



Update

Connecting the Remote End User: Finding the Right — and Safe — Solution

by Michael Enright,
Senior Consultant,
Cutter Consortium

Many IT executives have watched the proliferation of new Internet connectivity options with understandable caution. The Wild West world of supported and unsupported Wi-Fi hot spots in hotels, coffee shops, airports, and even homes presents attractive options for remote PC users looking to get online, but it also creates real security and system support concerns. As is often the case, the IT leader's challenge is to determine when to incorporate and support new technologies and services and what represents a deployable configuration that blends new capabilities with security and supportability.

Most companies today support only dialup connectivity for their remote users, but end users are becoming more and more attracted to the increased productivity promised by the "easy and pervasive" access of Wi-Fi hot spots and other connection methods. While at this point, perhaps only the usual suspects — the early-adopter technophiles — use the various Wi-Fi services or plug into wired Ethernet jacks in hotels, offices, and homes, more mainstream users are being enticed to try these connection methods, creating broader concerns about remote system stability along with data and network security.

This *Executive Update* explores some of the relevant issues

concerning today's commonly available connectivity solutions for remote PC users — dialup access, wired Ethernet connections, Wi-Fi, and cellular data networks — and proposes a hybrid solution that may provide the right blend of more pervasive access, increased productivity, and supportability for you and your remote users. We'll consider each technology/service across the following areas:

- **Distribution of connection points.** The overall distribution of the access points in urban or suburban areas for the given service. In rural settings, only dialup service is likely to be widely available.
- **Convenience.** The ease with which an end user can successfully connect to a service.
- **Supportability.** The likely impact of this service on the stability and functionality of a remote user's system and the resulting impact on the support organization.
- **Bandwidth.** The data rate (or range of rates) available with the service.
- **Security.** The high-level security issues for the service. A thoughtful risk assessment should be completed, and a network and data security policy should be developed and in place before

any remote access connection method is authorized.

DIALUP VIA PLAIN OLD TELEPHONE SERVICE (POTS)

Summary. Dialup is almost everywhere, usually easy and stable to configure and support, albeit at comparatively low data rates.

Distribution of connection points. The POTS network has an extremely broad global distribution of connection points (i.e., phone jacks).

Convenience. Using the dialup network from modern portable computers is generally simple once a suitable phone port has been located and the system connected. Most national or global ISPs provide “connection managers” that facilitate finding the best dialup phone number and connecting from a given location.

Supportability. Once a connection manager has been set up, most dialup networking seldom requires changes to system or network configurations, and many providers offer level 1 support for your end users as part of their service.

Bandwidth. Dialup connections are not fast by today’s standards; they’re commonly in the 20-kbps-to-48-kbps range.

Security. Unauthorized access to the network data between the remote system and network aggregation point is difficult due to the physical and logical topology of the circuit-switched POTS network. Most dialup services leave the remote system open as an IP-addressable Internet node, generally without a firewall.

A dialup variant worth noting that adds a significant degree of security is to have remote systems dial directly to a modem bank at the corporate firewall, bypassing the Internet. Connections made directly to the company network can have

a security profile similar to what exists on the corporate network (assuming proper configuration and physical security of the remote system).

WIRED ETHERNET

Summary. High-speed wired Ethernet connections are available in limited remote locations such as hotels and offices. Their availability is not likely to grow substantially, and while it’s often quick and easy for an end user to set up a wired Ethernet connection, it also can be troublesome and can create security and support issues.

Distribution of connection points. Availability of connection points is hit or miss, with most access in a limited set of hotels, offices, conference centers, and broadband-enabled homes with hubs or routers. Given the increasing distribution of Wi-Fi and other wireless services, it’s unlikely that the number of access points will grow.

Convenience. When the network behind the port is configured for “automatic network configuration” via DHCP, most modern portable computers will “just work” when connected, although occasionally only after a reboot. If the network does not use automatic network connection via DHCP, connecting a system may be difficult.

Supportability. If the network behind the port uses DHCP, and if your remote systems are reasonably modern, supporting wired Ethernet connections is usually fairly trouble-free. When remote networks require manual configuration, or a unique connection manager or a proxy server must be configured to enable access, support may become an issue. Occasionally, end users or third-party technical support personnel will modify important system and networking parameters, creating future system configuration problems and security issues.

Bandwidth. In general, the LAN speed will be between 10 and 100 Mbps, and the Internet network connection speed will frequently be 1 Mbps or greater.

