NETWORKING AND UNIFIED COMMUNICATIONS REFERENCE GUIDE

Boosting services for greater productivity and collaboration.

CDW.com/networking-ucguide | 888.667.4239

CDW®

The Right Technology. Right Away.®

NETWORKING

NETWORKING AND UNIFIED COMMUNICATIONS REFERENCE GUIDE

TABLE OF CONTENTS

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.

NETWORKING AND UNIFIED COMMUNICATIONS:

IMPROVED SERVICE, BETTER COLLABORATION

CHAPTER 1:

It doesn't take difficult economic circumstances to prod businesses into finding better ways to carry out their missions. Seeking ways to improve efficiency is the norm. This is especially true for IT departments, which are continually pressured to either improve operational capabilities or decrease costs — preferably both at the same time.

The network is now an established domain in most companies. It is an area that especially feels the push and pull of increasing functions while cutting costs. While a down economy can spur belt-tightening initiatives and stifle IT spending, firms still have great dependence on advanced network capabilities to drive revenue.

Today organizations want IT to be an enabler of growth. As the firm grows in size, a superior network infrastructure can make other inputs more productive, thereby helping to control costs. The idea is to have IT deliver more productivity- and profitability-building services — even as budgets are being reduced.

GREATER FUNCTION VS. LESS COST

The gains from having a robust IT network are immense as well as immediate. This type of infrastructure can provide dynamic and scalable services that deploy easily and allow for added functionality. The objective is to optimize the utilization of resources to streamline management and free diminished IT staff to work on the most mission-critical projects.

All the while applications continue to become more complex, and their reliance on a robust network continues to become even more pronounced. Software manufacturers increasingly create applications that utilize the resilient nature of IP. And they assume a high level of service availability for those applications.

Network infrastructures must provide dynamic and scalable services that not only deploy easily, but also allow businesses to add functionality as required. And IT managers have an obligation to decrease the Total Cost of Ownership (TCO) and increase ROI while still meeting the functional challenges of the data center.

Today's network requirements include a distinctive combination of more connectivity, information exchange and bandwidth. All of which makes the network element a critical part for facilitating and enabling other technologies.

NETWORKING TRENDS

The network lies at the heart of many enterprises. It connects the computers that manage the company's data. And it provides staff with information and communications. One source of its fragility is the immense number of new applications it is being asked to support.

Businesses have begun converging physical security and networking functions into one robust and easily managed solution. These initiatives, necessary to decrease TCO, nevertheless add to the complexity of the traditional IP network. Two other initiatives, virtualization and server consolidation, have similarly increased network importance.

Many server managers have leveraged their existing server resources through virtualization, using the network to distribute applications over a larger IT landscape. This added functionality

requires network solutions that are highly integrated, scalable, robust and easily managed.

To simplify management and ensure that no single solution operates without oversight, it is necessary to provide unification via an overarching management tool. Organizations now regularly depend on such network management solutions to identify outages and other network problems proactively rather than reactively.

In seeking to meet these sometimes conflicting needs, technical managers work to boost services by adding various application acceleration and bandwidth optimization devices to the network. These network devices enhance the responsiveness of critical IP-based applications.

UNIFIED COMMUNICATIONS TRENDS

Having laid network foundations with local-area and wide-area solutions, application functionality and productivity for the staff become primary concerns. With Unified Communications (UC), IT departments can offer streamlined communication solutions and advanced productivity applications throughout the network.

Because of the facets it incorporates and combines, UC is a powerful and complete communication medium that eliminates device and media dependencies. It has unquestionably changed, for instance, the way businesses provide connectivity between staff.

In a true UC environment, all voice, data and video, along with e-mail, instant messaging and calendaring applications, are fully integrated. This allows staff to access data on demand and effectively communicate and collaborate in real time with virtual teams anywhere in the world.

Advanced presence capabilities, for example, provide the real-time status and availability of other staff, including preferred methods of contact. With this level of presence, employees can quickly determine who is accessible and in what capacity.

UC solutions can further extend the capabilities of the communications network beyond the confines of the organization environment. Regardless of location, they can provide presence and voice communications via smartphone technology as if the employee were physically in the office.

Video communications and desktop collaboration are also emerging as salient UC solutions. Both provide tremendous benefits including the opportunity for substantial cost savings. Keep in mind, 80-to-90 percent of human communication is based on visual queuing. So video serves to significantly enhance the quality of virtual meetings.

Whether video communication is accomplished peer-to-peer through desktop interrogation, multisite video system or high-definition telepresence solutions, it allows coworkers to utilize the most effective mode of contact possible. This results in enhanced and more interactive communication in addition to reduced business travel costs.

Add the functionality of web conferencing — the ability to share documents, presentations and any stored media — and UC becomes not only thoroughly versatile but increasingly indispensable in today's communication environment. ◊

BUILDING A RELIABLE NETWORK

CHAPTER 2:

Today's networks incorporate a broad range of technologies. However, IT managers can't realize the promise of improved service and network availability unless they have a solid foundation on which to build.

Garnering enough robustness for the next generation of networks must be a high-level objective. A forward-looking solution will be one that provides the underpinning to meet expanding business needs.

REDUNDANCY AND RESILIENCY

With more reliance on the availability of systems, applications and data, the network must be up to the task of supporting critical traffic to maximize uptime. After all, if the network fails, so does everything riding on top of it.

Levels of reliability that used to be considered sufficient often won't prove effective for low-latency traffic. That's why it's critical to design a network that supports current and future technology requirements. Flexibility and scalability are key for future-proofing the UC platform.

A redundant network maximizes uptime and performance by eliminating single points of failure. Such a network offers multiple LAN or WAN paths and spare hardware components that kick in if a primary component fails. This helps ensure the availability of critical applications and data whenever and wherever users need them.

Another desired quality, resiliency, refers to fault-tolerance and failover mechanisms that can maintain network availability. Resilient networks provide reliability without requiring duplication of all the hardware they comprise.

In general, decreasing the complexity of the network eases troubleshooting and improves resiliency. Taken together, redundancy and resiliency add up to network reliability.

BUSINESS BENEFITS

A reliable network that supports current and future applications delivers ample advantages. One of the most critical benefits is maximizing uptime.

Many organizations seek 99.999 percent network availability, dubbed "five nines," which equates to only 5 minutes, 15 seconds of downtime per year. (See chart on page 8.) For some users, perhaps a slightly greater level of downtime will be sufficient.

The level of network downtime an organization and users can tolerate depends on its requirements as well as the type of traffic the network carries. Different parts of the network may have different availability requirements, and different redundancy requirements may be appropriate for different classes of service.

Whatever the goal, designing a solid network infrastructure often requires having redundant components. Having dual processors, power supplies and hot-swappable network cards in place can provide a high degree of reliability.

Network redundancy and resiliency also makes the most efficient use of expensive bandwidth. Proper bandwidth utilization helps conserve resources to offer the quality of service demanded by converged applications and time-sensitive traffic.

Here fine tuning the network can help make the most of a technology investment. This is opposed to simply throwing a bigger and more expensive pipe at the problem.

Redundancy will also improve an organization's disaster recovery posture. Business continuity requires the network to remain up and available. Redundant connections and intelligent routing protocols allow traffic to navigate around bottlenecks or failure points.

Uninterruptible power supplies and generators step in when there's a power outage. Hot-swappable hardware stands in if a component fails. And flexible failover options make for a graceful recovery should disaster strike.

Having a robust network in place also aids network management and reporting. Agents and management protocols do their jobs and report the results.

This makes it possible for administrators to gain a holistic view of the network. And reporting tools and predictive modeling can help ensure resilience by identifying trends or trouble spots and planning for future capacity requirements.

DESIGN AND IMPLEMENTATION

The first step in enhancing network availability is figuring out what you want and what you already have. How many users and sites does the network support? What applications does it carry? And how does traffic flow?

Determine the requirements and level of availability to support company functions and develop a network strategy accordingly. Upper-level management and users from all departments should help substantially in specifying needs and establishing operations requirements.

Only with these insights can adequate traffic priorities be set to maximize throughput efficiently. An IT governance board can offer useful input through the use of project and development milestones.

IT Asset Management

Planning a robust network requires performing a network audit to gain a deeper understanding of the hardware, software and Access Points (APs) in the existing environment.

This is where IT asset management systems come in.

Asset management systems serve as a repository for information. They can include data about equipment size, type, age, make, model, technology and compatibility.

Network inventory tools crawl the network to identify hardware and software assets — even those in remote or branch locations. This catalog of information will prove vital for managing software licensing, balancing usage and demonstrating licensing compliance.

IT can also use inventory and asset management tools to determine where PCs are and who is using them. And they can help identity which end-user systems may need upgrading to handle unified communications applications such as video conferencing.

Organizations that use IT asset management systems such as barcodes or Radio Frequency Identification (RFID) labels can quickly identify the location and type of desktops, servers, workgroup switches, wireless APs and any other network devices deployed throughout the enterprise. Such information is invaluable when it comes time to issue patches or upgrades.

Overall, an accurate assessment of the current environment along with a gap analysis will pinpoint what's missing. And it can assist in determining if the existing infrastructure can meet required levels of availability.

NETWORK ASSESSMENT

It's not enough to know all the pieces of the network. IT managers also need knowledge of how all the components fit together. A network assessment is designed to obtain a

detailed map of the LAN and WAN environment. The assessment should take into consideration the following factors:

- Current applications and data on the network, such as Voice over Internet Protocol (VoIP), e-mail, Structured Query Language (SQL), Common Internet File System (CIFS), Internet and video on demand
- Current network topology, including but not limited to network devices, physical and logical links, external connections, frame types, routed and routing protocols, application-specific protocols and IP addressing schemes
- Traffic and network utilization analysis

Many tools exist to facilitate network assessment. These range from basic device information output tools that display network device utilization to third-party tools.

For example, within Cisco Systems devices, one can view interface statistics, CPU and memory utilization, NetFlow and application flows using Network-Based Application Recognition (NBAR). Third-party tools that monitor networks, sniffers and Simple Network Management Protocol (SNMP) tools can also be used.

Another option is to get assistance from a third party. Technology experts can conduct onsite evaluations of a network, assessing installation standards, equipment, deployment, current maintenance programs and system capacity. This assessment can also determine whether the most suitable design elements are in place for maximum facility reliability.

The results of your network assessment should highlight any critical network issues that must be addressed, as well as forecast possible problems and risks. The assessment should also suggest remediation plans and position the network to seamlessly handle tomorrow's needs.

NETWORK DESIGN

After the requirements, audit and assessment are complete, the planning and strategizing phase can begin. Here IT managers go to work creating a new network configuration and identify what new network components, load balancing software and management and monitoring software will be needed. This is also an area where help from a third-party consultant may prove beneficial.

