



Networking and Unified Communications

TABLE OF CONTENTS

- 1** Executive Summary
- 2** Introduction to Networking and Unified Communications
- 3** The Data Center
- 4** Unified Communications
- 6** Security
- 7** Mobility
- 8** CDW Support

Executive Summary

In an effort to drive profitability and rein in costs, businesses are continually seeking to improve operational capabilities. Primary to this objective are today's burgeoning network infrastructures which are continually being asked to do more.

Applications are becoming more sophisticated and mission-critical. More software is written to take advantage of dynamic IP parameters. And an economic slowdown has companies relying on network-based technologies that reduce Total Cost of Ownership (TCO) and save money.

Consolidation is another trend bolstering IT efficiencies. Servers and storage are often the first affected by a consolidation initiative. However, data center consolidation is just as important in terms of optimizing infrastructure security, compliance and integrity.

The flourishing area of unified communications offers further testimony to the increased significance of the network. UC provides substantial benefit to the enterprise in terms of capabilities that allow staff to collaborate in real time, access critical information and communicate seamlessly with coworkers and customers — regardless of location.

.....

Introduction to Networking and Unified Communications

IT managers face a difficult task in trying to offer robust services and applications while reducing IT cost and complexity. The idea is to better optimize the utilization of resources to streamline management and free diminished IT staff to work other areas.

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

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

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

Network Solutions Trends

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

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

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

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

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

Unified Communications Trends

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

Infrastructure Optimization

Consolidation, virtualization and optimization technologies facilitate more efficient use of a firm's IT resources. Here are three approaches to consider:

- **SERVER AND APPLICATION VIRTUALIZATION:** This technology enables a business to take multiple physical servers, typically underutilized, and consolidate them onto a smaller number of physical servers.
- **BLADE SERVER CONSOLIDATION:** This approach fits servers compactly into a smaller rack space while saving on cabling, power and cooling costs.
- **APPLICATION CENTRALIZATION/OPTIMIZATION:** This technology permits an enterprise to migrate its remote office applications and data into the data center, while allowing fast and efficient access out to remote workers.

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

Whether at a desk, a branch office, working from home or connecting via cell phone, a staffer needs access to the same services and levels of functionality. Today's combined advances in networking and UC allow the IT department to make it happen.

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

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

Video communications and desktop collaboration have also emerged as promising UC solutions. Both provide tremendous benefits. Keep in mind, 80-to-90 percent of human communication is based on visual queuing. So video serves as a logical extension of the UC network.

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.

The Data Center

Whether physical or virtual, a data center is a central environment that houses and distributes data through various applications. Recently, bandwidth and energy cost increases, coupled with increasingly complex IT environments, have led businesses to consolidate their infrastructure by removing applications and data from remote offices and staff PCs and placing it all into a centralized data center.

With the onset of Voice over IP (VoIP), video conferencing and streaming media, the network has become even more critical to operations. 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.

Consolidating the data center allows businesses to provide rich applications, simplify management, build in redundancy and strengthen security. By centralizing remote office servers, virtualizing underutilized servers onto fewer physical ones and shrinking those physical servers down into blades, IT management can create an environment that proves far easier to manage, protect and secure.

Cloud Computing

Many IT departments now aim to achieve a “cloud computing” environment, with applications essentially “removed” from the hardware. This may allow 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 computing cloud. 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, 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 enable users to access necessary applications from anywhere.

Companies can gain numerous benefits from a shared application cloud. Disaster recovery, in particular, can benefit from this arrangement.

For example, a firm’s staff may not be able to get to the office because of a disruptive event. In this case, remote access to centralized applications allows users to securely obtain what they need from a home computer or other remote device or location.

Designing a Resilient Network

When designing a resilient network, IT must first determine the requirements to support the firm’s functions and develop a network strategy accordingly. Upper-level management and the various departments of the enterprise can help substantially in establishing operations requirements.

After establishing the requirements and developing a network strategy, the planning phase begins. This includes getting 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 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 a company to provide the highest degree of resiliency by segmenting traffic and preventing a single point of failure.

