Full-Speed Ahead:
How to Create a Solid Foundation for Government Modernization
It’s no secret that a potent combination of new digital technologies and rising constituent expectations is transforming government. The impact is being felt at all levels, from the largest state agencies and departments to the smallest municipalities.

For example, the Smart Cities concept is becoming ubiquitous, fueled in part by a White House initiative that is bringing millions of dollars to local communities to improve the life of residents. Projects like these can attract entrepreneurs and help current businesses expand, but only if local agencies differentiate themselves from competing locations. Digital modernization is an important way to do that.

For example, the city of Boston participates in New Urban Mechanics, a network of civic innovation offices composed of public and private organizations. One participant is Soofa, an MIT Media Lab spinoff that piloted solar-powered phone charging benches that are part Smart Cities, part Internet of Things. Benches based
on the pilot designs are now being installed in eight U.S. states and three countries.

That’s just one example of how the public sector is fostering a fertile age of innovation. States, cities and municipalities are also transforming their static, first-generation websites into interactive resources that help people and businesses quickly access important information and interact with state representatives.

Behind the scenes, state and local governments are making internal operations more efficient. This includes having access to cloud solutions and new types of applications, including Voice over Internet Protocol (VoIP), which delivers efficient services such as automatic call routing that tries various numbers associated with on-the-go workers before sending callers to voicemail.

All of these innovations have something in common — they require a high-speed and secure networking infrastructure. That takes a mix of reliable wide-area network (WAN) services, internal Wi-Fi networks and public wireless implementations to serve citizens, businesses and visitors.

Of course, networks alone aren’t the only consideration. Government leaders are also taking a fresh look at consolidating and updating their data centers, servers, email systems and other core areas. In some cases, the cloud is the answer for these initiatives; in other cases, it means contracting with managed service providers for their expertise, which frees internal IT staff to work on the agency’s mission-critical projects.

But because modernization consists of so many moving parts, planning and implementation can be difficult for resource-strained IT staffs. What’s needed is a strategic plan to guide government leaders to determine what new technology best serves their overall service goals. To start crafting this plan, decision-makers should focus on six key areas, including a special emphasis on the underlying networking infrastructure.
How to Create a Solid Foundation for Government Modernization

A. Smart City Services
The city of Charlotte, N.C., partnered with a local utility to create Envision Charlotte, an initiative designed to reduce energy use in large buildings by 20 percent over 5 years. As of June 2015, the city had reduced energy consumption by 16.1 percent in the 61 buildings taking part in the initiative, saving $17 million in energy costs.

B. Safer City Services
To improve public safety, Charleston, S.C., connects personnel, systems and applications across diverse organizations. Police officers and other first responders in Charleston can quickly communicate and retrieve data, images and forms to help them make accurate decisions. Various departments can work together more efficiently to address the needs of their neighboring jurisdictions.

C. Modern, Interactive Websites
After the state of New York relaunched its website with the design goal of improving user experience, the number of visitors doubled, mobile traffic tripled and page views quadrupled to more than 17 million.

D. Videoconferencing over IP
Courthouses are using Videoconferencing over IP for remote pleas and testimonies. For example, more than 400 courtrooms in the state of Michigan now have videoconferencing capabilities, which has saved the Michigan Department of Corrections nearly $5 million over 2 years.

E. Voice over IP
State and local agencies are using VoIP to eliminate the cost of maintaining traditional private branch exchanges (PBXs), the legacy and closet-sized hardware installations that historically handled phone calls. For example, Dayton, Ohio, is expected to save more than $500,000 from its 2015 VoIP implementation.
F. Cloud-First Initiatives
Software-as-a-service, infrastructure-as-a-service and other cloud models are helping the city of Miami, the state of Delaware and other government organizations transition from costly legacy applications to on-demand services that can grow and change as mission demands evolve.
Six Steps for Devising a Foundation for Success

Creating the Right Networking Infrastructure

From the largest states and cities to the smallest municipalities, the public sector is undergoing large-scale modernization projects. To serve constituents now and in the years ahead, government agencies need a strategy to build the right networking infrastructure. The following six steps can help state and local governments build a solid foundation for modernization initiatives.

