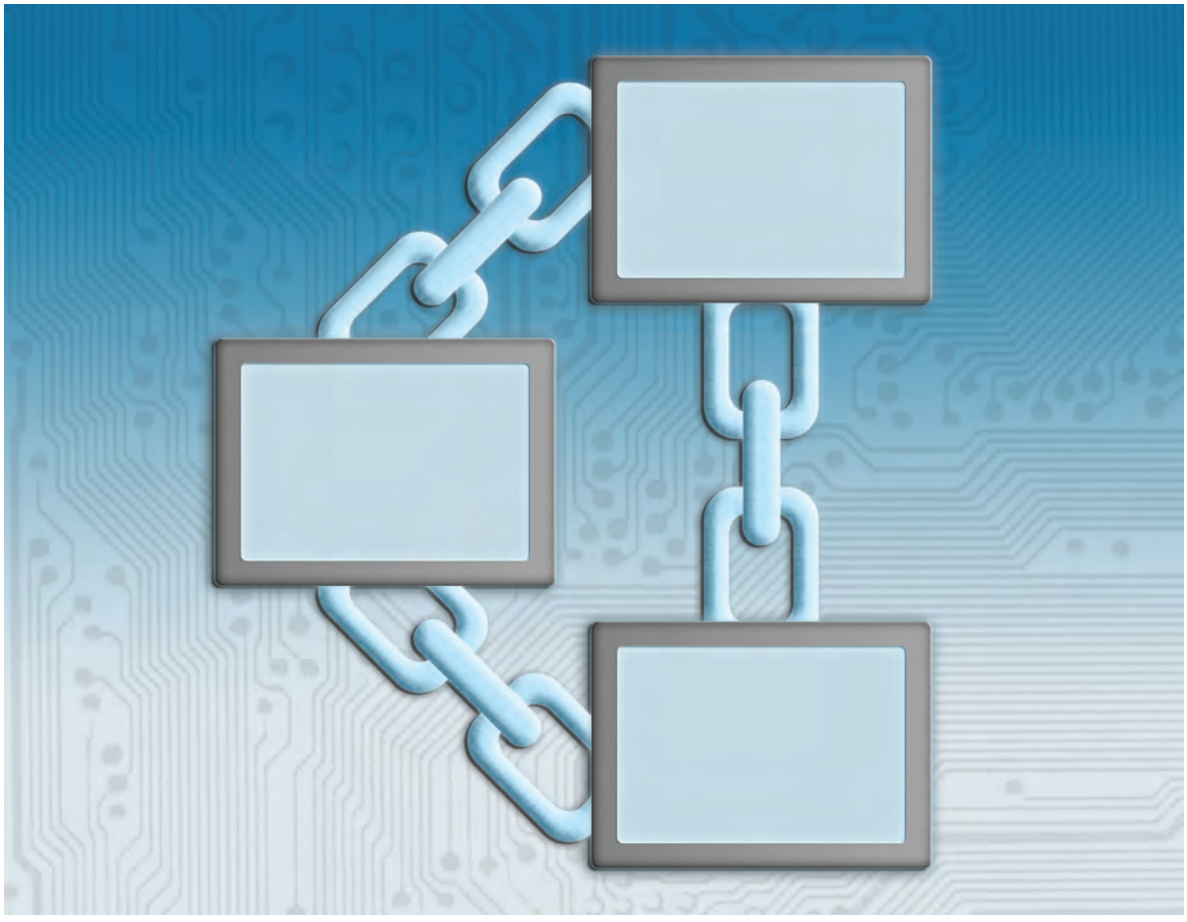
Online report sponsored by: CDW-G

# Network Infrastructure

## Full strategic report at:

www FCW.com/NetworkInfrastructure



**Inside:**

# UC solutions help streamline networks

Intense budgetary constraints, the administration's advocacy of data center consolidation, cloud computing, telework and a rush to adopt mobile computing throughout government are hastening the migration to unified communications solutions.

The concept behind converging voice, data, video and images has been around for many years. However, a confluence of factors is now driving government organizations to explore mobile computing technologies, cloud-based services, application delivery alternatives and wide-area network optimization tools.

