choices
   - Home Office Network Services Options
   - Central Site Network Services Options

4. Home Office Telecommuting Equipment Alternatives
   - Home Office Access Equipment Options
   - Creating More Bandwidth
   - Setting Up the Home Office

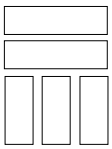
5. Central Site Telecommuting Equipment Alternatives
   - Central Site Equipment Options
   - Digital Modems

6. Security: Issues and Solutions
   - Understanding Your Security Requirements
   - Network Security Options

7. Managing and Supporting Your Telecommuting Program
   - Network Management Methods
   - Training and Supporting Your Telecommuters

8. Appendices
   - Appendix A: Telecommuting Scenario
   - Appendix B: Telecommuting Program Requirements Worksheet

Table of Figures
   - Figure 1. The Building Blocks of Telecommuting
   - Figure 2. BRI vs. Analog
   - Figure 3. File Transfer Times
   - Figure 4. Choosing the Right Access Lines
   - Figure 5. Typical Access Line Costs
   - Figure 6. ISDN PRI vs. T1
   - Figure 7. ISDN Availability
   - Figure 8. Types of Home Office Access Equipment
   - Figure 9. Remote Access Device Comparisons
   - Figure 10. Setting up the Home Office
   - Figure 11. Remote Access Servers
   - Figure 12. Network Security Methods
   - Figure 13. RADIUS diagram



1. An Introduction To Telecommuting

Telecommuting: The use of remote access technologies to maintain a useful office away from the traditional workplace. This office is usually in an employee's home, but can also be in a hotel room, at a client's site or in a telecommunications center that is shared by employees of the same company or different companies. Telecommuters include executives, managers, mobile workers, traveling professionals and other information workers who access their corporate network remotely, either part-time or full-time, during regular business hours, after hours or on weekends.

If you're reading this, your company has probably already decided to implement a telecommuting program or expand an existing one. You're not alone — companies with telecommuting programs in place already number in the thousands and an estimated 8.4 million workers telecommuted during 1994.* Add to that the number of corporate employees who worked after-hours from home, and the total number of telecommuters more than doubles. Industry experts predict that by 1998, close to 60 million people will work in some capacity, either part- or full-time, from home offices, satellite offices or neighborhood work centers.

**According to a February 1995 study by Link Resources Corp., New York, NY.*

Why Telecommute?

Telecommuting, which started out several years ago as a way to improve air quality and reduce freeway congestion, has now become a valuable and viable way for employees and companies to conduct business.

Organizations of all sizes and in all lines of business have embraced telecommuting for reasons that include:

Compliance with the State and Federal legislation. The Clean Air Act Amendments of 1990 mandates that over 100 major cities with severe or extreme ozone pollution must implement trip-reduction programs such as telecommuting to improve air quality.

Employee recruiting and retention. Telecommuting offers employees a flexible work schedule that makes a company attractive to potential employees. It also makes it easier for a company to hire qualified employees by extending the geographic area within which a company can recruit workers.

Reduction in overhead costs. When employees work at home, companies save money on facilities costs and infrastructure expenses such as energy consumption. Many "Work at home" programs allow employees to spend 2-3 days at home.

Reduced downtime in the event of extreme weather conditions, disasters or emergencies. Companies with telecommuters can be more resilient and responsive during disasters such as earthquakes, extreme weather conditions such as snowstorms or in the event of breakdowns in public transportation systems.

Telecommuting Benefits

Telecommuting Facts

- *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 telecommuter. (Gartner Group)*
- *Telecommuters at Pacific Bell exhibited 25% less absenteeism than other employees.*
- *The number of telecommuters will continue to increase at the rate of more than 10% per year through 1998. (Link Resources)*

Companies that have tried telecommuting are discovering that the benefits are often far greater than they had expected. These benefits include:

Increased productivity. Large telecommuting pilot programs and trials show that employees working at home — where they can work at any hour of the day or night — actually increase their productivity by 10 to 30 percent.

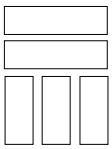
Improved quality of life. Telecommuting can reduce the stress of commuting, eliminate the interruptions and frustrations of the workplace and give workers more time with their families.

Decreased absenteeism. Telecommuters with colds or minor aches and pains are less likely to miss a day's work than their counterparts who must commute to the office. Telecommuters can also fit doctor or dentist visits or other personal appointments into their regular telecommuting schedule without taking sick leave.

Telecommuting Trends

Recent trends and developments in three major areas have fueled the growing acceptance of telecommuting as an alternative form of work.

Social Trends. Because of changing attitudes about work and leisure time and changes in the size, shape and nature of our families, workers are placing increasing importance on flexibility in their work lives. Telecommuting allows workers to enjoy a less-structured lifestyle, live where they want or where they can find affordable housing, and maintain a flexible work schedule that can accommodate child-care or elder-care responsibilities.



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

Technology Trends. For years, analog phone lines and modem technology have limited the type of work telecommuters could perform from home. For some telecommuters— those checking their E-mail or transferring small files — this is adequate. But for workers with demanding file transfer requirements — service representatives, computer programmers, engineers, or graphic artists, for example — sluggish modem speeds have forced them to limit the tasks they perform from home, or made it impossible for them to work from home, at all.

Thanks to recent advances in telecommunications technology, the options available to telecommuters have expanded beyond the limitations of analog modems. Now, high-speed, high-performance digital network services and sophisticated access equipment allow telecommuters to connect to corporate networks at speeds of 128 kbit/s and above. That means that a wider range of workers, including those with intensive data communications requirements, can now work from home effectively. And telecommuters, like their office counterparts, will be able to enjoy emerging high-bandwidth applications such as collaborative sessions, large file transfers, shared 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 have come on the scene that are tailor-made to fit the usage patterns and traffic requirements of many of today's telecommuters.

The cost of digital access equipment is coming down too. Vendors are adopting defacto standards that ensure interoperability with other vendors' devices and equipment is getting easier to set up and manage. And new security solutions are being introduced that minimize the increased risks associated with opening corporate networks to telecommuting traffic. The right time for your company to start telecommuting is now. By the end of the century, telecommuting will no longer be a luxury available to only a subset of the work force. It will become a necessity, offered by companies who want to remain competitive in the marketplace, recruit and retain valuable employees and comply with government mandates regarding improved air quality.

2. Getting Started

How To Use This Guide

The purpose of this guide is to help you make the difficult technology choices associated with setting up a successful telecommuting program in your own organization. You should be reading this guide if you're the planner who will design your company's telecommuting plan, the executive who will approve the plan, or the information manager who will bear the responsibility for implementing the plan and keeping it up and running.

It's a practical guide designed to address the needs of a variety of organizations with telecommuting needs ranging from the simple to the sophisticated. It explains the nuts and bolts of telecommuting technology, lays out the pros and cons of different telecommuting options and assists you in drawing up your own telecommuting plan.

When you have finished reading this guide, consult the case studies in Appendix A to get a feel for the telecommuting scenario that fits most closely with your own telecommuting needs. Then complete the Telecommuting Program Requirements worksheet (Appendix B). From there, you should have most of the information you need to lay out your telecommuting plan. If you would like assistance in determining your telecommuting requirements, fax a copy of your completed Telecommuting Program Requirements Worksheet to an Ascend Communications telecommuting consultant.

Bear in mind: the plan you come up with now will form the foundation of your company's telecommuting program into the next century. Make sure the telecommuting solution you choose will be able to grow to accommodate a larger number of telecommuters, handle emerging high-bandwidth multimedia applications and provide a smooth migration to an all-digital environment. Remember — the right technology solution for your telecommuters will be the one that gives them all the computing resources they need to do their jobs effectively. Choosing the right solution may mean the difference between a telecommuting program that never quite gets off the ground and one that makes employees happier, operates within its budget and improves your company's bottom line.

Assessing Your Remote Access Strategy

The Big Picture

Technology is just one aspect of your company's overall telecommuting strategy. When you take a look at the bigger picture, telecommuting also includes the larger issues of human resources and business processes.

A recent Gartner Group report entitled "Building Enterprise Strategies for Remote Access" advises companies to concentrate on the business issues involved in telecommuting before making decisions about technology. Its recommendation: identify the business drivers that have lead your company to set up a telecommuting program, identify the business value of performing work out of the traditional office environment and determine the management issues involved in telecommuting. Once these issues have been resolved, proceed to the final step — choosing the technology that supports your particular business processes.

