TCP/IP: The Best Protocol for Remote Computing

White paper developed for WRQ by Rysavy & Associates.

Visit http://www.wrq.com for additional information about WRQ.

Introduction

Remote computing is transforming the way companies conduct their business and the way employees do their jobs. In this white paper we explain what remote computing is, why its use is growing, what it means to your organization, and how you can take advantage of its benefits. In particular, we demonstrate the advantages of letting remote users use TCP/IP to gain access to the corporate network.

Remote computing refers to computing by employees who work at locations other than your corporate premises and who access your computer networks and services. There are some fundamental differ-ences between a worker using a high-speed network connection while on corporate premises and the same worker dialing into the network with a modem. Connection speed alone is different by a factor of more than 100. Other important differences exist as well. Once you understand these differences and are aware of the techniques and tools available, you will find it straightforward to develop a remote computing solution of your own.

The Distributed Nature of Computing Today

There are both societal and business trends driving the adoption of remote computing. From a social perspective, workers want and expect more flexibility in how they do their jobs. For example, some workers prefer to have dinner with their families and then work at home, rather than work late at the office. As workers and companies invent new work patterns that include working at the office and working from home, people's job satisfaction increases, companies reduce costs by needing less office space, and companies meet government mandates to reduce the amount of commuting. Meanwhile, the number of business travelers who need to connect to corporate information while on the road is increasing.

Mobile computers are becoming more common. Many workers use a mobile computer either to supplement their desktop PC or as their only computer. As a result, it is becoming easier for workers to take their computers on the road or home with them. Furthermore, an increasing number of families have PCs, which are also available for working at home. And remote users have an increasing number of connectivity options, including high- speed modems, ISDN (Integrated Services Digital Network), cable modems, and other new technologies. What remote workers are finding, however, is that to work productively, they need access to their corporate network. See Figure 1.

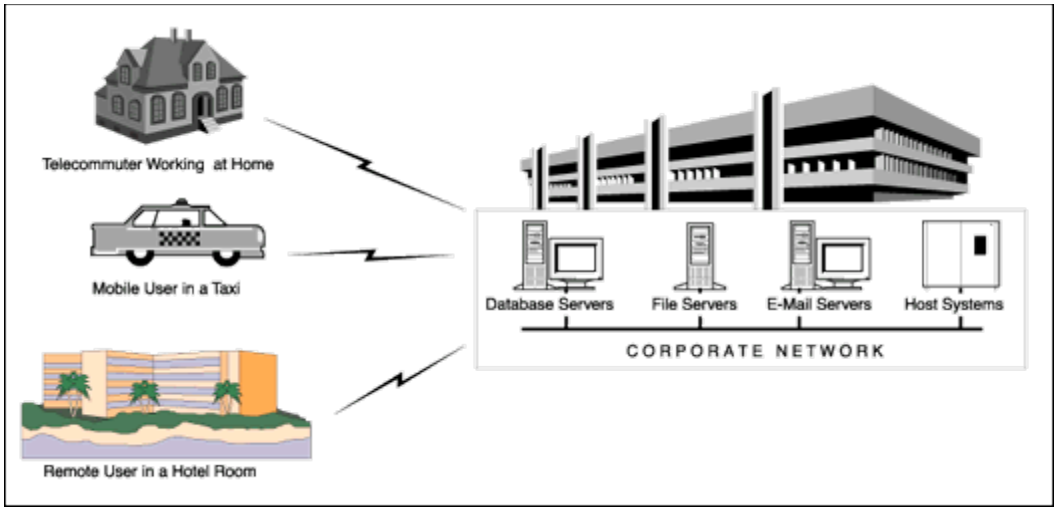

Figure 1: Increasing, workers want to access their company's network from anywhere

Corporate networks are becoming increasingly complex. Legacy systems consisting of hosts and terminals now coexist with LANs. File sharing systems on LANs are evolving into client/server systems. Companies spread across multiple locations are interconnecting their LANs and are also connecting to the Internet. Remote users need access to the full range of these corporate computing resources.

Fortunately, complete remote computing solutions are now available that allow both technical and non-technical people to access the corporate network easily and efficiently. In many cases, workers can use the same applications with the same user interfaces whether they are in the office or working remotely. It is no wonder that the population of remote computing users is growing so rapidly.

Remote Computing Overview

The term "remote computing" refers to all computer users working away from the main office. In this paper we cover issues affecting remote users in the following categories:

Telecommuters. These workers work part time or full time from their homes.