It is crucial to eliminate single points of failure. This can be achieved by creating redundant links to critical servers and network devices. However, redundant links can create issues.

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.

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

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

Conducting a Network Assessment

A network assessment is a key step in rolling out a resilient network. 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 scheme
- Traffic and network utilization analysis

Unified Communications

To make the most of the opportunities presented by the global economy, enterprises need a comprehensive, streamlined communication infrastructure. This is one that integrates all communication devices and software. It's also one that increases productivity, speeds customer service and most importantly reduces costs.

In the UC environment, all communication tools — from voice, data, video conferencing and instant messaging through e-mail and text messaging — are fully integrated in real time. This leveraging of communication tools adds significant efficiencies.

The technology gives businesses the ability to offer a seamless user experience to staff and customers regardless of location. Integrating all of these disparate technologies has become essential for effectively conducting business.

By bringing UC solutions to a centralized and secure environment, a firm can apply rapid changes to the entire environment as well as provide enhanced security and management. Centralization also allows a business to 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, companies have the ability to place staff anywhere within the organization regardless of job function. And firms can deliver consistent and tailored access to users based on the unique requirements and circumstances of those users.

Advanced Applications

Presence is one of the newer technologies and shows great potential. Unified presence is a standards-based platform that collects information from multiple sources about user availability and communication capabilities.

These are the next wave of solutions to roll out to the UC world. The information is used to provide rich presence status and facilitate presence-enabled communications. Presence applications allow staff to see the availability of others in the UC network instantly. In addition, this scalable and easy-to-manage solution can help workers:

- **INCREASE PRODUCTIVITY:** Customers can connect with employees and staff can reach colleagues on the first try by knowing their availability in advance.
- **ENHANCE COLLABORATION:** Share availability information and instant messages with customers or coworkers within the business.
- **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 communication capabilities in web directories, as well as other applications and management systems.

• IMPROVE FIRST-CALL RESOLUTION AND END-USER

SATISFACTION: Allows staff located anywhere to handle incoming calls pertinent to their expertise.

Mobility

Today's work environments are increasingly mobile. By extending the UC network to devices outside the formal network (such as mobile phones, home-office phones or two-way devices), users can establish connectivity methods based on personal convenience and preference.

UC users can now consolidate all calls with a single IP phone number and immediately connect from wherever they are working, allowing a business to provide even more responsive service with no additional effort. Mobile workers can also manage all voicemail using a single voicemail box.

Additionally, a user answering a call on a mobile device can seamlessly transfer the call to a physical desk phone after entering the office. And a call started on a physical desk phone can equally be transferred to a mobile device.

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

Regardless of user location, UC helps people connect via voice and video services. This kind of collaboration enables staffers to mutually engage on critical documents in a real-time format.

Unified Contact Center

A UCC extends the ability of a base UC solution into a true multifunctional contact center for either internal or external callers. It makes 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, UCC helps a firm rapidly deploy a distributed VoIP contact center infrastructure. This can offer staff, customers and other stakeholders a more robust experience through a variety of media including phone calls, e-mail, chat and more.

UCC segments callers, monitors resource availability and delivers each contact to the most appropriate resource in the office. 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. This includes 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 a company's operations rules. This processing enables the routing of each contact to the right place.

Unified Video

Current videoconferencing technology has improved the user experience so that it can now be used 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.

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 via the transmission of life-size, high-definition images and spatial discrete audio, TelePresence creates an innovative “in-person” meeting experience over the converged network.

There are additional benefits to be gained from extending video communication out across the enterprise:

- **EXTENSION OF UC PLATFORM:** Video telephone conferencing can become a further practical enrichment of user experience at the desktop via a unified software client.
- **INCREASE WORKGROUP COLLABORATION:** By eliminating travel, video maximizes scheduling time during the workday and incorporates access to operations-critical information and applications from the desktop.
- **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 work relationships.
- **REDUCTION OF TRAVEL EXPENSES AND CARBON FOOTPRINT:** It can serve to reduce travel at a time when gas and oil prices have made it prohibitive.