The network design must incorporate all gathered information concerning operations and technical requirements. The design should also include specifications for availability, reliability, security, scalability and performance.

Network engineers typically recommend designing a network in modules. Modules allow a business to provide the highest degree of reliability by segmenting traffic and preventing a single point of failure.

Whatever topology is chosen, it's crucial to eliminate single points of failure. This can be achieved by creating redundant links to critical servers and network devices. But redundant links can also create challenges.

For example, in Layer 2 switched environments, redundant links can cause switches to flood packets throughout the network. This can effectively halt the switching of production traffic.

Spanning Tree Protocol (STP) is a Layer 2 protocol designed to prevent such flooding by placing one of the redundant links in a blocking state. Although STP prevents Layer 2 loops, it's slow to converge. STP improvements such as Rapid STP help decrease the convergence time.

At Layer 3, advanced routing protocols enable the highest level of network resilience when using redundant links. Not only can advanced protocols load balance traffic over redundant links, but they can converge in a matter of seconds in the event of a primary link failure.

Aggregate redundant links at Layers 2 and 3 are a common best practice to increase resiliency. Technologies such as EtherChannel combine switched or routed links into one logical link, effectively doubling bandwidth on the link and minimizing convergence.

The switch or router sees aggregated links as a single link. Therefore, traffic continues to flow through the other links if one of the links fails.

It's a fine balancing act: Too few network connections can create single points of failure or choke traffic. While too many can increase complexity and hinder management.

Complete redundancy is expensive. So the goal is to strike that balance between redundancy and cost considerations.

Be sure to document the design phase to demonstrate how the proposed solution meets company needs. Network emulation tools can offer an idea of how the design would perform in a real-world environment.

CONNECTIONS

In adapting network design to increase reliability, it makes sense to review voice and data plans and any relationships with voice and data providers. Take the opportunity to scrutinize price, support, performance and usage agreements.

Your network assessment will have revealed the number and types of voice and data connections in use and the recovery methods. In many cases, carrier dependency is a firm's greatest vulnerability.

Map and study usage patterns to be sure that different paths

Network Availability Options

Availability is often noted as a percentage of uptime in a given year. The table below identifies the downtime allowed for a particular percentage of availability, presuming that the system is required to operate continuously.

Uptime	Nines	Yearly Downtime Per Year
99.9999%	Six	32 seconds
99.999%	Five	5 minutes, 15 seconds
99.99%	Four	52 minutes, 36 seconds
99.9%	Three	8 hours, 46 minutes
99.0%	Two	87 hours, 36 minutes
90%	One	36 days, 12 hours

reflect diversity in service providers for redundancy. Confirm, too, that unused connections are still viable. In some cases, service providers or staff may have turned off a circuit after an audit showed lack of usage.

Take the time to review data-service contracts and minimum annual commitments. If usage has been increased during the contract lifecycle, consider negotiating new pricing. But don't focus on rates alone — also examine service levels and find out what new technologies or features are available.

Service Level Agreements (SLAs) are negotiated agreements that should spell out the average anticipated volume of traffic, peak volume of traffic, average response time and maximum response time. The document should also outline penalties for noncompliance, such as billing credits.

Use network management and monitoring tools to track SLAs. Also, document the carrier or service provider's performance and hold vendors to the standards stipulated in the SLA. ◊

Loss Recovery

Despite the best-laid plans for redundancy, a natural disaster or technical failure could take down the network. What follows are some best practices tips for business continuity and disaster recovery.

- **Set recovery objectives.** Establish a Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Consider clustering, host-based replication, storage-based replication and Physical-to-Virtual (P2V) technology.
- **Rethink data storage options.** Focus on a data backup strategy. Consider Storage Area Network (SAN) technology, continuous data protection and tape archiving to improve the organization's ability to access mission-critical data after a disaster. Technologies such as data deduplication and hierarchical storage management help make the most of a storage investment by reducing the data to be stored and choosing lower-cost options when appropriate.
- **Evaluate virtual backup options.** Server virtualization aids recovery. Virtual servers can be more easily moved and restored between production and recovery sites. They also allow for dissimilar as well as less hardware at the disaster recovery site and facilitate easier failover and recovery.
- **Maintain power.** What if power were to go out for more than a few seconds? A combination of Uninterruptible Power Supplies (UPS), power protection and conditioning, and even a generator are key to protecting data and maintaining uptime during a blackout or other power disturbance.

APPLICATION DELIVERY

CHAPTER 3

Bandwidth is a limited resource that organizations must use wisely and judiciously — particularly in environments using UC. However, a growing array of web applications, e-mail attachments and files consume increasingly large volumes of bandwidth that often lead to slowdowns and breakdowns in network performance. This, in turn, can force the enterprise into expensive upgrades.

One of the most effective ways to reduce the cost of IT and supporting services at multiple locations is through server consolidation — especially when it is combined with server virtualization. But this still leaves a nagging problem: How can a business accommodate growth in bandwidth demand while improving service levels and keeping spending down? Moreover, IT must tackle the problem while delivering swifter response times and faster file transfers for users.

The solution is to rely on a combination of tools, including bandwidth management, LAN and WAN optimization, load balancing and application acceleration techniques. Together, these systems and strategies reduce bandwidth demands and improve service levels.

WAN OPTIMIZATION CONTROLLERS

At the center of this approach are WAN Optimization Controllers (WOCs), which use caching techniques to radically improve the speed and efficiency of a network. Because static objects are easiest to cache, the WOC does so automatically.

Essentially, the first time someone in a branch office requests a static object, the WOC passes the request onto the server and, as it delivers this object, the WOC stores a copy of it for reference. Then the next time anyone requests the same object, the WOC intercepts the request and sends the stored version. This approach greatly reduces transmission time and eliminates latency across a network.

The primary way WOCs reduce bandwidth is through a technique called dictionary compression, which compresses files by a factor of 10 to 30. Dictionary compression automatically monitors traffic flow while learning data patterns and storing them for future reference.

When it sees a pattern that it has learned, it substitutes a reference number for the actual data string. Then a WOC on the receiving end, which stores the same data sets, automatically substitutes the reference number for the original data.

The first time a file is sent across the network there are no incremental efficiencies because both WOCs must learn the data pattern. However, future exchanges are simplified and, if there's a change in a file, only the changes are forwarded to other WOCs along with the reference numbers for unchanged patterns. In addition, the WOC optimizes application protocols such as CIFS.

DEPLOYING WOC

Simply buying a WOC and switching it on does not guarantee outstanding results. Here are some best practices that help get the most from a WOC deployment:

Know what's on network. The first step in reducing bandwidth and providing better service is to understand what

data flows over the network. Optimizing and automating inefficiency is a losing proposition.

Companies that know how much and what type of nonessential traffic travels across the network are better positioned to engineer the network — and WOCs — for maximum efficiency. Yet it is also important that any monitoring tool updates its list of apps regularly. Without constant updates, a WOC's monitoring program lumps unknown apps into a common bucket and performance takes a significant hit as all applications are treated equally.

Apply QoS. Quality of Service controls are essential. They ensure that mission-critical traffic receives priority attention and routine traffic doesn't devour a disproportionate amount of bandwidth. IT can implement QoS at the router level, the WOC level or both.

The biggest obstacle to implementing QoS is defining it and developing a clear set of guidelines and requirements. A WOC should allow IT administrators to set up QoS based on results from monitoring. It should provide default settings for most applications, and it must interface with existing QoS policies.

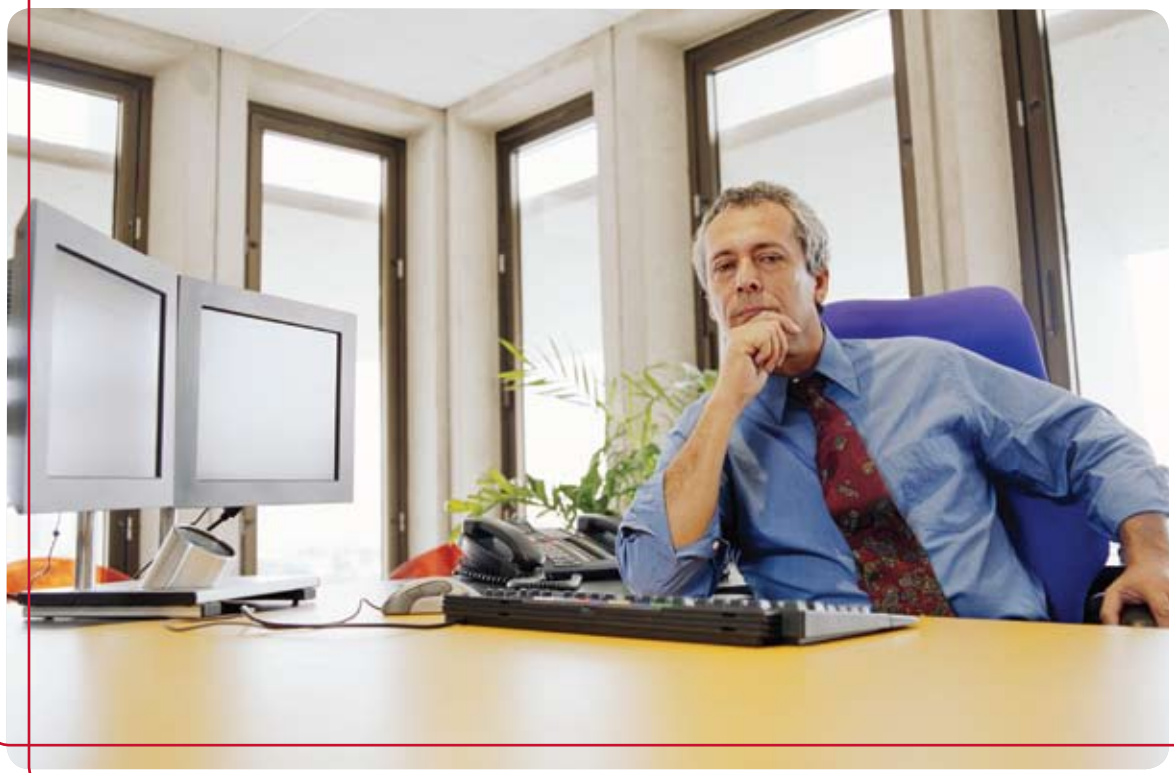
Set bandwidth parameters. It's vital to know how much bandwidth each app should receive. WOC bandwidth management lets network administrators set controls based on these parameters. This guarantees that less critical traffic doesn't crowd out critical apps. It also provides a way for a firm to prioritize traffic based on QoS policies.

For example, effective bandwidth management will ensure that non-essential website browsing doesn't affect critical applications. An organization can even adjust bandwidth based on the time of day and specific activities that occur at certain times, such as the crush for e-mail in the morning when employees first arrive at the office.

