MOBILITY
REFERENCE GUIDE

The collaboration and communication advantages of mobile technology

CDWG.com/mobilityguide | 888.563.4239

CDW·G®

The Right Technology. Right Away.®

MOBILITY
REFERENCE GUIDE

TABLE OF CONTENTS **CHAPTER**

WHAT IS A CDW•G REFERENCE GUIDE?

At CDW•G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology. Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

» We are pleased to also offer the **CDW•G IT Investment Guide.** It includes products and information to help you meet your mobility objectives.

MOBILITY'S VALUE PROPOSITION

NEW COMMUNICATIONS OPPORTUNITIES HAVE NUMEROUS BENEFITS

CHAPTER 1:

If the technological marvel of the 20th century was the ubiquitous switched-circuit telecommunications system, the early 21st century's equivalent is the build out of the data-everywhere, access-anywhere network. Whether running over copper, fiber optic or wireless, 21st century networks grow bigger and faster with each passing day.

The evolving way that organizations and individuals work is both driving and being driven by the spread of network technology. Work staff, partners and contractors are increasingly mobile and less tethered to a specific building or geographic location.

Over the next three to five years, one of IT's greatest challenges will be adapting these newfound mobile products and capabilities to the workplace. This reference guide serves as an introduction to developing a mobility strategy for your organization.

TRENDS IN MOBILITY

In the 21st century, high-speed communications coupled with expanding computing power (the size and cost of which continue to fall exponentially) has given people increased mobility and unheard of communications opportunities. Consider some of the options today:

- New organizations whose products and services are primarily knowledge-based can start out virtual, skipping the costs of real estate and associated overhead. Cloud computing and software as a service can postpone the need for a data center.
- Staffers can use technology to collaborate in a variety of ways, eliminating issues related to time and distance. Individuals can blend the puzzle pieces of their personal and work lives in such efficient ways that both benefit. Staff waiting at home for the plumber to show up? It's not a problem to continue working when they have access to a wireless notebook and the organization's virtual private network.

Moreover, realizing that productivity goes up when people have access to technology, organizations can significantly reduce fixed costs tied up in office space while offering greater flexibility to their staff and themselves. Talent can be found and hired anywhere without the need to relocate.

The green movement has given added impetus to the adoption of mobile technology simply by offering many people an alternative to the daily automobile commute. For those who must commute or travel as part of their job, onboard electronics even connect automobiles to the Internet.

Coupled with the virtualization of data center resources, which also reduces energy consumption, mobility has become an important component in many organizations' efforts to reduce their carbon footprints.

A subtle but equally important trend is being spurred by faster, more reliable and more ubiquitous wireless networks; lighter, faster and more graphically powerful portable computers and smartphones; and lower cost, yet stronger, security technology.

The cumulative result of all these advances is a more social, collaborative communication experience that greatly enhances the people-to-data connectivity that has defined mobility until now.

This offers an enormous increase in the return on investment of mobile capabilities. Thanks to more robust and flexible

Mobility Benefits Checklist

Any return on investment analysis should factor in both the measurable and intangible benefits of mobility, including the following:

- BETTER SECURITY: This encompasses less risk of financial or proprietary information loss; improved physical security derived from the ability to locate surveillance tools anywhere; enhanced continuity of operations due to improved remote access for staffers; and cost savings gained from shuttering expensive emergency sites.
- MORE RELIABLE COMMUNICATIONS AT LOWER COST: This means consolidating voice onto the IP network at headquarters and other large locations, and possibly eliminating redundant fixed-phone facilities — whether Voice over Internet Protocol (VoIP) or switched — for remote and mobile staff. After all, in this day and age, most people have a cell phone.
- TIGHTER INVENTORY CONTROL: The wireless infrastructure makes possible radio frequency identification of assets, including everything from notebooks to vehicles. Check with insurance carriers to see if premiums for loss coverage are negotiable when better controls are in place.
- REDUCED TRAVEL EXPENSES: Digital video and online collaboration tools have advanced to the stage where travel can be limited to only those trips that are absolutely necessary. Training, new deployments or service rollouts, and partner negotiations can all be accomplished more efficiently through video conferencing.
- INCREASED PRODUCTIVITY: The flexibility gained by staff who spend less time commuting back and forth to regional offices or headquarters often yields better performance.

provisioning, monitoring and access control technologies, this collaborative interaction extends to those people who the organization serves.

I.T. TOOLS IMPROVE

More efficient technologies benefit not only mobile staff and their project teams, but also the organization's network administrators and its technology teams.

For example, wireless network control tools coupled with faster 802.11n LANs offer unprecedented levels of performance and manageability. But they also add complexity to WLAN management in organizations with both 2.4 gigahertz and 5GHz networks. IT departments need to do their homework before buying a WLAN management tool, asking questions such as:

- Will the tool support the topologies as well as the specific gear already being used?
- Will it perform well with the wired LAN control tool?
- Is the tool's reporting compatible with the IT department's dashboard setup?
- Does the tool scale over time, and does it quickly reflect changes in day-to-day or even hour-to-hour utilization of the WLAN?
- How well does the management tool cover individual users' permissions and authentications?

With wireless implementations, as with security, maintaining a high-quality experience for users doesn't just happen. It requires planning. The growing spread of wireless networks throughout organizations, coupled with the diversity of standards that likely exist side by side, requires a remote, automated approach to managing access points.

Management includes more than monitoring whether APs are on or off, but also watching load performance and looking out for interference that might necessitate channel adjustments.

As capable as WLAN management products are, they must be evaluated in the context of their ability to work with your overall network plan. Along with the wireless devices, the rest of the infrastructure needs to be monitored and controlled as well.

This includes the switch and router configuration; security, authentication and ID management; and application performance. Meanwhile, network traffic is growing, and it all eventually ends up on the wires. Driving this growth are voice, video and rich media applications that ride right along with your data.

THE MOBILITY PLAN

As we'll discuss in more detail throughout this guide, whether you are planning to deploy a greenfield wireless network or adding to and updating an existing WLAN, you need to take three fundamental steps.

The first step is gaining a clear understanding of the goals of the network. This is derived from what the organization's management and staff need to do their jobs. But the IT team doesn't need to wait for guidance. It can make the case for new wireless and mobility technology and how it can help the organization accomplish its strategies and missions.

The second step is the site survey, which determines the most efficient way to lay out and install new equipment. The goal of the site survey is an efficient WLAN, with sufficient but not redundant coverage.

Tools for measuring radio broadcast patterns and interference can speed up the site survey, but there is no substitute for an experienced technician in surveying the targeted facilities. See Chapter 2 for details on performing this fundamental task.

Step three is security planning. Network access control (NAC) applications have come a long way in the past few years. They are the basic enforcers of enterprise policies for trusted use of the network, but they are only part of the picture.

Firewalls, antivirus software, single-use passwords, packet inspection and analysis are also major components in the security chain. Cloud storage and desktop virtualization might also figure into security planning, given that they can keep applications and data in stateless and more manageable forms.

Security planning extends to the endpoints, not just to ensure that only trusted users and devices can access the network, but also to reduce exposure in the event that a staffer's notebook, tablet, netbook or cell phone is lost or stolen.

Finally, the mobile plan should take into account the constantly changing types and form factors of endpoint devices. The challenge is to ensure user satisfaction while limiting devices to a manageable number. Desktop virtualization may offer an answer, allowing the network team to focus on the virtual software builds while users choose whatever devices they prefer. ◊

MOBILITY ARCHITECTURE

MAPPING OUT YOUR WIRELESS NETWORK

CHAPTER 2:

Implementing a mobility strategy for staff, contractors and guests is a lot easier to execute when the IT team works from an architecture — that is, a framework for all of the existing and yet-to-be-installed technology. The mobility architecture has two purposes.

First, it helps make sure that all technology deployments aim to serve the organization's mission by supporting users with necessary services in a reliable and secure manner. And second, the architecture ensures that technology is deployed efficiently, using standards and maintaining agility for future additions or upgrades.

The term "mobility," for our purposes, is synonymous with wireless, and wireless networking standards have been constantly evolving since their introduction. An architectural approach lets the organization plan for changing technologies.

