Preparing for the Network of Tomorrow, Today

A government executive's guide to understanding the **network of the future** and its role in transformative change.

government technology

AT&T

Images on cover and pages 2, 8, 18, 22 and 24 are provided by istock.com.
Images on pages 4, 6, 12, 14, 16 and 20 are provided by shutterstock.com.

90%
of state government agencies say at least 1/5 of their IT infrastructure is a legacy system.

In Dallas, intelligent sensors will detect when a street light is out and automatically alert repair crews. In the San Francisco Bay Area, officials will use video analytics from traffic cameras to monitor congestion and automatically adjust express lane tolls. And in Georgia, virtualization and other new technologies will enable the state's central IT organization to roll out new capabilities faster than ever before to support the needs of state agencies.

It's clear that state and local governments are in the midst of a technology revolution. Cloud models, "as-a-service" solutions, Internet of Things (IoT), artificial intelligence (AI), mobile devices and other innovations are already helping public sector organizations improve services to constituents; save money, time and labor; and keep workers happier and more productive.

But fundamental to these advancements is network connectivity on an unprecedented scale. As states and cities grow smarter and more connected, enterprise networks will need to be more scalable, available, accessible and secure than ever before — even as architectures, devices and applications continually evolve.

This is tough to do, however, when capital-intensive networks are reaching end of life and are difficult to maintain. According to a NASCIO survey, 90 percent of state government agencies say at least one-fifth of their IT infrastructure is a legacy system. It's a risky way to operate.[1]

"[Government agencies] used to be able to buy equipment for their networks, and as long as it still received power they could use it for a long time with the intent of using scarce government dollars as efficiently as possible," says George Spencer, associate vice president, AT&T Public Sector. "Over time, it's harder to maintain this equipment, so they fall behind."

Old network strategies simply won't work in an environment where new technologies emerge at an exponential pace, user expectations change rapidly and security threats continually multiply — all while state and local budgets remain stagnant.

It's time for forward-thinking government leaders to embrace a new approach. We call it the network of tomorrow. This guide will show you what it is, and how you can get there.

The Network of Tomorrow

The network of tomorrow is characterized as much by the technology that underpins it as the innovation it enables. While yesterday's network was based on capital-intensive hardware implementations, the network of tomorrow is software-based, enabling organizations to flexibly set up, change and secure network environments without purchasing and deploying expensive physical devices. Instead, features and capacity can be changed via software configuration. And intelligent automation within the network enables it to deliver a level of performance and reliability that is crucial in an everything-is-connected world.

"It's really about an intelligent network," says Greg Kaleski, product marketing manager, AT&T Public Sector. "The WAN is no longer a static, one-size-fits-all thing, because you can now control the route that different apps can take; you can have one vendor bringing in a wireline connection and another vendor bringing in a mobility connection and then route preferentially based on your needs."

The result of these capabilities is a network that quickly scales up capacity when it's needed and scales back down when it's not. This software-centric, cloud-based approach also alleviates staffing and resource burdens associated with in-house network deployment. Agencies can add applications to the network without waiting for the IT team to build out more bandwidth; therefore, new services roll out remarkably fast. Just as important, sophisticated security features are built in and maintained by top industry talent.

"Software-defined networking enables a new model and that's significant. We aren't just evolving; we are looking at a paradigm shift for how governments provide service to their end users," says Michael Keenan, technical sales manager, AT&T Public Sector. "We're moving from a model where you're locked in with different vendors and buying a whole bunch of boxes that you have to support to an approach where you are subscribing to a service and paying a rate for what you use."

Network of Tomorrow Tenets

Software-Defined Networking (SDN)
This is an architectural framework to create intelligent networks. Using virtualization, automation and other technologies, it enables organizations to respond more quickly to change, centralize traffic management and deliver network services anywhere in the network, regardless of the specific devices that the network connects to.

Network Functions Virtualization (NFV)
This replaces dedicated routers, firewalls and other traditional network hardware with software that runs on commercial servers and performs these functions through an application instead of hardware.

Network as a Service (NaaS)
This is a model for consuming network services virtually on a pay-for-use basis or for a monthly fee. The service provider is responsible for network operations and management.