Decide what to optimize. Although WOC offers tremendous advantages, it's wise to steer clear of the temptation to switch it on for all traffic. The technology works best for file transfers, web traffic and most essential traffic.

Keep in mind, WOC can actually undermine performance in niche areas. For instance, any attempt to optimize VoIP traffic will result in a slow down and provide little or no benefit.

Likewise, Transmission Control Protocol/Internet Protocol (TCP/IP) optimization can help video traffic. However, running it through dictionary compression provides no benefit and can actually degrade WOC performance.



Plan for encrypted files. WOCs aren't particularly effective for handling encrypted data. Typically, they overcome the problem of dealing with Secure Sockets Layer (SSL) traffic by learning the keys and decrypting the data, and then re-encrypting it before sending it back out on the network.

How WOCs learn and store encryption keys varies from product to product. It is something network managers need to understand up front. In fact, decryption is crucial. Without it, a WOC's benefits are severely limited.

Ready a monitoring strategy. One of the ways WOCs optimize data flow is by collecting all the packets between the central WOC and the branch office device within a single connection — and then hiding the individual connections. Because the data residing in the packets is replaced with reference numbers, deep packet inspection of application data becomes impossible.

This situation can cause issues if security and monitoring devices are placed on the network after the WOC is created. One solution is simply to put security and monitoring equipment in place before the WOC is switched on. Additionally, WOC manufacturers offer techniques to mitigate connection problems. However, an IT team must understand how these processes work and what pros and cons exist for particular scenarios.

Involve the security group. Not surprisingly, security is a key consideration in any WOC deployment. Furthermore, the implementation and integration process must involve the security team. There are several areas of concern, including decryption, hidden individual connections and changes that occur in the data packet.

If hackers gain access to the dictionary compression database, they might be able to reconstruct files and steal data. Although technical solutions exist for these issues, the IT security staff can ensure that there's an optimal balance between practical requirements and protection. They can also eliminate things falling between cracks and silos that may lead to risk.

LOAD BALANCING: OPTIMIZING DATA DELIVERY

As businesses move to centralized data centers and support critical applications across LANs and WANs, they must find a way to balance application loads. At the same time, they must offload key application-level functions from overburdened servers, like security, SSL encryption and content switching.

Load balancing helps facilitate greater data center efficiency. It is available in both hardware and software solutions. Simply put, it divides the amount of work a server must handle across two or more machines.

And because it balances out the overall load and maximizes data center resource utilization, the enterprise reduces bottlenecks on the network and end users have a faster computing experience. In addition, load balancing offers high availability with failover.

In many instances, organizations use load balancing to provide a single Internet service from multiple servers. These server farms offer support for heavily trafficked websites and high-bandwidth File Transfer Protocol (FTP) sites.

Many newer load-balancing appliances offer additional value, including the ability to examine network traffic, detect performance and security problems, and reduce bandwidth expenses. Key features include:

- **SSL Encryption Termination.** Rather than forcing the application server to deal with the overhead of terminating SSL encryption, most load balancers can offload such tasks, freeing up the application server to do what it does best: serve applications.
- **Compression.** Load balancers save on bandwidth by ensuring that traffic loads are distributed evenly among back-end servers. However, they can also perform significant bandwidth savings duties such as compression and traffic shaping.
- **Content switching.** Another key security feature that some products offer is content switching. In this case, the load balancer filters packets for specific data strings, such as credit card numbers or Social Security numbers, and ensures they are blocked before being carried across the WAN. This helps prevent data leakage.

GETTING THE MOST OUT OF A NETWORK

Performance over LANs and WANs is crucial, and the tools aren't limited to WOCs and load balancing. Another valuable tool is the Application Delivery Controller (ADC). This network device handles tasks that typically take place on websites in order to lighten the load on web servers. In many cases, ADC solutions also provide load balancing.

In fact, some view ADCs as the next generation of load balancers because it offers advanced features such as content manipulation, advanced routing strategies and highly configurable server health monitoring. ADCs also provide compression, caching, connection multiplexing, application-layer security, SSL offload and content switching.

Make no mistake; a focused network optimization strategy goes a long way toward achieving the best performance possible. It's a way to enable the network to run at a smooth and optimum level, thereby making the best utilization of resources and allowing maximum productivity. ◊

CONVERGED COMMUNICATIONS MAKES SENSE.

When it comes to implementing a converged communication solution, there are numerous factors to consider, including capabilities, cost and management. Having a trusted partner is essential as you look for the right solutions to meet your requirements.

When working with our customers to help them get all the benefits of converged communications, CDW focuses on three cornerstones: equipment, design and usage. We encourage companies to think about how meeting communication objectives will affect their implementations by asking the following questions:

- "What does my organization need from a converged communications solution, now and in the future?"
- "What new equipment, if any, do I need to meet communication objectives?"
- "How will my business continue to use the solution — and who will support it?"

For VoIP and converged communications solutions, we've got the products. But, more importantly, we've got the answers. Every CDW account manager is backed by a team of dedicated specialists. These certified professionals can help with all stages of your implementation. And our single-source, unbiased approach means that you get the right mix of hardware, software and solutions.

We cover all the bases, providing assessments — either over the phone or onsite — of your current technology assets to ensure that a solution is mapped to your organizational requirements. We help you calculate cost savings and projected ROI. We then help you identify, size and design your implementation, before configuring, testing and installing your solution. Finally, we offer continuous support, following up on the results that you're getting as well as checking in on your evolving needs.

Call your CDW account manager today to learn more about our comprehensive approach to unified communications.

CDW.com/cisco

Cisco® Unified Communications Manager

High-availability server platform for Cisco Unified Communications solutions

CDW 1152554

CALL FOR PRICING

- Comprehensive IP communications system of voice, video, data, and mobility products and applications
- Enables more effective, more secure, more personal communications
- Unified Communications is part of an integrated solution that includes network infrastructure, security, mobility and network management products
- 2RU-high unified communications manager offers tremendous power in a low-profile chassis that minimizes rack space

Cisco Unified IP Phone 7942G

Cisco Unified Communications Solutions unify voice, video, data and mobile applications on fixed and mobile networks

CDW 1300067

CALL FOR PRICING

- Incoming messages are identified and categorized on the display, allowing users to quickly and effectively return calls using direct dial-back capability
- Full-duplex speakerphone with acoustic echo cancellation
- Ready access to missed, received and placed calls (plus intercom history and directories)
- Internal 2-port Cisco Ethernet switch allows for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface

CDW.com/microsoft

Microsoft® Office Communications Server 2007 R2

Microsoft® Office Communications Server 2007 R2 Standard Edition

Delivers streamlined communications

Open License Business[1]

CDW 1677522

$684.99

- Increases productivity with integrated presence and real-time communication to locate people and share information quickly
- With advanced presence technology, Live Communications Server offers instant access to team members, partners, suppliers and customers across multiple geographies, time zones and organizational boundaries
- Builds solutions that are integrated with your existing Microsoft® infrastructure to deliver enterprise-grade security, scalability and manageability

[1]Purchase five licenses OR one processor license to qualify for the Microsoft Open License Business program; media must be purchased separately; call your CDW account manager for details

CDW.com/hp

Powerful. Intelligent.

Hard drives sold separately

HP ProLiant DL360 G6 Rack-mount Server

Quad-Core Intel® Xeon® Processor X5550 (2.66GHz)

CDW 1723407

$3159.00[2]

HP SMART BUY

$543 SAVINGS

[2]HP Smart Buy savings reflected in the advertised price; savings is based on a comparison of the HP Smart Buy versus the standard list price of an identical product; savings may vary based on channel and/or direct standard pricing

Unified Communication Health Check

CALL YOUR CDW ACCOUNT MANAGER FOR DETAILS

CDW Technology Services, a Cisco Systems Gold Partner with a Master Specialization in Unified Communications, offers consultation services to perform a quick and easy Unified Communications Health Check. In a one- or two-week process, an expert CDW engineer will:

- Review the existing configuration of each component of your UC infrastructure, e.g., CallManager, Unity, and your underlying network
- Explore current issues you may be experiencing through discussions with your staff and targeted network monitoring
- Deliver a document outlining our recommendations to improve the functionality, stability and performance of your solution, including a plan to mitigate risk and downtime in migrating to a new solution (as applicable)

TRIM DOWN
THE UC WAY

Save time and money by converging data, voice and video over one network. Carrying communications over the IP network allows businesses to consolidate separate PBX and TCP/IP networks, which comes with operational advantages. Voicemail, e-mail and text messages can all collect in a single inbox. Call centers can access records along with calls. And video conference participants can benefit from face-to-face communications.

Five ways a unified communications solution will help you reduce costs and tighten your belt include:

1. Cutting Conferencing Costs

By bringing conferencing capabilities in-house, firms can expect to save a minimum of 20 percent per year on conferencing costs, according to the tech market analyst firm Forrester Research.

2. Avoiding Long-Distance Telephony Costs

By switching from a traditional PBX system to VoIP, organizations can not only cut down or completely eliminate long distance and toll charges, they can also save money when it's time to restructure or expand.

3. Shrinking Your Travel Expenses

The average domestic business trip costs $1,002. The average international business trip costs $3,542. If you can eliminate even a few of these trips per year by utilizing web or video conferencing, the savings add up quickly.

4. Cutting Back on Training Expenses

Advanced conferencing capabilities allow workers to be trained where they sit, which means no more expensive travel to central training facilities.

5. Decreasing Staff Downtime

Since workers can be reached more easily and travel delays quickly become a thing of history books, project approvals happen much more quickly.

Call your CDW account manager today to learn more about how unified communications solutions can help your organization save money.

AVAYA Gold BUSINESS PARTNER

CDW.com/avaya

Avaya 9620 IP Telephone

CDW 1010566

CALL FOR PRICING

The 9620 IP Telephone features an intuitive interface with a bright backlit display and several LED lights and buttons to explicitly convey status to the end user. It also provides flexible support for add-ons in the future, all within a very stylish and professional design.

- Enhanced productivity of users through prompting for common telephony tasks
- More effective conference calls due to less reiteration because of the high-fidelity audio capabilities
- Provides investment protection — built on open standards with a modular platform that supports a wide range of modules and adapters

Avaya G350 Media Gateway

CDW 1046370

CALL FOR PRICING

The G350 Media Gateway is a powerful converged networking solution that packs an IP telephony gateway, an advanced IP WAN router, a VPN Gateway and a high-performance LAN switch into a compact (3U) modular chassis.

