NOVEMBER 2012

MOBILE SOLUTIONS

Boosting productivity and efficiency enterprisewide — from applications and infrastructure to internal and external users

800.800.4239 | CDW.com/mobileguide

CDW REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW PEOPLE WHO GET IT

WHAT'S INSIDE:

800.800.4239 | CDW.com/mobileguide

VISIT

CDW.com/mobility
for more information
on mobile solutions.

SCAN IT

Download a QR code reader on your mobile device to scan and see our full list of available mobility solutions and services, case studies and media library.

GET m.CDW.com ON THE GO

m.cdw.com is now available anywhere with our new mobile-friendly website or download the CDW app for your iPhone from the App Store.

What is a CDW Reference Guide?

At CDW, 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.

Building an End-to-end Mobile Strategy

Starting with a holistic approach to mobility to yield benefits and savings

Smartphone, tablet computer and ultrabook purchases number in the hundreds of millions per year. This onslaught of devices underscores the move toward mobility in organizations of all sizes across many industries, government agencies and educational institutions.

Organizations have embraced mobility-first approaches, starting with their users and working back from devices to wireless strategies, network infrastructures and data centers. Successful initiatives require a framework and strategy to ensure that all the pieces work together to deliver the efficiencies and flexibilities that mobility promises. Awareness of the typical mobility implementation cycle can help organizations prepare for what comes next in their mobility programs.

Today's Mobility Cycle

While it's hard to find a precise definition of mobility, the IT industry understands the term to mean giving workers access to network resources anytime, anywhere, from any device. This is where the mobility cycle begins. To facilitate that access, end users have taken the lead, requesting (from within their organizations) that they be allowed to use their own personal devices for work. Organizations have responded with bring-your-own-device programs.

Such BYOD strategies have quickly taken root, first in businesses and later followed by government agencies and educational institutions. Smartphones and tablets appeal to users who clamor for a single device for personal and professional use. This consumerization of IT prompts IT departments to adapt policy and technology to meet this demand.

However workers obtain their devices (through BYOD or as organization-issue equipment), the small physical size and sheer number of devices demand a way of tracking them. Organizations depend on IT staff to make sure devices remain configured properly, especially with respect to cybersecurity. Industry has responded to this need for specialized mobile device management (MDM) with comprehensive tools that integrate with network management systems.

Traditional client-server architectures may not be optimal for a full-out mobility deployment. More of the processing load shifts to servers from clients, which no longer take the form of standard PCs, with large disk storage and processors capable of executing most application requirements.

Wireless LAN infrastructures designed for ad hoc or visitor use are now in high demand by mobile users. The IT staff often discovers it needs to rearchitect the data center to accommodate virtual clients and upgrade the WLAN to accommodate a primarily wireless user base.

This growing use of rich media also drives infrastructure upgrades, both for onsite and remote mobile users. Organizations are adding audio/video and live chat functionality to the applications they deploy externally to users. Internally, video conferencing (again, both on the LAN and over distances) increasingly is used as a substitute for travel and in-person meetings.

With an optimized core infrastructure in place, the IT shop can then concentrate on media-rich, mobile applications. Employees typically use three basic classes of applications: enterprise or mission-specific, productivity/collaboration and newer task-specific apps that resemble those popularized by smartphones.

The Strategic Benefits of Mobility

While everyone gets the value of mobility, it's worth reiterating what exactly it really brings to organizations. Unlike telework or remote access, true mobility frees employees from fixed locations and being tied to a desktop or notebook PC. Mobility produces strategic benefits for internal staff, the organization as a whole and external users. Put another way, the organization gains efficiency at all three corners of the IT triangle: internal user endpoints, application/infrastructure and those whom the organization serves (external users).

Workers Become More Productive

American businesses spent $249 billion on travel in 2011, according to the U.S. Travel Association. That figure has fallen slightly from prerecession highs. But clearly, working people remain on the go. And that figure doesn't count the local travel that many employees do in their day-to-day jobs.

Organizations can render all of that travel time more productive by taking advantage of the latest mobility technologies such as lightweight devices, constant connectivity and mobile (and mobilized) applications.

The simple fact that smartphones, tablets and ultrabooks equipped with solid-state drives have significantly longer battery life and dramatically shorter boot times than PCs means workers can use even short stretches of time to gather and move data.

Mobile devices increase productivity by displaying and integrating productivity and collaboration functions with touch-screen technology. Using still cameras, high-definition video recorders and sound input, employees can gather a much wider range of field data with less effort than required using multiple discrete devices.

Tablets lend themselves to quicker data entry on forms because of their screen size. And don't overlook the speed at which staff can set up presentations and view them on mobile devices. In sales meeting scenarios, for example, the less effort and distraction spent fiddling with presentation technology, the more effective the sales effort itself becomes.

Mobile devices can even save fuel: The Air Force is experimenting with tablets to see if they can replace heavy paper flight kits (typically weighing around 50 pounds), potentially producing measurable fuel savings when applied across an entire fleet of planes. And the Federal Aviation Administration is working with airlines on a similar effort.

Data gathered in the field is generally of little use until employees upload it to be aggregated and made available to organizational applications. Many organizations find that they can enhance security and boost productivity by retrieving information wirelessly from mobile devices as it is collected. Broadband increasingly reaches more remote areas of the country, making this type of data retrieval much more feasible.

A recent FCC report on broadband throughout the United States found that the average Internet service provider delivers 96 percent of its advertised broadband speed. Whereas wireline's fast upload speeds are terminated at a Wi-Fi access point, mobile users will be able to achieve quick upload speeds no matter where they are.

Wireless broadband is also expanding. The three largest providers of 4G Long Term Evolution (LTE) wireless broadband spent $40 billion on capital improvements in 2011, most of which went to expansion, building out their networks' density and capacity in some areas and extending coverage to other areas.

External Users Benefit

In the 1990s and 2000s, consumers and businesses revolutionized the retail industry by putting it online. Today, virtually all business-to-consumer, business-to-business, business-to-government and government-to-citizen services are online accessible.

The next generation of e-commerce and e-government is now arriving in mobile form. Analysts have identified growing subsets of e-commerce, namely *m-commerce* for interaction via mobile devices and *t-commerce* for transactions performed specifically on tablets. These movements might be growing fast, but they're still works in progress.

To stay in front of them requires that organizations meet several challenges. They must reengineer web applications for mobility. That leads to a split in the road: Either go with a mobility-optimized web interface or take the app route.

A second challenge is tying the organization's mobility strategy to social media. Many of the popular social media platforms have become more mobile-oriented. The number of mobile Facebook users has been pegged at about 425 million (as of spring 2012). Mobile user surveys have found that the vast majority of users are never further than three feet from their mobile phones — awake or asleep.

Organizations that understand these trends and capitalize on them will be able to deliver products and services in the manner their customers want, which is basically on the go.

With the public sector, several organizations have created mobile applications to display certain government data, such as legislation status. The federal government has a formal mobility strategy to move agencies to mobile, transactional applications. State governments are slowly developing apps, but these tend to be informational at this stage, not transactional.

Many universities and higher education institutions, including Stanford University and Florida State University, are creating apps that meet a variety of campus needs, from navigating the campus to direct delivery of online educational resources. Regardless of sector, organizations can gain a closer relationship with both their internal and external users by adopting a mobility strategy that delivers information and supports transactions.

Mobility Spurs Savings

Mobility can bring budget savings to an organization, but not without careful planning. As the popular project management saying goes, first plan the work, and then work the plan. And no strategy involving network investments, application development and deployment of new devices will succeed without a solid business case.

To make that case, start by assessing conditions and goals. Given the prolonged downturn in the private sector and tight budget conditions in the public sector, organizations across the board want to find ways to make processes more efficient. Enabling mobility clearly brings process efficiencies and (ultimately) savings. That, plus growing demand for mobile-enabled interactions, makes for a strong case for mobility.

Next, consider the workforce and the degree to which it is dispersed. In the search for savings, some organizations look at office real estate to determine whether making a greater portion of the staff permanently mobile will let management shrink the physical footprint. A reduction in rent or facilities expenses will likely outweigh the costs of supporting more mobile workers.

