



Data Convergence

How government agencies can best take advantage of Voice over IP, web and video conferencing, and unified communications

TABLE OF CONTENTS

- 2 Convergence of the Network
- 2 Efficiencies Gained with a Converged Network
- 2 Leveraging the Converged Network
- 4 Implementation Best Practices
- 6 Building a Reliable Network
- 8 Manufacturer Options

Executive Summary

Convergence, which marries voice, video and data communications onto a single IP network, is a concept that is more than a decade old, but adoption is now kicking into high gear.

An increasing number of government agencies are reaping the benefits of a multipurpose network by deploying Voice over IP (VoIP), video conferencing and advanced communication applications, such as presence, instant messaging and web conferencing. These technologies provide faster, more effective communication and collaboration between staff, easier IT management, and cost savings for the entire organization.

Through VoIP, for example, traveling or teleworking government workers can have their office phone calls routed to their cell phones or to their notebook computers.

This white paper explains current trends related to convergence, details the technology's productivity and cost benefits, and shares best practices about how best to deploy VoIP, video conferencing and other unified communications (UC) applications.

The white paper also serves as a guide on how to build a reliable network that can handle all the bandwidth-intensive applications related to convergence.

.....

Convergence of the Network

Historically, organizations have used circuit switches for voice communications. Through convergence, the latest networking equipment treats both voice and video the same as any other form of packetized data traveling over an IP network.

Deployment strategies run the gamut and depend on an organization's needs and budget. Some only want VoIP because they need to replace their antiquated traditional PBX equipment or because they need to take advantage of advanced voice applications, such as unified messaging.

Some only need to implement video conferencing, while others want a full UC solution that ties together all the communications technologies, such as voice, video, instant messaging and e-mail.

Most government agencies pursue VoIP first, and once the implementation is successful, they explore video conferencing and other UC applications and implement them if there are strong business cases for them.

VoIP adoption has steadily increased over the past decade as the technology has matured and as manufacturers and IT administrators have perfected implementation techniques and best practices to ensure good voice quality and security.

While some organizations pursue a full IP telephony implementation, most take a phased approach and pursue a hybrid model that mixes new IP-PBX technology with old phone equipment. For example, an organization can install an IP-PBX system for call routing, but to save money, continue using existing digital phones. Gateway devices allow the two technologies to communicate and allow IT departments to migrate to IP phones as budget allows.

Video conferencing, particularly high-definition video in conference rooms, has seen a huge increase in adoption over the past year because, with the current state of the economy, organizations need to decrease travel expenses and because the cost of bandwidth from large service providers has dropped dramatically. The falling prices for bandwidth are a huge driving factor because video conferencing requires a tremendous amount of bandwidth.

Voice over IP Adoption on the Rise

Use of VoIP technology by U.S. organizations is expected to increase from about 42% at the end of 2009 to 79% by 2013, according to market research firm In-Stat.

Efficiencies Gained with a Converged Network

For most government agencies, it's no longer a question of whether they will implement convergence, but when. Networking and telecommunications equipment makers today are focusing their research and development dollars on VoIP, video conferencing and UC technologies, not on time-division multiplexing (TDM) equipment.

Making the transition to convergence much easier is the fact that networking manufacturers have been building convergence capabilities into networking equipment since the early 2000s. IT staffs that have purchased new routers and switches in recent years already have important convergence features built in, such as Quality of Service (QoS) and Power over Ethernet (PoE) support.

With traditional voice systems, organizations need to install and manage separate PBX systems in each office or campus location.

In contrast, VoIP and unified communications allow for a centralized architecture, where an IP-PBX at the main data center routes the calls to branch offices and campus locations over a wide area network (WAN). The branch offices or campuses deploy simple IP gateway equipment to communicate with the main IP-PBX at the main data center.

In this scenario, IT departments don't have to waste resources operating separate phone and data networks, and they no longer have to manage individual PBX systems at each location. They only need to manage one network and can manage the voice system centrally from the data center, which saves on maintenance and equipment costs.