- Designed to be a complete voice/data networking solution
- Ideally suited for enterprises with distributed branch office locations using 8-72 extensions
- Advanced TDM/IP architecture provides seamless connectivity and communications between a wide variety of analog, digital, H.323 and SIP-based telephony devices and applications
- Secures VoIP media streams using Advanced Encryption Standard (AES)

Microsoft

CDW.com/microsoft

NEW version

Microsoft® Exchange Server 2010

Microsoft® Exchange Server 2010

Achieve new levels of reliability and performance

Open License Business[1]

CDW 1911935

$684.99

The latest release of Exchange can help you achieve better business outcomes while controlling the costs of deployment, administration and compliance. Exchange delivers a wide range of deployment options, integrated information leakage protection, and advanced compliance capabilities, that combine to form one of the best messaging and collaboration solutions available.

- Lower IT costs with a flexible and reliable platform
- Delight users with anywhere access to communications
- Manage risk with protection and compliance capabilities

[1]Purchase five licenses OR one processor license to qualify for the Microsoft Open License Business program; media must be purchased separately; call your CDW account manager for details

hp invent

CDW.com/hp

HP ProLiant DL380 G6 Rack-mount Server

Two Quad-Core Intel® Xeon® Processors E5540 (2.53GHz)

CDW 1723415

$4399.00[2]

Hard drives sold separately

HP SMART BUY

$812 SAVINGS

intel Xeon inside™

Powerful. Intelligent.

[2]HP Smart Buy savings reflected in the price; savings is based on a comparison of the HP Smart Buy versus the standard list price of an identical product; savings may vary based on channel and/or direct standard pricing

CALL YOUR CDW ACCOUNT MANAGER FOR DETAILS.

Exchange Deployment Planning Services

Cutomers with Deployment Planning Services benefits under their Software Assurance program may be eligible for 1, 3, 5, 10 or 15 days in services credit towards Exchange Server 2010 and Office Communications Server 2007 R2 planning and design engagements or a Business Value Assessment to develop an ROI around the adoption of Microsoft Unified Communications.

DIAL UP

THE PRODUCTIVITY OF YOUR MEETINGS.

Does your conference room inspire collaboration and accomplishment?

Does your outdated equipment allow your people to maximize their efficiency?

Are you getting the most out of every one of your meetings?

As businesses look for ways to reduce operating expenses, video conferencing presents an increasingly affordable alternative to costly travel. Video conferencing provides real-time, face-to-face collaboration with clients, partners, contractors and employees over a broadband network. Video conferencing increases employee efficiency, as travelers are no longer forced to endure flights without Internet access, as well as long airport delays that sap productivity. Furthermore, the increased affordability of teleconferencing puts it well within reach of companies that thought it was outside of their budget.

Video Conferencing Systems Have Come A Long Way

In the past, video conference systems have been notoriously cumbersome to connect and use on a reliable basis. Additionally, today's communications users have become accustomed to simple yet powerful communication channels such as e-mail, phones, PDAs, instant messaging and much more. They expect video to be added to their daily options, but they require a similar level of user simplicity.

Easy To Use

Today's video conferencing solutions let you make the process as simple and seamless as placing a phone call or clicking a mouse. By taking the technical complexities out of the process, you can better meet the objectives of the end user.

Clear, Reliable Sound

Audio is often an overlooked aspect of the video conferencing experience. It is critical that organizations recognize how important acoustic quality is to the overall perception of the experience itself. Good acoustic quality lends credibility and effectiveness to the experience. Today's solutions let you pick up voices and other relevant audio signals with great clarity while eliminating irrelevant background noise.

Superior Picture Quality

Seeing is believing. Today's high-definition solutions give you a crisp, clear picture and video resolution that generates a true-to-life experience — letting you see facial expressions and body language clearly.

Talk to your CDW account manager today to learn more about video conferencing solutions and the productivity advantages they can deliver to your firm.

POLYCOM CDW.com/polycom

Polycom® HDX 7002™

For organizations that place importance on having beneficial meetings and communications that allow their team members to make educated and informed decisions

CDW 1387354

CALL FOR PRICING

- Data Compression Protocol is H.263++, H.264, H.261
- HD detail on content such as diagrams, project plans, multimedia presentations and more
- Utilizes features such as Polycom® HD Voice technology to deliver patented, crystal clear audio
- Polycom StereoSurround™ audio to separate room sounds into left and right channels to deliver physical sense spatiality to opposite-end participants

Polycom CX5000

Easily add group video collaboration to Microsoft® Office Live Meeting 2007 and Microsoft Office Communications Server 2007

CDW 1726377

CALL FOR PRICING

- Delivers a unique, engaging 360° group video experience
- Brings video, voice and content together in one seamless interactive session
- Advanced technology automatically changes the camera view so that the active speaker can always be identified, allowing participants to easily track the flow of conversation
- Easy to deploy — even remote offices or businesses with limited IT support can easily set up and configure the device

CDW.com/hp

Powerful. Intelligent.

Hard drives and blade chassis sold separately

HP Compaq Business Desktop 7000

Intel® Core™ i7 Processor 860 (2.80GHz)

CDW 1870917

$899.99[1]

HP SMART BUY

- Memory: 4GB
- 500GB hard drive
- DVD±RW
- Windows® 7 Professional

HP ProLiant BL490c G6 Blade Server

Quad-Core Intel® Xeon® Processor X5570 (2.93GHz)

CDW 1723369

$4013.99

- Memory: 6GB std., 192GB max. (PC3-8500R DDR3)
- Hard drives: none ship std.; up to two drive bays available

[1]HP Smart Buy savings reflected in advertised price; HP Smart Buy savings is based on a comparison of the HP Smart Buy price versus the standard list price of an identical product; savings may vary based on channel and/or direct standard pricing

Microsoft

CDW.com/microsoft

Microsoft HD LifeCam Cinema™

Notebook or desktop HD webcam

CDW 1838192

$69.99

- 720p HD widescreen
- Auto focus
- Digital microphone
- Works with Windows Live, Yahoo! Messenger, AOL Instant Messenger and Skype
- Mac®, PC compatible

CALL YOUR CDW ACCOUNT MANAGER TODAY

The CDW Technology Services team has a range of pre-sales services, including:

- Network assessments
- Design sessions
- Strategy planning sessions

The CDW Technology Services team also provides implementation and support services for unified communication solutions. With our proven methodology and operations, we can provide the most value when engaged in the beginning stages of a unified communication project.

VIDEO CONFERENCING

A KEY COMPONENT

OF A UNIFIED COMMUNICATIONS STRATEGY

In today's fast-moving global economy, project teams, partners and colleagues are distributed around the world. Frequent face-to-face meetings and meaningful dialogue are vital for success, but travel is expensive and time consuming. Traditional video conferencing systems have provided organizations with the ability to meet face-to-face — but for most people the quality of the interactions has been tolerable, but not always as enjoyable or as productive as an in-person meeting.

In many cases, the overall quality of the video was poor, the sound was hard to hear and the systems were cumbersome and difficult to use. The good news is video conferencing technology has reached levels that simply weren't possible a few years ago. It's now possible to provide a high-quality, high-definition visual experience in a cost-effective way.

It's easy to calculate the cost savings from implementing a video conferencing solution. Calculate the number of trips taken annually, multiply that by the cost (transportation to and from the airport, airfare, per diem, salary of time lost in traveling) versus the investment of the video conferencing solution (equipment, service, training, network). Cost savings made possible by IP communications can be so great that most businesses see a return on their investment in as little as four to 12 months.

In the future, global and decentralized organizations will increasingly rely on video communications and other rich-media collaboration to meet their objectives. However, the productivity of the interactive video experience is only as good as the technology behind it.

Getting Started with Conferencing and Collaboration

Your CDW account manager and certified unified communications specialists are ready to assist you with every phase of choosing and leveraging the right conferencing and collaboration solution for your IT environment.

Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- Detailed vendor evaluations and recommendations
- An assessment review of your existing environment, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- 24x7 telephone support as well as ongoing product lifecycle support

Contact your Account Manager or CDW Specialist today.

LifeSize® CDW.com/lifesize

LifeSize® Team 200™

Feature-rich, high-definition (HD) video

CDW 1658987

CALL FOR PRICING

- HD telepresence-quality video at 1280x720 resolution at 30 fps
- Four-way HD continuous presence (CP) multipoint conference with Virtual Multiway allows participant viewing control (patent pending)
- Support for single- or dual-monitor displays
- Support for video bandwidth from 128Kbps up to 4Mbps
- Standards-based support for H.261, H.263, H.263+, H.264 and H.239 compliant

lenovo CDW.com/lenovo

Lenovo ThinkCentre® M58e

ENERGY STAR® 4.0 compliance

CDW 1920740

$808.99

- Intel® Core™2 Duo Processor E8400 (3GHz)
- Memory: 2GB
- 320GB hard drive
- DVD-Writer
- Windows® 7 Professional

Monitor sold separately

Microsoft CDW.com/microsoft

Microsoft® LifeCam VX-3000

Desktop web camera

CDW 1025628

$23.99

- HD still (1.3 megapixels interpolated) photography
- Brilliant video (640x480 pixels)
- Built-in unidirectional noise-canceling microphone
- Fully integrates with the Microsoft® Windows Live Messenger to deliver a suite of market-first features that make web video calling a breeze

PLANTRONICS SOUND INNOVATION CDW.com/plantronics

Plantronics® Savi™ Office WO100

Wireless DECT 6.0 headset

CDW 1719435

$276.99

- Work smarter — switch and mix audio between PC and desk phone with one headset
- Integrates your PC and desk phone, providing hands-free communications for conference calls
- Premium PC audio with improved call clarity and lifelike fidelity with wideband PC audio — hear your conversations clearly every time

Wireline Services

CALL YOUR CDW ACCOUNT MANAGER TODAY

CDW's Voice and Data Specialists are here to help define and scope your needs along with connecting you to a provider that can meet your requirements both domestically and internationally. Our experienced carrier service specialists are up to date on the latest technologies and trends and have the knowledge and experience to make solid recommendations based on your business needs.

In addition, we will help navigate the matrix of vendor plans and assist you in negotiating your service agreements to ensure you receive the optimal level of service at the best price with all of our top providers, including AT&T, Sprint, Global Crossing, Qwest, XO, Verizon, Bandwidth.com, New Edge, Time Warner, Cbeyond, Level 3 and more.

NETWORKING MADE EASY

Does your network need work? Perhaps you want to upgrade your current networking hardware. Or you need a way to reduce bandwidth between your locations. Or you want to offer remote access to all your staff. Whatever the task, CDW can help.

Our certified networking specialists look at the lifeblood of your IT infrastructure — your network — its traffic, speed, reliability and manageability. As you add staff and applications, and the hardware to run it, from software to servers to notebooks, CDW can help handle the increased demand for network bandwidth.

WHAT YOU GET

- Expert consultation regarding Layer 2, 3 and 4-7 switching
- Application delivery solutions and support
- Wireless network infrastructure expertise
- Network installation and deployment
- Network analysis, monitoring, configuration and management
- CDW's award-winning technical support

SPECIALIST AREAS

Networking (LAN/WAN)

Telephony
Security
Power
Mobile Wireless
Server/Storage
Software
Voice and Data
Services
Desktop
Notebook

We're only a phone call away.

