



**NETWORKING AND
UNIFIED COMMUNICATIONS
REFERENCE GUIDE**



Boosting services
for greater productivity
and collaboration

CDWG.com/networking-ucguide | 888.676.4239



The Right Technology. Right Away.®

NETWORKING

NETWORKING AND UNIFIED COMMUNICATIONS REFERENCE GUIDE

TABLE OF CONTENTS CHAPTER

| | |
|-----------|--|
| 01 | Networking and Unified Communications: Improved Service, Better Collaboration 3 |
| | • Greater Function vs. Less Cost |
| | • Recent Networking Trends |
| | • Unified Communications Trends |
| 02 | Inside the Data Center 5 |
| | • Planning a Data Center Overhaul |
| | • Consolidating in the Data Center |
| | • Server Virtualization |
| | • Cloud Computing |
| 03 | Improving Network Performance 9 |
| | • How WOC Works |
| | • WOC Deployment |
| | • Load Balancing |
| 04 | Unified Communications 21 |
| | • Centralized UC Management |
| | • Communication and Collaboration Applications |
| | • The Contact Center |
| | • Video Conferencing |
| 05 | Securing the Network 25 |
| | • Role-based Server Security |
| | • Security Suites |
| | • Wireless Security |
| | • Cryptography: Authentication and Encryption |
| 06 | Wireless Mobility 29 |
| | • Designing Your Wireless Network |
| | • Working with 802.11n |
| | • Central Control |
| | • Conducting a Site Survey |
| | • Encryption and Authentication |
| | • Failover and Redundancy |
| | GLOSSARY 33 |
| | INDEX 35 |

WHAT IS A CDW•G REFERENCE GUIDE?

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

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

NETWORKING AND UNIFIED COMMUNICATIONS:



IMPROVED SERVICE, BETTER COLLABORATION

CHAPTER 1:

Greater Function vs. Less Cost

Recent Networking Trends

Unified Communications Trends

It doesn't take dire economic circumstances to prod government and educational organizations 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 organizations, and it is an area that especially feels the push and pull of increasing functions while cutting costs. Because the network often extends into almost all areas of an organization, changes to it have repercussions throughout an organization. This is an area that requires special care when planning any changes or upgrades.

GREATER FUNCTION VS. LESS COST

Some IT managers feel as though their networks are the victims in an escalating arms race. As bandwidth grows, software manufacturers create applications that utilize the resilient nature of IP and assume a high level of service availability. Applications running across the network grow in complexity; and so they increase their reliance on a resilient network. And to take advantage of all these great new capabilities, they must again ratchet up the network's capacity.

This means that the network is in a constant state of flux, and it's up to the IT team to best manage this ever-changing system. One constant is that the network needs to provide dynamic and scalable services that not only deploy easily, but also allow organizations to add functionality as required.

And in doing this, IT managers need to keep an eye on decreasing the total cost of ownership (TCO) while increasing the return on investment (ROI) — all while still meeting the functional challenges in the data center.

What's an IT manager to do? The best approach to meeting these competing demands is to boost services by adding various application acceleration and bandwidth optimization devices to the network. These network devices enhance the responsiveness of IP-based applications and are less expensive than simply upgrading the entire network infrastructure.

RECENT NETWORKING TRENDS

One bright spot for enhancing your existing network infrastructure is WAN optimization controllers. Another popular trend in networking right now is converging security and networking functions into one robust and easily managed solution. These initiatives, which help decrease TCO, nevertheless add to the complexity of the traditional IP network.

Another popular initiative, joining together virtualization and server consolidation, has been growing in popularity. This is in large part because of the proliferation of continuity of operations solutions, which in turn drive a need for greater redundancy in the form of network-based storage. Organizations are seeking out network storage devices that provide a scalable solution independent of the traditional distance constraints.

To meet this demand for greater storage redundancy, server managers are leveraging their existing server resources through

virtualization. This, in turn, allows the organization to use the network to distribute applications over a larger IT landscape.

Many organizations are also taking steps to simplify their networking management. Having a single overarching management tool ensures that no single solution operates without oversight. This also allows organizations to identify outages and other network problems proactively rather than reactively.

UNIFIED COMMUNICATIONS TRENDS

Once an organization has addressed its fundamental networking needs with local area and wide area solutions, application functionality and productivity for the staff become primary concerns. These concerns can be addressed by unified communications (UC) solutions, which allow IT departments to provide streamlined communications options and advanced productivity applications throughout the network environment.

UC incorporates and combines some of the most sophisticated communications technologies available. It has unquestionably changed the way that organizations address all facets of intercommunication among work staff. The maturation of UC has happened at the right time, as the entire work environment is shifting away from the traditional setup where work staff spend their entire day sitting behind a desk and toward a more mobile structure.

Work staff are now approaching their work responsibilities in numerous ways. Whether sitting at a desk, visiting at a branch office, telecommuting from home or connecting to the network via a cell phone, staff must have access to the same services and levels of functionality. Today's combined advances in networking

and UC allow the IT staff to facilitate this scenario.

One of the more popular UC trends right now is the use of presence technology. Presence allows end users to see in real time the status and availability of other coworkers, including preferred methods of contact. This allows users to fine-tune their method of communications with one another for maximum efficiency.

Advances in mobility solutions have further extended the capabilities of the communications network beyond the confines of the traditional work environment. Regardless of location, mobility can provide presence and voice communications via smartphone technology for an offsite worker the same as if he or she were physically within the "brick and mortar" office.

A pair of closely linked technologies that are being increasingly adopted are video communications and desktop collaboration. Both address a number of growing organizational concerns, from reducing the carbon footprint to improving conferencing functionality.

The improvements in video communications are especially exciting. Eighty to 90 percent of human communication is based in visual cueing. So any improvement to video communication is a boon for an organization's conferencing abilities. The adoption of video serves as a logical extension of an organization's UC network.

Whether video communication is accomplished point-to-point through desktop integration or by means of a full-scale telepresence solution, it allows coworkers to utilize the most effective mode of communication possible. Add the functionality of desktop collaboration — the ability to share documents, presentations and any stored media — and UC becomes not only thoroughly versatile but increasingly indispensable in today's work environment. ♦



INSIDE THE DATA CENTER



CHAPTER 2:

Planning a Data Center Overhaul

Consolidating in the Data Center

Server Virtualization

Cloud Computing

Data centers have been the beneficiaries of a great number of new technologies over the past few years, from virtualization to optimization and acceleration devices. Government and educational organizations now have many options to improve their data centers. Planning and mapping out any improvements you make to your data center becomes even more important now.

PLANNING A DATA CENTER OVERHAUL

A data center's physical infrastructure is the foundation for its success or failure. A solid infrastructure is an effective base upon which to build services, while deficiencies in infrastructure will plague the most diligent of data center managers.

Refreshing a data center provides organizations with an opportunity to move more effectively to contemporary technologies, such as blade-based computing and large-scale virtualization. Organizations also may find themselves in a much better position to provide flexible and cost-effective services.

But in designing or refreshing a data center, organizations must ask numerous questions in order to make educated decisions. Before you initiate a data center refresh, you will want to consider some best practices.

1. Plan for floor space. There are several factors to consider when it comes to space. First, providing adequate floor space for current and anticipated demand is essential. To estimate future demand, project your organization's growth using average-case and worst-case figures and find an appropriate target that fits within the maximum space, power and cooling constraints available without

building a new facility.

Also consider utilizing virtualization technology to save space. Among its many benefits, virtualization offers the ability to do more with less. Stacking your rack with servers running virtualization software will allow your data center to increase computing power while decreasing its footprint.

2. Run cabling under the floor. It's important to keep the cabling under the floor perpendicular to the airflow and completely away from the cold aisles so that it does not interfere with airflow. Because hot aisles do not have any bearing on airflow under the floor, they are a good location for cabling. Install ducts under the floor to further increase cooling efficiency.

Also, following the Technology Industry Association (TIA) standard 942, you can use a tiered distribution concept for cabling your equipment. Rather than cabling all data center components directly to your core network equipment, you can establish a distribution area in each aisle and cable individual racks to this distribution area.

In TIA parlance, this is referred to as a horizontal distribution area and can be thought of as a "wiring closet" for the aisle. This allows changes to be made between the server and the horizontal distribution frame without disturbing unrelated cabling.

Along with your cable distribution network (and using the same cable distribution channels), you can also install a common bonding network that will tie to your building's grounding system. This means each enclosure that is added to the data center should have access to a grounding point so that it is grounded properly.

3. Calculate your power and cooling. With the cost of energy accounting for nearly 25 percent of total IT budgets, and with the cost of cooling accounting for nearly half of data center costs, it's no wonder why power and cooling are major considerations when building a data center. The math is easy. The larger the data center, the more power it will take to run it.

Remember that power equals heat. The more heat you have, the more cooling you'll need to keep that heat at bay. Looking into more efficient ways to use power becomes paramount, as does finding ways to cool your data center more efficiently.

One interesting note to keep in mind about modern computing equipment: For planning purposes, at least, it is almost completely efficient in converting electrical power to heat. As a result, you can generally assume that every watt of electrical energy that you put into your data center will need to be extracted in the form of heat energy.

Because one kilowatt-hour is roughly equivalent to 3,413 British thermal units (BTUs), or 0.28 tons of cooling capacity, you can use your anticipated electrical load to drive the calculations for your cooling load.

4. Look to the future. How big is too big? Knowing what you need out of your data center today is the easy part. Figuring out what you'll need 10 years down the road is the challenge. Make sure that you clearly define your current and future requirements because these will affect data center design, size and location.