As the largest consumer of IT worldwide, spending more than $76 billion each year, federal departments face intense pressure to reduce IT expenses. Several recent initiatives, such as the Office of Management and Budget's 25-point implementation plan to reform federal IT management and the Federal Cloud Computing Strategy launched by federal CIO Vivek Kundra, advocate data center consolidation and the migration to cloud computing as viable ways to cut costs and streamline IT operations. Kundra estimates $20 billion of the federal government's IT spending budget is a potential target for the migration to cloud computing. The savings could "be used to increase capacity or be reinvested in agency missions, including citizen-facing services and inventing and deploying new innovations," he said in the Federal Cloud Computing Strategy report.

Separately, President Barack Obama signed the Telework Enhancement Act in December 2010, setting a deadline of June 9 for the implementation of far-reaching strategies for embracing telework throughout the federal government. (See related story, page s4.)

Government oversight organizations, including the General Services Administration, National Institute for Standards and Technology and OMB have drafted guidance, and GSA has launched new procurement vehicles to support agencies as they strive to achieve greater efficiency and adhere to the new mandates.

As a combined result of the new initiatives, the administration hopes to help federal agencies overcome challenges that they have faced for years in managing disjointed systems, networks and burdensome legacy platforms and applications.

Unified communications can help contribute to productivity gains and significant cost reductions, according to industry observers. UC not only provides more reliable and cross-functional communication but also increases resilience against network disruptions. In addition, UC enhances a sense of belonging and affinity among remote or mobile workers.

According to Brian Kopf, manager of unified communications for CDW, parent company of CDW-G, the definitions of unified communications are as plentiful as the companies that provide component technologies. "There is no such thing as one-size-fits-all in UC," he said.

The definition CDW uses is "the convergence of enterprise voice, video and data services and software applications to achieve greater collaboration among individuals or groups and improve business processes."

There are several broad categories of approaches to unifying communications on a single platform. Many agencies are pursuing either rich-media or telephony-centric approaches to implementation, he explained, while others are focusing on e-mail- or instant messaging-centric approaches. The array of available technologies make selecting a UC solution a complex undertaking, Kopf said. "There are many things to consider when deciding what is right for your agency, including the nature of your organization's work and its physical structure," he added.

Even though there are few industry-standard UC approaches, the range of solutions available enables government organizations to create tailored solutions that fit each organization's individual needs, he added.

## UC research underscores expansion

The results of a new 2011 CDW-G survey of 150 federal IT managers who contribute to decisions on the adoption of voice and telephony, conferencing, or messaging technologies, included several important findings.

- 59 percent said their agencies have developed a business case and/or strategic plan for the adoption of unified communications.
- 26 percent said their agencies have not developed a business case and/or strategic plan for the adoption of unified communications.
- 15 percent said they were unsure.

In the same survey, federal agencies already planning or implementing unified communications said they are leveraging one of the following approaches:

- An e-mail-centric approach 24%
- Rich-media conferencing approach 24%

- Telephony-centric approach 16%
- An enhanced business processes approach 15%
- Mobility-based approach 8%
- Instant messaging and presence approach 5%
- Unsure 8%

As far as the component technologies of unified communications, of the 150 federal IT managers surveyed:

- 79 percent said their agency has fully or partially deployed videoconferencing.
- 66 percent said their agency has fully or partially deployed voice over IP.
- 64 percent said their agency has fully or partially deployed instant messaging.
- 60 percent said their agency has fully or partially deployed unified messaging, meaning access to e-mail, voice mail and faxes is delivered via a common computer application or by telephone.
- 49 percent said their agency has fully or partially deployed presence technology. These are solutions that detect and convey information about a user's status, such as the type of device they are using, its operating environment, location and local time, and other messages the user chooses to announce.

With the convergence of communications technologies, the advent of greater mobility and cloud computing, federal agencies should expect to gain higher levels of convenience and efficiency in their network operations. Input published a new report in late February titled the "Federal Communications and Network Services Outlook, 2010-2015," examining trends and obstacles and identifying UC as pivotal to resolving infrastructure barriers for communications systems and practices within the federal government.

"These technologies provide tremendous benefits to government networking and communications in and of themselves," said Input senior analyst Richard Schum about the report. "We now see that even stronger enhancements occur when they are teamed together to create a cohesive, unified system. We believe these synergies will be a crucial factor in minimizing interoperability issues and improving the timeliness of communication for government agencies."

The Input report outlines how federal agencies that have not yet updated their communications backbones will likely move toward streamlined infrastructures that merge voice and data communications in the near future. A supporting survey conducted by Input revealed that only 36 percent of respondents said their agencies had already implemented some type of unified communications solution. Further, 61 percent claimed their agencies had not yet started moving toward unified voice and data communications, even though almost all participants said they would do so in the next five years.

