

# NETWORKING AND UNIFIED COMMUNICATIONS

## REFERENCE GUIDE



Simplifying  
communications  
for an evolving world.

[CDWG.com/networking-ucguide](http://CDWG.com/networking-ucguide) | 888.676.4239



The Right Technology. Right Away.®

# NETWORKING AND UNIFIED COMMUNICATIONS

## REFERENCE GUIDE

### TABLE OF CONTENTS CHAPTER

### WHAT IS A CDW•G REFERENCE GUIDE?

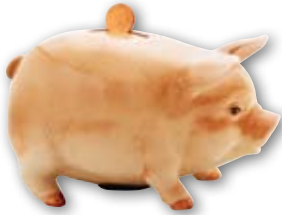
At CDW•G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology. Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face.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

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

<b>01</b>	<b>Introduction to Networking and UC</b> .....	<b>3</b>
	• Increasing Functions vs. Reducing Costs	
	• Network Solutions Trends	
	• Unified Communications Trends	
<b>02</b>	<b>The Data Center</b> .....	<b>5</b>
	• Return of the Consolidated Data Center	
	• Cloud Computing	
	• Consolidation Benefits	
	• Resilient Networks	
<b>03</b>	<b>Application Optimization Services</b> .....	<b>9</b>
	• Fine-tuning Application Functionality	
	• The Benefits of Application Optimization	
	• The Next Generation	
<b>04</b>	<b>Unified Communications</b> .....	<b>21</b>
	• Centralizing UC	
	• Advanced Applications	
	• Unified Contact Center	
	• Unified Video	
<b>05</b>	<b>Security</b> .....	<b>25</b>
	• VPN Varieties	
	• Virus and Worm Protection	
	• Firewalls	
	• Intrusion Prevention Systems	
	• The Evolving Perimeter	
<b>06</b>	<b>Mobility</b> .....	<b>29</b>
	• Centralized WLAN	
	• WLAN Security Strategies	
	• Successfully Deploying VoIP-over-wireless	
	<b>GLOSSARY</b> .....	<b>33-34</b>
	<b>INDEX</b> .....	<b>35</b>

# INTRODUCTION

## TO NETWORKING AND UNIFIED COMMUNICATIONS



### CHAPTER 1:

Increasing Functions vs. Reducing Costs

Network Solutions Trends

Unified Communications Trends

Organizations are constantly seeking to increase and improve operational capabilities while decreasing costs. And as network infrastructure continues to grow into an integral part of any organization's operations, the network now plays a profound role in this equation.

Many organizations cannot operate without a robust, resilient and responsive network. Great care must be given to designing, implementing and operating a network. In order to develop viable network solutions, one must consider a variety of factors and challenges.

### INCREASING FUNCTIONS VS. REDUCING COSTS

IT managers have a difficult task in attempting to offer robust services and applications while reducing operational costs. Applications continue to become more complex, and the applications' reliance on a resilient network continues to become even more pronounced. Software manufacturers increasingly create applications that utilize the resilient nature of IP and assume a high level of service availability for those applications.

IT infrastructures must provide dynamic and scalable services that not only deploy easily, but also allow organizations to add functionality as the organization requires it. IT managers, for their part, have an obligation to decrease the total cost of ownership (TCO) and increase return on investment (ROI), while still meeting the functional challenges of the data center.

In seeking to meet these sometimes conflicting needs, technical managers consistently work 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 critical to an organization.

### NETWORK SOLUTIONS TRENDS

Some of the network solutions that currently perform the function of enhancing an existing network infrastructure include application control engines (ACEs) and Wide Area Application Services (WAAS).

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

The proliferation of continuity of operations solutions has resulted in a strong need for redundancy in the form of network-based storage. Organizations need network storage devices that provide a scalable solution independent of traditional distance constraints.

Many server managers have thus leveraged their existing server resources through virtualization, using the network to distribute applications over a larger IT landscape. This added functionality requires network solutions that are highly integrated, scalable, robust and easily managed.

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

## UNIFIED COMMUNICATIONS TRENDS

Having laid network foundations with local area and wide area solutions, application functionality and productivity for the staff becomes a primary concern. With unified communications (UC), IT departments can offer streamlined communications solutions and advanced productivity applications throughout the network environment.

Because of the facets it incorporates and combines, UC is a powerful and complete communications medium for organizations. It has unquestionably changed, for instance, the way organizations address all facets of connecting with work staff.

Whether sitting at a desk, residing at a branch office, working from home or connecting via cell phone, a staffer must have access to the same services and level of functionality. Today's combined advances in networking and UC allow the IT staff to permit exactly such a scenario.

Advanced UC applications, for example, allow end users to see in real time the status and availability of other coworkers, including

preferred methods of contact. With this level of insight, coworkers can quickly determine which fellow coworkers are accessible and in what capacity.

Mobility solutions further extend the capabilities of the communications network beyond the confines of the organizational environment. Regardless of location, mobility can provide Presence and voice communications via smartphone technology as if a coworker were physically within the "brick and mortar" office.

Video communications and desktop collaboration have emerged as two of the most recent UC solutions. Both provide tremendous benefits. Eighty to 90 percent of human communication is based in visual queuing. So video serves as a logical extension of the UC network.

Whether video communications are accomplished point-to-point via desktop integration or by means of a full-scale TelePresence solution, they allow 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 communication environment.

With the right network infrastructure, the power that UC offers, as well as the newest network solutions, can propel an organization much more easily and efficiently toward its important goals. ♦



# NETWORKING AND UNIFIED COMMUNICATIONS: THE DATA CENTER



## CHAPTER 2:

Return of the Consolidated Data Center

Cloud Computing

Consolidation Benefits

Resilient Networks

In the 1980s, a paradigm shift in data center design occurred with the separation of applications and data between individual servers and desktops. This trend led away from the traditional “mainframe” data center to a proliferation of hundreds, even thousands, of servers. Each of these servers usually hosted individual applications and some level of local storage.

In addition, a need arose to host applications and storage at remote offices because of slow bandwidth from the home office. This paradigm led to a strong degree of duplication, and the increasing complexity that resulted required an infrastructure equal to the task of supporting it.

In particular, power and cooling for all the servers and desktops, IT staff and management software became infrastructure priorities, along with a large network to tie everything together.

## RETURN OF THE CONSOLIDATED DATA CENTER

More recently, another paradigm shift has begun. Bandwidth and energy cost increases, coupled with increasingly complex IT environments, have led many organizations to consolidate their infrastructure by removing applications and data from remote offices and staff PCs and placing it all into a centralized data center instead.

Consolidating individually siloed applications and their related storage has become another consolidation strategy.

As more and more organizations shift to a consolidated data center, it’s important to keep in mind that the network of today

must function as more than simple plumbing. It takes a highly skilled network architect to design the type of complex networks needed for a consolidated data center, and a seasoned systems engineer to implement them.

And with the onset of VoIP, videoconferencing and streaming media, the network has become even more critical to operations than ever before. Recommendations have thus become extremely valuable concerning the design and implementation of a complex and highly resilient network. As we will see, organizations need to put a great deal of planning and thought into any consolidation activities.

## CLOUD COMPUTING

Ultimately, many IT departments now aim to achieve a “cloud computing” environment, with applications essentially “removed” from the hardware, allowing for more efficiency, easier management, better resiliency and lower overall IT costs.

Cloud computing involves separating the data center into an application cloud, a hardware cloud and a compute cloud for high-performance computing and communications (HPCC) environments. Rather than tying specific applications to hardware (such as servers, network ports, etc.), the applications can be separated and managed as independent clouds.

As a result of this independence, the applications can move from server to server, or even data center to data center, without performance degradation or data loss. Hosting applications that formerly resided on individual desktops further enables users to access necessary applications from anywhere.

For a long time cloud computing involved substantial testing, since applications needed to allow for “one-to-many” sharing. This sharing was accomplished via terminal services, which not all applications would support. Today, however, many more options exist for hosting shared applications, including but not limited to application virtualization, desktop virtualization and blade PCs.

Organizations can gain numerous benefits from a shared application cloud. Disaster recovery, in particular, is an area that can benefit from this arrangement. For example, if the staff of an organization can't get to the office because of a disaster, remote access to centralized applications allows users to securely obtain what they need from the safety of a home computer or other remote device or location.

## CONSOLIDATION BENEFITS

Consolidating the data center allows organizations to provide powerful, rich applications, to simplify management, to build in strong redundancy and to strengthen security. And consolidation technologies facilitate 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 demands 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.

## STORAGE CONSOLIDATION

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, since virtualized servers reside on the storage area network (SAN).

Until recently, this fact had little impact on the Ethernet network. Now, however, a convergence of technologies has begun.

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

An even newer technology is Fibre Channel over Ethernet (FCoE). 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, as it requires low latency, high throughput and built-in resiliency.

## RESILIENT NETWORKS

A network's primary purpose is to support the organization's functions. So when designing a resilient network, one must first determine the requirements to support those functions and develop a network strategy accordingly.

Upper level management and the various departments of the organization can help substantially in establishing operations requirements. In most organizations, an IT governance committee consisting of upper-level management helps establish the operations requirements of the network.

## NETWORK ASSESSMENT

Upon establishment of the requirements and development of a network strategy, the planning phase can begin. Planning includes performing an accurate assessment of the current environment and a gap analysis to determine if the existing infrastructure, sites and production environment can scale to include a new, resilient infrastructure.