A third element of potential savings is the solution itself. Consider the costs to optimize the enterprise network, WLANs and applications against lower real estate and device costs and increased employee efficiency. In many cases, organizations will find they can go further on a given IT dollar with a full mobility strategy.

After all, mobile devices are powerful computers with far lower acquisition price points than desktop or notebook computers. By pooling and consolidating wireless data and voice plans, organizations can often negotiate far better deals with carriers.

Additional savings can be found in aligning the mobile strategy with other initiatives. For example, a switch from traditional clients to thin client mobile devices can produce immediate savings.

And by virtualizing user accounts rather than maintaining full-featured clients, IT departments can realize continuous savings over the long term through data center consolidation. Mobility and virtualization complement each other as the IT group moves from virtualizing applications to virtualizing clients. ■

MOBILITY: MOVING *BEYOND* SAVINGS

Implementing a mobility initiative can produce many intangible benefits that aren't immediately obvious. These can include the following:

MORE TOP-LINE REVENUE: Mobile transactions can draw new customers/users and increase interactions with existing ones. This particular metric is easily measured. But mobile enablement means the IT group must reengineer web applications as mobile apps. Not all devices have equal web display capabilities. And rarely do traditional desktop web designs translate to small screens.

IMPROVED TRANSACTIONAL PROCESSES: Some analyses look at transactions by comparing those done remotely using mobile technology with those done at a desk. The remote, mobile transaction can now be equally rich thanks to greater device compatibility, improved mobile web application design and ubiquitous broadband.

GREATER EMPLOYEE ACCESSIBILITY TO INFORMATION: Mobile devices act like thin clients in many applications. They display, but don't actually store or hold data such as documents or reports hosted on a remote server. So workers can access them from their home computers or remotely by using a smartphone or tablet. That accessibility can quicken decision-making and other processes dependent on those documents by separating them from time and place constraints.

ENHANCED IMAGE AND REPUTATION: As users grow increasingly more mobile, organizations can't afford to let their mobile initiatives grow stagnant. Organizations with up-to-date mobile access will draw more traffic and loyalty from users compared to those offering limited mobile capabilities.

BYOD Initiatives

Giving users what they want

The collective embrace of powerful smartphones and tablets over the past five years has changed users' relationships with technology. Workers have routinely traveled with computers for some time.

But the advent of the smartphone means people are never without computing power and connectivity. What's more, users find the combination of touch screens, light (but powerful) applications, handy form factors and high-resolution displays nearly irresistible.

When employees have more efficient processes and tools, productivity increases. And when productivity grows, businesses expand and become more profitable and educational institutions and governments deliver on their missions more effectively.

The Consumerization of IT

To understand how mobility is influencing business practices today, it's helpful to think back to the release of the PC, a technology initially marketed to consumers. Once people realized the benefits these machines could bring to their personal lives, this enthusiasm carried over into the workplace. Workers wanted to use PCs and popular applications to do their jobs more effectively.

As touched on in the previous chapter, the same thing is happening with tablets and smartphones. Seeing how useful these devices are in their personal lives, many workers have put pressure on organizations to let them use their personal devices to access the enterprise network. Initially, this meant allowing both personal and corporate e-mail accounts to coexist on the same device. Today, it also means access to enterprise data and applications.

This is a great example of *the consumerization of IT*, a term that refers to technologies that are initially adopted in the consumer market before migrating over to the business market. Several studies on the mobility movement and the consumerization of IT confirm this trend of people wanting a single, universal device for both work and personal use.

In 2011, an IDC survey found a gap between employees' (especially young employees) expectations for technology tools and organizations' abilities to meet them. A more recent Forrester Research study among 5,000 IT workers found that 25 percent of employees use their smartphones for work. Twenty percent said they would like a single device for work and personal use.

This trend has profoundly influenced organizations and their planning around mobile computing. They are now looking both outward to the needs of external users (such as customers or constituents), as well as inward in order to accommodate the desire of employees to use a single device.

Therefore, today's enterprise mobility initiatives need to include both internal and external components. The outward component is a matter of delivering services, products and missions optimized for mobile users. This can take many forms, such as

smartphone versions of retail websites or an app from the Federal Emergency Management Agency for information and status reports following disasters.

The inward component, accommodating mobile workers, may most directly affect the IT staff, even if the outward component has more leverage for revenue, market acceptance and reputation. Mobility typically requires support for at least one new operating system (OS), along with different network configurations and a broad build-out of wireless bandwidth.

BYOD Brings Benefits

Two years ago, BYOD rarely appeared in the technology press. It was a new idea. Today, dozens of blogs cover the topic. It stands, of course, for "bring your own device" — organizations allowing workers to choose which devices they want to use for accessing enterprise network resources.

Organizations may choose from a variety of approaches to BYOD plans. They may supply employees with devices, letting them choose from an approved list. Some organizations offer a flat monthly or yearly stipend to be spent on devices of the user's choosing (typically with a stipulation that the chosen device meets the organization's requirements for security and manageability). Many organizations go with full BYOD — workers choose devices from an approved list and pay for them.

Regardless of who pays the bill, many IT staffs have become more comfortable allowing employees to use their personal devices for work because mobile device management (MDM) solutions and advanced security techniques make it possible to protect the organization's data and applications housed on those devices.

A well-planned BYOD initiative can bring several benefits to the organization and its users, including the following:

PRODUCTIVITY: Staff are more efficient because mobile devices stay connected to the network and its resources, and people always have them close by. Various surveys have shown that mobile users work more hours per week than users tied to computers at fixed locations. Plus, today's mobile devices are more conducive to an anytime, anywhere flexible work schedule thanks to their all-day battery life.

SAVINGS: BYOD programs can reduce costs (even when the organization furnishes the devices rather than having employees pay for them). While highly capable tablets sell at price points far below full-featured notebook PCs, larger savings accrue in two other important ways.

First, organizations can reduce their telecom costs either by having employees subscribe to their own voice and data plans or by consolidating usage and renegotiating prices with carriers. Stipend programs, under which staffers receive a fixed monthly payment to apply toward their wireless plans, also offer organizations cost predictability.

One caveat: Simply reimbursing employees for the plans that they have is probably not a viable approach. >>>

PUT IT *IN WRITING*

Mobile devices bring new considerations for security and liability. To protect themselves, organizations must establish clear policies for which activities are allowed and which are prohibited, and have mechanisms in place to enforce them. Management should separate liability and responsibility from who owns or pays for the device, based on the principle that regardless of who owns the device, corporate or agency policies apply.

This is doubly true for organizations that have specific regulatory and compliance responsibilities, which is the case for nearly all: finance and accounting, healthcare, law and government contracting, to name a few. Publicly traded companies have the greatest compliance burdens.Privacy and security laws and regulations also bind government agencies.

Here is a sample of elements that should be included in agreements with employees using mobile devices on behalf of the organization:

1. Devices will not be used for anything that could be construed as an unfair trade practice, such as photographing competitors' documents.
2. Devices will not be used for anything illegal or contrary to corporate or agency policy, such as downloading or creating pornographic materials or sending threatening messages. (In government, workers need to be mindful of the Hatch Act, which forbids politicking while on the job or acting in any way that could be construed as mixing a public administration job with politics.)
3. There will be no use of personal e-mail accounts that may reside on a device intended for business use.

There is a lack of incentive to control costs under this model, and it is difficult to sort out which calls, texts, e-mails, roaming charges and data downloads were for work and which were for personal use.

A second way that organizations can realize savings is from reducing the administrative chore of managing mobile devices, especially when online activation portals let employees self-provision.

An enterprisewide plan, negotiated professionally by the IT group and the organization's procurement staff, will provide more cost control and predictability with employee devices using the master account.

EASED SUPPORT: Workers essentially manage their own devices, although MDM software gives the IT shop visibility into devices and how they are used. But (assuming the app portal is set up properly) device maintenance, upgrades and configurations within the device image set by the IT department are typically the responsibility of users, freeing up the IT staff for more productive matters such as new application development and establishment of BYOD policies.

Whether the organization supplies the device and allows personal use on it or the employee supplies the device and adds professional use to it, signed agreements allowing the right to wipe a device, remotely or in person, should be a requirement. Workers must also understand that remote wiping can possibly result in a loss of personal apps and data, such as photos and music.

