Telecommuting has been growing in popularity over the past several years, partly as a result of advances in technology, and partly in response to corporate downsizing. This has led to an increase in remote access. The result has been a proliferation of technologies used to support remote access telecommuters, and development of a range of issues of concern for corporations, including technology selection, management, and security.

As remote access continues to develop, it will become increasingly significant as a cost item for the enterprise, as well as raising concerns over management, security and efficiency. Meanwhile, it is providing a wealth of new options, and bringing communications, applications, and network services ever closer to the end user.
Development of an effective remote access solution for telecommuters and mobile workers demands consideration of a wide range of technical and managerial issues. The service must be easy to use and standardized for the end-user, providing telecommuting employees with access to all of the information and applications they regularly use. At the same time, it needs to be implemented efficiently and cost effectively, with sufficient security to ensure that the corporate network will not be compromised.

**Employer Issues**

Corporations need to determine the basic requirements of the remote access connections and develop a cost effective strategy for meeting them. There is a wide variety of options available, ranging from in-house solutions based on simple dial-up services to completely outsourced services over a managed VPN.

**Connectivity Solution.** The connectivity solution is an important basic issue, and it ranges from a simple in-house dial-up connection to an outsourced VPN. Remote Access Servers (RAS) are a typical in-house dial-up solution, and they range from simple solutions supporting a limited number of ports up to stand alone server systems which may handle 190 ports and above. A VPN can be added to a RAS, which secures the solution but adds another layer of complexity.

Access may be through a dial-in 800 number—the earliest solution—through a private network, or over the Internet. For an in-house solution, one important consideration is the availability of networking skills. The alternative to an in-house solution is a variety of outsourcing alternatives, ranging from insourcing, where an experienced vendor takes control of internal network equipment and runs it, to outsourcing of various portions of the network infrastructure. One increasingly popular method is to offload remote access to a managed VPN provider, which may be an ISP, or a service provider specializing in VPNs and running them across the networks of other carriers. If an outsourcing solution is selected, then the solution can be further tailored as to bandwidth available, points-of-presence (POPs), Quality of Service (QoS) and so forth, all of which may be embodied in a Service Level Agreement (SLA).

**Basic Connection.** For an in-house solution or to evaluate an outsourced solution, it is important to first determine the number of dial-in ports that will be required, then determine an appropriate transmission rate. The number of ports depends both upon the number of telecommuters, and their data requirements—which can vary substantially, from occasional e-mail access to long periods of online data processing. Data transmission rate, or bandwidth, requirements depends upon the nature of the data. It might range from simple low speed telephone dial up service, to DSL or other broadband options, with some consideration also given to whether data needs to be delivered in real time—as for, say, voice or multimedia—or where a more irregular delivery—such as for long data downloads—is sufficient.

**Remote Access Type.** The type of remote access to be used may be an issue. There are two basic strategies, excluding intermittent connection for email. These are remote node or remote control, which can be mixed. With remote node access, users dial into the remote access server and become a conventional network client, often over a VPN. The user connects to a dedicated remote computer over the network, controlling that remote system; while display and data input are sent over the line, the application runs on the host computer, which performs all processing. Software making remote control possible includes Citrix MetaFrame.

**Security.** Any dial-up connection requires security provisions, and the network needs to be guarded by a firewall. Messages sent or data transmitted across the firewall may need to be ensured, either through simple message encryption or through the use of a VPN—which effectively create one encrypted tunnel that isolates all network data traffic from other traffic and from observation over public access facilities. SSL VPNs are beginning to appear, offering clientless remote access VPN connections. These have now begun to displace IPSec-based VPNs.

**Scalability.** Scalability is often a requirement, since recent history suggests that remote access
users—and per-user bandwidth usage—will both continue to increase. A system which cannot be easily and efficiently upgraded to meet new demands could be costly in the long run. This is one reason that modular solutions have become popular, and also fuels the market for outsourcing.

**Management.** There are also a range of management issues which need to be dealt with, one of which is how to provide adequate service and equipment support for telecommuters, far from the corporate help desk. Ease of use and standard operating procedures are necessary to ensure that remote users can be supported.

**Budget.** Budget requirements also need to be addressed, including not only equipment and software costs, but also any maintenance and support charges that will be incurred on an annual basis. If a Managed Service Provider is selected as the connectivity solution, then costs might be high, but they will be predictable and inclusive, with service guarantees that might be of more importance than cost savings.

**Telecommuting Employee Issues**

The remote access solution requires significant infrastructure at the corporate office, but it also incurs a variety of requirements at the client side to ensure that jobs can be handled efficiently. A telecommuter needs to have the capabilities of an office available, and that means performing tasks that are undertaken by network administrators, receptionists, and others in the corporate setting. The equipment available must be capable of handling the workload as well as ensuring that data is secure and communications are adequate. A special emphasis must be placed upon communications, because this is the area most likely to suffer in a move toward telecommuting.