Making allowances for growth is the linchpin of any good data center design, and capacity planning pertains not only to storage or computing power but also to power itself. In the end, proper capacity planning can provide technological longevity for your data center and, therefore, your entire organization.

CONSOLIDATING IN THE DATA CENTER

One of the easiest and most effective upgrades an organization can make in the data center is to consolidate. Bandwidth and energy cost increases, coupled with increasingly complex IT environments, have led many organizations to consolidate their infrastructure.

This is facilitated by removing applications and data from remote offices and staff PCs and placing it all into a centralized data center. Another consolidation strategy is to consolidate individual applications and their related storage.

CONSOLIDATION BENEFITS

Consolidating the data center allows organizations to provide powerful and rich applications, to simplify management, to build in strong redundancy and to strengthen security. Each of the different consolidation technologies facilitates a more efficient use of IT resources:

- **Server and application virtualization:** This technology enables an organization to take multiple physical servers, typically underutilized, and consolidate them onto a smaller number of physical servers.
- **Blade server consolidation:** This approach fits your servers compactly into a smaller rack space while saving on cabling, power and cooling costs.
- **Application centralization/optimization:** This technology permits an organization to migrate its remote office applications and data into the data center, while allowing fast and efficient access out to remote workers.

By centralizing remote office servers, virtualizing underutilized servers onto fewer physical ones and shrinking those physical servers down into blades, an organization can create an environment that proves far easier to manage, protect and secure.

However, moving in this direction can have a tremendous impact on a network, and such a project requires a great deal of preparation. Higher server or network interface card (NIC) density per rack will require the use of faster switches. Furthermore, server portability (defined as the movement of a virtual server from one physical host to another) requires a properly designed resilient network.



CONSOLIDATE STORAGE?

Today, storage consolidation often goes hand-in-hand with server consolidation. Not only are organizations centralizing their ever-growing storage resources, but virtualization has also become a substantial driver, as virtualized servers reside on the storage area network (SAN). Until recently, this fact had little impact on the Ethernet network. But now a convergence of technologies is happening.

For years, storage connectivity was either direct-attached via SCSI or by means of a separate Fibre Channel (FC) network. Because of the cost of FC networks, many organizations embraced iSCSI as an alternative connectivity method. This method encapsulates block-level SCSI traffic in IP packets for transmission across the network.

A newer technology, Fibre Channel over Ethernet (FCoE), is gaining popularity. This protocol transmits the highly resilient and efficient FC protocol over a standard Ethernet network and allows for the use of existing FC storage arrays. This convergence puts even more demand on the network, which requires low latency, high throughput and built-in resiliency.

SERVER VIRTUALIZATION

Server virtualization often plays an integral role in any consolidation effort. The virtualization of multiple application servers onto a single physical server reduces the number of actual servers in the data center while at the same time increasing their utilization. Virtualization allows IT managers to do the impossible — reduce TCO and increase ROI in the data center.

To squeeze out the most efficiency and value you can from a server virtualization project, consider these six best practices.

1. Tap templates and customizations for rapid deployment.

Virtualization gives you the capability of creating a virtual server or desktop once, saving it as a template, and using customization scripts to make a mass rollout of similar servers and desktops very easy.

If you don't use customization and scripts, you will have to clone the master image manually, then boot up and make changes to each cloned image. Depending on the image size, this process could take upward of an hour or more. With customization and scripts, you will need only a few minutes to create your custom specifications and execute your script.

2. Build clusters of physical servers with shared storage. Take advantage of your virtualization software's native clustering and disaster avoidance capabilities by attaching your physical servers to a SAN. If you're currently clustering database and application servers, you may be able to greatly reduce and simplify those clusters.

Hardware upgrades for a cluster are as simple as migrating the virtual machines (VMs) from the old hardware, shutting down the old server and powering up the new server. Using a SAN also allows faster and easier disaster recovery if your physical server fails.

3. Use pre-built virtual machines. Ask the manufacturer if it has any pre-built virtual-machine images that you can deploy directly to your virtual environment. There is a wide variety of pre-built VMs available for web servers, databases, systems monitoring and more.

You can save a significant amount of time and reduce the possibility of human error by using a pre-built image when migrating to a new e-mail spam/virus scanning platform. By deploying a pre-built machine, you will already have 95 percent of the work done for you.

4. Create a cost-effective test environment. You're going to need a dedicated test environment for your critical systems, even after they're virtualized. In fact, all critical systems should have a test and development environment, but even your non-mission-critical applications can benefit from snapshots.

A snapshot allows you to save a virtual machine at a point in time, at which point you can begin moving the previously tested system changes to production. If the new patch proves troublesome, fixing it is as easy as rolling back to an earlier snapshot.

5. Control virtual-machine sprawl. One of the pitfalls of virtualization is the ease with which new virtual machines can be created. This can lead to significant inefficiencies in your virtual environment. It isn't necessary to create a separate virtual server for everything.

For example, you don't need to create a new virtual Apache web server for every web application; just use Apache's virtual host configuration. Every unneeded virtual machine uses system resources that could have been used elsewhere and adds to the number of VMs that your support staff will need to manage.

A good approach to controlling virtual-machine sprawl is to assess the performance requirements of a new service. If the load is expected to be low, and you have an existing virtual machine that can handle it, then use the existing virtual machine. Make sure to use the built-in performance monitoring tools, which will give you an indication of when it's time to begin splitting services onto new virtual machines. Proper change and configuration management is key.

6. Migrate your existing physical servers to virtual servers without the hassle. Most virtualization software has some form of physical-to-virtual system migration tool (such as VMware Converter) that can copy a physical server bit for bit to your virtual environment. There are typically a few different versions of the tool

with varying capabilities. Often the migration tool will be free, if only in a limited version. Assess your needs to determine which tool can do the job well.

CLOUD COMPUTING

A survey of new technologies in the data center would not be complete without considering cloud computing. In this instance, the term “cloud computing” refers to what used to be called software as a service (SaaS).

The nuances of this term are still evolving, but the central idea turns on the concept of having a service provider deliver an organization’s IT resources over the Internet. This approach allows for access to the network at any time, whether from a cell phone, from the office desktop or anywhere else users can get an Internet connection.

The benefits derived from cloud computing include increased flexibility in the network environment, rapid scalability to meet greater or reduced service demands and a decrease in IT staff time devoted to day-to-day data center tasks. With less time devoted to data center maintenance, IT staff can devote their energies to projects that support the organization’s mission and move it forward.

Cloud computing is not perfect and does not suit every organization’s needs. Software licensing fees can often be a

barrier to adopting cloud computing. Organizations with up-and-running data centers are often reluctant to abandon the significant investment they’ve made in this licensing and then take on the sometimes hefty annual fees for cloud computing.

Cloud computing also requires a certain comfort with new ways of doing things in the data center, so organizations will sometimes find resistance in the IT department to a new approach to networking.

If your organization is going to consider cloud computing, be sure to address the following:

- **Constant connectivity:** Without an Internet connection, all of your organization’s IT services from the cloud are inaccessible.
- **Resistance to change:** You can expect some resistance from IT staff members who operate the data center and finance managers looking for ROI from the data center.
- **Security concerns:** Most service providers address security, but you still must protect your organization’s information as it traverses the Internet.
- **Selecting and negotiating with providers:** This is a new service with new parameters. Be sure to do your homework to know what your needs are and what you should expect from a provider. ♦



IMPROVING NETWORK PERFORMANCE



CHAPTER 3

How WOC Works

WOC Deployment

Load Balancing

Web applications, e-mail attachments and files can quickly consume your organization's valuable backbone bandwidth when serving users across numerous locations, and slowdowns can lead to demands for expensive upgrades. One of the best ways to reduce the cost of supporting IT services at multiple locations and branch offices is server consolidation, especially when combined with server virtualization (covered in Chapter 2).

But how can organizations accommodate growth in bandwidth demand and support projects that promise cost savings, such as server consolidation, while holding spending down? And what can IT do to appease users who want swifter response times and faster file transfers?

The answer is to use a combination of bandwidth management, WAN optimization and application acceleration techniques. Together, they can reduce bandwidth demands and improve service. WAN optimization controllers (WOCs) combine these tools, and many major network manufacturers produce WOC devices, including Blue Coat Systems, Cisco, Citrix, Juniper Systems and Riverbed Technology.

HOW WOC WORKS

WAN optimization controllers reduce bandwidth requirements for web applications and speed delivery by caching objects. Static objects are easiest to cache, and WOCs can do so automatically.

The first time someone in a branch office requests a static object, the WOC passes the request on to the server. When the object is delivered, the WOC stores a copy of it. The next time someone

requests the same object, the WOC intercepts the request and sends the stored version. This greatly reduces transmission time and eliminates latency.

Some WOCs can provide this service for dynamic objects if these objects change only over long periods of time. The WOC can store an object for a set period before refreshing it. The IT team must understand the dynamic objects to determine appropriate time-out values.

WOC DEPLOYMENT

The most significant way that WOCs reduce bandwidth requirements is by a technique called dictionary compression. Dictionary compression reduces the bandwidth needed to send files and large amounts of data by a factor of 10 to 30.

Dictionary compression works by learning patterns in the data. The WOC automatically monitors the traffic flow, learning short sequences of data and storing them. When it sees a pattern it has learned, it removes the pattern and substitutes a reference number. A receiving WOC, which is automatically learning the same patterns and reference numbers, removes the reference number and puts the data pattern back in the packet.