Call your dedicated account manager to connect with any of our technology specialists.

The Right Technology. Right Away.® • CDW.com • 800.808.4239

UNIFIED COMMUNICATIONS

CHAPTER 4:

UC Redefines the Enterprise

Core Capabilities

A More Efficient Network

It's no secret that computer networking is constantly evolving and continually redefining the way business gets done. Yet one of the most significant changes over the past few years is the adoption of UC technologies.

UC includes a broad range of technologies encompassing converged networks; simple IP telephone and messaging systems; IP-based systems that fuse voice, data and video platforms; and communication and collaboration applications.

Unified communications is changing the way businesses act and interact. It is simplifying network administration, cutting costs and providing an array of capabilities that weren't possible only a few years ago.

Generally, UC offers four core capabilities, combined in some fashion to meet the specific needs of the enterprise: Telephony and VoIP, Messaging and Presence, Conferencing and Collaboration, and Call Center Management.

TELEPHONY AND VoIP

IP telephony provides smarter and more efficient ways to initiate and receive calls, including the ability to route calls to a person or device regardless of location. It also provides computer-telephony integration so that contacts and notes pop up when a person calls, or an individual can click on a contact or phone number in an e-mail and dial.

These features are also valuable as employees seek telephony and other solutions that work across notebook computers, netbooks, smartphones, Portable Digital Assistants (PDAs) and other wireless devices. Increasingly, they want to manage communications across different phone numbers, voice mailboxes and e-mail accounts. UC routes calls automatically to the right device at the right time.

What's more, IP telephony can be less expensive and far more efficient than conventional telephony. Consider that in today's mobile environment, the ability to connect to the right person depends not only on being able to view their availability, but also discerning what device they're using.

By extending the UC network to devices outside the formal network (such as mobile phones, home office phones or two-way devices), users can establish connectivity methods based on personal convenience and preference. This makes it possible to communicate via preferred method whether at home, at work or on the road.

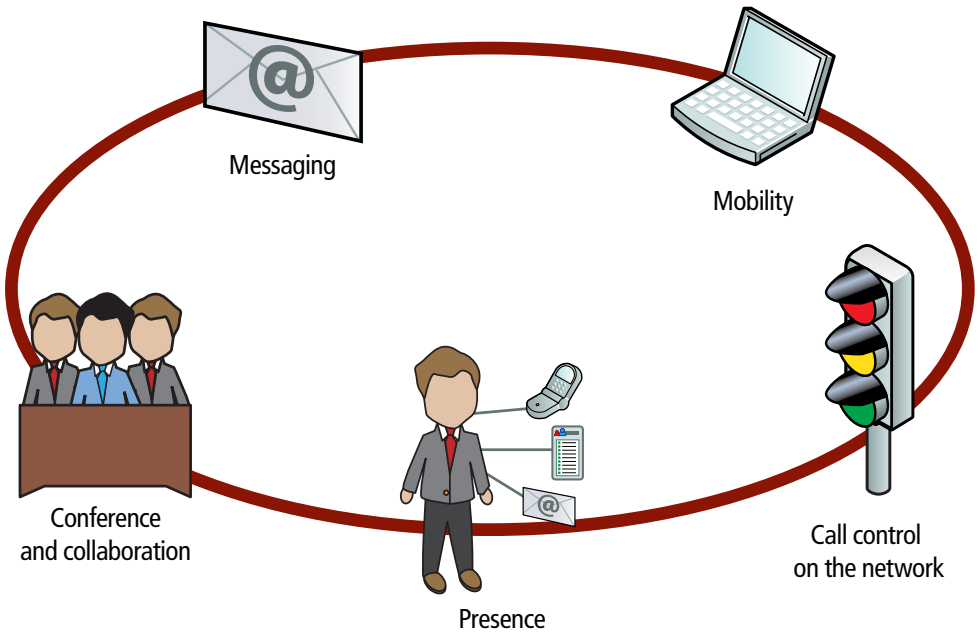
An added benefit of UC is that it provides single-number reach technology. This feature allows users to consolidate multiple calling paths and devices within a single IP phone number. Organizations wind up with enhanced responsiveness, and workers no longer find it necessary to share private mobile phone numbers.

Single-number reach also allows mobile workers to manage all their voicemail messages within a single voicemail system. If the recipient doesn't pick up the call on a mobile line, the unanswered call is stored in the centralized UC voice messaging system or another designated voicemail system.

Finally, IP telephony provides far greater flexibility for everyone. An individual can answer a call on a mobile device and then seamlessly move the call to a physical desk phone upon physically

CORE UNIFIED COMMUNICATIONS CAPABILITIES

UC functionality is designed to reduce costs, boost productivity and enhance customer relations while improving mobility and home office options.



entering the office — or vice versa. This feature eliminates the need to hang up and redial a call already in session.

MESSAGING AND PRESENCE

This technology removes physical barriers to effective communication. It enables the sharing of information between individuals and devices using various communication methods, including voice, e-mail, unified messaging and instant messaging.

Today's messaging technology creates the possibility of real-time, text-based communication between two or more participants via the Internet or an internal network. What separates Instant Messaging (IM) from technologies such as e-mail is the perceived synchronicity of user communication.

Moreover, many IM services offer additional features. These can include such things as immediate receipt of an acknowledgment or reply, group chatting, conversation logging, file transfers and conferencing services.

UC offers the added advantage of providing "presence," which allows network users to see others currently on the same network or system. If a user is actively using e-mail, instant messaging or video conferencing capabilities, then a "buddy list" can notify other users regarding this person's status and availability.

The information is used to provide status for coworkers and facilitate presence-enabled communications between them. This scalable and easy-to-manage solution provides:

- **Enhanced collaboration.** Staff can share availability information and instant messages with coworkers and others.
- **Streamlined communications.** Users can view the telephony status of their coworkers and click from a PC to call them.
- **Leverage presence-enabled operations applications.** Workers can share presence information and user communications capabilities in web directories and management systems.
- **Improved first-call resolution and end-user satisfaction.** An organization can route calls to staff or outside consultants with the appropriate level of expertise.
- **Increased productivity.** Employees and others are able to connect with colleagues on the first try because they can see their availability in advance. This reduces missed phone calls and voicemail messages. Industry studies show that the ability to view the availability status and the preferred communication methods of coworkers trims "wasted time" by one-third or more.

CONFERENCING AND COLLABORATION

This technology provides a more effective and productive means of interacting with others through a combination of methods, including audio, web and video applications. These interactions can take place on an impromptu and real-time basis — without regard to time zones or locations.

Conferencing and collaboration applications provide advanced capabilities that enrich an organization's operations. They take advantage of converged networks and allow coworkers to interact more effectively. This, in turn, reduces costs and increases productivity across an enterprise.

Geography and time zones become largely irrelevant with the use of conferencing technologies. They connect people seamlessly through voice, web and video services and enable real-time document sharing and collaboration. Team members can view and markup documents in real time, view presentations, and use whiteboards and other tools to create new files, spreadsheets and documents.

Conferencing applications are flexible enough to handle one-on-one meetings or large conference calls. Collaboration technology permits the sharing of specific documents, computer desktops and applications.

Audio conferencing enables staff to conduct meetings more conveniently and efficiently. It offers one of the easiest ways to communicate with a group of participants, in different locations, at the same time. Typically available via service providers, audio conferencing solutions vary in the capabilities provided as well as cost structures.

Web conferencing solutions are designed to conduct webinars, presentations or meetings over the web. Participants typically sit at their own computers and are connected with other participants. Web conferencing solutions providers vary by the multimedia features and management tools offered.

Consequently, business and IT leaders from a wide range of industries — including medicine, law, accounting, manufacturing, finance and retail — are turning to conferencing applications to solve a variety of challenges. Some of the benefits include:

- Enhanced innovation
- Increased efficiency and less wasted time
- Making projects and resources seamlessly available to multiple participants
- Eliminating the need to pass a project back and forth between multiple stakeholders, thus risking misunderstandings and errors

Video conferencing is at the center of this trend. In the past, proprietary systems and a lack of standards made video conferencing a "hit or miss" proposition.

Today IP has created a standards-based platform offering outstanding performance at an extremely low price. Consequently, a wide range of industries are turning to a variety of solutions including:

- Desktop video conferencing systems for peer-to-peer contact
- Multisite connections (also known as room-to-room)
- High-end telepresence systems that deliver high-definition and in lifelike images

This combination of tools makes video conferencing technology ideal for everything from routine desktop phone calls to board meetings, high-end presentations and speaking engagements.

To be sure, video conferencing extends a company's reach and adds a dimension that isn't possible via e-mail and a phone. It also allows remote workers to maintain viable, productive relationships that simply aren't possible through audio-only teleconferencing.

The result: Organizations reduce travel expenses and carbon footprint while creating new ways to share information and interact.

Deploying video communications, as part of a conferencing solution, is now as straightforward as switching on a traditional voice service. With the addition of video-capable phones and desktop cameras, it's possible to initiate calls to anyone else with service by simply clicking a button.

CALL CENTER MANAGEMENT

UC is also changing the contact center and ushering in a new era of productivity for the enterprise. Call center management leverages telephony applications, messaging technology and customer databases into an efficient, unified system.

Voice, iChat, e-mail, instant messaging, Customer Relationship Management (CRM) tools, web collaboration and other tools join together to provide the best possible communications experience for your customers.

Call center management solutions can instantly provide employees with resources to deliver a higher level of customer service. They can quickly find answers to inquiries and connect with subject matter experts without having to put customers on hold or transfer them to another department.

Ultimately, UC provides more sophisticated traffic handling and communications management features within a network. It also makes it possible to tap into skills-based contact routing, voice self-service, computer telephony integration and multichannel contact management.

By combining automatic-call-distributor functions with IP

telephony in a single, unified solution, a contact center can avoid long waits for customers and rapidly deploy a distributed VoIP contact center infrastructure. Contact center technology lets organizations segment callers, monitor resource availability and route each customer to the most appropriate resource in the organization.

It also enables smart transfers. An agent can escalate a call or send it to a specialist, and customer notes or account information move with the call.

A UC-based contact center taps into features that are either usavailable or difficult to integrate under conventional telephony. These include: caller ID, caller-entered digits, web-form submitted data and caller database information.

With the right set of rules and user-defined scripts, this makes it simple to route inquiries correctly and provide tiered service levels. Yet it also monitors available resources and adjusts call routing and other activities based on a caller's needs, current staffing skills and availability, Interactive-Voice-Response (IVR) status and queue lengths.