Research Shows Active UC Planning and Progress

A CDW poll, released in January 2009, shows a gathering momentum for the implementation of Unified Communications (UC) — despite an economic downturn. Survey results indicate:

- Only 6 percent of organizations report their UC deployments are complete
- 20 percent are actively implementing UC
- 33 percent are actively planning for implementation
- 70 percent are currently in the UC planning and implementation phases and expect to complete their adoption within two years

The CDW Unified Communications Tracking Poll is based on a survey of 766 IT professionals working on unified communications or component technologies in business, government, higher education and healthcare. For a copy of the complete survey, please visit <http://www.cdw.com/uctrackingpoll>

Multilevel IP Telephony Build Out



Most medium-to-large enterprises will use one of several different strategies to deploy IP telephony — leading eventually to a unified communications infrastructure. In reality, a company can find itself at any of three different stages — with each level offering more features and capabilities.

1. CONVERGED NETWORKS: This stage involves creating a converged network. That means integrating a telephone system and IP-based data networks into one single network.

To do this, Quality of Service (QoS) switches and routers along with voice- and data-capable hardware is needed. Applying QoS to both routers and switches becomes more important as more traffic flows through the network.

QoS switches prioritize traffic on the network so that critical traffic can pass first, resulting in significant performance improvements. Next, choose a router that enables a converged network and will be able to support the more demanding requirements of a fully developed UC solution.

2. TELEPHONY AND VoIP: The second stage involves implementing a VoIP solution on a converged network. Here, IT selects the IP phone hardware and software that will run on a converged network infrastructure.

An Internet Protocol Private Branch Exchange (IP-PBX) will need to be incorporated. This business telephone system is designed to switch calls between VoIP users on local lines and switch calls between VoIP users and traditional telephone users.

IP-PBX switches enable Internet access, VoIP communications and traditional telephone communications to run on a single line to each user. The switches will support a certain number of extensions.

The extension can be located anywhere with Internet access. And multiple units can be used to increase the number of extensions or unite a company that has many locations under a single PBX system.

Features include: “Find-Me, Follow-Me,” call transfer, visual voicemail, videoconference and Customer Relationship Management (CRM) capabilities.

Also consider Power over Ethernet (PoE) technology. It allows the powering of office devices like VoIP phones and wireless access points, using your Ethernet cable without any interruption to the data traffic travelling along the same copper wires.

3. UNIFIED COMMUNICATIONS: Here the UC solution comes to life by integrating converged network and VoIP solutions with instant messaging software, videoconferencing software and other mobility tools, such as cell phones, PDAs, e-mail, presence and more.

Depending on the size of your rollout, you may require dedicated unified communications servers to support your UC strategy. Some UC solutions, for example, support IP telephony, unified client software, presence, instant messaging for business, unified messaging, rich-media conferencing, mobility solutions and application development.

Security

The notion of perimeter security holds little meaning in today's computing environment. In fact, electronic collaboration and commerce among business partners, along with the need for remote access, means the network perimeter is disappearing.

To address potential threats while providing access to the network and its services, businesses need to think about security in new ways. Security based purely on strong edge protection is no longer sufficient. A variety of strategies need to be implemented.

Firewall/Virtual Private Network

Firewall/VPN appliances typically provide users with a Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) VPN with encrypted tunnels, making an enterprise's network available to its mobile workers from anywhere in the world. At the same time, they offer a robust firewall to protect the network from hackers, viruses and worms that try to infiltrate via the Internet.

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

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

Web application firewalls will actually proxy Hypertext Transfer Protocol (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.

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.

Network Access Control

NAC determines device access to a wired or wireless network. More specifically, NAC can assess the state, or posture, of a network device.

Based on device posture and user identity, NAC determines what network services the device should be granted. NAC also provides both an architecture to repair unhealthy devices before they attach and prevents unauthorized ones from attaching.