This guide does not address the business planning or human resources issues that must be considered in preparing for telecommuting.

Understanding how your existing network infrastructure currently handles remote traffic from branch offices, telecommuters, mobile workers or clients is the first step in planning your telecommuting program.

Once you have a firm grasp of how your company is handling remote access today, consider how telecommuting fits into your remote access plans. If your telecommuting program is a sizable one, you may decide to consolidate your telecommuting traffic with traffic from other remote users onto a single access line. You may want to eliminate the separate access devices you use today and consolidate all of your remote traffic onto a single remote LAN access server. At the same time, you may eliminate some of the management and support headaches you've experienced by deciding to install equipment that is easy to manage and based on industry-wide standards.

In the long run, implementing a telecommuting program may force you to rethink your whole remote access strategy. It may be a lot of work, but it gives you the opportunity to save money on access lines and equipment, increase management, support and security in your network, improve the remote access services available to your users and plan ahead for the growth of telecommuting within your organization.

The Building Blocks of Telecommuting

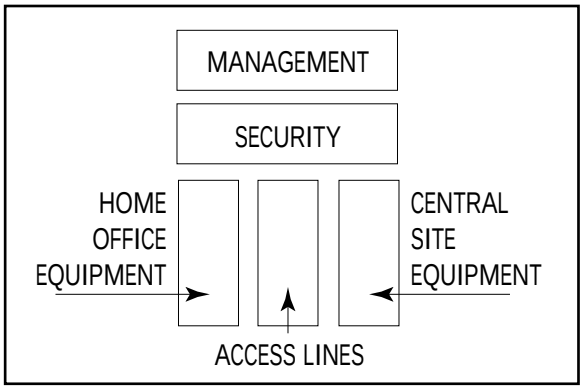
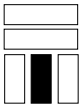
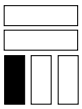


Figure 1
The Building Blocks of Telecommuting

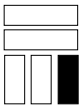
Setting up a telecommuting program is a big undertaking, but becomes easier if you realize that it's a step-by-step process that can be broken down into discrete, manageable building blocks. Use these building blocks to construct your telecommuting program:



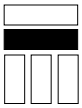
Network Services (analog, ISDN, Frame Relay). These are the network lines (ie:Telephone Company) that will carry data traffic between your telecommuters' locations and your central site.



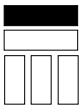
Home Access CPE (Customer Premise Equipment). At your telecommuters' homes, equipment is needed to allow telecommuters the ability to connect to the selected network services.



Central Access equipment. At the corporate central site, access equipment is needed to support traffic from multiple concurrent telecommuters.



Security. You will need to put security mechanisms in place to cut down on the risks associated with opening your network to telecommuters outside your facility.



Network management. You should be able to manage your telecommuters' access lines and equipment as part of your existing network management system.

The following sections of this guide discuss the building blocks of telecommuting in detail. Section 3 explains how to choose both the appropriate network services and central site access lines; Section 4 discusses home office access equipment used for telecommuting; Section 5 looks at central site equipment options; Section 6 explains network security options and discusses the trend towards server-based security; Section 7 describes methods for managing telecommuting programs and supporting users.

3. Network Services: Making the Right Choices

Network Services — the pipes that send data from an endpoint location such as a telecommuter's home or a corporate central site into a carrier's network — are the link that will connect your telecommuters with the resources on their corporate network.

In setting up your telecommuting program, you will need to consider two types of access lines — home office access lines and central site access lines.

First, consider home office access lines, the lines that connect your telecommuter's PC with the carrier's network. Then determine your central site access lines, the pipes that will route traffic from telecommuters onto the corporate network . The speed, the kind and the number of access lines your telecommuters use will determine the access lines you need at your central site.

Home Office Access Line Options

Consult Figure 4 "Choosing the Right Access Lines" on Page 14 to help you determine the best access line for your telecommuters' needs. Figure 5, "Comparing Access Line Usage Costs" On page 15 will help you decide which access line will be most economical.

Each of your telecommuters will need an access line to link their computer at home with the corporate network, the Internet or other online services. The network service you choose for them should be the one that lets them perform their job duties just as effectively from home as they can from the office.

Consider the following issues before you choose access lines for your telecommuters:

Usage Patterns. Understanding your telecommuters' usage patterns will help you decide what kind of access lines they need. How often will they access the corporate network? What kind of tasks will they perform from home? What type of files will they send across the network? What sort of response times do they need to perform their jobs effectively? For example, a customer service representative at a bank who queries a database all day may need a nearly-constant high-speed network connection to perform his job. On the other hand, an attorney working at home who only downloads a few large files each day may be satisfied with a low-speed network connection.

Typical Data Usage By Job Type

Low Volume, Occasional Frequency, Low to Medium Speed: Project Manager, Office Administrator, Copywriter

Medium to High Volume, Occasional Frequency, Medium Speed: Technical Writer, Salesperson, Accountant

High volume, High Frequency, High Speed: Graphic Artist, Engineer, Computer Programmer, Technical Support Specialist

Cost. To figure out which access line solution will be most cost-effective, estimate the number of hours per month each of your telecommuters will use their network link and how far away they live from their phone company's serving office. Also factor in the cost of the access equipment they will need to support a particular type of access line.

Availability. Your phone company may not offer certain types of network services — ISDN or Frame Relay, for example — in the geographic locations where some of your telecommuters live. Check with them in advance to find out if you will be limited to certain access lines in certain locations.

Types of Home Office Access Lines

Choose access lines with capabilities that dovetail most closely with your telecommuters' usage patterns. You have four main types of home access lines to choose from:

- Analog
- Switched 56
- ISDN BRI
- Frame Relay

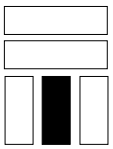
Analog. This is the same service you use in your home for voice conversations. Analog lines can carry digital data traffic at speeds up to 28.8 kbit/s.

Advantages: Ubiquitous; inexpensive.
Disadvantages: Too slow for heavy usage or high-bandwidth applications; lengthy call set-up time (up to 40 seconds). 93% connect rate.

Because of aggressive pricing and marketing by carriers and increasingly widespread availability over the last two years, ISDN is becoming the access line of choice for the majority of today's telecommuters.

ISDN BRI. Integrated Services Digital Network is an all-digital service that can simultaneously transmit voice and data over a single twisted pair connection. ISDN Basic Rate Interface access lines consist of two 64 kbit/s channels called "B" channels that carry either voice or data and a third "D" channel used primarily for signalling. Some access equipment allows users to combine the two "B" channels of an ISDN BRI line to achieve a total throughput of 128 kbit/s.

Advantages: High-speed; relatively low-cost; 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
Disadvantages: Not available in some areas.



	BRI	Analog
SPEED	64 kbit/s on each B channel 5 times faster than analog Call setup time: 300 milliseconds	Up to 28.8 kbit/s on dial-up modem Call setup time: >8-15 seconds
FLEXIBILTY	Two simultaneous calls can be made over a single BRI. Bandwidth expansion is possible through combining B channels. Up to eight telephones, computers, or fax machines can be linked to a single BRI. B channels can be used for voice and data.	Only one call can be made at a time. A telephone, computer, and fax machine can share an analog line. Only one telephone number can be assigned to an analog line.
COST	Faster speeds result in less usage and higher productivity.	Slower speeds result in higher usage and lower computer productivity.

FIGURE 2
BRI versus Analog

Switched 56. Switched 56 is an end-to-end switched digital service that supports data transport over a carrier's network at 56 kbit/s. Multiple Switched 56 lines can be combined to achieve throughputs of 128 kbit/s or higher using equipment that can perform inverse multiplexing. Switched 56 is a good choice for telecommuters in areas where ISDN is still unavailable.

Advantages: Twice the speed of modems; available in some areas where ISDN is not.
Disadvantages: Typically expensive if your telecommuters live a long distance from the phone company's serving office.

Switched vs. Dedicated Services
Switched services such as ISDN and Switched 56 are usually more economical for telecommuting because charges are determined by usage — the more you use, the more you pay. Dedicated services such as Frame Relay are billed on a fixed monthly rate. Frame Relay may be the best choice for telecommuters with heavy usage requirements who must access their corporate network more than 3 hours a day.

