

# BUILDING AN INTELLIGENT NETWORK FOR Smart Communities

**M**unicipalities across the country are taking on smart community initiatives. For example, Kansas City is installing video sensors to spot badly parked cars and has installed digital kiosks that serve as city guides. Columbus, Ohio, is building a “smart corridor,” where vehicles can connect to each other and surrounding infrastructure. In New York City, New York University and other organizations are using sensors to collect data on pedestrian traffic, air quality and energy consumption. Examples like these are popping up across the nation in pockets of innovation.

What do these examples have in common? Each of these smart community initiatives requires a robust, intelligent network to serve as its foundation. To stay on the right track and build the smart communities of tomorrow, IT leaders need to establish an underlying intelligent network infrastructure — before adopting cloud architectures, “X-as-a-service,” IoT, data analytics and other technologies commonly associated with smart projects.

An intelligent network provides fast, secure, reliable connectivity to a multitude of applications, devices and resources wherever they are, even as needs change and grow. By leveraging this network to process and exchange the data on which smart projects depend, organizations can realize smart community goals such as stimulating economic development, improving quality of life, increasing public safety, encouraging citizen engagement and more.



## THE NETWORK OF TOMORROW: AN ECOSYSTEM OF CONNECTIVITY

As the foundation for a smart community, an intelligent network must:

- ⇒ **Provide ubiquitous access** to the internet, cloud and other computing services, even for remote locations and unconventional devices
- ⇒ **Support real-time applications** such as Voice over IP (VoIP), video conferencing, community storage and online transaction processing
- ⇒ **Ensure security and reliability** for a broad range of devices and applications
- ⇒ **Maximize application performance** (i.e., reduce network latency and packet loss)
- ⇒ **Reduce operating costs and simplify management**

This level of functionality requires a sophisticated ecosystem with a range of Internet Protocol (IP) and telephony deployment options. These options include fixed connectivity (i.e., fiber or Ethernet) for high-bandwidth connections, low-bandwidth wireless connectivity

(i.e., Long Range, Low Power WAN) for machine-to-machine (IoT) devices, and high-bandwidth wireless connectivity (Wi-Fi and 4G LTE) for mobile devices.

Agencies also need the ability to physically extend networks to reach and connect with new IoT devices and other technologies that support smart community capabilities — often across a large geographic area and to unconventional endpoints. Compounding the challenge, agencies need to provide widespread access to data coming from these technologies, while still maintaining data security.

In developing an intelligent network that enables these capabilities, many cities struggle with a siloed, outdated network infrastructure, bandwidth that is too slow to support real-time operations and applications, and a network infrastructure that is not designed to prioritize and optimize the flow of traffic across the smart community ecosystem. To address these challenges and pave the way for smart community projects, state and local governments often need to re-imagine and modernize their current network.



## LAYING A STRONG FOUNDATION: KEY CONSIDERATIONS

The best strategy for any smart community initiative is to start with an intelligent network that is flexible enough to handle myriad applications and can evolve to provide more advanced capabilities over time. To build a flexible, resilient, carrier-grade network, consider the following:

- ⇒ **Identify key “anchor applications” and their required support metrics**, review the available network technologies and map network solutions to the application requirements. Know exactly how each application will be used before choosing it.
- ⇒ **Ensure sufficient bandwidth to support remote, IoT, mobile and cloud-based applications**, especially for dense urban areas where high demand can slow the network to unacceptable levels. Implement policies and mechanisms for prioritizing network traffic and optimizing bandwidth use based on an asset’s level of importance to the organization. Consider cooperative relationships with local universities and businesses to supplement bandwidth and high-performance computing at peak periods.
- ⇒ **Design for scalability to accommodate new users, devices, servers and applications**, as well as increasing volumes of data and data traffic. Avoid creating data silos within departments and plan for internal and external users to access the network. Simplify operations by using virtualization technologies to help control and manage network services.

## Securing IoT

IoT has expanded the network attack surface to include millions of network-connected devices, sensors and applications. In recent months, cybercriminals have used vulnerabilities in these devices to launch massive spam and distributed denial-of-service (DDoS) attacks. In one high-profile incident, cybercriminals used IoT devices such as webcams and DVRs to launch a massive botnet attack on a popular DNS provider that triggered outages across the United States and Europe. State and local governments can reduce risk by approaching security on these devices as they would approach any other application or resource on their network. This includes changing default user names and passwords; segmenting critical services; testing for vulnerabilities; updating devices regularly; and using encryption, authentication, authorization and other traditional security mechanisms as needed.

⇒ **Build in security and privacy from the beginning by establishing transparent rules for the use of data** and implementing mechanisms to systematically track every new point of connection, evaluate and mitigate the risks it poses, and perform continuous monitoring. Update legacy systems that were not designed with secure network connectivity and storage in mind.

⇒ **Reduce operational costs by centralizing network management, automating network provisioning and adopting network-wide policies** to drive application and network changes. Label, inventory and track every piece of network equipment and application, device or sensor. Doing so will help IT personnel manage patches, updates and repairs as well as reduce time-consuming errors related to misidentification or improper handling of mission-critical pieces of the network.

⇒ **Ensure financial viability by providing funding for long-term maintenance, repairs, management and upgrades — or by tapping into new revenue streams.** Beware of creating a fixed budget with hard numbers that don't account for inflation. Create a system that allows awards and authorizations to adjust to inflation without requiring additional rounds of approval from city councils or other governing bodies.

⇒ **Develop a multi-step roadmap that begins with simple connectivity** and then incrementally adds IoT components, applications and other smart community technologies. Once connectivity is in place, build public confidence and support by starting with low-hanging fruit (i.e., smart street lights or smart trash cans) that provide quick return on investment.

⇒ **Establish partnerships with third-party providers that offer project management over the entire network ecosystem,** as well as customized services and a well-established, properly vetted network of vendor partners. This will help you realize the promise of smart community initiatives while saving time and money and reducing risk.



### FURTHERING YOUR SMART COMMUNITY GOALS

Smart community projects begin with a focus on citizens. Network infrastructure determines how a smart community begins, evolves and ultimately improves the lives of those citizens. With the right network infrastructure, state and local governments can create smart communities that include smart buildings, smart infrastructure (water, heat, transportation, power) and smart services. Intelligent networks require the careful combination of multiple components. Most municipalities will need the services of a third party to create a robust network foundation that supports their smart community goals. Government IT leaders should choose a provider that is experienced in innovation, network modernization and the complexities of connectivity in a smart community environment.

---

*This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Ciena and CenturyLink.*

For: **ciena**  
Experience. Outcomes.



**CenturyLink**<sup>®</sup>

Ciena is a network strategy and technology company that helps governments translate best-in-class technology into constituent value through a high-touch consultative business model helping governments build secure communication networks that connect agencies, states, counties and smart communities. We believe in driving an industry ecosystem and offering the greatest degree of flexibility in how governments consume technology to deliver the most rewarding experiences and outcomes to their constituents. [www.ciena.com/sled](http://www.ciena.com/sled)

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. Our services are used by public sector customers of all sizes— from the largest and most critical government agencies to rural schools. Headquartered in Monroe, Louisiana, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. [www.centurylink.com/ges](http://www.centurylink.com/ges)

Produced by: **CENTER FOR DIGITAL GOVERNMENT**

The Center for Digital Government is a national research and advisory institute focused on technology policy and best practices in state and local government. The Center provides public- and private-sector leaders with decision support and actionable insight to help drive 21<sup>st</sup>-century government.

The Center is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

[www.centerdigitalgov.com](http://www.centerdigitalgov.com)