The assessment should take into consideration the following:

- Current applications and data on the network, such as VoIP, e-mail, structured query language (SQL), common Internet file system (CIFS), Internet and video-on-demand
- Current network topology, including but not limited to: network devices, physical and logical links, external connections, frame types, routed and routing protocols, application specific protocols, and IP addressing schemes
- Traffic and network utilization analysis

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

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

## DESIGNING THE NETWORK

Actual design of the network is the third step in building a resilient network. The network design must incorporate all gathered information concerning operations and technical requirements. It must also include specifications for availability, reliability, security, scalability and performance.

Network engineers commonly recommend designing a resilient network in modules. Modules allow an organization to provide the highest degree of resiliency by segmenting traffic and preventing a single point of failure.

For example, in the diagram below, the campus network consists of access, distribution and core modules. The access module provides Layer 2 connectivity to workstations and end users. It connects through redundant links to the distribution module.

The distribution module provides routing between users in the access module and other advanced features such as quality of service (QoS), gateway redundancy and other security features. The distribution module connects to the core module utilizing

multiple high-speed Layer 3 links in order to take advantage of high convergence of advanced routing protocols. The core module provides high-speed switching to other modules in the infrastructure.

## RESILIENCY AT LAYER 2 AND LAYER 3

In designing resilient networks, it is crucial to eliminate single points of failure. This effort includes having redundant links to critical servers and network devices. Redundant links can create problems, however.

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

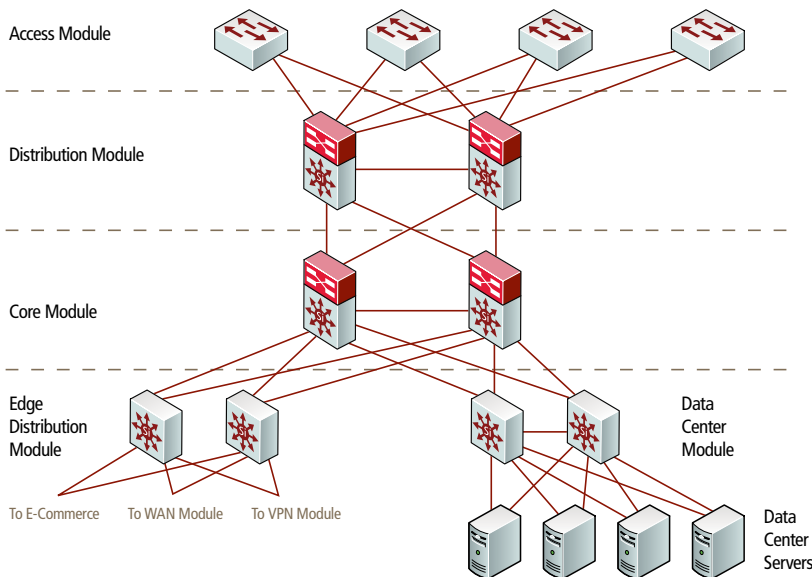
Spanning tree protocol (STP) is a Layer 2 protocol designed to prevent such flooding by placing one of the redundant links in a blocking state. Although STP prevents Layer 2 loops, it is slow to converge. STP improvements (such as Rapid STP) help decrease the convergence time.

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

Aggregate redundant links at Layers 2 and 3 are a common best practice to increase resiliency.

Technologies, such as EtherChannel, combine switched or routed links into one logical link, effectively doubling the bandwidth on the link and minimizing convergence. Since the switch or router sees aggregated links as a single link, traffic continues to flow through the other links if one of the links fails. ♦

## AN ACCESS, DISTRIBUTION AND CORE MODULES SETUP



# Gigantinormous.

It's the only word we could come up with to describe our Configuration Center capabilities.



The CDW® Configuration Center can handle your configuration needs. Our A+ and vendor-certified technicians can custom configure, image and test hundreds of systems every day. And that's just the beginning. We handle everything from basic installation of hardware and software to high-end enterprise configuration services at one of our three Configuration Centers. We offer a variety of services to keep your organization up and running at optimum efficiency.

Get configured. Call 800.808.4239  
or visit [CDWG.com](http://CDWG.com)

The Right Technology. Right Away.™



# NETWORKING AND UNIFIED COMMUNICATIONS: APPLICATION OPTIMIZATION SERVICES



## CHAPTER 3:

Fine-tuning Application Functionality

The Benefits of Application Optimization

The Next Generation

Application optimization services are one of the fastest growing network solutions in today's data center. The primary benefits of these technologies are that they accelerate applications and decrease their response times.

They also provide additional security features for the applications and enhance their availability for users. As applications become more critical to organizations, the ability of those applications to function efficiently has likewise become increasingly important.

## FINE-TUNING APPLICATION FUNCTIONALITY

Application optimization aims to increase the response time of operations applications over wide area network (WAN) connections. Typical data networks carry a variety of traffic types that possess different priority levels and functions. Network managers are always looking for ways to increase response times for the more critical applications without expending a large amount of capital toward bandwidth.

Organizations also look for ways to decrease latency while moving to a more centrally managed system. However, Internet traffic is increasing at an exponential level. Web servers increasingly serve more and more web pages to end users, resulting in an alarming increase in response times. Increased response times result in servers becoming overutilized.

Consequently, networks are increasingly attempting to offload CPU-intensive web services, such as Secure Sockets Layer (SSL), to network devices in order to use CPUs as minimally as possible.

In a 2007 study titled "Magic Quadrant for WAN Optimization Controllers," the research firm Gartner cited the following reasons that cause increased response times for organizations on their critical applications:

- Traffic that isn't time sensitive, such as e-mail, backups and personal web access, can swamp WAN links, leading to slow response times for operations-critical applications.
- Global centralization of branch office servers and data centers can expose latency-sensitive protocols, also leading to slow response times.
- File transfers, operating system patch distribution and similar applications (such as the delivery of training videos) can quickly saturate WANs.
- Repeated transmission of the same or similar files, objects or data patterns can create opportunities for data compression.

## FUTURE DEVELOPMENTS

The consumer market has driven much of the development of application optimization technology. There has been a growing demand for integrated solutions that offer a wide array of functionality. Manufacturers have responded by providing redundant and highly complex application optimization solutions.

Future developments will likely include application optimization products that provide generic traffic control such as HTTP, TCP, FTP, etc. Another area ripe for development is application optimization solutions that provide traffic-shaping functionality for unique applications and vertical markets.

## THE BENEFITS OF APPLICATION OPTIMIZATION

Organizations currently deploy application optimization solutions in the data center and branch offices for numerous reasons, including faster deployment of applications. IT departments can dynamically respond to changing operations demands by rapidly

provisioning network infrastructure. This helps bring applications into production in a more timely and cost-effective manner. Some of the benefits include:

- **Better return on investment, greater efficiency and utilization:** Organizations can reduce those costs associated with scaling server farms and centralized applications by optimizing the use of existing server resources and offloading nonessential server functions to the network.
- **Increased staff and end-user satisfaction:** Improved application response times result in higher staff and end-user satisfaction, increased productivity and greater operations efficiency for the organization.
- **Consolidation of branch-office servers:** Large numbers of file and print servers and storage devices in branch offices represent both significant operating expenses and data protection risks. Branch office consolidation creates initiatives to move branch servers to data centers.

Also important to consider is the recent rise in application-based attacks, which most traditional firewalls do not repel effectively, if at all. With application optimization, however, such threats are addressed not just at the network layer, but at the application layer, better protecting the integrity of an organization's systems.

## THE NEXT GENERATION

IT decision-makers face the challenge of providing reliable and acceptable applications and service to users while responding to consolidation, budget constraints and regulatory compliance. This is no easy feat. But application optimization provides a way to satisfy all of these demands.

Application optimization offers a portfolio of application networking products and technologies that enable organizations to deliver end-to-end operations processes across their entire infrastructures and to all users everywhere, while optimizing the resources needed to accomplish this task.

A couple of newer application optimization services that IT departments should take a closer look at are application control engines (ACEs) and Cisco's Wide Area Application Services (WAAS).

## APPLICATION CONTROL ENGINE (ACE)

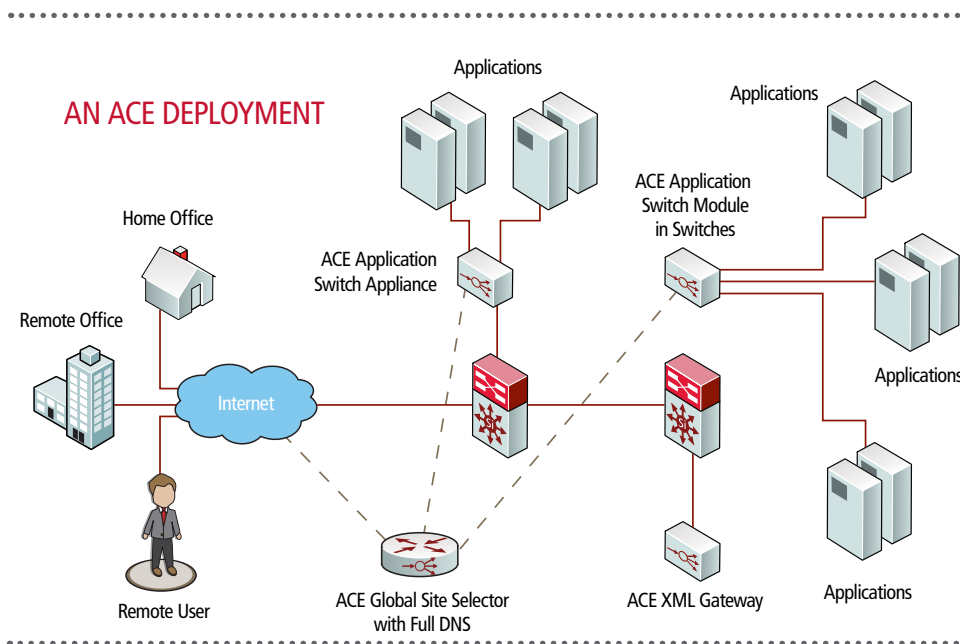
ACE devices represent the next generation of application networking. They maximize throughput, acceleration, availability and security for critical operations applications. Traditional networks have leveraged the network layer to provide redundancy, load-balancing and security functions for such applications.

