digital™

Remote Access in the Modern World

Access Features That Remote Users Want, with the Control IS Managers Need

Digital believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Digital is not responsible for any inadvertent errors.

Digital conducts its business in a manner that conserves the environment and protects the safety and health of its employees, customers, and the community.

DEC, DEChub, DECserver, HUBwatch, NetRider, and the DIGITAL logo are trademarks of Digital Equipment Corporation.

All other names, products, and services are trademarks or registered trademarks of their respective holders.

Contents

Section **Page**

Introduction

This guide was developed to help IS professionals analyze and select the best remote access solution to meet their specific needs. It touches on the issues of information access and application performance for remote users, while addressing key IS requirements for managing and securing the data and networks supporting those users. The guide will examine the market forces driving the requirements for remote access solutions, along with Digital's approach to addressing those requirements.

Market Background

In recent years, various social, economic, and technological forces have changed the landscape of enterprise networks. Where once the network was defined by distinct physical attributes, today network boundaries are blurred in the wake of new technology and shifts in the competitive marketplace.

Global competition, for instance, has had a direct impact on business structure. In answer to increasing competitive pressures, enterprises are distributing their organizations by placing branch or satellite offices closer to customers. Business travelers, sales professionals, service technicians, and others may find themselves in a wide range of remote locations — and these locations will likely change daily. As a result, the network is often extended over wide and diverse areas. In addition, advances in technology and changes in corporate culture are permitting more and more staff to *telecommute* — to work in their homes and extend the network even further. In fact, this phenomenon continues to grow as telecommuting is spurred on by growing demand (and in certain cases, legislative requirements) for parental leave, for job sharing, and to reduce the number of automobiles on the road. All these remote users represent a large constituency — and responsibility — for the network manager.

The issue for these users — and for the network manager — is access to information on the enterprise network. It seems like a simple requirement: remote users need information to perform their jobs. But that is only one side of the equation. While the network manager strives to provide users with network access, issues such as compatibility and performance, along with control and security, loom as significant challenges.

As remote access has emerged in the marketplace, its requirements have been driven primarily by users. Mobile and workplace pioneers adrift without a lifeline back to the corporate offices used any methods they could find to gain access to the network. Today, however, the number of remote users is reaching a critical mass, extending the horizon of the enterprise network well beyond the walls of the corporate headquarters. Therefore, greater responsibility

and opportunity lie with the network manager to implement a remote access solution that satisfies enterprise-wide requirements, not just individual demands.

Market Snapshot

- PC shipments expected to grow to approximately 190 million by early 1997, from 100 million in 1991 and 160 million today
  – International Data Corp. (IDC)

- PC-based remote access market estimated at $966 million by 1998, from $345 million currently
  – International Data Corp. (IDC)

- Sales of remote access products estimated to reach $2.23 billion by 1997
  – Infonetics Research, Inc.

Motivating Factors

Let's examine the motivating factors for both users and network managers. Remote users — more so than their counterparts in the corporate office — are making individual choices about the kinds of systems and applications they use. Therefore, one will find on the client side a broad mix of DOS and Windows PCs, Macintosh systems, and UNIX workstations. These clients simply want to gain access to network information without complication and without any significant degradation in application performance.

From the IS viewpoint, however, the issues are not so simple. The network manager is challenged to support a heterogeneous mix of client systems and software — there are far too many remote users now to address each requirement singly. As a result, the network manager must have a broad-base solution that satisfies the needs of his or her entire constituency. In addition, with the network expanding to include ever greater numbers of individual — and often mobile — users scattered in a multitude of remote locations, the issues of management and security quickly rise in importance.

Remote Access Technologies

Clearly, the focus has shifted from user-oriented solutions to more strategic and proactive solutions originating from within IS. It is incumbent upon vendors, therefore, to provide remote access solutions that balance the client's need for easy access and performance with the network manager's need for security and control.

