Cisco Solutions for Connected Roadways

Contents

Introduction

Departments of Transportation (DOTs), roadway authorities, and cities around the globe are focusing on enhancing the safety of road users, reducing traffic congestion, and achieving sustainability goals. To meet these objectives, it's more important than ever to securely connect our critical roadways and intersections infrastructure to enable seamless communications to distributed equipment. It's also essential to access data that is necessary to optimize operations and pave the way to support emerging and innovative vehicle technologies, including Cellular Vehicle-to-Everything (C-V2X) communication. Equipment including video surveillance and detection systems, weather information systems, Light Detection and Ranging (LiDAR), and radar systems collect data about road and traffic conditions and can detect vulnerable road users. This data can be leveraged to control dynamic message signs and traffic controllers and can also alert systems to reduce congestion and increase safety.

In this brochure, we will discuss how a secure, resilient, agile network can help traffic operators achieve their goals. With Cisco® solutions, DOTs, roadway authorities, and cities and counties can successfully digitize to achieve their most important business outcomes—and build a foundation for future growth and innovation.

Challenges and opportunities for transportation professionals

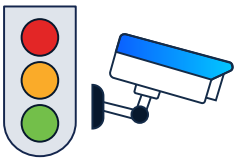
Transportation, including roads and highways, is one of the critical infrastructure sectors identified by America's Cybersecurity and Infrastructure and Security Agency (CISA) and the EU NIS2 Directive. Roadways infrastructure faces constant cyber and physical security risks. And as more Intelligent Transportation Systems (ITS) are connected, the attack surface dramatically increases. End-to-end protection against cybersecurity threats is essential for these connected systems. Therefore, traffic operations teams require visibility of everything connected at the roadside and assurance that assets cannot be tampered with. They also have to comply with ever more stringent cybersecurity regulations such as US TSA and EU NIS2.

A secure architecture requires a scalable, multi-layer approach to ensure the physical security of connected equipment at the intersection, together with network port-level security, network segmentation support, and application-level security. It should also provide secure control of access to connected devices for maintenance, troubleshooting, and upgrades. To meet these needs, DOTs and roadway operators need a solution that leverages all layers of security to protect equipment, applications, data, and people.

Traffic operations teams are contending with limited resources and need to minimize outages while ensuring compliance with organizational policies. To successfully drive digital transformation, they need complete solutions that meet the needs of all their stakeholders.

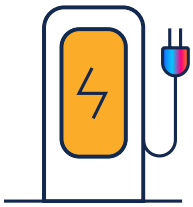
What's driving roadway digitization

As traffic operations and road user needs evolve, there is increasing focus on digitization of roads, highways, and intersections. DOTs, roadway authorities, and cities and other transportation agencies are looking for solutions to help them modernize their highways, bridges, and tunnels, as well as securely scale roadside digital infrastructure. They are seeking to drive more efficient, resilient, and sustainable traffic operations—and to build a foundation that will enable innovation. Their initiatives include:



Roadway modernization

Providing a safe and fluid road user experience, Intelligent Transportation Systems (ITS) help improve traffic management by using data from connected equipment.



Electrification

Addressing sustainability and climate change goals, driving an increased need for scalable charging infrastructure.

Connected vehicles

Leveraging the benefits of connected car technologies, such as autonomous driving and vehicle-to-everything communication, accelerating infrastructure investment.

Solution for connected roadways

Cisco, a global leader in industrial networking, offers a wide range of solutions to help you securely connect roadways infrastructure to enhance road user safety and meet sustainability goals. Our validated designs and solutions help you create a secure digital infrastructure that can help increase operational efficiency and reduce costs, while providing a foundation to support emerging vehicle technologies like C-V2X.

Our solutions for roadways combine high performance and highly scalable connectivity with comprehensive cybersecurity capabilities fused in the network, and AI-assisted management for simplified operations.

Cisco's rugged networking portfolio offers fixed, cellular, and wireless options to connect roadside assets using the best possible technology. These networking products are built to withstand harsh environmental conditions. Cellular interfaces are modular to simplify upgrades and protect investments. Compute capabilities are built in to enable data collection and processing at the edge.

Because protecting roadways infrastructure from cyberthreats is key, we are fusing advanced cybersecurity features with the network to enable in-depth protection and eliminate gaps in defense. Cisco networking equipment has built-in Next-Generation Firewall (NGFW) capabilities to provide visibility into all connected roadside devices and their security postures, enforces network segmentation, and enables least-privilege secure remote access.

To minimize complexity and space requirements, advanced security as well as data collection and processing capabilities are built into the industrial routers and switches themselves—with no additional hardware required. Centralized management and configuration simplify operations of large infrastructure and ensure security policies are consistent across all sites.

Let's take a closer look at some of the many use cases for Cisco's solutions for connected roadways and intersections.