Frame Relay. Frame Relay is a fast-packet switching technology that has become popular within 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. Frame Relay requires a dedicated connection to the network.

Since Frame Relay pricing is based on a flat fee and is distance-insensitive (Tariffs as of August 1995), it is a good choice for telecommuters with usage requirements averaging more than three hours per day and for telecommuters who would otherwise pay long distance rates to connect to their corporate network . In some areas today a 56 kbit/s Frame Relay circuit costs as little as $125 a month — less than ISDN if the line is used more than three hours everyday.

Advantages: Economical in frequent-usage, high-bandwidth situations.
Disadvantages: Expensive if users must set up Permamnent Virtual Circuit (PVCs) to a number of different locations. Technically more demanding.

FIGURE 3
Response times vary considerably depending on the speed of your telecommuters' access equipment and the size of their files.

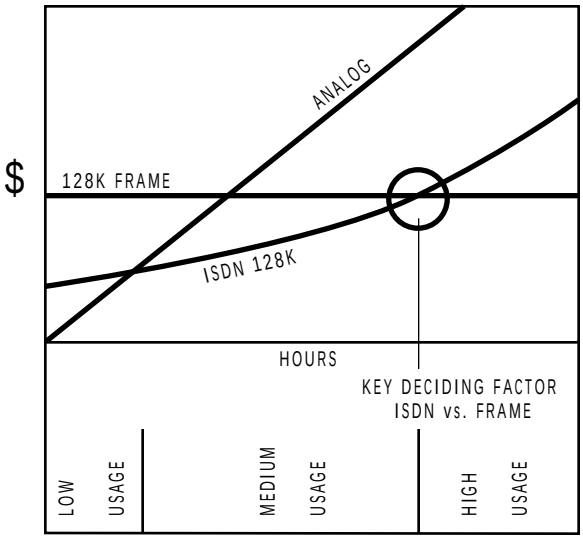
FILE TYPE	FILE SIZE	9.6 kbit/s	28.8 kbit/s	64 kbit/s	128 kbit/s	512 kbit/s
WORD PROCCESSING (20 pages)	40 kbytes	33 sec.	11 sec.	5 sec.	2.5 sec.	.625 sec
SPREADSHEET	100 kbytes	83 sec.	27 sec.	12.5 sec	6.25 sec.	1.6 sec.
B&W PRESENTAION	1 Mbyte	14 min.	4.5 min.	2 min.	1 min.	15 sec.
CAD/CAM	2 Mbytes	29 min.	9 min.	4 min.	2 min.	30 sec.
DIGITIZED PHOTOGRAPH	4 Mbytes	56 min.	19 min.	8 min.	4 min.	1 min.
COLOR PRESENTATION	10 Mbytes	139 min.	46 min.	21 min.	10 min.	2.5 min.
X-RAY FILES	100 Mbytes	23 hrs.	8 hrs.	3.5 hrs.	1.7 hrs.	26 min.

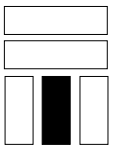
FIGURE 4
The kind of access line you need depends on your telecommuters' usage patterns and bandwidth requirements.

	ANALOG	ISDN BRI	SWITCHED 56	FRAME RELAY (56K)
SPEED				
low	✥			
medium		✥	✥	✥
high		✥		✥
FREQUENCY				
occasional	✥	✥	✥	
frequent	✥	✥	✥	✥
VOLUME				
low	✥			
medium		✥	✥	✥
high		✥		✥
INSTALLATION COST				
low	✥	✥		
medium		✥		
high			✥	✥
MONTHLY LINE COST				
low	$ 50.00*	$ 75.00*	$ 85.00*	$ 80.00*
medium	$ 75.00*	$100.00*	$175.00*	$125.00*
high	$100.00*	$150.00*	$350.00*	$250.00*
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

*Prices shown are approximate. Price varies by location and carrier.

Comparison of costs based on monthly usage.





Central Site Access Line Options

Once you've decided the type of home office access lines your telecommuters will need, your next step is to choose access lines and equipment that will handle the telecommuting traffic coming into your central site.

You can break down the process of choosing central site access lines into three main steps:

Step 1: Estimate how much traffic your telecommuters will generate. Base this estimate on the total number of telecommuters in your program, the combined bandwidth of their access lines, and their predicted usage patterns. Make sure to take into account peak traffic periods on certain days of the week or month or during certain times of the day, when a large number of users may need to access the network resources at the same time. Plot your results to determine how much bandwidth you will need to support your new telecommuting program.

Step 2: Consider telecommuting in the context of your existing remote access strategy. Most likely, your network already has some combination of analog, Frame Relay, ISDN or Switched 56 access lines that handle remote traffic from branch offices, mobile workers or after-hours telecommuters. Combining your telecommuting traffic and your existing remote access traffic onto a single access line will not only save you money on access line costs but also on equipment, management and support costs, as well.

Home Office	Analog	$12 - $30 / line per month
	SW56	$30 - $75 / line per month
	BRI	$22 - $50 / line per month
	Frame Relay	$125 / month
Central Site	T1	$200 - $500 / month
	PRI	T1 + $100 - $525 / month

FIGURE 5
Typical Access Line Costs

Step 3: Choose the central site access line option that best fits your needs. There are several ways to increase the bandwidth coming into your central site:

Replace the separate low-speed lines you currently use for your existing remote access traffic with a T1 or ISDN PRI pipe. The new high-speed pipe will handle your telecommuting traffic as well as the traffic from your remote offices and mobile workers.

If you already use a T1 or PRI to transmit data, you can route your telecommuting traffic onto your corporate network over your existing access line.

T1 or ISDN PRI?
Whether you decide to install a new access line to handle telecommuting traffic or consolidate existing remote access traffic and telecommuting traffic onto an existing access line, you have a choice of two access lines:

T1. A channelized 1.544 Mbit/s pipe that is divided into 24 channels. Each channel is capable of carrying up to a 56 kbit/s voice or data stream. Using T1 access equipment, users can preallocate certain channels on a 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 available in speeds of 128-, 256-, 384-, 512- and 768-kbit/s.

ISDN PRI. ISDN Primary Rate Interface lines are based, physically and electrically on a T1 line but are channelized differently. They contain twenty-three 64 Kbit/s channels and a single "D" channel for signalling. Like T1s, ISDN lines can be provisioned to support all kinds of data traffic, including Frame Relay and Switched 56, as well as voice traffic. Unlike T1s, which require channels to be preallocated to either voice or data traffic, the channels on ISDN PRI lines can be dynamically allocated to handle either voice or data on a call-by-call basis.

Reallocate some of the bandwidth from the T1 or PRI line that carries the voice traffic from your PBX to accept data traffic from your telecommuters.

The ISDN Advantage

ISDN PRI lines are becoming popular for remote access applications because they can allocate bandwidth on a call-by-call basis to either voice or data. Customers using PRI lines instead of T1s have been able to reduce the number of channels they use by 25 percent, according to Pacific Bell.

	PRI	T1
SPEED	64 kbit/s on each of 24 channels (24th channel used for all signaling*) Call setup time: 300 milliseconds	56 kbit/s on each of 24 channels (Because in-band signaling uses 8 kbit/s) Call setup time: 3 to 5 seconds
FLEXIBILTY	Any channel can be used for inbound calls, outbound calls, or 800 calls, on a call-by-call basis. Channel is not allocated if the destination number is busy ("look-ahead routing"). Allocate channels by time of day, e.g., more voice calls during day and high speed data transfer at night.	Channels are pre-assigned for type of calls, so some channels can sit idle while other channels ring busy. Channel is allocated for the call while it checks to see if destination line is busy. 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.

FIGURE 6
PRI versus T1

ISDN AVAILABILITY

According to Bellcore's 1994 ISDN Deployment Study, the following are RBOC's projections for ISDN deployment in 1995: Ameritech 81%, Bell South 71%, NYNEX 49.8%, SW Bell 66%, Bell Atl 77.2%, GTE 50%, Pac Tel 82.6%, US West 50.7%.