Because IT departments no longer need separate teams to manage telephony and network operations, they can retrain and redeploy staffers to take care of critical IT needs in other areas.

The new network architecture also allows organizations to decrease their energy bills by turning off devices on the network during off-hours. IP phones and wireless access points, for example, are powered through Ethernet cables. Through a product such as Cisco System's EnergyWise, IT administrators can remotely turn off the devices during off-hours or on weekends.

Leveraging the Converged Network

Convergence breaks down the barriers that previously existed between different communications technologies. Historically, the office phone, cell phone, e-mail, instant messaging, video and web conferencing worked separately from each other.

As the name suggests, unified communications ties them together on the converged network. The technology empowers staff with new ways to communicate and collaborate, which improves worker productivity, lowers total cost of ownership and even bolsters continuity of operations planning.

The different technology focal areas of convergence offer many unique benefits for organizations.

VOICE OVER IP: By moving voice onto the data network, staff can take advantage of single-number reach, a function that allows phone calls to simultaneously ring a staffer's office phone, cell phone and computer, making them easier to reach and ensuring that important phone calls aren't missed.

When connected through a virtual private network (VPN), workers can launch phone software (called softphones) on their computers and securely dial and receive phone calls with their office phone numbers.

Through the unified messaging feature, voicemail and faxes are now available as attachments on e-mail, allowing workers to listen to their voicemail or retrieve their faxes from their computer or smartphone e-mail inboxes.

The visually impaired and people with disabilities can also access their e-mail over their phones and have their e-mails read to them. Workers at organizations that deploy unified communications typically cite unified messaging as their favorite feature because of the convenience of being able to retrieve all their messages in one place.

Popular Unified Communications Applications

Audio conferencing and unified messaging are the most popular unified communications features. Seventy-six percent of organizations that use unified communications have deployed these two functions. Other popular unified communications features are desktop application integration (66%), instant messaging (60%), presence (59%), video conferencing (53%) and web conferencing (51%).

Source: Info-Tech Research Group

Once implemented, VoIP saves money in several ways:

- By routing voice calls over the IP network, calls between offices are now internal, saving government agencies from long-distance charges. While over the past decade long-distance charges have dropped considerably, VoIP still provides a cost savings.
- A technique called "least cost routing" saves money on long-distance calls made outside your organization. Calls are first routed across your IP network to the office closest to where you are calling before it leaves the internal network.

For example, if a staffer in Washington, D.C., needs to call an outside number in New York, the call travels across the internal network to the organization's New York office, and from there the phone system dials out to the outside New York number. That makes it a local call, saving your organization on long-distance charges.

- IP phone systems feature conference call capabilities, so agencies no longer have to pay for third-party conference call services.
- VoIP allows IT staffers to deploy new phone lines faster and more cost effectively. The technology removes the expense of paying service providers to move, add or make changes to phone lines. IT departments can quickly and easily configure new phone lines when needed.

And once configured, the phones are plug-and-play. If workers move desks, they simply unplug their office IP phones, plug them in at their new desks, and the network will recognize the phones and immediately work.

VIDEO CONFERENCING: About 90 percent of human communication is based on visual cues, so video conferencing is an improvement over audio conference calls. Staff can read each other's body language and determine if people are paying attention, are confused or are understanding what is being said.

Video conferencing allows government staffers in different locations to hold meetings without having to travel, which not only reduces travel costs and saves time, but it also helps government agencies go green by reducing carbon emissions. Because of the advances and high quality of video conferencing, the technology has become a viable alternative to actual face-to-face meetings.

Manufacturers offer a range of video conferencing technologies at different price points, from desktop IP phones with video conferencing screens to high-definition video conferencing equipment for conference rooms.

The higher-end equipment ranges from a single, large flat-screen monitor that allows people to see each other around a table to top-of-the-line telepresence equipment, which uses multiple large screens to make people appear life-size, as if they were in the room with you. Smaller locations can also deploy smaller tabletop video conferencing units.