For example, the first time the file is sent there is no reduction as both WOCs learn the pattern. When someone else requests the same file or a file that has the same patterns, the WOC substitutes a series of reference numbers for the patterns. If there's a change to the file, then only the changes are sent, along with reference numbers for unchanged patterns.

TCP/IP traffic is optimized by adjusting the flow control parameters. Application protocols, such as Common Internet File System (CIFS), are also optimized by the WOC.

The problem with CIFS is that it can slow file transfers over the WAN. CIFS was created for use over LANs. But with server consolidation, it now comes into play on WANs, and latency creates inefficiencies. Microsoft is aware of the problems with the protocol and has improved it in the latest version, but WOCs can still bump up performance.

Simply buying a WOC and turning it on will not guarantee benefits. Here are the steps you'll want to take to get the most from your WOC deployment.

1. Know what's on your network. The first step to reduce bandwidth and provide better service is to understand what is flowing over the network. Optimizing without knowing what types of traffic are using your network is wasted effort. It is important to know how much and what type of nonessential traffic flows over the network. (It is always surprising to discover how much nonmission traffic moves through the pipes.)

Knowing how much traffic is using Port 80 (HTTP) doesn't

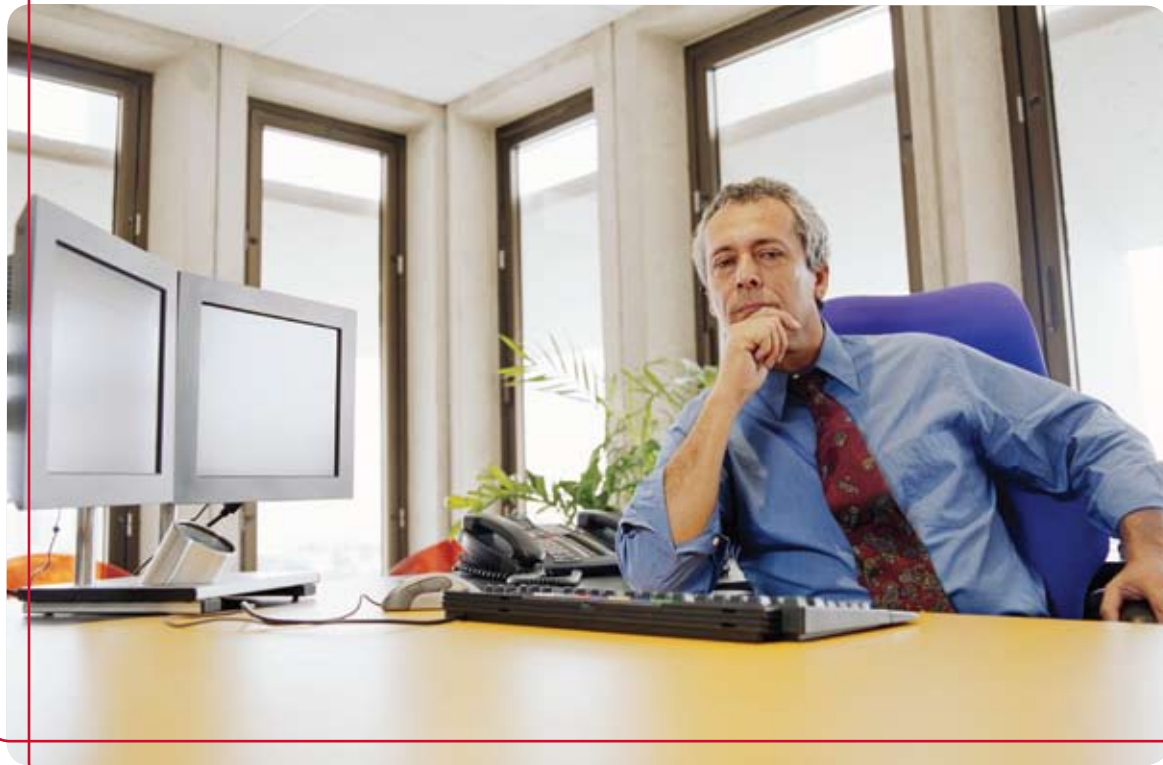
help IT much because an increasing amount of both critical and nonessential traffic uses a web interface. It's important to understand the applications in use. Is it SharePoint, SAP or some peer-to-peer application?

It's also important that any monitoring tool updates its list of apps often. New apps become available all the time, especially nonwork apps. Without regular updates, a WOC's monitoring program will lump unknown apps into a common bucket.

2. Apply QoS. The next step is to implement Quality of Service controls. This will ensure that the critical mission traffic receives priority attention and nonmission traffic does not consume bandwidth.

IT can implement QoS on the router, the WOC or both. The biggest obstacle to implementing QoS is how difficult it is to specify. A WOC should allow QoS policies to be set up easily based on the monitoring results, provide default settings for most applications and interface with existing QoS policies.

3. Set bandwidth parameters. The next step is to decide how much bandwidth each app should receive. WOC bandwidth management lets network administrators set controls on how



much of the available bandwidth an application receives. This guarantees that less-critical traffic can't crowd out critical apps; it's a must-have feature on any WOC.

This way, an organization can prioritize traffic based on its QoS policies. For example, if users can access consumer sites such as Amazon, bandwidth management can control the amount of bandwidth allowed, ensuring it doesn't affect critical applications. The amount can even be adjusted depending on the time of day.

4. Decide what to optimize. It's tempting with the acceleration and optimization provided by a WOC to turn it on for all traffic. It is a good idea to turn it on for file transfers, web traffic and most essential traffic, but not for everything.

For instance, Voice over Internet Protocol traffic should not be optimized, as the process will slow it down and provide little benefit. TCP/IP protocol optimization can help video traffic, but running it through dictionary compression provides no benefit and can degrade WOC performance.

5. Plan for encrypted files. WOCs are unable to apply many of their techniques on encrypted data. They overcome this problem for Secure Sockets Layer (SSL) traffic by learning the keys and decrypting the data, and then re-encrypting before sending it back out on the network.

How they learn and store the keys varies from product to product and is something network managers need to understand. Decryption is important — without it, the WOC benefits are limited to QoS and bandwidth management, and there is no bandwidth reduction benefit.

6. 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 WOC in one connection, then hiding the individual connections. Because the data in the packets is replaced with reference numbers, deep packet inspection of application data becomes impossible. This can create a problem if security and monitoring devices are placed on the network after the WOC.

One solution is to place security and monitoring equipment before the WOC. Additionally, WOC manufacturers offer techniques to mitigate the connection problem, but it is important that the IT team learn how these processes work and if there are any downsides for their particular needs.

7. Involve the security group. Any WOC deployment should be coordinated with the security group. There are several areas that concern security, including the decryption process, hidden individual connections and changing the data in the packet.

Additionally, if hackers gain access to the dictionary compression database, they might be able to reconstruct files. There are solutions to most of these challenges, but the IT security team

needs to know how the technology affects the organization's overall data assurance and infrastructure protection practices.

Ultimately, a WOC can reduce bandwidth requirements, often significantly delaying the need for a WAN upgrade. Plus, it can satisfy users by moving data and minimizing app response time.

LOAD BALANCING

As organizations move to centralized data centers and support critical applications across WANs, they need to find a way to balance application load while offloading key application-level functions, such as security, SSL encryption or content switching, from overburdened servers. To facilitate this, many organizations turn to load balancing via a software or hardware solution.

Load balancing divides the amount of work that a server has to do between two or more servers so that the work gets done in the same amount of time, allowing all of the network's users to be serviced quicker. This technique maximizes data center resource utilization and throughput, minimizes response time, and provides high availability with failover.

One of the most common applications of load balancing is providing a single Internet service from multiple servers. This is known as a server farm. Server farms are often used to support heavily trafficked websites and high-bandwidth FTP (file transfer protocol) websites.

Many of the newer load-balancing appliances also offer other value to organizations, such as the ability to examine network traffic, detect performance and security problems, and reduce bandwidth expenses. Here's a look at some of the additional features available:

- **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, but they can also perform significant bandwidth savings duties such as compression and traffic shaping.
- **Content-switching:** Another key security feature some products offer is content-switching, where the load balancer filters for certain 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. ♦

CONVERGED COMMUNICATIONS



MAKES SENSE.



When it comes to implementing a VoIP solution, there are a lot of factors that your organization must consider including: compliance, cost and management. Having a trusted partner is essential as you look for the right solutions to meet all your requirements.

When working with our customers to help them get all the benefits of converged communications while they plan for compliance, CDW•G focuses on three cornerstones: equipment, design and usage. We encourage customers to think about how meeting a mandate will affect their VoIP implementations by asking the following questions:

- “What does my organization need from a VoIP solution, now and in the future?”
- “What new equipment, if any, do I need to meet the mandate?”
- “How will my organization continue to use the solution — and who will support its mandate?”

For VoIP and converged communications solutions, we’ve got the products. But, more importantly we’ve got the answers. Every CDW•G 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 workforce and current technology assets to ensure that your 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•G account manager today to learn more about our comprehensive approach to unified communications.

CALL FOR PRICING

Cisco® Unified Communications Manager

High-availability server platform for Cisco Unified Communications solutions
CDWG 1152554



- 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

\$383.03

CDWG 1300067



- Support for wideband (G.722 codec, adherence to TIA 920), including handset, headset and speakerphone
- Full-duplex speakerphone with acoustic echo cancellation
- IP address assignment can be statically configured or configured through the DHCP client
- Dedicated headset port eliminates the need for a separate headset amplifier and allows the handset to remain in its cradle



**Microsoft® SQL Server® 2008 Standard Edition
Open License Government¹**

\$690.26

CDWG 1542739



For display only

SQL Server® 2008 delivers on the Microsoft® Data Platform vision by helping your organization manage any data, any place, any time. It enables you to store data from structured, semi-structured and unstructured documents, such as images and music, directly within the database.