CASE STUDY

Managed Services and SDN Pave the Way for Growth

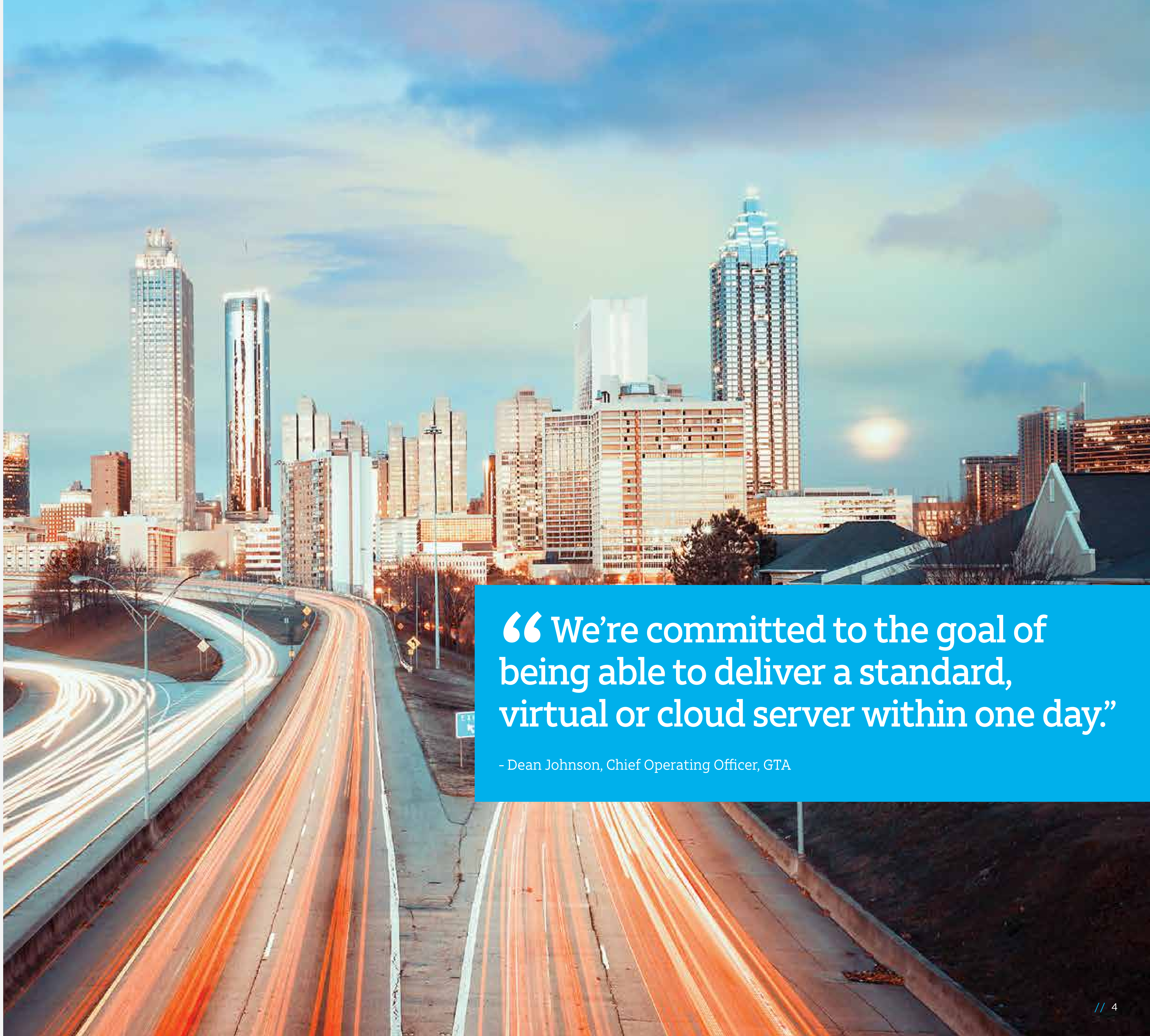
The Georgia Technology Authority (GTA) is the central IT authority for the state of Georgia. In collaboration with AT&T, it's using a managed services approach to deliver wide area network (WAN), local area network (LAN), voice and other network services to the 1,300 state and local government entities that it serves. A third-party integrator handles the day-to-day coordination and management of service delivery. When end users need new network capacity, changes or repairs, they simply put in a request for service.