COLLABORATION TOOLS: Manufacturers offer computer software that allows workers, through a single user interface, to check their colleagues' availability online. And if they're available, workers can instant message, hold an audio or video chat, and hold web conferences where two or more people can share presentations, edit documents and collaborate on a whiteboard.

Tips for Deploying Video Conferencing in Conference Rooms

1. AIM STRAIGHT AHEAD. For the best visibility, place the video camera and screen at the end of a table, so the camera points down the length of a table. That way, people can turn their heads and face the camera, allowing people on the other side of the video conference to see their faces.

In addition, place the microphone at the center of the table, and consider using extension microphones so people don't have to lean over one mike to talk and be heard.

2. USE SIP. Video conferencing systems support two industry standards: H.323 and SIP (Session Initiation Protocol). Organizations that want to video conference with people outside their organization but use different manufacturers can simply use the same communications protocol for the two systems to work together. Most have standardized on SIP.

3. WIRED IS BETTER THAN WIRELESS. For notebook computer users who dial into a video conference, a wired network will offer a more stable connection than Wi-Fi. For better voice quality, notebook users should also use a headset with a microphone, rather than rely on a computer's microphone. Users should also shut down their applications, so they are not competing with the video conference application for bandwidth.

Users can easily set up video and web conferences with two or more colleagues by scheduling them on Microsoft Outlook or Lotus Notes. Manufacturers primarily offer these real-time collaboration tools for PCs, but some are starting to offer the same feature set for mobile phones.

The collaboration tools, combined with unified messaging, allow an increasingly mobile and dispersed workforce to stay in constant contact, regardless of whether they are at the office, at home or on the road.

For example, through the use of presence, users can share information about their availability and preferred method of communication. Staff can see whether their colleagues are available, on the phone, or busy and can't be disturbed. Presence also tells them the best way to reach them at the moment, such as through an instant message, phone call or e-mail message. It eliminates the frustration of playing telephone tag, speeds up communication and improves productivity.

The UC tool can also bolster the government's efforts to increase teleworking among its work staff and aids in operations continuity. If an emergency or disaster prevents staffers from traveling to their offices, staff can telework and use the UC tool to communicate.

CALL CENTER MANAGEMENT: For agencies that run call centers, IP-based call center technologies integrate phone, e-mail, instant messaging, web collaboration software and customer relationship management tools on one unified system, which improves customer service.

EMERGENCY NOTIFICATION: If an emergency occurs, UC equipment can serve as an emergency notification system that broadcasts important information immediately to government staff in agency buildings.

For example, some manufacturers' IP phones can act as an intercom, so if administrators need to alert workers right away, they can call the IP phones and the IP phones answer via speakerphone, allowing everyone in the vicinity to hear the message.

Implementation Best Practices

Here are some implementation best practices that will allow your organization to get the most out of convergence.

1. Time your implementation to replace aging equipment.

To maximize IT spending and staff resources, many IT departments time a VoIP implementation to coincide with a needed network upgrade and/or a needed replacement of a PBX.

2. The IT department needs to work as a team. The telephony, networking and server teams all own a piece of a UC solution, so teamwork is critical to an implementation's success as well as ongoing management and maintenance.

For example, the telecom team has extensive knowledge of the current PBX and voicemail systems in use, trunking configurations, and information on the user base and their phone numbers. The networking team must determine the organization's network capacity and complete any necessary network upgrades.

VoIP over Wi-Fi

Equipping staff with Wi-Fi mobile phones allows them to roam the office or campus and still have phone access. Here are some implementation best practices.

1. PERFORM A SITE SURVEY. This allows IT administrators to determine how many access points are needed and where to locate them to ensure full wireless coverage. Full coverage is important because it allows phone users to roam from access point to access point without interruption. Manufacturers offer modeling tools that allow IT managers to do their own site surveys.

2. DO MORE CABLING THAN NECESSARY. To install access points, you must run Ethernet along the ceilings. Install 20 feet of additional cabling in case you need to move access points later to ensure full coverage.