The traditional Layer 3 provided sufficient functionality for this purpose until user traffic started to surpass network capacity. Organizations had to deal with serving increased web traffic without sufficient capital expenditures. The need for efficient use of existing network resources became apparent. Organizations began to demand products that would provide network-based applications with flexibility, scalability and redundancy.

ACE modules offer exactly what organizations are looking for; they allow organizations to accomplish primary IT objectives for the delivery of applications. And they allow organizations to:

- Accelerate application response times
- Protect applications at Layer 7
- Provide redundancy for network applications
- Permit more efficient use of existing data center resources

The following diagram illustrates how a potential ACE deployment would look in a production environment.



ACE modules deliver a broad set of features, providing functionality from Layer 3 to Layer 7. The capabilities of a traditional network cannot extend beyond Layer 4, restricting control over certain features inherent in network applications. ACE devices can provide control at Layer 7, making them more relevant to the applications they support.

For example, ACE devices improve application efficiency through traffic management and the ability to offload CPU-intensive functions such as SSL encryption, HTTP compression and user-based management. The ACE modules can take highly intensive tasks, such as encrypting and decrypting SSL sessions, and move them to hardware-based ASICs (acoustic sensor control and integration system, or microprocessors).

They also provide a last line of defense for network applications. In traditional networks, firewalls were the only defense mechanisms that applications had for protecting data. ACE devices have the ability to perform deep packet inspection and can block common network-based attacks. An integrated firewall in the ACE device provides protection above and beyond that offered by traditional host-based and network-based firewalls.

The ACE market is growing fast and has recently become more competitive. Some of the top manufacturers are: Cisco, F5, Riverbed and Citrix. Each manufacturer utilizes its own proprietary algorithm to provide the application optimization services. In general, however, they all provide the following services:

- Server load-balancing
- Protocol differentiation services
- HTTP header manipulation

- Fail-over
- Network address translation (NAT)/ Port address translation (PAT)
- SSL acceleration
- Caching
- Virtualized services
- Application management services
- Asymmetric routing

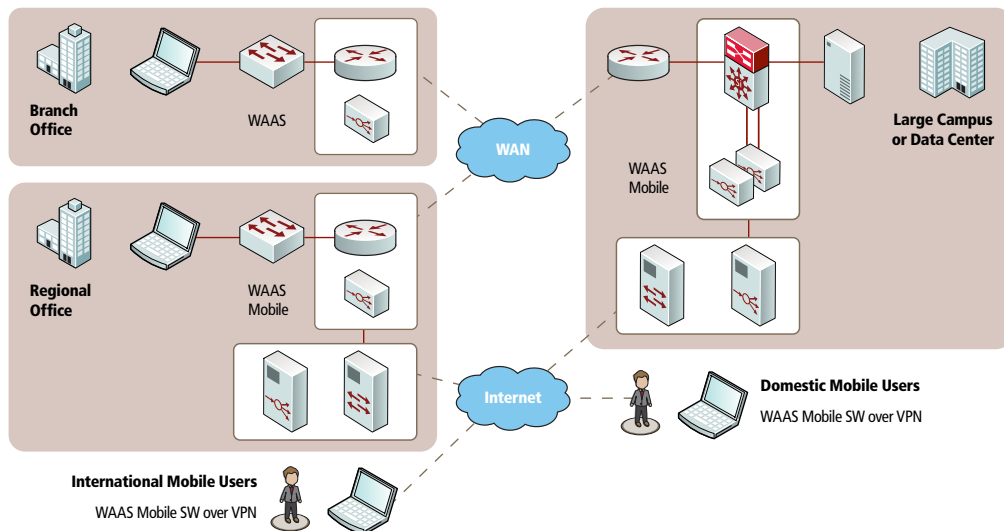
### CISCO WAAS

Wide Area Application Services (WAAS) is an application optimization product introduced by Cisco to accelerate performance over a WAN. It can deliver video to branch locations and provides local hosting services for satellite offices. The Cisco WAAS solution allows organizations to centralize applications and storage in the main data center while maintaining LAN-like response times.

Utilizing WAAS, organizations can perform the following tasks:

- Application acceleration
- Data consolidation
- Data protection
- Minimization of bandwidth utilization
- Management of application deployment ◊

### A CISCO WAAS DEPLOYMENT



# CONVERGED COMMUNICATIONS



There are many benefits to implementing a VoIP solution for your organization: reduction of costs, enhancement of productivity and increased mobility for starters. But many organizations, in their zeal to get a system in place, oftentimes overlook one of the most important aspects of implementing a VoIP solution: security.

The first rule in any situation: never rush in when you don't know what's waiting for you on the other side. It's a sure-fire way to defeat. By knowing the strengths and weaknesses of IP convergence, you put yourself in a better offensive and defensive position.

It's important to note that like the rest of your data network, IP telephony systems and unified communications servers are susceptible to denial-of-service attacks, intrusion, and slowdowns or freezes. In addition to zero-day threats, your top challengers are:

- Security not being implemented because it was unplanned for or too complex
- Vendor-specific vulnerabilities that have yet to be addressed by current best practices

Surprisingly, most VoIP exploits are not the result of the technology, but of poor implementation. Fortunately, CDW•G can coach you through the proper setup of the technology, and train you how to be on guard against new attacks.

With the appropriate security measures taken at implementation, your IP network can be even more secure than traditional PSTN lines.

#### Tips to a secure VoIP network:

- Implement voice and call signal encryption to protect all voice data between network endpoints and callers
- Set up a fail-over solution for crucial systems and voice communications in case of service disruption
- Ensure that your storage systems are up to the task of logging and securely retaining digital recordings of individuals' interactions

#### Our Approach to VoIP

First, we assess. Our specialists analyze your entire workforce and assess your communications needs. To make any transition easier, we'll work with your current network infrastructure and equipment that's already in place. Once we determine your organization's requirements and map them to best-in-class technology solutions, we then provide comprehensive ROI analyses and total cost of ownership (TCO) reports.

Next, we implement. We identify, size and design integrated hardware, software and service solutions for multiple locations. We then provide configuration, testing, high availability and installation through controlled deployment and services.

Then, we support. Audit feedback and reports ensure your new technologies deliver desired results. We support organizational needs as they evolve to constantly improve performance and scalability.

**Call your dedicated CDW•G account manager today to get an IP telephony ROI assessment at no cost or obligation.**



#### CALL FOR PRICING

Complete solution

Backed by the industry-leading ProCurve Lifetime Warranty<sup>1</sup>

#### HP ProCurve Switch 3500yl-24G PWR Intelligent Edge

20-port 10/100/1000BASE-T with one open module slot and four dual-personality slots  
CDWG 953149

- Ideal for full-featured gigabit PoE Edge networks
- Ensures bandwidth capabilities to the network edge
- Integrated PoE on all 10/100/1000BASE-T ports
- Supports a maximum of four 10GbE ports
- IPv6 Host Ready with future software upgrade

<sup>1</sup>For as long as you own the product, with next-business-day advance replacement (available in most countries); call your CDW•G account manager for details



#### HP ProCurve 2610-24-PWR Switch

24-port 10/100BASE-TX Fast Ethernet managed, rack-mountable switch with two 10/100/1000BASE-T ports and two mini-GBIC slots and PoE

**\$1086.28**

CDWG 1387296

- Secure, reliable 10/100 connectivity with enterprise features
- Flexible, scalable PoE for converged networks and remote offices
- Ideal for VoIP applications, wireless LANs, surveillance cameras and network edge connectivity
- Static routing, robust security and easy-to-use management features
- ProCurve Lifetime Warranty with advance, next-day replacement



#### HP ProCurve 2626-PWR Switch

24-port 10/100BASE-TX managed, stackable, PoE-compliant switch with two dual-personality ports

**\$1097.24**

CDWG 558726

- Basic IP Routing — enables automatic routing with up to 16 external routes (including one default route) in IP networks
- Rapid Convergence Spanning Tree Protocol (802.1w) — increases network uptime through faster recovery from failed links
- Secure access to manage the switches — all access methods (CLI, GUI or MIB) are securely encrypted through SSHv2, SSL and/or SNMPv3
- QoS — offers real-time traffic classification (IEEE 802.1p) with CoS and Layer 4 prioritization



#### HP ProCurve 2810-24G

24-port 10/100/1000BASE-T Gigabit Ethernet managed, stackable, rack-mountable switch

**\$1190.01**

CDWG 1034441

- Layer 2 managed 10/100/1000 stackable switch
- IP multicast snooping and data-driven IGMP: automatically prevents flooding of IP multicast traffic
- Gigabit-ready for bandwidth-hungry applications
- Offers high-performance, robust security and traffic prioritization, and exceptional reliability
- Shallow form factor designed for smaller wiring closets
- Scalable for expanding network requirements
- Lifetime warranty featuring advance, next-day replacement



# REACH A HIGHER LEVEL

## OF COMMUNICATION



VoIP telephony — using an organization's broadband connection to carry its entire telecommunications, including voice and video — offers one of the most effective ways to maximize a network, and allows organizations to utilize new Unified Communications features such as instant messaging, video and web conferencing, presence and notification services.