Mobile Employees. These workers work from a variety of locations, including cars, trains, airports, hotels, and other companies. Examples include field workers, such as repair technicians, mobile salespeople, and traveling executives. While mobile workers use many of the same applications as other remote workers, they have some unique requirements. Specifically, they are more likely to use technologies that let them communicate from anywhere, such as wireless communications.

Alternate Work Site Employees. These workers work in centralized work sites that provide office resources, such as copiers, faxes, and meeting rooms. These sites are remote from the corporation and can support employees from multiple companies.

Figure 2 shows the elements of a remote computing solution used to support different types of workers.

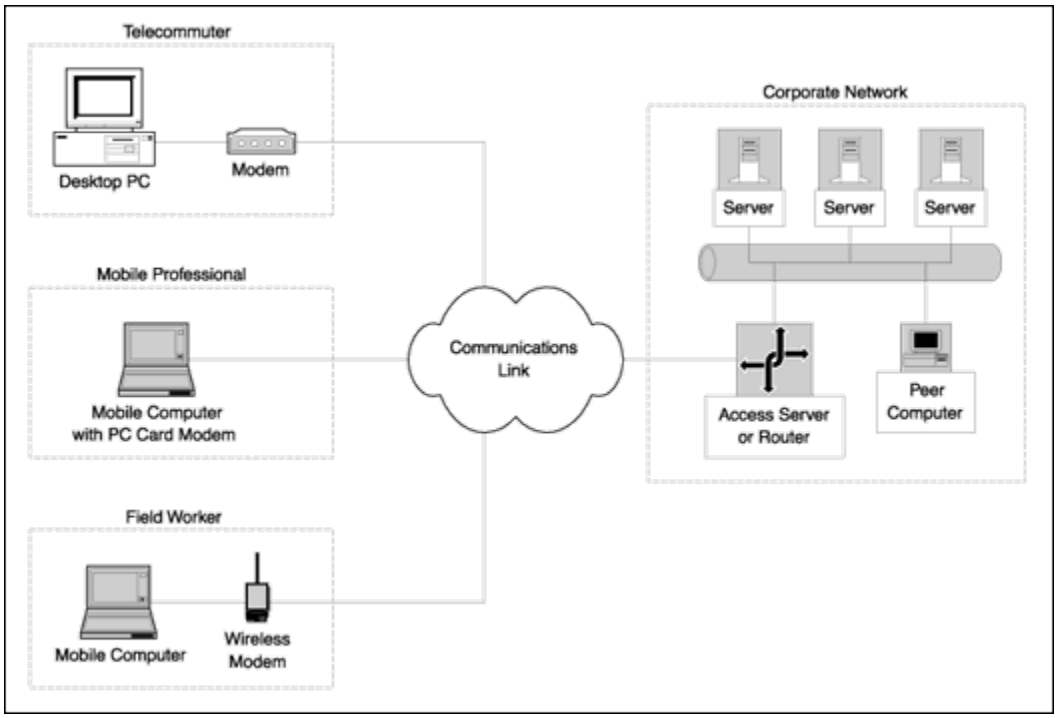

Figure 2: Elements of a remote computing solution

The principal elements of remote computing solutions include:

Remote Computer. Depending on the type of worker, this could be a desktop PC at home, a mobile computer, a specialized handheld computer, or even a personal digital assistant.

Networking Software. This is the software that allows the user to access the corporate network. When using the TCP/IP protocol stack, the software includes Serial Line Interface Protocol (SLIP) and/or Point-to-Point Protocol (PPP) drivers that allow the stack to communicate over wide-area links. TCP/IP is the only networking software that readily supports all categories of remote users.

Modem. Different types of users take advantage of different types of modems. A worker at home might use a desktop modem or ISDN adapter, a field worker might use a wireless modem, and a mobile professional might use a PC card modem for communicating over cellular or hotel room telephone connections.

Communications Link. The link is generally provided by a service provider, such as a telephone company. New communications options include ISDN, high speed data services over television cable, frame relay, and dedicated data connections.

Access Server or Router. This device connects the communications link to the corporate network. Access servers support telephone connections over phone lines, including digital ISDN connections. Smaller access servers typically can service 1 to 8

remote users simultaneously, whereas an enter-prise server might support 100 users. A common guideline for initial deploy-ment is to provide 1 external port for each 10 remote users. If the connection is a network connection to a network such as the Internet, the access server is referred to as a router.

Peer Computer. This is a computer on the cor-porate network that a remote user might want to access. It could be the worker's own office computer or a fellow worker's computer on a collaborative project.

Server. This is the system the remote worker needs to access. Its services include host-based applications, files, databases, e-mail, printing, faxing, and authentication.