Step 1: Manage with Constituents in Mind

The expectations of constituents and what government demands from technology continue to grow. A decade ago, photographing a pothole and sending it with its location coordinates to the public works department was a dream. Now, citizens take services like this for granted. As new mobile apps, social networks and the Internet of Things promise a world of even greater connectedness, government stakeholders must challenge each other to always ask themselves, “What’s next?”

To answer that question, IT and department managers must communicate regularly to identify top opportunities for new constituent-facing and internal services. Technological innovation is certainly a key driver — IT managers must update their peers on the art of the possible — but agencies must avoid scattershot reactions to what are billed as the latest and greatest solutions.

Evaluations must start with considering ways to better meet mission goals, address constituent needs, increase service and uptime levels, and meet budgetary requirements. With those parameters in place, agencies have a framework for determining what networking and related IT capabilities will have the biggest impact.

Step 2: Blend Old and New Technology

Unlike sexy startups in the commercial world, state and local governments don’t have the luxury of a clean slate when it comes to implementing new technology. Government IT managers should audit their current networking
environment, including all hardware, software and service contracts. With this information in hand, they can identify gaps in networking capabilities and prioritize new investments according to which ones have the potential to deliver the most value.

Fortunately, when it comes to modern networks, agencies can choose from a range of effective options — some well-established, others representing the latest advancements in key standards.

Start by re-evaluating existing WAN services. These essential resources maintain high-speed and reliable connections to the internet, as well as the various divisions and field offices that multi-location agencies maintain to deliver citizen services. The foundation technology for effective WANs is Multiprotocol Label Switching (MPLS), a bedrock standard that after years of supporting critical applications has proven its resiliency and self-healing characteristics. If network problems arise that threaten to slow performance, MPLS can automatically reroute traffic around broken segments and other trouble spots to minimize any problems to the end-user experience.

MPLS is also the foundation for easy network sharing among multiple government agencies. The usage of the network is optimized and operations are simplified, offering a framework to conserve government resources.

Building on the maturity and effectiveness of MPLS is Metro Ethernet (aka Carrier-Grade Ethernet), which brings the simplicity of the ubiquitous local-area network (LAN) protocol to WANs. Leading WAN service providers can tailor Metro Ethernet to the unique needs of each agency to connect several facilities within a metropolitan area. The best providers combine the ease of management available from traditional Ethernet LAN technology with a highly resilient and reliable optical fiber network.

Before committing to a Metro Ethernet provider, officials should look for services that comply with the Carrier Ethernet 2.0 specification from the Metro Ethernet Forum, which defines WAN-related capabilities that go beyond those used in traditional Ethernet LANs.

Because of widespread familiarity with Ethernet among IT technicians, Metro Ethernet is a good choice for agencies that plan on using their in-house staff to manage core routing of network traffic.

As new mobile apps, social networks and the Internet of Things promise a world of even greater connectedness, government stakeholders must challenge each other to always ask themselves, “What’s next?”

David Kidd
However, not all agencies consider it viable to devote internal IT resources to core routing. For those that want to offload these WAN responsibilities to an outside service provider, there’s Internet Protocol Virtual Private Network (IP VPN). Like Metro Ethernet, IP VPN runs as a layer on top of an MPLS base, but with the fundamental difference being that the service provider manages routing requirements.

Otherwise, Metro Ethernet and IP VPN offer similar networking capabilities for connecting multiple, geographically dispersed sites within a private and secure network. This includes comparable quality of service, latency rates and data delivery ratios. Look for services that offer the flexibility to grow to multiple gigabit per second (Gbps) speeds, and that provide protected connectivity to data centers and other high-bandwidth locations.