Equipment required by telecommuters may include the following:

- **Personal Computer.** Requirements vary from remote and home offices, where a full-function desktop computer may be essential, to laptop computers for remote access on the go, or even PDAs and Pocket PCs—often used as a more mobile supplement the laptop or desktop system than as the main system.
- **Modem.** The modem, and its specifications, differ according to data and voice requirements. The base options are an analog modem—generally V90 or the new V92 standard—or ADSL, depending upon service availability. For on the road or highly mobile situations, a cellular modem or WiFi (802.11b) card may be considered.
- **Software for Communications, Collaboration, and Data Access.** A wide range of software products is available to support the teleworker, from basic communications programs to specialty products such as remote control products, where the remote worker takes control of a remote desktop PC which does the actual processing, collaboration suites such as Lotus Notes, and a variety of messaging products.
- **Telephone Connections.** Two lines are often required, though ADSL and V92 modem users, among others, can accept voice calls while in data sessions. Wireless connections and/or other broadband access systems such as cable modem, satellite, and microwave may also be considered, depending upon availability.
- **Voice Mail.** Telephone answering systems and voice mail are almost always necessary, even with wireless phones, to ensure that all incoming calls can be handled. Smart phone features, such as call diversion and caller identification can also be useful. These services can be handled either through installation of special hardware or as carrier services.
- **Security and Support.** Telecommuters need to have some form of data protection, such as a UPS—although laptops, with their integrated battery, can provide their own UPS capability. Some form of data backup is also necessary, and must be handled by the telecommuter, since there is no IT manager watching out for things or handling this as a routine task. Finally, the premises, including equipment, must be secured against theft. Laptop theft for the purpose of accessing corporate networks is, in fact, a considerable threat to overall corporate data security.
Analysis

Remote access and telecommuting are supported by a variety of government initiatives, by price reductions and improved technology in remote access solutions, by reduced dial out costs, by multiple PoP providers and the public Internet, and by a growing free agent community resulting from corporate downsizing and mergers.

Telecommuting provides a wide range of potential advantages to companies, including the following:

- Access to external talent, such as experts who live out of geographical proximity to the office.
- Improved efficiency and better communications. This is particularly important for road warriors, such as product representatives and agents. Seamless access to corporate data can be made available in virtually any location.
- Improved productivity for some workers, based on numerous surveys which have shown workers at home or on the road may be more productive than workers at the office, due to elimination of long commutes, improved focus and concentration, and capability for workers to set their own hours.
- Reduced operational costs through reduced need for expensive metropolitan office space.
- Improved employee morale, leading to better job satisfaction and lower turnover. A study at Nortel, for example, found that 90 percent of work-from-home employees reported increased job satisfaction and 73 percent had decreased stress levels.

These advantages can only be realized if an efficient and effective remote access infrastructure is put into place. As more and more companies turn to telecommuting and mobile workforce solutions, the range of options is likely to increase. Corporate IT departments need to develop a strategy that is suited to the specific conditions of their workplace, and supports the needs of telecommuting employees without compromising security and manageability.

One of the most promising areas of growth is in outsourced VPN services, which can provide secure access to corporate networks from numerous access points around the country, and can support sufficient bandwidth to handle most access requirements. Another area that needs to be examined is the growing use of wireless technologies, including broadband cellular and 802.11b. A wireless network can make the telecommuter truly mobile by bringing the office directly to the work situation—such as a client site, for sales representatives, or a remote equipment installation for inspectors.

Recommendations

Growth in telecommuting and remote access is inevitable. Companies are seeing continuing growth in the number of mobile professionals, as well as in the number of free agents working from home. The continued Web enablement of corporate networks and applications has encouraged this trend by making it possible to handle most tasks that might be undertaken by information workers from any location that might be served by an IP connection—whether through the public Internet or through dial in access to corporate servers. This has resulted in a proliferation of infrastructure solutions, and need to carefully evaluate remote access requirements to ensure that the most efficient and effective solution can be put into place.

Issues that need to be addressed include the number of telecommuters that need to be supported, growth and scalability, the type of workload to be undertaken, data requirements, communications requirements, security, available corporate network experience, and budget. An outsourcing solution is frequently the
最容易实施，且提供了各种额外的优势，但它可能很昂贵。对于拥有相对较少远程工作雇员的小公司，基于小型远程访问服务器的内部解决方案可能是首选策略。对于更大、更复杂或分布更广的解决方案，应选择基于个人互联网帐户或管理服务的策略——在两种情况下，通常使用VPN。在大多数情况下，可能需要一定程度的外包。

**About the Author**

Brian J. Dooley是Faulkner Information Services的常任撰稿人，并且是Faulkner的顾问委员会的成员。Brian在过去15年中一直在跟踪高科技行业，包括计算、数据网络和电信行业，特别是国际电信。

**Web Links**

[返回到报告顶部]

美国远程办公协会: [http://www.knowledgetree.com/ata.html](http://www.knowledgetree.com/ata.html)

Cyberworkers: [http://www.cyberworkers.com](http://www.cyberworkers.com)

FiberLink: [http://www.fiberlink.com](http://www.fiberlink.com)

国际电信工作协会及委员会: [http://www.workingfromanywhere.org/](http://www.workingfromanywhere.org/)

iPass: [http://www.ipass.com](http://www.ipass.com)

[返回到报告顶部]