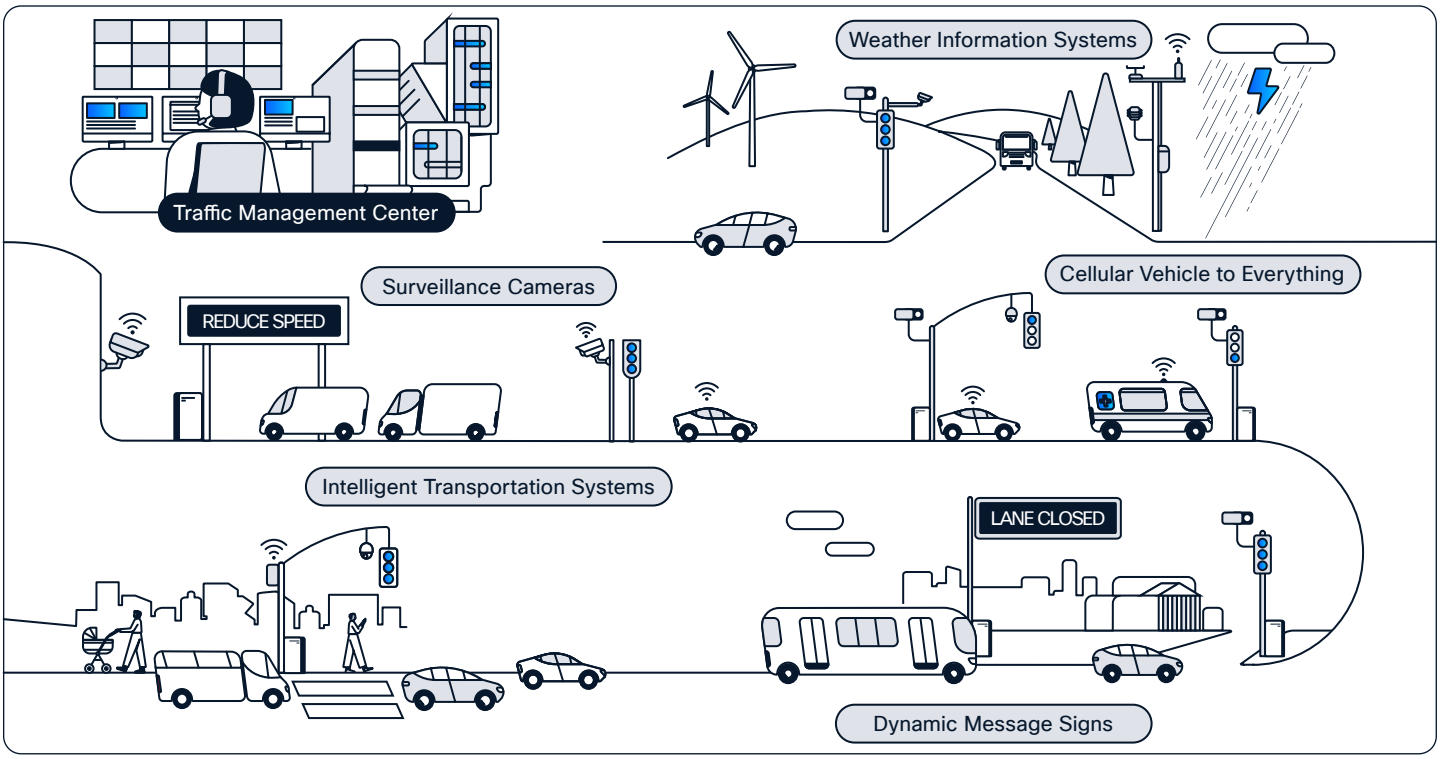


Figure 1. Cisco's integrated architecture securely connects roadway infrastructure to enhance safety and operational efficiency

Connected Intelligent Transportation Systems (ITS)

Connecting ITS equipment at intersections and the roadside is key to reducing accidents and fatalities, reducing congestion, and achieving sustainability goals. It also helps boost operational efficiency and reduce costs. Equipment and systems such as traffic signal controllers, surveillance and detection cameras, weather information systems, Wi-Fi access points, and digital signage need to be connected reliably and securely. This enables data from these systems to be leveraged to gain insights to help with process optimization and enhance the flow of traffic. However, systems can number in the thousands, and fiber may not be available at every location, so cellular or wireless connectivity may also be required. Some devices may be off the grid, powered using solar panels and batteries. And managing and maintaining everything remotely can be challenging and expensive. Network devices providing connectivity need to be able to withstand extreme temperature and humidity fluctuations and be compact enough to fit inside roadside cabinets. And the more connected equipment you introduce, the greater the potential cyber risk.

Challenges

- Lack of connectivity and space at the roadside and at intersections.
- Remote sites using solar panels and batteries can't power cellular routers.
- Risk of cyberattacks due to lack of visibility into connected devices and their security posture, limited physical security in roadside locations, and lack of control of external access to equipment.
- Outages and delays in troubleshooting and maintenance due to lack of awareness of issues with connected equipment.
- Expensive and time-consuming truck rolls for maintenance and troubleshooting of connected equipment.

Benefits of Cisco solution

- Scalable, modular fiber, wireless, and cellular solutions in compact, ruggedized form factor for connecting systems at the roadside and at intersections.
- Low power routers enabling cellular connectivity with just 5W.
- Visibility of connected assets and their security posture, and zero trust remote access, embedded in switches and routers.
- Network access control preventing unauthorized devices to physically connect to a network port at a remote location.
- Advanced network security with Next Generation Firewall (NGFW) and intrusion protection (IDS/IPS) features to keep roadway assets safe from cyber threats.
- Support for centralized management and configuration of industrial devices in the transportation management center to help simplify operations.