Ameritech
(800) TEAMDATA
Illinois, Indiana, Michigan, Ohio, Wisconsin
www.ameritech.com/solutions/data/isdn/isdnfrm1.htm1

Bell Atlantic
(800) 570-ISDN
Delaware, Maryland, New Jersey, Pennsylvania, Virginia, Washington D.C., West Virginia
www.bell-at1.com/customer/consumer/isdn

Bell South
(800) 428-ISDN
Alabama, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee
www.ocn.com/cgibin/lookup

Nevada Bell
(702) 333-4811(small businesses)
(702) 688-7100 (large businesses)
Nevada

NYNEX
(800) GET-ISDN
New York, Massachusetts, Rhode Island, Vermont, Maine, New Hampshire
http://www.atria.com/-htk/ISDN.htm1
*FAQ on NYNEX home ISDN

Pacific Bell
(800) 4PB-ISDN (ISDN service center)
(800) 995-0346 (24 hr. automated ISDN)
California
www.pacbell.com/products/SDS-ISDN/isd-21.htm

Southern New England Telephone (SNET)
(800) 430-ISDN
Connecticut

Southwestern Bell
(800) SWB-ISDN
Missouri, Texas, Arkansas, Oklahoma, Kansas

US West
(800) 246-5226
Arizona, Colorado, Minnesota, Nebraska, Oregon, South Dakota, Washington

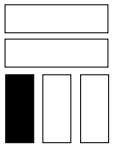
Other ISDN Service Providers

Cincinnati Bell - (513) 566-DATA
Ohio, Kentucky

Rochester Telephone -
(716) 777-1234
New York

Stentor - (800) 578-ISDN
Canada
www.stentor.ca/basic/products/isdn/isdn.htm1a

FIGURE 7
ISDN Availability



4. Home Office Access Equipment: The Alternatives

Once you've chosen the access lines that fit your telecommuters' needs, your next step is to choose the equipment that will physically connect their computers with these lines. Access equipment falls into two categories: home office equipment and central site equipment.

ANALOG	MODEM
ISDN BRI	ISDN TERMINAL ADAPTER BRIDGE ROUTER INTEGRATED ACCESS DEVICE
SWITCHED 56	DSU BRIDGE ROUTER
FRAME RELAY	BRIDGE ROUTER

FIGURE 8
Home Office Access Equipment Options by Type of Access Line

Home Office Access Equipment Options:

Modems, ISDN Terminal Adapters, DSU/CSUs, Bridges, Routers, and Integrated Access Devices

Home office access equipment (CPE) has an interface on one side that connects to the access line from the phone company; on the other side, it plugs directly into an interface on your telecommuters' PC or into a small home LAN.

The network service you have selected will determine the access equipment options available to you. If you select an analog line, for example, a modem is your only choice of access equipment. If you decide to use an ISDN BRI circuit you can choose among three access equipment options – ISDN terminal adapters, ISDN bridges or routers or Integrated Access Bridge/Routers (see Figure 8: Types of Home Office Access Equipment).

The following types of access equipment are available:

Modems. Modems, standalone devices or cards that fit inside PCs, are today's workhorses of the telecommuting world. Advances in modem technology have boosted the maximum throughput of V.34 modems to 28.8 kbit/s – a data transfer speed adequate for the needs of many of today's telecommuters. And modems are still a must in cases where analog lines are a user's only option – hotel rooms or customer sites, for example.

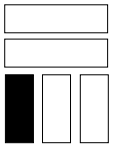
Advantages: Inexpensive; Familiar; Easy to use.
Disadvantages: Low speed; Unable to handle multimedia and large graphic files.
Cost: $100 to $300
Access Lines: Analog.

DSU/CSUs. In the telecommuting world, Data Service and Channel Service Units, the digital equivalent of analog modems, are required to terminate Switched 56 access lines. They come built into larger equipment such as routers or can be purchased as standalone units that connect to a PC's serial or Ethernet port.

Advantages: Inexpensive compared to other digital access equipment.
Disadvantages: Comparatively low speed; No capacity to bond channels together to achieve higher throughput.
Cost: $300 to $400
Access Lines: Switched 56 or network service.

ISDN Terminal Adapters. These simple devices provide ISDN compatibility to PCs by translating data into ISDN compatible-data using a method called rate adaption and performing signalling and call setup over the "D" channel. Although most ISDN terminal adapters today only transmit data over one 64 kbit/s "B" channel at a time, vendors are working on specifications that will soon allow the devices to bond the two "B" channels together.

Advantages: Less expensive than ISDN bridges or routers; Faster than modems.
Disadvantages: Contain no intelligence; Currently limited to 64 kbit/s throughput.
Cost: $350 - $600
Access Lines: ISDN



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

Advantages: Easier to set up and manage than routers or ISDN Integrated Access Bridge/Routers.
Disadvantages: More expensive than ISDN Terminal Adapters or DSU/CSUs; inefficient use of bandwidth can result in broadcast storms.
Cost: $900 to $2,000
Access Lines: ISDN; Switched 56; Frame Relay

Routers. These intelligent devices connect remote users to corporate networks over ISDN, Switched 56 or Frame Relay wide area network links. Their routing tables that can be programmed either statically or dynamically to route data over a network to a particular network address. Because they are protocol-dependent, they 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 efficiently over multiple networks; makes efficient use of network bandwidth.
Disadvantages: More expensive than other access equipment; more complex to set up and manage than bridges.
Cost: $900 to $2,000
Access Lines: ISDN; Switched 56; Frame Relay

ISDN Integrated Access Bridge/Routers. A new type of equipment that comes with an ISDN port and either one or two analog ports. Since Integrated Access Bridge/Routers let you route analog and digital traffic over a single BRI line, they eliminate the need for multiple access lines into a telecommuter's home office. 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 kbit/s throughput
Disadvantages: More complex to set up and provision than other access equipment.
Cost: $900 to $2,000
Access Lines: ISDN

FIGURE 9
Remote Access Device Comparisons

	Modems	ISDN TA	Bridge / Router	Integrated Access Device
Access Line	analog	1 B channel	2 B channels	ISDN and analog
Advantage	- low cost - easy	- low-cost ISDN	- high performance - secure - remotely manageable	- solves home wiring limitations - analog support - lower cost line charges - multiplex voice & data traffic
Disadvantage	- slow - limited media & device support	- slow only 64 kbit/s - not upgradable - no management - no security	- cost - no analog support	- slightly longer installation for analog & ISDN connections
Cost	$200 - $500	$350 - $600	$900 - $2,500	$900 - $2,000

Setting Up The Home Office

Before your telecommuting program gets off the ground, your telecommuters will need a full range of equipment that lets them perform their job from home the same way they do in the office. That means setting up an office in their homes that duplicates most of the functionality of their corporate workspace. To do that effectively, most telecommuters will need:

- A computer with a built-in modem
- A printer
- Fax capabilities (fax software or as a stand-alone fax machine)
- A telephone
- An answering machine

Too Much Equipment, Too Many Lines

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

The ISDN Solution: Using ISDN eliminates the need for three separate access lines. Since ISDN handles both analog and digital traffic, telecommuters can carry on voice conversations, send and receive faxes and transmit data at high speeds onto their corporate network over a single ISDN line. That increases your telecommuters' performance, saves money on phone charges and cuts down on the number of phone lines coming into your telecommuter's home.

Other ISDN features allow users to:

- Automatically allocate channels for incoming or outgoing calls and faxes.
- Handle two calls simultaneously (both digital, both analog or one analog and one digital).
- Set up a call in one-to-two seconds.
- Support up to eight pieces of equipment to the same line (phones, fax machines, answering machines, etc).

The "typical" SOHO (small office/home office) has at least two lines: a voice line with a telephone and an answering machine, and another line for fax machine or modem. More and more users are finding they need a third line: a dedicated line. Why? If they are running a remote session they must choose between missing either voice calls or incoming faxes. Understandably, users are finding this an increasingly unacceptable situation. So they order a third analogue line only to find out that new wiring must be run all the way from the telephone pole through and into the house walls – at great expense. An ISDN integrated access device with dynamic bandwidth management allows two lines to behave as three, and uses existing wiring.