### CDW•G Telephony Experts let you add the expertise — without adding headcount.

At CDW•G, every account manager is backed by a team of specialists. And those specialists receive extensive training and industry-standard certifications, so what you get is experience — without the expense.

CDW•G telephony specialists' expertise covers in-depth knowledge of name-brand products and industry leaders, including but not limited to:

- Polycom® HD voice audio/video conferencing
- Cisco® Unified Communications
- Avaya Communication Manager and IP Office and Partner
- ShoreTel® Enterprise IP Phone Systems
- Nortel Meridian, CS1000 and BCM
- 3Com® Secure Convergence
- Plantronics® headsets

### CDW•G Telephony offerings:

- Customized phone system solutions (including hardware, licenses and software)
- VoIP and TDM PBX design and configuration
- Audio conferencing
- Video conferencing
- Conference bridging
- Unified messaging

### We put your telephony needs first.

We work directly with leading manufacturers to make your telephony decisions easy, cost-effective and hassle-free. We can help you find the best telephony solutions based on the most advanced technology available, allowing your organization to improve processes and improve your ability to respond to needs with a sense of urgency.

### Simply contact your dedicated CDW•G account manager to be linked up with our experts.



### Cisco® Catalyst® 2960-48TT Switch

48-port 10/100BASE-TX Fast Ethernet managed, rack-mountable switch with two 10/100/1000BASE-T ports

**\$1601.98**

CDWG 850882

- More network switch capacity to support bandwidth-intensive applications
- Converged solutions, such as IP telephony voice-over WLANs and video services
- High-availability and uninterrupted access to information enterprise wide
- More manageable solutions, reduced cost and complexity
- Greater protection against external security threats



### CALL FOR PRICING

**Cisco Unified Communications Manager**  
High-availability server platform for Cisco Unified Communications solutions  
CDWG 1157641

- 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



### CALL FOR PRICING

**Cisco IP Phone 7961G**  
Full-featured, enhanced manager IP phone  
CDWG 918776

- Provides six programmable backlit line/feature buttons and four interactive soft keys that guide a user through call features and functions
- Audio controls for high-quality duplex speakerphone, handset and headset
- A built-in headset port and an integrated Ethernet switch are standard with the Cisco Unified IP Phone 7961G
- Higher-resolution grayscale pixel-based LCD
- XML applications and double-byte languages



### CALL FOR PRICING

**Cisco Unified IP Conference Station 7937G**  
CDWG 1350352

- Superior wideband acoustics with the support of the G.722 wideband codec
- Support for IEEE Power over Ethernet (PoE) or the Cisco Power Cube 3
- Expanded room coverage up to 30 feet by 40 feet with the optional external microphone kit
- Support for a third-party lapel microphone kit
- New larger backlit liquid crystal display (LCD)



# DO MORE WITH SIMPLE VOICE OVER INTERNET PROTOCOL (VOIP)

## SOLUTIONS FROM CDW•G



### Communicate MORE effectively.

For large organizations, the ability to add or delete a phone line based on new or lost headcount can be time-consuming and expensive. Yet it is a crucial facet of maintaining streamlined, effective communication and consistent workflow.

When it comes to a communication solution, you want one that is easy to install, simple to deploy and one that can be efficiently managed without external assistance. The number one priority, and ultimate goal, is to ensure that your communication technology platform provides optimal workflow productivity and efficiency — after all, a phone system should help, not hinder, your organization.

### Advice that's MORE solution-based.

CDW•G is a leading provider of technology solutions focused exclusively on serving large organizations. Our experience allows us to act as a true technology partner, enabling your organization to achieve the right solution as you transition to a Voice over Internet Protocol (VoIP) solution.

### More integration. More support.

CDW•G provides the added support to help organizations optimize a VoIP solution to ensure your network technology can scale as your IT needs evolve:

**One-stop resource.** Your CDW•G account manager, backed by industry-certified specialists and working with account executives, offers an expert resource to help achieve your organization's ideal VoIP solution.

**Technology specialists.** Certified technology specialists with deep expertise in voice and data, telephony,

networking, software licensing, document imaging, security, storage and more, team with your account manager to create your ideal solution

**Comprehensive support services.** CDW•G provides comprehensive assistance — before, during and after your purchase. We offer 24x7 online support, as well as the convenient My Account portal on CDWG.com, which provides 24x7x365 access to your latest order and purchase information, helpful online guides and real-time status of your account team

**Asset tagging.** Tagging helps you easily manage the tracking of your organization's VoIP solution by serial number, order number, date of purchase, invoice number or other criteria

**Call your dedicated CDW•G account manager today to learn more about what an effective VoIP solution can do for your organization.**



**Avaya G350  
Media Gateway**  
CDWG 1046370

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

- Designed to be a complete voice/data networking solution
- 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)



**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



**ShoreTel® {Pure IP}  
Unified Communications  
Solutions**

Delivering Unified Communication platforms based on feature-rich IP telephony solutions  
CDWG 1214100

{Pure IP} Unified Communications Solutions from ShoreTel® deliver performance, reliability and value

Transform your communications by connecting people and information more efficiently. Our distributed software architecture gives you unmatched reliability, scalability and manageability all in an easy-to-use system. Organizations of any size can seamlessly integrate all communication — voice, video, data, messaging — to optimize organizational processes and increase productivity. It's easy with ShoreTel.

- With high-quality video conferencing
- Unified Communication systems with voice, IM, e-mail, and video conferencing
- Easy-to-learn and use, award-winning systems
- High-quality video that is as easy as a phone call
- Productivity-enhancing features for users
- New switch models for increased IP phone capacity
- Rich support for mobile workers



**ShoreTel  
ShorePhone IP 230**  
CDWG 1008782

Ideal for the knowledge worker who relies on telephone communications, the IP 230 delivers a wealth of features including three line appearances, eight function keys, four soft keys and a headset jack.

- MGCP protocol
- 24-character x 5-line display
- VLAN, DiffServ/ToS, 5004/udp QoS
- Wideband, G.711u/a, G.729a codecs
- 802.3af PoE (standard) or local power (optional)



# REDEFINE YOUR EXPECTATIONS

## OF VIDEOCONFERENCING.



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 videoconferencing 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 meeting in person.

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-definition visual experience in a cost-effective way.

### Ease of use.

In the past, videoconference 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 more.

Today's videoconferencing solutions let you make the process as simple and seamless as placing a phone call. 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 videoconference 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 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.

### Build a better communication experience.

Use video to work smarter. Get the rich interaction of face-to-face meetings and leave the ambiguity of e-mail and telephone calls behind. Share presentations, documents and multimedia with everyone at the same time, allowing dispersed colleagues to collaborate more effectively.

### Eliminate jet lag.

Connect with colleagues across the globe in seconds instead of wasting valuable hours in airports and on planes. Touch base with partners in different locations without leaving your office or bring them together for a videoconference call. It's simple, cost effective and doesn't require advanced scheduling or an IT technician.

### Experience the difference.

CDW•G can help you build a videoconferencing solution that combines an immersive, high-definition video experience with a rich set of features to deliver powerful, flexible and easy-to-use video communication solutions.

**Call a dedicated CDW•G account manager today to find out more about our high-definition videoconferencing solutions and what they can do for your organization.**



### Microsoft® Office Live Meeting

An online conferencing tool

One Year Service Subscription **\$2785.01**

CDWG 862038

Microsoft® Office Live Meeting is a hosted web conferencing service that connects and engages audiences in online meetings, training, and events through a reliable, enterprise-class hosted service. With meeting attendees participating from their PCs, you can deliver a presentation, kick off a project, brainstorm ideas, edit files, collaborate on whiteboards, and negotiate deals at a fraction of the cost and without the hassle of travel.