"Managed services save the state a lot of time, effort and resources; the network is secure, reliable and recoverable; and there's a built-in refresh cycle so technology is always up to date," says Dean Johnson, Chief Operating Officer of GTA.

The solution has also alleviated the need for a large staff of skilled network technicians because qualified service providers handle day-to-day technical tasks.

As part of its collaboration with AT&T, GTA plans to implement SDN and more virtualization within the next few years. SDN is essential for Georgia to meet its growing IT demands, including delivery goals that GTA established in a new contract for server services. GTA needs to enable faster network provisioning so that it will align to the rapid provision capabilities the service provider plans to implement.

"We're committed to the goal of being able to deliver a standard, virtual or cloud server within one day," says Johnson. "These aggressive timelines are light years from where we are today, and they would be very difficult to meet without introducing more automation and some prepackaged functionality — such as pre-assigned IP addresses, VLANs and firewall configurations — that we're currently working with AT&T to architect and engineer."



> “We're committed to the goal of being able to deliver a standard, virtual or cloud server within one day.”
>
> - Dean Johnson, Chief Operating Officer, GTA

Future Ready

The network of tomorrow helps state and local organizations prepare for many current and future challenges and trends, such as cybersecurity, mobility, IoT and other innovations.

Enhancing Cybersecurity

According to NASCIO, security and risk management has been the No. 1 priority of state CIOs for the last five years.[2] But recruiting and retaining qualified IT and cybersecurity staff is a huge challenge for state and local governments, who are losing expertise and institutional knowledge at the same time they must compete with the private sector for skilled IT and cybersecurity personnel.

"Many state and local governments struggle to acquire and maintain the resources required to gather intelligence and protect themselves, their constituents and their critical infrastructure from digital attacks," says Princess Young, a cybersecurity awareness program lead for the Department of Homeland Security.[3]

And although cybersecurity is a top priority in most organizations, the approaches many of them take to prevent breaches are antiquated.

"The prevailing methodology in cybersecurity right now is the defense-in-depth approach, where organizations put hardware appliances in place to do specific security functions," says DuWayne Aikins, principal architect, AT&T Public Sector. "But that's costly and time consuming, and by the time those solutions are installed they need to be refreshed. They simply can't keep up with the rapidly evolving threat landscape or today's extensive network ecosystem."

Today's attacks are often stealthy, targeted and persistent; range from ransomware and distributed denial of service (DDoS) attacks to encrypted malicious web traffic and phishing attacks; and exploit vulnerabilities in cloud services, mobile applications, the IoT and other resources.

Emerging technologies and the movement of data to and from off-premises locations further expose the network to vulnerabilities and risks. Traditional security hardware such as firewalls, routers and intrusion prevention systems cannot protect data once it leaves the enterprise, and it is inadequate against threats that use encryption or other legitimate resources to make it past ordinary lines of defense.

The modern threat environment requires a shift in focus to intelligence gathering, incident detection and rapid remediation. The network of tomorrow allows states and local governments to easily incorporate these functions via virtualization and managed services. In addition, the network of tomorrow is easier to set up and provision than a traditional network, which means IT and cybersecurity teams can quickly adjust configurations to reduce risks and remediate threats.

> “When functions are centralized and virtualized, it’s a lot easier to have a unified security posture.”
>
> - DuWayne Aikins, Principal Architect, AT&T Public Sector

"When functions are centralized and virtualized, it's a lot easier to have a unified security posture," says Aikins.

"The use of software and virtualization is vital for both current and aspiring cybersecurity professionals to face the unique challenges that this field presents," adds Young. "These technologies are particularly powerful when combined with other resources and research, including everything from educational programs to other risk management solutions."

Looking into the future of network security, Don Parente, associate vice president of engineering and architecture, AT&T Public Sector, foresees the increased use of SDN for network compartmentalization. Many government intranets have thousands of public sector employees on them. With such ubiquitous access, the insider threat and the risk of unauthorized access increase.

"With SDN, we can quickly set up purpose-built networks with very few people on them. If you can define a network in near real-time and reduce authorized communities to smaller groups, then you can contain information more easily," says Parente.

Tips for Success: Engagement and Communication are Key

Industry experts agree that open information sharing within an organization and with technology vendors is vital to maintaining a robust security posture. George Spencer, associate vice president, AT&T Public Sector, says that many CISOs and their organizations make the mistake of going at it alone and think their team and security controls are sufficient to fully protect their environment.