- Trusted — run your most mission-critical applications on a secure, reliable and scalable platform
- Productive — reduce the cost of managing your data infrastructure while streamlining development of data applications
- Intelligent — drive operations intelligence throughout your organization

¹Purchase five licenses to qualify for the Microsoft Open License Government program; media must be purchased separately; call your CDW•G account manager for details



Hard drives sold separately



**HP ProLiant DL360 G6 Rack-mount Server
Two Quad-Core Intel® Xeon® Processors X5550 (2.6GHz)**

\$5815.42

CDWG 1723313

- Memory: 12GB std., 192GB max. (PC3-8500R DDR3)
- Hard drives: none ship std.; up to eight SFF hot-pluggable SATA/SAS drive bays available, 2.4TB max. storage



CDW•G Unified Communications

Integrate multiple communication networks into a single, unified system to enable more effective communication and collaboration with staff, partners and customers.

- Call Center Management
- Conferencing and Collaboration
- Messaging
- Telephony and VoIP

Call your account manager today to generate a solution designed specifically for your needs.

TRIM DOWN THE UC WAY



You save time and money when you converge transactions, e-mails and phone calls over one network. Carrying communications over the IP network allows organizations 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 transfer records along with calls. And video conference participants can have real-time access to files.

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

1. Reduce Conferencing Costs

By bringing conferencing capabilities in-house, organizations can expect to save a minimum of 20 percent per year on conferencing costs, according to Forrester.

2. Avoid 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 will also save money when it's time to restructure or expand.

3. Shrink Your Travel Expenses

The average domestic business trip costs \$1002. The average international business trip costs \$3542. If you can eliminate even a few of these trips per year by utilizing web or video conferencing, the savings add up quickly.

4. Cut 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. Decrease 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•G account manager today to learn more about how unified communications solutions can help your organization save money.

CALL FOR PRICING

Avaya G350 Media Gateway

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

CDWG 1046370



- Designed to be a complete voice/data networking solution
- The G350 Gateway is ideally suited for enterprises with distributed branch office locations using 8-72 extensions
- An 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
- For communications security, the G350 can secure VoIP media streams using Advanced Encryption Standard (AES)



CALL FOR PRICING

Avaya 9620 IP Telephone

CDWG 1010566



With a combination of audio quality, an improved user interface with a context-sensitive display and a stylish, professional design, Avaya sets the new standard for enhanced productivity and an enhanced end-user experience.

- Intuitive user interface
- Superior audio quality
- New design and display
- Modules and adapters
- Phone models designed for user profiles



Microsoft® Office Professional Plus 2007

Share information and work across geographical or organizational boundaries

Open License Government¹

\$374.05

CDWG 1065967



Microsoft® Office Professional Plus 2007 will help you and your organization work more efficiently and effectively with a set of powerful tools for creating, managing, analyzing and sharing information.

- Deliver better results faster
- Work together more effectively
- Get more out of your information
- Control content, streamline processes
- Accelerate performance with the power of integrated innovation

¹Purchase five licenses to qualify for the Microsoft Open License Government program; media must be purchased separately; call your CDW•G account manager for details

Microsoft

PERFORMANCE MODEL

HP ProLiant DL380 G6 Rack-mount Server Two Quad-Core Intel® Xeon® Processors X5550 (2.66GHz)

\$6206.44

CDWG 1723259



Hard drives sold separately

- Memory: 12GB std., 192GB max. (PC3-8500R DDR3)
- Hard drives: none ship std.; up to eight SFF hot-pluggable SAS/SATA drive bays available, 6TB max. storage
- 16MB Level 3 Cache
- Two Embedded NC382i Dual-Port Multifunction Gigabit Server Adapters



CDW•G Unified Communications

Integrate multiple communication networks into a single, unified system to enable more effective communication and collaboration.

- Call Center Management
- Conferencing and Collaboration
- Messaging
- Telephony and VoIP

Call your account manager today to generate a solution designed specifically for your needs.

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 organizations 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 well within reach of organizations 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 consumers have become accustomed to simple yet powerful communications media 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•G account manager today to learn more about video conferencing solutions and the productivity advantages they can deliver to your organization.

CALL FOR PRICING

Polycom® HDX 7001™

Video conferencing kit
CDWG 1387351



- Data Compression Protocol is H.263++, H.264, H.261
- High-definition (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



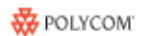
CALL FOR PRICING

Polycom® CX5000

Easily add group video collaboration to Microsoft® Office Live Meeting 2007 and Microsoft Office Communications Server 2007
CDWG 1726377



- 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 organizations with limited IT support can easily set up and configure the device



Microsoft HD LifeCam Cinema™

Notebook or desktop HD webcam

\$69.82

CDWG 1838192

- 720p HD widescreen
- Auto focus
- Digital microphone
- Windows Live™ Movie Maker
- LifeCam Dashboard
- Windows Live Call Button
- Works with Windows Live, Yahoo! Messenger, AOL Instant Messenger and Skype
- Mac®, PC compatible



Powerful. Intelligent.



Hard drives sold separately

HP ProLiant BL490c G6 Blade Server

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

\$4003.96

CDWG 1723369

- Memory: 6GB std., 192GB max. (PC3-8500R DDR3)
- Hard drives: none ship std.; space for up to two SFF non-hot-pluggable Solid State Drive bays available, 1.8TB max. storage



Monitor sold separately

HP SMART BUY

HP Compaq Business Desktop 6000 Pro

Stable and secure

\$699.99¹

CDWG 1860085

- Intel® Core™ 2 Duo Processor E7600 (3.06GHz)
- Memory: 2GB
- 250GB hard drive
- DVD±RW
- Windows® 7 Professional
- Windows XP Professional Downgrade installed²

²Windows XP installed with Windows 7 Certificate of Authenticity and logo; Windows 7 media included; customer has rights to both Windows 7 and Windows XP Professional



CONTACT YOUR CDW-G ACCOUNT MANAGER TO FIND THE RIGHT SERVICE FOR YOUR SERVER

HP Hardware Support Onsite 6-Hour Call-to-Repair Service

Decrease server downtime with committed 6-Hour Call-to-Repair for hardware problem resolution

- Remote problem diagnosis and support
- Onsite hardware support
- Materials included
- Enhanced parts inventory management



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 communications 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 organizations see a return on their investment in as little as 4-12 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•G 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•G Specialist today.

CALL FOR PRICING

LifeSize® Team 200™

Feature-rich, high-definition (HD) video
CDWG 1658987



- 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



ClearCube® C7130 C/Port

Full functionality of an Intel® dual-core based PC

\$473.80

CDWG 1494134



- Connects desktop peripherals to a centralized PC Blade over standard Category 5 homerun cabling up to 200m
- While only the size of a paperback book, the C/Port gives the user the full functionality of an Intel dual-core based PC
- Solid State — requires no special software, has no moving parts that can fail, contains no removable parts which discourages user tampering and theft



NEC MultiSync® 4215

42" digital signage display

\$276.30

CDWG 1536042



Protective-glass and touch-panel-ready

- High-performance panel and an abundance of advanced technologies that promote extended use
- 500 cd/m² brightness and DVI input with HDCP
- Landscape and portrait orientation
- Three-year parts and labor, including backlight



Logitech® C600 Webcam

2.0 megapixel webcam

\$79.99

CDWG 1838465



- Widescreen HD 720p video
- RightLight™ 2 technology
- Built-in mic with RightSound™
- Includes Logitech Vid™
- True 2.0-megapixel sensor with glass lens



CDW•G Installation Services

IT departments are stretched thin. Technology costs are unpredictable. The design, implementation and protection of your new technology demands expertise and time that many in-house IT professionals simply don't have. Our highly-certified specialists will help you get the most out of your technology by providing expert solutions that meet your unique needs with minimal disruption of operations. CDW•G partners with only the finest industry-leading service providers to bring solutions right to your door.



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•G 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•G 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•G'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.

UNIFIED COMMUNICATIONS



CHAPTER 4:

Centralized UC Management

Communication and Collaboration Applications

The Contact Center

Video Conferencing

One of the most noticeable changes to the network environment over the past few years has been the increased adoption of unified communications (UC) technologies. UC includes a broad range of technologies including converged networks; simple IP telephone and messaging systems; complex IP-based systems that fuse voice, data and video platforms; and communication and collaboration applications.

Organizations have been turning to UC systems for the variety of messaging, voice and video capabilities they offer including telephone switches, desktop applications, mobility products, and conferencing and collaboration tools.

Generally, UC offers five core capabilities, combined in some fashion to meet the specific needs to an organization:

- 1. Messaging:** This technology enables the sharing of information between individuals and devices using various communications methods including voice, e-mail, unified messaging, instant messaging (and presence).
- 2. Conferencing and collaboration:** This technology provides users with a more effective and productive means of interacting with each others through a combination of technologies including audio, web, video and whiteboard applications.
- 3. Mobility:** This technology extends the enterprise network telephone system to mobile networks.
- 4. Call control on the network:** This helpful technology offers the ability to do call parking, call forwarding and flexible number assignments including adds, drops and changes.

5. Presence: This useful technology allows network users to see others who are currently using the system, which facilitates communication among users. If a user is on e-mail, then a buddy list can notify other users to send a message to that user.