3. SERIOUSLY CONSIDER 802.11n.

Organizations should consider 802.11n for two reasons: prices continue to drop and it's the latest technology, offering faster speeds and greater reliability.

You need a Gigabit Ethernet LAN to take full advantage. Use the 5GHz frequency because it enables the highest wireless throughput and has the least interference.

4. SECURE THE WIRELESS CONNECTION. Use the Wi-Fi Protected Access 2 (WPA2) security standard, which is an industry best practice. Take advantage of wireless intrusion prevention and security software tools. Wireless sensors can scan the airwaves and look for sources of interference, rogue access points and misconfigured devices that can result in a security risk. They can also seek out threats, such as denial-of-service attacks.

The server team is also involved because IP-PBX systems run on servers and unified messaging, video conferencing and other UC tools tie to e-mail and calendaring software, such as Microsoft Outlook or Lotus Notes.

3. Hire expertise. VoIP and video conferencing may require a major network infrastructure upgrade. If your staff doesn't have the expertise, consider hiring a third-party service provider to perform a network assessment and installation. (There's more on assessing and upgrading the network in the "Building a Reliable Network" section.)

4. Train the IT staff. The IT staff may not have experience managing a telephony system on the IP network, as well as video conferencing and other UC applications. So if you plan to manage UC in-house, invest in training. If you hire third-party service providers to install the equipment, have your staff work alongside them during the installation so they can learn from them.

5. Run pilot projects first, and implement unified communications in phases. Don't try to implement a full UC solution all at once. Successfully deploy one technology, such as VoIP, before deploying video conferencing and other UC tools.

Pick a small group of users and test the technology to make sure it works with no packet loss, delay or jitter. Perfect the network and phone configurations and work out the bugs before a mass deployment. When the pilot is successful, deploy office to office or department to department. And once it's successful, move on to the next UC application.

7. Get buy-in from users and train them. For an implementation to succeed, the IT organization must explain the benefits of the technology and get the staff comfortable with it.

To reduce help desk requests, provide classroom training to familiarize users with the new IP phones, video conferencing equipment and UC tools. Provide them with cheat sheets or offer online resources with training manuals and discussion boards. Immediately after implementation, make sure experienced telecommunications technicians are onsite to troubleshoot and answer questions.

Also, roll out UC in phases. Don't introduce 10 new features simultaneously and expect users to pick them up immediately. Give users time to get accustomed to VoIP and then introduce another tool, such as instant messaging, and so on.

Building a Reliable Network

If you thought network performance and uptime was important before, it's now even more critical with voice and video added to the mix.

Voice calls over IP are typically about 64Kbps, but video requires between 768Kbps to 2Mbps for high-definition quality and 2 to 5Mbps for each telepresence screen. Network hiccups would result in unintelligible phone calls and video full of jitter, causing frustration among users. Downtime would be even worse as all communications would grind to a halt.

Fortunately, the tech industry has developed best practices for building a high-availability network and optimizing LAN and WAN performance. Before installing VoIP, video conferencing and other UC tools, network administrators must ensure the network is solid. They must determine whether the infrastructure has the capacity to handle the new high-bandwidth requirements and whether it can prioritize traffic. The first step is a network assessment.

Network Assessment

The IT team should take inventory of the network topology and analyze everything, including network devices, physical and logical links, external connections, frame types, routed and routing protocols, application-specific protocols, and IP addressing schemes. By performing this exercise, the IT staff can identify single points of failure, and the organization can then install redundant switches and routers.

One best practice is to use traffic analysis tools to first find out what your current traffic usage is. And then use the tools to inject simulated voice and video traffic onto the network to determine your new bandwidth requirements and see whether the infrastructure can handle the new load.

Network Design

The next step is network design. The key to a reliable network is to build in redundancy throughout the network.

Each router and switch should have redundant configurations, such as dual power supplies, dual processors and dual supervisors, so if one component fails, the other keeps the device operating. The servers running the IP-PBX and other communications software should also have built-in redundancy, such as multiple Network Interface Cards (NICs).