"It takes an army to successfully win the battle on an ongoing basis," he says.

Spencer recommends organizations engage in public-private partnerships and keep the lines of communication open.

Young agrees: "Collaboration across all sectors is increasingly vital to the security of organizations and individuals across the nation. Sharing threat indicators, potential risks, observed trends and new technologies allows us to build resilience against cyber threats."

> “With virtualized security functions, greater visibility and automated controls, we can add capacity and take advantage of new opportunities much faster.”
>
> - Phil Bertolini, CIO, Oakland County, Mich.

CASE STUDY

Improving Security with SDN

The use of shared services is a main tenet of Michigan’s Oakland County Department of Information and Technology. Recognizing that not all departments and agencies have the IT expertise and resources to do everything on their own, the county uses a model where the larger organization shares services with smaller ones. One example is its G2G Cloud Solution, which provides e-commerce capabilities to counties throughout the state and is supported by network services from AT&T.

“We’ve found that by sharing, smaller governments don’t need to buy and we can lower our overall cost of transactions,” says Phil Bertolini, CIO for Oakland County.

Security is woven into shared services. This approach takes the burden off smaller departments and helps ensure they are protected. Ultimately, it also protects the network as a whole.

“Without the network, none of this happens. The cloud, IoT and other innovations don’t work without connectivity,” says Bertolini.

To that end, the county is in the middle of a complete modernization of its networks. SDN and virtualization are key aspects of the overhaul and will enhance the department’s ability to quickly secure and manage traffic across these networks.

“With virtualized security functions, greater visibility and automated controls, we can add capacity and take advantage of new opportunities much faster, at far lower cost and with more consistent security policies across the network,” Bertolini says.

Government on the Go

State and local agencies need to provide ubiquitous, on-demand network access to multiple groups of users, including a new generation of remote workers and a diverse constituency.

"Governments are trying to support a workforce that increasingly includes employees who want to log in from home or a local café. They are also trying to accommodate remote work to alleviate the high cost of office space and improve productivity and workflows for people in the field," says Keenan.

At the same time, citizens, businesses and private partners expect 24/7 access to personalized, consumer-like mobile services, as well as smart city innovations that improve quality of life, save taxpayer dollars and spur economic growth.

This demand for a more mobile-friendly government not only increases WAN traffic and bandwidth requirements, but also introduces new routing challenges as thousands of devices at the edge attempt to access network resources and cloud-based services. Smart devices, which are now the computing device of choice for many users, strain the network even further and create unpredictable demand by streaming video, using VoIP and performing other data-intensive processes.

Traditional hardware-based network approaches cannot scale as quickly and flexibly as needed to meet this demand. They cost too much, take too long to deploy and rely on human intervention.

The network of tomorrow provides flexible, software-based network services that, in essence, can run themselves. By allowing the network to automatically create virtual network connections, these services can provide processing power and new routes on demand. Organizations can accommodate citizen, workforce and line-of-business demands for secure, reliable, high-performance mobile connectivity within days — if not hours.

Using SDN and virtualization, for example, agencies can automatically provision additional capacity in the event of a disaster; use quality of service (QoS) prioritization to ensure critical applications are continuously available to mobile users; differentiate routing so highly sensitive mobile communications travel a different, more secure route than other types of data; and optimize routing to make the best use of existing resources.

Tips for Success: Plan for the Non-Wired WAN

In the near future, schools and some government agencies won't have wired connections anymore because their networks will be based on 5G or 6G cellular connections. As this evolution continues, organizations that support WAN will have to consider non-wireline solutions and their strategy to implement them.

"With WAN, you have to start thinking about mobile data connections, because whether they're supportive, backup or — with the advent of 5G — primary WAN connections, you're now moving away from a purely wireline model to these new technologies," says Spencer.