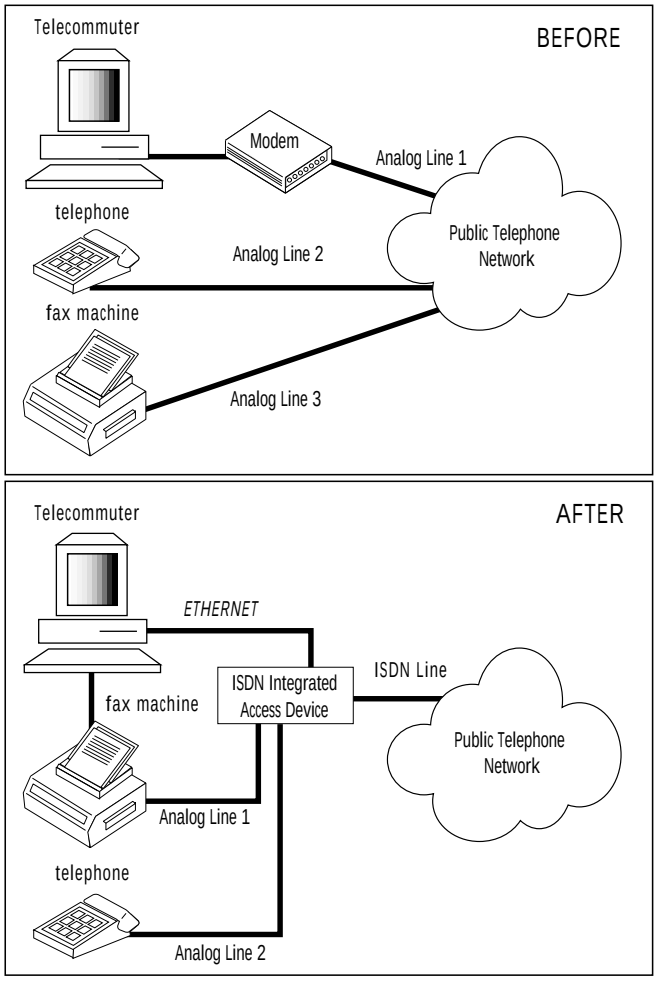


FIGURE 10
Setting up the Home Office

A new type of access device called an ISDN Integrated Access device has recently come to market that helps users take full advantage of these ISDN features. It contains an ISDN port and either one or two analog ports that telecommuters can use to connect analog phones, fax machines or answering machines to their ISDN line. (Note: Includes a network terminating unit or NT-1 that the phone jack plugs into it.) The equipment can be located anywhere in your house and connected over standard inside phone wiring.

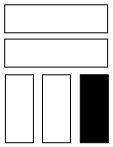
Creating more bandwidth

Some access equipment contains special features that can be used to create more bandwidth for your telecommuters.

Inverse multiplexing. Inverse multiplexing creates extra bandwidth by combining multiple digital channels into a single high-speed data stream for transport across a wide area network. This feature can be used to combine two or more Switched 56 kbit/s channels into a higher-speed pipe or to aggregate the two 64 kbit/s B channels of an ISDN line into a128 kbit/s pipe. Inverse multiplexers are available as standalone units or as features of routers.

Dynamic bandwidth allocation. A feature of some access equipment that adds or subtracts bandwidth from a connection in real time to accommodate changes in data flow from end user applications. DBA saves you money by cutting back bandwidth when you don't need it. It also increases the performance of your equipment by automatically expanding bandwidth to accommodate increased demand from bursty file transfers.

Compression. Compression, a feature built into most access equipment, is another method of creating more throughput for telecommuters. Compression can be useful in cases where users need to transfer large text files. But beware. Compression may actually degrade performance in situations involving graphics files or data files downloaded from the World Wide Web that have already been compressed.



5. Central Site Telecommuting Equipment

Back at corporate headquarters, you will need new access equipment to handle the increased amount of data traffic flowing back and forth between your telecommuters and your corporate network.

Remote Access Servers Defined

Your best choice of central site access equipment is a remote access server. Simply put, remote access servers allow a number of telecommuters at different locations to dial in over a wide area network link, establish connections to their corporate LAN as if they were locally attached and then disconnect those connections when they have completed their work.

On the wide area network side, a remote access server connects to the fractional T1, T1, ISDN PRI or Frame Relay access line that you've set up to handle your telecommuter traffic. On the other side, it connects to your local area network.

For organizations faced with the need to handle exploding traffic from telecommuters and other remote users, remote access servers have become the access equipment of choice. They are rapidly replacing more traditional approaches to remote connectivity: terminal emulation, a method that limits a remote user to the functions of a dumb terminal and does not support client/server applications; and remote control, a method that requires a dedicated PC on the corporate LAN for each remote client and uses proprietary technologies between the client and the server.

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

Consolidate access lines. Because they can consolidate traffic onto a single high speed access line (ie.: ISDN PRI or T-1), remote access servers eliminate the need to pay for and manage separate analog, dedicated and digital dial-up lines coming into your central site.

Replace digital access devices. One remote access server can replace multiple access devices — terminal adapters, DSU/CSUs, routers — that might be cluttering equipment rooms and wiring closets at your corporate headquarters.

Eliminate modem bank. By installing a remote access server with digital modem capabilities you can get rid of the separate modem banks and terminal servers that you're probably using today to handle calls from traveling professionals and customers.

Reduce network management costs. Reducing the number of access lines and access devices at your central site lets you reduce the time and cost of maintaining and troubleshooting your network, too.

Improve network security. Separate lines with separate modems & adapters can not be secured. Remote access servers offer a single point of entry and can be very secure.

Your choice of remote access server will depend on the number of telecommuters and other remote users you need to support, the kind of access lines you're planning to install, and your network management and security needs.

In general, avoid low-end solutions that require external modems or other access devices. They require you to allocate a fixed number of analog and digital channels. They will also be difficult to manage. Instead, look for a solution that is flexible and scalable, features integrated digital modems if you need to handle both analog and digital traffic, and can be scaled to accommodate additional users as your remote access needs grow.

Features of Remote Access Servers

In order to keep up with the boom in telecommuting and mobile computing, remote access server technology has matured considerably over the last few years. Today, remote access server vendors offer products that are designed for a broad range of remote access applications and vary considerably in price, features and functionality.

Basic units are available that support just a few users, connect to external analog or digital access devices and target only a single wide area network service such as analog or ISDN BRI. Mid-range remote access servers typically work with several different protocols, come with access devices integrated into the unit itself and support between 16 and 32 users. High-end units are distinguished by a broad range of features that can include the ability to work with multiple types of remote clients, support for a breadth of WAN interfaces such as ISDN, Frame Relay and Switched 56, availability of integrated network management features, comprehensive routing features, terminal server, digital modems, and inverse multiplexer.

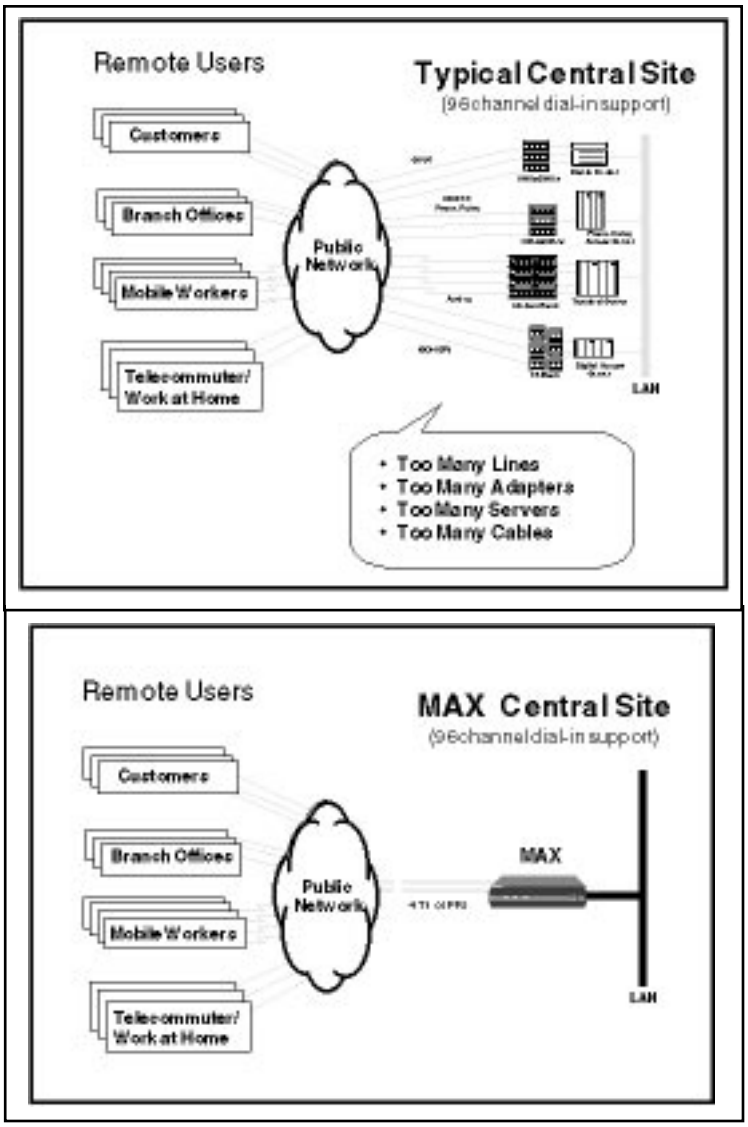


FIGURE 11
Remote Access Servers

Figure 11 shows a typical central site with or/and without a remote access server.