A UC-based contact center is more than a way to manage phone traffic effectively. Because the environment uses IP technology, it incorporates multichannel features such as web chat, e-mail, click-to-contact, screen sharing and even remote desktop computer support and diagnostics. These features allow a customer and agent to interact in a way that makes sense for them and the specific situation they're dealing with.

A MORE EFFICIENT NETWORK

One of the biggest selling points for UC architecture is that it helps centralize a firm's communications and consolidate its management capabilities. Bringing UC solutions to a centralized and secure environment allows companies to apply rapid changes to the entire company and embrace enhanced security and management.

A centralized solution provides other benefits too. Most importantly, it allows a firm to easily and inexpensively bulk up its communications and collaboration infrastructure with applications such as presence, instant messaging, desktop collaboration and emergency notification.

UC technology offers the ability to establish specific rules for handling and routing calls. This includes: call parking, call forwarding and flexible number assignments, including adds, drops and changes. Moreover, users can plug phones and devices in and UC will route the calls or messages to their current location.

This not only provides unparalleled convenience for users,

but also reduces costs and overhead for IT administrators who can manage one converged network rather than separate voice and data networks. UC also leverages sophisticated contact center features.

Moreover, UC significantly enhances an organization's staffing options. It's possible to allow staffers to connect to the network from anywhere, including home or satellite centers. In fact, a growing number of companies are turning to this approach in order to further reduce costs and provide a more flexible work environment for employees.

With advances in desktop video conferencing, web conferencing and desktop collaboration, a business can provision resources without regard to job function or geographic location. This federated approach to services is a boon for organizations, and it provides a level of flexibility and agility that is paramount in today's ultra-competitive global business environment.

The ability to manage communications and collaboration beyond the four walls of the enterprise means that business and IT leaders can provision resources in a consistent and effective way — based on unique requirements and circumstances. Ultimately, this approach leads to greater ROI.

These days, building an effective UC strategy is about dollars and sense. As organizations look to develop more efficient ways to manage customers and data — and control costs — unified communications is increasingly at the center of the networking universe. ◊

WIRELESS NETWORKING

CHAPTER 5:

The factors leading to wireless LAN rollouts have been years in the making. The year 2010 begins the third decade in which wireless LAN technology has been available.

In the years since the early 1990s when products first hit the market, their benefits have been widely accepted. They free employees, as well as partners and customers visiting a corporate campus, from the tether of a desktop computer or a wired network connection.

They eliminate what is often a costly — and time-consuming — effort to extend network cabling and electricity to individual desktops or hard-to-reach locations. And they help knowledge workers remain productive regardless of where they're sitting.

Of course, the myriad wireless LAN benefits cited above were available before 802.11n. But with the new standard's support for up to 600Mbps, 802.11n products can legitimately rival the performance of wired infrastructure for the first time.

VOICE COMMUNICATIONS

Businesses are looking for ways to tie voice communications into their wireless LANs. This will serve to ensure maximum return on infrastructure investments.

In certain vertical industries, companies are using Wireless LAN (WLAN)-enabled phones to send voice traffic wirelessly within a campus or building. The Wi-Fi handsets liberate users from the constraints of traditional wired handsets. Calls can be made and received anywhere there is a Wi-Fi hotspot.

In addition, companies will perform "dual-mode" communication, whereby a single dual-mode phone can operate over the cellular network as well as the Wi-Fi network. Such phones can pass seamlessly between Wi-Fi and cellular networks so users experience no interruption in service.

Certain industries have already embraced Wi-Fi-enabled voice communication. These include healthcare, retail and manufacturing. In any of these fields, a phone uses the wireless LAN in the same way any other device, such as a notebook computer does.

DESIGNING A WIRELESS NETWORK

The 802.11n wireless networking standard was ratified in 2009. This long-awaited final ratification changed the standard very little from its Draft 2.0 version, meaning that many manufacturers were already incorporating this standard into their product lines.

To maximize wireless network performance, purchase equipment that is compatible with 802.11n. Take note, 802.11n equipment requires a gigabit connection to each AP in order to provide the increased bandwidth offered.

IT managers want to be able to enjoy the performance improvements of up to 600 megabits-per-second throughput and the increased coverage that 802.11n wireless promises. To help get the most out of the wireless standard, consider the following five points:

1. Look for modular access points. Modular products allow for swapping out networking cards to facilitate an easier migration to 802.11n. Keep in mind, the current generation of 802.11n products doesn't yet support the full theoretical potential of 600Mbps speeds. Therefore, you may find yourself upgrading hardware in a few years if the higher speeds are important to your organization.

Most wireless equipment manufacturers offer 802.11 access points that function in several operational modes. The three primary modes include:

- **Mixed mode:** This lets 802.11n devices coexist and interoperate with legacy 802.11a/b/g devices on the same wireless LAN. Most enterprise WLAN equipment will use mixed mode by default to ensure legacy compatibility.
- **Legacy mode:** In this mode, the AP behaves like an 802.11a/b/g device. However, because it uses some of the 802.11n physical layer enhancements, performance is improved. This configuration could be used when an enterprise includes new 802.11n APs, but is not yet ready to enable full 802.11n operation.
- **802.11n mode:** Some manufacturers' access points can be configured to accept association requests only from other 802.11n devices. IT departments may choose this configuration to achieve the best possible throughput.

2. Check to see if your wireless access points require more than 15.4 watts. Most Power over Ethernet (PoE) switches support the 802.3af standard. Therefore, they can supply a theoretical maximum of 15.4 watts of power to PoE-capable devices.

After losses from cabling and power supplies, however, the real power output may be closer to 12-to-13 watts. Note: A new, recently ratified standard, 802.3at, promises to supply up to 24 watts.

Power requirements of 802.11n access points vary. Some manufacturers require more than 15.4 watts. Others claim to work within the current standard. When using APs that claim to work with standard 802.3af power, be sure to understand exactly how much power the AP requires and how it behaves if it gets less than that.

3. Consider how aesthetic concerns may affect performance. Wireless gear used to be fairly simple, with a single antenna or two at most. Today, some of the newer products feature as many as six antennas.

This may sound like a nonissue. However, some devices may be considered unsightly when positioned within the confines of a well-appointed building interior.

One solution is to hide APs in a drop ceiling. However, be mindful of double checking AP performance in this scenario.

4. Understand potential network design issues. There has been debate for the past few years over whether an 802.11x wireless network should be based on stand-alone "thick" or "thin" APs powered by a central controller.

The earliest wireless networks were primarily thick, meaning that most of the intelligence resided in each access point. As wireless networks expanded, the industry moved toward a thin model where all the intelligence resides in centralized controllers.

Currently, there's some concern that with the increased throughput of the 802.11n standard, the centralized controllers (and the uplinks to them) won't be able to handle all the traffic. Whether or not this is a network issue will depend on deployment size, the location of controllers and the usage patterns.

5. Focus on spectrum and channel planning. The growing consensus is that the 5 gigahertz (GHz) spectrum is best for enterprise wireless. This is because it is a much cleaner space than 2.4GHz.

The 802.11n standard allows running either the 2.4GHz or 5GHz space. Therefore, deciding what frequency to use will be based on the firm's need to support the legacy 802.11a/b/g protocols.

Many of the 802.11n APs on the market feature dual radios. These are a good choice — at least for the next few years — because many of the notebooks supported will work only with those legacy standards. If 802.11a is not in full deployment, consider using one radio to run 802.11n in 5GHz and the other to run 802.11b/g in 2.4GHz.

CENTRAL CONTROL

After access points, the second key feature to look for is a wireless controller that allows for central management of the WLAN. This is in contrast to older wireless networks where each access point operated independently and required individual attention with every upgrade or configuration change.

A centralized WLAN controller provides a central repository for all software, configurations and device settings. By automatically performing tasks, such as adjusting access point transmit power settings and communication channels in order to eliminate user connectivity problems, administrators can focus their attention elsewhere, knowing that the wireless network can largely take care of itself.

Controller-based wireless networks offer many additional benefits beyond centralized management. Because near-constant communication occurs between the access points

and the WLAN controller, the controller will also have a view into the wireless space around the entire organization.

Reports and alerts can be generated when threats such as rogue access points or ad hoc computer networks are present. If these entities are deemed to be a threat to the organization, they can be "contained," thereby preventing insecure connections to the LAN and protecting the business. By providing such benefits, a properly deployed WLAN controller can prove a powerful security asset.

CONDUCTING A SITE SURVEY

The purpose of the site survey is to determine coverage areas and locate dead spots in the enterprise facility. A site survey may indicate areas where an additional access point or two may be needed. Even if a WLAN exists, a wireless analysis can improve the network.

Be sure to utilize site survey tools that can handle 802.11n. The 802.11n standard offers much greater coverage than 802.11g and 802.11a standards. Because it achieves this through technologies such as Multiple Input/Multiple Output (MIMO) and channel bonding, it's important that site survey tools understand 802.11n to get an accurate survey.

Active survey products, such as AirMagnet, have been updated to communicate with 802.11n networks. In addition, many wireless manufacturers are in the process of upgrading their predictive survey tools to understand 802.11n.

A workaround, when using an older survey tool, is to do a site survey for 802.11a, which will give you the access point density you need for 802.11n. This makes good sense, especially when supporting legacy protocols. However, when doing a "greenfield" installation with plans to support only 802.11n, a newer site survey tool is best.

There are other tools available for analyzing a wireless network — both free and for purchase. These solutions provide a task-by-task process by which the surveyor studies a facility to understand the Radio Frequency (RF) behavior, RF coverage areas, RF interference and the appropriate placement of wireless devices.

Capacity Planning

When setting up a WLAN, keep in mind the number of users who may be accessing each AP at any one time. Many WLAN access points claim to support a theoretical maximum of 256 clients, but real-world performance is about 10 percent of that, or about 25 clients.

Slow-performing networks are most likely suffering from too few APs. This may be in spite of offering a large coverage area. Having a higher concentration of APs can be beneficial. In the event that one AP fails, others will pick up the slack and increase their broadcast levels to accommodate for the outage. A higher concentration of APs will allow the network administrator some leeway to restart a malfunctioning device.

ENCRYPTION AND AUTHENTICATION

Authentication is the process in which the network grants access to a wireless user. This involves the passing of credentials from the end-user device to the network.

If the user provides the appropriate credentials, the network grants it access. Failure to pass the authentication process results in the network denying the end user a connection.

After the device is connected to the WLAN, encryption serves as the mechanism for hiding and protecting the traffic being exchanged. Encryption translates the traffic into a cipher that only the intended recipient can decode.

When choosing the proper authentication and encryption mechanisms to protect wireless users, first identify all the device types that will utilize the WLAN. Identifying the devices allows defining the security capabilities of each. Some devices support a wide variety of authentication and encryption types; others support a much smaller set.

