Cisco Connected Roadways and Intersections

Connect and secure your roadways and intersections

Benefits

- **Security:** Protect critical roadside assets with security capabilities built into network devices.
- **Scale and innovate:** Create a solid foundation to support new capabilities across extensive geographies.
- **Enable IT and Traffic Operations collaboration:** Address the needs of Traffic Operations and IT for successful digitization.

Optimizing today and ready for the future

Roadway and intersection technology has evolved at an amazing pace since the first traffic lights were installed a century ago. Today, autonomous vehicles and other innovations are becoming a reality. And while vehicles themselves are becoming smarter, more connected, and autonomous, from a safety perspective, the protection of vulnerable road users (cyclists, pedestrians, etc.) is top of mind. At the same time, the need to reduce congestion and meet sustainability goals is increasing. This has resulted in a need for new innovations such as Intelligent Transportation Systems (ITS) and new charging infrastructure to support more sustainable and safer travel.

These developments are taking place in an environment where intersections number in the millions and roadways range from two-lane roads to complex multilane and multimodal configurations.

The need to connect, secure, and optimize our critical roadway and intersection infrastructure is more obvious than ever. Organizations responsible for highways and traffic management are building the foundation for automating outcomes and improving situational awareness to improve safety, increase efficiency, and reduce emissions. Meanwhile, vehicles are beginning to communicate status and alerts to systems at the roadside and to other vehicles in and around the roadway, increasing the need for reliable connectivity with low latency. This need will only increase with the growing numbers of Connected and Autonomous Vehicles (CAVs).

This solution brief provides an overview of use cases and describes how Cisco's validated solutions support these by providing a ruggedized, secure network that provides a foundation to support new innovations, meet the needs of Traffic Ops and IT, and address the need for scalability.