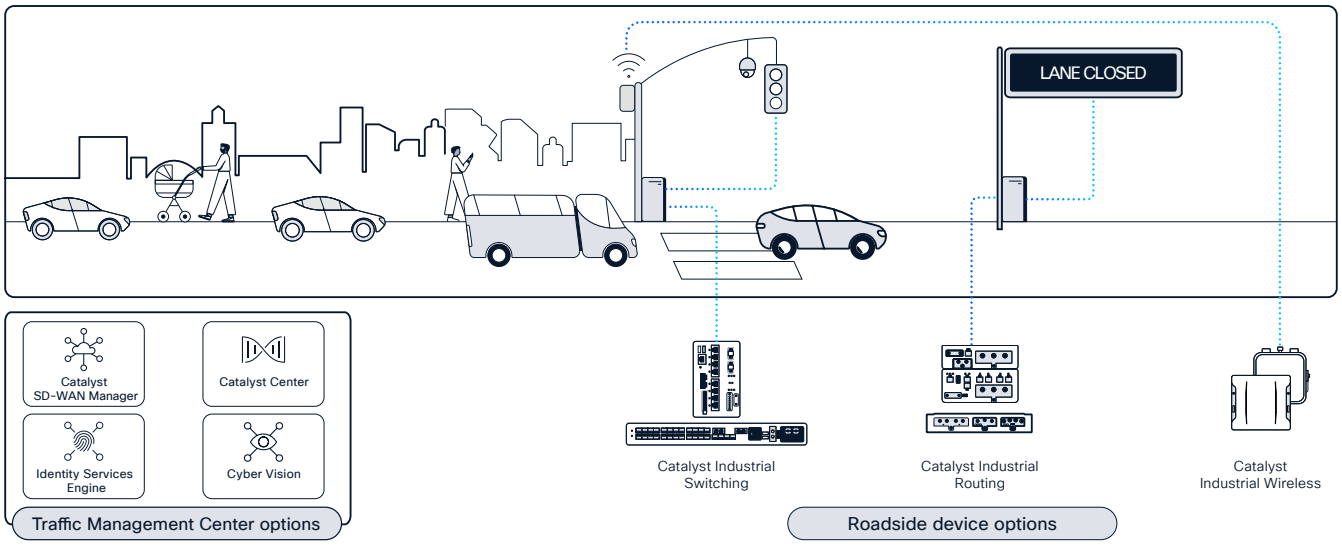


Figure 2. Secure Intelligent Transporatation Systems (ITS) architecture

Cellular Vehicle to Everything (C-V2X)

Supporting innovations such as C-V2X communication and connected autonomous vehicle (CAV) corridors requires numerous systems and equipment, including LiDAR, radar, cameras, sensors, Roadside Units (RSUs), and traffic controllers to be connected. Connectivity must be secure, reliable, scalable, and support high bandwidth, low-latency communication. Minimizing latency is vital as communication delays can have a major impact. For example, agencies need to know immediately if an emergency vehicle needs priority at an intersection and to have visibility of local congestion. Access to data, which needs to be collected and processed quickly to support a wide range of use cases including wrong way driver or curb speed warning applications, is also necessary.

Challenges

- Lack of connectivity and space at the roadside and at intersections.
- Need to support corridors of intersections to allow seamless travel.
- The potential impact of cyberattacks that could be catastrophic.

Benefits of Cisco solution

- Secure reliable, scalable, high bandwidth, low latency communication that scales to support multiple intersections, with vehicles able to travel seamlessly for long distances.
- Visibility of connected assets and their security posture, and zero trust remote access embedded in switches and routers.
- Reduced latency with local collection of data from LiDAR, radar, and other sensors.
- Small form-factor ruggedized hardware that fits easily inside the roadside cabinet.
- Centralized management and configuration of devices and security policies to help simplify operations.