Digital Equipment Corporation has developed a remote access solution that directly addresses the need for balance — the NetRider Remote Access solution. It is a solution borne out of our own experience managing one of the largest enterprise networks in the world. It is one of the most complete solutions available today for those who are looking to start acquiring remote access technology or to add to their existing capabilities. And the Digital NetRider Remote Access solution incorporates technology and capabilities that best serve the interests of network managers and remote users alike.

The Digital NetRider Remote Access solution includes:

- Access servers supporting heterogeneous clients and protocols
- Industry-standard PPP client software for AppleTalk, IP, and IPX connections
- Remote node, remote control, and terminal access capabilities
- Accounting and management facilities
- PAP, CHAP, and Kerberos security
- An enhanced version of Mosaic for Internet browsing

Let's examine these technologies and capabilities in more detail.

Types of Remote Access

The first issue an IS manager must face is implementing a remote access solution that users will accept. After all, if the remote users are not happy with the solution, they are unlikely to use it. As a result, they may seek their own solutions — leading back to the security and management problems the IS manager wishes to eliminate.

When considering a remote access solution, one must first consider how it will be applied. Users within a branch office, for instance, are most likely connected by a local area network (LAN) at their site. Gaining access to the corporate network, therefore, requires connecting the branch-office LAN to a LAN at the headquarters facility, known as LAN-to-LAN access. Supporting such a connection typically requires synchronous communications links and some form of routing technology.

Another type of remote access technology allows the individual user to gain access to the corporate network via asynchronous, dial-up links — usually across the public switched telephone network. With this type of remote access — utilizing an access server — the user attains full peer status on the corporate network as though he or she were locally connected.

Digital provides support for both types of remote access through specialized network modules and software that provide seamless network access from the remote user to the backbone. For example, Digital offers low-end access routers, such as the DECwanrouter 90 and the DECbrouter 90, which support LAN-to-LAN access. Connecting individual users to the corporate network, however, requires a different solution. To support remote access by individuals, Digital offers products called access servers, which are incorporated into complete remote access solutions. This guide will focus on key issues and solutions for this type of access.

Access Servers

Access servers can provide individual users with inexpensive access to the information and resources on a corporate network via dial-up connections using standard telephone lines. With telephone lines available to nearly any remote user, and with the cost of telephone service relatively low given typical usage, dial-up capability is an important method of remote access. In addition, with the advent of higher-speed asynchronous modems and forms of data compression, it proves to be a very viable method of access.

Access servers reach beyond more traditional terminal servers to support the requirements of today's remote user. Information today includes far more than simple text and data — corporate networks are vast repositories for graphics, tables, and images, as well as formatted text and data. And the PCs, Macintosh clients, and UNIX workstations in the field need access to it, just as much, if not more so, than those working inside the office.

The Digital Approach

An access server, such as the DECserver employed in Digital's NetRider Remote Access solution, provides the dial-up access remote users need. An industry-standard PPP solution, the DECserver supports virtually any type of client — DOS, Windows, Macintosh, UNIX — providing the network manager with much needed heterogeneous client support, and remote users with the unencumbered access they desire. The access server's operating software provides for auto-sensing of datalink protocols coming over a port — enabling the

network manager to configure the port to automatically recognize SLIP, CSLIP, or PPP and start the correct session — and it provides essential security and accounting features. Perhaps most important, though, the system can handle both remote and local connections of terminals, printers, and PCs, as well as support remote node, remote control, and terminal emulation applications. This provides a variety of access alternatives without the need to have multiple types of servers on the network. Indeed, the access server component of the NetRider solution is Digital's DECserver access server module. With a proven track record in the terminal access market, this asynchronous communication server is well suited to providing both local and remote access for a variety of systems.

DECserver90 Access Server module component of the NetRider System

Remote Node versus Remote Control

Having gained access to the corporate network, remote users want to take full advantage of the computing capabilities on their laptops and desktops. In many instances, that means having full-peer status on the network to enjoy their graphical interfaces and graphics-based applications and data. Often, however, a remote user's task requires accessing large databases to conduct queries and generate reports. There are two different applications — remote node and remote control — that can accommodate remote users based on the type of activity they wish to engage in on the corporate network.

