Network Convergence:
The Right Path for Modernization

Network modernization is becoming more urgent as public sector organizations strive to keep pace with mobile, cloud and other innovations that their legacy systems weren't designed to handle. In a recent Center for Digital Government (CDG) survey of 386 state and local government, public safety and education decision-makers, 40 percent of respondents said their network is not meeting current needs.[1] A different survey found that 60 percent of state chief information officers (CIOs) view at least 40 percent of their systems as "legacy systems due for replacement or modernization."[2]

Network convergence is a modernization strategy that equips state and local governments to meet constituent demand for digital services and respond to the requirements of an increasingly network-centric world. Managed services offer a pathway toward network convergence that can alleviate financial hurdles to modernization and help agencies address challenges created by IT staff retirements.

What is Network Convergence?

Network convergence refers mainly to the co-existence and management of different types of media — voice, video and data — over the same physical connection. As IT networking evolves, the concept of network convergence is expanding to also include different types of network-based resources such as mobile, cloud, the Internet of Things (IoT), virtual private networks (VPNs) and other technologies.

Network convergence encompasses more than just the physical components of the network. It also involves planning and managing the network in a way that allows enterprise IT organizations to flexibly accommodate the need for more storage capacity, computing power, communications bandwidth and other resources on demand. Implementing that type of agility is crucial, as government networks must support important trends, including the build out of the IoT, growing use of police

body camera video and increasingly mobile public workforces. Network convergence enables governments to respond to these workload changes and shift toward a highly connected and network-centric future.

A Painful Legacy

Today, many government organizations run separate networks for voice, data, wireless and other services. Separate networks create wasteful redundancies, erode efficiency, and create security and privacy risks. These legacy systems also present staffing problems as aging IT employees retire from the government workforce. Incoming workers aren't fluent in obsolete programming languages, and the silver tsunami is carrying away years of knowledge about existing IT environments. IT decision-makers surveyed by CDG are aware of the issue, but few have a solution yet. Almost 70 percent of survey respondents say they expect the retirement of experienced IT staff to impact their network, but just 18 percent have concrete plans to address the loss.

A Path to Modernization and Opportunity

Network convergence creates a path to modernization by incorporating all of an organization's network technologies into a single network environment — from VPNs and mobile applications to cloud services, video conferencing and more. Instead of assigning discrete resources to each component, network convergence pools resources.

This approach reduces physical infrastructure (e.g., servers, cabling and bandwidth) and operational (e.g., energy and square footage) costs; automates and optimizes systems for faster, more reliable service; and lets agencies access more sophisticated system intelligence.

In addition, the leaner network environment simplifies management and cuts IT staffing requirements. Instead of having a separate team for each network (e.g., local area network, storage area network), organizations can have a single team. The net effect is that agencies need fewer IT employees to support their networks, helping them to cope with retirements and enabling them to free up funding for strategic investments.

How Network Convergence Benefits Agencies and Their Communities

The CDG survey indicates that many public sector agencies are in the early stages of planning for network modernization. More than half of survey respondents say network transformation is or will be part of their agencies' strategic IT planning. Network convergence offers a modernization strategy that aligns with key priorities for state and local agencies. Here's how:

Stronger protection for citizen data and critical infrastructure. The process of adapting disparate systems to a converged model requires rigorous planning. As organizations review and re-organize these systems, they have the opportunity to systematically apply their data governance model and evaluate whether data and systems are secure at all points. They can then take measures to protect these resources as needed. In addition, a converged network gives organizations complete, consolidated visibility over all endpoints and resources, allowing for more rapid detection and a coordinated response to threats and vulnerabilities. It also eliminates redundancies in security technologies (e.g., security information and event management) and centralizes control so that agencies can more easily authenticate users (e.g., humans, IP phones, body cameras and IoT), authorize who (or which device) can access what resources, and apply acceptable-use policies.

Smarter government decisions. Agencies can take advantage of unified communications and modern tools that propel collaboration to a new level. Organizations can run multiple collaboration applications on demand and over the same ubiquitous network. Doing so provides opportunities to improve decision-making, reduce travel expenses (via virtual meetings), fight crime, increase productivity and more.

BEST PRACTICE:
WEIGH THE TOTAL COST OF OWNERSHIP AND OPPORTUNITY COSTS

The true costs of legacy environments compared to modernized converged networks are not always reflected in fiscal budgets. Consider the personnel and operating costs of maintaining legacy equipment over time, as well as the costs of lost productivity and missed opportunities associated with delaying modernization.

Better support for public safety and other mobile government workforces. With network convergence, unified communications and other network-based services are available to case workers, emergency responders, law enforcement officers and other employees wherever they are, regardless of device. Remote workers can securely access and submit data and images from the field, use enterprise applications, consult with colleagues, monitor equipment and perform other tasks efficiently and in real time. Doing so streamlines processes and allows organizations to respond quickly and appropriately to events. These capabilities also help attract and retain younger workers who expect the seamless use of technology throughout their day.

Enhanced government efficiency and agility. Today's cloud environments, virtual workloads and business processes require high performance and scalability. These demands will grow as network-based services access ever-larger volumes of structured and unstructured data on enterprise platforms. When optimized, a converged network allows data to pass through the network with the least number of hops and at an extremely high throughput. In addition, the underlying architecture is designed for scalability and flexibility. Organizations can allocate bandwidth and other resources where needed or add capacity on demand.

