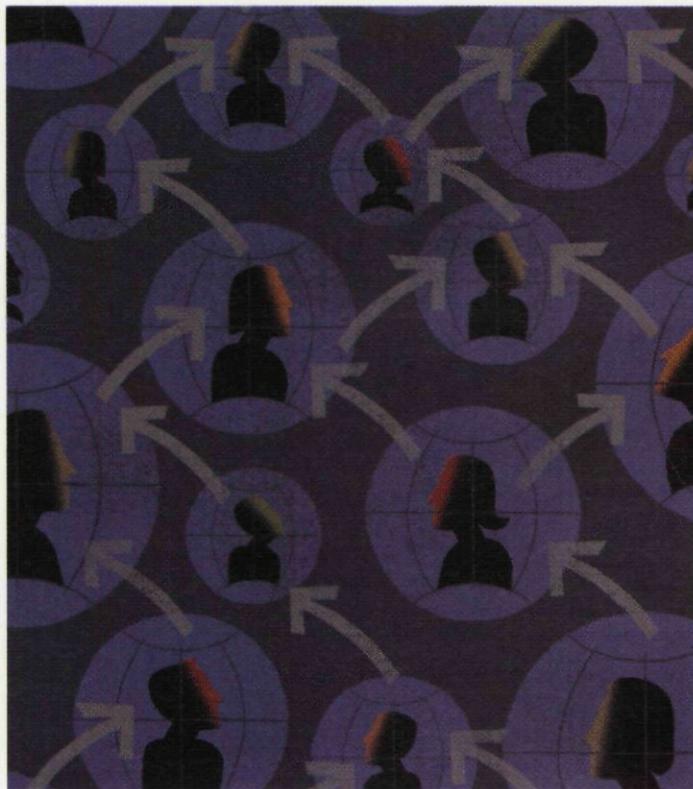


Telecommute Safely

Use Internet technology to keep cost down.

by James P. Davis



Technology is shortening the daily office commute and providing a secure and economical link to clients, customers and satellite offices. With just a few keystrokes from a remote location with Internet access, users can link to an office network so that, for all intents and purposes, they're virtually working in that office. Not only is such a link relatively inexpensive, it provides enhanced communications security.

Does such a link require the installation of a hot, new, expensive technology that requires intensive training of the organization's staff and information technology experts? Not at all, thanks to virtual private network (VPN), a technology that actually has been around since the mid-1990s but failed to gain popularity because the

accounting profession has been slow to adjust to both advanced technology and, oddly enough, to modern management styles. In those "old" days, VPN was still considered high-tech, thus keeping technophobic managers at bay. Also, many older-generation managers distrusted telecommuting, believing that those working out of the office would be laggards and beyond their control. Many of today's managers now recognize both the efficiencies and economies of telecommuting.

» Key to Instructions

To help readers follow the instructions in this article, we use two different typefaces: **Boldface** type is used to identify the names of icons, agendas and URLs.

Sans serif type shows the names of files and the names of commands and instructions that users should type into the computer.

PRIVATE AND PUBLIC LINKS

A VPN is essentially a software or hardware bridge for connecting a remote user to a company's local area network (LAN), which is a private network, via the Internet, which is a public network. And it does

this without compromising privacy. VPN applies protocols for encapsulating and encrypting data flowing between a LAN and a remote computer. The result: It's as secure as the LAN itself.

A VPN also is far less expensive to set up and operate than its alternative—leased data lines, which would cost, depending on the distance and transmission speed, from a couple of hundred dollars a month to a couple of thousand.

COST AND COMPLEXITY

The cost of a VPN setup depends on how much special hardware is needed and the type of VPN connection desired. Most offices with networks already own most of the necessary components, which include a server (the computer that manages network resources), a router or switch (to distribute files within the network) and a firewall (software or hardware to prevent unauthorized access into or from the network). Most VPN implementations use software set up within the firewall. Also required is an Internet connection. A broadband connection, such as a digital subscriber line (DSL) (from an Internet Service

Provider (ISP)) or cable (from a television cable company), is sufficient. A dial-up account is too slow to be usable unless you are deploying special linking software such as Citrix or Microsoft Terminal Server. However, those remote-access solutions are more expensive to implement and maintain. The ISP also must provide a static Internet Protocol (IP) address—a permanent Internet address.

A VPN can be configured for three types of connections:

■ **Remote access.** This links a remote user to an organization's network via its server or desktop PCs and provides full network access from any place with an Internet connection. The user could, among other things, create documents or update an appointment calendar—in short, accomplish any on-site computer-related task. This is the simplest type of VPN to set up.