Input analysts say an accelerated adoption of UC is expected as the synergies related to the interconnectivity of mobile and cloud-based computing technologies continue to grow. "Cloud computing offers the promise of providing unified communications-as-a-service to be accessed through existing clouds," said Lauren Jones, principal analyst for Input. "Especially for those civilian agencies that have been slow to consider unified communications and may not have a UC architecture and infrastructure fully in place to support it, moving to UC as a managed cloud service might make a lot of sense."

The report is available on Input's website at *FedCommunications.input.com*.

Getting to a UC platform requires careful thought and planning. Without a single, standard solution for UC, agencies are instead pursuing rich-media or telephony-centric approaches to implementation while others focus on e-mail- or instant messaging-centric approaches.

There are many things to consider when deciding what is right for any agency, including the nature of the agency's work and its physical structure, Kopf said.

CDW-G's UC experts offered the following advice to successfully implement UC:

- Identify the weakest link in the chain. If the current network is not strong enough to handle an increase in traffic brought on by UC, it's not likely an agency can achieve optimal results. This is why it's so important to review the organization's current network environments, assess current and future needs, and incorporate those requirements into a scope of work for design and implementation. Because UC is not a one-size-fits-all, packaged solution, it works best to take a phased approach. What is best for any agency is a network and UC solution set that can keep running, even when the weakest link is at or near maximum capacity.
- Don't shortcut the training. Training employees on the maintenance and use of UC components is essential. Begin preparing them for implementation during installation and configuration. The goal should be to launch a reliable system that won't disrupt daily operations.
- Implementation is easier than one may think. It's not easy to sell the idea of a revamped, agencywide communications system, while recovering from the toughest economy since the 1930s. However, once management understands the benefits and compelling operating efficiencies that UC brings, agency executives will quickly overcome many of the early apprehensions they might have had about network security, equipment and capital cost requirements. ▲

# Telework Enhancement Act boosts UC

The passage of the Telework Enhancement Act in December 2010 underscores the growing need for better secure remote access to ensure that only authorized users gain access to government networks and information. As mandated by the law, federal agencies must improve the use of telework as a strategic management tool.

The law requires agencies to notify all federal employees about their eligibility status for telework by June 9.

Other important telework policies and programs to be set up by the June deadline include:

- Establishing a policy authorizing eligible employees to telework.
- Requiring a written telework agreement between employees and managers to ensure that telework doesn't diminish employee or agency performance.
- Providing an interactive telework training program, to be completed before the signing of the telework agreement, to employees who are eligible to telework and their managers.
- Requiring each executive agency to incorporate telework into its continuity-of-operations plan.

In February, the Office of Personnel Management issued its annual Status of Telework Report to Congress with information about the number of federal teleworkers. The report found an increase of 11,046 in agency-reported teleworkers from 2008 to 2009. This brings the agency-reported federal government total to 10.4 percent of eligible employees teleworking, or 5.7 percent of all federal employees.

Meanwhile, other industry reports indicate the number of federal employees teleworking may be higher. According to a report in January by the Government Business Council, sponsored by CDW-G, 89 percent of federal workers surveyed reported that they work outside the office, more than half of them at least weekly.

Although 97 percent of federal employees are required by their agencies to use authentication measures such as passwords, security tokens and biometric identifiers, most take still more security precautions to protect agency data. Respondents noted that they proactively lock their screens when they are away from their computers and only use secure network connections and agency-issued machines to further secure information.

"Today's cyber criminals have multiple routes for illegally acquiring information, whether by stealing physical machines, tapping into unsecure wireless networks or propagating malware," said Andy Lausch, vice president of federal at CDW-G. "Federal employees — the majority of whom spend at least some time each week working remotely — keenly understand that they must take extra steps to secure confidential and sensitive agency data."

Most of the respondents surveyed agreed agencies could improve the functionality, responsiveness and ease of use of IT offerings provided outside of the office. While away from their regular offices, respondents perform routine tasks including checking work-related e-mail messages; reading, composing or sending work-related documents; and participating in work-related calls. Seventy-one percent of respondents said they are eligible for telework. In addition to working from home or a telework center, respondents said they work remotely while in transit to work, at another agency's office, from program sites and while traveling.

## What agencies should do

In a recently published report titled *"Implementing Telework: Lessons Learned from Four Federal Agencies"* by Scott Overmyer, professor and director of the master's degree program for information systems at Baker College in Flint, Mich., made recommendations for what agencies should do now to comply with the telework law, including developing a comprehensive telework plan.