THE 802.11n STANDARD

The Institute of Electrical and Electronics Engineers (IEEE) has continuously updated its 802.11 wireless standard since its inception in the late 1990s. Each generation of the standard, embraced under the Wi-Fi banner, advances the speed, security and reliability of wireless LANs.

Each iteration has spent several years in gestation. What happens typically is that products regularly come out carrying the latest designation before it is finalized. With each successive generation, early adopters have emerged that test out the technology and share their experiences with the IT community.

The newest version is 802.11n. It was adopted in final form in fall 2009 after a long debate and many revisions. 802.11n is significantly faster and less prone to radio interference than its predecessor, 802.11g. It operates in the 5 gigahertz range and can yield theoretical maximum data transfer speeds of 600 megabits per second.

Relative to the 2.4GHz band used by earlier 802.11 equipment, 802.11n is more immune to static from Bluetooth transmissions, wireless telephones and the ubiquitous microwave oven. The fast data transfer is achieved by using multiple antennae and a technique called spatial division multiplexing. Together, this is known as multiple input, multiple output (MIMO) transmissions.

If lack of interference and data motion at wire speeds convinces you that 802.11n is WLAN perfection, you're only half right. In a greenfield installation, a purely 802.11n environment might tempt some CIOs to dispense with the installation of fixed Ethernet wiring altogether.

In such an environment, keep in mind that not all 802.11 routers and access points (APs) are created equal and that much testing would be required to check data speeds relative to distance from a particular manufacturer's AP. Plus, the remote manageability and Quality of Service (QoS) options in 802.11 equipment, whether using standard g or n, vary from manufacturer to manufacturer.

But this discussion is somewhat more academic than real world. Few enterprises can actually have a pure 802.11n installation if existing infrastructure already includes 802.11g. It's also unlikely that every client PC would initially have an 802.11n card. So until

all clients are upgraded or replaced, the IT department will have to contend with a mixed 802.11g/n environment.

That means there are trade-offs to be considered. For example, it may be necessary to run the newer 802.11n APs in dual mode to accommodate the legacy gear.

Power poses another issue. 802.11n equipment in dual mode or in full MIMO requires more than the standard 13 watts available via Power over Ethernet (PoE), which is sufficient for 802.11g. That may require the added cost of running AC electrical wiring to AP locations.

There is also the enterprise-wide network to consider. Ultimately, Wi-Fi traffic reaches the wired backbone. Given the speeds achievable with 802.11n, network administrators should plan for increased video, voice and other multimedia data. This backhaul traffic can slow down the core network for all users — mobile and tethered — while causing degradation in latency-sensitive material such as Voice over Internet Protocol (VoIP).

Other Mobility Options

Slower to develop as a market in the United States, networking based on the IEEE 802.16 standards uses microwave radio transmissions to connect remote locations or enable mobility in campus or building settings. Around 2001, the wireless industry dubbed these technology offerings WiMax.

The newest version of the standard, 802.16y-2008, applies to equipment operating at or just below the 3,700MHz band. Use of such equipment requires a license (and a license fee) from the Federal Communications Commission.

Microwave technology supports WiMax distances of up to several miles, depending on the power of the equipment used. Thus, WiMax can be effective in delivering outdoor connectivity, for example, by bridging cellular service to Wi-Fi hotspots. But microwave links require line-of-sight connectivity.

Cellular access should not be confused with WiMax. Many organizations simply purchase cell service accounts coupled with external devices that attach to notebooks via USB or PC cards. Some interior locations benefit from cellular signal boosters. Newer notebooks have third generation (3G) cellular antennae built in, but that can limit the choice of carriers.

Cellular data accounts can be expensive. Individuals may pay $60 per month or more for unlimited downloads. But organizations should use their buying power to negotiate rates based on anticipated bundled requirements, just as they do for voice cell phones. A workaround option is to have staff use their cell phones for mobile data access.

For many organizations, having their users access network resources without the need for an Ethernet cable (via Bluetooth technology) is a handy way to solve the "last mile of access" issue. Recent software improvements have simplified the pairing function between Bluetooth devices, making local printing, synchronizing smartphones and enabling hands-free phone operation routine.

In deploying Bluetooth, which operates in the 2.4GHz range, network administrators must keep in mind the potential interference caused by two closely situated devices running on the 2.4GHz band: Bluetooth devices and 802.11g gear.

The effect of interference is a squeeze on throughput, not an outright loss of connection. The causes of interference are complex, rooted in the differing protocols employed by the two technologies. As a practical matter, IEEE research on collaboration techniques has minimized the interference problem.

CONDUCTING A SITE SURVEY

The irony of mobility is that the provisioning of mobile technology itself requires detailed analysis of the fixed infrastructure of equipment that gives users the ability to operate anywhere. That's where the site survey comes in. A successful site survey requires a thorough understanding of goals, applications and acceptable network performance characteristics needed to make mobile work fully productive.

In recent years, the increasing popularity of mobile apps has raised expectations of what the network ought to be able to deliver at the workplace. Perceived technology gaps between personal and work experiences can affect morale among an organization's staff.

So think of the site survey as the CIO's homework. Specifically, the site survey should lead to an installation with these characteristics:

- Guaranteed high network availability, with no dead zones, areas of high interference or low bandwidth locations;
- Scalability, which allows for the addition of more users without sacrificing performance or swamping the core network;
- Central management, which is more than rooting out rogue wireless clients or access points, important as those duties are.

Moreover, the site survey should encompass what might be called "buildability." APs must be mounted somewhere, and must be fed with Ethernet wiring. Some, as noted, will require AC power.

Physical security of devices and respect for the visual or design integrity of the facility are also key factors to balance against economical installation and access for repair or replacement.

Conducting a site survey comprises a combination of tasks. It's an eyes-open inspection of the facility, looking for sources of interference or signal blocking. And it's a measuring exercise, using tools for creating an efficient AP placement map. (Tools used for the site survey are a matter of choice. Manufacturers of

networking equipment offer tools of their own, but several third-party vendors also offer tools.)

On the physical front, the survey team must note things such as large support columns, service areas with microwave ovens and specialized equipment that might induce interference. For example, access might be needed in rooms containing elevator gear; heating, ventilation and air-conditioning (HVAC) equipment; or electrical distribution junctions.

Also, be alert for labs or clinical areas containing domain-specific gear, such as medical or scientific equipment. You'll also want to watch for potential environmental hazards, such as moisture, vibration or temperature extremes.

The site team can save a lot of time initially by using a blueprint or map of the facility that provides a picture of which obstacles can be moved and which can't.

AP placement is complicated by the completion of the 802.11n standard. To start with, the predictive radio performance analysis software the site team uses will require upgrading (although you will still need to take multiple measurements that include signal strength as well as quality, expressed as signal-to-noise ratio at different distances from each AP location).

The coexistence of both 802.11b/g and 802.11n requires careful planning to avoid interference with legacy 2.4GHz equipment. The a/b/g standards use bandwidth differently than n, so if the network staff expects to support the older standards, this will affect both the location of 802.11n APs and whether they are set directionally or to multipath mode.

That's why keeping a detailed map of existing and planned infrastructure is so important. Not all APs will be set the same way. And for the site survey, testing should be done with the manufacturer and model of the AP to be installed.

APs are not all created equal, even if they are certified under the same standard. The biggest variable among APs is their fall off in signal strength with distance. Keep in mind that one goal of the site survey is to produce a plan for a mesh of wireless coverage with neither the inefficiency (and cost) of overlap nor dark areas of low connectivity.

Throughout the site survey, it is important to always keep applications and users in mind. For instance, wireless VoIP is more sensitive to slowdowns and latency in packet delivery than other types of data transfers. Ask whether video, large files of still imagery or other demanding applications are expected.

Another factor to measure is capacity per sublocation. A large classroom or auditorium might be expected to house tens or hundreds of simultaneous users, creating periods of peak demand. Small conference rooms and workgroup areas can probably get by with less coverage.

And as noted, beyond the wireless upgrade itself lies consideration of the wired backbone and whether it is up to the task of handling traffic from the mobile network without becoming a bottleneck. For many organizations, the biggest client on the backbone will be the mobile network.