There are a number of differences between working remotely and working at the company. Because the communications link for the remote connection is much slower, many network applications and pro-cedures operate more slowly. Security is an issue, since intruders may attempt to break into the cor-porate network through the access server. Additionally, support is more difficult since support personnel cannot easily get to the remote worker's computer. However, with the right approach, you can readily overcome these challenges.

The single element that determines the most broadly what services a remote user can access with what ease is the networking software used. As we discuss in the next section, TCP/IP is clearly the best choice for giving remote users the greatest number of communications options.

Networking Protocols and Remote Computing

Before you can develop your approach to remote computing, you must carefully identify all the resources and services that a remote user needs to access. These could include mail servers, file servers, database servers, fax servers, hosts, peer workstations, the Internet, and even the worker's own workstation in his or her office.

As part of this process, you should identify all the applications that your remote users need to use. Some applications can run locally on the users' computers with no interaction with your corporate network, but other applications need to communicate with your network. To determine their communications needs, you must consider the networking protocols the applications use.

Some remote computing software products, like remote control or dial-up remote e-mail, come with their own communications protocols and drivers. But these are usually proprietary solutions that support only that particular product. In nearly all instances your workers can do more from their remote locations if you provide them with a general purpose networking solution.

The first step in providing a flexible networking solution is to identify which networking system you wish to extend to the remote worker. The most common networking systems used in corporate environments today are NetWare's IPX/SPX, NetBEUI, and TCP/IP. We examine these more closely below.

NetWare's IPX/SPX

NetWare is Novell's network operating system. It is based principally on the Novell IPX/SPX networking protocol, though NetWare also supports other protocols. Applications access the IPX/SPX protocol stack through either NetWare specific interfaces, Windows Sockets (WinSock), or NetBIOS. For dial-up and remote connections, users have the choice of using Novell's NetWare Connect (a NetWare Loadable Module or NLM), or third-party remote access servers that are usually based on PPP.

A remote computing solution based on extending the NetWare protocol gives users access to NetWare-based services, including file, print, and e-mail servers. But if users need to access other systems, such as UNIX-based client/server systems, IBM mainframe hosts, and the Internet, then NetWare is not the optimal approach. More important, the IPX/SPX protocols were designed for the high-bandwidth environments of LANs and are not efficient over slow wide-area links.

NetBEUI

NetBEUI is the networking protocol used by Microsoft and IBM networking products, including LAN Manager, Windows for Workgroups, and Windows 95. It uses NetBIOS as the interface to the applications layer. For dial-up connections, you have the choice of using either Microsoft's Remote Access Service (RAS) link protocol or PPP over the wide-area link. The access server can be a dedicated access server or a Windows NT server.

A remote computing solution based on extending the NetBEUI protocol gives users access to NetBEUI services including file, print, and e-mail servers. But as in the case of a NetWare-based solution, if users want to reach other types of services, they need to use a different approach. This approach is TCP/IP.

TCP/IP

Beginning as a government-financed research project in the 1960s, TCP/IP today is the most broadly used wide-area networking communications protocol, due in part to its being the core technology of the Internet. Because the TCP/IP protocol is so popular and considered the only open networking standard, network managers can choose from a large number of sources for interoperable software and hardware. These products, combined with advances in communications media, such as optical fiber and wireless data networks, yield an unprecedented set of choices for designing wide-area networks.

Compared with NetWare and NetBEUI, a remote computing solution based on TCP/IP offers users access to the broadest range of services on a corporate network, while providing comprehensive options for network management and security. TCP/IP also performs very well

over wide-area connections since it was designed from the beginning for these types of connections, unlike other protocols, which were designed primarily for local-area networks.

TCP/IP, the communications network standard of the 1990s, is not static; rather, it is evolving to support new requirements. For example, IP version 6 increases the address space so that every imaginable device on the planet can have its own IP address, including your toaster. Companies that previously used other networking protocols are quickly upgrading their products to operate over TCP/IP. For heterogeneous networks comprising a mix of hosts and client/server systems, TCP/IP is the common denominator.

Applications interface with TCP/IP protocol stacks using WinSock in a Windows environment. To support remote workers with dial-up or other point-to-point connections, you have the choice of using SLIP or PPP protocols. SLIP is a simple encapsulation method that works only for TCP/IP, whereas PPP is more flexible and supports other networking protocols as well.

