Payoff

Today's increasingly mobile work force requires occasional access to the corporate LAN. Network managers must decide whether the solution for their company is remote control access, remote node access, or a mix of the two.

Introduction

The remote LAN access market is considered by many industry analysts to be the next major networking frontier. By 1998, almost every major company will have a remote access capability to support the productivity requirements of an increasingly decentralized work force. The most common job functions that require remote access are sales, marketing, administration, management, finance, and accounting. According to International Data Corp., most remote users want to be able to access electronic mail and transfer text files. Almost half of all remote users want to transfer graphics files or need access to online services.

Only a few years ago, the most common approach to remote access was remote control, in which a user dialed into a PC at the office. The office PC then logged into a file server where the needed information was stored. The remote PC takes control of the office PC's monitor and keyboard, allowing the remote user to view and manipulate information, execute commands, and exchange files. Because it requires two PCs for every remote user, remote control can be an expensive and inefficient solution to set up and manage, especially when multiple users require remote access simultaneously.

A new class of products has emerged—remote node. Whereas remote control establishes a connection between two PCs and usually relies on dial-up connections by modem, remote node relies on a remote access server that is set up and maintained at a central location. Many remote users, all at different locations, can thus share the same resources. Remote node connections to the remote access server can be established by dial-up bridges or routers or modems. Dial-up bridges and routers serve branch offices; modems are typically used by mobile workers and telecommuters.

Remote Node Versus Remote Control

Until recently, remote control was the remote access method of choice. However, with the introduction of powerful, portable notebook computers, affordable fast modems, bridges and routers, more advanced compression algorithms, and client/server applications, remote node is gaining popularity. With remote node, multiple PCs at different locations dial into the headquarter's server, which enables them to operate as though directly attached to the corporate LAN. Both methods are illustrated in Exhibit 1.

Remote Node and Remote Control Access

Remote Control: A Software Solution

Remote control is essentially a software solution. Special remote control software is required to run on two computers: the remote system and the host system. The remote
system can be a branch office PC, a home PC, or a portable computer whose location changes daily. The host system can be any computer attached to the LAN that is configured for remote access.

With remote control, mobile workers using laptops or branch office workers using workstations take control of PCs on the corporate network. All the user's keystrokes and mouse movements are sent to the corporate PC and the image on that screen is forwarded back to the laptop for display. It is as if the user were sitting in front of a network-attached PC. Remote users do not need copies of programs on their computers, since the programs actually run on LAN-attached workstations at the corporate headquarters.

The remote control method offers several advantages:

- It enhances the performance of applications that do not require a Graphical user interface. These applications are usually not designed for the client/server architecture and are centrally processed. Applications such as data base queries can take advantage of the host's processing power without being dependent on the relatively limited power of the remote system.

- Remote control access maintains corporate investments in older and slower workstations, portable PCs, and modems. Because remote control does not require local processing, it is not necessary to equip every remote user with powerful computers, high-capacity disk drives, and fast modems.

- There is no need for additional software licensing because the remote system does not require any additional application software. All processing takes place on the host system.

At the same time, remote control has certain disadvantages, including the following:

- Performance is usually poor when using graphics-based applications such as Microsoft Windows, spreadsheet packages, or imaging applications because of the time it takes for images and screens to be transmitted over dial-up lines.

- Remote users cannot access network services as if they were directly connected to the LAN and are often required to learn new methods of accessing network services through the host system.

- Implementing remote control poses technical challenges. The host system must be running so the remote user can take advantage of the application software that resides in it. If the host system has been turned off or experiences a problem, the remote user is unable to work.

- With all remote access methods, security is a concern. When using remote control, the host system's monitor displays all the information that is being processed remotely, allowing the casual observer to view all screen activity, including E-mail and confidential information.

- The remote user can only access and run E-mail or other applications while connected to the host system through a dial-up line. All work must be done over the dial-up line,
which can translate into high-usage charges, especially if large file transfers are involved.

Even with these limitations, for remote data entry and small file transfers, the remote control method can be an effective and economical solution.