UC has made significant advances the past few years and is starting to fulfill its initial promise of a seamless user experience, regardless of location. But managing communications continues to be challenging for organizations as they navigate this continued expansion in communications technologies.

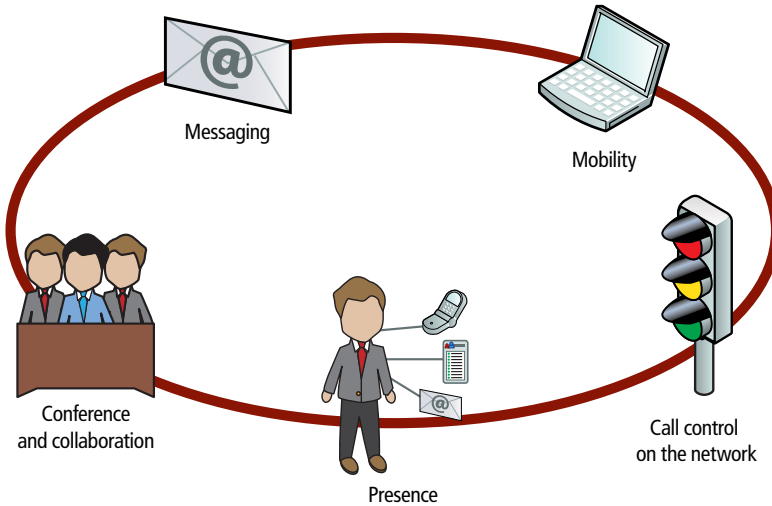
These technologies now expand communication further than ever from the user's desk and include such devices as the standard office telephone, mobile phones, PDAs, notebook computers, e-mail and video solutions. Integrating all of these disparate technologies has become increasingly essential for organizations, and UC is the answer.

CENTRALIZED UC MANAGEMENT

UC helps centralize your organization's communications, giving you improved management capabilities. Bringing UC solutions to a centralized and secure environment allows organizations to apply rapid changes to the entire organization as well as provide enhanced security and management.

A centralized solution allows an organization to easily and inexpensively add many more communication and collaboration applications to the network such as presence, instant messaging, desktop collaboration and emergency notification. With the advances in video conferencing from the desktop, web

THE 5 CORE UC CAPABILITIES



- **Enhance collaboration:** Staff can share availability information and instant messages with coworkers within the organization and between departments.
- **Streamline communications:** Users can view telephony status of their coworkers and click to call them.
- **Leverage presence-enabled operations applications:** Workers can share presence information and user communications capabilities in web directories and management systems.
- **Improve first-call resolution and end-user satisfaction:** This technology allows staff anywhere in the organization to handle incoming calls pertinent to their expertise.
- **Increase productivity:** Staff are able to connect with colleagues on the first try thanks to knowing their availability in advance.

conferencing and desktop collaboration, you can assign workers to locations anywhere within the organization regardless of job function.

This centralization of services is a boon for organizations, as staffers need to count on the delivery of communications services regardless of location inside or outside the organization. This ability to deliver consistent and tailored communication access to users based on their unique requirements and circumstances will yield a strong ROI for organizations that adopt a UC solution.

COMMUNICATION AND COLLABORATION APPLICATIONS

Advanced applications refer to the second tier of UC technologies, which are designed to enrich an organization's operations. These are applications that take advantage of converged networks, allowing coworkers to communicate and collaborate more effectively, enhance the communication itself, reduce costs and increase productivity.

PRESENCE

Presence applications are standards-based platforms that collect information from multiple sources about user availability and communications capabilities. The information is used to provide detailed presence status for coworkers and facilitate presence-enabled communications between them. This scalable and easy-to-manage solution can help workers:

With presence applications, coworkers can see the availability of others in the UC network instantly. This is a valuable communication tool, as recent research indicates that a reduction in staffer "wasted time" of up to 34 percent is possible when staff are able to view the availability status and the preferred communication methods of coworkers.

INSTANT MESSAGING

Often a part of a presence solution, instant messaging (IM) is a technology that creates the possibility of real-time, text-based communication between two or more participants over the Internet or some form of internal network or intranet. What separates IM from technologies such as e-mail is the perceived synchronicity of user communication. The speed of communication via IM versus e-mail is noticeably faster.

Many IM services have additional features such as immediate receipt of acknowledgment or reply, group chatting, conversation logging, file transfer and conference services.

Many organizations will allow for the "federation" of IM solutions. Federation allows users outside of the IM solution to be added to a user's IM contact list. This capability has proven quite valuable for organizations that need to maintain effective communications between departments, outside agents or representatives and others.

MOBILITY

Today's work environments have become increasingly mobile. The ability to connect to the right person depends not only on being able to view their availability, but also discerning what device to use to reach them. 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.

SINGLE NUMBER REACH AND SINGLE VOICEMAIL

UC single number reach technology gives users the ability to consolidate all of their call paths with a single IP phone number and immediately connect from wherever they are working. This helps organizations provide enhanced responsiveness with no additional effort. For mobile workers, this technology also reduces the burden on coworkers to have to share private mobile phone numbers.

With single number reach, mobile workers can also manage all of their voicemail using a single voicemail box. If a mobile call cannot be answered, the unanswered call is stored in the centralized UC voice messaging system or other organizational voicemail system.

Additionally, a staff member answering a call on a mobile device can seamlessly move the call to a physical desk phone upon physically entering the office. And a call started on a desk phone can equally be moved to a mobile device. This feature eliminates the need to hang up and redial a party or conference call already in session.

MOBILE VOICE ACCESS

Extending an organization's voice system to traveling staff is another great benefit of UC's communication and collaboration applications. Mobile voice access technology shares all of the major IP communications features with traveling workers.

For example, a mobile coworker who needs to call one of the organization's offices while traveling can use a mobile voice access line to place the call, which will be processed as if it came from the organization's home office. Dialing such a line from the mobile phone places the call on the organization's IP communications network over a tie line. This can lead to extensive savings on telecommunication bills for mobile staff.

CONFERENCING AND COLLABORATION

Regardless of user location, UC offers the ability for people to connect through voice, web and video services as well. This kind of enhanced collaboration further increases the value of UC when it is coupled with the ability to share and work on critical documents in a real-time format.

Whether in a one-on-one format or in a conference call

setting, collaboration technology permits the sharing of specific documents, computer desktops and applications. Some of the benefits of collaboration include:

- Encouraging innovation in operations processes;
- Increasing efficiency and minimizing wasted time;
- Making projects and resources available to multiple participants;
- Eliminating the need to pass a project back and forth between multiple stakeholders;
- Maximizing working relationships with coworkers, departments and outside agents.

THE CONTACT CENTER

Contact center technology extends a base UC solution into a true multifunctional contact center for either internal or external callers. Contact center technology utilizes the UC infrastructure to deliver skills-based contact routing, voice self-service, computer telephony integration and multichannel contact management.

By combining multichannel automatic-call-distributor functions with IP telephony in a single, unified solution, a contact center can assist an organization with rapidly deploying a distributed VoIP contact center infrastructure.

Interacting with the public and other stakeholders becomes much simpler and benefits from improved features. Contact center technology lets organizations segment callers, monitor resource availability and delivers each contact to the most appropriate resource in the organization.

The software profiles each caller contact using related data such as dialed number and calling line ID, caller-entered digits, web-form submitted data and caller database information. Simultaneously, the system monitors the resources available in the contact center to meet caller needs, including staff skills and availability, interactive-voice-response (IVR) status and queue lengths.

This combination of caller data and contact center data is processed through user-defined routing scripts that graphically reflect an organization's operations rules. And this processing enables the routing of each contact to the right place. Regardless of staff location, the system delivers a rich set of call-event and end-user-provided data to the targeted desktop as a contact arrives, helping the organization personalize service and increase its efficiency.

A centralized UC environment significantly enhances these solutions by allowing staffers to connect to the network from anywhere. Staff, for example, do not have to remain in a physical call center location but can function as a home-based agent that is securely connected to the organization's voice environment.

CONTACT CENTER ROUTING

The routing functions of a contact center setup provide for the intelligent distribution of contacts as they enter the organization's network, enhancing the overall caller experience. If a contact needs to be redirected, the contact center applies operations logic and sends the contact to the best available resource.

For contacts flowing between sites or among staff members, skill groups or IVR systems, the routing function optimizes each caller's interaction by retaining collected data, thereby eliminating the need for the caller to restate information all over again.

Contact center technology also expands the data resources available for making contact routing decisions and for populating staff desktop applications. For instance, the logic in the contact center can perform a lookup in the caller database during call routing in order to guide its decisions as to which call goes where. You can also use information from customer relationship management applications to match callers with staff and expand the data available to screen pop-up applications.

With a contact center system, end users can access the call center via a variety of communications methods. Traditionally, dialing into an 800 number was the only way to reach staff for communications, but multichannel support for unified centers can extend a user's reach beyond traditional voice to include direct web chat, e-mail and click-to-contact options.

In each of these cases, all of the collected end-user data can still be provided to the staff member accepting the communication, regardless of contact method.

VIDEO CONFERENCING

No discussion of UC would be complete without a look at the most significant advances in the technology, namely video. Being able to extend video services and collaboration to all users in a meeting, no matter the connectivity method, is a technological advance that is changing the way that organizations communicate.

The vast majority of all human communication is through visual cues. People regularly observe and assess subtle nonverbal cues from others in conversations. Video communications has (until recently) proven a difficult solution to deploy successfully and effectively in volume. However, UC technologies now embrace all facets of communication. Video has become the next logical step for an organization to include in its communications network.