Given TCP/IP's ascendancy in both local- and wide- area networks, and given that one goal of remote computing is to access a wide variety of resources, we can see why TCP/IP is the key component of many remote computing solutions. As we explore in the remainder of this white paper, TCP/IP offers the following benefits to remote computing:

- Coexistence with NetWare when users need to use both TCP/IP and NetWare.
- Use of NetBIOS applications.
- Access to host systems.
- Ability to support both remote node and remote control approaches.
- Ability to operate over various communications links, including wireless connections.
- Seamless access to the Internet.
- Secure and safe communications using established security tools.
- Ready support from the company's network support staff, thanks to standardized network management tools.

Using the TCP/IP Protocol

To minimize the difficulty of configuring and managing the remote workstation, we recommend that you use as few networking protocols as possi-ble, ideally only one. Below we discuss how to use TCP/IP side by side with NetWare; how to use TCP/IP instead of NetBEUI with NetBIOS applications; and how to use TCP/IP to access host systems.

TCP/IP and Novell NetWare

Many companies today use Novell NetWare with its IPX and SPX protocols. Many of these companies today are also using TCP/IP over their networks. What if your remote users need to

use both TCP/IP and IPX/SPX? The answer is to use products that support both IPX and IP networking protocols over a PPP link. With these products, you install an Open Datalink Interface (ODI) driver that supports both a TCP/IP and an IPX/SPX protocol stack on the remote workstation. At the corporate site, you install either an NLM on a NetWare server or a dedicated server, such as a Shiva LANRover, that supports both IP and IPX protocols.

Keep in mind that NetWare protocols are not ideal for dial-up connections. You will need to optimize logon procedures and carefully select what applications your remote workers use.

If remote workers are trying to access NetWare file servers, an alternative approach is to use an IP connection to a workstation on the corporate LAN that acts as a gateway to a NetWare file server. We look at this approach in more detail in the next section.

TCP/IP and NetBIOS

NetBIOS is not a networking protocol but a general purpose networking interface between applications and communications protocol stacks. NetBIOS is currently used with TCP/IP, NetBEUI, IPX/SPX, XNS, VINES, and Open Systems Interconnect (OSI).

One important reason to consider NetBIOS is because it is supported by both Microsoft's and Novell's networking products. Using the combination of NetBIOS and a TCP/IP stack, a remote client can connect to servers running Windows 95, Windows for Workgroups, or Windows NT. And if the server has access to other services on the LAN, then these other services can be made available to the remote client as well. The advantage of this approach is that you do not have to install a separate networking protocol such as NetBEUI or NetWare on the remote workstation.

Figure 3 illustrates how a remote worker might access a NetWare file server using this approach. In the figure, the Windows Network Services include RAS. Users can also take advantage of NetBIOS over IP to access files on peer workstations.

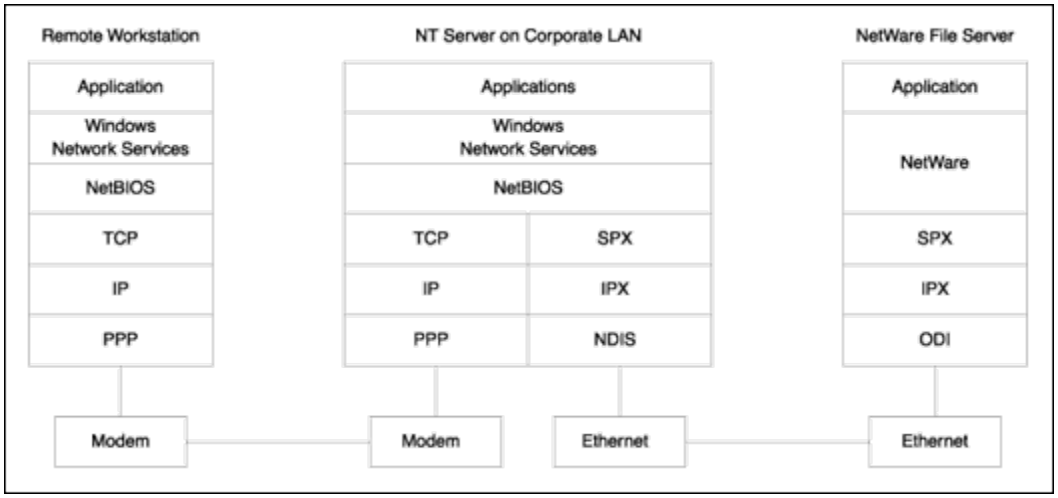

Figure 3: Accessing NetWare file server via intermediate server

TCP/IP and Host Access

Some of your remote workers may need to engage in host/terminal sessions with host systems from companies such as IBM, Digital, or HP. Host-based applications are a good fit for remote computing because both the application and the data reside on the host. The only information sent to the remote workstation is screen updates, making sessions well suited for slower links.