**Remote Node: A Client/Server Approach**

Industry trends toward client/server applications and Graphical user interface-based applications are driving the demand for remote node solutions. The remote node architecture is similar to a client/server application architecture. The remote system acts as a client and the communications server provides access to the desired server. Applications or portions of the applications are processed on the remote system. Only network data, such as E-mail, is transmitted over the line. Because remote node access is transparent, it is an ideal access method for client/server-based applications.

Remote node permits users to dial into the network and receive LAN access as if they were locally attached. Although access is slower, a user can still access a file server directly instead of having to transfer the file to a local drive, which is required with the remote control method. To edit a document on a network drive, for example, a remote node user simply opens it instead of first transferring the document to a local drive. This makes remote node much easier to use than remote control.

The remote system performs client functions while the home office-based servers perform true server functions. This allows remote users to take advantage of the remote processing power to implement graphical Windows applications. Whereas remote control entails connecting directly to the host system, the remote node connects to a remote access server. When connected to the corporate network, network resources appear to be local, as if the remote user is directly attached to the LAN.

**PROS.**

Remote node offers the following advantages:

- Performance is better with this method than with the remote control method when using graphics and Windows-based applications because screen images are not transmitted over the line.

- Remote users do not need retraining to access network resources or to use remote applications. User are linked to the computer and the network as if they were directly connected to the LAN.

- Remote access servers support modem pooling and hunt groups, allowing the network manager to support only one telephone number for multiple dial-in users.

- Remote user productivity does not depend on the connection to the corporate/branch office. Applications are resident on the remote system and can be run independently.

- Because user productivity is not totally dependent on the remote connection, usage-based line charges can be minimized. For example, when accessing E-mail remotely, the remote user is not required to maintain an open telephone line connection to the corporate/branch office while reviewing messages. The user can establish the connection to download messages, disconnect the line, then read messages offline at a
more convenient time. This offers an opportunity to cut down on connect time, which translates into reduced costs.

CONS

Remote node also has its disadvantages:

- Remote node requires additional application software licensing for each remote user because applications run independently on each remote system.
- Remote node requires an investment in more powerful remote computers, higher-capacity disk drives, and higher-speed modems, bridges, or routers.
- Because remote node users access the network as if they were locally attached, unwanted intruders are able to navigate the network without learning complex access procedures.

Remote Access Servers

Remote access servers typically reside at the headquarter's location and in effect enable remote users to become fully functioning nodes on the corporate LAN. Servers feature an expandable number of WAN ports to allow access by multiple users. A variety of protocols are usually supported. In multivendor, multiplatform networking environments, some remote users may be dialing in with different computers (e.g., Apple PowerBooks, Disk Operating System-based notebooks, and UNIX-based laptops). Each user may also be using a different communications protocol. Remote access servers should be capable of supporting a wide range of protocols so users can access the network directly using TCP/IP, Internetwork Packet eXchange, AppleTalk, NetBIOS, NetBEUI, DECnet, VINES, and Xerox Network System.

Faster Connections

The choice of protocol is often as important as the choice of remote access method. Novell's IPX, for example, can perform poorly over low-speed dial-up lines. IPX requires every data packet to be acknowledged before the next one is sent. This “send and wait” characteristic of IPX translates into 200 milliseconds of dead time between packets.

One solution to this problem is to integrate the new breed of V.fast modems into the remote access server. Connections of between 21.6K b/s and 28.8K b/s are achievable 95% of the time. With compression, these speeds are fast enough for IPX.

Another solution is to use TCP/IP over the V.fast connection, since most remote access servers already support this protocol stack. Unlike IPX, which must wait for packet acknowledgments before sending more packets, TCP/IP can keep sending packets while waiting for acknowledgments from the receiver. Although some TCP/IP vendors perform better than others over a V.fast connection, the use of TCP/IP can still minimize dead time during transmissions.

Dial-up Bridges and Routers

Remote dial-up bridges and routers establish a dial-up link with a similar dial-up bridge or router at the central site (see Exhibit 2), enabling multiple PCs attached to a remote workgroup LAN to appear as though they were attached to the centralized LAN. These
devices—which perform bridging or routing, as appropriate for the protocol being used—usually establish dial-up links over switched digital 56K b/s or Integrated Services Digital Network Basic Rate Interface (basic rate interface) circuits. ISDN is the preferred type of link, since the device can take advantage of the D channel to quickly set up and tear down connections.

