To improve decision-making and response times, state Departments of Transportation (DOTs) are implementing next-generation Intelligent Transportation Systems (ITS) that collect, aggregate, analyze, and report on data from ever more sophisticated sensors, video cameras, and other devices embedded into transportation infrastructure. Using this data, DOTs can prevent accidents; respond to emergencies quickly; optimize traffic flow; and keep motorists up to date about hazards, slowdowns, route changes, and more. However, much like roadways that carry vehicles, the networks carrying ITS data are vulnerable to congestion and disruptions that can slow traffic to barely tolerable levels at best or bring everything to a crashing halt in a worst-case scenario.

Multiple vulnerabilities and operational demands threaten DOT networks. For one, a next-generation ITS is laden with thousands of devices, many of which are bandwidth-intensive and latency sensitive. If bandwidth or performance demand exceeds what is available, these devices cannot function properly — if at all. That means video footage may become jittery, data required for real-time traffic updates or rerouting may be delayed to the point of losing its value, and DOT decision-makers may not be able to access critical applications in real time.

Environmental and human-caused disasters are another common source of network slowdowns and outages. DOT networks often stretch across miles of terrain that expose optical fiber and network equipment to things like rock slides and floods. Humans, too, are responsible for fiber cuts — both accidental and intentional — as well as malicious hacks into the network itself.

To ensure the massive volumes of data coming from ITS devices can be accessed, processed, shared, and acted on 24 x 7 — despite disasters, congestion, or other events — DOT network operators are building resiliency into their networks. By intelligently and dynamically providing the network availability, performance, and flexibility ITS requires, a resilient network helps DOTs ensure motorists reach their destinations safely and quickly. It also takes pressure off short-staffed IT teams by automating network management tasks and enabling the network to easily evolve as new technologies appear on the horizon, driverless vehicles gain ground, and rural broadband initiatives — boosted by federal stimulus funding and other programs — shift into high gear.

Roadblocks to resiliency
The following challenges impede network resiliency:

- **Insufficient fiber infrastructure.** Despite the necessity of border-to-border coverage for truly effective and equitable ITS within states, many DOTs lack sufficient, if any, coverage in rural or remote areas.

- **Legacy routing technology.** Legacy routing protocols cannot support the performance requirements of ITS applications. Instead of dynamically routing traffic based on application requirements, legacy technologies route traffic along static, predetermined paths, which can lead to network congestion and application failures.

- **Lack of intelligent network management software.** Without these tools, DOTs cannot easily leverage excess capacity to ensure optimal performance and availability. They also are not able to share excess capacity with local and state agencies to reduce costs or address the digital divide. Finally, they have to send network teams into the field to address issues that could be handled virtually — and more quickly and cost-effectively — from the main operations center.

- **Staffing shortages.** DOTs typically have a limited number of staff who already have their hands full with the deployment, tracking, and replacement of thousands of ITS devices. DOT staff simply does not have the time to add network management and routing to their workload.

Creating a resilient core for ITS
Each DOT has a unique path to ITS. Regardless of the ITS devices, sensors, and applications chosen, it is important to start with a resilient network foundation.
“The end environment, such as cameras and sensors, will change. When you think about future-proofing and automating your network, you need to make sure all those core fundamentals of networking are established and resilient first,” says Bob Fifer, ITS and Network Branch Manager, Colorado Department of Transportation (CDOT).1

The CDOT network supports a highway system with more than 9,000 lane miles, 1,500 miles of fiber optic cables, 2 data centers, and approximately 8,500 devices. “It’s a technology-alive network that gives us information so we can create thoughtful and sound decision-making in real time,” Fifer notes.

Key components of a resilient network like CDOT’s include:

- **Carrier-grade fiber-optic network.** A carrier-grade network provides scalable, extremely high-capacity bandwidth to support roadside cameras, sensors, and real-time ITS processes. Dense Wavelength Division Multiplexing (DWDM) technology is one way to efficiently and cost-effectively scale capacity on demand, especially where data must be transmitted over long distances. By allowing multiple carrier signals to be transmitted through one single fiber link, DWDM helps DOTs extract the highest performance from their fiber investment.

- **Redundant connectivity.** Redundancy refers to doubling up on circuits and network equipment in critical locations so network services continue to function in the event of a failure or disruption in the primary technology.

- **Intelligent, self-healing infrastructure.** “Seconds mean lives in our world. We have to detect, react, and inform in seconds — not minutes or hours,” Fifer says. ITS helps drive rapid response time — but only if network resources are available to power its processes. Next-generation network technology is able to route network traffic around an outage or congested area on the network ring. DOTs can also intelligently and automatically allocate bandwidth on demand based on predefined policies.

- **Virtualization at the edge.** The closer decision-making is to the edge — where data from cameras, sensors, and other devices is gathered — the faster and more impactful decisions will be. By virtualizing and automating the provisioning of network resources and business applications close to the edge, DOTs can create powerful real-time data hubs for advanced traffic management processes. Virtualization also alleviates network management burdens by monitoring network traffic without human involvement and only alerting staff when predefined thresholds have been exceeded.

- **Encryption of in-transit data.** Encrypting in-transit data ensures the privacy and security of data at the network level, and helps guard against attacks and network breaches that could impact performance or potentially bring down the ITS.

### Getting it right

The following steps can help DOTs get started on the path to greater resiliency:

- **Fail fast.** ITS technology is evolving quickly. To keep pace, deploy technologies as soon as they are minimally viable, evaluate solutions regularly, refine as you go, and be prepared to let go of strategies or tools that do not pan out.

- **Have a Network Operation Center (NOC).** Monitoring and managing fiber, data centers, devices, and other assets becomes increasingly complex as the number and diversity of assets grows. Having a dedicated NOC, along with software-defined tools, frees up staff and helps ensure optimal network performance and availability.

- **Optimize fiber assets.** Continually seek ways to extract maximum value from existing assets — whether via technologies such as DWDM, or strategies such as sharing fiber with other communities or agencies.

### Preparing for the inevitable

With cyberattacks on the rise and natural disasters making headlines regularly, prudent DOT leaders must continually reevaluate probabilities and prepare their networks for high-impact events that they once considered rare. A well-designed network helps ensure ITSs perform optimally and survive the unthinkable by building in resilience from the ground up. With a resilient network core, DOTs can go beyond ensuring business continuity — they can also optimize resources, reduce complexity, alleviate pressure on IT staff, and strengthen security.

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

---