Also take into account an evaluation of the levels of security required by the company, the sensitivity of different categories of data and the ease of use for end users. You will also want to consider governing body regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act (SOX).

The network's security is strengthened by avoiding the use of static pass phrases or stored passwords. Taking advantage of a Remote Authentication Dial-In User Service (RADIUS) server to dynamically process authentication requests is wise and highly advised. Doing so prevents unwanted devices from connecting and ensures that only approved, valid devices attach to the WLAN.

A RADIUS server processes authentication requests. It either validates a user as authentic and grants access to the network, or denies access because of a failed authentication attempt. These servers can maintain separate user databases for authentication purposes. Or they can tap into another existing user database, such as Microsoft Active Directory.

There are two main types of encryption used on WLANs at present: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP encryption is substantially weaker than WPA. However, depending on what kind of data you are trying to

protect, it may be a good fit. For instance, using WEP to encrypt nonessential data may be appropriate.

Any essential data will benefit from the added strength of WPA encryption. WPA is much stronger and can be managed with randomly changing keys, via the 802.11x standard.

Each time a mobile device changes APs, it has to reauthenticate against the system. In the case of 802.11x, this involves hitting the RADIUS or authentication servers and could cause logon delays. Deciding to go the 802.11x route may require additional logon servers or RADIUS servers to handle the authentication and ensure network performance.

VLANs and Tunneling

Secure guest user access to the Internet is a common requirement for today's WLANs which can drastically increase productivity and effectiveness. Businesses can make such access secure by logically separating the guest user traffic to a segmented Virtual Local Area Network (VLAN) and controlling access via access control lists.

Another increasingly popular method for providing secure guest access involves implementing a guest anchor WLAN controller. This strategy allows tunneling all guest user traffic to a secure location, typically outside of the firewall.

Web pages served by these controllers also allow the firm to restrict access to the guest network. This is done by requiring users to enter a set of credentials into the page before obtaining Internet access.

FAILOVER AND REDUNDANCY

One of the last steps in setting up your WLAN is determining how much redundancy or failover a business needs. Consider purchasing multiple wireless controllers so that if one of them has a problem or needs to be rebooted, interruptions will be kept to a minimum.

Also check to see whether APs can have "master" and "slave" controllers. This will allow them to switch automatically to the controller that is online.

Installing or upgrading a wireless network is a major investment in an organization's infrastructure and shouldn't be taken lightly. Proper planning, equipment selection and implementation will ultimately determine the success or failure of the WLAN. ◊

SECURING
THE NETWORK

CHAPTER 6:

These days, it's impossible to operate a business without paying close attention to network security. It seems security breaches are making new headlines daily. What's more, today's attacks are more targeted against specific industries and enterprises.

As e-mail, documents, database files and other data, information and knowledge travels in and out of an enterprise, the risk of loss grows. A single breakdown or breach can result in significant financial losses, an exodus of customers, and regulatory or legal challenges.

What's more, new business models, embracing the global nature of business, have made businesses more vulnerable to data and identity theft. All of which have made protecting the network and UC environment a substantial task.

Many experts agree that a multilayer approach to security can help to identify, isolate and stop attacks prior to significant damage being done. As a result, network security must be addressed in several ways.

BASIC NETWORK SECURITY

Malware — including viruses, Trojan Horses, rootkits and other threats — has exploded in recent years. Security experts say that more than 1 million computer viruses exist and the number grows daily.

Unfortunately, data theft and destruction is a persistent threat — along with the risk of stolen credit card data, Social Security numbers, passwords and company secrets. Unlike in the past, where hackers looked to have fun or claim fame, today they are looking to make a profit on pilfered data.

Meanwhile, botnets — malware that seizes control of systems and uses them for spamming and Denial-of-Service (DoS) attacks — are exploding. In fact, numerous sources report that as many as 1 million computers worldwide are part of these "zombie" networks.

Also increasing in numbers are SQL injection attacks, a category of vulnerabilities that can afflict web applications. Difficult to detect, these types of attacks can be the cause of disastrous data breaches.

To counter network threats and vulnerabilities, up-to-date antimalware protection on the desktop and the network is essential. It is the first line of defense against viruses and other software threats delivered through e-mail, web pages, USB sticks and other media, and through the network itself.

Increasingly sophisticated hardware and software-based firewalls can help prevent potentially damaging data from flowing in or out of an enterprise. Some organizations are also turning to Wi-Fi analyzers and WLAN intrusion detection to provide security across multiple locations.

Another essential tool is an Intrusion Detection System (IDS). It detects packets of data that pose a risk and prevents them from entering the enterprise.

Improved programming — including the avoidance of dynamically generated SQL code — can assist in preventing SQL injection attacks. Reviewing applications for vulnerabilities, ensuring that vulnerabilities are patched and scanning for attempted breaches can also be helpful.

A major trend in server security in recent years has been the widespread adoption of integrated security suites. Indeed, as security has become more complex and solutions have propagated, businesses have discovered that suites provide a more consistent and streamlined approach to protection while reducing overall costs and IT overhead.

Most suites include antivirus, antispyware, firewall, e-mail protection, intrusion prevention and device control within a single product. A central management console allows IT to manage and reconfigure the environment as needed.

Cost of Compromised Records

Make no mistake: a data breach has a substantial cost. Research conducted by Forrester Research indicates that every record compromised costs an enterprise somewhere between $90 and $305. Consequently, a breach of 1,000 records could result in a direct loss as great as $305,000.

Worse, the cost of discovery, notification and response averages $50 per record; lost employee productivity leads to another $30 per record; and regulatory fines sometimes reach into the millions of dollars. Opportunity costs and indirect costs, including restitution, additional security and audit requirements, also figure into the total cost.

AUTHENTICATION AND NETWORK ACCESS CONTROL

Antivirus software on desktops, notebook PCs and servers is only a starting point. Authentication and identity-based security using Network Access Control (NAC) is also gaining acceptance.

The former verifies a user's identity using a password or token. The latter uses a defined set of protocols and policy rules to determine who has access to the network or specific parts of the network once they have logged in.

Increasingly, NAC controls extend beyond employees and incorporate consultants and non-employees who require access to systems. NAC may also cover mobile and wireless devices.

In fact, more advanced NAC solutions allow administrators to grant access for certain dates and times or under specific scenarios. In addition, NAC solutions provide tools to provision other devices on the network, including mobile devices, fax machines, IP phones and printers. And IT can introduce and roll out services in phases.

This makes it easier to ensure that components work correctly. It also allows IT administrators to know that profiling and provisioning are set up correctly before the company rolls them out.

CONTENT FILTERING

Keeping undesirable content out of an enterprise is an ongoing chore. Web filtering helps to solve the problem by blocking selective content and IP addresses.

However, it's often a double-edge sword. Too lax of a policy can result in malware streaming in from rogue sites. Too aggressive of an approach to blocking incoming data packets makes it impossible for employees to get work done.

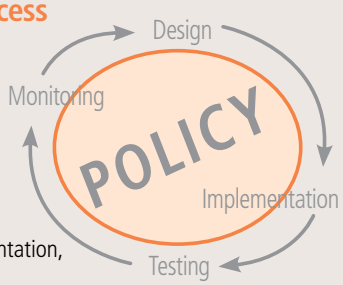
Successful content filtering, like most security tools, revolves around an understanding of risk tolerance. The best solutions provide a flexible and scalable approach that works with various devices, operating systems and user environments. These applications provide granular controls and reporting — usually available through a web-based dashboard.

Several vendors also offer e-mail filtering, which blocks spam and malicious messages. Some applications extend protection beyond malware and offer the ability to monitor outgoing e-mail and data flow as well.

Using robust policy management tools, businesses can build rules that help protect against theft. While at the same time they can ratchet up regulatory and compliance capabilities.

Security as a Process

Network security should be approached as a never-ending process or a series of steps or phases. This process consists of four phases: design, implementation, testing and monitoring.



WIRELESS NETWORK SECURITY

As companies turn to wireless communications and make it a core part of the enterprise, WLAN and Wi-Fi protection play

an increasingly important role in thwarting cybercrooks and malicious insiders. This risk translates directly into the need for wireless intrusion prevention, data encryption and access controls.

It also means that IT must monitor connections and, when necessary, detect rogue access points. Fortunately, newer WLAN systems provide a centralized manage console that configures all APs within an environment. The controller pushes the specific configuration to the individual APs and monitors them in real time.

IT executives must also monitor wireless cards and their control applications. In most instances, built-in networking features make it possible to create ad hoc networks. For instance, an individual may connect his or her computer to another in order to share files.

The ad hoc network, while convenient, creates potential threats. Unless an organization maintains separate wired and wireless networks, a user can gain access to the wired LAN via the wireless connection. This scenario exponentially increases the odds of a hack or breakdown.

An enterprise can reduce this threat by barring wireless devices from creating or attaching to ad hoc networks. Specifying that end devices attach only to known networks further aids in securing the end device more effectively. An even better approach is to deploy a solution that forces the deactivation of wireless network interfaces whenever the wired interface is active.

However, the threats don't stop there. A clever attacker can also impersonate a legitimate wireless AP. Traffic sent by users that's associated with this "evil twin" AP is subject to interception or alteration. These so-called "man-in-the-middle" attacks are typically defeated using varying combinations of the cryptographic controls.

An enterprise must also tap into wireless encryption to protect data as it flows between computers. Although WEP provides a basic degree of protection, it isn't adequate for today's business security requirements.

Consequently, most organizations are turning to far more robust encryption methods such as WPA and WPA2. All Wi-Fi compliant devices built after March 13, 2006, meet WPA2 standards.

APPLICATION SECURITY

Another important component in an overall security strategy is the use of application security. Most medium- and large-sized businesses may utilize hundreds of applications. With non-existent or inadequate security, these apps may be in the sweet spot for hackers.

To counter, application security typically monitors applications throughout their lifecycle in order to prevent security exceptions within the actual application. It also takes into consideration an underlying system possibly vulnerable because of flaws in the design, development, deployment, upgrades or routine application maintenance.

Application security provides vulnerability testing and secure application development platforms, real-time attack protection, granular access and identity management. Application security can also provide risk and compliance protection.

Today organizations are building more complex databases and turning to Web 2.0 and Service Oriented Architecture (SOA) components. Consequently, the need for stronger application security continues to grow.

ROLE-BASED SERVER SECURITY

The move to a role-based security model represents an evolutionary step in the development of security. It began to provide platform security capabilities traditionally offered only by third-party software vendors.

These tools include configuration wizards that walk a system administrator through the server configuration process using a role or set of roles (such as Active Directory Domain Controller, DNS Server, SQL Server) and specific security settings. Once the configuration process is complete, role-specific security tools take effect.

One of the most important components of a role-based security model is integration with Active Directory. Created by Microsoft, Active Directory is a technology that provides an assortment of network services.