**Remote Dial-up Bridges and Routers**

Bridges and routers have internal tables containing the hardware addresses of all nodes detected on the network. If a workstation needs to access a server resident on a distant LAN, the bridge or router recognizes that the destination address is remote, sets up the call on the ISDN D channel, provides the workstation with the required bandwidth on one or two B channels, then terminates the connection using the D channel. The call setup and tear-down procedures take only a few milliseconds, which makes the entire process transparent to the user. This may be the optimal solution for small workgroups that need to access another LAN occasionally for large file transfers, but cannot economically justify a full-time leased-line connection.

**Hybrid Solutions for Resource Pooling**

Network administrators can offer both modes of operation—remote node and remote control—to their users and let them decide which one is most appropriate to their needs and environments. For this there are hybrid remote access solutions that integrate remote control, remote node, and other communications services in a single multiprocessor server. A fully loaded system can run a wide range of communication services concurrently, including remote node, remote control dial-in, dial-out, host computer gateway, facsimile, E-mail, and bulletin board services. Such products ship with all necessary hardware and software fully installed, configured, and tested.

In essence, such servers provide the means for resource pooling, allowing communications resources to be shared and allocated by need. This approach reduces the requirement for hardware resources, such as modems, telephone lines, and communications ports, since they are shared among all users and are not allocated on a one-to-one basis.

Each communication service executes on a separate application processor, exchanging data packets over the server's high-speed bus. Multiple processors run concurrently, transferring and exchanging data packets over the bus. This provides a unified gateway to remote offices, telecommuters, mobile users, dial-in customers, host computers, and outside online services. Such servers typically support from two to 64 lines. Ports can be dynamically assigned as needed for dial-in or dial-out functions. A variety of connections are usually supported as well, including dial-up and leased lines, X.25, frame relay, Integrated Services Digital Network, and RS-232.

Several security levels are available. They include dial-back and restricted port access, in addition to requiring valid user IDs and passwords. The security can be customized to meet specific network requirements, including disabling security. Some vendors even include error recovery software in their products, which greatly contributes to the fault tolerance of their systems. An auto-reboot feature, for example, provides unattended recovery from software “hangs” and other failures.
Network Management

Many companies looking to implement remote access are more concerned with the extra management burden than they are with the cost of the actual hardware and software. While many vendors concentrate heavily on the price of remote-access products, network administrators have to look beyond price alone and consider the products’ manageability. Otherwise, these products could turn out to be more expensive in the long run.

Fortunately, many vendors of remote access servers support the Simple Network Management Protocol. Simple Network Management Protocol support facilitates ongoing management and integrates the remote access server into the management environment commonly used by network administrators. Support for simple network management protocol (SNMP) allows the server to trap several meaningful events. Special drivers pass these traps to any simple network management protocol (SNMP)-based network management platform, such as Hewlett-Packard's OpenView, IBM's NetView/6000, or Sun's SunNet Manager.

The management station, in conjunction with the vendor-supplied Information Base, can then display alerts relative to the operation of the server. The network administrator is notified when, for example, an application processor has been automatically reset because of a time-out, or when there is a hardware failure on a processor that triggers an ALM (antilocking mechanism) reset, a type of reset that ensures that the entire system and all other users are not locked by the failing processor.

Management utilities allow for status monitoring of individual ports, the collection of service statistics, and the viewing of audit trails on port access and usage.

Types of Connections

The choice of remote access connection boils down to analog and digital, and whether it is more economical to use dial-up services or leased lines.

Digital lines and services are always better than analog lines and services, especially when large amounts of information must be exchanged. Digital lines and services offer lower error rates and faster call setup times.

Although exhibiting poorer performance than digital lines and services, analog lines and services can be more economical for smaller applications that are used infrequently. In addition, the modems and software are inexpensive, making analog lines attractive even when large numbers of branch office workstations and portable computers require the capability for remote access.