This plan should be part of the agency's mandated effort to establish policies for telework eligibility and determine employee eligibility. In addition to including information on eligible positions, Overmyer said the plan should answer the following questions:

- What is telework, and how does it function for the employer and employees?
- What is expected of the teleworker?
- What is expected of the organization?
- What organizational positions and job responsibilities qualify for telework?
- What is the agency telework training plan?
- How will teleworker performance be evaluated?
- What are the continuing education requirements and opportunities for teleworkers?

Also, agencies should be working on clear, written policies and telework agreements, according to the report. Written policies outlining the roles and responsibilities of teleworkers and managers are crucial, Overmyer said, so there will be no misunderstanding of expectations.

To comply with the new law, training for employees and managers should receive high priority. At a minimum, training should address management and performance, in addition to information technology, software and security. Managing an increased number of employees from a distance will require special skills and techniques. ▲

# Five network upgrade pitfalls

CDW-G's team of technology experts recently highlighted the primary pitfalls that can arise for public-sector organizations when they upgrade their network infrastructures. The following list highlights some of the most common network upgrade problems, along with advice for resolving each concern.

### Problem 1: Missing network visibility for management.

As networks grow, cheap, unmanaged switches aren't scalable and don't accommodate the requirements that arise in larger networks. A lack of visibility into network performance for a 100-user network can turn a minor problem, such as a failing network interface controller, into a broadcast storm that could bring down the network.

**Advice:** CDW-G's team of experts recommends that agencies avoid this problem by spending a little extra to purchase managed switches that can provide the visibility into network operations as required.

### Problem 2: Choosing not to purchase Gigabit or Power over Ethernet (POE) switches for agency access layer networks.

Both POE and Gigabit switches are often overlooked features when expanding or upgrading a network. Although adding those features might increase the cost of the network, they will provide significant savings for any government organization by helping to avoid a "forklift upgrade" when implementing IP phones or wireless 802.11n networks for enhanced mobile access to government networks.

**Advice:** CDW-G experts suggest that agency customers consider possible future upgrades to network infrastructures when purchasing replacement networking equipment to avoid costly upgrades when migrating to IPv6 or wireless mobile networks.

### Problem 3: Choosing to reject Layer 3 switches in small to midsize networks.

Government customers using Class C networks are limited to 254 hosts or IP addresses. Growing networks can use up IP addresses pretty quickly. Once an organization gets to 254 hosts, it will need to create a new network or subnet. In order to communicate from one subnet to another, the agency will be required to route between the two subnets.

**Advice:** By incorporating the use of Layer 3 switches, government organizations will be better able to route between subnets and avoid running out of IP addresses.

### Problem 4: Using only 802.11n wireless on 2.4 GHz radio and not 5 GHz radio.

A primary property of the 802.11n wireless protocol is that throughput is increased by channel bonding, or combining two 20 MHz channels to make a wider 40 MHz channel. On 2.4 GHz frequency radios, only 11 channels are available, and only three of those are nonoverlapping. Newer 5 GHz radios have 23 nonoverlapping channels, which is ideal for channel bonding and transmitting wirelessly via 802.11n. On 2.4 GHz radios, there is a much higher probability of interference between access points trying to use the same channel. This limits the number of access points that organizations can deploy and the distance at which access points can be spread apart.

**Advice:** To avoid interference, it makes sense to buy dual-band access points for 802.11n networks. Single-band solutions might cost less but won't work as well in networks with multiple access points.

### Problem 5: Buying gray-market networking equipment.

Buying network equipment from gray-market sources can be risky. Although generally low pricing might make certain gray-market devices attractive, government organizations must be experts in whatever products they purchase and will be on their own if manufacturer support or updates on the device's operating system are required at a later date.

**Advice:** CDW-G recommends avoiding gray-market purchases for major networking purchases, such as wide-area network optimization, server load balancers, security, core switches and routers. An agency gains full support from the manufacturer when in compliance with supplier licensing requirements. ▲

# USGS serves up vital earthquake information

The magnitude 9.0 Tohoku earthquake that took place March 11 near the northeast coast of Honshu, Japan, resulted in 6,000 hits per second on the U.S. Geological Survey's earthquake-related websites, which are delivered via a content delivery network (CDN) service.