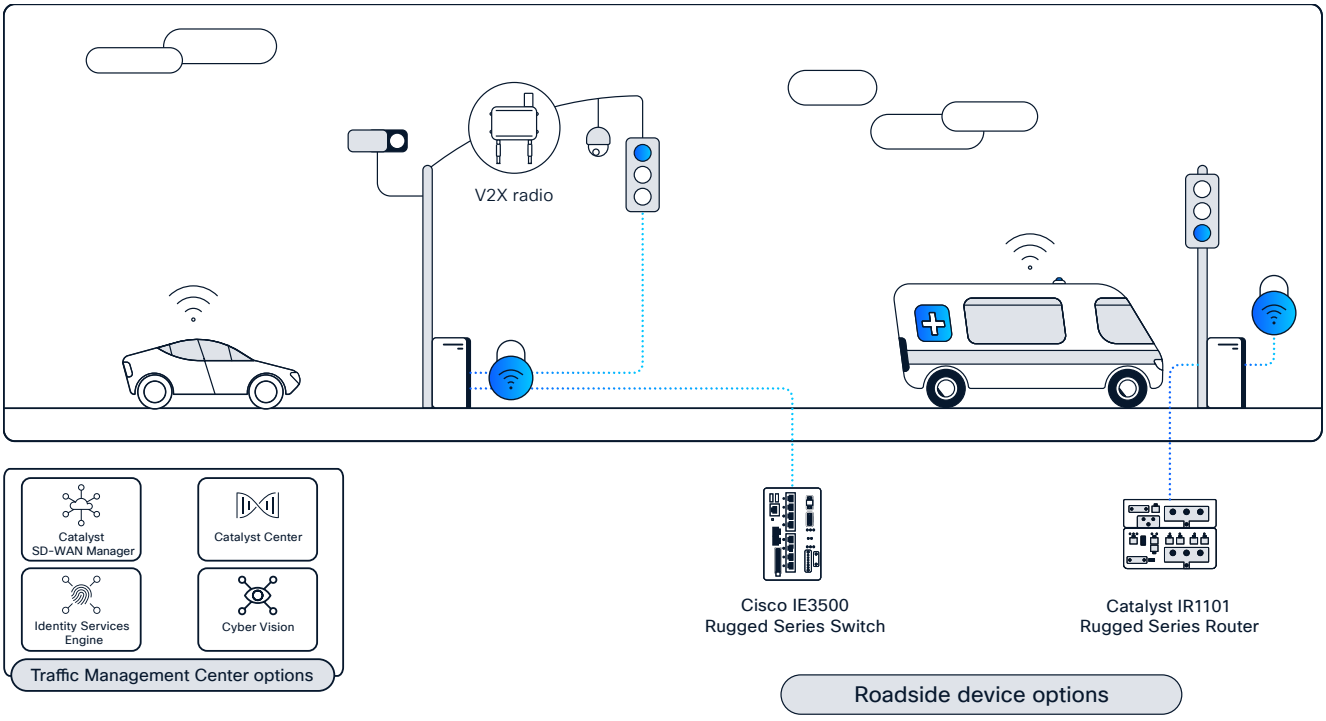


Figure 3. Secure C-V2X infrastructure enables intelligent and safer vehicle mobility.

Dynamic Message Signs (DMSs)

To help drivers get where they need to, safely and efficiently, DMSs, variable message signs, and changeable message signs help to optimize traffic flow by providing alerts, warnings, and general information to support a wide range of use cases, including wrong way driver or curb speed warning applications, and general traffic condition information. Message signs require significant investment to deploy, and connectivity must be secure to ensure that the messages shown are timely and accurate. If a sign displays the wrong message, fatalities could result. And signs may be in difficult-to-reach locations, making them challenging to troubleshoot and upgrade.

Challenges

- Lack of secure and reliable connectivity to message signs in diverse remote locations.
- Temporary signs using solar panels and batteries can't power cellular routers.
- Risk of cyberattackers hacking into signs.
- Lack of space to accommodate equipment and the risk of damage to network devices due to extreme temperature and humidity fluctuations.

Benefits of Cisco solution

- Scalable, modular fiber, wireless, and cellular solutions in compact, ruggedized form factor to fit inside a roadside cabinet.
- Low-power routers enabling cellular connectivity with just 5W.
- Zero-trust remote access embedded in switches and routers, to let operations staff and vendors remotely configure and monitor signs securely without the need for point hardware solutions.
- Access to data, with collection and processing on the network device, with support for the NTCIP 1203 protocol required for DMS communication.
- Centralized device management and configuration for devices and security policies help simplify operations.