- the remote access server soluiton supports all services (T1, E1, FT1, analog, ISDN, SW56, and Frame Relay)
- integrates routing, terminal server, digital modem pooling, and multiplexing
- dynamically switches up to 96 channels, to and ports, to any service

Evaluating Central Site Remote Access Servers

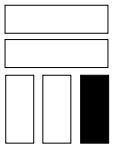
The central site solution must scale to support whatever number of remote sites required. The following items gives the key evaluation criteria for these products:

	ASCEND MAX 4000	CISCO 7010	COMBINET 900	GANDALF XPRESSWAY
Price with 4 PRI	$18,500	$50,950	$22,050	$30,900
Price with 4 PRI & 48 modems	$54,500	$113,950	$60,825	$66,225
Maximum Number of PRIs	4	4	1	6
Digital Modem Ports	48	none	none	none
Full Channel Sharing	yes	no	no	no
MP+ Support	yes	no	no	no
Compression	Hardware	Software	Hardware	Software
Frame Relay	yes	yes	no	yes
Video Integration	yes	no	no	no
PBX Integration	yes	no	no	no
Price Per B-channel	$193	$530	$230	$322
Rating	High	Medium	Low	Medium

The Ascend MAX 4000 was given a "High" rating and the others were given medium or low ratings due to the considerations listed below:

Ascend MAX 4000

- Router and bandwidth manager that supports four PRIs.
- Supports up to 48 digital modem ports that support modem calls over ISDN PRI.
- MP+ assures that Ascend configurations can scale easily to larger configurations by adding more MAX 4000s.
- Hardware compression will support the demands of 96 channels with no performance degradation.
- Can dynamically allocate B-channels from the PRI pool to support ISDN, modems, switched 56, and Frame Relay.
- Provides mixed media integration supporting video conferencing and PBX integration.



Scalability (MAX. PRI Ports in a single Chassis). The maximum number of PRIs that can be supported in a single unit. Some vendors require separate boxes which can cause difficulties with two B-channel calling since both B-channel calls must go to the same chassis so that the data they carry can be integrated into a single datastream.

Full Channel Sharing. A product, like the Ascend MAX 4000 that supports digital modems can use the same set of PRI B-channels for modem, ISDN, and Frame Relay connections. The other products use external modem banks that must be supported by a separate set of dialup phone lines.

MP+. An extension to the PPP Multilink Protocol developed by Ascend that addresses the connection control issues that were not included in RFC1717 which defines the PPP Multilink Protocol (MP). MP+ controls adding and subtracting B-channels in a large telecommuting network that integrates voice, data, and facsimile. MP+ is the defacto standard protocol used by 90% of the major Internet Service Providers.

Compression. Products with hardware compression can support the full throughput potential of four PRIs. Products with software compression cannot keep up with two or more PRIs.

Video Integration. Is the ability to support video protocols and dynamically allocate B-channels in the PRI pool for videoconferencing calls.

PBX Integration. The ability to allocate a fixed number of B-channels from the PRI pool to connect to a PBX as voice trunks using manufacturer specific protocols.

WAN interfaces. Analog; Switched 56; Frame Relay; ISDN BRI; ISDN PRI; T1

Digital Modems. Integrated digital modems allow a single remote LAN access server to support both analog and digital users. They also allow a smooth migration path as more and more users decide to make the move from analog to digital access lines. Digital modems work by taking the Pulse Code Modulation-encoded digital data steams sent by analog modem users, converting them to their original analog waveform and then performing the necessary demodulation. Digital modems also convert outgoing analog signals to analog waveforms and then into PCM data streams, allowing for transport over digital facilities. Key to reducing errors, external devices cannot manage and secure.

6. Network Security: Issues and Solutions

Security Planning

Network security is one of the most important issues to consider when you draw up your telecommuting plan. If your company has security policies and procedures in place, follow them. If it doesn't, draft your own telecommuting security policy and present it to your management for approval.

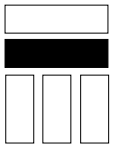
Be sure you understand your network security needs before you draft your security policy. Is your company in a high-risk business where industrial competitors or foreign concerns may be interested in your data? Would you incur legal liability if certain network data was stolen or lost? Are you possibly at risk from pranksters or dishonest or disgruntled employees? Perform a risk assessment to determine how vulnerable your data actually is to security breaches and to decide which network resources need protecting.

Ultimately, the amount of security you need will depend on how critical your network resources are to the operation of your business, the value you assign to those resources and the likelihood that they will be compromised. Is it likely that a competitor would break into your network and steal your customer database? If they did, how much would your company loose in sales revenues? Based on answers to questions like these, decide how much you're willing to spend on the security mechanisms that protect your network resources.

Remote Access Security

Chances are, your company will reap substantial benefits from telecommuting. Yet along with the benefits of telecommuting come increased security risks caused by opening your network to remote access.

The measures you're currently using to guard against security breaches at your corporate worksite are inadequate for securing your network resources in a telecommuting environment where users are not under your direct control, equipment is located in unsecured home offices and communications links are vulnerable to snooping.



Whether your company is public or private, whether your telecommuting implementation is large or small, the security solution you choose should:

Be largely tranparent to users. Users will go to great lengths to undermine security methods that are difficult to use. To make sure that doesn't happen, choose a security solution that makes logging on from a home office as easy as logging on from a workstation that's physically attached to the corporate LAN.

Provide ease of administration. The system you choose should be easy to set up, and should let you add and change users' security profiles easily, down the line. Telecommuters should be able to access multiple servers or subnets without being added to the system multiple times and use the same password to access resources anywhere within the network.

Provide adequate security. A security system should authenticate users, protect the network communications link from eavesdroppers and protect network resources from unauthorized access.

Security Options

Following are descriptions of the the most commonly-used security solutions: restricted access, incoming call ID, callback, PAP, CHAP, dynamic password authentication servers. They are 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 into your central site access equipment a list of remote node addresses (a PC address) that can dial into the network. Incoming calls from an address that is not on the list are rejected.

Advantages: Protects against accidental access by users dialing an incorrect phone number.
Disadvantages: Validates the equipment, not the user, so stolen equipment can be used to gain network access.

Incoming Call ID. This security method checks a telecommuter's authorized phone number which is programmed into the central site equipment against the phone number provided by the telephone company's network switch when an

access attempt is initiated. 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 access equipment must also support incoming call ID.

Advantages: Very secure, since defeating it requires tampering with the phone company's central office switch.
Disadvantages: This service is not available in all areas.

Callback. With callback, a telecommuter dialing into a terminal server or remote LAN access server must identify themselves with a password or identification number. The server then automatically terminates the connection and calls back the user at a telephone number that has been programmed into the server.

Advantages: Reliable for verifying a call from a particular site, such as a telecommuter's home.
Disadvantages: 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 Internet Engineering Task Force 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, but PAP does not encrypt the ID number or password as it travels across the network link.

Advantages: Password database is encrypted.
Disadvantages: Password is transmitted in the clear, making it very easy to snoop the line and pick up passwords.