Video conferencing technology has improved the user experience to a level where it is now a viable mode of communication internally among staff and externally with other departments and end users. The seamless blending of high-quality audio and video provides advantages to users on both sides of a virtual meeting. All of the participants are privy to the nonverbal cues that further contextualize and inform dialogue.

There are several additional benefits to be gained from extending

video communications across the organization.

Extension of UC platform: To maximize staff effectiveness, use of UC solutions should not stop at traditional forms of communication such as e-mail and phone. Video telephony conferencing can enrich the user experience at the desktop via a unified software client.

Increased workgroup collaboration: Video allows staff to maximize scheduling during the workday by eliminating travel between locations and incorporating access to operations-critical information and applications from the desktop.

Over the past few years, manufacturers have rolled out UC solutions that integrate former stand-alone communication methods such as voice and video. This integration has provided streamlining and optimization across the organization via both desktop and mobile devices.

Video telephony enables meeting or project participants to minimize delays that arise from participant handoffs. With video, information is more easily shared among team members.

Access for remote workers and teleworkers: Remote users often find it difficult to feel connected to colleagues. Video helps these staffers maintain viable, productive relationships in a way that audio-only teleconferencing cannot.

Reduction of travel expenses and carbon footprint: Budgetary challenges have made air travel prohibitive for many travelers. Even ground travel can now prove unreasonably expensive. Organizations and their work staff have begun to seek more cost-effective ways of meeting.

In conjunction with financial initiatives to limit travel, many organizations are taking on a social responsibility to decrease their carbon footprints. Peer-to-peer video conferencing can support the dual benefit of travel savings and green IT compliance.

MORE VIDEO OPTIONS

Deploying video communications within a UC solution has now become as simple as implementing traditional voice solutions. With the addition of video-capable phones or desktop cameras, the UC control mechanism can establish a video call automatically (if both parties have the capability for such service).

Along with desktop video conferencing, organizations can acquire feature-rich methods of video communications via telepresence solutions. Telepresence technology offers a fully immersive video conferencing experience, which is provided via an innovative "in-person" meeting experience that allows users to feel as though they are in the same room with other participants.

Telepresence delivers real-time, face-to-face interactions using advanced visual, audio and collaboration technologies. These technologies transmit life-size, high-definition images and spatially discrete audio, precise enough for you to discern participants' facial expressions. ◇

SECURING THE NETWORK



CHAPTER 5:

Role-based Server Security

Security Suites

Wireless Security

Cryptography: Authentication and Encryption

Network security needs to be addressed from several different angles. Securing your servers is at the heart of any durable security strategy. As Microsoft is the leading provider of critical server-side software, it plays a dominant role in addressing the challenges posed by a shifting threat environment, as well as increased demands by end users for greater access and interoperability.

There are many other solutions providers offering excellent server protection. However, many of the trends in server security revolve around Microsoft's server software.

ROLE-BASED SERVER SECURITY

Windows Server 2003 shed the "one-size-fits-all" model of security and introduced a model based on the notion that servers have differing security needs. These needs depend on the role they play within an organization's network scheme. A SharePoint server, for example, has security requirements above and beyond those of a file server. From a security perspective, the two server types cannot be treated identically.

The move to a role-based security model represented an evolutionary step in the development of security for the Microsoft Windows Server Platform. It began to provide platform security capabilities traditionally offered only by third-party software vendors. Microsoft Forefront Security, a suite of products designed for the existing Microsoft server platform, is the end result of Microsoft's role-based server security push.

The Security Configuration Wizard is at the center of Microsoft's efforts to streamline and homogenize Windows server security.

Using a wizard-based GUI, it walks 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).

The administrator has the ability to select important security settings and import or export preconfigured security templates. Once configuration is complete, the role-specific platform security tools mentioned above become functional. Forefront Security for Exchange, for example, provides robust security support for Microsoft's unified messaging server platform.

LEAST PRIVILEGE

Microsoft's role-based security configuration tool would have little value had it not also made significant changes to the server-application components of its operating system. In particular, Microsoft has invested heavily in threat mitigation around its Internet Information Services (IIS) offering.

IIS utilizes ISAPI (Internet Server Application Program Interface) filters to mitigate various URL-based attack routes and incorporates a highly restricted privilege model for executing server-side scripts and compiled content.

ACTIVE DIRECTORY SECURITY

Microsoft's directory services platform, Active Directory, has several unique risk-mitigation capabilities. Two features in particular allow organizations to better control access into their vital directory service assets: the ability to stop and start the

Active Directory service hosted on a domain controller, and the option to deploy “read-only” domain controllers.

Of course one vendor alone cannot address every single new security challenge and threat. Still, Microsoft’s threat and risk mitigation technologies make significant headway, providing organizations with capabilities that will more effectively keep their confidential intellectual property secure.

Every security engineer knows that a system is only as strong as its weakest link, and compromise at any layer can provide unauthorized parties access to sensitive data. For this reason, it is critical to secure from the bottom up. Role-based security for the operating system, supplemented by additional upper-layer application enhancements, will go a long way toward protecting an organization against security threats.

SECURITY SUITES

In addition to the push toward role-based security, another major trend in server security solutions over the last few years has been security suites. As security solutions have propagated, organizations have increasingly sought out best-of-breed solutions. Rather than seeking out particular solutions from multiple vendors, organizations have sought out solution suites.

These suites package together several security solutions, such as antivirus, antispymware, firewall, e-mail protection, intrusion prevention and device control, into one product. A central management console is a key feature in many security suites, which save the IT team’s time and resources when making updates or doing any kind of reconfiguration.

There are many security suite options available, with Symantec’s Endpoint Security, McAfee’s Total Protection and Trend Micro’s NeatSuite all offering substantial, multilayered protection for servers.

WIRELESS SECURITY

Another important angle to protecting your network is securing its wireless communications. More and more organizations are embracing easy-to-manage wireless architectures, with security being one of their top motivators. Controller-based wireless local area network (WLAN) systems have become the solution of choice.

In older, manually configured systems, every access point (AP) added to the environment increased the risk of misconfiguration and the potential inability of users to connect to the network. Thankfully, those days are gone.

Instead, WLAN systems now use a centralized controller that configures all APs in an environment. The controller pushes the specific configuration to the individual APs and monitors them.

Controller-based systems have many features that assist IT staff in enhancing the security of a network environment.

ROGUE DETECTION

Rogue APs are typically introduced into a wireless environment by work staff. Often, these individuals are attempting either to bypass security policies or provide wireless coverage in a work area that is not covered by the organization’s wireless network.

Some individuals who introduce rogue APs have more malevolent intentions. For example, a person wishing to tamper with personal data files may use a rogue AP to gain access to the organization’s wired network, and thereby gain access to other assets.

In a controller-based system with proper placement of legitimate APs, it is much simpler to pinpoint the location of a rogue via triangulation. Triangulation can have an accuracy rate of better than 95 percent.

Upon detection of a rogue AP, IT staff has several options for mitigating the threat. These include:

- Physically locating the rogue and removing it;
- Sending de-authentication messages to clients attached to the rogue AP;
- Using the system to locate and shut down the switch port to which the rogue has attached.

While most rogue APs are placed with good intentions, they present a major security risk that IT staff need to address.

PERIMETER CONTROL

Wireless infrastructures supporting perimeter control will refuse a user access to the network if the user’s signal lies outside particular parameters. This new type of access limitation is still being refined and does have one drawback. It cannot always distinguish with 100 percent accuracy whether a user is within the allowed area for wireless coverage or not.

Nevertheless, many manufacturers have placed a high priority on implementing perimeter control. Placing directional antennas on the building perimeter and pointing them toward the interior can help boost accuracy and minimize signal leakage. This tactic directs the radio frequency energy inward rather than outward, making it more difficult for an outside user to see and attach to the wireless network.

CRYPTOGRAPHY: AUTHENTICATION AND ENCRYPTION*

Traditional networks possess some physical barriers that complicate illegal access. But WLANs do not, so wireless security

*For more information on authentication and encryption, see Chapter 6.

relies heavily on cryptography to protect information. The two most prominent applications of cryptography in wireless networking are user authentication and traffic encryption.

AUTHENTICATION

Some organizations allow anyone within signal range to access their wireless networks and restrict access to private resources through other means. Other organizations consider their wireless networks private, only granting access to authorized users.

In order to facilitate this second scenario, it's necessary to verify the user's identity. There are many ways to accomplish this. By far, the most common set of approaches are variations of the extensible authentication protocol (EAP).

There are numerous varieties of EAP, and unfortunately this has created a lot of confusion. Each of these protocols use various cryptographic techniques in order to prove the identities of users and systems before allowing them to join the wireless network.

Both Wi-Fi Protected Access (WPA) and WPA2 require EAP authentication, which utilizes a backend authentication server to validate the end user and/or the device requesting access to the network. Some EAP types require client and/or server side certificates. Such types include, but are not limited to:

- EAP-TLS (transport layer security)
- EAP-TTLS/MSCHAPv2 (tunneled transportation layer security/Microsoft challenge handshake authentication protocol version 2)
- EAP-PEAP/GTC (protected extensible authentication protocol/generic token card)
- EAP-PEAP/MSCHAPv2 (protected extensible authentication protocol/Microsoft challenge handshake authentication protocol version 2)

Other EAP types, such as EAP-LEAP (lightweight extensible authentication protocol) and EAP-FAST (flexible authentication via secure tunneling), do not require certificates.