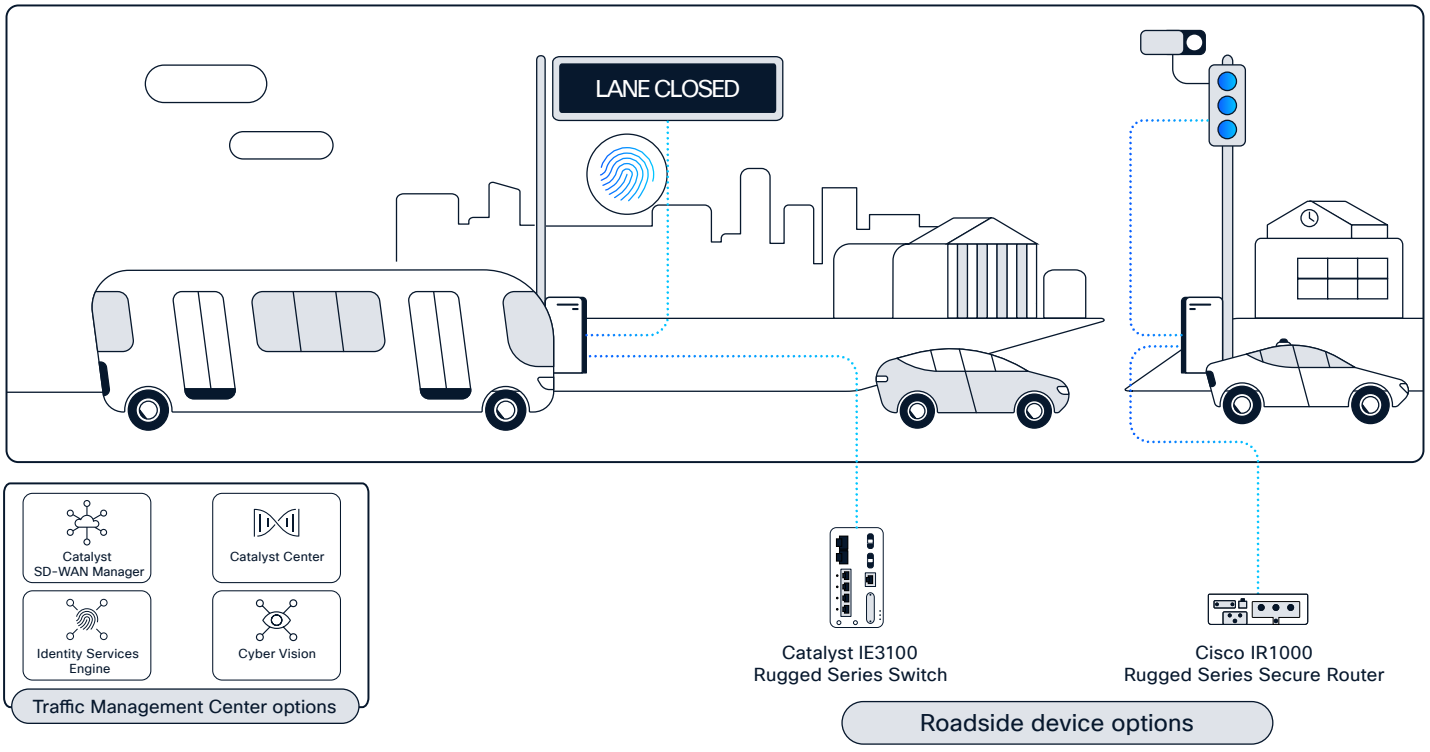


Figure 4. Secure connectivity for dynamic message signs ensures reliable and timely public information.

Rural Remote Weather Information Systems (RWIS)

Real-time updates from weather information systems, especially those in remote, rural areas, can help transportation agencies enhance safety, reduce congestion, and improve travel times. They provide the data needed to help divert drivers and other road users away from areas experiencing bad weather such as fog, ice and snow, or even extreme heat. Secure, reliable connectivity is needed to ensure that updates are provided to the traffic management center quickly and accurately.

Challenges

- Need to deploy environmental sensors to collect weather conditions data.
- Lack of network connectivity in many remote or rural areas.
- Limited power with equipment using solar panels and batteries to run.
- Remote, harsh locations and lack of space for roadside equipment.
- Specific protocol (NTCIP1204) support required to collect data from weather information systems.

Benefits of Cisco solution

- Scalable, modular fiber, wireless, and cellular solutions in compact, ruggedized form factor that's easy to install in remote locations and is built to withstand harsh weather conditions.
- Low-power routers enabling cellular connectivity with just 5W.
- Local collection and processing of data, with support for NTCIP1204. This reduces latency and increases the speed of updates to traffic management centers and signage to enable timely alerts to be provided.
- Centralized management and configuration of devices and security policies to help simplify operations.

