Four Partial Solutions for Remote Network Access

Four different solutions can help to meet your remote-access needs. Managed-service providers are positioning themselves to direct all four, but this will come at a price.

Remote networking was once the privilege of salesmen and traveling professionals. Its expansion has continued and accelerated, given the benefits of teleworking and the growth of high-speed Internet access. The issue now is which access methods are best for your enterprise. The solution was simple when there were only analog modems. Today, however, four methods can help to meet your remote-access needs:

- Maintaining your own modem banks and dialing directly into the enterprise
- Using a managed analog dial-access service from a service provider
- Running your own Internet-based virtual private networks (VPNs)
- Maintaining an enterprise portal that you can access from any Internet connection

These solutions could be used on their own, but for maximum effect, use at least three of the four. You also should evaluate which portions of your remote-access solutions to insource or outsource.

Direct-Dial Access

Remote access began as soon as there were modems — the oldest and most-traditional form of remote connectivity. You had to maintain your own modem banks and users, and dial via local or toll-free telephone numbers to reach the office. Direct-dial access was secure because it enabled a direct connection from the user to the office. However, it also was one of the most-expensive methods from a total cost of ownership perspective, when you tally the costs of the phone call, modem banks, software, maintenance and management. Direct-dial access
costs have dipped in recent years, with some dedicated toll-free number charges dropping to as low as 2 cents per minute. The cost of modem banks also are much lower with, for example, Cisco's Digital Modem Network Modules, as compared to older Shiva equipment. However, total costs for direct-dial access are still mostly higher than for managed services.

When to Use

Remote maintenance and monitoring for IT employees via direct-dial access is still the fail-safe method. All other reasons should be viewed only as point or temporary solutions, such as remote management or for purely local-dial access, where there isn't a phone charge. As soon as you start using toll-free numbers for remote access, you also should begin using managed remote-access solutions.

Managed Remote-Access Services

The original managed remote-access services supplied low-speed dial-up access via X.25 networks (offered by providers such as IBM, Sprint and CompuServe). They provided a dialer client to remote users while providers managed centralized authentication into the network. The services are the same today, but they are more secure, more reliable and more cost-effective.

Managed remote-access services also offer more options. At a minimum, managed-service providers (MSPs) will offer dial-up Internet access for as low as 30 cents per hour, but you must add your own VPNs to the connections.

In addition, MSPs offer dial-up, xDSL or wireless access to secure IP networks that don't go over the Internet. MSPs fully manage the VPN, provide Level-2 and sometimes Level-1 help desk support, and handle all ongoing operations support. Their services can cost $15 to $20 per user per month as a fixed cost option, or 60 cents to $1.20 per hour with a use-rate structure. Equipment maintenance fees can be added to these charges.

Telecommunications operators play a major role in the managed remote-access market, but network aggregators are starting to set its direction. Providers such as Fiberlink, Gric Communications and iPass offer analog access worldwide by including dial-up access numbers from hundreds of Internet service providers in the dialers. Aggregators, being network-independent, focus on service delivery and provisioning flexibility. They also are expending efforts to support xDSL, cable modem and Wi-Fi users. Providers such as MegaPath Networks and TManage specialize in these broadband options, and offer useful centralized purchasing and support services.
Be aware of how much some of these high-speed services cost. AT&T, for example, charges approximately $6 to $7 per user per month to use its client access via wired broadband connections — but this is on top of whatever you pay for xDSL at home. It could be cheaper as a replacement for what you might be charged in a hotel or Wi-Fi hot spot, but you have to keep track of how much time you're online. As a result, it's more cost-effective to have the resources to manage your own VPNs from high-speed locations.

**When to Use**

Managed remote-access services are more cost-effective for traveling employees, and for those who don't want to manage their own analog equipment. You also should consider current prices to receive Wi-Fi from traditional analog aggregators, because the total cost via iPass, for example, can be cheaper than going directly to Wi-Fi providers such as Boingo Wireless or Wayport.

**Do-It-Yourself VPNs**

If you're a teleworker with high-speed access at home, then managing your own VPN can be more cost-effective. At-home workers must have high-speed connections to the Internet, and installed some sort of remote VPN client onto their computers.

The most-common encryption standard is IP security (IPsec). The client software and the central site VPN can come from a firewall or router vendor, or from a separate VPN device. The leading vendors for such solutions, respectively, are Check Point Software Technologies, Cisco Systems and Nortel Networks.