- Make presentations and demonstrate applications
- Multiple speakers can present to a large audience
- Give a PowerPoint® presentation
- Demonstrate software
- Conduct a group web tour
- Host a webinar



Microsoft



### CALL FOR PRICING

#### Nortel Software Communication System 500

The Software Communication System 500 provides a full suite of intuitive and easy to use applications  
CDWG 1591066

- Find me/Follow me — sophisticated and easy-to-use, keeps your mobile employees accessible
- Conferencing — advanced, flexible and user-friendly multi-party conferencing capabilities (including Meet Me conferencing)
- Auto Attendant — enterprise-grade attendant for a personalized customer experience
- Choice of Softphones for making phone calls from a PC as well as presence, secure instant messaging and video conferencing capabilities



### CALL FOR PRICING

#### Nortel IP Phone 1535

IP Phone 1535 videophone uses SIP to establish both voice and video calls and is targeted at enterprises or multi-site organizations that desire increased collaboration between sites  
CDWG 1591930

- Easy-to-use multimedia capabilities including personal video conferencing and audio recording along with still image and video captures which can be stored on the phone
- Supports integrated applications including web browsing, POP-3 or IMAP-based e-mail access, calendar with alarms, video supervision and image, sound and video library storage
- High-resolution, 16-bit color, Thin Film Transistor (TFT) display delivers superior user experience
- Flexible connectivity with both wired Ethernet (10/100) and IEEE 802.11b/g Wi-Fi® supported

NORTEL  
Authorized Distributor

You can't predict  
every server mishap.  
Good thing CDW•G has a plan.



When the unexpected happens, you need to be ready. CDW•G can help you devise a plan and put it into action. We have a team of experts who work with you to identify your unique needs and determine which warranty upgrades and extensions ensure you're protected. Whether you need onsite repair or a disaster preparation solution, we can help make sure you're covered.

Plan for the unexpected. Call 800.808.4239  
or visit [CDWG.com](http://CDWG.com)

The Right Technology. Right Away.®



# NETWORKING AND UNIFIED COMMUNICATIONS: UNIFIED COMMUNICATIONS



## CHAPTER 4:

Centralizing UC

Advanced Applications

Unified Contact Center

Unified Video

Unified communications (UC), formerly known as IP telephony, has made significant advances in the past few years and has started to fulfill its initial promise of a seamless user experience regardless of location. Still, managing communications continues to be challenging for organizations as they navigate this continued expansion in communications technologies.

These technologies now expand 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, finally, video solutions. Integrating all of these disparate technologies has become increasingly essential for organizations. Unified communications is the answer.

## CENTRALIZING UC

By bringing UC solutions to a centralized and secure environment, organizations can apply rapid changes to the entire organization as well as provide enhanced security and management. For example, imagine an organization that has 1,200 workers in 10 offices around the country. Some of these offices range from very small 10-person sites to medium 100-person sites.

They all need access to the same services. These services could be unified messaging (delivery of voicemail to e-mail), 5-digit dialing across the organization, mobility and extension of services to off-network devices such as cell phones. Via UC technology, the organization can scale an entire solution to provide the right services to the right people, regardless of office size.

Until recently, putting a full unified solution into a 10-person office

was quite expensive. But today, these services can be delivered, secured and managed from a central site far more cost effectively. With a centralized solution, an organization can also add many more advanced applications to the network such as Presence, instant messaging, desktop collaboration and emergency notification.

Moreover, with the advances in video conferencing from the desktop, web conferencing and desktop collaboration, organizations have the ability to place workers anywhere within the organization regardless of job function.

Staffers need to count on the delivery of communications services regardless of location inside or outside the organization. While UC brings together a host of formerly stand-alone technologies, it actually allows organizations to deliver consistent and tailored access to users based on the unique requirements and circumstances of those users.

In a recent 2008 survey of CIO's conducted by IDG Research, some consistent responses arose as to why an organization would make the move to unified communications. Some of the top reasons are:

- Reduction in operational costs
- Greater security in network access
- Ability to streamline and optimize operations processes
- Increased flexibility in infrastructure
- Consolidation of infrastructure
- Simpler maintenance

## ADVANCED APPLICATIONS

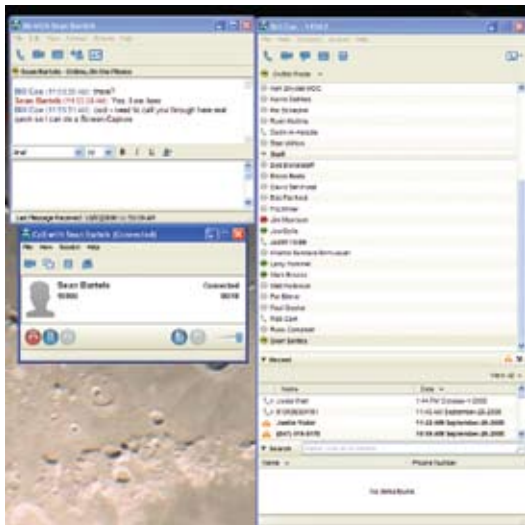
Advanced applications are the next wave of solutions to roll out to the unified communications world. When organizations start to examine the potential benefits of a UC solution, Presence is generally at the forefront of the discussions.

### PRESENCE

Simply put, Unified Presence is a standards-based platform that collects information from multiple sources about user availability and communications capabilities. The information is used to provide rich Presence status and facilitate Presence-enabled communications. This scalable and easy-to-manage solution can help workers:

- **Increase productivity:** Connect with colleagues on the first try by knowing their availability in advance
- **Enhance collaboration:** Share availability information and instant messages with coworkers within your organization or between agencies
- **Streamline communications:** View telephony status of coworkers from a variety of applications, such as Cisco Unified Personal Communicator, IBM Lotus Sametime or Microsoft Office Communicator, and simply click to call them
- **Leverage Presence-enabled operations applications:** Expose Presence information and user communications capabilities in web directories, as well as other applications and management systems

### CISCO UNIFIED PERSONAL COMMUNICATOR WINDOW



- **Improve first-call resolution and end-user satisfaction:** Allow individuals anywhere in the organization to handle incoming calls pertinent to their expertise

Presence applications allow work staff to see the availability of others in the UC network instantly. Recent research indicates a reduction in staffer “wasted time” of up to 34 percent by simply being able to view the availability status and the preferred communication methods of coworkers.

### INSTANT MESSAGING

The image below is an example of an application that not only provides Presence capabilities, but also extends instant messaging (IM) solutions. IM 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.

It is important to understand that what separates IM from technologies such as e-mail is the perceived synchronicity of user communication. Though it is beyond the scope of this guide, many IM services have additional features: immediate receipt of acknowledgment or reply, group chatting, conversation logging and file transfer, and conference services such as voice and video.

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 in reaching them.

By extending the UC network outward 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

Unified communications users now have the ability to consolidate all calls with a single IP phone number and immediately connect from wherever they are working. An organization can provide even more responsive service with no additional effort. For mobile workers, Unified Mobility (UM) also reduces the burden of having to share private mobile phone numbers.

Mobile workers can also manage all voicemail using a single voice mailbox. If a mobile call cannot be answered, UM will store the

unanswered call in the centralized UC voice messaging system or other organizational voicemail system.

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

### MOBILE VOICE ACCESS

Extending the organization's voice system for traveling staff has also become significantly enhanced in today's UC world. UM technology makes all major IP communications features available to traveling workers.

For example, a mobile staffer who needs to call one of the organization's offices while traveling can use a mobile voice access line to place the call as if 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. The connection is completed, and telecom costs are minimized.

### COLLABORATION

Regardless of user location, unified communications can connect people via voice and video services. This kind of collaboration further enhances the value of UC by coupling these services with the capacity for mutual engagement on critical documents in a real-time format.

Whether one-on-one or in a conference call setting, collaboration permits the sharing of specific documents, computer desktops and applications. Some 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

### UNIFIED CONTACT CENTER

A unified contact center (UCC) extends the ability of a base UC solution into a true multifunctional contact center for either internal or external callers. UCCs make use of the unified communications infrastructure to deliver skills-based contact routing, voice self-service, computer telephony integration (CTI) and multichannel contact management.

By combining multichannel automatic-call-distributor (ACD) functions with IP telephony in a unified solution, a UCC helps an organization rapidly deploy a distributed voice-over-IP (VoIP) contact center infrastructure.

UCC segments callers, monitors 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 and contact center data is processed through user-defined routing scripts that graphically reflect an organization's operations rules. 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, personalizing service and increasing efficiency.

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

### UCC ROUTING

The routing functions of a UCC provide further intelligent distribution of contacts as they enter the organization's network, enhancing caller experience. When a contact requires redirection, the UCC applies operations logic, sending the contact to the best available organizational resource.

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

Unified contact centers extend the sources of data available for making contact routing decisions and for populating staff desktop applications. For instance, the logic in the UCC can perform a lookup in the caller database during routing in order to guide its decisions. You can also use information from customer relationship management (CRM) applications to match callers with staff and expand the data available to screen pop applications.

With a UCC, end users can access the call center from 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, the complete end-user detail can still be provided to the staffer accepting the communication, regardless of the method of connection.

## UNIFIED VIDEO

No discussion of UC would be complete without a review of the most significant advances in the technology. The ability to extend video services and collaboration to all users in the sessions, no matter what the connectivity method, continues to expand communications options.

The vast majority of all human communication is visual by nature. People regularly observe and assess subtle nonverbal queues from others in conversations. Video communications has, up to now, proven a somewhat daunting solution to deploy successfully and effectively in large numbers. However, UC now embraces all facets of communications. Video has become the next logical step for an organization to include.

Current videoconferencing technology has improved the user experience so that 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, as all are privy to the nonverbal cues that further contextualize and inform dialogue.

There are several additional benefits to be gained from extending video communications out across the organization.