Network engineers generally recommend designing a network in three modules. The access module, made up of Layer 2 switches, is the location where users with computers gain access to the network. The core module, with Layer 3 switching, serves as the backbone of the network. And the distribution module, which resides in the middle, routes traffic between users in the access module and the core.

Networking equipment in each module must be redundant as well. Install backup switches and routers, so if one fails, the other picks up the workload.

To ensure redundancy on the WAN, use two separate carriers to connect to buildings.

While redundant links eliminate single points of failure, they can create problems. For instance, in Layer 2 switched environments, redundant links can cause looping in switches, where packets circulate endlessly in the network.

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. While STP is considered slow, a newer protocol called Rapid STP (RSTP) speeds the convergence time.

At Layer 3, advanced routing protocols enable a high level of network resilience when utilizing redundant links. Not only can advanced protocols load balance traffic over redundant links, they can converge in a matter of seconds if the primary link fails. Resiliency of routing protocols can further be enhanced by fine-tuning some adjacency related timers to allow for faster failover.

How VoIP Users Can Survive a Network Outage

If despite all your best efforts a network outage occurs that prevents the IP-PBX in the main data center from communicating with your branch offices, all is not lost. The gateway devices at branch offices, which typically communicate with the IP-PBX, can take over call routing duties, allowing users in the branch offices to continue to use their phones.

Cisco embeds its “Unified Survivable Remote Site Telephony” feature in several of its Integrated Services Routers. Avaya offers a similar failover feature, called “Local Survivable Processor,” in its Avaya Media Servers and Gateways.

Another option is using Nonstop Forward/Stateful Switchover (NSF/SSO). In the event of a primary route processor failure, this technology allows for continuous packet flow by maintaining state information for the secondary route processor. And end-node resiliency can be increased by using first-hop redundancy protocols such as the Virtual Router Redundancy Protocol (VRRP).

Improving Bandwidth/Optimizing the LAN and WAN

Each organization's situation is unique and bandwidth needs depend on the current network architecture, current applications in use and future application plans. If an organization is deploying VoIP or video conferencing, Gigabit Ethernet speeds at the core and 100Mbps to the desktop may work if users make use of very few applications.

However, if government agencies do a lot of file transfers and plan to implement both VoIP and video conferencing, networking experts recommend that organizations deploy Gigabit Ethernet at the access module.

Having Gigabit Ethernet at the distribution module may work, but it's recommended that organizations bundle Gigabit Ethernet together or use 10 Gigabit Ethernet in that layer, as well as 10 Gigabit Ethernet at the core. Your organization may not need all that bandwidth right away, but it future-proofs your system.

There are products available that allow network administrators to bundle Gigabit Ethernet links together to create one logical link. Not only does it increase bandwidth, but it also helps with uptime because the switch sees the aggregated links as one single link. If one link fails, traffic continues to flow through the other links.

To further improve network reliability, network administrators should consider the following best practices:

1. To minimize congestion, implement QoS to give voice and video traffic priority over data traffic. Then segment voice and video traffic into their separate virtual local area networks (VLANs), which improves performance.

- **QOS ON THE LAN:** When configuring QoS on the switches, give the highest priority to VoIP traffic, and then give the second highest priority to video conferencing. Voice and video traffic are then marked for preferential treatment, and if there's network congestion, all the devices on the network will expedite their delivery.

The technology is akin to driving in the HOV lane on the highway or having a police escort with sirens blazing and car lights flashing; you reach your destination quicker.

UC Benefits

What benefits of unified communications are very important to your organization?

- Reduced operating costs: **54%**
- Increased productivity: **50%**
- More reliable communication: **44%**
- Improved cross-functional communication: **37%**
- Mass emergency notification: **33%**

From a survey of 915 IT professionals in government, business, education and healthcare, featured in CDW's 2010 unified communications tracking poll.

- **QOS ON THE WAN:** Choose a service provider that has implemented an Multiprotocol Label Switching (MPLS) network with QoS in place to prioritize voice traffic over data traffic.