IMPROVED WORKER MORALE: Broad experience reveals a high degree of enthusiasm and acceptance for BYOD programs. Workers are freed from the burden of carrying multiple devices for their work and personal lives. BYOD can also be a strong recruiting point for potential hires.

New Management Challenges

The concept of BYOD presents new challenges for the IT team and network management staffs, which is precisely why BYOD should not mean "bring any device." Just because a worker may still own an Apple Newton or Palm VII shouldn't obligate the organization to support it or let it access the network.

IT leaders need to balance letting staff use appealing, up-to-date devices against the support costs and security risks of managing multiple OSs. That's why an enterprise mobility strategy must set limits while remaining flexible, which can sometimes be a tall order. It's important to avoid establishing guidelines in a vacuum. Get the input and support of business units, human resources and legal counsel. Be sure that the resulting policy covers the following:

OSs: Currently, the norm is for organizations to support up to three: BlackBerry, because it's the legacy system for many businesses and agencies; Apple iOS; and Google Android. But keep in mind that Windows is likely to become a bigger player as Microsoft refines its mobile strategy and perfects Windows 8.

ACCEPTABLE USE: Because these are personal (and often personally owned) devices, organizations need to sandbox (or, logically isolate) applications. Also, the organization should not allow activity that wouldn't be acceptable on traditional organizational PCs. For example, online gambling, pornography or using the device to harass others are all activities typically off limits.

SECURITY: Any BYOD strategy must give the organization the right to install whatever security updates it deems necessary and to erase the device with good cause, even if that means the worker loses personal data. ■

Device and Provider Options

Putting the right notebook, tablet or smartphone and features in users' hands

There's a widely told story about a government agency's painstakingly slow but well-intentioned attempt to get a single Android OS device approved for its users. The sticking point was security. There was some uncertainty within the organization about the device's security features. It was eventually approved — but only after the vendor stopped manufacturing it.

Effective mobility strategies require arming users with up-to-date devices while ensuring reasonable and predictable costs and a high degree of security. Simple in concept, this can be a tall order in execution.

An enterprise looking to deploy a fleet of mobile devices will likely place a priority on functionality, adaptability to enterprise software and security. As the previous chapter covered, today's organizations also need to take their users into account.

The consumerization of IT and BYOD have raised the profiles of users in the device deployment equation. This ultimately complicates device deployment for organizations. Having a clear understanding of users and their needs is imperative.

Know Thy User

Determining what mobile devices to bring into the workplace starts with knowing and categorizing who will be using them. Implicit in the drive to greater mobility is the idea that nearly anyone in an organization can and should be mobile, at least part of the time.

In planning for mobility, it's useful to categorize employees into three general buckets: office workers, mobile users and field agents.

Office workers: The needs of day-to-day office workers are important when thinking about mobility. Today, few organizations reject the notion of allowing employees opportunities to telework.

The Telework Enhancement Act of 2011 liberated many government workers legally (if not culturally) from the need to be in the office every day — reflective of this trend in the wider corporate world. Many commercial organizations recognize that telework boosts morale and productivity. And when fewer people commute, organizations reduce greenhouse gas emissions.

For people who primarily work in an office or telework regularly, a notebook PC offers the ideal platform. Their work requires typing, data entry, working with spreadsheets and using specialized applications for particular work.

These tasks are best accomplished with a 12-inch or larger screen, full-size keyboard and sufficient ports to accommodate a docking station, larger monitor, Ethernet connection, speakers and any other myriad peripherals they may hook up to their notebooks. Yet the whole package is portable, and nearly all notebooks have built-in broadband, Bluetooth and Wi-Fi connectivity.

Mobile users: This group is defined as workers who have an office (which might be a home office) but travel regularly — for example, sales or engineering managers. For them, appropriate platforms include compact notebooks, the new class of ultralight notebooks or inexpensive netbooks.

These devices pack easily but still sport classic keyboards. They are all lighter than full-size notebooks. Similar to office workers, these mobile workers typically require connectivity features, but need them in a lighter form factor with longer battery life – for example, enough power to work on a long flight.

Such workers are likely to also have a smartphone for e-mail, synchronized calendar and basic productivity software.

Field workers: Employees in this group spend most of their time on location. They benefit the most from advancements in mobile technology.

Whether salespeople, social workers, systems engineers, police officers, forest rangers, financial auditors or hourly line workers in technical industries, these workers share a common need to gather field information and store it in an enterprise system. When in the field, they typically need access to organizational resources such as laws and regulations, product information, and customer or constituent records.

For this group, the advent of powerful computers in the form of smartphones, tablets and ultralight notebooks provides a much-needed step up in productivity.

Device Options

Organizations and their users face a wide array of mobile devices from which to choose. The choices continue to grow, as do their features and power. A common approach to sorting through all of these options is to categorize them by screen size.

Smartphones: These devices have the smallest screens, which are typically under four or five inches measured diagonally. A smartphone is roughly defined as a telephone coupled to a computer running applications optimized for the small screen. Except for a sync-power port and a headphone jack, they communicate with onboard wireless connectivity.

Most devices run a full workday on a single charge. The smartphone market is moving to all touch screen, but many workers still prefer the tactile feedback and greater precision of a thumb-size keyboard.

Tablets: These can range in size from around six or seven inches up to 11 or 12 inches. The most recent tablets are thin, entirely touch-screen controlled, and have in-use battery lives of up to seven hours and standby power of about a week. They share processors and general hardware architecture with smartphones, but they don't function as phones. The addition of Skype or similar applications can effectively offer telecom functionality.

Netbooks: These devices are essentially shrunken notebooks with low-power-consumption processors. They have screens up to 12 inches in size and complete (if small) keyboards.

Ultrabooks: These super-thin notebooks can range in size from 11 inches to about 14 inches. The newest generation of devices have metal alloy chasses, solid-state drives and battery lives of roughly six hours. They typically weigh about three pounds and have tablet-like battery life. But they also have one or more USB ports, an Ethernet port and an external monitor port.

They have a much higher price point than netbooks but have more-capable processors, more memory, and higher-end graphics and resolution. Similar to tablets, they typically have a long standby power life, which means most users never need to shut them off. Therefore, they rarely require shutdown and rebooting.

Rugged PC/tablet combos: These devices, with screen sizes up to 12 inches, are designed for all-weather,

HOW TO *BEST EQUIP TELEWORKERS*

Teleworking in the mobility age implies that workers out of the office will not necessarily be at home or at a remote telework center, which was the model prevalent just a few years ago.

Organizations should consider continuing to equip the occasionally mobile office worker with a device incorporating a full keyboard. The weakness of smartphones and (to a lesser degree) tablets is that their tiny physical or virtual keyboards are ill-suited to the levels of typing demanded by applications typically used by office workers. While manufacturers offer keyboards that are close to full-size for devices that lack them, the keyboards detract from the portability and usability of the devices.

Therefore, the newer class of ultrabooks with solid-state drives might be the one-device answer for these teleworkers. Out of the office, they bring the tablet-like features of fast booting and long battery life. Within the office, they include Ethernet and USB ports. (The MacBook Air is the exception in that it lacks an Ethernet port.)

outdoor use and use in other harsh environments. They feature keyboard, touch and stylus input. Some models can withstand significant knocks and drops. The tradeoffs for these hardened machines are their weight (ranging up to 10 pounds) and their pricing (often approaching $3,000).

Standard notebooks: These are full-featured portable computers with screen sizes ranging up to 17 inches. Notebooks overtook desktop PCs in the marketplace when manufacturers closed the performance gap between these computing form factors.

They feature very large hard drives in addition to on-board optical drives and multiple ports. They are available in a wider range of configurations than any other device. Battery technology and power management have improved to the point where notebooks can sustain an average use of up to five hours.

Choosing the Right Device

In choosing devices, think first of the organization's mission — what work are employees actually doing? The primary considerations are how people will interact with the device and what applications the device must support.

For example, workers who perform financial fieldwork might need a screen size suitable for displaying a spreadsheet and an input method for navigating such documents. Employees documenting location-based conditions may do better with less obtrusive touch-screen devices loaded with forms designed for that type of screen.

Battery life is another important consideration. Longevity may be less of an issue for mobile workers who travel to different indoor locations throughout the workday and have access to power outlets. For employees typically in situations where plug-in power is not so readily available, battery stamina is that much more important.