LOCATION SERVICES

A well-planned mobility architecture and resulting network are determined primarily by users and the mission of the organization. But the network also provides services useful to the CIO and technical departments, thanks to its ability to correlate activities and assets with logical and physical locations within its boundaries — and beyond.

Location services can serve both mission and support activities. Either way, they share the ability to triangulate among radio sources to give the approximate location of assets ranging from cell phones to vehicles. When combined with widely available geographic positioning services, location services can extend

Teaming Wi-Fi with RFID

Data loss is a recurring security problem for a data-dependent organization. And one of the most low-tech ways to lose data is via mobile users who misplace their notebooks, tablets and cell phones, or have them stolen.

Luckily, most notebook thieves only want to make a few dollars on the hardware, so they often wipe the hard drive or remove it and throw it away.

You can't do much about lost or stolen assets from airports or car trunks. But coupling radio frequency identification (RFID) with the enterprise mobility network enables the tracking of IT equipment and any item to which a Wi-Fi RFID tag can be attached.

This combination of Wi-Fi with a real-time location system (RTLS) application helps you avoid the need for a separate RF network that could cause interference with the mobility network and double costs.

And 802.11 RTLS is more than a security approach. To bring mobility full circle, it can enhance services to mobile users in a variety of ways.

For instance, it can help people find a cart-mounted television, video conferencing gear or any needed piece of equipment. Passive tags added to staff ID badges can let others throughout a building or campus know when a particular conference room is occupied. They can also help people find other people.

beyond the organization's own network.

For network administrators, an important location service is keeping track of mobile assets. Knowing the whereabouts (and time-of-day usage) of notebooks and smartphones can help recover lost items and reveal suspicious use patterns.

Comparing the number of devices at a given location with the site plan's estimates also provides information that can help the network team coordinate and adjust AP density and layout to better match real-world needs.

Coupled with a geographic information system, location services include vehicular tracking information that can be loaded into route-planning software programs. That puts mobility to work on operational cost containment.

Location application services deliver value-added information based on knowing where items are. For government agencies, grant applications, economic development efforts, emergency dispatch, and maintenance of parks, roads and buildings exemplify activities benefiting from location application services.

For educational institutions, such services can assist with keeping tabs on AV equipment, tracking the utilization of classrooms and other facilities, and recovering lost or stolen notebooks in one-to-one programs.

MANAGING THE WLAN

A wireless mobile network implementation requires sophisticated management systems equal to that of a wired network. One of your WLAN's most valuable management systems is remote monitoring (RMON). Planning for monitoring of the mobile network is a discipline unto itself.

An important driver for RMON planning is the degree of granularity the IT staff requires. For example, will it be necessary to assess the health of each AP, or will it be sufficient to see how segments of the network are working by relying on onsite investigation of alarms that might arise within a given segment?

Best practice today means integration of wireless and wired network management through a single console, a solution available from a variety of vendors.

Whereas wireless networks in the early days of Wi-Fi were often added ad hoc (perhaps at the behest of individual users or workgroups), mobility is an assumed capability of the 21st century enterprise network. Mobile users expect the same level of service and bandwidth as those who never unplug from the wired infrastructure.

Using a controller-based management architecture, system administrators can monitor wireless APs for performance, remotely configure them or even shut them off. The administrator can also monitor and adjust the interaction between APs and the backhaul function to the network switch, which aids in the diagnosis and repair of bottlenecks before they affect users. Modern network managers incorporate robust reporting functions that summarize operations over time.

Security considerations also drive RMON planning. It might be necessary to do 24x7 monitoring of outdoor network segments; the same goes for segments of the network in high-traffic or high-occupancy areas. Conference rooms and areas that are typically empty at night might require less oversight during off hours. System administrators should also watch for unauthorized or rogue devices attempting to join the network.

The management plan should couple with the user support plan. In instances where the IT department desires manned RMON at all times, it doesn't necessarily have to offer user support. For example, an organization with 10,000 daily mobile users could offer 6 a.m. to midnight support six days a week, striking a balance between adequate user support and costs. ◊

MOBILE INFRASTRUCTURE SECURITY

KEEPING YOUR DEFENSES UP TO DATE AND ROBUST

CHAPTER 3:

Infrastructure and Network Security

Protecting Your Wireless Network

Endpoint Security

In this day and age, it's a wonder that network and security administrators are able to sleep at night. Hardly a week passes without news of a large cybersecurity breach taking place somewhere. Networks in both the public and private sectors are under assault.

Chief information security officers are confronted with an Internet environment in which their networks are continuously probed and attacked. And by all expert accounts, the motivation of cybercriminals is becoming primarily economic.

Money and industrial or trade secrets seem to be the primary goals. But data of any kind has potential value to someone somewhere. So no one is safe from this burgeoning threat.

The technologies and products that support mobility add to the complexity of the cybersecurity challenge. Wireless networks, if not secured and managed properly, present a distinct class of vulnerabilities. Mobile applications — and the simple fact that staff are often traveling around carrying gigabytes of their organization's information — create both cyber and physical vulnerabilities.

But neither the mobility industry nor government and educational organizations are sitting idly by, hoping for the best. On the contrary, these groups are partnering to discover best practices and standards for cybersecurity.

Cyber defense is never a set-and-forget function. Cybercriminals are endlessly adaptive in their enterprise. Each time one vulnerability is addressed, the cybercriminals find another way in.

Security experts agree it would be an overwhelming task for any organization, whether a small school district or the Department of Defense, to analyze and respond to every threat on the Internet. No one can control the threat environment any more than one can control the weather.

A far more effective and efficient approach is to continuously assess your own organization's vulnerabilities, create a strategy for protecting them, then maintain the defenses.

INFRASTRUCTURE AND NETWORK SECURITY

Protecting the mobility environment is a subfunction of protecting the organization's network. Protecting the infrastructure requires an in-depth approach. Such a strategy plays out in several ways. Here are some examples:

- Encryption of data is applied not just to data in motion through the virtual private network (VPN), but also to data at rest both in the data center and on mobile devices.
- A simple password approach to access is replaced with a two-factor authentication plan, or with extremely sensitive resources, three-factor authentication, which can be accomplished in ways that don't overly frustrate users.
- Remote network monitoring is augmented by physical surveillance and sensor information as part of a continuity of operations (COOP) plan.
- Firewalls, in conjunction with specialized tools that gather detailed network information, are used to conduct forensic investigations into events after they happen.

WIRELESS SECURITY CHECKLIST

An assessment of wireless networks should answer these four basic questions:

- Is the radio coverage adequate?
- Are all of the access points configured so that they comply with the organization's policies?
- Have all vulnerabilities been identified?
- Can rogue devices be detected?

- In-house staff who operate and secure the network are augmented when appropriate with specialized managed-service providers.

A strategy starts with knowing your vulnerabilities and maintaining a list of your most important assets.

It's important to remember that basic network security maintenance is vital to an organization's mobility strategy. Remote and mobile workers may be profoundly affected by denial of network resources.

A vulnerability assessment can be made using any of the numerous proprietary and open-source tools that are available. Better tools that give you a more thorough assessment can aid in demonstrating compliance to various standards, such as Sarbanes-Oxley (SOX) rules, the Federal Information Security Management Act (FISMA) or the Payment Card Industry Data Security Standard (PCI DSS).

Tools can also generate reports on your network's vulnerabilities and compare them with the National Institute of Standards and Technology's annually updated National Vulnerability Database.

Even before deploying a tool, the network team should take some basic steps, including the following:

- Make sure security patches for operating systems, web browsers and other software components are up to date.
- Update your antivirus, antispyware and antispam filters.
- See if password and other credential policies are sufficiently robust. For example, does your organization require that passwords be at least eight alphanumeric characters in length?
- Have up-to-date knowledge of the top cybersecurity risks. Several nonprofit organizations, such as the SANS Institute, regularly publish updated lists of the most common Internet and application vulnerabilities.

From a technology standpoint, network and infrastructure security depends on several classes of products.