The fastest and most expensive choice is to use fiber-based transport solutions for the “last mile” link. At the other end of the spectrum is digital subscriber line (DSL), a more economical and widely available choice, but not one that performs as well as fiber for high-speed or interactive traffic, such as video or large graphics files. Hybrid fiber coax (HFC) blends the benefits of these two options for agencies looking for a middle-ground balance of price and performance.

<table>
<thead>
<tr>
<th>Agency Need</th>
<th>Relevant Technology</th>
<th>The Payoff for Government</th>
</tr>
</thead>
</table>
| Backbone for WAN connections to the internet and satellite agency offices | Ethernet or IP VPN | • Mature, proven track record for reliability  
• Reroutes traffic past problems to maintain high performance  
• Foundation for network sharing and optimization of resources |
| Easy-to-use WAN protocol for linking dispersed facilities | Metro Ethernet | • Offers the simplicity of the ubiquitous LAN protocol  
• Can be tailored for individual needs  
• A good choice when in-house staff manages core routing of network traffic |
| WAN technology for when outside service providers manage core routing | IP VPN | • Like Metro Ethernet, runs as a layer on top of an MPLS base  
• Integrates with your network at layer 3 (IP)  
• Outsourcing mundane tasks and management allows IT staff to focus on constituent needs |
| High-speed connections for creating private networks | A secure and private networking solution such as IP VPN or Metro Ethernet | • Excellent choice for connecting data centers or other high-speed/low-latency applications |
| Quickly react to new wireless standards and shift traffic patterns to keep Wi-Fi performance at optimum levels | Managed Wi-Fi services | • SLAs designed to ensure agency performance requirements  
• Can save costs by mitigating capital investments for new equipment and staffing |
Step 3:
Optimize Internal and External Resources

Re-evaluate how to balance investments in internal resources with contracting for outside services or working with existing service providers. Agencies must decide whether to contract only for the network links themselves, and devote their internal staffs to bring them to life — including procuring, implementing and managing new routers, performing ongoing network maintenance and addressing any breakdowns.

The alternative is contracting with an outside provider to deliver high-speed networking services, including the physical and management components. In addition to determining who takes responsibility for the network, the choices come with important financial considerations — internal management requires expenditures for hardware and other items from capital budgets, which means upfront investments and depreciation allowances. In addition, prudent organizations will want to maintain a rainy day fund for unplanned equipment failures. By contrast, payments for the service-provider approach come from the operating budget and are predictable from month to month.

As they weigh the pros and cons of these approaches, agencies should consider their technology road maps for the next 18 months as well as over the next 2 to 3 years. After analyzing the mission goals and the networking capabilities that will be required to support them, decision-makers will have a clearer idea of what’s needed to keep pace with technology advancements, new security threats and industry best practices.

Wi-Fi Evolves

WANs aren’t the only part of the networking infrastructure that need extra attention to support modern government services. Wireless networks keep government employees productive by enabling on-the-go collaboration and access to important data and applications. But like WANs, the wireless landscape is dynamic. New capabilities, such as the Wave 2 enhancements to the 802.11ac standard, arrive regularly to provide additional capabilities in coverage and bandwidth. In addition, shifting

Network Reliability:
More Important Than Ever

According to a 2016 report from the Ponemon Institute, the average cost of an unplanned outage for government is $476,000. Across all enterprises, the average cost per minute of an outage is $9,000.8
traffic patterns constantly impact where and how many access points are needed to keep performance at optimum levels. This makes network design and management a full-time job that can strain internal networking staffs.

For reasons such as these, agencies are turning to managed Wi-Fi services operated by specialists who can give wireless networks their complete attention. Managed Wi-Fi services not only optimize resource allocations, but can save costs by mitigating capital investments for new equipment, as well as payroll expenses for a staff of skilled technicians.