CHAP. When a telecommuter dials into a server that uses Challenge Handshake Authorization Protocol, the server sends a random challenge (key) that the software in the telecommuter's modem, bridge or router uses to encrypt the password and return it to the server. Since CHAP encrypts the password when it travels across the network, snooping is very difficult.

Advantages: Secure against eavesdroppers.
Disadvantages: Since CHAP's password database is in plain text form it is vulnerable to snooping; as is the same with PAP.

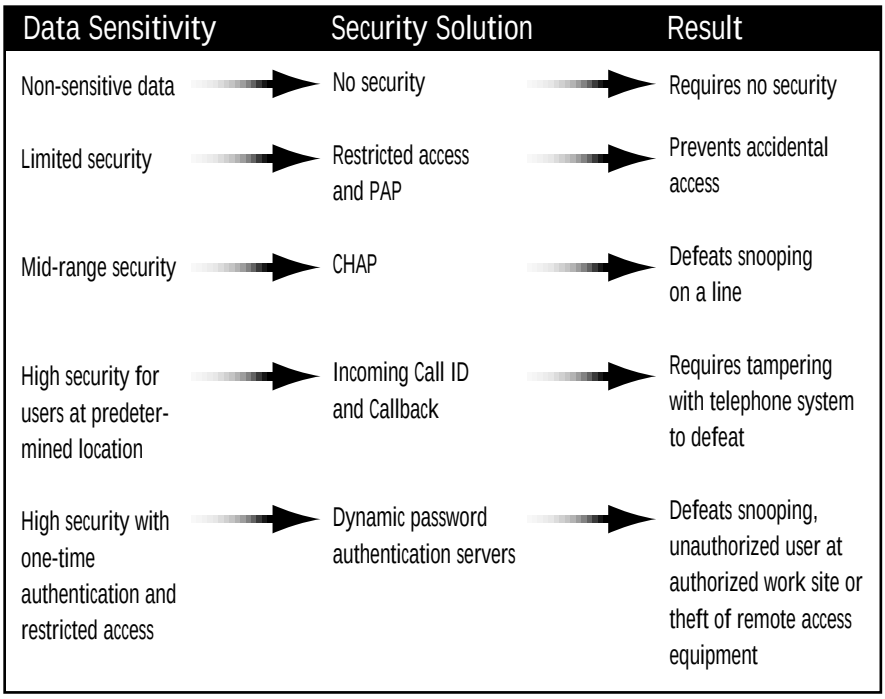


FIGURE 12
Network Security Methods

Dynamic Password Authentication Servers. These are third-party products which consist of software that runs on a UNIX machine and two-factor password generators that generate dynamically-changing passwords. Password generators can be software-based or hardware-based "tokens" the size of credit cards that telecommuters carry with them. Both kinds of password generators use two-factor authentication, a method that requires the user to provide something they know (a password or personal identification number) and something they have (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 only a 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 a Data Encryption Standard (DES) encrypted password good only for a single use.

Advantages: Harder to defeat than other security methods since passwords are dynamic; good for traveling workers who are not statically located and may use different computer equipment.
Disadvantages: Third-party products may cause compatibility problems in multivendor environments unless managed by RADIUS.

Dynamic Password Authentication Server Vendors

- *CryptoCARD, Inc./Buffalo Grove, IL.*
- *Digital Pathways Inc./Mountain View, CA.*
- *Enigma Logic Inc./Concord, CA.*
- *Lee Mah DataCom Security Corp. /Hayward, CA.*
- *Security Dynamics Inc./Cambridge, MA.*
- *SmartDISK Security Corp./Naples, FL.*

RADIUS: An Emerging Security Administration Standard

A protocol called RADIUS (Remote Authentication Dial-In User Service) from Livingston Enterprises Inc., now in the Internet Engineering Task Force standards-definition process, provides management services to authentication servers on a distributed network.

RADIUS functions as an information clearinghouse that stores authentication information about all of a network's users as well as complete user profiles consisting of access restrictions, destination-specific routing, packet filtering and billing information. Used in conjunction with Kerberos, CHAP, Netware Directory Services 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.

When users request access to a RADIUS-managed network, their request is passed directly from the remote LAN access server that answers the call to the RADIUS server (See Figure 13). The RADIUS server looks up the user and passes his authentication request to the authentication server that contains information about that user. Once the user has been authenticated, the RADIUS server passes the authentication information back to the remote LAN access server, along with user profile information contained in the RADIUS database. The user is then granted access to the network according to the parameters contained in the RADIUS profile.

RADIUS performs two important functions. It simplifies security administration by allowing a central database to manage authentication services for all users on a network, regardless of their location. It also allows remote access products to interoperate with third-party security systems from different vendors on the same network.

In order to take advantage of RADIUS' capabilities, look for password authentication server vendors and central site access equipment vendors that are incorporating support for this emerging standard into their products.

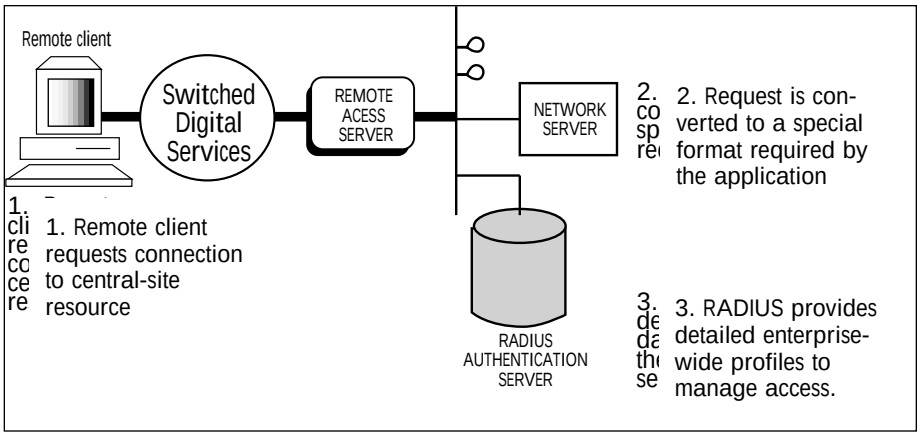
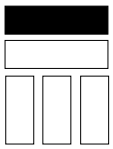


FIGURE 13
How RADIUS (Remote Authentication Dial-In User Service) Works



7. Managing and Supporting Your Telecommuters

Putting computers and access equipment in the hands of hundreds — or thousands — of telecommuters in physically remote locations introduces a whole new level of complexity to the job of managing your company's network. Make sure you can manage your telecommuters with the same tools and procedures you are already using to manage the network equipment and workstations in your corporate office environment.

A standards-based network management system is your best bet. If you're already using a proprietary scheme to manage remote users, check to see if it's compatible with other protocols you are running on your network, can be integrated effectively under your overall management umbrella and can scale to support more users as your telecommuting program grows.

Remember: the decisions you make now about managing your telecommuters will impact your network's performance for years into the future. Look for a management system that provides operational functions such as troubleshooting, general diagnostics, information about dial-in and dial-out activities including protocol errors, number of data packets sent and successful and unsuccessful logon attempts. It should also provide administrative functions including accounting, hardware and software inventory, virus protection, diagnostic tools and software distribution.

Network Management Options

Two standards-based network management systems are widely used today:

SNMP. Simple Network Management Protocol is a defacto standard for managing devices on a network. Today, most remote access equipment is SNMP-compatible, which means that it can be managed by SNMP-based network management systems such as SunNet Manager or HP Open View under the same umbrella as the devices on the rest of your network.

Telnet. You can also manage your telecommuters using Telnet, a straightforward tool designed specifically for managing remote connections. Installed on a central site management workstation, Telnet software, a part of the TCP/IP protocol, works by establishing a "virtual terminal" session with a telecommuter's computer over a wide area link. This allows you to remotely perform configuration, diagnostics and other control functions that otherwise could only be performed by a locally-attached terminal.

Custom Management Solutions. Many vendors offer proprietary methods protocols and management applications to manage their equipment. Still other innovative vendors have devised ways to access their equipment for management via Telnet over their proprietary management protocol. This is done to provide the same manageability features yet avoid higher manufacturing costs imposed by the memory needs of SNMP and Telnet.