Firewalls are the most basic appliance for protection. They consist of software tools that scan incoming packets for anomalies or indicators that represent unauthorized traffic. Firewalls can be purely software but typically are hosted on a dedicated rack appliance. They perform a variety of techniques that can be purchased in all-in-one devices or as individual point solutions.

An emerging class of tools collects large volumes of data about network traffic and couples that collection with analysis that provides forensic, after-the-fact information about intrusions. Other tools add analytics to pinpoint network and application problems.

Antivirus software operates at the firewall, server or individual workstation level. The variety of malware being used by cybercriminals is rising at an accelerating rate, so it is important for antivirus products to be updated regularly.

Do-it-yourself security is complex and expensive. Many organizations outsource all or part of their cybersecurity. Third-party vendors offer various levels of service ranging from comprehensive operation of security functions to providing incident response and remediation. Other services include network monitoring and supplying threat intelligence gleaned from sensors scattered throughout the Internet.

PROTECTING YOUR WIRELESS NETWORK

Within the domain of cybersecurity, protecting a wireless network is a subspecialty because of the added dimension of radio. The basic objective of a wireless-network security plan is network access control (NAC). Authorized users have controlled access at the server, application or file level depending on their individual role. But NAC blocks any network access from unauthorized or nontrusted endpoints.

Wireless security, since the advent of wireless networking, has been a constant work in progress. Early (and relatively weak) security standards, created by the industry itself through the Wi-Fi Alliance, were superceded by the IEEE 802.11i standard, adopted in 2004.

Since then, Wi-Fi Alliance certification has gone through two iterations. To be certified today, products must have a WPA2

designation, which refers to the second generation of an 802.11i implementation called Wi-Fi Protected Access.

Think of WPA2 as the wireless-device industry's approach to implementing the IEEE standard. WPA2 also meets Federal Information Processing Standard 140-2, published by the National Institute of Standards and Technology (NIST).

As background for implementing a NAC tool, it's worth noting that use of industry-standard products will make it easier to implement a security program that includes access control.

For the wireless network, NAC takes two forms. It can either prevent the addition of rogue access points (APs) to the network using an Ethernet port, or prevent unauthorized access to an authorized AP.

Rogue access points are sometimes installed by staff with the best of intentions, such as improving localized radio reception. Or they can be installed secretly by either internal staff or visitors wishing to do harm. Rogue access points have been found hidden in wiring closets, even within racks.

Regardless of how they were installed, rogue APs pose three threats:

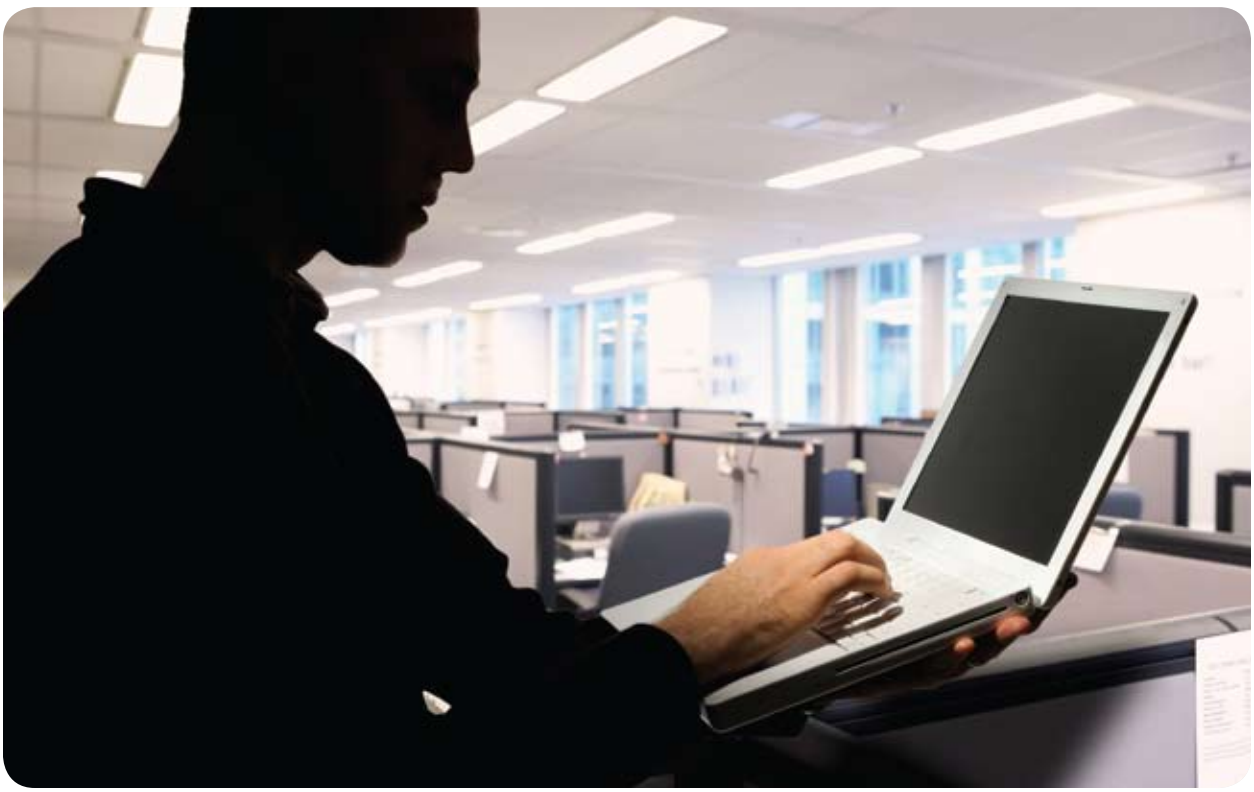
- The potential for unauthorized access to network resources;
- The potential for interference with the coverage and reception patterns established following the site survey (see Chapter 2);
- The possibility that a misconfigured AP will create security vulnerabilities on the network.

Prevention of rogue APs starts with a comprehensive map of those approved by the network team. Meanwhile, administrators should reiterate that neither staff nor guests may plug in their own APs.

Beyond that, finding rogue APs requires a detection tool. Here again, there are robust proprietary and open-source choices. They analyze traffic on the network to detect and locate APs that don't belong and assess the threat level they represent.

Rogue APs can also be found by monitoring radio signals in a given airspace. Unwanted signals will quickly pinpoint the location of unwanted devices.

Stopping access initiated by rogue devices requires more than password protection on the network. A comprehensive NAC tool challenges devices attempting to connect on the basis of user identity and network security policies. It should be **f**exible enough to allow guest access for vendors and other visitors, and can be configured in a variety of ways depending on whether the main concern is malware, policy enforcement or guest access.



Is Managed Security Right for You?

Total cost of ownership analysis often makes the case for adding contractor support to the management of an organization's network security. Here is a list of questions you'll want to ask for evaluating potential partners and building your service-level agreement.

- Does the provider have sufficient resources to scale as your needs grow?
- Does the contractor offer continuity of operations services?
- What response time does the contractor guarantee should a cybersecurity event occur? What level of detail will the firm generate in after-the-fact analysis reports?
- Will the contractor provide defense in depth? For example, can it analyze your websites, where vulnerabilities may lurk, or scan attachments coming into your e-mail system?
- Does the contractor have a dedicated account team that understands your organization and its vulnerabilities?

NAC tools let authorized users check endpoint devices for up-to-date patch levels, antivirus programs and operating system service packs. The chosen tool should link to a database of authorized devices, which will help avoid false positive reports. Such false reports may prevent legitimate users from gaining the access they need to do their work and create an unnecessary burden for the IT team, who must hunt down and verify or fix the problem.

ENDPOINT SECURITY

Endpoint security should meet two requirements: keep data safe should the endpoint device be stolen or lost, and make sure only recognized devices in the hands of authorized users gain access to the network.

A growing number of organizations are implementing full-disk encryption for notebook computers so that stored information is inaccessible to anyone not possessing the decryption key. That's a good strategy, but it doesn't prevent the sniffing out of keystrokes or web information traveling over wireless networks as open text.

Organizations should consider a keystroke encryption program to tackle the keylogger problem. A variety of branded and freeware programs exist, both as stand-alone products and as part of comprehensive antivirus suites.