More responsive digital services. Citizens expect government transparency and the same types of web services they access in the private sector. In many government organizations, it can take six months or longer to plan and build out the infrastructure for a new web service. With network convergence and cloud-based applications, an organization can scale out infrastructure on demand to deploy sophisticated, integrated services in just days. In addition, a converged network ensures that performance and availability are robust enough to provide rapid, reliable access to services.

Taking the Money Issue Off the Table with Managed Services

The CDG survey found growing interest in a managed services-based model for network modernization. This interest is likely driven by the fact that managed services can help agencies respond to challenges around financing network improvements and coping with anticipated IT staff shortages.

Sixty percent of survey respondents say insufficient funding is the biggest barrier to adopting a converged network model. Managed services stretch network dollars further by minimizing upfront costs and reducing complexity. They also reduce the need for highly skilled IT staff, which helps agencies address staffing worries and cuts long-term operational costs. Managed services are now widely accepted in state and local government for IT-related tasks. Almost two-thirds of states already use a managed service for some or all of their IT operations.[3]

In the case of network convergence, state and local governments can leverage managed services to provide the infrastructure and management layer between enterprise, cloud and managed network services. With visibility into network resources throughout the enterprise, managed services providers (MSPs) can monitor and manage routers, switches and other technology to optimize performance, security and other parameters.

The benefits of managed services include:
- ✓ **Reduced capital investments** related to network convergence and management by leveraging the MSP's infrastructure and technology
- ✓ **Predictable long-term operating costs** by using pre-negotiated pricing models
- ✓ **On-demand scalability** and accelerated solution deployment and modernization through the MSP's existing technology

ASKING THE RIGHT QUESTIONS

Network convergence solutions vary depending on an organization's unique needs and environment. But the following questions can help state and local governments get on the fast track to network modernization.

- **Needs-based approach** What business problems are we trying to solve? Do our goals align with our mission? What are the operational and opportunity costs of not modernizing?
- **Planning** Have we completed a network inventory? How are we preparing for change management? What funding models are available?
- **Strong data governance model** What are our security standards and policies? What do we need to update to align with today's network capabilities?
- **Balance and control** What mix of insourced, outsourced and cloud-based services are we comfortable with?
- **Procurement** How do we set up procurement for managed and cloud-based services? What are the terms and conditions? Do we have a contract vehicle that multiple organizations can use?

- ✓ **Alleviation of staffing shortages** and the exodus of IT staff skilled in legacy systems by offloading IT management tasks to MSP personnel
- ✓ **Optimal performance** by delegating management to a team whose core business and resources are dedicated to the management of the converged network
- ✓ **Improved security posture** by providing high-availability architecture and comprehensive distributed denial-of-service (DDoS) attack detection and response capabilities, as well as dedicated analysts and engineers for patches, monitoring, backups and advanced intelligence on emerging cyber threats

Bringing the Future into Focus

Connectivity demands on state and local agencies will continue to grow. Digital innovations and the opportunities they afford are too compelling to ignore. Network convergence positions state and local agencies for the future by providing agile, scalable and efficient network capabilities that respond to evolving demands. In fact, the CDG survey found that each step toward network convergence correlates with increasingly higher network satisfaction among users.

Managed services will become more popular as a method for implementing network convergence, as state and local agencies look for ways to lower financial barriers to network modernization and address IT staff shortages. This strategy can help put network convergence within reach of cash-strapped, personnel-drained organizations. Using this approach, state and local governments are well-poised to launch their networks into the future.

CHOOSING THE RIGHT MSP

Agencies face a barrage of technology and configuration decisions when implementing network convergence. The field of security technology vendors alone is vast. A qualified MSP can help agencies sift through the options and make choices that fit their unique situation. When evaluating managed services providers to support network convergence, consider:

- **Scale and scope** Partner with a provider that offers an extensive portfolio (including big data and security solutions) and can scale services to meet your organization's ongoing needs. Many MSPs cannot provide end-to-end solutions, so organizations end up with piecemeal systems that they must manage individually.
- **Hands-on experience** Ask about experience in the public sector and at the scale your organization requires. Ensure the provider has expertise in voice and data networks, as well as with the cloud.
- **Interoperability** Choose an MSP that uses open standards-based technology and is not married to any one brand or product. Doing so simplifies the integration of legacy systems and ensures that the organization is not locked in to a specific vendor.

This piece was developed and written by the Center for Digital Government custom media division, with information and input from CenturyLink.

ENDNOTES
1.   Center for Digital Government. Network-Powered Transformation. August 2016.
2.   http://www.nascio.org/Publications/ArtMID/485/ArticleID/412/2016-State-CIO-Survey-The-Adaptable-State-CIO
3.   Ibid.

PRODUCED BY:

CENTER FOR
DIGITAL
G O V E R N M E N T

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

FOR:

CenturyLink®
Government

CenturyLink helps government, education and public safety sector organizations implement proven IT solutions to address public infrastructure continuity, ensure safety and security, facilitate economic growth, build stronger educational systems and augment technology needs. To learn more, **visit: www.centurylink.com/ges**