Remote Node

Remote node takes full advantage of the processing power of the remote user's PC. It enables the remote user to connect directly onto the network and act as a full LAN peer member. It is as though one had extended the network wire to the remote user, the only difference being that the wire is not Ethernet, but rather the slower asynchronous line. In remote node, packets from the corporate LAN are sent across the asynchronous line to the remote PC or Macintosh, where the application executes locally. It is ideal for applications that are truly client/server such as E-mail, or groupware applications such as Lotus Notes. It is also appropriate for quickly copying home a file that you've been editing to make final corrections.

While remote node is appealing to users and offers a great deal of flexibility, there are drawbacks. For instance, performance is dependent on a number of factors beyond simply the raw line or port speed of the server. In addition, security and accounting are issues that must be considered.

Remote Control

With remote control, the user dials into an access server to take over control of a PC or host connected to the network. Processing remains on the corporate network while screen updates are sent to the remote laptop or desktop. Therefore, remote control is ideal for obtaining information from large databases — keeping the processing local to the LAN, rather than attempting to send the entire database over an asynchronous line. When the database search is completed, all that is sent to the remote user are the results.

Remote control also holds additional value specifically for the network manager. Using remote control, help desk personnel can log on to a user's PC and perform diagnostics directly, often resolving problems on the spot. In addition, security and management are easier since databases and systems being accessed still reside physically on the LAN.

Remote control, however, still has its limitations. For instance, if the remote user is not using the same version of software as the gateway PC or host, problems may arise. If the remote user needs a specific application, it must be on the local PC in the appropriate version; otherwise the remote user will be unable to perform his or her task.

The Digital Approach

Remote control emerged as a more popular application before remote node, and it would be easy to think of it as old technology, soon to be replaced entirely by remote node. As we can see, each still has its place in the remote access world. In developing the Digital NetRider Remote Access solution, Digital carefully studied the benefits of both applications. As a result, the Digital NetRider client software provides remote node capabilities for Macintosh clients, as well as for PC clients using TCP/IP and IPX. In addition, the package provides IPX clients with remote control capabilities. In fact, IPX

clients can dynamically toggle between remote node and remote control by simply clicking on a graphical *button*. The Digital NetRider solution even supports access by terminals — or systems using terminal or TN3270 emulation — for those users who may prefer this simpler, but consistently reliable, technology. (See sidebar.)

Terminal Emulation

Terminal emulation was one of the first applications used for remote access. It is a popular method because it is a capability provided by most commercial communications software products and it uses standard telephone dial-up links. In addition, through terminal emulation, basic text characters can be shared with nearly anyone. Terminal emulation also offers consistent response times and eliminates for IS managers the worry of backing up data — all processing remains at the host, which simply sends screen updates to the client.

The Digital NetRider package is the type of broad-base solution network managers can implement to satisfy the needs of their entire remote user constituency. As we have seen, it contains popular methods of access, giving users the flexibility to choose the method that best meets their needs. But what of the IS manager? As stated at the beginning of this guide, in today's widely distributed network environment, there must be a balance between satisfying the remote user's needs and meeting the IS manager's requirements.

Success Factors for the IS Manager

To be successful, a remote access solution must satisfy the IS manager's requirements to support heterogeneous clients and protocols, ensure adequate performance, maintain management control, and provide adequate security. In addition, a remote access solution should make sense in a cost-of-ownership analysis.

In the following section, we examine these issues in detail.

Heterogeneous Client/Protocol Support

To support a range of remote client types, and maintain control over multiprotocol connections, the IS manager needs a versatile method of connecting remote users to the corporate network. In addition, that method must provide reliable communications using existing telephone services.