Security. It’s not possible to determine a “normal” security profile for a wired Ethernet connection because, to a large degree, the network topology determines the ease with which data can be captured and a system probed or attacked. Some situations are by their nature more secure (as, for example, when the Ethernet port is on a switched network behind a trusted corporate firewall versus when the port is on a “shared wire” hub network and connected directly to the Internet without a network firewall). Support for wired Ethernet will likely require the assumption that the system will be on an “open” network and exposed as an unprotected node on the Internet.

WI-FI (802.11B AND 802.11G) HOT SPOTS

Summary. Commanding a large share of today’s buzz, Wi-Fi is perhaps the technology that will most generate end-user enthusiasm for more pervasive online access. But with occasionally complicated connection requirements, different security models, and a mix of free and for-fee services, it may be the most frustrating for end users as well as a difficult and expensive technology to support.

Distribution of connection points. Wi-Fi access points seem to be sprouting everywhere, some as fee-based services offered by companies in hotels, stores, restaurants and airports; others offered deliberately as free network connection points; and many unknowingly left open to the world when Wi-Fi is installed as part of a home or business network.

Convenience. Wi-Fi hot spots create a heterogeneous set of services that overlap at times, utilizing a variety of security methods,

commonly including unprotected or open Wi-Fi access points (those with no security enabled); Wired Equivalent Privacy, or WEP; and the more secure Wi-Fi Protected Access, or WPA. Each encryption method requires a unique configuration in the mobile system, and the tools and operating system support for configuring and connecting to a Wi-Fi access point remain complex and difficult to use. When Wi-Fi “just works” — particularly when a system auto-configures to an open network with a broadcast network name (service set identifier, or SSID) or when the user has signed up with a particular Wi-Fi service provider that limits connections to its hot spots — remote systems can connect fairly easily. When Wi-Fi doesn’t “just work,” connections can be downright frustrating for end users.

Supportability. If remote users limit themselves to one Wi-Fi service provider, and a single network profile can be created and supported for that service, support of Wi-Fi can be minimal, but this configuration limits online access greatly because no provider today has pervasive coverage. Support for end users attempting to use multiple services, or enabling end users to self-configure for “found” Wi-Fi access points, will likely be difficult, expensive, and potentially frustrating for both end users and support organizations.

Bandwidth. The speed of a Wi-Fi connection depends on both the variant of Wi-Fi available (802.11b provides up to 11 Mbps; 802.11g up to 52 Mbps) and the signal strength at the remote system (Wi-Fi connection speeds decrease as the signal strength weakens). The Internet network connection speed between the access point and the Internet will frequently be 1 Mbps or greater.

Security. As with wired Ethernet, it’s impossible to declare a “normal” security profile for a Wi-Fi connection, but security may be

more of a concern for Wi-Fi than wired Ethernet because of the common availability of open Wi-Fi access points and the ease with which Wi-Fi enables a malevolent user to access the network. IT managers will likely have two options: (1) assume all Wi-Fi connections are open with unencrypted network traffic and Internet-visible systems and configure the systems accordingly, or (2) create a known, secure Wi-Fi profile and limit Wi-Fi use to services that support that profile.

CELLULAR DATA NETWORKS

Summary. Cellular data networks provide always-on networking covering much of the population centers and transportation corridors where business is transacted. The service can be provided and supported by a single partner, at data rates from dialup equivalent to broadband levels.

Distribution of connection points. Cellular data networks cover most metropolitan business areas and many of the transportation corridors in the industrialized world. Inside coverage areas, connections are possible almost anywhere, similar to areas where a cell phone can be used. While the cellular carriers continue to invest heavily in upgrading the speed of their data networks, it’s not likely that the data network footprint will change significantly in the short term (to cover more rural areas, for example).

Convenience. Connection to wireless cellular data networks is likely to be similar to dialup networking in ease of use. Most service providers have connection manager software that enables one-click connections to their networks, usually via a PC card added to a laptop.

Supportability. Once a connection manager has been set up, cellular data networking seldom requires changes to system or network

configurations, and many service providers offer level 1 support for end users as part of their service.

Bandwidth. Today’s cellular data networks are a combination of various 2.5G and 3G technologies, and data rates vary with signal quality. In general, today’s cellular data networks provide data rates of between 20 kbps and 2 Mbps or more, with a minimum of 30 to 40 kbps commonly available.