Memory is less of a consideration for mobility than is storage. Ultrabooks have mini Serial ATA (mSATA) or solid-state drives (SSDs) with average capacities of 128 to 256 gigabytes (a fraction of the terabyte spinning drives found on some notebooks).

Manufacturers have assumed that ultrabook users are more likely to depend on remote server or cloud storage in conjunction with their mobile devices, with only application software residing on the machine. The device needs at least 2 gigabytes of memory for caching data until the user uploads it.

The device's cellular network is another consideration. Note that the Integrated Digital Enhanced Network (IDEN) is scheduled to be decommissioned by June 2013. There are now three options available in North America:

- **Global System for Mobile Communications (GSM):** This is most common in worldwide, with AT&T and T-Mobile networks using GSM. Phones for these networks require a SIM card.
- **Code Division Multiple Access (CDMA):** This is a legacy standard in the U.S. and parts of Asia, with Verizon and Sprintnetworks using CDMA technology.
- **4G LTE:** This wireless broadband standard is expanding in coverage and capacity, with all major U.S. carriers investing heavily in it.

As a practical matter, for domestic use it makes little difference which technology the device uses as long as the rate plans and coverage of the carrier meet the organization's needs. GSM phones with accessible cards can easily switch networks when users travel overseas.

Feature Considerations

Manufacturers operate in a continuous race to add new features to their devices.

/// CERTAIN DEVICE FEATURES THAT MAY HAVE ONCE BEEN CONSIDERED GIMMICKS NOW HAVE CAPABILITIES SUITABLE FOR BUSINESS USE. ///

Certain features that may have once been considered gimmicks now have capabilities suitable for business use.

Take cameras, for instance. Within the limitations of lenses that can fit inside a mobile device, smartphone cameras have moved into the 8-megapixel resolution range. For many consumers, phone cameras have replaced point-and-shoot digital cameras. For organizations, this means employees can perform pictorial- or image-oriented information gathering using their mobile devices.

Many models are also capable of

producing high-definition video suitable for field data gathering or even creating videos for posting on the organization's website. A miniature tripod equipped with flexible gripper can enhance the use of smartphones for video production.

Don't overlook audio playback as a feature useful in work. Users can create or hear instructions, podcasts and verbal field notes with voice recorder–equipped devices.

Bluetooth connectivity is critical for hands-free vehicular communications using wireless headsets or in cars with built-in Bluetooth technology, and even for printing via Bluetooth-equipped printers.

Devices tend to differ more widely in their web-browsing capabilities, less because of compute power and more because not all browsers are created equally. This becomes an important consideration for deploying applications that have a web front-end, both for employees and for the public.

The hundreds of millions of deployed smartphones and tablets use not only a variety of operating systems, but also a variety of operating system and browser versions.

Rich as the choices might be, IT departments need to cut through the hype that surrounds new devices and test models before committing them to enterprise use. Battery life, screen resolution, camera performance, browser speed and rendering fidelity vary widely from device to device. And they often don't live up to advertised specifications. It need not be a massive test — many organizations equip two or three users within each of various employee subgroups to see how devices measure up.

Choosing a Provider

In many ways, an organization's selection of a wireless provider is as mission-critical as its choice of a cloud computing services provider (another area of rising IT importance). The growth in mobility has pushed spending on wireless voice and data plans above spending for landline telecommunications. And because so much business is transacted in a mobile fashion, the coverage affects reliability, productivity and business continuity.

Organizations must do their homework before soliciting bids from carriers for wireless services. Crafting a good request for proposals requires a thorough inventory of the organization's total wireless needs. It's important to examine both voice and data use because carriers treat each service separately, with separate pricing plans.

Another good practice is to close out pre-existing, individual user accounts in support of the anticipated organizationwide plan. That will ease administrative burdens and aggregate all usage for better leverage when negotiating with carriers. In the end, users or contractors who pay for their own plans might find themselves with better rates under the enterprise deal.

Still another useful exercise to help guide the IT department is a usage survey. It's a way to gather objective information about how different parts of the organization will interact with mobile devices. A survey should encompass the following elements:

Total number of users: Management will have to decide whether this includes contractors and part-time employees. That decision will depend on the extent to which these adjunct workers access enterprise data and applications (which also guides whether to include their devices in a mobile device management strategy).

Where employees work and travel: People who travel outside the contracted carriers' coverage areas are likely to incur roaming charges. The organization needs to anticipate these charges as part of mobility cost management.

Anticipated usage policies: Factor in restrictions on data downloads or messaging. Because users don't incur data charges when working in a Wi-Fi zone, some organizations permit large file downloads outside of Wi-Fi only in emergency situations.

Data requirements per user: This requires careful analysis of applications and what users need in terms of data movement.

Keep in mind that data flows two ways. For example, in calculating average

monthly usage, remember that users who download and edit documents will likely upload them too. Moreover, many commercial mobile apps synchronize and back themselves up when users invoke them, and that means more back-and-forth data.

Data use analysis can yield the benefit of getting organizations to think about application design. How an application is set up for mobility can exert a lot of influence on how much data travels back and forth.

A form-based app, for instance, can store the form display locally so that only American Standard Code for Information Interchange (ASCII) data entered on the form actually moves across the carrier's network. Or, if data upload is not time-critical, the application can be configured to store data locally until the device is within the carrier's coverage area. That would minimize roaming charges.

Regardless of application designs, analyzing anticipated data usage, user locations and total anticipated talk time will help the organization approach carriers with an accurate picture of their usage requirements.

Activation Considerations

Once the IT department has determined organizational needs, it's ready to approach carriers. The big four national-coverage companies — AT&T, Sprint, T-Mobile and Verizon — dominate the wireless carrier market in the United States. Many regional carriers cover specific sections of the country.

Unlike other contractors that organizations typically work with, wireless carriers also have a large consumer side to their businesses with a bewildering variety of plans and phone options. Organizations need not feel like individual consumers at the mercy of companies that operate more like utilities than customer-facing organizations. Many organizations consult with resellers that work with those carriers for better results.

One area that may be contentious during contract discussions with carriers is data rates. Carriers see data as an important source of profit and return on investment for the tens of billions of dollars they collectively spend annually on their networks.

Newer, faster devices and consumer demand for viewing bandwidth-hogging video can cause individuals to reach their monthly data plan limits (the largest of which currently top out at around 5 gigabytes) within days. On the other hand, 5GB of data is more than sufficient for the thousands of e-mails and text messages that a worker might typically send during a billing period.

Assuming that the organization will be paying for wireless (rather than reimbursing employees for their own plans or giving them a flat stipend), it's important to establish how the carrier will bill for data — per user or mobile device, or in total? If billing is in total (and this will be measured against an organization's limit), then the organization should ask carriers to provide information on individual service use. If any problems arise, this data can provide clues to possible rogue or unauthorized use, or whether the total service plan needs to be reallocated among types of users or user groups.

Going forward, 4G coverage will be an increasingly crucial carrier consideration. The market, once thought to be a competition between WiMax and Long Term Evolution (LTE) technologies, has settled on LTE. AT&T, Sprint and Verizon are all investing in LTE build-out, but coverage and signal strength for each carrier can vary by location.

Other carrier considerations include the following:

International calls: Determine how such calls are handled in terms of rates and billing. Carriers typically offer two types of plans: straight per-minute charges for a low volume of international calls, or volume plans that typically carry a monthly access fee but very low per-minute rates.

Roaming charges: This area represents another potential cost drain. Roaming has become less of an issue domestically, but can be expensive for employees who travel overseas. Enterprise pricing is negotiable. Charge options can include per-message or per-call fees, received message fees and monthly access charges that include tight data limits. Charges tend to be higher for mobile-to-mobile calls from overseas than for mobile-to-landline calls.

Device availability: AT&T, Sprint and Verizon all offer popular Android, BlackBerry, iPhone and Windows devices, plus tablets and netbooks. (T-Mobile does not at this time support Apple devices.) Also growing in enterprise popularity are mobile Wi-Fi hotspot devices for notebook computers. These devices support several Wi-Fi-equipped devices sharing a single wireless broadband account.