Many host systems support Telnet connections, which use TCP/IP for communicating between the host and a remote PC. On the remote PC, you run terminal emulation software, which emulates the terminal type for that host. Figure 4 shows the layers involved in a remote connection to a host.

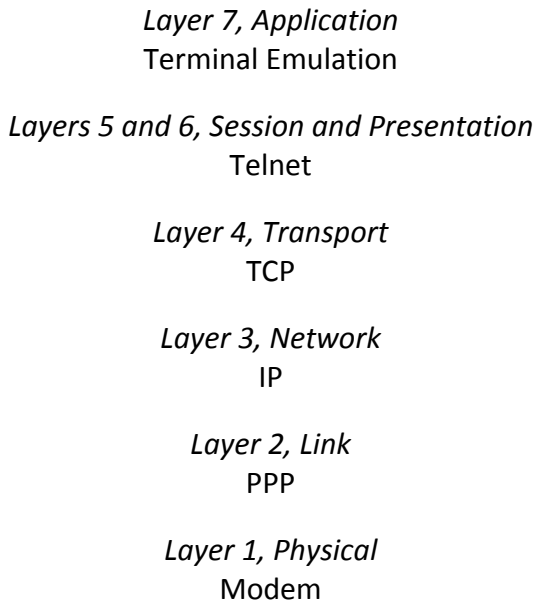

Figure 4: Using terminal emulation with Telnet.

The protocol for TCP/IP terminal communications with IBM hosts is TN3270 for IBM mainframes, including system 390, and TN5250 for IBMís AS/400 midrange systems. If the host does not support TCP/IP directly, there are gateways available with which the remote workstation can communicate using TCP/IP. See Figure 5.

For remote workers who need mainframe connectivity, you should consider TN3270E, which is an enhanced version of TN3270. TN3270E offers a number of advantages, including the ability for the host application to print at the remote location.

Telnet sessions can also be used to communicate with Unix servers and VAX hosts. In the case of HP 3000 hosts, you need to use a protocol called NS/VT.

Users can also use modems to dial directly into asynchronous host gateways, but these sessions are based on proprietary protocols, and do not give users access to as many other network-based resources as TCP/IP.

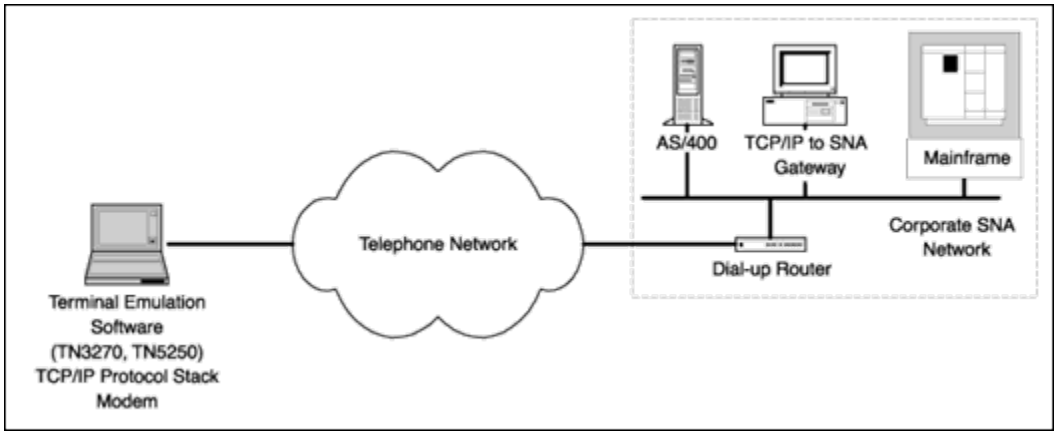

Figure 5: Accessing IBM hosts via a gateway.

Other Considerations with TCP/IP Remote Computing

Once you have chosen TCP/IP as your networking protocol, there are a number of other items you should consider when designing your remote computing solution. These include whether to use remote node or remote control; what communications link to use; whether the remote worker needs access to the Internet; what security measures to use; and how to manage remote network connections. In this section, we examine each of these items.

Remote Node versus Remote Control

The two most common approaches of making the corporate LAN available to remote users are remote control and remote node. Both of these approaches can take advantage of TCP/IP network connections.

With remote control, the remote user's PC dials and connects to a PC on the LAN. Both the remote PC and the PC on the LAN are running remote control software, which makes the remote PC operate like a dumb terminal attached to the local LAN PC where the application runs. The remote user's keystrokes are transmitted to the LAN PC, which responds to them as if the user were seated at the PC typing them in right there. Simultaneously, the LAN PC's display is transmitted to the PC of the remote user, who sees exactly the same display as on the LAN PC. In this way, the remote worker takes over and controls the LAN PC. Remote control has some good usages, but it typically requires more hardware at the corporate LAN to support remote workers than remote node. Though some remote protocol products use proprietary protocols over modem links, others can operate over network connections including TCP/IP networks.