**Extension of UC platform:** To maximize effectiveness, use of UC solutions should not stop at traditional forms of communication such as e-mail and phone. Video telephony conferencing can become a further practical enrichment of user experience at the desktop via a unified software client. Videoconferencing becomes as simple as a phone call. Organizations should examine which videophone systems are already compatible with their UC solutions.

**Increased work-group collaboration:** Video maximizes scheduling time during the workday by eliminating travel times between locations and incorporating access to operations-critical information and applications from the desktop.

Over the past year, manufacturers have rolled out UC solutions that integrated formerly 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.

Organizations that incorporate video telephony into their UC architectures enable 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:** Traveling and remote users often find it difficult to feel connected to colleagues. Video gives these staffers a far more palpable means of maintaining viable, productive relationships than audio-only teleconferencing. It gives them much the same advantages of actual presence in a meeting and thereby encourages their full engagement.

**Reduction of travel expenses and carbon footprint:** Continued increases in gas and oil prices 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 increase, many organizations are taking on a social responsibility to decrease their carbon footprints. Videophone conferencing can support the dual benefit of travel savings and green IT compliance.

## ADVANCED 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 significantly extended methods of video communications via TelePresence solutions. Offering a fully immersive video conferencing experience, TelePresence creates an innovative “in-person” meeting experience over the converged network that allows users to feel as though they are in the same room with other participants.

It delivers real-time, face-to-face interactions using advanced visual, audio and collaboration technologies. These technologies transmit life-size, high-definition images and spatial discrete audio, maximizing the ability, for example, to discern facial expressions for crucial discussions and negotiations across the “virtual table.” With actual face-to-face meetings becoming more difficult, this technology offers the closest thing to it.

# NETWORKING AND UNIFIED COMMUNICATIONS: SECURITY



## CHAPTER 5:

VPN Varieties

Virus and Worm Protection

Firewalls

Intrusion Prevention Systems

The Evolving Perimeter

The ubiquity and low cost of Internet access makes it an ideal medium for establishing connectivity between work staff and the network, as well as organizations and their branch offices. But the Internet also creates all sorts of difficulties for securing an organization's network.

One of the most popular approaches to securing communications is a virtual private network (VPN). VPNs provide a secure, private network connection. When a VPN is created over a public medium such as the Internet, the connection is encrypted to ensure privacy.

## VPN VARIETIES

There are different variations on the VPN. Internet protocol security (IPsec)-based, site-to-site VPNs connect remote sites. Smaller deployments of site-to-site VPNs may terminate at a firewall or dedicated VPN concentrator.

However, at the enterprise level, site-to-site VPN deployments are usually set up router-to-router. Such router-to-router VPN implementations use technologies such as dynamic multipoint VPN (DMVPN) or generic routing encapsulation (GRE) tunneling. These technologies allow for better scalability, support multicast and provide redundancy via the use of routing protocols.

A remote access VPN, on the other hand, connects a PC to a remote network. Historically, remote access VPNs have used the IPsec suite of protocols and have therefore required dedicated client software on the PC. IPsec and Internet key exchange (IKE)

are both purpose-built security protocols focused on secure key exchange and encrypted confidential communications.

## VPN STRATEGIES

Recently, many organizations have started to readdress their remote-access strategy. Secure Sockets Layer (SSL) VPNs have gained widespread acceptance and have slowly begun displacing IPsec as the remote access technology of choice.

SSL generically refers to all common protocols for encrypting websites, including SSL version 3 and Transport Layer Security (TLS). SSLv3 and its successor, TLS, have the capacity to encrypt not just web traffic but any traffic.

SSL VPN refers to two different types of remote access experiences: A customized web portal that provides access to key network services and applications, and a full-tunnel SSL client that provides like-for-like replacement of the full-tunnel IPsec client. The ability to accomplish remote access goals with the portal alone obviates the need for a full-tunnel client.

SSL VPN has some significant advantages over IPsec VPN:

- It usually requires no new client for the portal experience, since an existing browser will suffice.
- It works from any location with Internet access and eliminates compatibility issues that IPsec has had with intermediary firewalls and network address translation (NAT) devices.

- It eliminates operating system TCP/IP stack adjustments made by IPsec clients.

Concerning this last point, protocol overhead created by IPsec lowers the packet size that can be sent inside the IPsec wrapper, potentially making it necessary to adjust the maximum transmission unit (IP MTU). This adjustment can prove tiresome to troubleshoot.

## VIRUS AND WORM PROTECTION

Viruses and worms infect a host by exploiting the host's vulnerabilities. These vulnerabilities are found in software, and a patch may or may not exist to secure them. Such malware can also result from a staffer inadvertently launching a virus program.

### THE EVOLUTION OF BOT NETWORKS

A BOT (short for robot) is a host infected by malicious software (a virus or worm) that places it under the control of a remote command-and-control server without the PC owner's knowledge.

Typically, the malicious software installs as a kit on the infected host. This kit often includes hacking utilities, a spam engine and a means of communication back to the command server in order to receive commands and new software.

A BOT network can marshal tens of thousands of PCs under the control of a single server. The STORM worm of 2007, for instance, created a BOT network estimated at more than 2 million hosts. The owner of a BOT network can then use the army of PCs to launch attacks on a third-party website, send out spam, or use the BOT as a launching point for any customized attacks within the network that the BOT resides.

The methods of virus/worm writers have undergone a sea change recently. Before, hackers built viruses, worms and associated BOT networks to disrupt operations via denial of service. Curiosity or fame served as the principal motivations for them.

Today, the motivation has become almost exclusively financial. Spam is a multibillion dollar business, and a real, liquid market exists for stolen credit card numbers. These maturing markets have driven innovations from the creators of BOT networks.

They now quietly build efficient, self-healing BOT networks that evade detection by running on port 80 and rotating the command-and-control server via fast-flush domain name system DNS. Expect the proliferation of BOT networks to increase and infection techniques to evolve.

A variety of complementary security strategies should be used to protect the enterprise against BOT-infected hosts:

- Keep antivirus and patching up-to-date on end-points.

- Install a host-based intrusion prevention solution (HIPS) on end-points. HIPS products protect a host based on behavior, and will thus stop the unknown, or zero-day, attack.
- Watch traffic at egress. Solutions such as IronPort's Web Security Appliance watch all outbound traffic headed to hosts with a poor reputation. Gaining visibility of such traffic will indicate potential BOTs within the network.
- Log DNS requests. The audit trail of a DNS server can provide valuable forensic evidence in the event of a security incident.
- Consider implementing web proxy and e-mail gateway services that block spam and unwanted content by web reputation at the network edge. The most common vectors for infection include e-mail and web browsing.

## FIREWALLS

The network firewall serves as the most basic level of defense in the network. It provides a state-aware security barrier between different network trust zones. Often, an organization deploys its first firewall at the Internet edge and uses it to separate the internal organization network (the trusted inside) from the Internet (the untrusted outside).

The firewall advertises public-facing services, such as web, FTP and e-mail, to the Internet. However, it places these services in a third security zone, a demilitarized zone (DMZ). Additional security zones can be added as needed.

By default, the firewall allows network traffic to move from the more trusted zone to the less trusted zone without restriction. It also grants return traffic related to existing connections. However, the firewall denies all other traffic from the less trusted zone to the more trusted zone unless specifically permitted via an access list. This capability provides a high level of protection up to the network connection level.

From this core concept, firewall strategy has extended in two directions: placement and functionality.

### FIREWALL PLACEMENT

Because firewalls separate security zones that possess varying levels of trust, it often makes sense to implement a firewall wherever a differentiation of trust occurs. For example:

- **Within the data center:** Employ a highly available, high-performance firewall solution to separate key server segments from production user traffic.
- **At the wide area network (WAN) edge or at the remote office:** Separate remote offices and the central site into separate zones.



- **In manufacturing environments:** Separate sensitive IP-enabled production line equipment from PCs and notebooks found on the office network.

### INCREASED FIREWALL FUNCTIONALITY

Application-layer firewalls have the ability to look beyond the TCP header and into the application protocol. This visibility allows the firewall to sense protocol violations, attacks or negotiation to a different port.

As one example, session initiation protocol (SIP) will use its control channel to negotiate subsequent ports for voice payload traffic. Without visibility into the Layer 7 commands, the firewall would block the subsequent data transfer. Additionally, an application-level firewall can potentially block traffic that is using a well known port for other purposes. An example of this activity would be Skype's use of the www port (port 80).

Web application firewalls will actually proxy HTTP and HTTPS traffic, effectively brokering the connection. This "man-in-the-middle" approach allows the web application firewall to comprehensively protect public-facing web servers. Web application firewalls will protect against SQL-injection and cross-site scripting attacks. They also have the ability to white list and black list the behavior of attached web clients.

Additional capabilities in newer firewalls include content inspection, malware protection and even antispam protection. Turning on additional services, however, may impact the

performance of the firewall.

Finally, personal firewalls provide a base firewall capability at the PC level. If the PC initiates the connection, the firewall permits return traffic. It denies any other traffic, however, unless explicitly permitted.

The traditional edge firewall is losing relevance as organizations blend different security capabilities into a single platform that the industry terms unified threat management (UTM). In this context, expect to see further capabilities added to the firewall platform and a significant increase in the use of web application firewalls as a response to the most prevalent current threats.

### INTRUSION PREVENTION SYSTEMS

Over time, intrusion detection systems (IDS) have given way to intrusion prevention systems (IPS). Rather than alerting security administrators to potential security intrusions that have already occurred, IPS can block security threats in real-time and reset network connections as necessary.