Point-to-Point Protocol

One of the most popular methods today for establishing remote connections over telephone lines is Point-to-Point Protocol (PPP). PPP was developed by the Internet Engineering Task Force over the last six years and is quickly becoming the standard in UNIX and PC markets. PPP provides a standard method for transporting multiprotocol data packets over any type of point-to-point link and can take advantage of several different types of public network services — standard analog telephone service, digital telephone service such as ISDN, or frame relay. In addition, PPP can carry many different types of network protocols — including TCP/IP, AppleTalk, and IPX simultaneously. Additionally, PPP is a more robust datalink protocol that can negotiate links by performing all necessary handshaking between remote clients and the network.

PPP versus AppleTalk Remote Access Protocol

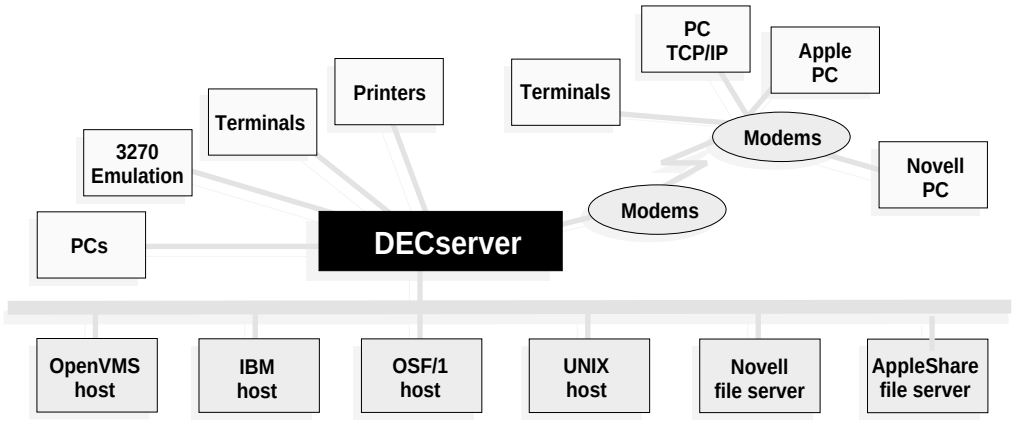
For Macintosh clients, the most popular method of accessing AppleTalk networks from a remote location has been the AppleTalk Remote Access (ARA) Protocol. ARA is limited, however, to carrying only AppleTalk — so a Macintosh user who might need to make an IP

or IPX connection is simply out of luck. PPP, on the other hand, can carry many different types of network protocols at once, which offers many practical benefits. For instance, PPP offers a fast, direct approach to accessing Internet services, as opposed to ARA, which must perform additional encapsulation of IP packets into AppleTalk packets. PPP simply avoids the overhead of IP encapsulation and eliminates the need to fragment IP packets to fit AppleTalk.

PPP is more versatile than ARA in its ability to support multiple types of access (dial-in, dial-out, etc.) along with multiple types of links (ISDN, frame relay, etc.). Better performing than ARA, PPP offers greater efficiency by delegating error correction and data compression to the modem, rather than retaining these functions within the protocol. As a result, the access server is able to effect higher performance. Finally, PPP provides Macintosh users with the same features that they are accustomed to with ARA, making a PPP solution just as easy to use.

The Digital Approach

Digital recognizes PPP as the protocol of choice for remote access. Therefore, the Digital NetRider system includes an industry-standard PPP remote access solution for both PC and Macintosh connections. This approach provides users with the freedom to make IP connections simultaneously with an AppleTalk or IPX connection.



Performance

When examining performance issues, there are a number of potential bottleneck areas that stand out — both at the remote site and at the server. A remote access solution that addresses these performance issues stands not only to make the IS manager's life easier, but also to ensure acceptance by the user community.