CASE STUDY

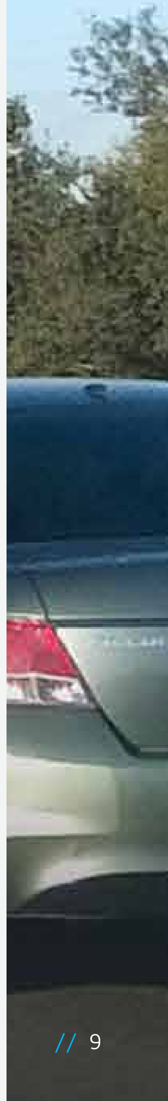
Using Technology to Beat Traffic

The Contra Costa Transportation Authority (CCTA) in California's Bay Area is working on several projects that rely on mobile connectivity to improve transportation across the region. One project is to relieve heavy congestion along Interstate 680. The project will rely on video cameras to monitor traffic speeds, and then use that data to automatically set tolls for express lanes. In addition, when traffic drops below a certain speed, buses will be able to use the right shoulder, and ramp meters will hold traffic on nearby onramps until a bus passes by. All of this will be coordinated via the wireless network.

When asked what organizations should consider when undertaking similar projects, Randy Iwasaki, Executive Director of CCTA, emphasizes the importance of network reliability and flexible bandwidth.

"Network safety from both the transportation and mobile connectivity perspective is going to be increasingly important," Iwasaki says. "You're going to get a lot more data from cell phones in the future and you need a network that can handle that. You have to have a redundant system to ensure network communication is never lost, and you need expandable bandwidth for quickly relaying high volumes of video and other data back and forth."

> “You're going to get a lot more data from cell phones in the future and you need a network that can handle that.”
>
> - Randy Iwasaki, Executive Director, CCTA



The Explosion of Endpoints

States and cities are adopting IoT technologies to do everything from manage energy efficiency in public buildings to monitor flood levels.

While IoT brings new levels of efficiency, cost savings and innovation to state and local governments, it also creates new complexities. IoT not only increases the amount of data traveling across the network, but also the number of endpoints — potentially hundreds of thousands — connecting to the network. In addition, each device and use case has unique requirements for power, bandwidth, reliability and communication with other applications or devices. These requirements impact the type of network technology IoT requires (e.g., Bluetooth, Wi-Fi, 4G, or Ethernet/LAN); depending on the use case, organizations may need to create multiple network connections.

IoT security is also a challenge. Besides concerns about device vulnerabilities, organizations must be sure the network itself and data connected to devices is protected.

Next-generation networks give organizations the tools they need to flexibly set up, customize and secure IoT networks. SDN allows them to centrally manage data flows on highly distributed IoT networks; NFV allows them to virtually provide the unique combination of functions that each IoT use case requires; and NaaS allows them to quickly add bandwidth as needed. For example, an organization can partition part of the network infrastructure to provide a virtual dedicated space for a specific application.

> “You can mitigate that (human) threat by separating networks for things from networks for people.”
>
> - Don Parente, Associate Vice President of Engineering and Architecture, AT&T Public Sector

Tips for Success: Implement an Intranet of Things

When it comes to IoT security, AT&T advocates for an “**Intra**net of Things” rather than a public internet of things. An **Intra**net of Things is an internal network with private IP addresses. With a next-generation network, organizations can easily set up an **intra**net for a specific purpose.

“People are one of the main causes of breaches — whether because they mistakenly click on a malicious email or intentionally do harm. With the flexibility of an advanced, software-based network, you can mitigate that threat by separating networks for things from networks for people,” says Parente. “The network is already there. It’s just a simple matter of provisioning.”

> “With a video camera and AI system, we can dispatch crews when the park needs attention.”
>
> - Michael Sherwood, Director of Innovation and Technology, Las Vegas

CASE STUDY

Smart City Connectivity Streamlines Asset Management

The city of Dallas and the city of Las Vegas are using their networks to take IoT to the next level of smart city innovation. In Dallas, a Living Lab in the historic district is home to an intelligent street light project that uses the network to automatically notify the city when a light is out or needs repair.

In Las Vegas, the city’s Innovation District is piloting a park maintenance program that sends video images of the park to the cloud for analysis, and then alerts staff when the grounds are littered or need other care.

Jennifer Sanders, Executive Director at the Dallas Innovation Alliance, paints a picture of the types of benefits that accrue in both use cases.

“Usually when there’s a lighting outage, a citizen must report it to 311 or the utility, or repair trucks roam around looking for outages,” she says. “Now, intelligent sensors will detect that the light is out and automatically notify the city. This creates operational savings by enabling crews to plan repairs and routing more efficiently.”

Besides reducing the cost of truck rolls and labor, the system will also reduce the number of wasted trips by ensuring the right parts are on the truck when it goes to a job.