Mobility doesn't have to mean a smartphone for everyone, either. Be sure to consider basic phones, often offered for free, for basic users. Carriers offer refurbished phones for a fraction of the price of new phones. And it's also worth considering ruggedized and push-to-talk devices for field workers.

Equipment end of life: Ask the carrier if it buys back old phones (or at least accepts them for recycling). ■

CHAPTER 4

Mobile Device Management and Security

Controlling and safeguarding sensitive content with the right tools

CIOs worry — with justification — about cybersecurity risks posed by the variety of devices connected to their networks. And for several years after smartphone adoption began soaring, that wariness often held back mobile devices from deployment as enterprise network endpoints. The one prominent exception was allowing their use as e-mail clients, and that was driven primarily by Research In Motion's encrypted forwarding service for its BlackBerry devices.

But with the right policies and technologies, the IT department can mitigate cybersecurity concerns so that they are no longer a deterrent to an enterprise mobility deployment. Secure mobility takes a risk management approach supported by appropriate solutions and the understanding that mobile OSs can be secured.

Setting Device and Security Policies

Security starts with device selection. If the organization is supplying the devices, it need not be overly narrow in what it offers employees. Conversely, if there's a BYOD plan in place, it need not allow anything and everything.

Regardless of who owns the devices, the IT team should proceed from the proposition that a mobile initiative must put the organization's needs and concerns ahead of individual users. It's okay to restrict device options to only those running OSs with the latest security extensions. Keep in mind that sometimes the latest feature-rich versions of mobile OSs introduce new security holes.

One popular OS with a much-publicized update was immediately revealed to have six potential security weaknesses. That's not to say that the major vendors don't take security seriously — they do. For example, new and forthcoming releases incorporate sophisticated features such as address space layout randomization (ASLR), a technique that protects data in the device's memory.

The takeaway: Evaluate new OS versions before allowing them access to the network.

Policy should also include a ban on known, risky third-party applications.

While the manufacturers exercise some control over the developers allowed into their app markets, low developer registration fees provide small protection against developers whose apps are deliberately designed to violate sandbox barriers.

The IT department should also specify the software that must go on mobile devices, not just what stays off. A robust market exists in third-party security products designed to prevent data exfiltration and interapplication data exchange. The same goes for encryption, remote monitoring and virtual private network (VPN) software. When an employee chooses an ultralight PC or Mac, installation of the organization-standard antivirus package and regular updates should be required.

Every robust security policy for mobility should include a last-resort security control — that is, a way to logically destroy a device if it falls into the wrong hands or is violated by a cyberattack of some sort. This doesn't need to dampen employee enthusiasm for BYOD, because software now exists to let an organization separate enterprise data from personal data. Depending on how it's configured, the system administrator can remotely wipe the entire device or just selected partitions.

Some mobile device management (MDM) software lets managers create virtual machines running enterprise applications within a device's memory. These VMs can be targeted for removal, leaving personal pictures and e-mails untouched.

The IT group should work with the legal and HR departments in crafting these policies. Keep in mind that employees' private information on devices used for work may not be legally subject to the same monitoring and disclosure that applies to organizational information.

Mobile Device Management

Choosing the mobile devices that the organization will support is easy compared to choosing a mobile device management solution. MDM tools support provisioning, monitoring and protecting the organization's mobile devices. These tools also assist in enforcing policies.

At least three dozen companies distribute MDM software, ranging from some of the most popular names in software and security to niche vendors that specialize in one or two mobile OSs. An enterprise-worthy MDM needs to support all of the platforms the organization needs to support.

MDM software resembles network-based client support tools that mass-distribute applications, updates and security patches, except that mobile device managers typically do it wirelessly. The typical MDM package should enable remote provisioning, configuring, securing, locking and wiping devices. It should also provide access to inventory and software licensing information.

The mobile policies previously established by the organization will help narrow down the potential choices of MDM solutions. The organization's policy, as noted, should specify OSs, applications, usage, security and access. Obviously, the chosen MDM package must expressly support the provisions in that policy.

When comparing MDM offerings, it's important to make distinctions about precisely what is being managed. Devices themselves are reasonably inexpensive commodities, but the enterprise data they access is a precious resource, perhaps the organization's most precious resource. Therefore, organizational risk resides in data, not in the devices. That means the MDM solution should focus on protecting access and data as well as on locating lost devices.

Most of the large MDM vendors distinguish between pure device management and content management. Device management focuses on registration, inventory, location and tracking, and user authentication. Content management focuses on functions such as securing document distribution and monitoring enterprise network access patterns.

Some vendors further refine the subfunctions of their MDM offerings to include expense management. They let the IT staff limit individual user or device roaming charges, international calls or data usage. The MDM tools enable the IT shop to create reports showing trends and highlighting the outliers.

It can be easy to forget that mobility still includes compact netbooks, full notebooks and ultrabooks that use standard OSs designed for traditional chips. Some high-end MDMs can manage such devices in addition to the pool of iOS, Android, BlackBerry and Windows Mobile gadgets.

For many organizations, a key differentiator in MDM software is whether the solution is console-based or in the cloud. Traditional MDM products reside on an organization's enterprise

servers, much like other management tools. Other solutions are hosted by vendors in a cloud and are offered via a software-as-a-service (SaaS) model. Several providers offer both options.

With all cloud or SaaS solutions, organizations pay a predictable monthly fee and hand over responsibility for software updates to the provider, moving the expense to a more predictable operational cost. Keep in mind that some providers add a per-device surcharge for cloud hosting.

Still, cloud hosting offers easier scaling upward or downward when necessary. And geographically dispersed organizations can enjoy fast response times to issues because providers often operate data centers in different time zones.

MDM licensing costs can vary. Costing models can include per device, per month or a one-time perpetual fee per device, meaning the software is licensed for as long as the device is in use. IT managers will want to clarify whether the license includes maintenance and upgrades.

Encryption's Role in Mobility

The statistics are astonishing: More than half of Americans misplace a mobile device once a month, while one in four lose or damage their cell phones every year. More than 100 cell phones are lost or stolen every minute. Transit authorities in major cities each take in about 200 lost mobile devices every day. It takes the average person an hour to realize that his or her cell phone is missing. The most optimistic statistic puts the recovery rate for lost cell phones at 50 percent, although no one knows for sure.

Considering the picture these figures paint, organizations will deal with this issue frequently. How the device is equipped for cybersecurity will determine whether the loss is merely a $100 nuisance or a catastrophic loss of intellectual property and privacy.

As alluded to earlier, the real value in a lost mobile device isn't the hardware itself but the information it contains. The Symantec Smartphone Honey Stick Project showed that 89 percent of people who find a lost mobile device admit to at least peeking at the information it contains. It's hard to imagine a better justification for mobile encryption of data.

Encryption applies a mathematical algorithm to a data file that renders it unreadable. With the correct electronic key, the authorized recipient of the file can decrypt it. Encryption can take place at the file level, or the administrator can choose to encrypt entire disk volumes.

In practice, encryption requires its own infrastructure within the network to distribute keys and credentials for authorized users, and to manage the policies and rules the organization chooses to apply. But to be effective, encryption must require little effort from individual users — otherwise, they may try to work around it.

Normally, using encrypted data requires two-factor authentication, with the second factor being a randomly generated, one-time password delivered to the device via text message or to a small key fob the user can carry on a keychain. On the horizon, new phones may have facial recognition built in. If used, facial recognition could replace the password, but not the encryption key.

Encryption ensures that data at rest (stored on the device) is unreadable should an unauthorized person take possession of the device. And moving files in their encrypted format protects data in motion.

In crafting a mobile strategy, organizations should consider the additional option of encrypting phone calls. An employee might be overheard in a public place, but someone intercepting the radio signal will not be able to understand the conversation. Also consider MDM software that maintains phone logs, whether or not calls are encrypted.

Encryption services and their management consoles are either housed on a server within the organization or hosted as a third-party cloud service.

MOBILE VPNs

For some applications, organizations may choose to use the enterprise virtual private network (VPN) to transmit data. For example, data gathered in the field on a mobile device is immediately uploaded to a host, rather than stored locally. It may not be necessary for device software to encrypt the data because encryption will occur within the VPN.