Active Directory has several risk-mitigation capabilities, including single sign-on, the ability to store settings and other data in a central directory. It also offers streamlined updates and patch management, an ability to stop and start the Active Directory service hosted on a domain controller, and the option to deploy "read-only" domain controllers.

Data Encryption

Authentication alone cannot prevent unauthorized access to a network. In today's business environment, individuals exchange files on a regular and ongoing basis and data travels over wireless networks, including unsecure Wi-Fi hotspots.

Although a wireless network may be encrypted, the documents and files it contains may not be. This means that anyone who comes across a sensitive file — by accident or design — has access to it and all of its contents.

Consequently, businesses are turning to file and e-mail encryption, which not only protects data stored on computers, but also secures files residing on backup disks and in archival systems. More advanced solutions allow users to encrypt individual files as well as entire partitions or virtual disks that adjust dynamically to space requirements.

Some solutions also generate ZIP files and folders. In fact, it's possible to build self-decrypting archives that automatically decrypt themselves after successful authentication.

In addition, a growing number of organizations are turning to full-disk encryption to lock down computers and servers. It ensures that all the data stored on a disk is encrypted, including applications.

In order to gain access to the data, an individual must authenticate properly. Hardware-based full-disk encryption is capable of locking everything, including the underlying Master Boot Record (MBR). It is available on a growing number of notebook computers.

DATA LOSS PREVENTION

Organizations are also turning to newer tools such as Data Loss Prevention (DLP) to quell internal theft and breaches that sometimes result from authorized employees intentionally or inadvertently sending sensitive data beyond the enterprise. DLP catalogs an organization's data and then watches for it as the data exits internal systems.

DLP relies on content discovery, file system protection, network protection and GUI/kernel protection to provide a comprehensive defense. Among other things, DLP can block the transfer of content from one application to another.

It can also thwart the use of encryption when it is not appropriate. And it can limit cutting and pasting, screen captures and printing, and transferring data across media. Central policy management and reporting tools are built into DLP solutions. These vastly improve the ability of IT and security managers to track data flow.

Simply put, DLP provides a unified way to oversee policies, workflow and data motion. This is very important in an ever-changing business and IT environment.

In the end, a comprehensive and multifaceted approach to network security provides more thorough and consistent protection across an enterprise and beyond. It boosts the ROI from the networking, unified communications and other initiatives that increasingly drive productivity and bottom line results. ◊

GLOSSARY

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

802.11N
Ratified in 2009, the Institute of Electrical and Electronics Engineers (IEEE) 802.11n standard is an amendment to the IEEE 802.11 wireless networking standard. It improves network throughput over previous standards including 802.11b and 802.11g. 802.11n offers an increase in data rate from 54Mbps to a maximum of 600Mbps.

APPLICATION DELIVERY CONTROLLER (ADC)
A data center network device, the ADC helps with tasks performed by websites in an effort to balance web server loads. Application delivery controllers are usually located between the firewall/router and the web server farm.

CONTENT FILTERING
This is a filtering technique whereby material is restricted or allowed based on analysis of its content, rather than other criteria, for example, its source. This type of filtering is most often used on the Internet to filter e-mail and web access.

DATA LOSS PREVENTION (DLP)
This security function protects data from unintentional as well as intentional breaches made from inside the company. It also protects against data loss from external attack. These systems identify, monitor and protect data in different states, including data at rest, in motion and in use, often through the use of deep-content analysis.

DICTIONARY COMPRESSION
This term refers to a process used to reduce the bandwidth needed to send large files and large amounts of data over the network. A WAN Optimization Controller (WOC) learns the patterns of data being transmitted over the network. When the same pattern is detected again, it substitutes the pattern for a reference number. These caching techniques help to reduce the number of bits flowing over the network.

INSTANT MESSAGING (IM)
This technology allows for real-time, text-based communication between two or more participants over the Internet or some form of internal network or intranet. IM features include immediate receipt of acknowledgment or reply, group chatting, conversation logging and file transfer.

LOAD BALANCING
This process is used to balance a workload between multiple computing devices. In the data center, load balancing is used to appropriate work between two or more servers. This can help get work done in the same amount of time, thereby speeding service to all network users.

NETWORK AVAILABILITY
This is often noted as a percentage of uptime in a given year. It typically identifies the downtime allowed for a particular percentage of availability, presuming that the system is required to operate continuously.

POWER OVER ETHERNET (PoE)
This networking technology allows electrical power to run over CAT-5 or higher cable. No additional power cabling is needed for the connected device, making overall cabling less complex and crowded.

PRESENCE
This is a platform that collects information about internal user availability and communications capabilities. The information provides presence status organization-wide and facilitates presence-enabled communications between an organization's staff.

QUALITY OF SERVICE (QoS)
QoS refers to network mechanisms that assign different priorities to different applications, users or data flows, or that guarantee a certain level of throughput to the data flow.

REDUNDANCY (NETWORK)
This is a network system or component of a network system typically used to guard the primary system from failure. These types of secondary resources can include both hardware and software components.

RESILIENCE (NETWORK)
The ability to maintain an acceptable level of network service in the face of intrusive obstacles.

SECURITY SUITE
These include security solutions packaged together into one product. The suite can include such solutions as antivirus, antispyware, firewall, e-mail protection, intrusion prevention and device control. Central management is a key feature of security suites, saving IT time and resources.

SERVER VIRTUALIZATION
This represents the virtualization of multiple application servers onto a single physical server. Each virtual server can run its own full-fledged operating system, can be independently rebooted and remain logically distinct with consistent hardware profiles.

SINGLE NUMBER REACH
This technology gives users the ability to consolidate all of their call paths with a single IP phone number. It allows them immediate connectivity from wherever they are working. Users can also take advantage of a single voicemail box for all of their messaging needs.

SPANNING TREE PROTOCOL (STP)
STP is a Layer 2 protocol that provides path redundancy (while avoiding loops) for any bridged LAN when the initial link fails. Redundant links are provided via a tree that connects all of the network's switches.

SQL INJECTION ATTACK
This code injection technique exploits a security vulnerability occurring in the database layer of an application. The vulnerability will manifest itself when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or is not strongly written and thereby unexpectedly executed.

STORAGE AREA NETWORK (SAN)
A SAN consists of a high-speed network that interconnects different types of data storage devices with associated data servers. Users benefit from the opportunity of tapping into what appears to be a single pool of storage. Although the storage devices are remote, they appear to be locally attached to the operating system.

STORAGE VIRTUALIZATION
This includes the process of separating logical storage from physical storage. Physical storage can then be shared across multiple servers. The physical storage devices behind the virtualization layer are viewed and managed as if they were one large storage device.

TELEPRESENCE
This term often refers to a set of video conferencing technologies that allow a user to feel as if they are present at a remote location. This is done through manipulating the user's senses with stimuli that give the feeling of being in a different setting.

UNIFIED COMMUNICATIONS (UC)
UC generally refers to a "one-wire" infrastructure communications system that often includes some or all of the following components: voice, unified messaging, video, mobility, web/data collaboration, conferencing and presence management. Emergency notification systems can make use of a UC setup as well.

VIRTUAL LOCAL AREA NETWORK (VLAN)
A VLAN is a logical local area network that extends beyond a single, traditional LAN to a group of LAN segments. A VLAN acts as if it were connected, even though it may actually be physically located on different segments of a LAN.

WAN OPTIMIZATION
This refers to an approach to improve network services to branch users, working to enhance both the WAN itself and the travel of applications across it. This is often done through an optimized version of Transmission Control Protocol (TCP) and other common protocols.

WAN OPTIMIZATION CONTROLLER (WOC)
A WOC is a device that addresses a number of networking performance needs, such as increased bandwidth, WAN optimization and application acceleration.

WI-FI PROTECTED ACCESS (WPA AND WPA2)
A Wi-Fi security certification program developed to replace Wired Equivalent Privacy (WEP). WPA utilizes TKI protocol and Extensible Authentication Protocol (EAP) to secure wireless traffic. WPA2 builds on WPA, extending stronger data protection via Advanced Encryption Standard (AES) to personal and enterprise users.

WIRELESS EQUIVALENT PRIVACY (WEP)
WEP is a wireless security protocol for wireless LANs. It is now considered unreliable when used alone. WPA was developed to address WEP's vulnerabilities.

INDEX

Disclaimer

CDW
One CDW Way
200 N. Milwaukee Avenue
Vernon Hills, IL 60061

Your account number is	Key Code

PRESORTED STANDARD
U.S. POSTAGE
PAID
PERMIT NO. 1
CAROL STREAM, IL 60188

100125
Flyer 75740

CDW.COM/NETWORKING-UCGUIDE
888.667.4239

ABOUT THE AUTHORS

IMRAN ABBAS, CCIE, manages East Coast Network Solutions and Unified Communications Practices for CDW. Mr. Abbas has a B.S. in information management systems and is finishing his M.S. in information management. He is an active member of the Internet Engineering Task Force (IETF) and the Financial Industry Regulatory Authority (FINRA). »

« ERIC RIVARD is a Network Solutions Architect for CDW. Eric holds a B.S. in information technology and is finishing his M.B.A. Mr. Rivard holds numerous certifications, including: Microsoft Certified Systems Engineer (MCSE), CheckPoint Certified Security Engineer (CCSE), and Cisco Certified Network Professional (CCNP). Eric has written three books for Cisco Press.

WILLIAM COE manages the Unified Communications Solutions, Central Operation, for CDW. While at CDW, Mr. Coe has helped establish advanced UC solutions for healthcare systems with Vocera Communications, and is developing the video business solutions for desktop-video-to-room-based TelePresence. »

« HOWARD WEISS manages the Network Solutions Team in the western half of the United States. Throughout his 11-year tenure as a technologist at CDW, Howard has helped build multiple teams from the ground up, including the IBM presales team, Field Solutions team, the HP FieldSE team and now the Network Solutions team.

MIKE GUTKNECHT, CCIE #7712, is a Security Solutions Architect with CDW's Advanced Technology Group. Mike consults with customers on a wide range of security topics, focusing on mitigating organizational risk cost effectively. He holds an M.B.A. degree and a B.S. degree in physics. »

« JOSH ZENNER is a Wireless Solutions Architect with CDW. He has many years of experience designing and implementing wireless solutions, with a focus on healthcare, manufacturing and enterprise-class organizations. Josh specializes in finding ways to utilize wireless technologies to make organizations more efficient and profitable. He works out of Wausau, Wis.

NETWORKING AND UNIFIED COMMUNICATIONS
REFERENCE GUIDE

LOOK INSIDE for more information on:

- Building a robust network to meet expanding business needs
- Utilizing WAN optimization controllers
- Upgrading unified communications capabilities
- Taking advantage of 802.11n improvements