Department of Transportation challenges

IT professionals encounter seemingly never-ending challenges and demands that can impact the quality of the motorist experience. Maintaining the ability to provide applications that allow safe, efficient traffic flows on a 24/7 basis keeps Department of Transportation (DOT) directors awake at night. Any threat or vulnerability that impedes traffic manager access to data from remote roadside ‘smart’ devices can cause serious consequences.

DOT decision-makers are constantly collaborating with other jurisdictions, state CIOs, and vendors to ensure resiliency and business continuity. Successfully navigating those challenges depends on ‘anytime, anywhere, always-on’ access to applications and data in private data centers and public clouds.

Resiliency rises to the forefront

Network resilience mitigates risk. Regardless of the disruption, resilient networks prevent costly downtime and keep processes moving by maintaining a high level of service.

Data and applications remain secure and available 24/7. With network resilience in place, engineers gain confidence that network management tools will quickly and precisely respond to any event.

Meeting the current and future needs of transportation systems requires a muscular approach that combines network resilience with automation solutions and increased bandwidth.

This new approach to network design builds through:
- Increased service agility
- Unified service management and network optimization
- End-to-end service delivery
- Enhanced encryption methods

Become stronger, faster, and smarter

Drivers for the technological future of DOTs include ensuring motorist safety, building enhanced abilities to monitor road conditions, controlling traffic flow, and communicating with motorists. Yet, matching those drivers with Intelligent Transportation System (ITS) technologies like Pan-Tilt-Zoom network cameras, roadside sensors, smart traffic signals, and vehicle-to-anything (V2X) involves the transfer of large amounts of data.

Planning for that future establishes a new level of breakthrough thinking as IT directors see the opportunity provided by new ITS technologies, analytics, and high-capacity fiber networks.

Just as athletes need the proper equipment and coaching to hit performance goals, successful transportation system strategies require new network services and the trusted expertise offered by Ciena.

Future-proof your network

Ciena’s Packet-Optical Platforms provide DOTs a highly resilient, scalable, next-generation network that meets the needs of current ITS applications while ensuring capacity for future initiatives like autonomous vehicles. Leveraging Wavelength Division Multiplexing (WDM) technology, DOT networks combine multiple wavelengths into a single optical fiber.

This technique optimizes fiber utilization, ensuring a high return on fiber investments.
Challenge

- Ensuring resilient, always-on access to data from thousands of remotely deployed sensors, video cameras, and monitoring devices
- Reducing complexity in the network and ensuring scalability to support evolving ITS and autonomous vehicle applications
- Becoming more agile and flexible in operations, accomplishing more with less

Opportunity

- Orchestration of multiple domains and vendors and management through single ‘pane of glass’
- Improve operational agility and cost reduction while ensuring priority of critical network traffic
- Flexibility to rapidly add network functions at and capacity where and when needed
- Simplifying the network while evolving towards a more automated, software-defined network environment

Improve operational efficiency and resiliency

Ciena’s Manage, Control and Plan (MCP) assists network engineers with solving complex network optimization and service management through network capacity demand planning and visualization tools.

Enhance data security

Through the use of Ciena’s WaveLogic™ Encryption solution, DOTs can deploy managed encryption solutions that include Encryption as a Service and Layer 0-1 encryption to ensure the security and privacy of in-transit data.

Was this content useful? Yes No