Leading IPS systems have developed a few key features that dramatically improve the value of the technology:

- Inclusion of protocol engines to detect some of the more common, sophisticated attacks based on protocol violations, TCP replay and IP fragmentation
- Contextualization of fired signatures that provides more value to the event (such as: What is the value of the potential victim

host? How can one trust that the fired signature is a real security threat? How severe is the attack if the fired signature denotes a real threat?)

- Alerting on statistical network traffic anomalies
- Collaboration with security event management products to collect and correlate security threats and actively alter IPS behavior based on a changing network security posture
- Incorporation of IPS features into existing networking products such as routers and firewalls, resulting in fewer appliances to manage and more straightforward, high-availability designs

In the last few years, IPS has tipped into mainstream adoption. Some of this momentum has developed from compliance requirements such as the Payment Card Industry Data Security Standard (PCI DSS). Intrusion prevention is typically deployed first at the Internet edge, next at the data center and finally at the WAN edge or remote office as necessary.

Consider the following when evaluating IPS systems for your environment:

- Take into account the performance implications to adding IPS as a service or module on a firewall or router. Typically, the firewall or router has a much higher throughput capacity than the IPS. Will the IPS impact throughput meaningfully?
- Identify the current monitoring strategy. Some organizations automatically protect against the most severe threats and log the remaining information without active monitoring — a low-cost, administrative approach. To get a comprehensive view of the network's security posture, though, a security event management technology is recommended.
- Ask the following questions: Where should I position the IPS? Where are the threats? Where is my most sensitive data located?

## THE EVOLVING PERIMETER

Traditional perimeter security measures do not provide adequate protection in today's computing environment, which includes flash drives, Skype, instant messaging, IP-enabled phones, notebooks connecting to diverse networks of varying quality, VPN and web portals accessible from a foreign PC and guest/contractor access to both internal-wired and wireless segments.

To address potential threats while providing access to the network and its services, organizations need to think about security in new ways. Security based purely on strong edge protection — known to security professionals as “hard crunchy shell, soft chewy center” — is no longer sufficient.

The following questions prove valuable in thinking through a security strategy:

- Does an operational reason exist for allowing Skype and/or IM clients? If not, a security policy could prohibit their use. Firewalls and proxy-server technology at the network edge could stop such traffic.
- Do we provide network services to guests and contractors? Network access control (NAC) can allow a customization of available network services based on the identity of the user and the security posture of the connecting PC, thereby protecting your production network while still opening the door to foreign PCs.
- How do we protect the traveling notebook? In order to allow users to safely connect to foreign networks, the end-points must have protections in place such as: host-based intrusion prevention, personal firewall, antivirus and patches.
- How do we safeguard sensitive data? Classify your data into tiers, then locate it. If the data is centralized, then firewalls, intrusion prevention, strong access control and auditing serve as relevant tools. If sensitive data is widely distributed, either work to centralize it or look at data loss prevention (DLP) technologies.
- How do we ensure that highly sensitive data doesn't leave the organization? Different DLP technologies can prevent sensitive information from exiting the organization via e-mail, web, FTP and portable media. Some of these products work at the end-point by constraining user behavior. Others work at network egress. Multiple layers of protection are preferable.
- How do we manage insecure user behavior? The best security protections cannot defend against a user who inappropriately shares valid login information.

Two principal approaches exist for counteracting this weakness. Teaching users about secure computing practices, including password protection, is an ongoing best practices campaign. Two-factor authentication, by contrast, combines a known password with a physical key such as an RSA token. This one-time password resists replay and provides very strong protection against the threat of weak or shared passwords. ♦

# NETWORKING AND UNIFIED COMMUNICATIONS: MOBILITY



## CHAPTER 6:

Centralized WLAN

WLAN Security Strategies

Successfully Deploying VoIP-over-wireless

The popularity of utilizing wireless (or Wi-Fi) networks for delivering applications and services to mobile users within an organization has continued to increase in recent years. This trend is due largely to advancements made in wireless LAN security, reliability and capability. Organizations now leverage the investments they make in a quality wireless network to deliver more services to their workforce than simple data connectivity.

Today's Wi-Fi networks have the capability to provide services such as Voice-over-IP (VoIP) applications, real-time locating systems (RTLS) and robust wireless security features. Such services make staff more efficient and protect the organization at the same time.

## CENTRALIZED WLAN

Increasing the number of applications that rely on the wireless network likewise increases the organization's dependency on it. To ease the burden that this reliance may place on technical staff, most organizations now choose to implement controller-based wireless networks.

In contrast to the wireless networks of yesteryear, where each access point operated independently and required individual attention with every upgrade or configuration change, these systems utilize a centralized wireless local area network (WLAN) controller to provide a central repository for all software, configurations and device settings.

By automatically performing tasks, such as adjusting access point transmission 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.

These controller-based wireless networks, or unified wireless networks as they are often referred to, 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 wireless network can prove a powerful security asset.

## ASSET TRACKING

RTLS is another popular service provided by unified wireless networks. It uses access points to triangulate device locations. Doing so makes it possible to see, in real-time, the location of all wireless assets within a given area. This information can include all Wi-Fi enabled devices (such as notebooks, barcode scanners, VoIP phones or devices tagged with active radio frequency ID (RFID) tags.

An organization can attach active RFID tags to any non-Wi-Fi enabled device to permit tracking. These devices can subsequently



be located in real-time or tracked over time. This allows personnel to replay a device's location history over a defined amount of time. Alerts can even be generated based on a device's location, notifying staff if a device leaves the building or enters a restricted area.

### VOIP

VoIP has become the second most popular type of traffic utilizing wireless networks today — second only to basic data connectivity provided to staff and guest users. In recent years, with the increasing popularity of VoIP telephony systems, many organizations have sought ways to provide voice services to their mobile users. Utilizing the wireless network to achieve this goal has proven very successful.

For example, users of wireless VoIP phones can roam throughout a facility during the workday, while remaining accessible and providing value to the organization and coworkers as they do so. Such a strategy makes everyone more efficient.

With the recent introduction of dual-mode phones, the popularity of deploying voice-over-wireless applications will only continue to grow. These phones can operate over both cellular and Wi-Fi networks. This fact allows users to consolidate their voice devices and carry one phone for use both in the office and out.

### WLAN SECURITY STRATEGIES

Ensuring an organization's security when implementing a wireless network is a must. While an organization must consider several angles to accomplish this goal, user security and network protection are two of the most crucial.

Protecting wireless data stands as one of the most important facets of wireless security. In order to protect wireless data, an organization must choose the appropriate security mechanisms to protect the traffic. In making this decision, it must carefully consider two aspects of security: authentication and encryption.

### AUTHENTICATION AND ENCRYPTION

Authentication is the process by which the network grants access to a wireless user. It 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 refusing the end user the opportunity to establish a connection.

After a wireless device is connected to the WLAN and they begin to pass traffic, encryption serves as the mechanism for hiding and protecting traffic. It works by translating the traffic into a cipher that only the intended recipient can decode.

When choosing the proper authentication and encryption

mechanisms to protect wireless users, an organization must first identify all the device types that will utilize the WLAN. Identifying the devices makes it possible to define the security capabilities of each. Some devices support a wide variety of authentication and encryption types; others support a much smaller set.

In addition to end-user capabilities, selecting the proper security mechanisms also requires an evaluation of the levels of security required by the organization, the sensitivity of the data and ease of use for end users.

It may also require consideration of governing body regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) or the Sarbanes-Oxley Act (SOX).

Organization environments of all kinds should avoid using static pass phrases or stored passwords. Taking advantage of a Remote Authentication Dial-in User Service (RADIUS) server to dynamically process authentication requests is wise and highly advised. Doing so prevents unwanted devices from connecting and ensures that only approved, valid devices attach to the WLAN.

RADIUS servers process authentication requests. They either validate a user as authentic, subsequently granting access to the network, or deny access because of a failed authentication attempt. Often these servers can maintain separate user databases for authentication purposes, or they can tap into another existing user database, such as Microsoft Active Directory.

## 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. An 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 (ACLs).

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

Guest access web pages provided 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 prior to obtaining Internet access.

## WLAN SECURITY BENEFITS

By leveraging the security tools built into today's wireless networks, an organization has an effective means of monitoring and preventing wireless threats. Access points can also act as sensors, constantly scanning for wireless threats that could

potentially compromise an organization's security. These threats often include rogue access points and ad-hoc network connection sharing.

When such threats are detected, administrators receive an alert, allowing them to make an informed decision on how to eliminate the risk. All organizations should have a wireless threat policy that defines protocol for eliminating threats once detected.

Implementing a WLAN with the capability to provide such services now makes an organization far more secure. The constant scanning these services provide, in fact, gives IT personnel a view into the wireless world that few have had before.

## SUCCESSFULLY DEPLOYING VOIP-OVER-WIRELESS

In VoIP-over-wireless deployments, mobile devices connect to a wireless network in order to carry voice communications. Deployments of such technology have their own unique requirements to make them successful.

This fact arises from the extremely time-sensitive nature of voice communications, as well as the crucial need to roam throughout a facility without losing connectivity. Despite these special demands, mobile voice solutions provide many benefits to an organization when designed and implemented correctly.