Smartphones have become network endpoints, not only for e-mail and the exchange of attached documents but also for numerous workday applications — everything from meter reading automation to government census data. In choosing handheld devices for your organization, an important consideration is how easily they can be managed from a central console.

Remote manageability allows IT administrators to deploy applications, remove unauthorized programs that can introduce security threats, and disable lost or stolen devices. The glut of consumer technology may have users clamoring for IT support for this or that device, but unless they can be efficiently and effectively managed, unauthorized devices should never become endpoints on critical mobility networks.

Smartphones can also be enlisted in a two-factor authentication setup if you designate them to display the time-synchronized, one-time passwords issued by the authentication server. (See more on this in Chapter 5.) ◊

BUILDING YOUR MOBILE NETWORK

HOW TO CHOOSE THE RIGHT SOLUTION

CHAPTER 4:

Organizations in all sectors have been working toward greater mobility for decades, basically since computers started taking over operational functions. It wasn't so long ago that remote users employed modems and acoustic couplers to connect to mainframes over switched-circuit telephone lines. Choosing a carrier was a lot simpler back in those days.

Today, mobility is a technology that is in wide use by the general population. Consumer-driven though it may be, the mobile provider environment poses a challenge for organizations seeking to equip remote and mobile workers doing mission-critical work.

The mobile network you create requires choices among a variety of technologies and suppliers. In this chapter, we'll delve into the important considerations that will go into building your mobile network.

Keep in mind that while there are indeed many choices, the value per dollar today in terms of network efficiency is vastly superior to that of the era when the choice was between public-switched service or expensive, proprietary, value-added networks. Having a variety of choices to sift through is a good thing.

CHOOSING A MOBILE PROVIDER

One of the great efficiency benefits of mobile communications is that staff on the go no longer have to worry about finding a pay phone. For network managers, one administrative headache has been replaced by another. Those telephone credit card accounts have largely gone away. In their place are hundreds or thousands of mobile devices, each with an associated account.

But you can make smart choices that will mitigate future overhead costs.

Before picking a carrier, it's important that you have a complete inventory of your requirements. Providers offer varying levels of service depending on your organization's size, so the more needs you can aggregate, the better your negotiating position will be.

At a minimum, your mobility inventory should answer these questions:

- How many users will need to be provisioned?
- Where will they work? What is their base location, their territory (if applicable), and will they regularly travel outside the United States?
- Will the mobile device be users' primary means of communication, or will they also have a fixed location equipped with a desk phone? If the fixed location employs VoIP, that opens the possibility of dual-mode phones with a single phone number that users can take anywhere.
- What, if any, restrictions will need to be placed on groups of users or individuals? For example, will some users be allowed to make overseas calls or send an unlimited number of text messages? What about uploading photos and other large files?

High-level university officials may have little need for the multimedia bells and whistles (although you can make provisions for them to pay for the extras themselves), while government field inspectors might routinely employ photography in their day-to-day work.

Don't overlook the needs of the technology and financial management teams of the organization. Inventory tracking requirements and the degree of granularity needed in monthly bills can also help you talk to carriers. For instance, will the organization want to see every call that every staff member makes, or the monthly total per user, or some other degree of detail?

Most important, you must be able to present your prospective providers with a complete list of the services you will need. This is essential if you want to receive complete and comparable bids.

The totality of needs will effect not only costs, but also the provisioning of users, the complexity of billing for usage and the available handset choices.

When searching for a mobile provider, here are some considerations and the important questions they entail:

- If the organization's users will need access to mobile broadband services on their phones for applications, rather than merely voice calling, then the carrier's broadband maps will play a part in the decision. Obtain an estimate of what users' monthly data requirements will be.

  KEY QUESTIONS: What are the carrier's data rates, and are they billed as an organizational aggregate or as individual, phone-by-phone usage? How complete is the carrier's broadband coverage in the specific areas in which users operate?

- If the organization uses VoIP for location-based landlines, will the VoIP infrastructure extend to the mobility wireless network? Handsets with dual capability for cellular and Wi-Fi exist (not to be confused with cordless VoIP desk phones).

  KEY QUESTIONS: Does the carrier offer feature-rich, affordable, dual-mode phones? How will VoIP and voice calling be accounted for in billing, given that VoIP can accommodate data?

- How many users travel overseas, where the global system for mobile (GSM) is standard? If you choose a code division multiple access (CDMA) service carrier for domestic service, traveling users will need phones that operate on both networks, usually with a chip that can be switched out. In the United States, AT&T and T-Mobile use GSM. Sprint, Verizon and smaller niche carriers use CDMA.

  KEY QUESTIONS: How are international calls billed, and what are the per-minute price differentials?

- What are the organization's specific geographic patterns of usage? Whether CDMA or GSM, coverage by a given carrier varies from city to city. Rural area reception can be inconsistent, and you might need a secondary carrier for specific areas.

  It is probably worth the price of a plane ticket and car rental for the IT staff to visit applicable remote locations your organization is likely to need service in to see for themselves the quality of the reception.

  KEY QUESTIONS: Does the carrier apply roaming charges to accounts making off-network calls? Does it supply rural broadband?

  Still another question is whether the carrier offers a choice of centralized billing versus making individual users responsible for their own charges. If the organization is reimbursing staff for mobile charges, the individual responsibility plan, as one carrier calls it, can mean better control at the expense of significant administrative overhead. The reverse is true if all users' charges flow to a single central bill.

DEVICE OPTIONS

Consumer trends are largely driving device choices at the workplace today. Organizations face a bewildering choice of cell phones to choose from, many of them carrier-specific.

In a perfect world, from the user's standpoint, each staff member could pick out their dream device and bring it to the IT department for provisioning. From the CIO's standpoint, the most economical option in terms of cost and administration is to give everyone the same device.

Of course, neither extreme is practical nor desirable. You want to have control over the sheer variety of mobile devices to provision and administer, but it's also necessary to offer a range of options for users to choose from.

Phone choices must take into account technology and features. Choices are driven by how the phone will be used, looping you back to the original inventory of functions and applications compiled during the carrier selection phase.

Chief device technology choices include:

- Compatibility with the organization's applications, including e-mail
- Battery life
- Memory capacity
- Whether a QWERTY-style keyboard is required
- Form factor: brick, flip or slider
- Network required: CDMA, GSM or a niche network such as an Integrated Digital Enhanced Network (IDEN) for push-to-talk requirements
- Remote management and kill capability for lost or stolen devices

Among the device features to consider:

- Camera and/or video recorder
- Voice recorder
- Global positioning capability
- Music playback
- High-quality web browsing and display
- Bluetooth

One way to determine which phones to offer is to divide users into two basic groups: those who work primarily in the office and require a mobile device for basic voice communications, and those who are primarily mobile workers who depend on their handheld mobile devices as much as they depend on their notebook PCs.

The first group would be eligible to choose from a selection of two or three basic phones. The more mobile group might choose from a similar selection of smartphones.

Many organizations also have specialized staff. For example, field agents who are out in harsh weather or other environments subject to variations in humidity or temperature. Most handsets are surprisingly rugged, but special ruggedized phones and PDAs that can withstand hazards such as drops onto hard surfaces or immersion in water are available.

SECURING THE MOBILE NETWORK

Without a doubt, cybersecurity is a top concern of technology departments and the organization's management alike. Not a week goes by without an account in the media of some breach of security in which information is lost.

The big change in cybersecurity over the past several years is the growing percentage of hacking for which the goal is theft, rather than simple vandalism. Working in organized

The Satellite Option

For wide-area mobility under most circumstances, it's worth investigating whether some user requirements justify satellite telephone service. Several carriers compete for service with a range of options, including text messaging and data-only for fleet communication of sales, inventory or other information.

Not surprisingly, satellite services can be expensive compared to ground-based cellular. Handsets themselves cost anywhere from $500 to $2,000, depending on features and the satellite network that supports them. For temporary needs, satellite phones are also available for month-by-month rental.

Satellite telephony is something of a specialized discipline because of the unique equipment and operating bands used by satellite data. Some applications require ground stations that can be either fixed or portable.