One of the most important factors in achieving adequate performance on the client side is the modem. Therefore, remote users should be equipped with the fastest modems possible that will support their applications. Windows applications also represent a potential bottleneck since they are limited to 19.2 Kb/s data transfer speeds on a serial link. New technologies are emerging, however, that can reroute application traffic from the serial port to a parallel port. Some modem manufacturers even incorporate such redirection into their modems.

At the access server, line and port speeds can also lead to performance issues if the line speeds cannot support the flow of data coming in.

The Digital Approach

Digital offers two remote access server options in the Digital NetRider solutions. One access server is designed for small networks, while the other is designed to support a greater number of remote users. The 8-port access server supports line speeds of 57.6 Kb/s. The Digital NetRider 900 access server features 32 ports with a line speed of 115.2 Kb/s — the highest in the industry. In addition, the Digital NetRider client package supports the latest V.34 (28.8 Kb/s) modems, which are currently the fastest modems available on the market. With this powerful combination, network managers are assured of maximum performance in a remote access solution.

Security

By opening up the corporate network to access from anyone located remotely, security is a justifiable concern. There are a number of ways to provide IS managers with the support they need to ensure network integrity and protect the enterprise's valuable information assets. In addition to traditional log-in, there are protocol-specified

security mechanisms, server-based authentication (dial-back and encryption), separate LAN security servers, and token-based security.

PPP specifies two security mechanisms — Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). The first mechanism, PAP, provides a simple way for a remote device to establish its identity, or authentication. With PAP, a remote device sends identification information about itself, along with a user-entered password, to the access server immediately upon establishing the communications link. Authentication takes place at the server, and if the communication is authenticated, the connection continues until a successful two-way handshake is achieved.

The second PPP security protocol, CHAP, uses a three-way handshake. CHAP offers a higher degree of security than PAP, since the password is never transmitted over the link, thus frustrating attempts by network listeners to ascertain the password. It is also more difficult to intrude upon because it sends a challenge to the client to provide the correct response. Those attempting to intrude via a repeat attack on passwords will not be successful.

Some access servers provide additional "built-in" security features, such as the encryption of information being sent or received. Other access servers support dial-back capabilities, which attempt to authenticate a user by calling back to where the server believes the user should be.

For a greater degree of security, many organizations implement a separate LAN-based security server, which authenticates remote users immediately upon dialing in. One such server-based method uses Kerberos — a security protocol developed jointly by Digital and the Massachusetts Institute of Technology. Kerberos is very popular in university and government settings. Another server-based method is from Security Dynamics, called SecureID, which provides one additional level of security. SecureID includes a hardware token that acts as a key on the remote user's system, and then interacts with the Security Dynamics server on the network. Both server-based authentication methods require the purchase and use of a separate server on the LAN.

The Digital Approach

The Digital NetRider solution supports both PAP and CHAP, as well the high-security capabilities of Kerberos. Unique to the Digital NetRider solution is the combined use of PAP and Kerberos. With this approach, the network manager can manage all user passwords from a single, central database. In a typical scenario, the user would authenticate to the access server by entering his or her password on the PC or Macintosh client. The client sends this information to the access server via PAP. The access server then would authenticate the user by a request to the Kerberos server on the LAN. Particularly important for larger organizations, the PAP/Kerberos combination eliminates the need to manage passwords across distributed access servers; rather, authentication is kept to a single dedicated point. The result is high security that is easily managed.

Management and Accounting

Because managing a network is already so complex, the success of a remote access solution depends on easy-to-use management features. In fact, if a remote access system is difficult to manage — whether in configuration, setup, access, or modifications — it really is not a "solution" at all.

As remote access becomes more and more prevalent, accounting also becomes more important. For instance, by providing the identity and number of users accessing the network, a remote access solution can help IS managers plan capacity requirements, run audit trails, and ensure security. Accounting information also provides remote access providers — corporate network managers or Internet Access vendors — with data that can be used in charging clients for access.