Security. Network traffic is comparatively secure, as many networks incorporate encryption in their systems. But security must be determined for each service and underlying technology. Most remote computers on a cellular data network will be visible as IP-addressable nodes on the Internet.

WHERE DOES THIS LEAVE US?

The time has come for IT leaders to plan for their next generation of supported remote Internet access, particularly as more mainstream end users are increasingly likely to attempt to use one or more of the various connection options, raising the probability of security lapses, creating new support issues, and increasing the cost of inaction.

A hybrid solution combining cellular data networking with dialup as a backup connection method is a reasonable option as a deployable solution for enabling increased online productivity while maintaining service levels, system integrity, and information security. Service providers such as T-Mobile, Cingular, AT&T, Verizon, and Sprint in the US, and T-Mobile, Vodafone, and NTT DoCoMo internationally, cover most of the urban and suburban environments in which business is transacted, and their services enable easy login with a stable, remote network configuration for your remote systems. Cellular data network connections are at least as fast as dialup and available

almost anywhere in covered areas, enabling laptops to be booted up and online within a couple of minutes, so users can quickly check or send e-mail or verify online business data before (or during) meetings. Since network signals are inevitably not available everywhere (and likely never will be), dialup provides an effective secondary connectivity method, and many of the cellular carriers can also supply national and international dialup service plans. Some carriers even have a network of Wi-Fi hot spots that augment their cellular data networks.

In the meantime, Wi-Fi services will continue to evolve, with the potential for both broader distribution of access from single partners and the creation of Wi-Fi roaming capability in the future. Wired Ethernet will continue to be available and may make sense as part of a supported corporate solution, particularly if your company does business with a large provider of wired Ethernet products. Dialup will clearly continue to provide an important base level of connectivity, with dialup access's stability, ease of use, and the near-universal availability of access points making up for its lower data rates. And of course, there are always new technologies arriving, such as satellite data networks, WiMAX, in-flight Wi-Fi Internet access on aircraft, and even Bluetooth-enabled solutions looming in the future.

If you're ready to consider adopting a new remote access solution, a reasonable approach would be to initiate a pilot program that would include some of your organization's early-adopter end users and members of the technology organization itself. The goal of the program would be to test actual services and

configurations to determine which service provider, if any, most closely matches your needs, including:

- Demonstrated usability of the network for business and productivity applications
- Successful implementation and usability of a single connection manager, enabling connection to the first choice and backup connection methods
- End-user usability, quality, and consistency of experience
- Analysis of the advertised and observed network coverage
- Adequacy of level 1 support
- Network support of non-PC devices (e.g., 3G cell phones, PDAs)
- Pricing
- Quality of the service provider as a partner

At the conclusion of your pilot program, you'll be in a position to either (1) create a proposal and action plan for broader rollout of new remote connection services and remote system configurations for remote users, or (2) create a document demonstrating the proactive analysis of the opportunity and the issues and shortcomings found with the new connection technologies and services. This document can be distributed to others in management as well as to remote users to help them understand the issues preventing the company from enabling new and otherwise attractive remote connection solutions.

The assessment and piloting exercise should be repeated as remote connection technologies

and services evolve, probably every 18 to 24 months. This will continuously position your company and IT organization to effectively address changing user requirements and expectations in the face of new options for pervasive, always-on computing for remote users.

ABOUT THE AUTHOR

Michael Enright is a Senior Consultant with Cutter Consortium's Business-IT Strategies Practice and President of Hamilton Technology Advisors. At Hamilton Technology Advisors, Mr. Enright brings more than 20 years' experience in the creation of leading-edge technology-based products and services to business executives, technology leaders, and investment professionals facing important business and technology decisions.

Mr. Enright recently served as CTO at Harvard Business School Interactive, where he led the development and launch of several new distance-learning products for HBS. Mr. Enright's experience includes leadership roles at IBM, Digital Equipment Corporation, and Compaq as well as in fast-moving, high-growth companies such as Wavefront Technologies, Spyglass, Cambridge Research Associates, and CMGI/MyWay.com. He has extensive technical knowledge and experience in scalable networked systems, Internet and Web technologies, wireless networks and mobile computing, digital audio and video production and delivery, high-performance computing, collaboration and community networking applications, 3-D graphics, knowledge management, and data visualization. He can be reached at menright@cutter.com.