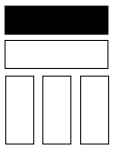
Home Office Access Equipment Management Features

Some home office access equipment contains special remote management features. Check for these useful features before you make a buying decision.

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

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 particularly useful in the telecommuting world,\ where traveling to a telecommuters' home 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 constantly reestablishing a network connection and saves costs by only establishing a connection when needed.



Training and Supporting Your Telecommuters

Part of a network manager's responsibility involves training telecommuters to use their new equipment before they start telecommuting, and providing them with technical support afterwards.

Thorough training is essential, since a simple problem like an improper password sequence or missing printer driver may result in hours or even days of missed work. According to Gartner Group, one hour of training your telecommuters on equipment and software can save as much as five hours of technical support later.

Also make sure to arrange for service contractors who can service equipment at a telecommuter's location and handle any support issues that your help desk cannot resolve.

Just as important as training is making technical support available to your telecommuters.

At the beginning, you may have to spend considerable time setting up telecommuters' accounts, passwords and security files. After that, most companies find that telecommuting does not require them to increase their support program significantly.

Some restructuring of your support program may be necessary, though, to accommodate your new telecommuters. Extending your support hours or rescheduling personnel to support users working after business hours or in different time zones may be in order. You may also encounter some new support issues, such as traveling professionals in hotel rooms who must access your network through different types of PBX equipment.

Appendix A: Telecommuting Scenarios

Scenario 1: A Small Company with a Single Location: Remote LAN Access

The majority of telecommuting programs being set up today are in small companies like this one. For many of the users in these companies, modems and analog phone lines are still adequate. But some user's bandwidth requirements are increasing and new digital services like ISDN are becoming widely available. Network managers at companies like these must choose a telecommuting strategy that will accommodate modem users today but allow for changing user requirements and the migration to an all-digital environment within several years.

Telecommuting Needs:
Number of locations: 1
Number of telecommuters: 15-25
Types of traffic: e-mail; file transfer; database access
Frequency of data usage: Low to medium
Typical distance from office: Less than 30 miles

In an effort to increase productivity and provide its employees with a more flexible workstyle, this small firm with 50 employees is planning to implement a telecommuting program.

During the assessment of its telecommuting needs, the firm identifies three different categories of telecommuters: attorneys who will be telecommuting just one day a week or working after hours who primarily need access to e-mail and small files; attorneys who will work from home more than one day a week and need to perform database research and download large legal documents; and administrative staff who will need access to spreadsheets and database files from their home computers.

Already installed on the law firm's LAN is a terminal server that supports incoming modem calls from customers, attorneys who travel on business, and a few members of the law firm who already telecommute or work at night.

Telecommuting Solution:
Services:
Access Lines (Home Office Users): Analog; ISDN BRI; Switched 56
Access Lines (Central Site): ISDN BRI's

Equipment:
Home Offices: V.34 modems; Pipeline 25 ISDN; Pipeline 50 LS56
Central Site: MAX 800 Remote LAN Access Server (supports all telecommuter services)

To accommodate this variety of users, the firm decides to replace its analog terminal server at its corporate site with an Ascend Pipeline 800 WAN Access Switch equipped with eight digital modems. All analog and digital traffic comes in over the BRI lines.

Access equipment at the telecommuters' sites will vary. The attorneys who plan to telecommute only one day a week will continue to access their corporate LAN using modems and analog phone lines at speeds varying from 14.4 to 28.8 kbit/s. The attorneys who spend more time at home and need to download large files will achieve data transfer speeds up to 128 kbit/s by installing ISDN BRI lines in their home offices. The two administrative staff members who plan to telecommute – the controller and the network manager – also opt to install BRI lines to their homes. The network manager installs a BRI line; the controller, who lives in a suburb where ISDN is unavailable, installs a switched 56 access line.

Savings and Benefits:

- The ISDN lines now handle all incoming traffic
- Replacing terminal servers and modems with a single remote access switch simplifies management and support
- Home office equipment is easy to set up and manage
- Pipeline 25 saves on extra lines and line charges being required for work at home.
- Central site equipment can support more users and migrate to an all-digital environment if the firm's telecommuting needs expand.

Scenario 2: A Medium-sized Organization with Remote LAN Access and Internet Access needs

Telecommuting Needs:
Number of locations: 1
Number of telecommuters: 150-200
Types of traffic: e-mail; file transfer; database access, graphics, Internet access
Frequency of data usage: Low, medium, high
Typical distance from office: Up to 50 miles

A rapidly-growing, high-tech corporation with corporate headquarters in Silicon Valley decides to set up a telecommuting program so that its employees with demanding work schedules can access the corporate LAN from home during the day, during evening hours and on the weekends. The new program is also designed to comply with the State's Clean Air Act that mandates that the company reduce its number of automobiles by 20% within the next few years. About half of the companys' 400 employees, including executives, technical writers, computer programmers and sales staff, are eligible for the program.

A dozen or so employees – mostly programmers – have already set up home offices and access the corporate LAN using ISDN or Switched 56 access lines that terminate on standalone DSU/CSUs and ISDN terminal adapters at the central site. Traveling sales staff also access the LAN using laptops and modems.

Before: The company was maintaining a hodge-podge of separate access lines – analog, Switched 56 and ISDN BRI – and separate access devices – modem racks, ISDN terminal adapters and CSU/DSUs – to support its telecommuters and traveling workers. Managing all of these different services and equipment and maintaining tight network security was putting a strain on the company's network management staff.

After: The Ascend MAX 4000 Remote LAN Access Server consolidates incoming calls from analog, digital and Frame Relay callers onto a single access line. The MAX eliminates the need for separate access lines and separate access equipment and simplifies and improves network management and security.

Telecommuting Solution:
Services:
Access Lines (Home Office Users): Analog; ISDN BRI; Frame Relay
Access Lines (Central Site): ISDN PRI

Equipment:
Home Offices: V.34 modems; Pipeline 50 ISDN; Pipeline EtherFrame, Pipeline 25
Central Site: Ascend MAX 4000 Remote LAN Access Server (supports all remote access services)

Sales staff who travel frequently will continue to access their corporate network resources using high-speed modems but now come in over a PRI line, and are processed on digital modems. Technical writers, executives and administrators who frequently transfer large files such as presentation graphics or spreadsheets over the network frequently get ISDN BRI access lines installed in their homes. Computer programmers with heavy usage requirements who are online to the network nearly eight hours a day find they can save money by switching from ISDN BRI access lines to 56 kbit/s Frame Relay circuits.

The company sets up a gateway to the Internet through the MAX so that telecommuters dialing in to the corporate LAN can access LAN resources and the Internet with a single phone call.

Savings and Benefits:

- Internet gateway simplifies telecommuter access to the Internet.
- Integrating all incoming traffic onto a single PRI line eliminates the need for multiple access lines at the central site and saves money on access charges.
- Replacing multiple DSU/CSUs, ISDN terminal adapters and modem banks with a single remote LAN access server makes management and support easier.
- Up to 48 digital modems in the MAX support traveling users and customers in a single access device with digital reliability.

Name:
Company:
Telephone Number:

Telecommuting Program Requirements Worksheet

The purpose of this worksheet is to help you determine your telecommuters 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 telecommuting program, fax a copy of this completed form to Ascend Communications at (510) 337-2668. One of our telecommuting 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 SW56 lines? Today_____ Planned _____
   d. How many Frame Relay circuits? Today_____ Planned _____

   * Leased line connections are not supported in this analysis.

Central Site Circuit Requirements

4. Analog Circuits
   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 circuits needed (multiply number of users by percentage): _____
5. ISDN Circuits
   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 circuits needed (multiply number of users by percentage): _____

6. Switched 56 Circuits

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 circuits needed (multiply number of users by percentage): _____

7. Frame Relay Circuits

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 circuits needed (multiply number of users by percentage): _____

10. Central Site Circuit Requirements

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

b. ISDN circuits (from 5c): _____

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

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

e. Total _____

f. Divide total by 23 (number of circuits in a PRI or T1) = ÷23_____

g. Total number of PRIs or T1s required: _____

11. Central Site Equipment Requirements

a. Divide the total from 4c by 8.
This will give you the total number of digital modem cards _____

b. Divide the total from 4c by 48.
This will give you the total number of Ascend Max 4000's required. _____

NOTES

NOTES

NOTES