VPNs identify the client attempting to connect by its IP address, which works fine for stationary devices. But mobile devices are on the go, moving from a Wi-Fi hotspot in a building to a 4G cellular network and then again to a new Wi-Fi hotspot. A conventional VPN connection won't withstand all that location shifting.

Mobile VPN clients create a logical IP address for the device together with a tunnel tied to that logical address, rather than to a specific physical address. The result is a connection that stays engaged even as the user roams from place to place.

This enhances mobility by preventing users from having to repeatedly log on to reestablish their VPN connection. That in turn boosts productivity, especially for workers performing location-based data gathering and transmission.

Small organizations with only one office or department tend to go with a hosted application, thereby avoiding the capital investment in new software and the staff required to maintain and operate it.

For very large mobile deployments involving something on the order of several thousand devices, the organization is more likely to have the financial and technical resources in-house to host its own MDM solution.

Adopting Multifactor Authentication

People tend to use their mobile devices in a completely unprotected manner. Anyone in possession of such a device can glean a great deal about the owner. Aside from requiring the use of rudimentary device-lock features built into smartphones, an organization's MDM strategy should also install and enforce the use of robust authentication to access resources on mobile devices.

Authentication solutions are more involved than what comes with mobile devices natively. There are several options available:

- **Software tokens** that generate one-time passwords that can be used in conjunction with usernames and semi-permanent user-generated passwords;
- **Mobile digital IDs** (often used for those with financial responsibility) that are strong enough to let users sign transactions;
- **Digital certificates** that can establish a user's credentials in web transactions.

Luckily, digital certificates are easier to deploy than to explain. Basically, they create a digital version of a trusted user's name, serial number, expiration date and personal encryption public key, all bound to the signature of the issuing authority.

In practice, the digital certificate attaches to a message to give the recipient trust in the identity of the sender. Digital certificate software should conform to the X.509 standard of the International Telecommunications Union. This decades-old standard specifies the architecture for public key infrastructures and the relationships among key issuers and key holders.

The use of digital certificates and software tokens addresses a fundamental premise of mobile security — namely, that more than one method is necessary to safely authenticate users to the network and to one another. The user name–password combo remains a viable factor, but a second factor is also necessary.

For simple access, many notebook PCs have fingerprint readers, but few smartphones sold in the U.S. have them. Therefore, the random password becomes necessary.

Guarding Against Malware

Until recently, mobile OSs didn't garner much attention from the malware developers. Malicious hackers stuck mainly to the Windows PC universe, developing a constant threat of evolving viruses and Trojans.

But that's changing. Security software makers that track developments in malware report an explosion of malicious software aimed at hundreds of millions of mobile devices. For example, McAfee reported that by early 2012 it had identified nearly 10,000 types of mobile malware. Most were targeting the Android OS, which runs on the majority of extant devices.

Mobile malware takes several forms. Phishing e-mails, crafted to look as if they are coming from a trusted source (such as the user's own organization or a well-known company or federal agency) contain links that lead to the installation of malicious software. Particularly for mobile devices, malware developers are embedding similar links in phishing text messages or messages of missed calls on Skype mobile clients.

CONFIGURATION SERVICES **KEEP CONTROL**

For security and manageability, organizations should tighten the allowable configurations, or machine images, for both fixed and mobile devices that access their networks.

MDM solutions provide efficient provisioning of devices with the organization's approved configurations. Configuration consists of more than ringtones and corporate logo wallpaper. In fact, those personalization settings are probably not worth bothering with as part of the enterprise configuration.

The MDM tools include the standard set of apps configured with the organization's usage policies, lists of URLs bookmarked in browsers and security features. All of this takes place wirelessly with most MDM packages.

Configuration doesn't stop with the initial provisioning of the device. It should also include application lifecycle management, ensuring each device has up-to-date versions and security controls. Regular over-the-air scanning should let the IT team know if a device is out of band in terms of configuration and create alerts to possible security problems.

These cause the user to inadvertently download rootkits that cede control of the phone to a remote server.

The best protection is a strong policy specifying what apps users may not download to their devices. At the least, third-party apps should be restricted to the vendor's own marketplace. For example, if the app doesn't exist in the Android Market or the Apple App Store, the organization probably doesn't want it on the phone. The policy should include a ban on any third-party file sharing, wallpaper and free apps.

Keep in mind that the OS vendors review authorized applications when they are published. Google operates its Bouncer service to continuously scan its market, looking for bad apps and ridding itself of them when found.

Presuming applications are clean when they are installed, IT managers are responsible for preventing future malware. The major antivirus vendors offer mobile OS versions of their protective software integrated into their MDM solutions for provisioning devices. The more comprehensive products combine antivirus with firewall and browser protection and cover all of the major mobile OSs.

Mobile antimalware products should include basic antivirus protection, particularly for Android and Windows devices, but should also include mobile-specific functions. For example, these include blocking suspicious texts or phone calls and scanning apps for odd behavior. If a mobile backup app stores data on servers in Russia, this is cause for concern given that Russia, China and other economic rivals to the United States have been regular sources of cyberattacks, intellectual property theft and malware.

These products may also include sandbox functionality that prevents leakage of data from one application to another. In BYOD setups, the IT department must be especially vigilant about walling off enterprise applications and data files from users' family photos, coffee-shop locators and any other common app that attempts to use data from adjacent apps. ■

WLAN and Network Support

Firming up the infrastructure for improved mobility

Increased mobile device use underlines the importance of a well-designed wireless LAN. Many organizations still operate a hodgepodge of Wi-Fi devices, some originally installed for the convenience of guests visiting conference rooms. Today, nearly everyone in an organization is a wireless user.

As mobile devices become the main work tool for a rising number of workers, it may be time to rethink the WLAN infrastructure so that offices, buildings and campuses are free of weak or dead zones, and so the WLAN can provide the bandwidth required to maintain an Ethernet-level quality of service (QoS).

To keep a check on costs, no organization wants mobile workers using precious carrier data plan minutes when wireless access points (APs) can be placed nearly anywhere throughout the enterprise's infrastructure. Supporting full mobility requires deploying equipment that uses the latest wireless standard (currently 802.11n, with the next generation, 802.11ac, under development).

The advantages of 802.11n include support for multichannel, multiantenna input-output for robust signals, use of the 5 gigahertz frequency for lower interference from other emitting sources, and sufficient bandwidth to carry multimedia applications.

Start with a Site Survey

Achieving thorough WLAN coverage without needless spending requires a site survey to determine the optimal locations for APs. The site survey will guide the network crew to avoid blockages, steer clear of sources of interference and ensure that power is available to the APs.

Don't rely on antiquated rules of thumb when determining where to put 802.11n APs. Numerous software products support WLAN site surveying.

These planners take into account the propagation patterns of antennae; the effects of walls, pillars and other barriers; the required level of signal overlap to avoid disruption of

latency-sensitive applications; and the density of usage that a particular area might get. For example, a classroom or auditorium intended for rows of people using notebooks will require a different WLAN configuration than a courtyard or cafeteria.

A site survey should also take into account AC power sources and the possible need to string electrical power to some APs. Devices should not be placed in locations where IT staff will have difficulty reaching them should they need to be swapped out or adjusted. Keep in mind that many devices operate with Power over Ethernet (PoE) and don't need additional AC cabling.

Once the survey and siting are roughed in, permanent installation should wait until the IT staff tests the layout. Testing should involve real devices running the actual applications the organization uses. Include a sufficient number of simultaneous users to stress the WLAN and ensure it will perform adequately. Keep in mind that pure signal strength is not a sole predictor of WLAN performance.

CASE STUDY

Read about how a grocery store chain's wireless LAN upgrade keeps it competitive:

CDW.com/mobileguide3

Controller-based Management & Monitoring

In a sense, all network monitoring is application performance monitoring. The point of making sure the enterprise network operates optimally is to ensure that applications run correctly. This is more important than ever in the mobility era, requiring consideration of these increasingly common scenarios:

REMOTE COLLABORATION: Users with wireless endpoints can collaborate from distant locations using multimedia application suites that may include video.

SKIPS AND JUMPS: Data packets move along a series of networks linking the enterprise backbone, WLANs and contracted cellular broadband. The WLANs constitute a subinfrastructure with unique management demands.

CLOUD COMPUTING: Applications and servers are hosted in the cloud (typically by a third-party vendor), which adds another traffic layer that can affect performance and should come with its own service-level agreement.