Michael Sherwood, Director of Innovation and Technology for the city of Las Vegas, points out the benefits of using AI with IoT.

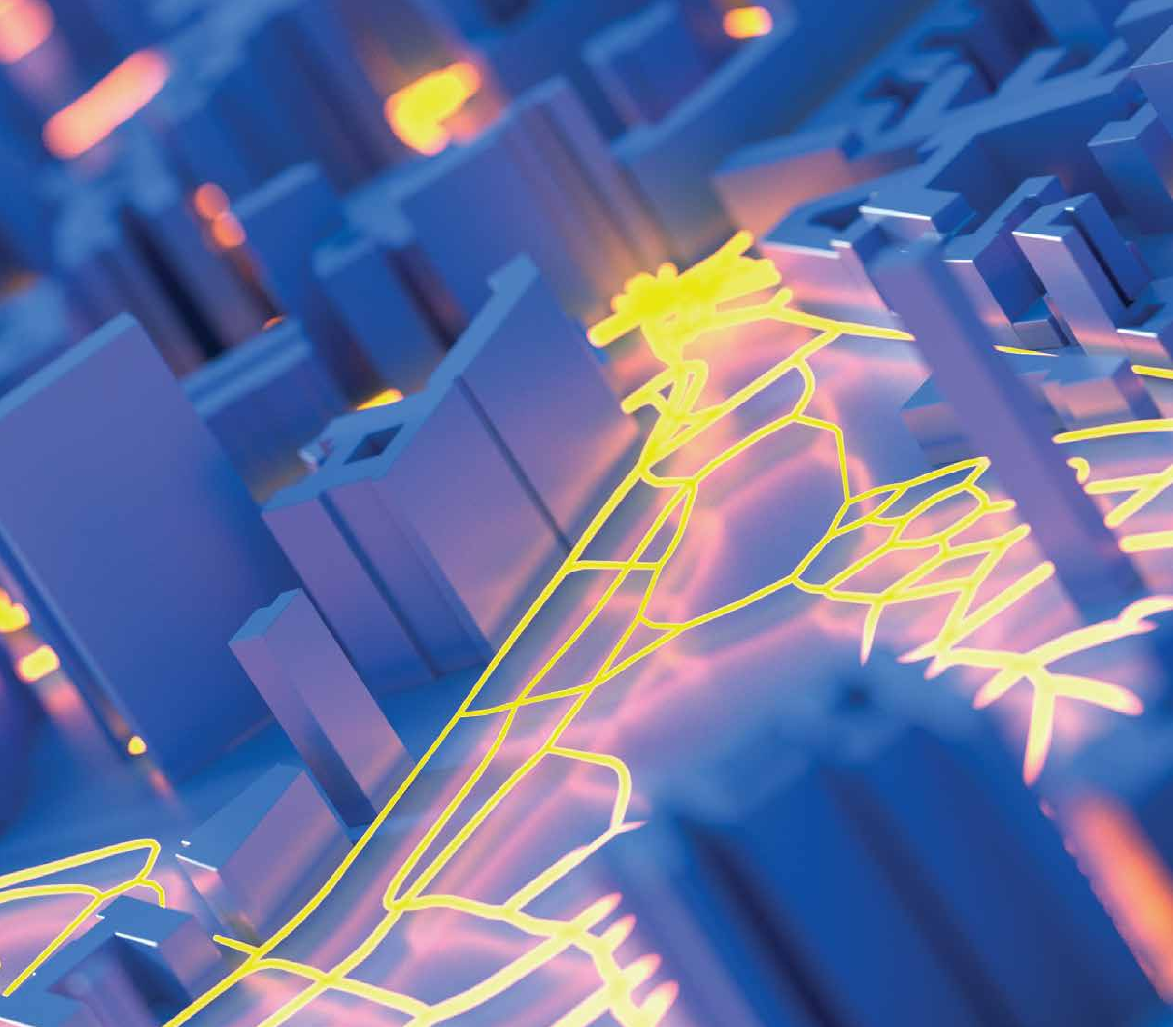
“Today, we manage a park by sending a crew out whether the park is dirty or clean. It’s an inefficient use of resources. With a video camera and AI system, we can dispatch crews when the park needs attention,” he says.