To increase the odds of successfully deploying a wireless VoIP solution, an organization must first define the mobile devices to be used. As noted earlier in relation to security, each device type has its own characteristics and requirements and may need different levels of coverage and signal quality in order to function properly.

## SITE SURVEY

After defining the devices and their individual requirements, a site survey of the areas requiring wireless coverage becomes indispensable. This process involves placing wireless signaling gear in the area and using special software or equipment to gather information about the site with regard to wireless networking.

It ensures proper quantity and strategic placement of access points throughout the area in order to efficiently provide coverage. It also verifies sufficient coverage overlap between access points so that the users will have the ability to move freely through areas and roam seamlessly between them.

Note that a site survey physically conducted on premises remains the only reliable method for identifying the required number of access points and their proper placement.

During the site survey process, it is important to take user and device density into consideration. In areas where the potential exists for a large number of users, add the appropriate number of

access points to accommodate the traffic. Placing too many users on one access point can degrade performance for everyone.

## DESIGN AND IMPLEMENTATION

Following the site survey, design the wireless network to meet organizational goals, taking into account the need for redundancy, scalability and management. Choosing to use a wireless network to provide voice almost always implies that the organization views the WLAN as a mission-critical service. In that case, redundancy, such as implementing redundant WLAN controllers, becomes crucial.

It may also prove wise or necessary to provide redundant access point coverage to essential areas. Deploying a scalable WLAN will ensure a capacity for growth and adaptation to the evolving needs of the organization.

Choosing a wireless network with a robust management solution will eliminate the need for frequent or lengthy human interaction to keep things operating smoothly. Planning for these requirements during the design phase prevents future issues from arising.

Upon completion of design, physical installation begins. During installation, it is imperative to monitor progress and make sure that all aspects of the implementation occur according to plan.

In particular, make sure that access points and antennas are mounted in the correct locations and that the coverage is propagating through the facility as anticipated. Vigilance at this stage of the process will prevent user issues from arising after the WLAN goes into production.

Adhering to proper procedures in discovery, planning and execution will result in a robust WLAN capable of providing the services and applications required by a mobile workforce. The wireless network will become fully capable of supporting the mobile voice needs of the organization.

The following additional recommendations will help to ensure a successful wireless VoIP implementation:

- Implement end-to-end Quality of Service (QoS) to provide priority to voice traffic on the network.
- Utilize 802.11a whenever possible, as it remains much less susceptible to noise and interference issues that can occur when using 802.11b/g.
- Install diversity or multiple-input multiple-output (MIMO) antennas to combat issues arising from multipath distortion.
- Set the transmit power on the access points to a similar strength as that used by the clients in order to prevent one-way audio problems.

- Provide coverage to all areas where a user may expect to use a mobile phone, which may include stairwells, elevators and maintenance zones.
- Identify potential sources of interference that could negatively impact wireless LAN performance such as cordless (non-Wi-Fi) phones, microwave ovens and neighboring wireless networks; remove them or adjust accordingly.
- Inform users where they can and cannot expect to have service if coverage by the wireless network will not exist throughout the entire facility.

Finally, continually evaluate the coverage after implementation of the wireless network. The wireless environment is constantly evolving. Be sure to monitor it for any issues that could effect user connectivity.

A range of tools exists to assist with this process. Some, such as AirMagnet's Wi-Fi Analyzer and Survey products run on user notebooks and can be used to diagnose potential issues, while others are more automated, such as Cisco's Wireless Control System (WCS) software. ♦



# 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.

---

## APPLICATION CONTROL ENGINE (ACE)

ACE is a controller platform that integrates application delivery and security functions. ACE benefits include increased application availability and scaled application performance — and it can be helpful when facilitating data center consolidation.

## AUTOMATIC CALL DISTRIBUTOR (ACD)

ACD is a hardware and software system that routes incoming calls to a specific group of phone terminals within an organization. Part of the UCC, the ACD helps outside callers reach the right staffer within the organization via caller profiling software and tracking of internal staff availability.

## 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.

## COMPUTER TELEPHONY INTEGRATION (CTI)

A part of the UCC solution, CTI enables a computer to act as a call center that can integrate computer and phone interactions. These interactions can include voice, e-mail, web and fax data.

## DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK (DMVPN)

DMVPN is a Cisco-based enhancement of the VPN configuration that combines GRE tunneling, IPsec encryption and Next Hop Resolution Protocol (NHRP). DMVPN benefits include lower VPN security costs, simplified communication between branch offices, reduced deployment complexity and increased application resiliency.

## ETHERCHANNEL

EtherChannel is a Cisco-based switch technology for port trunking. EtherChannel brings together multiple physical Ethernet links to fashion one logical Ethernet link that provides greater bandwidth and minimizes convergence.

## FIBRE CHANNEL OVER ETHERNET (FCOE)

FCoE is a proposed standard engineered to enable Fibre Channel to move over high-speed Ethernet networks. Facilitating Fibre Channel traffic across existing Ethernet infrastructures can extend the reach and capability of SANs.

## HOST-BASED INTRUSION PREVENTION SOLUTION (HIPS)

A HIPS is a software-based solution that runs on a computer and prevents unauthorized access to the machine. A HIPS provides firewall and intrusion detection and prevention capabilities, protecting against viruses and other common software vulnerabilities.

## INTERACTIVE VOICE RESPONSE (IVR)

IVR is a call center phone technology used to handle high call volume. IVR allows computers to detect voice and touch tones and then respond with prerecorded or dynamically generated audio recordings to direct the caller on how to proceed.

## NETFLOW

NetFlow is a Cisco-based protocol that collects information on network traffic including version number, sequence number, input/output interface indices, timestamps on flow start/finish times, number of bytes and packets, Layer 3 headers and routing information.

## NETWORK BASED APPLICATION RECOGNITION (NBAR)

NBAR is a classification engine feature found in Cisco routers and switches that recognizes a variety of applications, including those that use dynamic TCP/UDP port assignments. Upon the application being recognized and classified by NBAR, the network arranges services for that application, emphasizing efficient use of bandwidth and QoS.

## 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.

## REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

RADIUS is a networking protocol used by many ISPs that provides centralized access, authorization and accounting management for users, allowing them to connect to and utilize a network-provided resource.

## SECURE SOCKETS LAYER VIRTUAL PRIVATE NETWORK (SSL VPN)

SSL VPN is a form of virtual private network that does not require the installation of specialized software on end users' computers and typically runs on any PC with a browser.

## SPANNING TREE PROTOCOL (STP)

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

## 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.

## TRANSPORT LAYER SECURITY (TLS)

TLS is a cryptographic protocol (and successor to SSL) that provides secure communication and data transfer over the Internet. TLS guarantees end-point authentication and communication privacy.

## UNIFIED CONTACT CENTER (UCC)

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.

## UNIFIED MOBILITY (UM)

A Cisco-based solution, UM allows users to redirect incoming IP calls to up to four different designated devices, including user cell phones and IP phones.

## UNIFIED PRESENCE

A Cisco-based solution, Unified 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.

## 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.

## WIDE AREA APPLICATION SERVICES (WAAS)

A Cisco-based solution, WAAS is a comprehensive wide area network optimization solution that accelerates applications, eliminates data redundancy and optimizes transport flow.

# INDEX



Advanced applications .....	21-22	Presence.....	4, 21-22
Application control engine (ACE) .....	3, 10-11	Secure Sockets Layer (SSL) .....	9, 11, 25
Application optimization .....	9-11	Site survey .....	31-32
Bots.....	26	Storage area network (SAN) .....	6
Cloud computing .....	5-6	Unified contact center (UCC) .....	23
Consolidated data center .....	5	Unified communications (UC) .....	4, 21-24
Desktop collaboration .....	4, 21	Unified mobility (UM).....	22-23
Fibre Channel over Ethernet (FCoE).....	6	Unified threat management (UTM) .....	27
Firewalls.....	10-11, 25-28, 31	Unified video.....	24
Instant messaging (IM) .....	21-22, 28	Virtual private network (VPN).....	25, 28
Intrusion prevention system (IPS) .....	27-28	Virtual local area network (VLAN) .....	31
iSCSI.....	6	Voice over Internet Protocol (VoIP).....	5-6, 23, 29-32
Network address translation (NAT).....	11, 25	VoIP over Wireless .....	31
Network assessment.....	6	Wide Area Application Services (WAAS).....	3, 10-11
Network design .....	7	Wireless local area network (WLAN) .....	29-32

## Disclaimer

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.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® 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, Centrino Logo, Core Inside, Intel, Intel Logo, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, 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 implementation. 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. ©2008 CDW Corporation. All rights reserved.



CDWG.COM/NETWORKING-UCGUIDE  
888.676.4239



# ABOUT THE AUTHORS

IMRAN ABBAS, CCIE, manages the 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 is the Unified Communications Solutions Manager, 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 Advanced Technology Group. Mike consults with customers on a wide range of security topics, the primary focus being 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 CiscoPress.



HOWARD WEISS manages the Network Solutions Team in the western half of the United States. Throughout his 10-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 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

090114 • Flyer 59316AB

### LOOK INSIDE for more information on:

- Utilizing application control engines (ACEs)
- Harnessing the power of Presence
- Updating video communications
- Fine-tuning a VPN security strategy



ISO 9001:2000 certified