The other approach is remote node, where a remote user's workstation is a full network node, using the same networking protocol stack as other workstations on the LAN. The difference is that rather than the protocol stack communicating with a network interface card such as an Ethernet card, it communicates with a modem or other wide-area link. See Figure 6.

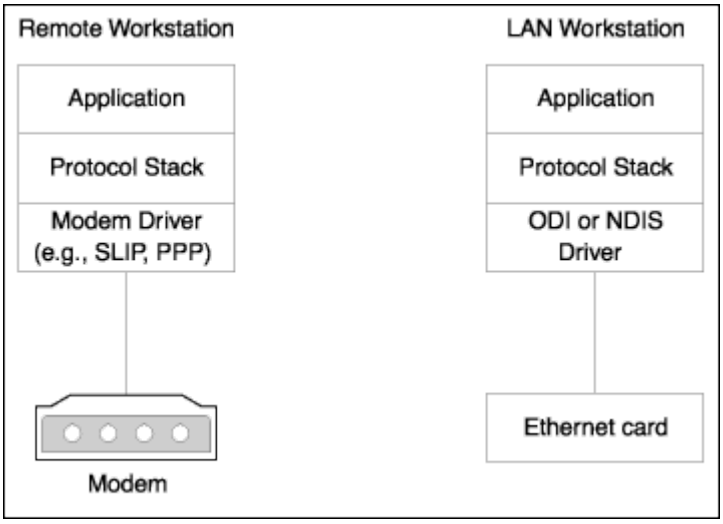

Figure 6: Comparison of remote node and LAN workstations

The advantage of a remote node solution is that the remote user has a work environment identical to a local LAN userís. The disadvantage is that performance can be slower over a modem link. Operating NetWare from a remote node is particularly slow. In comparison, TCP/IP is quite well suited for remote nodes, partly because it comes with well-defined modem protocols including SLIP and PPP, and partly because TCP uses an efficient windowing protocol that allows it to transmit a series of datagrams (packets) before receiving acknowledgment that prior datagrams were received correctly. A remote node solution based on TCP/IP gives your users access not only to servers on the LAN but also to mainframe and midrange hosts.

One important consideration is that while it may be common to load an application from a file server when the workstation is located on a LAN, the same operation is much slower over a remote link. Keep all your applications on the remote computer's hard drive, and use the remote link only to access data.

Whether you use remote control or remote node depends on your application, but in either case you can take advantage of TCP/IP network connections.

Communications Links and Modems

Most remote workers today use conventional modem connections over dial-up circuits, but many new options are becoming available. All of these options support TCP/IP communications.

One option that is now starting to grow after years of dormancy is ISDN, offering data rates of 64 Kbps per channel, and allowing two channels to be combined for a rate of 128 Kbps. With

compression, users can obtain up to 500 Kbps of throughput. ISDN is very well suited for remote computing. Many ISDN cards appear like network cards to the protocol stack, and come with an NDIS or ODI network driver, or support the new WinISDN interface. Though a higher speed connection like ISDN may cost more, it may well pay for itself in higher productivity, especially if the worker has to exchange a lot of data with the corporate LAN.

To communicate over ISDN, the remote worker needs an ISDN adapter, which is either an external device or an internal card. The computer connects to an external ISDN adapter either via a serial port or via a network connection using Ethernet. TCP/IP operates over ISDN connections using the PPP protocol.

Another option that will soon be available is a cable modem, a special modem that connects workstations to the cable television network. See Figure 7. Cable companies are testing data rates from 1 Mbps to 10 Mbps. One restriction is that cable companies will primarily be offering TCP/IP-based data access to the Internet, so that a remote worker who wants to connect to a corporate LAN will have to do so via the Internet. As we will discuss further, connecting to the corporate network through the Internet raises security concerns.