There are three common deployments:

- **INLINE NAC:** For most small- and medium-size networks, inserting an inline NAC appliance into the network on one or more Virtual Local Area Networks (VLANs) represents the easiest method of deployment. The appliance then intercepts all IP/MAC layer traffic and adjusts the VLAN assignment according to the device's role (such as inside, guest or quarantine).
- **OUT-OF-BAND NAC:** For medium-to-large companies, an out-of-band NAC appliance provides the benefits of inline NAC without the risk of network

bottleneck. Only the posture assessment traffic is required to go through the NAC appliance. Upon completion of the assessment, NAC adjusts the VLAN and access lists of the switch port to which the host is connected.

- **DHCP REGISTRATION:** For large organizations, especially those that cannot use a NAC agent because of lack of workstation control, Dynamic Host Configuration Protocol (DHCP) registration systems provide a workstation- and network-agnostic solution. Rather than enforcing security through VLANs, as in the first two options, a DHCP registration system uses overlapping IP subnets to achieve the same goal.

Intrusion Prevention Systems

IPS is an active security technology that 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 (e.g., 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. 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.

Messaging and Web Security Appliances

Businesses today need another approach to security to counter increased accountability by customers, partners and compliance regulations; greater sharing of sensitive intellectual property; and "rampant mobility" of data. The old paradigm was to bolt even more security gadgets onto the infrastructure. This is not so today.

Messaging and web security appliances protect the organization against malware, spam, viruses, spyware, malicious websites and inappropriate surfing. They also help safeguard vital company information and ensure compliance with e-mail privacy regulations. Best of all, this protection comes with an affordable and simple-to-manage solution.

The integrated protection, offered by these types of security appliances, secures more effectively and eliminates the cost and headaches of piecemeal products. And they are available as a virtual appliance that extends the e-mail and web security solution to virtualized platforms.

Mobility

The popularity of utilizing wireless (or Wi-Fi) networks for delivering applications and services to mobile users within an enterprise has continued to increase in recent years. This trend is largely due to advancements made in wireless LAN security, reliability and capability.

Today's Wi-Fi networks have the capability to provide services such as VoIP applications, Real-Time Locating Systems (RTLS) and robust wireless security features. Such services make staff more efficient and protect the business at the same time.

Centralized WLAN

Increasing the number of applications that rely on the wireless network likewise increases the firm'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.

This is in contrast to the wireless networks of yesteryear, where each access point operated independently and required individual attention with every upgrade or configuration change. Systems now 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. They know that the wireless network can largely take care of itself.

WLAN Security Strategies

Protecting wireless data stands as one of the most important facets of wireless security. In order to protect wireless data, an enterprise must choose the appropriate security mechanisms to guard 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.

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 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 company 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, a business 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 firms 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.

Primary Manufacturers

Businesses have numerous options for finding the right networking and unified communications solutions for their needs. Several manufacturers offer both networking and unified communications products.

CISCO: The firm designs, manufactures and sells IP-based networking and related communications products such as switches, routers, security solutions, network storage and unified communications products to integrate voice, video, data and mobile applications. In addition to the IP hardware, Cisco offers network management tools, software and services to round out its solution offerings.

AVAYA: The firm is a top manufacturer in the unified communications space. Its product offerings include integrated web conferencing solutions, mobile solutions, voice messaging solutions, unified messaging platforms, video conferencing technology, UC suites and desktop telephony solutions.

IBM: An industry leader, the firm has a presence in many areas, including networking. The company offers a variety of servers including blade servers, cluster servers, mainframes, Linux servers and UNIX servers. IBM also has several operating systems and storage systems to complement its networking offerings.

MICROSOFT: The firm has a presence in the UC world through its two server offerings: Office Communicator 2007 and Exchange Server 2007. Office Communicator 2007 assists with real-time communications, enabling several different communications options including instant messaging, voice and video. Exchange Server is messaging and collaborative software.