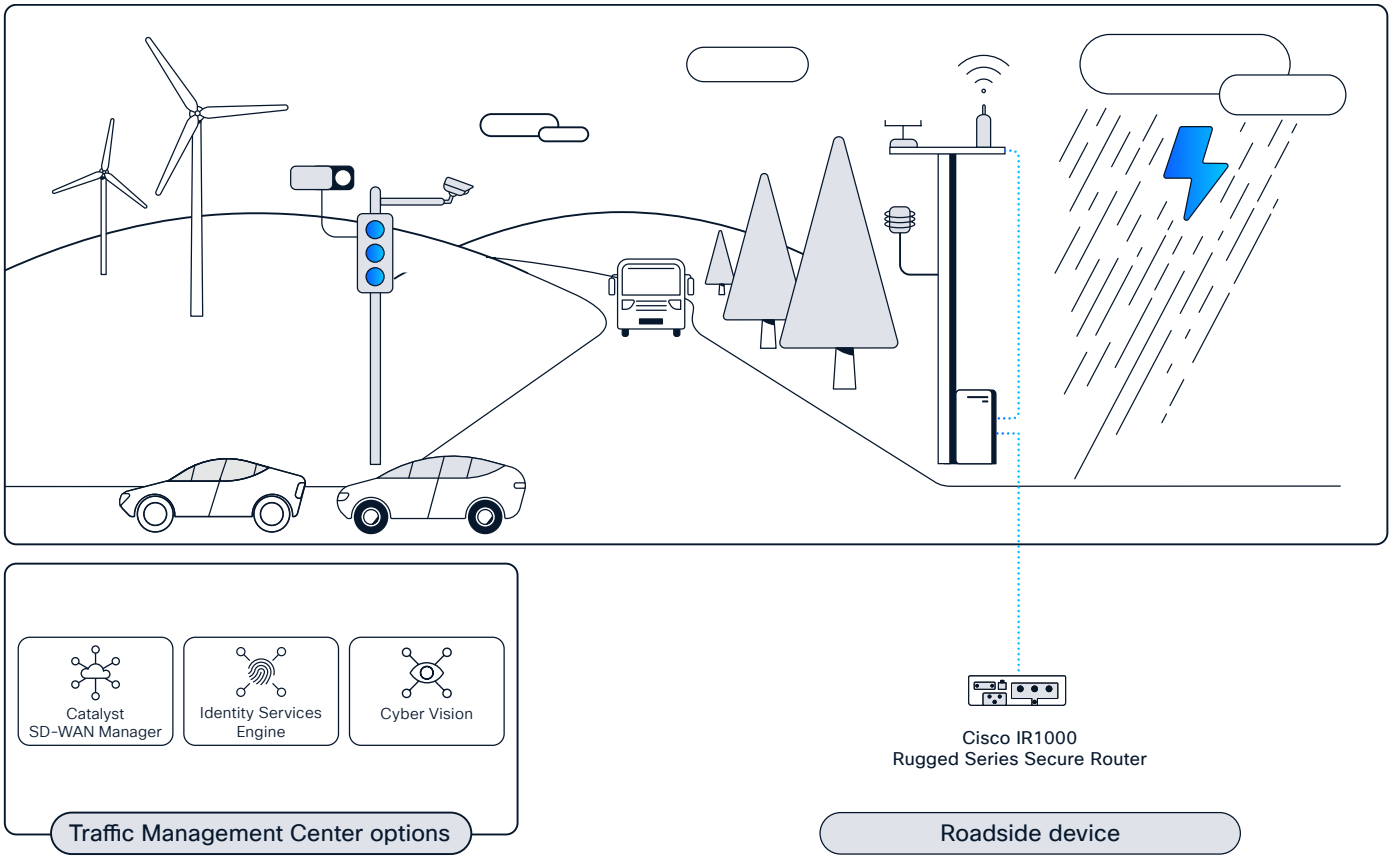


Figure 5. Reliable connectivity for rural weather systems ensures timely safety alerts for road users.

Video surveillance and monitoring

The ability to monitor an intersection or roadway area is critical for real-time situational awareness. Video surveillance cameras can capture live video streams on demand, assess them for immediate response, and store for future review and analysis. Increasingly, cameras can carry out analytics directly on the captured video stream without the need to forward video to a separate system. Real-time footage of pedestrian, cyclist, and vehicle activity around an intersection or other roadway focus areas can be analyzed to identify vulnerable pedestrians and provide alerts to prevent accidents and improve traffic flow. Secure connectivity and access control to cameras are key to prevent tampering that could cause accidents and fatalities. In remote locations, power sources for cameras may also be scarce.

Challenges

- Lack of time visibility of pedestrians, traffic and congestion, accidents, and traffic violations.
- Lack of connectivity to cameras across a wide geographic area to support live streams.
- Risk of cyberattacks on cameras or manipulation of video data.
- Lack of availability of power sources 24x7 in remote locations.

Benefits of Cisco solution

- Secure, high bandwidth and scalable connectivity in compact, ruggedized form factor for streaming HD video streams from cameras anywhere.
- Reliable and perpetual Power over Ethernet (PoE) with up to 90W per port.
- Wireless connectivity to support camera deployment where fiber is not available.
- Secure and maintain all connected assets remotely through zero-trust visibility to eliminate the need for extra point hardware solutions.
- Support for connectivity and collection of data to enable use cases such as number plate recognition, red light camera, allowing certain cars to merge, and tolling.
- Centralized management and configuration of devices and security policies to help simplify operations.

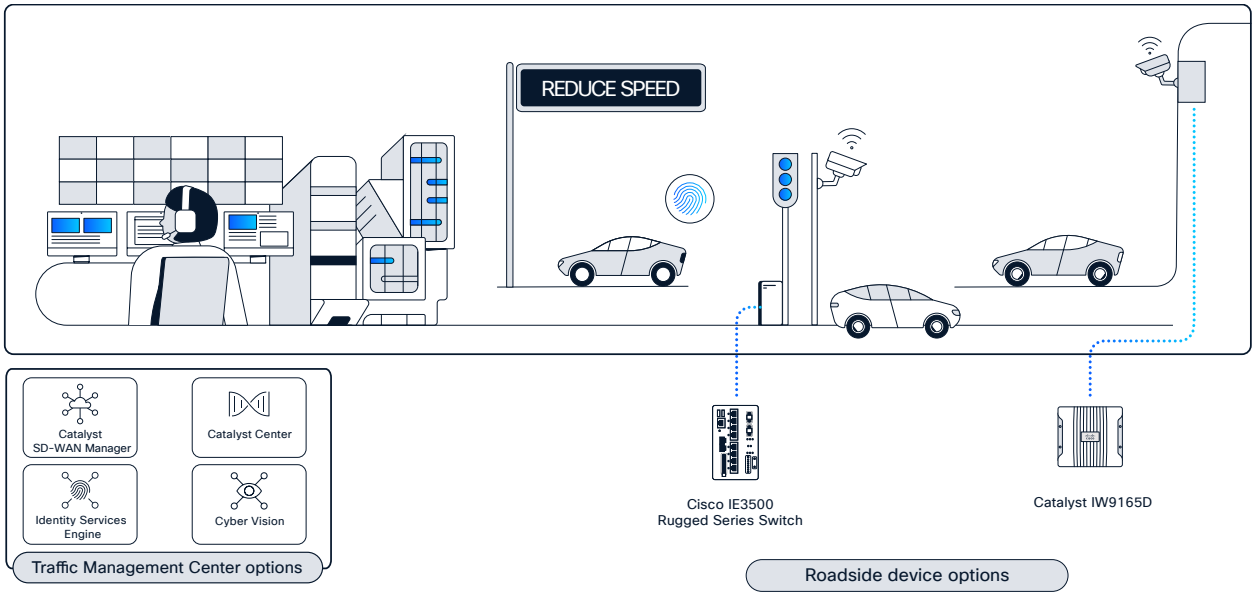


Figure 6. Secure, high-bandwidth connectivity enables real-time video surveillance for improved situational awareness.