The cost for these solutions is in the VPN devices, the management expenses and the xDSL services. For full-time teleworkers, nearly all firms pick up the cost. For part-time at-home workers, however, many firms offer the solutions as an employee benefit and don't pick up the cost, or they only pay a portion of it.

You must choose what to pay for, based on your needs. If you pay for access charges, they can be the most expensive of the four solutions, but also provide the best bandwidth. Because of this, you also can expect to pay more for increasing your central site's bandwidth. If not, you'll create a "choke point," and the value of the faster connection will be lost.

The drawback of these always-on high-speed connections is security. They will always be open to attack, so we recommend a few precautions:
• Set the VPN connection to time out and disconnect after a fixed period of disuse.

• Ensure that remote users have two personal firewalls: one software-based to catch "Trojan horses" when they leave their point of origin, and one hardware-based to translate network addresses and provide inbound blocking.

• Ensure that remote virus detection software is installed on remote computers, and that it's automatically updated and can’t be disabled.

Be aware that most xDSL and cable modem providers state within customer agreements that their standard offers can't be used for business purposes. Many have threatened to disconnect users who aren't paying for higher-price, business-class services. However, most providers have stopped using threats and are switching to tiered pricing models, where it's assumed that business users will pay for higher bandwidth.

Currently, for example, most business-class xDSL services cost 50 percent to 100 percent more than consumer-class services, even though the quality is the same and there are no service-level agreements. If you purchase business-class xDSL services, you may save money from such providers as Covad Communications, TManage or AT&T, rather than buying directly from local telephone companies.

When to Use

If AT&T is your provider, use company-implemented and managed VPNs to avoid AT&T's individual authentication fees. Beware of other vendors that propose these charges but do nothing more than provide an access client and authentication. If you're managing your own site-to-site VPN, consider a do-it-yourself approach for remote workers. If you already are using analog dial-up services from an MSP that isn't charging for a bring-your-own-access solution, consider discarding your solution and switching over your high-speed, at-home workers to your analog access client's VPNs.

Enterprise Portal Access

The previous three access solutions use a dialer or access client. By "Webifying" applications, however, you can provide access to the office from any device on the Internet, and secure the connection using Secure Sockets Layer (SSL) technology that's built into every browser. This form of enterprise portal access, called "clientless VPNs," will dominate the next three years, but it will require the addition of authorization and access control services to provide fine-grained, centrally managed privileges. Deploy it as part of a thin-client architecture to prevent data from
Another downside to portal access, along with additional security requirements, is that it does nothing to address network performance. Thus, for full-time or part-time teleworkers, you must add in one of the first three network-centric solutions (see Note 1).

When to Use

If you already have placed a front-end Web interface on your business applications, and if you have lower security risks or concerns, then SSL-based remote access should be your primary access method. The portal-based approach is the best solution for most business-to-business or business-to-consumer transactions.

Right Mix

Users generally can be divided into groups based on the type of access they have. For example, clerical employees who don't have laptops could be given portal access, but only to check e-mail. Full-time teleworkers should have xDSL or cable modem access, and depending on the security requirements, they also could be given portal access or a full IPsec VPN client. "Road warriors" may have all four options, but supporting these options is costly and difficult to manage. Some firms may be staffed to support this, but most aren't.

That's why MSPs are positioning themselves to do it all. AT&T, for example, can offer a full array of analog, xDSL, Wi-Fi or bring-your-own-access services. It has partnered with Aventail to offer SSL-based portal access. AT&T (and most other providers) is even willing to add your direct-dial numbers to its access client, so the only things you have to manage are your modems.

This solution comes with a price, however. AT&T is one of few MSPs that charges you to use its access client ($6 to $7 per user), as long as you use your own access service.

iPass is also bundling all four solutions and partnering with Aventail. We expect that the rest of the market will follow suit and have fully bundled options by 2004. That should lead to better competition and lower rates.

**Bottom Line:** The remote-access market is moving toward clientless virtual private networks, but it's not going to happen overnight. You still need to support as many as three of the four options (that is, direct-dial access, managed remote-access
services, do-it-yourself virtual private networks and enterprise portal access). However, if you want to avoid having to manage all four, use a managed-service provider. You still may have four solutions, but you'll only have one vendor to manage.

If you want to control costs but still offer multiple access methods, you can save money by having an MSP manage the analog services while you manage the high-speed remote workers; or you can choose an MSP that won't charge you to use its access client on a bring-your-own-access site. Include a clause in your contract to prevent the provider from adding charges in the future.