Differing opinions exist as to which EAP type is best. Generally, more mutual authentication makes for a more secure network. Mutual authentication reduces the risk of unwittingly attaching to a rogue AP. Keep in mind that the average user will not use the network if the authentication process becomes too complicated.

ENCRYPTION

Authentication alone cannot ensure the restriction of network access to authorized users only. By definition, wireless signals travel freely through the air, making wireless networks vulnerable to eavesdropping. To counter this threat, networks can elect to encrypt some or all traffic so that only authorized users (those

with the proper cryptographic keys) can decrypt and read network traffic.

Wired Equivalent Privacy (WEP) comes in either 40-bit or 128-bit key lengths. These keys can be either statically defined (on a per-network or per-session basis) or rotated dynamically over time.

With static WEP, the user enters a key once. That key never changes. Dynamic WEP, on the other hand, changes the key every few minutes. In the past, WEP alone served adequately to keep data safe. But today, WEP keys can be cracked within a matter of minutes or seconds if the intruder gathers enough data. Free tools are available on the Internet for just such a purpose, requiring little or no knowledge of wireless networking to make use of them.

Therefore, WEP alone should be considered unreliable and useless for data security. Depending on their age, some end devices may only support static WEP. These devices should be upgraded or discarded at the earliest opportunity.

WPA was introduced in October 2003 to address problems with WEP. It incorporates temporal key integrity protocol (TKIP) based on Draft 3 of the IEEE 802.11i standard. WPA comes in two varieties, personal or enterprise. Personal WPA uses a preshared key (PSK) that is statically entered into the client and the AP. The PSK can be between eight and 63 characters long, but for adequate protection it should contain at least 32 characters.

In addition, the PSK should incorporate a combination of upper- and lower-case characters, numbers and special characters. The PSK should be as random and complex as possible, containing no dictionary words, as it is generally only entered once.

PSK enterprise mode relies on an authentication server to generate the unique keys for each user. Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector. Combining TKIP with the much larger initialization vector defeats well-known key-recovery attacks that WEP has historically been prey to.

In addition to encryption, WPA provides payload integrity. WEP uses cyclic redundancy check (CRC). This leaves WEP insecure with regard to payload integrity because someone can alter the payload without knowing the WEP key. WPA instead uses message integrity code (MIC) in a frame counter to help stop replay attacks.

A replay attack occurs when an eavesdropper records some transaction on the network (for example, a user clicking the "submit" button on a web form) and simply replays the same packets. If the network (or, in this case, the web application) is not protected against replay attacks, it would appear as though the user had clicked the button twice.

While not foolproof, WPA using MIC is nevertheless superior to

WEP for replay attacks and should be utilized if your organization's devices do not support anything stronger.

WPA2, ratified in June 2004, uses all the elements of the IEEE 802.11i standard. In addition to TKIP and MIC, WPA2 utilizes the newer and stronger algorithm known as counter-mode/CBC-MAC protocol (CCMP), which is based on the Advanced Encryption Standard (AES). AES is a 128-bit encryption method that represents the next generation of encryption.

The federal government requires AES for all of its online transactions. AES also meets all the requirements for Federal Information Processing Standards (FIPS) 140-2, and includes a mechanism for key caching that allows for faster client reauthentication.

Given the option, users should always choose WPA/WPA2 over WEP. All Wi-Fi compliant devices built after March 13, 2006, meet WPA2 standards. Most AP manufacturers allow for a mixed mode of WPA and WPA2 clients on the network. Organizations should strongly consider moving to a wireless network using WPA2 enterprise because it currently provides the greatest assistance in securing all valuable assets.

WIRELESS ENDPOINT ATTACKS

Users should realize that, by default, most wireless cards and their control applications allow for the formation of ad hoc networks. A simple example of an ad hoc network would be one notebook attaching to another to share files. Ad hoc networks, while convenient, create problems when a device attached to the wired side of an organization's network has its wireless card

functioning. A hacker can easily attach to the notebook wirelessly and use it to gain access to the wired network.

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

The problem doesn't stop there, however. A clever attacker can also impersonate a legitimate wireless AP. Traffic sent by users associating with "evil twin" APs is subject to interception or alteration. "Man-in-the-middle" attacks of this nature can be defeated using varying combinations of the cryptographic controls described here.

REVIEW SECURITY FEATURES

Wireless networking, when properly implemented, has become more secure than ever. Most manufacturers have advanced security features deactivated on new equipment to make it easier for users to attach to the network without a lot of configuration. Unfortunately, though, most people don't take the time to change the default settings.

In addition, many organizations assume that because they haven't deployed a wireless network, wireless security isn't an issue for them. Unfortunately, this isn't the case. For example, nearly every organization has some notebooks, and nearly every notebook comes with a wireless interface enabled by default.

As mentioned above, these interfaces can expose a notebook to attack, even if the organization has no wireless infrastructure of its own. So organizations need to get into the habit of reviewing the security features of all devices that can connect to a wireless network prior to initial user access to the device. ♦





WIRELESS MOBILITY

CHAPTER 6:

Designing Your Wireless Network

Working with 802.11n

Central Control

Conducting a Site Survey

Encryption and Authentication

Failover and Redundancy

Today, many organizations have come to rely on their wireless networks as a key aspect of their operations. Wireless networks no longer offer simply data connectivity, but help deliver and support a variety of user applications, such as VoIP. Increases in wireless local area network (WLAN) capabilities, reliability and security features have helped spur the broad adoption of wireless technology.

With wireless technology now playing such an integral role in an organization's network operations, it is important to plan out and build this complicated resource so that your organization can reap as much benefit from it as it can.

DESIGNING YOUR WIRELESS NETWORK

The first step when setting up a WLAN is deciding what equipment to use. You may not know at first how many access points or controllers you will need, but this can be determined later when conducting the wireless site survey.

When shopping for wireless equipment, there are a few key features that you should keep in mind. The first is radio frequency. The 802.11n wireless networking standard was recently ratified. 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 over the past few years.

You want to be sure to purchase equipment that is compatible with 802.11n. And with 802.11n equipment, you will need a gigabit connection to each AP in order to provide the increased bandwidth that your network will require.

WORKING WITH 802.11N

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

1. Look for modular access points. The current generation of 802.11n products don't yet support the full theoretical potential of 600Mbps speeds. Modular products allow you to more easily swap out the networking cards (to facilitate an easier migration to 802.11n). But keep in mind that 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 are:

- **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 AP with improved performance because it uses some of the 802.11n physical layer enhancements. 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. Some 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 and 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. A new standard, 802.3at, promises to supply up to 24 watts, but it's not ready yet.

Power requirements of 802.11n access points are all over the map: Some manufacturers require more than 15.4 watts, others claim to work within the current standard. If you're using APs that claim to work with standard 802.3af power, be sure you understand exactly how much power the AP requires and how it behaves if it gets less than that.

For example, some 802.11n APs start scaling back functionality if they don't receive enough power. If your manufacturer's APs require more power than 802.3af can deliver, your options include prestandard 802.3at switches from manufacturers such as Cisco Systems, or midspan PoE injectors from manufacturers such as PowerDsine. Whichever you choose, your best bet is to test the switches and APs in a real-world environment before you go live.

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 new products are downright cumbersome, with as many as six antennas.

This may sound trivial, but you don't want to put ugly gear on the walls or ceilings of your organization's buildings. You may also have to hide APs in a drop ceiling, which could become an issue if it interferes with the wireless signal, putting a damper on performance. In some cases, you may need to plan on rolling out a few extra APs to provide solid coverage.

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; the APs were essentially dumb radios, and all the intelligence resided in centralized controllers.

There's now some concern that with the increased throughput of 802.11n, the centralized controllers (and the uplinks to them) won't be able to handle all the traffic. Whether or not this is an issue for your network will depend on your deployment size, the location of your controllers and the usage patterns. While there's no right or wrong answer, it's an issue you should understand and monitor as you roll out 802.11n.

5. Focus on spectrum and channel planning. The growing consensus is that the 5 gigahertz spectrum is best for enterprise wireless because it is a much cleaner space than 2.4GHz. The issue is complicated because 802.11n allows you to run in either the 2.4GHz or 5GHz space. You'll need to decide which frequencies to use, and whether you want to support the legacy 802.11a/b/g protocols.

Many of the 802.11n APs on the market feature dual radios, a good choice at least for the next few years because many of the notebooks you'll support will work only with those legacy standards. If you haven't deployed 802.11a widely, consider using one radio to run 802.11n in 5GHz and the other to run 802.11b/g in 2.4GHz.

You could also add 802.11n to the mix in 2.4GHz, but keep in mind that it limits your ability to enable channel bonding, a performance-enhancing feature in 802.11n that lets you "bond" two 20-megahertz channels into one 40MHz channel. Because 2.4GHz allows for only three nonoverlapping channels, you'll be able to run only one 40MHz bonded channel, which would severely limit your deployment options.

CENTRAL CONTROL

After access points, the second key feature that you will want to look for is a wireless controller that allows for central management of your WLAN. 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 organization. By providing such benefits, a properly deployed WLAN controller can prove a powerful security asset.

CONDUCTING A SITE SURVEY

Now that the equipment has been selected, you are ready to start your site survey. This might be the single most important phase of the deployment.

The purpose of the site survey is to determine coverage areas and locate dead spots in your buildings. A site survey may indicate areas where you need to place additional access points, as well as areas where you can forgo an access point or two. If you already have a WLAN, you might improve your network by using some wireless analysis tools and examining your coverage area.

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 your site survey tool understands 802.11n to get an accurate survey.