The peak Web traffic record achieved by USGS still stands at 52,000 hits per second following the 7.2 magnitude earthquake that occurred on Easter Sunday 2010. USGS now has additional metric data available on site traffic, which shows that earthquake sites received 400,000 visits and 1.5 million page views on an average day for the month surrounding the latest Honshu earthquake. The peak following the recent Japan earthquake and tsunami was 900,000 visits and 2.5 million page views per day.

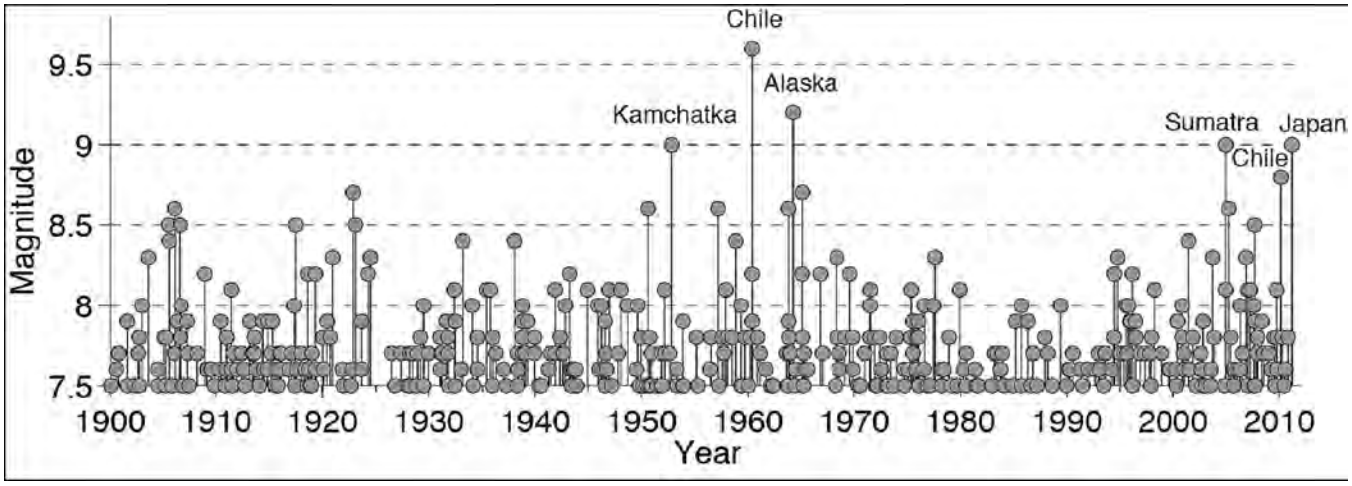
According to Lorna Schmidt, program manager for the USGS Enterprise Web Program, earthquakes that occur in the United States, particularly in densely populated areas result in significantly larger spikes on our websites than those that occur outside the United States. Such massive spikes in data and information requests, produced by flash crowds who felt the earthquake, generally occur very soon after an earthquake event. "Such spikes, or peaks, generally have a precipitous drop off to a more smooth, elevated request rate for some period surrounding the event. This may be due to news coverage, family interest or other means of distributing information in the event," she said.

USGS relies on a Level 3-supplied CDN to manage the flash crowds for earthquake data requests and provides cached access to data from globally distributed systems. Access to source data is critical to USGS' primary mission, providing updated, refreshed content to citizens as well as internal programs and processes. The CDN allows USGS to get the job done with an infrastructure that is leased through a CDN contract, rather than owned, to reduce costs.

During the recent 9.0M Japan earthquake and tsunami, the Level 3 CDN performed bursting, which replicates requested data through the global network, serving increasingly more bandwidth to users until peak demand was satisfied. Then the CDN eased off replicating as demand drops back to more typical levels. USGS pays service fees both for DNS and bursting charges.

Data coming into USGS, such as earthquake sensor and

**A History Of Large Earthquakes**




Source: USGS
Figure courtesy of Charles Ammon, after Ammon et al., SRL, 2010

streamflow data, travels multiple paths from thousands of stations to redundant systems to ensure delivery to the USGS emergency notification system and to the public. USGS Web content hosted within the NatWeb infrastructure, such as local science centers and many National USGS Program sites, is managed in a cloud of file and Web servers at three data centers across the United States. Each center's servers are configured identically for backup purposes, with data replicated among all servers.

The current environment supports the agency's continuity-of-operations plan and allows USGS to continue to provide access to natural resources data, no matter how great the demand. A CDN with a worldwide presence reduces geographic latency, or the distance between the requester and server, USGS officials explained.