With both cities engaged in numerous complex smart city projects, the importance of a flexible, scalable, reliable and secure network cannot be overstated.

“We’re a mix of Wi-Fi, fiber, cellular and microwave networks; it’s important to have a network that supports multiple use cases and connectivity options,” says Sanders.

Sherwood notes that security is always top of mind in IoT projects.

“We have a living, breathing network made of many systems combined together. The most important piece of IoT is the data, and we need to protect that data to protect people, public safety and the network as a whole,” he says.



The Promise of a Faster Network

The fifth generation of mobile networks, 5G, will ultimately revolutionize the way government entities operate and serve citizens. In December 2018, AT&T became the first and only company in the U.S. to offer a mobile 5G network. 5G and edge computing have the capacity to deliver an unprecedented opportunity to augment and elevate the human experience.

Edge computing can shift the workload of transmitting vast amounts of data away from hardware to the network, through software-defined applications. This model allows businesses to route applications' specific traffic to where they need it and where it's most effective, whether that's in the cloud, the edge of our network or on their premises. Today's applications are high-performance and power hungry, generating massive amounts of data that require real-time computing power.

"Edge computing helps fulfill the promise of the cloud to transcend the physical constraints of our mobile devices," says Andre Fuetsch, president of AT&T Labs and chief technology officer, AT&T Communications. "The capabilities of tomorrow's 5G are the missing link that will make edge computing possible."[4]

Mobile 5G will be about more than just speed. It will also eventually bring ultra-low latency — a key enabler for virtual reality, autonomous vehicles and IoT, all of which depend on a highly efficient network response to orchestrate data rich experiences. Meeting the security challenge for 5G mobile networks is a key focus for service providers, manufacturers and other stakeholders. Some believe moving computing power and other capabilities closer to the edge inherently makes networks less secure. However, technologies such as network virtualization and edge computing together with device management and automated threat detection and response will help create more flexible and highly secure networks to meet this challenge. Software-defined networking makes it possible to develop a multilayered approach to security that simultaneously considers the communication layer, hardware layer and cloud security. Government operations stand ready to benefit from sophisticated access management capabilities while increasing their security against distributed attacks by cyber threats.

In addition, AT&T is working to enable an ecosystem of 5G devices, all connected to an intelligent, software-driven network that can react in near real-time. With these capabilities, ideas that seemed like science fiction will increasingly start to become reality. Tomorrow's robots will be deep learners, harnessing edge computing to process massive amounts of data in order to get smarter as they go about their business. The successful progression of 5G networks will deepen the human-machine relationship.

AI and human "hybrid intelligence" combines human knowledge, flexibility, beliefs, and instincts along with the blindingly fast speed and steadiness of machine logic.

"Robots will learn from their mistakes and share what they learn collectively so all of the robots improve over time," says Ken Goldberg, UC Berkeley Professor of Robotics, Automation and New Media.[5] Instead of fearing a robot revolution, we can look forward someday to working alongside intelligent machines designed to help us successfully achieve our goals.

In addition, 5G will eventually support an explosion of immersive experiences as mixed reality and digital twins expand our reach. Digital twins are real-time digital models of our cities, factories and other environs that could enable predictive, crystal ball-like simulations. As populations continue to grow, city planners are constantly challenged with the impacts to traffic patterns, pedestrians, video surveillance, real estate and more. Over the next decade, the network will become an overlay on top of our physical world. Virtually every object, every interaction and every observation will become a piece of data which informs advanced simulations. The use cases across the public sector seem limitless.

5G's ultra-fast speeds and ultra-low latency will ultimately help enable a convincing virtual world for learners to collaborate as never before. Recess could become in-the-field research by superimposing a digital understanding of physics on playground equipment. Imagine high school students thousands of miles away controlling a robot inside an active volcano. And graduate students across the world exploring the rain forest together and virtually discussing their findings. Each of these learning experiences will be social, connected, collaborative and immersive — driving deep engagement and elevating the human experience.

The AT&T 5G Innovation Program, launched in February 2019, will develop ideas and test use cases with industry leaders on AT&T's live mobile 5G network. The goal is to bring future 5G experiences to life today.

"What's vital here is to create the right conditions for 5G innovation to flourish," says Fuetsch. "We believe 5G will ultimately be the "yes, you can" network — regardless if you're a global enterprise, government agency, education institution, small business or consumer. These are just some of the ways we're fostering innovation in 5G environments to create tomorrow's unforeseen inventions."