The Digital Approach

The Digital NetRider solution is designed for ease-of-use, by both the end user and the IS manager. For end users, it supplies the ability to dial in and interact with the network in the fashion most compatible with their daily work pattern. And it does so with easy-to-install graphical applications. For the IS manager, it is manageable via SNMP-based management systems, such as Digital's HUBwatch

graphical management software, as well as HP's OpenView and SunNet Manager. Telnet remote console is also provided to give the IS manager a number of management options.

Also provided with the Digital NetRider system is a Windows-based configuration utility, which allows the IS manager to quickly configure the remote access server. In fact, with the utility's ability to copy from port to port or server to server, an access server can be up and running in a matter of minutes.

The Digital NetRider solution can account for significant user actions such as user logins, logouts, session connects, disconnects, password failures, user ID, protocol, and a number of other parameters. This information can be harvested to an accounting log, which can then be analyzed through an accounting application, giving the IS manager much needed data for network planning.

Cost of Ownership

Cost of ownership is another key concern for the IS manager in choosing a remote access solution. There are a number of issues that affect the total cost of ownership beyond just hardware. Ease of management, comprehensiveness of the solution, and scalability also factor into a long-range view of the remote access solution.

When providing dial-up remote access, one must take into account the individual capabilities of the users and their applications. Some users prefer remote node access, while others will want remote control, and still others, terminal emulation. The critical question here is, Does the IS manager need to purchase separate systems for each type of access, or does the remote access solution provide all three?

As discussed above, management is an important issue for the IS manager, and it figures significantly into the overall cost of a remote access solution. More complex management translates directly into time — and possibly additional staff — which one can easily view in terms of cost. Therefore, a remote access solution that is easier to manage will be less costly over the long term.

In addition, scalability should be considered in the cost analysis. A "solution" that must be replaced every time the load increases will quickly drain the IS budget. And with the number of remote access users on the rise, scalability becomes a major concern.

The Digital Approach

The Digital NetRider solution offers outstanding cost-of-ownership. In a recent assessment conducted by an independent evaluation firm, following a methodology developed by *Communications Week* magazine, the Digital NetRider system topped the ranking in price/performance among five contending remote access systems. In addition, Digital NetRider came in with the lowest cost per server port, lowest cost per client, and lowest overall system cost in the same comparison. While the raw numbers are impressive, the Digital NetRider solution offers further cost-of-ownership advantages due to its range of capabilities. Because it is a complete solution, there is no need for the IS manager to purchase separate terminal servers, remote control servers, and remote access servers — Digital NetRider provides all three in a single package.

Its ease of management is also important assurance to the IS manager that management costs and staffing will be minimal. In terms of scalability, the Digital NetRider system is based on a modular approach to ensure that your investments are protected as load increases and the supporting remote access system expands. An IS manager can start with an eight-port Digital NetRider 90 standalone system — complete with all the software required for end-user access and LAN management. If the system's accounting features indicate a need for more ports, one might consider the Digital NetRider 900 32-port system. The system can even be plugged into a DEChub chassis, which supports up to seven access servers — and as many as 224 ports when using the Digital NetRider 900 system. In the final analysis, no other remote access system on the market can compare with total cost of ownership of the Digital NetRider solution.

Conclusion

In a comprehensive analysis of remote access technologies and capabilities, Digital has engaged in extensive research, conducted wide-scale testing, and drawn upon its own experience to produce a complete end-to-end solution. The Digital NetRider Remote Access solution contains specific design features that not only appeal to remote users, but also provide for the needs of the IS manager. Faced with the prospect of tying more and more remote users into their corporate communication network, IS managers must not only provide client functionality, but also retain control and manageability of the extended network. For versatile client access, high-performance access capabilities, excellent cost of ownership, and reliable security, the Digital NetRider solution is the ideal choice.

For More Information

For more information about the Digital NetRider Remote Access solution and other Digital network solutions, contact your local authorized Digital reseller or consult with a Digital sales representative. To find your nearest sales office in the United States, call 800-457-8211.

Digital Corporate World Wide Web Home page:
http://www.digital.com/home.html


digital™