Aside from the expense, satellite service has a few drawbacks. Indoor reception of satellite signals can be poor. Severe weather or solar activity can sometimes affect satellite reception.

Also note that not all services cover the globe. Iridium, for example, blankets the earth with service. Other networks with lower prices operate only a few or even a single satellite covering a limited area.

Nevertheless, for some applications a satellite option is the only solution and should be considered a potential tool in your organization's mobility toolbox.

associations, some groups launch botnets of malware that quietly take up residence on networks and remain benign for months or even years.

In one common scheme, perpetrators communicating internationally via the Internet rent botnets from another party to distribute malware that seeks out passwords, credit card numbers and similar data.

One example is the widely dispersed Conficker worm that was used to distribute the Waledac keylogger. Browser-based, man-in-the-middle attacks, in which sophisticated phishing aimed at certain individuals in business and government tricks the recipients into giving up banking or financial network credentials, are also growing in number.

As mobile devices take on an increasing role in accessing an organization's applications, it would be wise to think about encryption plans for smartphones, which are essentially handheld computers. In effect, they function as a gateway between the outside world and the organization's network. Instances of cell phone delivery of malware are still rare, but hackers are constantly finding new attack vectors as existing ones are blocked.

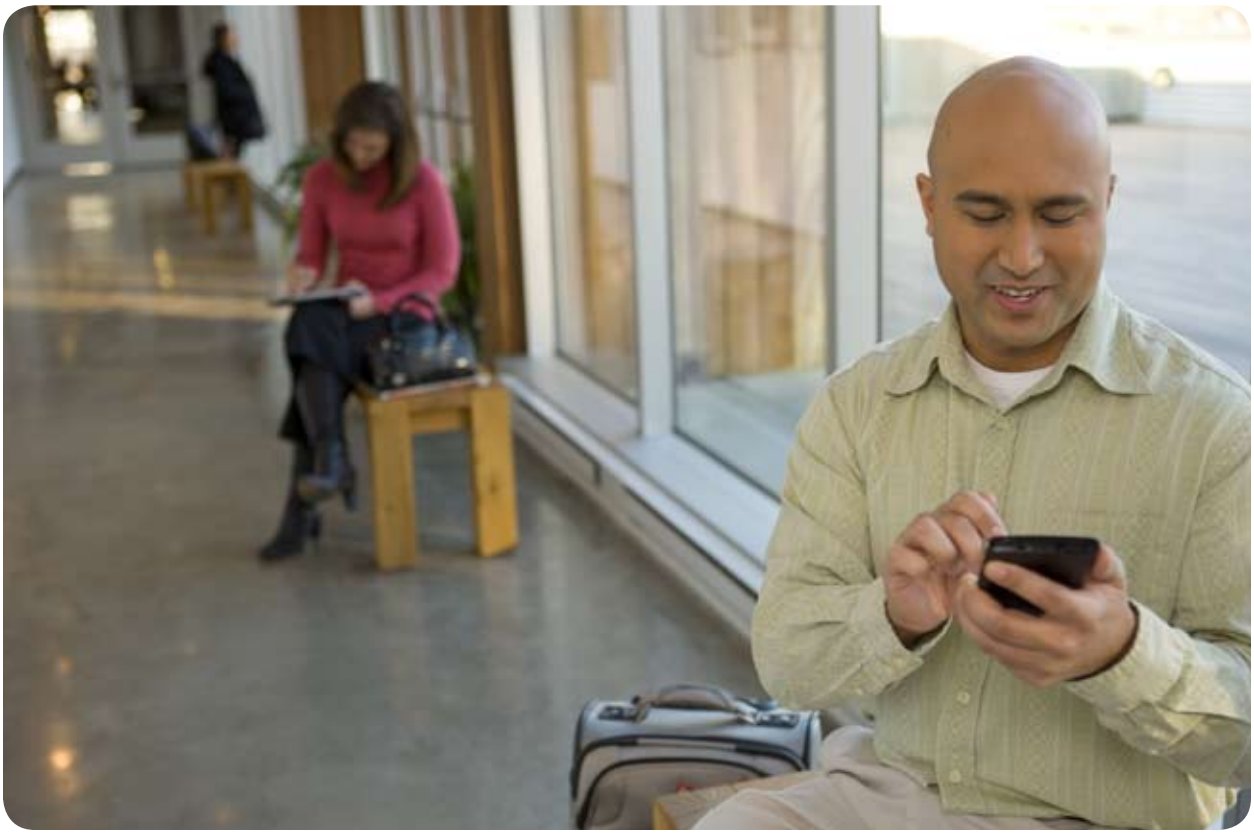
Applications exist that let users run common office productivity applications on smartphones and also access e-mail attachments, and therein lies the problem. When you also consider the growing use of social media sites on handheld devices, the threat increases.

The best approach to data protection is to have a comprehensive cybersecurity plan for all of the organization's networks and the assets connected to them, including wireless subnets, computers, storage subsystems, and even fax machines, copiers and cell phones.

The foundation for any successful security program is user education. That means clear rules that are enforced, coupled with security training that each staff member receives at least annually.

The surest route to keeping your organization's data secure is to instill the following user-security habits in the staff:

- Log off when not working
- Be vigilant with mobile equipment and report



losses immediately

- Stay away from e-mail attachments and suspicious websites
- Try to be circumspect about the information posted on social media sites

User awareness notwithstanding, data in a mobile environment is slightly more vulnerable than data in a completely wired environment. But the fundamentals don't change.

Data at rest in storage media attracts a lot of attention because it's in a static location, which makes it easier for an unauthorized user to zero in on. When a virtual private network is used to transport data, that data is encrypted. Even if sniffed out, it would be of no value.

A growing number of organizations are taking advantage of the increasing efficiency of encryption products to simply encrypt databases containing critical or confidential data.

INTEGRATING YOUR MOBILE AND WIRELESS NETWORKS

A comprehensive mobility network is really a combination of two networks: the public cellular network and your own wireless network. The Wi-Fi zones are extensions to the organization's network, which in turn will have VPN links to remote staff (who may also be mobile; see Chapter 5).

These two networks can be integrated to some extent with VoIP, using devices that work on both. Dual-mode phones are simply cell phones that also contain Wi-Fi and a telephony application. Most smartphones include Wi-Fi, but typically not Wi-Fi telephony that would connect a phone call through the nearest access point.

T-Mobile briefly offered a home service for Wi-Fi calls that would transfer a call to its cell network once out of Wi-Fi range, but abandoned that offering in 2008.

Other mobile device options available include the following:

- Phones equipped with third-party applications such as Skype for making Wi-Fi calls are offered by some carriers, which, in effect, combine cell service and Wi-Fi in a single device.
- Pure Wi-Fi phones can be used throughout a facility where there is radio coverage and at public hotspots when staff are on the move, but these are single-use devices.

The dual-mode market itself has not been very robust, in part because of the technical difficulties involved in handing off an existing call from the Wi-Fi to the cellular network. Telephony as a data application is particularly sensitive to latency and interruption. So even within a Wi-Fi hotspot, the results can be less than perfect.

Given the paucity of dual-mode phones available on the market and the lack of carrier enthusiasm for this service, an in-house enterprise solution is likely the best option if your organization wants to pursue these capabilities.

VoIP itself is a highly developed solution supported by all of the major networking manufacturers. A variety of cordless VoIP phone options are available for ease of use within the office. ◊

? QUESTIONS FOR CARRIERS

In settling on a principal carrier for mobile data and telephony, your organization is choosing more than a monthly mass of minutes and the handsets they are delivered on. Users and the team responsible for mobility services, as well as finance and accounting, will be interacting with the carrier at some level every day.

That's why it's important to consider some of the less tangible qualities of what makes a good mobile partner. Some questions to ask potential carriers include:

- Will my organization have a dedicated account manager or team serving my account as a single point of contact?
- Can problems be solved by individual users without the need to involve the network or telecommunications manager?
- What auditing services are offered, and how detailed is the information available?
- Are unused minutes on one user account applicable to another account that has used excessive minutes?