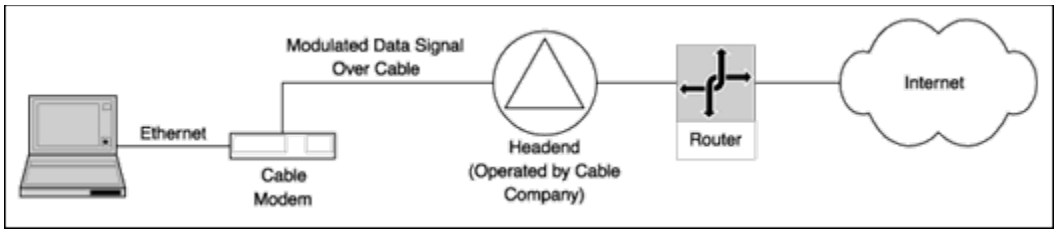

Figure 7: Using cable-based modems to access the Internet

More expensive alternatives include dedicated data connections, such as leased lines or frame relay. These are of interest only to power users who need to exchange very large amounts of data. The modems in this case are replaced by routers, Channel Service Units (CSUs), and Data Service Units (DSUs).

Mobile users should consider wireless networks. Cellular Digital Packet Data (CDPD) networks, available from a large number of cellular companies, offer TCP/IP-based communications over the cellular telephone network. These networks require special wireless modems. Another alternative for mobile users is to use a PC card modem that supports a direct connection to a cellular telephone. We discuss wireless links further in the next section.

Wireless Links

With wireless communications, users can conveniently communicate from almost any metropolitan location. The two principal methods include circuit-switched connections and packet-switched connections.

Circuit-switched connections are similar to conventional modem connections, the difference being that instead of connecting a modem to a telephone jack, the user connects the modem to a cellular telephone. This approach works well so long as the modem supports specialized

cellular communications protocols, the telephone supports data connections, and the cellular operator has deployed modem pools that translate between cellular protocols and conventional modem protocols. Fortunately, these items are all becoming broadly available, and users can enjoy reliable communi-cations of up to 14,400 bps. Users can also make circuit-switched connections using digital cellular networks, though currently service is mostly restricted to Global System for Mobile Commun-ications (GSM) networks in Europe.

In contrast to circuit-switched connections, using packet-switched connections the modem never places an actual call but simply sends and receives packets of data. The user pays only for the amount of data sent and received rather than paying for the amount of time connected.

There are a number of service providers offering nationwide packet data service today, but for remote computing the most important is CDPD, offered by most cellular carriers. CDPD networks route IP packets, transport data over radio channels at over 10 Kbps, and have a connection to the Internet. See Figure 8.

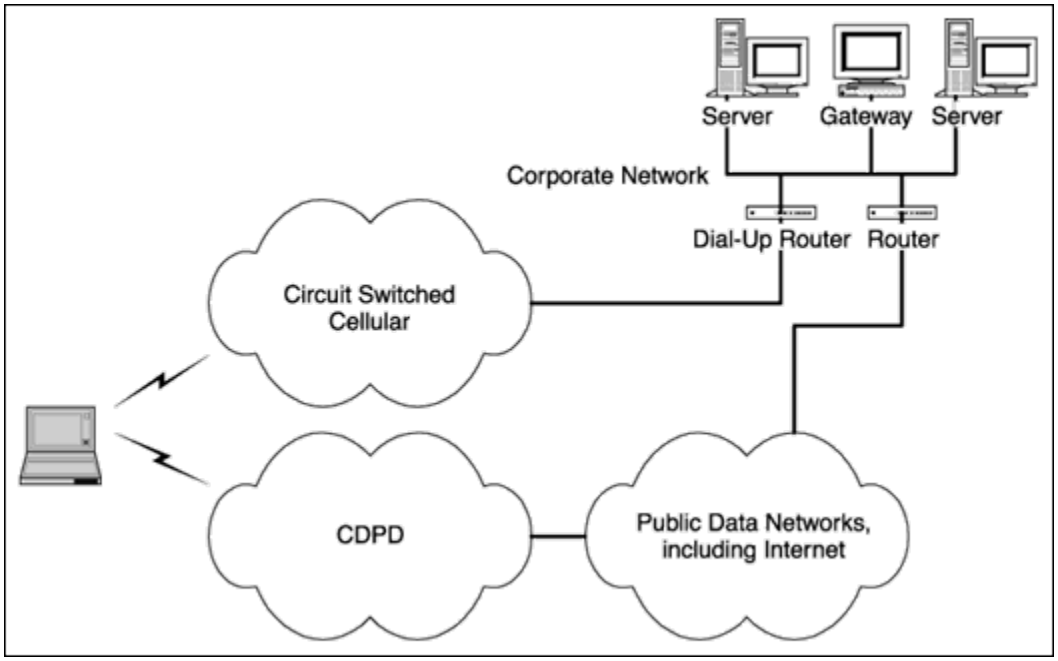

Figure 8: Wireless networks

To use TCP/IP over the CDPD network, you must choose a TCP/IP stack optimized and certified for use over CDPD. Such a stack optimizes communi-cations for faster throughput, minimizes communications overhead to reduce service costs, and includes specialized error recovery methods to handle the varying signal quality of wireless links. WRQ, with its Reflection networking software, is the industry leader in providing TCP/IP communications for CDPD networks.