NORTEL: The company offers a diverse range of networking and unified communication products: contact center suites, communications servers, Ethernet switches, switched firewalls, threat protection systems, VPN solutions, PBX solutions, optical network solutions, unified messaging technology, wireless network products, wireless mesh systems and WLAN products.

CDW Support for Network Solutions and Unified Communications

When companies implement advanced technology solutions, they want to rely on a partner that delivers comprehensive product knowledge, solid technical expertise and total service capabilities. They need a source with in-depth expertise and comprehensive capabilities. That's exactly why organizations of all sizes rely on CDW.

Networking Solutions

There are three types of networking solutions that the CDW Advanced Technology Team can help businesses design: Resilient Networks, Application Optimization and Storage Networking.

Resilient Networks:

As mission-critical applications and traffic rise, companies of all sizes are becoming more dependent on their IT networks. Fortunately, new technologies are available to help boost network resiliency. Consider CDW if your planning includes:

- Network convergence
- Moving to a new location
- Acquiring another company
- Consolidating from multiple remote sites to a more centralized model
- Engaging in telecommuting initiatives
- Tending to an existing collaboration mechanism or adding one
- Implementing a new data center or upgrading an existing one

Application Optimization:

Here's a way to increase productivity and cut costs. By taking full advantage of system resources, computing results can be achieved faster and more accurately. And maximizing apps is usually less expensive than adding to current resources. Turn to CDW for assistance with app optimization if you are:

- Experiencing slow application performance over a WAN
- Engaging in telecommunication initiatives
- Interested in centralizing data, services and applications
- Have a need for high application availability

Storage Networking:

Separating storage resources from servers simplifies network management. That reduces TCO and cuts costs. It's also a great way to improve the reliability, performance and efficiency of the network. Let CDW help accommodate your growing storage needs when in the process of:

- Implementing a new Storage Area Network (SAN)
- Upgrading or improving access to a SAN
- Installing iSCSI, Fibre Channel or Fibre Channel over Ethernet (FCoE)
- Planning for business continuity and disaster recovery

Partner with the Pros

CDW's Advanced Technology Team can provide professional expertise across all major phases of a networking project including:

- Assessment
- Project Management
- Support
- Planning and Design
- Implementation

Unified Communications Solutions

UC provides the technology architecture by which businesses can communicate and collaborate more efficiently — whether internally or externally. A matrix of communication types, it provides a seamless communications system across multiple networks, applications and devices. Put CDW to work on your UC initiative if you are:

- Currently using a PBX system
- Lacking PBX support
- Approaching PBX end-of-lease
- Building a new location
- Acquiring another company
- Maintaining a mobile workforce
- Have an existing call center or a need for one
- Have an existing collaboration mechanism or a need for one

UC benefits and features include:

- Call Control
- Video Conferencing
- Presence/Desktop Collaboration
- IP Phones/Softphones
- Reporting Analytics and Management
- Self-Service Applications
- Unified Messaging
- Web and Audio Conferencing
- Mobility and Wireless Telephony
- Contact Center
- Legacy PBX Integration
- Carrier Services

Day-2 Support Options

In striving to help you optimize UC investment, we offer end-to-end support that helps maintain operations efficiency and improve productivity. Look to CDW for these services:

- CDW's VoiceAdvantage — 24x7 support for our voice installations
- Cisco Managed Unified Communications — monitoring and management of client voice server infrastructure/networks in our data center; offered at three levels: Advanced Monitoring, Proactive Maintenance and Availability Management

CDW pre-sale services include: planning and pre-sales design, product selection and pricing, professional services scoping and contract development. In addition, the CDW Pre-Sales Team offers UC roadmaps designed to determine business needs, evaluate current network status, deliver gap analysis and provide an estimate of services required.

A Trusted Partner

CDW stands strongly positioned to provide the best network and unified communications solutions for you. Our ability to tailor an end-to-end solution to meet your specific needs remains second to none.

CDW also offers you extraordinary value in the depth and breadth of the resources we command, the solid relationships we've built with industry leaders, the expertise of our engineers and their vast experience with the planning, implementation and support of complex solutions.