In a fast-changing environment, government agencies can risk placing the wrong bets on emerging technology. Managed services, whether for WANs or Wi-Fi, let service providers take on these risks.

Managed Wi-Fi services not only optimize resource allocations, but can save costs by mitigating capital investments for new equipment, as well as payroll expenses for a staff of skilled technicians.

Step 4: Engineer Networks for Security and High Availability

WAN services based on MPLS offer a solid security foundation because by design they segment each customer’s traffic flows into what’s essentially a private network that keeps unauthorized people from hacking into the communications channel to intercept data.

Whether on Wi-Fi or wired networks, agencies can further protect themselves by adopting the Extensible Authentication Protocol (EAP) and the WPA2 encryption standard, which together block unauthorized individuals from signing into a protected network and scramble data to make it unreadable if it falls into the wrong hands.

For high availability, it’s important to create duplicate physical connections to critical facilities to ensure they are reliably connected to the internet. By having two separate paths to buildings, agencies protect themselves from scenarios where a construction crew, for example, accidentally severs a connection during a digging project. If one link breaks, traffic automatically flows to the backup to keep operations running smoothly.

Industry-wide standard metrics don’t exist in the networking industry, so individual service providers may use different measuring methods such as uptime. For example, some providers aggregate data from all of their networks and then determine the collective downtime seen throughout the entire sample and formalize this system-wide approach in service level agreements (SLAs). However, this may not provide an accurate measurement of what individual network circuits are experiencing, creating the possibility that certain customers may see significantly poorer performance and not have recourse to enforce the terms of the SLA.

A better approach is for contracts to be based on monitors running per circuit in the agency’s own environment. This way, if network latency, downtime or other areas don’t meet agreed-upon terms, agencies can ask for refunds.

Step 5: Develop KPIs That Accurately Gauge Performance

Step 6: Continuously Re-evaluate Service Needs and Networking Innovations

Again, this is best done by the same stakeholders who assessed technology opportunities and needs in Step 1. As part of their ongoing meetings, this combination of IT and department representatives should schedule time for
identifying how innovations may enable new service models. These discussions should also factor in expanded reliance on emerging technologies — such as cloud, the Internet of Things, big data and artificial intelligence — and the potential impact of each on the WAN and wireless infrastructure.

Looking Toward the Future
Digital transformation is reshaping state and local government — it’s also putting CIOs in a challenging position. On one hand, they must become change agents who proactively advise department heads about the unfolding opportunities and risks represented by rapid technological innovation. At the same time, IT leaders must ensure valuable existing services continue to support the current needs of constituents. Both efforts are best served with a modern networking infrastructure that brings higher availability and greater security to wide-area and wireless communications.

The right multi-part strategy helps stakeholders achieve their networking goals with the best mix of internal and third-party resources. The payoff is clear: Government delivers the advanced, interactive services citizens and businesses expect today, and agencies further capitalize on Smart Cities, the Internet of Things and other transformational initiatives that will define the future.

Endnotes
1. http://newurbanmechanics.org/about/
2. https://citiesspeak.org/category/technology/
Cox Business knows the ability to securely link locations, public services and emergency response teams is critically important — and becoming more crucial every day. Cox Business offers innovative solutions designed to provide network diversity, operational continuity and the security that government organizations require. In addition, Cox Business solutions are present on nearly every military base throughout the U.S. So whether you have a single communications need, or want to rebuild an entire network, we’ll help strengthen your government agency with solutions that can grow with your ever-changing needs. Call 866-419-6026 or visit www.coxbusiness.com/government.

Many Cox Business services are delivered over Nokia core networking equipment and software that ensures secure, reliable connectivity and capacity to support the digital revolution underway in government. Nokia networking equipment’s support for quality of service, traffic shaping, and new managed service models allows Cox Business and government IT departments to provide cost-effective services that are delivered precisely to customer specifications. For more information, visit www.nokia.com.