It adds up to a complex string of links for the IT staff to monitor. The more diverse and far-flung the network, the more urgently organizations need a common view of it for monitoring and management purposes.

The deployment of multiple WLANs compounds this need. Organizations are increasingly dependent on their WLAN infrastructure. This is partially driven by mobility, but not entirely. In some cases, WLANs are replacing wired networks because wireless provides flexibility in locating people and IT resources without having to move cabling.

As pointed out, the most logical way to provision and otherwise manage wireless devices is wirelessly. That requires a management console from which to carry out those tasks. But WLAN usage itself tends to scale and descale quickly. The objective of WLAN management is avoiding degradation in WLAN performance and the maintenance of seamless user sessions as employees, contractors and guests move about a building, courtyard or campus.

Achieving those goals in turn requires the ability to monitor APs. More than simply observing traffic, the network administrator needs the ability to provision and configure APs while maintaining a single view of how the entire network is performing.

Buildings and campuses usually consist of multiple, interoperating WLANs. So administrators also have to deal with the issue of scale and how it increases complexity. For example, APs are not used only for network access. They also perform network bridging and backhaul. Yet few organizations want, or can afford, to have a full-time network administrator at each location.

An enterprise-level controller, coupled with a management console from which to run it, becomes an effective solution for maintaining WLAN performance in many organizations.

/// ALTHOUGH IT IS PURELY A SOFTWARE SOLUTION, WHEN RUNNING ON A MOBILE DEVICE, A VPN CAN BE A DRAIN ON THE BATTERY. ///

To be enterprise-grade, a controller should perform certain essential functions. The first of these functions are discovery and provisioning of the APs. Cisco's protocol for this function is called Control and Provisioning of Wireless Access Points (CAPWAP).

The controller may also manage radio channels to avoid interference or assign coverage if an adjacent AP fails. It can also enforce enterprise policies for security, quality of service and the handling of virtual LAN traffic.

When choosing a WLAN controller, it's important to build in expectations of future growth. Manufacturers offer controllers in increasing capacities, starting with the ability to manage a handful of APs up to units that can manage more than 500 APs. Without enough overhead capacity, the controller itself can become a bandwidth bottleneck.

Because large organizations may need to cluster multiple WLAN controllers, it's important to choose a manufacturer that can scale, or that at least makes devices that interoperate with other brands.

Supporting Remote Access

Mobile remote access and fixed-location remote access share the use of a public telecom infrastructure to connect to the organization's own network. But connecting gets more complicated when mobility means actually being in motion (as opposed to just being stationary and connecting to a wireless signal). Maintaining the virtual private network session in these scenarios is more difficult.

When in motion, a mobile user can move among APs on the WLAN, between a carrier network and a public Wi-Fi hotspot, or even among networks within a specific carrier's domain. Mobile access technologies such as USB modems are smart enough to switch from 4G to 3G when coverage changes (or even to slower networks such as 1xRTT in rural areas). But not all applications can withstand these network changes.

Mobile VPN solutions offer a way to address this issue. They are designed to achieve session persistence in conjunction with seamless roaming. They also may include file compression to make the most efficient use of whatever bandwidth is available. Be sure to research the power consumption required by competing mobile VPNs. Although they are purely software solutions, when running on a mobile device, they can be a drain on the battery.

Mobile VPNs build on the common VPN standards of IP security (IPsec) and secure sockets layer (SSL) by assigning a logical IP address to the mobile device that appears to be fixed to the VPN tunnel emerging from the enterprise 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 in common 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 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, tablets 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 enterprises and educational institutions, such services can assist with keeping tabs on AV equipment, tracking the utilization of classrooms and meeting rooms, and recovering lost or stolen mobile devices. ■

PREPARING FOR 802.11ac

The next generation of the Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 promises to initiate the beginning of the end for wired networks. Final 802.11ac standards remain in development, with full ratification scheduled for sometime in the second half of 2013.

The new standard is theoretically capable of delivering gigabit-per-second speeds by using a variety of technologies in the 5 gigahertz radio spectrum. Chief among these is bandwidth of up to 160 megahertz, compared with 40MHz for the current 802.11n standard.

Manufacturers are shipping prestandard products because the chipsets are available. While it's unlikely that products conforming to the final standard will produce the maximum theoretical throughput, in the long run, 802.11ac will have a significant effect on mobility.

It may be too early to buy products suitable for enterprise use. However, it's not too early to think about preparing the infrastructure for 802.11ac.

A major consideration for this new standard will be power. Existing APs can generally operate using Power over Ethernet on the same Category 5 cable that carries the data. But 802.11ac APs are likely to need either two PoE lines or an AC power source.

This is because achieving 11ac's highest potential bandwidth of 1.3Gbps requires the activation of more radio antennas on the APs, which need more power to operate. Depending on the placement of APs, this could require major wiring work.

Network staff may also need to perform a new site survey because the 5MHz band has different ranges and propagation characteristics than that of 802.11n devices operating in the 2.4MHz band.

Organizations may want to consider purchasing a few prestandard units, together with a few notebook PCs containing 802.11ac transceivers. By testing how the APs and mobile devices interact in areas known to be difficult, the IT group can begin formulating a more detailed plan for what will be required to move the organization to the new standard.

The Right Applications for the Job

Boosting mobile productivity and communication with effective apps

Computing, whether fixed or mobile, is dependent on applications to get work done. Mobile application deployment that focuses solely on people and their mobile devices interacting with transactional applications in the cloud or the data center misses a big advantage of mobility — namely, mobile people-to-people interaction.

Initially, the mobile phone enabled convenient, anywhere conversation between people. Today, unified communications (UC) extends the enterprise to mobile devices, allowing mobile workers to not only talk and exchange e-mails with colleagues, customers and constituents, but also use a wide variety of collaborative applications.

UC Applications

Multimedia communication — principally, online meetings that combine two-way video communication together with documents and presentations — have become one of the more exciting applications of mobile technology. That people can interact with others in such a robust and multifaceted manner is thanks to both small and large technological developments, such as adding a front camera to devices and carrier investment in broadband.

That improved bandwidth has also spawned more flexible mobile collaboration tools. Some of them combine several elements to allow users to escalate an interaction from a simple exchange of text messages to a phone call or full online meeting.

The foundation for these applications includes synchronization of contacts between desktop, server and mobile devices; the ability of a device to broadcast a person's status (such as "available" or "in a meeting"); and access to an organizationwide directory.

A third class of collaboration software based on UC brings social networking and content creation into the collaborative mix. One example is a socialized version of Cisco Systems' popular WebEx. It has a Facebook-like interface enabling discussions, wiki-style document postings and on-the-fly teaming (temporarily linking up staff from across the organization for a specific project). Such tools come in mobile versions for the mainstream platforms.

Many UC apps rely on the open standard Extensible Messaging and Presence Protocol (XMPP). The Internet Engineering Task Force adopted XMPP a decade ago specifically for messaging and presence applications.

Enterprise Apps Go Mobile

One of the next phases of software development will make enterprise applications mobile. This will involve more than simply rendering interfaces designed for a 17-inch monitor suitable for a small screen and touch interface. It will also require new architectures that are better suited for thin clients than for client servers.

Currently, some mobilized apps merely display bitmaps on mobile devices, with all instruction execution occurring at the server. While there's

CONTENT *AND* APPLICATION MANAGEMENT

Organizations embracing mobility are putting their intellectual content on mobile devices. Beyond mobile device management, there is the more specific challenge of managing applications and content, along with the need to address potential leakage of important data.

Mobile content management is typically offered as a cloud software service with secure servers from which employees access proprietary documents. Value-added services supply the IT department with usage analytics giving clues to anomalous activity, such as users downloading at odd hours or in out-of-band quantities, or where users are located when accessing secure information.

Mobile application management (MAM) is another subset of MDM geared specifically to controlling the creation and distribution of mobile apps. MAM applies to both internally developed and third-party apps. MAM functions include not only provisioning devices but also making sure devices have the latest software versions, enforcing policies on who can use which apps and developing reports on usage patterns.

room for development, a number of important application categories already sport robust mobile interfaces:

ACCESSIBILITY APPLICATIONS: Applications made accessible for people with disabilities are one of the most active areas for software publishers. By combining all of a smartphone's internal features — scalable display, sound, touch and voice input, vibration, compass and gyroscope — it's possible to enhance applications for better accessibility, as well as turn out productivity applications specifically created for people with hearing or sight impairments, loss of fine motor skills or combinations of disabilities.