REMOTE ACCESS

SETTING UP SECURE AND RELIABLE MOBILE COMPUTING

CHAPTER 5:

One of the most obvious ways that office cubicle culture has changed in the past 20 years has been the increased adoption of teleworking programs. Mobile technologies play a key role in making this possible.

Over the past two decades, in a kind of chicken-and-egg scenario, increasingly robust mobility technology has spurred more remote and mobile working, which in turn has pushed demand for more services that people can use at the office.

The most effective IT departments will be advocates for mobility. In so doing, they will strike the right balance between user needs, security, efficiency and manageability.

In Chapter 4, we described the devices and carriers needed for mobility. In this chapter, the focus will be on the chain of services between remote and mobile devices and the networks they access.

It's worth taking a closer look at how to properly connect mobile staff so you can ensure that they have secure and reliable means of accessing the organization's network resources that they need to do their jobs.

DELIVERING REMOTE ACCESS

Organizations should not look to embrace a single way to furnish remote access because there is no single type of staffer working out of the principal fixed locations. An organization must deploy several strategies to meet the needs of various types of staff, including the following:

- **Fixed-location remote staff:** This group comprises people who work primarily out of a remote office that is too small to have its own IT infrastructure or onsite support person. The general rule of thumb is that a tech support person is not cost effective for locations with fewer than 50 users.
- **Teleworkers:** This group comprises staff who work from home. Increasingly, this includes even senior managers who are hired without the requirement of relocating, precisely because of how robust mobility capabilities have become.
- **Mobile remote staff:** A wide range of positions fit within this category: inspectors, field agents, customer support staff, trainers or anyone with a territory.
- **Central location staff who travel frequently:** This group comprises people who might have an office or cubicle in a principal location, but are often on the road.

As noted in Chapter 1, wireless mobility is also an important service within fixed locations such as headquarters or school campuses, especially multibuilding campus settings where people move from office to conference room to courtyard to cafeteria, notebooks under their arms, for meetings or classes.

Wireless service is also made available to contractors, suppliers, maintenance and repair people, guests or any other visitor who might need access to either the organization's network or the Internet.

The mobility access strategy should also take into account specialized needs. These can include:

- Push-to-talk service for easy voice collaboration;
- Outfitting vehicles with wireless communications linked to geographic positioning for tracking and route optimization,
- Radio frequency identification (RFID) of assets that move or can be moved.

The mobile access infrastructure is not, of course, for the sole benefit of mobile workers. It also lets the IT team manage remote PCs and other devices; ensure that security patches and OS service packs are up to date; and bar unauthorized access.

SETTING UP REMOTE STAFF

Staff in fixed remote locations are going to communicate with the organization's network in one of two ways.

A carrier-supplied, leased, dedicated private line is an option if there's a need for constant uptime or for the use of high-bandwidth applications — or both. This is typically more expensive than other options, but you can get faster scalability, 24x7 support, redundant routing for higher assurance and support for niche application formats such as Asynchronous Transport Mode (ATM) in addition to IP traffic.

For situations where a fully private line is not cost effective or would be overkill, organizations can use virtual private networks. VPNs create an encrypted point-to-point link, or tunnel, over the Internet. Turnkey VPN solutions are available from a number of major manufacturers.

Fixed-location VPNs use Internet Protocol security (IPsec), standards that apply to the network layer of the Open Systems Interconnection (OSI) suite. IPsec VPNs operate without regard to the applications traveling over them. In practice, they give remote users the same access to network resources as LAN-connected users. But they do carry the overhead and expense of licensed client software that must be kept up to date.

Remote locations supplied with a VPN will require an ISP. Don't overlook the potential for using the same carrier you use for mobile phones to negotiate a favorable price.

Another choice is a Secure Socket Layer VPN. With an SSL VPN, users can access only services and applications that are allowed by the administrator. The control takes place by means of a software applet coming from the host during each session,

so there is no endpoint software required. There are also SSL VPNs that are completely web based, which is ideal for mobile staff.

ONLINE COLLABORATION

Being remote or physically separated on a large campus doesn't mean people can't collaborate face to face. Virtual meeting solutions have grown nimbler, easier to use and cheaper each year.

There are many options available for high-definition, high-fidelity video conferencing. Telepresence is the most expensive option and requires dedicated equipment with a studio or conference room. However, manufacturers portray this technology as being cheaper than the tremendous costs and aggravation associated with frequent travel.

Major manufacturers are making these lifelike systems interoperable with legacy standard-definition and desktop video conferencing systems. This means that not everyone participating in a virtual audio-video meeting needs to be in a studio.

If seeing people isn't necessary for a particular meeting, an audio conference call can support online collaboration tools that let people see presentations or share documents. Organizations can purchase server versions of collaboration software, or remote offices can access software-as-a-service accounts that charge by the session.

SECURE REMOTE ACCESS

There is no reason to expect or accept a lower level of security from remote and mobile users than from your organization's central location or other large office locations.

Two-factor authentication for access control is a great improvement over simple passwords. No matter now many warnings are issued, research shows time and again that there will always be a number of staff members who use weak passwords for convenience.

Luckily, ever fewer applications let users choose weak passwords. But even with strong passwords, network administrators must deal with the persistent presence of keylogging programs distributed by botnets. Keystroke encrypting programs can help.

Two-factor authentication adds a layer of verification to something users know (a password, for instance). The second factor can be biometric information, usually a fingerprint.

Iris scanning, facial recognition and other more exotic biometric techniques don't yet have the maturity of fingerprint systems.

Fingerprint ID requires either a peripheral reader or notebook PCs equipped with an integrated fingerprint reader. These are available on most high-end units made by major PC manufacturers.

> Organizations should not look to embrace a single way to furnish remote access because there is no single type of staffer working out of the principal fixed locations.

The other route to two-factor authentication is the use of one-time passwords (OTPs). Passwords, typically eight-digit random numbers, are generated by a dedicated OTP server, a different OTP being generated every 30 or 60 seconds. Each user has a unique account on the OTP server.

Passwords reach users in any of several ways. Some manufacturers issue tokens no larger than a USB memory stick with a small display. Inside the token is a clock synchronized with the server clock, synching the password on the token at a given moment to the password on the host system.

OTPs can also be delivered via simple text messages, or a cell phone can take the place of the token.

OTHER SECURITY CONSIDERATIONS

It is important to keep in mind that phishing (e-mail schemes in which cybercriminals masquerade as trusted sources) are growing in sophistication. In recent months, they have been increasingly targeted toward people likely to have financial-network credentials.

Such names are readily available on most organizations' websites. They convince the targets to enter financial credentials, which are captured in a man-in-the-middle server and used to take money from accounts, often within as short a time period as two minutes.

Remote workers should be particularly on guard against communications that might be phishing attempts. Establishing a

policy covering what will (and will never) be asked for via e-mail can mitigate the danger. A known point of contact within the organization should also be established to verify the legitimacy of questionable messages.

The convenient portability of mobile devices also makes them prone to loss or theft. When a mobile device is out of its owner's hands, someone else can easily access the device's services (for example, make unauthorized phone calls), extract private information or alter the information stored on it. Steps need to be taken to protect stored data.

As mentioned, many mobile devices can be configured so that the user must enter a password before accessing the device. But it is possible to bypass these controls. For example, if an attacker is willing to take the device apart and mount its hard drive in another system, the contents can be easily accessed.

Other devices encrypt their contents and require proper user credentials in order to decrypt any stored information. Generally, these two security features will provide adequate protection for the information stored on mobile devices.

Another security solution offered on many mobile devices is the ability to remotely disable and wipe information from the device if it is reported missing. This strategy is effective if the theft is reported promptly and the device hasn't been accessed prior to the issuance of the "self destruct" signal.

Virtualization Security Benefits

Two separate technology developments have renewed interest in virtualizing individual users' desktop environments. These are the emergence of cloud computing and the introduction of a variety of new computer form factors, including ultralight netbooks and a new generation of tablets.

Approaches vary, but the basic idea is to separate operating systems, applications, data and user settings into centrally stored services that are available to whatever device a user happens to be using at the moment. The central store could be the data center, or it could be a commercial cloud.