Cisco portfolio for connected roadways and intersections

Cisco's solutions for connected roadways and intersections deliver secure, reliable, scalable connectivity with comprehensive in-depth security fused in the network. Our portfolio includes fixed, cellular, and wireless options with edge compute capabilities for data extraction enabling advanced use cases. Our industrial routers and switches embed these network security and data extraction capabilities, eliminating the need to deploy additional hardware solutions.

Explore the product portfolio

Cyber Vision is a comprehensive OT security solution embedded into switches and routers. It offers full visibility into connected roadways equipment and their security postures, enabling traffic operations to maintain a detailed inventory of ITS devices, assess risks, manage vulnerabilities, detect malicious traffic, and drive regulatory compliance.

Secure remote access to assets, also a Cyber Vision feature, enables every switch and router to provide zero trust remote access to any roadways equipment. Operations teams gain self-service remote access capabilities to run operations without IT bottleneck, while least-privilege access policies are enforced to help control risks from remote users.

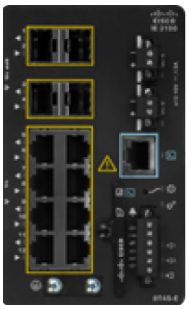
Segmenting networks to protect operations is made simple with Cyber Vision. It automatically groups roadways assets and suggests policies between groups, so you can easily restrict what device can communicate with what. Enforce policies directly with industrial switches or use Identity Services Engine (ISE) for even more controls.

Identity Services Engine (ISE) helps you secure every port of your roadside networking equipment to ensure only the devices or users you trust can connect and communicate only with the resources they need to.

Cisco Catalyst® SD-WAN Manager lets you easily deploy, secure, and manage the WAN infrastructure connecting your ITS equipment, at the roadside and at intersections and to the traffic management center. It centralizes and automates network management to let you easily run large infrastructures and manage firewall rules enforced by your Cisco industrial routers to unify security policies and eliminate gaps in defense.

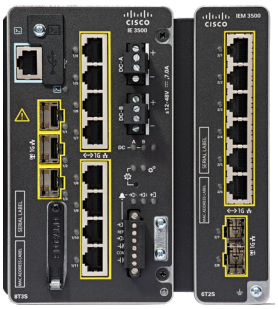
Catalyst Center enables you to connect, secure, and automate network operations for your industrial switches. It helps to reduce operational costs with capabilities including AI-assisted workflows and assurance, and centralized management of industrial switches to simplify operations.

Meraki Dashboard accelerates city-wide efficiency by centralizing the management of traffic cabinets, utility infrastructure, public safety systems, and parking meters within a single cloud-native Meraki dashboard.



Catalyst IE3100 Rugged Series switch

Ultra-compact form-factor fixed DIN rail switch with 6, 10, 12, or 20 ports and PoE.



Cisco Catalyst IE3500 Rugged Series switch

Modular, high-performance platform offering up to 24 Gigabit Ethernet ports, multiple 10G uplinks, and robust PoE capabilities for scalable, secure industrial networking.

Cisco Catalyst IE3100 and IE3500 Heavy Duty Series Switches

The same high performance, secure switches, but in an IP67-rated enclosure enabling easy outdoor deployments.

Cisco Catalyst IE9300 Rugged Series switch

Aggregation and fiber backhaul for multiple Catalyst access rings offering 10G uplink capacity for high-bandwidth backhaul to the traffic management center.

Cisco Catalyst IR1000 Rugged Series Secure Routers

Ultra-compact router with powerful firewall capabilities providing 5G and LTE connectivity using only 5W. Ideal anywhere space, power, and security requirements leave no room for trade-offs.

Cisco Catalyst IR1101 Rugged Series router

Highly modular, expandable router enabling a choice of connectivity including public and private 5G and LTE, and advanced firewalling capabilities.

Cisco Catalyst IR1800 Rugged Series router

Securely connect your roadside assets with dual simultaneous 5G cellular support, next-generation firewall (NGFW) capabilities, and more.

Cisco Catalyst IW9165D Heavy Duty Access Point

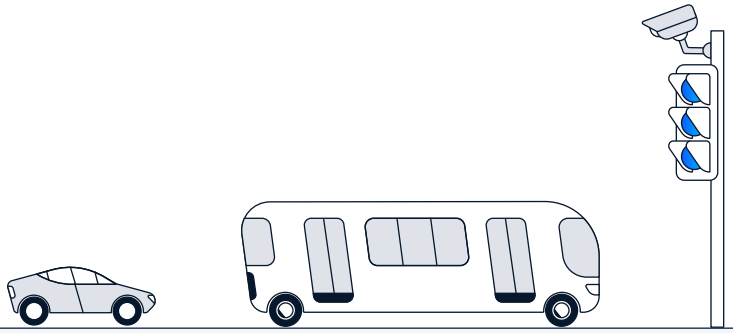
Dual-radio 2x2 access point with integrated antennas for easy deployment outdoors without enclosure. Enables simultaneous Wi-Fi services and wireless backhaul for connected assets.