Code Factory's Mobile Accessibility for Android is one example. And the iPhone gets plaudits from the accessibility community for native features such as a voice-over screen reader and zoom magnification.

SOFTWARE REENGINEERING TOOLS: These tools turn PC client-server applications into mobile apps. The art is preserving functionality while fitting software into an environment marked by a small screen, smaller memory and storage, touch interface, and a different processor architecture and operating system.

But it's more than that. Developing (or redeveloping) applications for internal deployment or for services to customers requires a different kind of thinking, given the nature of mobility and mobile apps.

Analysts now advise organizations to think mobile first when developing new applications. Yet surveys show that no more than 20 percent have a formal mobility strategy. This means forward-thinking organizations with mobile development strategies have an opportunity to move ahead competitively.

Engineering software is a burgeoning area for mobility, and not just for software engineers. For example, several computer-aided design vendors publish mobile applications for mechanical engineers.

Autodesk's flagship product AutoCAD offers not only a mobile reader/editor for iOS and Android devices, but also an array of more than a dozen design-related mobile apps. Lesser-known MultiEducator offers Formulator, a line of apps encompassing formulas for several engineering fields, such as electrical and architectural engineering.

What's more, storefronts become important adjunct applications as organizations develop a larger number of mobile apps. For public-facing apps, organizations sometimes use both their own websites and the application markets operated by device vendors as distribution channels.

But having an internal storefront (more accurately, an application distribution center) will give the organization more control over security and role- or rights-based downloads. The storefront can also function as a place for employees or customers to share feedback on the usefulness of an application.

This is not something the internal IT staff needs to develop itself. Several vendors publish turnkey storefront software packages, some of which include mobile device management functionality. ■

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

Glossary

802.11ac

The next-generation standard for wireless networking, 802.11ac will likely gain ratification by the end of 2013. A standards designation of the Institute of Electrical and Electronic Engineers (as is its precursor, 802.11n), it promises a theoretical top speed of 1 gigabit per second, making it a viable replacement for wired Ethernet. It uses the 5 gigahertz band, where it encounters less radio frequency interference.

802.11n

This current standard for wireless LANs supports 54 megabits per second up to a theoretical 600Mbps and multiantennae deployments.

Address Space Layout Randomization (ASLR)

ASLR is a security technique used on mobile devices to prevent data exfiltration. It scatters pieces of important data files across different memory blocks, making it difficult for attack software to predict the target's specific address.

Android

Android is an open-source mobile operating system developed by Google. Android has the largest user base among mobile devices because several manufacturers build smartphones based on the OS.

App

An app refers to an application designed specifically for a mobile device. Apps are typically differentiated from client-server applications, with web interfaces that have been redesigned for mobile web browsers.

Bring your own device (BYOD)

BYOD is an organizational strategy for letting employees choose (and often pay for) the mobile device they wish to use for work. It derives from the popularity of smartphones and tablets among consumers, the devices now being capable of executing enterprise applications.

Code Division Multiple Access (CDMA)

CDMA is a 3G wireless telecommunications standard used mainly in the United States. The latest revision supports download speeds of 15.6Mbps. It is slightly slower than the competing GSM standard.

Consumerization of IT

This term refers to the adoption (for professional or business use) of IT products first entering the market as consumer electronics. The term typically refers to smartphones and latest-generation tablets.

Control and Provisioning of Wireless Access Points (CAPWAP)

CAPWAP is a Cisco Systems–developed protocol for letting a controller manage a few to hundreds of APs.

Controller, WLAN

A WLAN controller is software (which may come bundled on a blade or rack network appliance) used to manage wireless LANs from a single location or via a web browser.

Digital certificate

A digital certificate is an encrypted

attachment to an electronic message that contains the sender's unique identity elements. A receiver with the corresponding decryption key can be confident of the sender's identity.

Encryption

Encryption is the application of a mathematical formula to a data set that scrambles it and renders it unreadable. Only users with the correct key can decipher a message or file. Numerous standards cover the encryption field. The strength of encryption is expressed as the number of bits in the key, with the current highest-level standard being 256 bits under the Advanced Encryption Standard.

Global System for Mobile Communications (GSM)

GSM is a 3G wireless telecommunications standard used widely in Europe and in the United States by AT&T. GSM phones in general can't be switched to CDMA networks.

iOS

iOS is the operating system used by Apple for its iPhone smartphones and iPad tablets.

Long Term Evolution (LTE)

LTE is the most common fourth-generation wireless broadband technology deployed in the United States. It is used internationally and builds on the GSM standard, but it is also used by CDMA carriers such as Verizon.

M-commerce

M-commerce refers to deployment of applications designed by commercial or government organizations specifically for mobile devices and intended for use while customers or constituents are mobile.

Mobile Application Management (MAM)

MAM is software for controlling the creation and distribution of mobile apps. MAM applies to both internally developed and third-party apps. MAM software typically supplies information on usage patterns of mobile content. It can also include scanning functions to check for suspicious or disallowed behavior, such as seeking information from other applications.

Mobile Device Management (MDM)

Mobile device management refers to software for remotely and wirelessly provisioning, configuring, monitoring and erasing mobile computers, smartphones and tablets.

Mobility

Mobility encompasses the products, services and IT architectures designed to let employees of an organization work anywhere, anytime, with access to enterprise applications and data.

Smartphone

Smartphones are handheld devices, with screens up to 4 inches diagonally, that combine telephones and computers. Four operating systems dominate the smartphone market: Google Android, Apple iOS, Research In Motion BlackBerry OS and Microsoft Windows.

Tablet

A tablet is a larger handheld device with features comparable to a smartphone, but without the telephone function. Tablets typically have virtual or software keyboards, touch screens, high-resolution displays, extremely thin form factors and are light weight. Some notebook PCs, often ruggedized, convert to tablets but also have hardware keyboards. These types often use stylus input.

Ultrabook

An ultrabook is a notebook computer characterized by a full mechanical keyboard, solid-state hard drive, built-in wireless connectivity, long battery life (compared with heavier PCs with rotating drives), and an extremely light (often magnesium or aluminum alloy) chassis. Ultralight notebooks weigh between three and four pounds.

Unified Communications (UC)

UC refers to the integration of telephone, e-mail, text, video and collaboration software in the same device and operating on a common network infrastructure.

Virtual private network (VPN)

Virtual private network is a method of creating a secure communications tunnel using encryption and operating between a server and a user device over the public Internet. Mobile VPNs virtualize the IP address of the mobile device so sessions aren't interrupted when the user moves between wireless edge networks.

Virtualization

Virtualization is the rendering (as a purely software object) of all of the computing resources that make up a server or user account, including memory, operating system and applications. Virtualization enables consolidation of desktop or server machines and use of thin clients. User virtualization often accompanies mobility initiatives.

Voice over IP (VoIP)

VoIP technology converts analog voice signals into digital Internet Protocol packets so calls transmit over the enterprise data network. Digitizing of voice enables many features not available on analog switched systems.

Wireless LAN (WLAN)

A wireless LAN is a system of two or more radio frequencies and wireless access points (transceivers) using an IEEE 802.11 standard. Because the 802.11 standard applies to frequencies and power levels with limited, local range, creating a WLAN requires careful planning of the location and configuration of the transceivers.

Index

ABOUT THE CONTRIBUTOR

STEPHANIE SULT is a Mobility Solution Architect with CDW, specializing in the healthcare industry. In her role, Sult develops and implements comprehensive enterprise mobility solutions for CDW's healthcare clients. She specializes in enterprise mobile management, mobile device management, carrier activation services, telecom expense management and mobility IT help desk services. Sult holds a bachelor's degree in business administration from Saint Mary's College (Ind.) and currently resides in Chicago.

LOOK INSIDE FOR MORE INFORMATION ON:

- Crafting a comprehensive BYOD strategy
- Picking the right mobile device, plan and carrier
- Managing and securing a mobile fleet
- Boosting productivity with the right mobile apps