- **VLAN:** Take advantage of 802.11q VLAN tagging and segment voice traffic and video traffic into their own VLANs. That way, no other traffic can get in the way and consume all the bandwidth.

The technology not only improves performance, but makes the network easier to monitor and strengthens security. Separating voice traffic on its own VLAN is more secure because VLANs are dedicated locations on the network, which are not accessible unless users or devices are given rights to access them.

2. Take advantage of WAN optimization and application acceleration equipment. This strategy will improve the utilization of bandwidth and speed the delivery of applications between the main data center and branch sites.

Application acceleration equipment, from manufacturers such as F5, Riverbed, Blue Coat, Citrix and Cisco, performs services such as load balancing, caching and speeding SSL encryption. The technology indirectly aids VoIP traffic. By reducing bandwidth usage in other applications, the equipment frees up bandwidth for VoIP.

3. Proactively monitor the network with network management tools. These tools can alert you to performance problems and warn you if you need more capacity.

4. Use uninterruptible power supply (UPS) units and generators. This will allow you to survive a power outage and keep the network up and running.

5. Network security is critical, particularly in VoIP

deployments. Because calls are now routed on the converged network, the phone system is at risk to all the threats facing a typical network that can disrupt service. That includes viruses, worms, hackers and denial-of-service attacks.

Other traditional telephony threats are also a concern, such as eavesdropping and “toll fraud,” where outsiders take control of the phone system to make calls.

If you’ve built a secure data network, many of your VoIP security issues are already taken care of. To protect the network, IT organizations must have a good security policy in place, including several layers of security. That includes firewalls, intrusion prevention and detection systems, and using VPNs to encrypt phone calls between office locations and to secure the calls from workers using softphones.

Other VoIP security best practices include the following tips:

- Implement voice encryption;
- Track manufacturer security bulletins, new firmware releases and software upgrades;
- Fix the security vulnerabilities in networking equipment, IP phones and server operating systems;
- Change the default passwords on IP phones and the administrative software for VoIP systems;
- Lock down open ports and unnecessary services on the VoIP system.

You will also want to use the 802.1x protocol for port-based network access control, so client devices connecting to the LAN are authenticated with a RADIUS server. Another option is to install a network access control device, which authenticates devices on the LAN and checks to ensure they meet security policies, such as having the latest security patches, before they are allowed access onto the network.

Manufacturer Options

Government agencies have numerous options for finding the right networking, unified communications and video conferencing solutions for their needs.

Avaya

Avaya is a top manufacturer in the unified communications world. Its product offerings include integrated web conferencing, voice messaging and desktop telephony solutions, UC suites, unified messaging platforms and video conferencing technology.

Brocade Communications Systems provides a large portfolio of networking equipment for carriers, data centers and campus networks, including campus switches that enable VoIP, video conferencing and other UC applications.

Cisco

Cisco covers the full spectrum of networking products including switches, routers, Wi-Fi equipment, network management tools and software. Cisco is also a major player in unified communications, offering VoIP equipment, UC applications, contact center applications and UC management tools.

HP offers a wide breadth of products including computers, networking equipment, servers and storage. HP StorageWorks P4000 G2 SAN Solutions (formerly named LeftHand SANs) are iSCSI-based storage area networking devices. HP also recently acquired 3Com, which offers VoIP equipment and UC tools.

IBM

IBM has a presence in many areas, including networking. IBM’s UC application, Lotus Sametime, provides users with real-time communications, such as presence, instant messaging, voice and video chats, online meetings and collaboration.

Logitech/LifeSize

Logitech offers webcams, headsets and microphones for video conferencing over computers. LifeSize, a division of Logitech, offers high-end, high-definition video conferencing equipment.

Microsoft

Microsoft has a presence in the UC world through their two server offerings: Office Communicator 2007 and Exchange Server 2007. Office Communicator 2007 assists with real-time communications, enabling instant messaging, voice, video and web conferencing.

Polycom

Polycom specializes in high-definition video conferencing equipment, including telepresence. The company also offers webcams and desktop and wireless IP phones.