Version control, updates, security patches and storage become easier to manage, and users know the data they see on the device at hand is the latest available. One large IT manufacturer has recently been testing this for its own staff, calling it device-independent mobility.

Your IT department must still maintain secure access routes, but issues surrounding remote data at rest are fewer. Remote and mobile users become potentially more efficient because, with devices and the rest of their IT operations untethered, they can access more than one environment on a given device.

With respect to tech support, even if the main location of the organization maintains an in-house tech crew, it might be worthwhile to augment support for remote locations using a local or national service contractor for catastrophic events. In the event of a remote-office server meltdown, fire, flood or other loss that can't be resolved over the network, a prearranged service contract eliminates the delay of sending home-office staff to a remote location. ◊

Mobile Workers and the Cloud

Regardless of the architectural path you choose, cloud computing offers potential for provisioning mobile users. The cloud encompasses several layers of service up to and including complete outsourcing of IT. Short of that, cloud providers offer applications, infrastructure, platforms and application development environments as services.

In thinking about cloud services for remote users, there are some important questions to ask the cloud-service provider and your own IT staff before proceeding:

- What is the exit strategy if you want to take a particular service back in-house?
- How does the cloud provider ensure security? Will it provide evidence of testing and auditing of network activity?
- What are reasonable expectations to include in a service-level agreement in terms of uptime, network performance and response to trouble tickets?
- Which project, user group or function should be the first to use the cloud?

GLOSSARY

This glossary serves as a quick reference to some of the most essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

802.11i

The IEEE standard 802.11i describes the security specifications for wireless local area networks. It was ratified in 2004.

802.11n

The most recent amendment to the IEEE standard for achieving wireless networking is 802.11n. Ratified in 2009, it comprises specifications for WLANs operating over the 5GHz radio band and employing MIMO.

Access point (AP)

In wireless networking, an access point is a fixed-location device that wireless computers and other devices connect to a LAN or to other wireless devices. The AP includes or is connected to a router that connects wireless and wired networks.

Backhaul

This term refers to data traffic from access points or whole WLANs that is transported to the trunk or primary wired network of the organization. Aggregated wireless traffic backhaul can cause a strain on the LAN.

Bluetooth

Bluetooth is an unlicensed radio communications protocol for wirelessly connecting computing devices within roughly 30 feet of each other. Bluetooth is typically used to pair printers, earphones and other peripherals. Like some 802.11 standards, Bluetooth operates at 2.4GHz.

Cloud computing

Cloud computing is a computing setup in which various user resources such as applications, data and storage are housed in a central, shared facility — the cloud — that communicates with individual computers over the Internet. Cloud facilities differ from data centers in that they are typically commercial operations that individuals or organizations subscribe to.

Code division multiple access (CDMA)

CDMA is a technique for achieving high-capacity cellular communications via bandwidth sharing. It is used primarily in the United States by carriers Sprint and Verizon.

Desktop virtualization

Desktop virtualization is a form of computing in which an individual computer's applications, user settings and data are located on a central server, separate from the physical machine. It permits device-independent computing and easier administration of multiple users.

Dual-mode phone

This term refers to a cellular telephone capable of communicating with both a carrier network and a wireless LAN. The phone is capable of maintaining a call session even when moving between the LAN environment and the cellular coverage area.

Global system for mobile communication (GSM)

GSM is the main system for mobile communications in Europe and Asia, and used by T-Mobile and AT&T in the United States. It creates capacity with time division multiplexing, as opposed to code division multiplexing used by the incompatible CDMA.

IPsec VPN

This term refers to a virtual private network using the Internet Protocol security standard for creating an encrypted, point-to-point tunnel for secure communications between a host and a remote client in a fixed location.

Keylogger

A keylogger is a computer application that records and transmits the keystrokes made by a user. Keylogging can be used as a surveillance or training tool, but can also be installed secretly by cybercriminals with the intention of intercepting passwords and other confidential information.

Multiple Input/Multiple Output (MIMO)

MIMO refers to technology employing up to four antennae for both transmission and reception of data in an 802.11n wireless network. MIMO helps maximize wireless data speeds.

National Institute of Standards of Technology (NIST)

NIST, a part of the U.S. Commerce Department, has the stated mission of promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve the quality of life. Its Computer Security Resource Center develops standards and guidance for cybersecurity useful to both government and industry.

Network Access Control (NAC)

NAC provides a way to prevent unauthorized devices or endpoints from logging onto a network. Vendors typically bundle NAC software onto a rack-mount appliance sold as a turnkey solution for enforcing security policies.

One-time passwords (OTPs)

One-time passwords are random number strings generated by a special OTP server and transmitted to users as a component in two-factor authentication. The passwords are valid for 30 or 60 seconds and must be used in conjunction with the user's regular password.

Radio Frequency Identification (RFID)

RFID is a method of counting, tracking or timing physical objects to which an antenna has been affixed that correlates to a unique serial number. The antenna communicates via radio to a transceiver that can be located up to several hundred yards away.

Remote monitoring (RMON)

RMON is a method for gathering information about the status and performance of distributed network components. RMON systems generate data that allow administrators to analyze network operations and prevent or repair problems. Many RMON products display data in a graphical dashboard.

Rogue

In the networking field, a rogue is an unauthorized access point or mobile device attached to or attempting to connect with a wireless network.

Secure Socket Layer virtual private network (SSL VPN)

An SSL VPN provides mobile users with encrypted access to the enterprise network. SSL VPNs enable access via a web browser and require no client software.

Site survey

The sum of activities required to ensure the installation of a successful wireless network is called a site survey. A site survey aids in the planning of access point locations, and also helps networks bypass sources of interference and guarantee adequate performance in all of the intended user locations.

Wi-Fi Protected Access (WPA2)

WPA2 is the commercial product implementation of the IEEE 802.11i standard for wireless network security incorporating strong encryption.

Wireless local area network (WLAN)

A WLAN uses the 802.11b/g/n standard, usually as implemented by the Wi-Fi Consortium of wireless equipment manufacturers.

WLAN controller

A WLAN controller is software for managing devices on a wireless network that lets administrators remotely monitor and configure access points. Most products also enable load balancing among APs as well as authentication of users.

Worldwide Interoperability for Microwave Access (WiMax)

WiMax is a wireless broadband technology for transmitting data using the 2.5GHz frequency over a distance of several miles. It is based on the IEEE 802.16 standard.

Voice over IP (VoIP)

VoIP is technology for the transmission of voice communications, converted into digital packets, using the Internet.

INDEX

Disclaimer

CDW·G

CDWG.COM/MOBILITYGUIDE
888.563.4239

ABOUT THE CONTRIBUTORS

« PEYTON ENGEL leads a team of security engineers at CDW. With the team since 1998, he has been responsible for its growth and management, including sales and marketing, since 2001. Peyton has presented his security research at national conferences including DEFCON (2004, 2006), ToorCon (2002, 2005) and USENIX/LISA (invited speaker: 2003, 2005). Peyton's chief technical interests are software security and the security relationships between systems in large networked environments.

« THOMAS R. TEMIN is a broadcaster, writer, editor and consultant with 30 years of experience in media and information technology products and services. Temin was executive vice president and editor-in-chief for PostNewsweek Tech Media, responsible for editorial content, in print and online, of the award-winning *Washington Technology* and *Government Computer News* magazines as well as *Government Leader* and *Defense Systems*.

« JOSH ZENNER is a Wireless Solutions Architect with CDW. He has spent the last nine years designing and implementing wireless solutions, with a focus on healthcare, manufacturing and enterprise-class organizations. Josh specializes in finding ways to utilize wireless technologies, such as wireless VoIP and RFID/asset-tracking systems, to make organizations more efficient, all while maintaining the highest levels of security.

MOBILITY
REFERENCE GUIDE

100617 • Flyer 75760AB

LOOK INSIDE for more information on:

- Taking advantage of 802.11n
- Fine-tuning your Wi-Fi architecture
- Securing endpoint devices
- Choosing the right mobile provider

ISO 9001 SRI CERTIFIED ISO 14001 SRI CERTIFIED

GSA Contract Holder

SmartPay™ GSA