Security

Security is a major concern in most networking environments, but more so when remote access is offered to mobile users and branch offices. After all, remote access virtually invites intrusion from hackers who are pre-disposed to tampering with or stealing sensitive information. Appropriate safeguards must be taken to prevent remote access from becoming a serious liability.

Depending on the size of the network and the sensitivity of the information that can be remotely accessed, one or more security methods can be employed.
Authentication
This involves verifying the remote caller by user ID and password, thus controlling access to the server. Security is enhanced if ID and passwords are encrypted before going out over the communications link.

Access Restrictions
This involves assigning each remote user a specific location (i.e., directory or drive) that can be accessed in the server. Access to specific servers can even be controlled.

Time Restrictions
This involves assigning each remote user a specific amount of connection time, after which the connection is dropped.

Connection Restrictions
This involves limiting the number of connection attempts or the number of times connections can be established hourly or daily.

Protocol Restrictions
This involves limiting users to a specific protocol for remote access.
There are other options for securing the headquarters LAN, such as cryptography and call-back. Cryptographic handshakes make a calculation at the client and server ends; both must match for access to continue.

Call-back
With call-back, the client's call is accepted, the line is disconnected, and the server calls back after checking that the phone number is valid. While this method works well for branch offices, most call-back products are not appropriate for mobile users whose locations vary from day to day. However, there are products on the market that accept “roving call-back” numbers. This feature allows mobile users to call into a remote access server or host computer, type in their user ID and password, and then specify a number where the server or host should call them back. The call-back number is then logged and may be used to help track down security breaches.

Point-to-Point Protocol
When peers at each end of the serial link support the Point-to-Point Protocol suite, more sophisticated security features can be implemented. This is because point-to-point protocol (PPP) can integrally support the Password Authentication Protocol or Challenge-Handshake Authentication Protocol to enforce link security. Of the two, challenge-handshake authentication protocol (CHAP) is the more robust protocol. PAP uses a two-way handshake for the peer to establish its identity. This handshake occurs only upon initial link establishment. An ID/password pair is repeatedly sent by the peer to the authenticator until verification is acknowledged or the connection is terminated. However, passwords are sent over the circuit in text format, which offers no protection from playback by network intruders.
CHAP periodically verifies the identity of the peer using a three-way handshake. This technique is employed throughout the life of the connection. Once established, the authenticator sends a challenge message to the peer. The peer responds with a value calculated using a one-way hash function. The authenticator then checks this response against its own calculation. If the values match, the authentication is acknowledged; otherwise, the connection is terminated. Challenge-Handshake Authentication Protocol provides protection against playback because the challenge value changes in every message. Because the password is never sent over the link, it is virtually impossible for an intruder to learn it.

Encryption

When wireless services are used for remote access, encryption is essential for protecting sensitive information as it crosses the airwaves. The devices at both ends run the encryption software for coding and decoding the information. Although encryption software constitutes an added expense when using packet radio services, a new wireless service based on Cellular Digital Packet Data technology employs authentication and encryption as integral features, preventing casual eavesdropping.

Conclusion

Remote access has become one of the top priorities in many companies. Network managers must be prepared to provide effective and reliable remote-access solutions to meet the needs of the decentralized and increasingly mobile workforce.

Modem-based solutions are recommended for smaller applications such as electronic mail. Work group applications that require large intermittent volumes of bandwidth—such as presentation graphics, desktop publishing, document imaging, and CAD/CAM—are more suited to on-demand bridge and router solutions. If a variety of dial-in and dial-out services must be supported concurrently to meet the widely differing needs of users at an enterprise level, a communications server may be the answer.

The technology is available from a variety of vendors to support remote-access applications. With a clear understanding of the applications, protocols, and security requirements that need to be supported, the right choices for cost-effective remote access can be made.

Author Biographies

Nathan J. Muller

Nathan J. Muller is an independent consultant in Huntsville AL, specializing in advanced technology marketing and education. He has more than 22 years of industry experience and has written extensively on many aspects of computers and communications. He is the author of eight books and more than 500 technical articles. He has held numerous technical and marketing positions with such companies as Control Data Corp., Planning Research Corp., Cable & Wireless Communications, ITT Telecom, and General DataComm, Inc. He holds an MA in social and organizational behavior from George Washington University.