### Lessons learned

Over the years, USGS has learned that testing the system is important. In addition, monitoring Web sites before, during and after an event can help improve resiliency. In all phases of the information life cycle, organizations must build and account for redundancy. USGS officials recommend that organizations design any Web infrastructure with performance demands and outages in mind and plan for the necessary redundancy upfront. The current server infrastructure, along with the use of a CDN, allows USGS to gather data and keep it available even when demand peaks during emergency situations.

As part of life cycle planning, the Enterprise Web Program and USGS will continue to evaluate strategies for delivery of USGS content and information, taking into account a fluctuating budget, security, performance and technology requirements. ▲

## A little background

At the U.S. Geological Survey, the mission is science, including the collection, analysis and distribution of data and information used to help answer an array of complex questions that span multiple disciplines in the realm of natural sciences.

USGS has 9,000 employees in 400 locations around the world. USGS maintains data centers in the United States, but its technology reach extends to streamgauges, volcano sites and earthquake reporting stations around the world.

In 2010, USGS reported the following from Netflow statistics and log file analysis:

- 3.8 petabytes of data transferred from all ports in and out of USGS.
- A total of 949 terabytes of Web traffic in and out of USGS, not including content delivered by Level 3 to public earthquake-related websites and www.usgs.gov.
- 127 terabytes of data delivered by NatWeb, which hosts half of USGS' websites, including www.usgs.gov, but not NWISWeb or the earthquake sites.

# Let UC join existing upgrade projects

Although it might seem counterintuitive, organizations that have already successfully implemented unified communications claim it works best to combine a UC deployment with other changes already in development.

For example, federal organizations are working to consolidate data centers and add better remote access capabilities to achieve compliance with key federal mandates, including the Office of Management and Budget's 25-point plan and the Telework Enhancement Act.

Organizations that have successfully implemented UC, as indicated in CDW-G's 2011 Unified Communications Survey, reported that along with deploying UC solutions, they are also often doing at least one of the following:

- Establishing a new call center or expanding an old one.
- Integrating or consolidating two or more existing networks.
- Expanding or deploying a telework program for a significant portion of the organization's workforce.
- Replacing obsolete or inadequate existing networks.
- Implementing a continuity of operations plan and supporting capabilities.
- Integrating branches of distributed operations, such as field offices.

That is why CDW-G executives recommend that IT managers take advantage of the opportunity to update communications systems by discussing with top agency management officials how to couple telework and consolidation improvements with improvements in communications that can enhance the organization's efficiency and generate savings. ▲

## Best practices for securing wireless network access

Security practices for protecting wireless networks, especially connections to primary wired infrastructures, have matured in recent years. It's now possible for wireless local-area networks to not only achieve the performance rates of wired networks but also remain equally well protected if IT managers implement the right combination of security measures.

CDW-G's technical experts offered the following advice for how to better secure wireless access.

- **Beware of spoofing assaults.** When devising wireless security strategies, network administrators must remain wary of spoofing, a longtime practice in which hackers hijack the communications of users who believe they're sending sensitive information through a secure pipeline.
- **Encryption and authentication features**, now considered a standard feature of switches and access points, must be used to protect wireless transmissions. Defending against vulnerabilities is complicated because wireless signals can travel through walls, leaving networks open to intrusions outside an organization's building.
- **Special intrusion prevention systems for wireless environments** can help network administrators quickly identify unauthorized devices that try to break through security defenses. That is critically important for federal agencies and departments when securing areas where wired and wireless networks intersect.
- **Wireless-savvy intrusion prevention devices are worth examining** because they can beat back denial-of-service attacks designed to crash networks. Geofencing, a virtual perimeter around a geographic site, and other related techniques can be used to help IT managers grant access only to devices running at known and trusted physical locations.
- **A virtual LAN is another wireless security tool** that can help regulate traffic using access control lists to guard against vulnerabilities that arise when guest users must find a way to connect to the Internet via a wireless link. IT managers might instead choose to dedicate a wireless LAN controller to divert guest traffic to a secure location outside the organization's firewall.

Source: CDW-G


Today, government agencies rely on optimized connectivity. We get it. With dedicated account managers, solution architects and partnerships with leading vendors like Cisco, Brocade and Avaya, we can help you design and build a solution that's fast, flexible and secure. One network, reliable, with bandwidth and communication for all.

**Get things moving at CDWG.com/networking**

CISCO PARTNER Gold Certified

BROCADE

AVAYA

+

CDW·G PEOPLE WHO GET IT™