Mobile 5G will be about more than just speed. It will also eventually bring ultra-low latency — a key enabler for virtual reality, autonomous vehicles and IoT.

Getting Started

Industry experts recommend the following suggestions to better understand, design and activate the network of tomorrow.

UNDERSTAND

Identify stakeholders' needs.
The Georgia Technology Authority (GTA) invites executive branch agencies to actively participate in defining business and technical requirements and evaluating proposed solutions.

"Doing so helps ensure that service providers meet individual agencies' needs in addition to the needs of the enterprise, and helps to ensure buy-in throughout the life of the relationship," says Johnson of GTA.

Understand the current landscape and environment.
Document what is on your network or what connects to your network (e.g., data, applications, mobile devices, SaaS applications, IoT sensors) and understand how each component impacts your network.

DESIGN

Develop a plan.
Clarify business goals and map those goals to the appropriate technology. Consult with the vendor community to understand what's possible and determine a roadmap for getting there.

"Organizations usually need help to understand and segment their scope of work into areas. They have to take into account applications, resources, budget, procurement vehicles and more. It's not just about technology. It's about what happens on Day 2 and how you operationalize it and take care of it," says Samantha Thibault, director of emerging technologies, AT&T Public Sector.

Prioritize.
Don't wait to resolve every issue before getting started. Determine what you can do most quickly, look for quick wins and break projects into smaller, iterative pieces.

"Doing things with software is much faster than doing things with hardware. You can instantiate new network functions virtually, simply by logging into a portal," says Keenan.

SDN and virtualization also allow organizations to develop and test disruptive technology more quickly and iteratively, which allows them to fail faster.

"Failure is a part of innovation, and it's better to fail early than at a large scale," Keenan says.

Incorporate all anticipated work into a single plan.
A master plan facilitates project management, helps standardize approaches and allows you to negotiate the best rates and contracts.

Update network procurement practices and policies.
Be sure RFPs and other processes can accommodate new service models, such as NaaS. Where possible, take advantage of other organizations' contract vehicles to streamline procurement.

Formalize processes.
Doing so ensures network capacity and security requirements are always considered (and budgeted for) when new services are added or infrastructure changes are made.

Pick your vendors wisely.
Choose a stable, experienced vendor that has a history of success and a culture of innovation.

ACTIVATE

Educate.
Be sure procurement staff and legislative bodies understand the unique characteristics and requirements of a next-generation network. Provide IT personnel ongoing training in managing services and performing other tasks that are not traditionally within their purview.

Communicate.
Share information and solicit input internally, across departments and agencies, and with vendors to encourage adoption and stay current on opportunities and risks.

CONCLUSION

The Future is Now

The hardware-defined networks of yesterday can no longer keep up with the shifting network landscape and growing demands of today and tomorrow. The network of tomorrow allows users to simply go to a web portal to set up, change and secure network capabilities on demand. In just a short time, the portal will be seen as a stepping stone to even greater possibility, where applications can automatically self-provision additional bandwidth and the network becomes increasingly programmable.

Regardless of where government organizations stand on the road to the network of tomorrow, it's time to move forward. The opportunities are waiting, and the future is now.

Endnotes:

1. NASCIO. The 2016 State CIO Survey – The Adaptable CIO. September 2016.
2. NASCIO. State CIO Top Ten Priorities for 2018 (as well as for 2014, 2015, 2016, 2017). nascio.org/Portals/0/Publications/Documents/2017/NASCIO-TopTen-2018.pdf
3. All quotes from Princess Young received via an email interview in July 2018.
4. AT&T Futurist Report "A Faster, Smarter Future: Emerging Applications for 5G and Edge Computing" in collaboration with the Institute for the Future (IFTF)
5. Ibid

AT&T

Our first name has always been American, but today you know us as AT&T. We're investing billions into the economy, providing quality jobs to over 200,000 people in the U.S. alone. We're supporting the veterans who make our country stronger and providing disaster relief support to those who need it the most. By bringing together solutions that help protect, serve and connect — committed AT&T professionals are working with the public sector to transform the business of government. No company is more invested in America's future than AT&T.

att.com/publicsector

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

govtech.com