Cisco Catalyst IW9167E Heavy Duty Access Point

Tri radio 4x4 access point in an IP67 certified enclosure. Designed for high-performance wireless connectivity supporting simultaneous Wi-Fi services and wireless backhaul using a variety of external antennas.

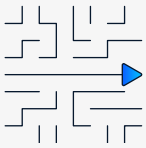
Why Cisco?

Only Cisco provides a full portfolio of solutions that deliver the security, scale, and simplicity you need for connected roadways and intersections. Our solutions enable you to:



Secure your critical infrastructure

Keep your roadside infrastructure secure with proven solutions for visibility and policy enforcement.



Increase safety and address congestion

Digitize your ITS with high bandwidth, flexible connectivity to protect road users and control traffic flow.

Drive C-V2X and innovate

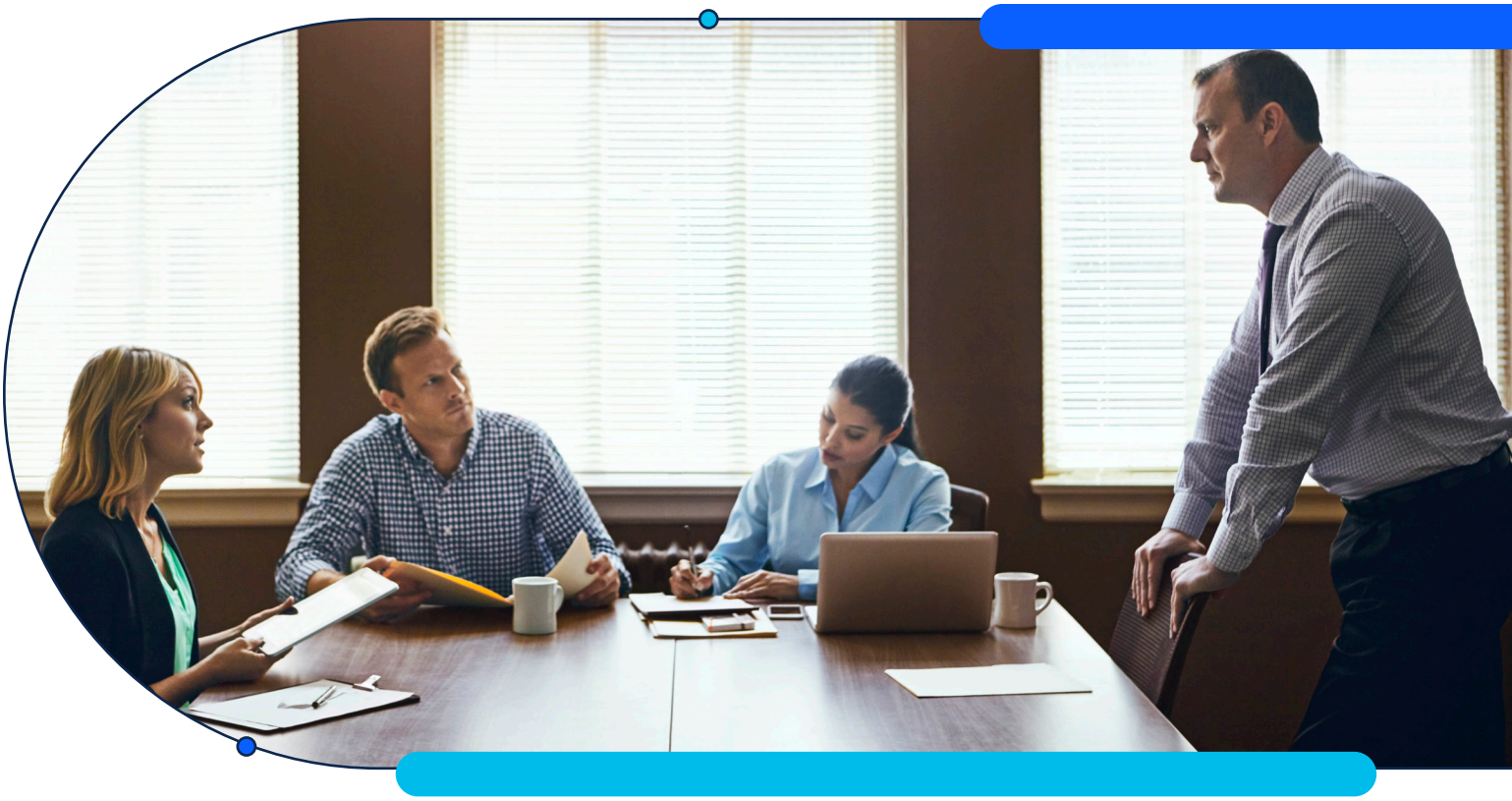
Create a solid foundation to enable, scale, and support new applications, with proven solution designs.

Enhance sustainability and reduce emissions

Provide the access to data needed for insights to reduce congestion and travel time and optimize traffic flow.

Additional resources

- Request a demo
- Infographic
- Connected Roadways and Intersections
- Industrial IoT Portfolio Brochure



C22-6531001-00 09/26