Active survey products such as AirMagnet have been updated to communicate with 802.11n networks. Many wireless manufacturers are in the process of upgrading their predictive survey tools to understand 802.11n, but you need to be sure — so ask.

One workaround if you are 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 if you want to support legacy protocols. However, if you’re doing a greenfield installation and plan to support only 802.11n, you’ll be best served by a newer site survey tool.

There are other tools out there for analyzing a wireless network, both free and for purchase. NetStumbler is an open-source product that many network administrators use when tracking wireless issues. NetStumbler will allow you to see different access points, the channels they are operating on and the signal strength they’re receiving.

Fluke Networks has an entire line of products designed to help troubleshoot or design wireless infrastructures. The InterpretAir software is a site survey tool that can be used to map the network, as well as determine coverage areas based on the WLAN

equipment in use. Trapeze Networks has a site survey tool that can tell you exactly where to place your APs after you run through a wizard that asks about your building construction and user locations.

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, despite offering a large coverage area. By having a higher concentration of APs, 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 to restart an AP in the event of a malfunctioning unit.

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, you must first identify all the device types that will utilize the WLAN. Identifying the devices allows you to define the security capabilities of each. Some devices support a wide variety of authentication and encryption types; others support a much smaller set.

You should also take into account an evaluation of the levels of security required by the organization, 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

*For more information on encryption and authentication, see Chapter 5.



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.

As mentioned in Chapter 5, there are two main types of encryption used on WLANs at present: WEP and WPA. WEP encryption is substantially weaker than WPA, but depending on what kind of data you are trying to protect, it may be a good fit. For instance, if you are using WEP to encrypt nonessential data, you should be fine.

However, 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, which in the case of 802.11x involves hitting your RADIUS or authentication servers and could cause logon delays.

If you decide to go the 802.11x route, you may need additional logon servers or RADIUS servers to handle the authentication and keep the rest of your network performing adequately.

VLANS AND TUNNELING

Secure guest user access to the Internet is a common requirement for today's WLANs and can drastically increase productivity and effectiveness. Your organization 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 your organization to tunnel all guest user traffic to a secure location, typically outside of the firewall. Web pages served by these controllers also allow the organization to restrict access to the guest network 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 your organization 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. Check to see whether your APs can have "master" and "slave" controllers that will allow them to switch automatically to the controller that is online.

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

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.

CLOUD COMPUTING

This term refers to a computing arrangement that emphasizes the sharing of resources. Cloud computing separates the data center into an application cloud, a hardware cloud and a computing cloud. This allows applications to be separated from specific hardware locations and allocated across the network as needed, thus making for easier management, better resiliency and lower costs.

CONSOLIDATION

Consolidation is an efficient approach to utilizing server resources in order to decrease the total number of servers and/or server locations that an organization is using. This is facilitated by removing applications and data from remote offices and placing these resources in a central data center, and also by consolidating individual applications and their related storage.

CONTACT CENTER

A multifunctional contact center available to both internal and external callers, a UCC offers skills-based contact routing, voice self-service, computer telephony integration and multichannel contact management. It can segment callers, monitor resource availability and deliver contacts to the most appropriate resource in the organization.

DICTIONARY COMPRESSION

This term refers to a technique used to reduce bandwidth needed to send large files and large amounts of data. A WOC learns the patterns of data being transmitted over the network. When it detects the same pattern again, the WOC substitutes the data pattern with a reference number, and a receiving WOC (that is

learning the same patterns) will identify and swap back in the substituted data for the reference number.

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

EAPs are universal authentication protocols that have mutated into numerous variations. They use a variety of cryptographic techniques to verify the identities of users and systems before allowing them to join the wireless network.

FIBRE CHANNEL OVER ETHERNET (FCOE)

FCoE enables SAN traffic to travel over an Ethernet network. This traffic moves across the link layer and uses Ethernet to transmit the FC protocol. The benefit of this approach is that it allows a seamless integration between FC networks and network management software.

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

Load balancing is a data center technique where processing work is split between two or more computers so that the work gets done in the same amount of time. All network users receive faster service as a result.

MOBILE VOICE ACCESS

This technology shares all of the major IP communications

features with remote staff, allowing them the same access to the organization's voice system as though they were at their desk.

POWER OVER ETHERNET (POE)

This networking technology allows electrical power to be 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

Presence is a platform that collects information about internal user availability and communications capabilities. This 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.

SECURITY SUITE

Security suites package together several helpful security solutions, such as antivirus, antispyware, firewall, e-mail protection, intrusion prevention and device control, into one product. Central management is a key feature of security suites, saving IT teams time and resources.

SINGLE NUMBER REACH

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

STORAGE AREA NETWORK (SAN)

A SAN consists of a high-speed special purpose network (or subnetwork) that interconnects different kinds of data storage devices with associated data servers on behalf of a large network of users. Although the storage devices are remote, they appear to be locally attached to the operating system.

TELEPRESENCE

This term refers to a set of 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 location. Telepresence also allows the user to affect the remote location by transmitting the user's movements, actions, voice, etc.

TEMPORAL KEY INTEGRITY (TKI)

The TKI protocol is used with the WPA standards, improving data encryption by scrambling the keys using a hashing algorithm and by utilizing an integrity-checking feature.

TIA-942

TIA-942 is a standard published by the Telecommunications Industry Association (TIA). It lays out the requirements and guidelines for the design and installation of a data center, covering facility planning, the cabling system and the network design.

UNIFIED COMMUNICATIONS (UC)

UC generally refers to a "one-wire" infrastructure where numerous systems such as e-mail, voicemail, cell phones, PAs, printers and Internet all reside on a single data and VoIP network. Emergency notification systems can make use of a UC setup as well.

VIRTUALIZATION

Virtualization is a broad term that generally refers to the creation of a virtual version of a device or resource (such as a PC desktop or a server) that is then located on a partitioned execution environment, such as a server. Several virtualized versions can exist in the same environment once it is partitioned. The virtualized versions can be accessed via the execution environment, with the accessing user interacting as though it were a single, logical resource.

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 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 standard developed to replace WEP, WPA utilizes TKIP protocol and EAPs to secure wireless traffic. WPA2 builds on WPA, extending stronger data protection via Advanced Encryption Standard (AES) to personal users and enterprise users.

WIRELESS EQUIVALENT PRIVACY (WEP)

WEP is a wireless security protocol for WLANs that utilizes encryption. It is now considered unreliable when used alone. WPA was developed to address WEP's vulnerabilities.

INDEX



| | | | |
|--|---------------|--|-----------|
| 802.11n | 29-31 | Pre-shared key (PSK) | 27 |
| Authentication | 26-28, 31-32 | Quality of Service (QoS)..... | 10-11 |
| Blade servers..... | 6 | Rogue detection..... | 26 |
| Centralized UC management | 21-22 | Role-based server security | 25-26 |
| Cloud computing | 8 | Security suites | 26 |
| Collaboration | 21-22, 23, 24 | Server virtualization | 7-8 |
| Communication and collaboration applications | 22-23 | Single number reach | 23 |
| Contact center | 23-24 | Storage area network (SAN) | 7 |
| Data center consolidation | 6-7 | Storage consolidation..... | 7 |
| Data center overhaul..... | 5-7 | Telepresence | 4, 24 |
| Dictionary compression..... | 9, 11 | TIA-942..... | 5 |
| Encryption..... | 27-28, 31-32 | Unified communications (UC) | 4, 21-24 |
| Extensible authentication protocol (EAP) | 27 | Video conferencing | 21, 24 |
| Fibre Channel..... | 7 | Virtualization..... | 3-4, 5, 7 |
| Fibre Channel over Ethernet (FCoE)..... | 7 | Virtual local area networks (VLANs)..... | 32 |
| Instant messaging (IM) | 21, 22 | WAN optimization controllers (WOCs)..... | 9-11 |
| Load balancing..... | 11 | Wi-Fi Protected Access (WPA) | 27-28, 32 |
| Power over Ethernet (PoE) | 30 | Wired Equivalent Privacy (WEP)..... | 27-28, 32 |
| Pre-built virtual machines | 7 | Wireless endpoint attacks..... | 28 |
| Presence..... | 4, 21, 22 | Wireless security | 26 |

Disclaimer

The terms and conditions of product sales are limited to those contained on CDW•G's website at CDWG.com. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. For all products, services and offers, CDW•G® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. CDW®, CDW•G® and The Right Technology. Right Away.® are registered trademarks of CDW Corporation. All other trademarks and registered trademarks are the sole property of their respective owners. CDW and the Circle of Service logo are registered trademarks of CDW Corporation. Intel Trademark Acknowledgement: Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel Viviv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Viiv Inside, vPro Inside, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. AMD Trademark Acknowledgement: AMD, the AMD Arrow, AMD Opteron, AMD Phenom, AMD Athlon, AMD Turion, AMD Sempron, AMD Geode, Cool 'n' Quiet and PowerNow! and combinations thereof are trademarks of Advanced Micro Devices, Inc. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a \$250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding networking and unified communications technology. CDW•G makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding networking and unified communications implementations. Furthermore, CDW•G assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication. The content contained in this publication represents the views of the authors and not necessarily those of the publisher.

©2010 CDW Government, Inc. All rights reserved.



CDWG.COM/NETWORKING-UCGUIDE
888.676.4239



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). »



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. »



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. »



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.



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.



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

100119 • Flyer 75738

LOOK INSIDE for more information on:

- Protecting against wireless endpoint attacks
- Utilizing WAN optimization controllers
- Upgrading your unified communications capabilities
- Taking advantage of 802.11n improvements