The principal considerations today with wireless communications are cost and deployment. Circuit-switched communication is possible anywhere there is cellular coverage, and usually

costs the same as a voice call. CDPD is currently available in most major cities; costs range from 3 cents to 10 cents per kilobyte depending on the pricing plan.

For both circuit-switched and packet-switched wireless connections, TCP/IP is an excellent choice. In particular, it allows remote users to use the same applications and same networking protocol however they connect to the corporate network.

Internet

With the explosive growth of the Internet, it is worth considering the roles the Internet can play for remote computing. There are two cases:

- Accessing the Internet through the corporate connection
- Connecting to the corporate network via the Internet

In the first case, if your company's network already has a connection to the Internet, then a remote computing solution based on a TCP/IP connection automatically gives your remote users access to the Internet. Whatever Internet security measures you have in place for local users on the LAN should apply equally to remote users.

In the second case, the Internet is used as a way for remote users to access the corporate network. The biggest issue in this case is security. If remote workers can access your servers from the Internet, then so can potential intruders. Few companies have used this approach so far, but so long as you use security tools that provide adequate authentication and privacy, this approach has its merits, especially as more avenues become available for Internet access, including high speed data services over television cable and public Internet kiosks. Performance can also be a factor when using the Internet because IP traffic may have to traverse multiple intermediate nodes compared with a direct dial-up connection.

However you choose to incorporate the Internet in your remote computing solution, TCP/IP gives you the flexibility you need.

Security

Any solution that lets remote users access the network also makes your network potentially vulnerable to intruders. When developing a security policy, you will always confront a tradeoff between security and convenience: The more secure your network is, the less convenient it is for your users. As an analogy, a house with no doors or windows is secure but is not very convenient.

In general, the more services you provide for remote workers, the more careful you must be with security. For example, a dedicated dial-up e-mail server poses less risk than an IP router, and an IP router with password protected dial-up access poses less of a risk than a router connected to the Internet. Fortunately, there are an increasing number of effective off-the-shelf security solutions, such as firewalls, available for TCP/IP networking.

Security involves both protection against eavesdropping, called privacy, and protection against unauthorized users, called authentication. To authenticate TCP/IP users, several different approaches are available. One is Kerberos, a method whereby users authenticate themselves with a centralized authentication server, and then can access other servers. Kerberos, which works with applications such as Telnet and FTP, offers the benefit of a single logon procedure to access multiple servers.

For PPP links, including dial-up connections, two common authentication methods include Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). Between these two, CHAP is more secure because it does not send unencrypted passwords across the link.

Another security option is SOCKS, a flexible security method that allows applications to communicate across firewalls. With the number of security options for TCP/IP growing rapidly, you can implement a security policy that meets any need.

Network Management

In designing your remote computing approach, you need to consider how to manage your extended network. Since your users are remote, managing and supporting their systems can be more difficult: You can no longer just walk down the hallway to check on a user's workstation.

One question is whether to dynamically assign IP addresses to your remote users or to use fixed ones. The advantages of dynamically assigned IP addresses are that users can access your corporate network via multiple subnets and that you will need a smaller pool of IP addresses since only a subset of your remote workers will be connected at any one time.

You should consider TCP/IP stacks for the remote workstation that incorporate a Simple Network Management Protocol (SNMP) agent. The agent will allow you to collect network statistics from a centralized location.

Finally, look for TCP/IP stacks that have good diagnostic tools and that can capture system events. Some stacks will even log events, such as Windows problems. These tools will aid greatly in troubleshooting. In many cases users will be able to resolve problems themselves, and if they do report problems to network managers, they will be able to provide more detailed information.

WRQ and Remote Computing

WRQ is one of the leading suppliers of TCP/IP technology today. Moreover, WRQ is well known for high-quality products and its commitment to providing thorough and effective solutions, including excellent support.

WRQ's products do more than provide basic functionality: They are robust under demanding situations; they provide detailed diagnostic and management tools; and they are designed to integrate into a large number of different environments. In particular, WRQ's Reflection Mobile™ and other Reflection® products include enhancements that make them an ideal choice for remote users with modem or wireless connections.

Finally, WRQ is a leader in other enterprise connectivity technologies that can play an important role in your remote computing solution, including Intranet/Internet applications, PC X server software, and terminal emulation for UNIX, Digital, IBM, and HP hosts.