■ **Intranet connection.** This links two or more offices while providing each with access to the organization's network. Such a connection allows data to be stored and shared from a single access point (the main office) as opposed to maintaining separate and often duplicate information on every satellite office server. A retailer, for example, could maintain a single database of inventory accessible by all remote locations. This arrangement is more complicated and usually requires a consultant to do the setup.

■ **Extranet.** Such a link provides secure access directly to another LAN. An accountant could make adjustments to a client's books instead of relying on the client to post them. This setup also is complex and may require a consultant.

SO WHAT'S THE PRICE TAG?

Assuming a small organization (up to 10 users) has the basic hardware (a LAN, a router and a firewall) and would rather engage a consultant to set it up, the cost can range between \$30 and \$50 per user. A midsize organization (11–50 users) that wants to connect two remote offices would have to spend between \$800 and \$1,200. Large operations would pay \$2,000 and up. Pricing for installation of these services can vary depending on your location. It doesn't take extraordinary technical skill to set up a basic VPN configuration as you'll see in "Setup Time," at right; however, it is strongly recommended that any remote-access installation be set up by an experienced consultant to make sure all security aspects are given consideration.

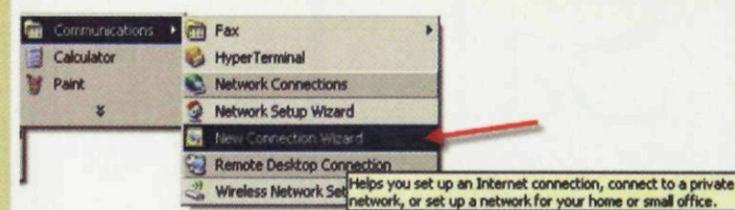
Once your VPN is set up, not only will staff members be able to telecommute, but any data stored on the network will be immediately available to all the remote users and any data the remote users produce will be immediately available on the network. That alone will generate huge savings in effort and time, and you'll wonder why you waited so long.

James P. Davis, CPA/CITP, is a senior accountant of Colby & Co., PLC, a public accounting and consulting firm in Chesapeake, Va. His e-mail address is jdavis@colbycpa.com.

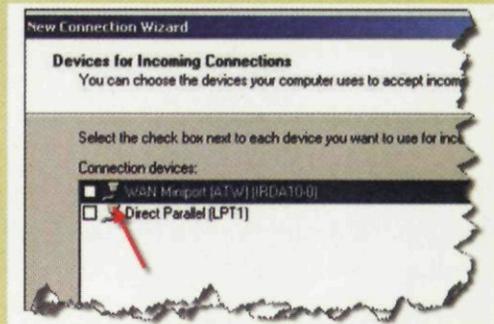
Setup Time

How to Set Up a Basic VPN Link

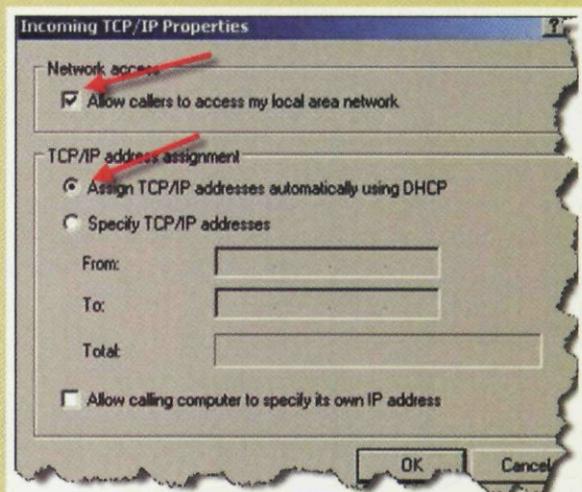
Begin by clicking on Start, All Programs, Accessories, Communications, New Connection Wizard.



Then click on Next and select Set up an advanced connection. Click on Next and select Accept incoming connections. Click on Next. Do not select any Connection devices.



Click on Next and select Allow virtual private connection. Click on Next and select the user accounts you want to allow access to your PC. Click on Next and highlight the Internet Protocol. Click on Properties and make sure there is a check next to Allow callers to access my local area network.



Now you must select how remote computers will get IP addresses. Generally, selecting the first option—assigning the addresses

Copyright of *Journal of Accountancy* is the property of American Institute of Certified Public Accountants and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.