The connected roadways and intersections journey

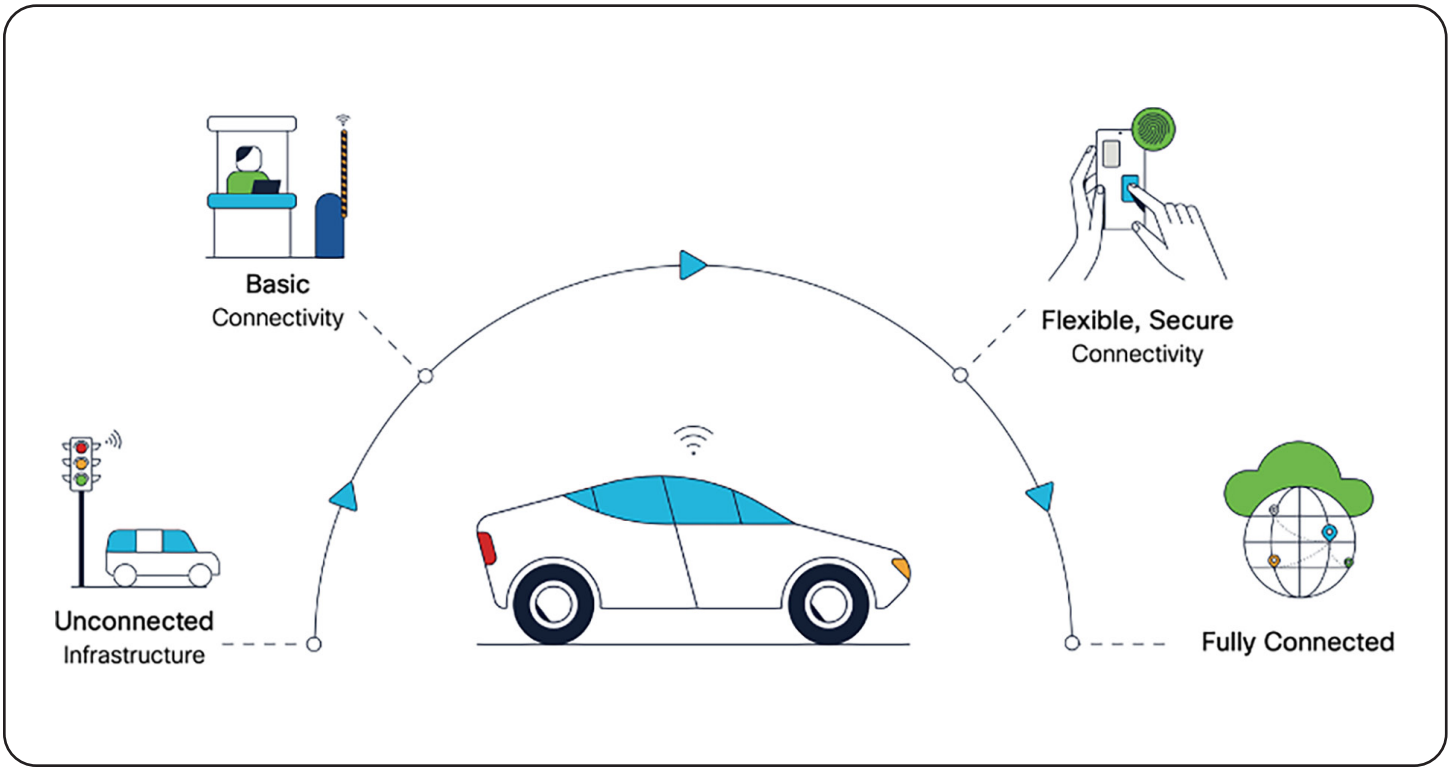


Figure 1. Stages of connectivity

Roadway operators may have to manage and optimize legacy deployments while also planning for the future and advanced roadway deployments. Technology for roadway installations can be at different phases of digitization and this solution brief provides guidance to an operator, traffic engineer, or architect on a logical path to evolving their roadway transformation efforts.

The figure above depicts different stages for a connected roadways and intersections solution, starting with minimal connectivity and ending with a fully integrated network solution. Hybrid solutions are also possible and even likely. Cisco believes that the goal should be to achieve the highest level of customer benefit and successful outcome while ensuring operational resilience and maintaining security.

Why Cisco connected roadways and intersections

Cisco is a global leader in networking and security and provides a wide range of products to address connected roadway and intersection solutions, with security being a key area of focus. By applying our secure and hardened industrial networking and IoT expertise, and working with industry leaders to address challenges in the industry, we have created innovative technology solutions that optimize and secure critical connected roadway and intersection infrastructure. Our goal is to protect your investment by providing an evolutionary path from today's isolated roadways and intersections to secure, connected roadways to support the transportation needs of today and tomorrow.

Since the inception of IP networking, Cisco® Validated Designs (CVDs) have been used to validate, architect, and configure industry best practices and technology solutions. CVDs highlight the solution use cases and architect the flow from the edge device to the application, validating the key Cisco and third-party components along the way. Each aspect of the architecture has been thoroughly tested and documented with sample configurations, helping to simplify integration and de-risk implementations.

The goal is to provide a solution that's simple, fast, reliable, secure, and cost-effective. For further reading, Cisco has developed the Connected Roadways and Connected Communities Infrastructure CVDs to specifically address the networking and security needs of roadway operators.

Roadways and intersections use cases

The wide-area communications options available at a given roadway site will greatly influence the outcomes and capabilities for any use case along the roadside. The availability of dependable lower-latency, high-bandwidth connectivity (fiber, LTE cellular, wireless, DSL) allows for more advanced network and data management options; however, sites with bandwidth constraints may be limited to simpler use cases such as remote management and monitoring. Understanding the network and the technology that can be deployed at a given site will enable traffic engineers to best determine the use cases and devices they can support.

Key use cases

This section presents a number of the key use cases that we see in connected roadways and intersections.

1. **Connected traffic management and recovery:** This is the most familiar use case, involving remote management, reporting, and access to traffic signal controllers for adjustments of traffic light Signal Phase and Timing (SPaT) at intersections. In addition to basic management of the traffic signal controller, this use case supports Automated Traffic Signal Performance Measures (ATSPM). This functionality involves collecting and reporting signal timing and traffic volume information to give transportation engineers an understanding of arterial and intersection patterns, providing clearer insights and actionable information to optimize traffic flow and reduce emissions. Remote monitoring of intersection health and early automated fault detection can maximize uptime and shorten recovery time, leading to a more resilient roadway system.

2. **Video surveillance and monitoring:** The ability to monitor an intersection or roadway area is critical for gaining real-time situational awareness along the roadway. Through the use of video surveillance cameras, live video streams can be obtained on demand and viewed for immediate response and/or stored for future review and assessment. Additional analytics can be deployed on the camera or on localized edge compute to make the camera a sensor. Many roadway operators have or are in the process of upgrading their cameras, often to models supporting 4K video, which greatly improves the clarity available to the Traffic Management Center (TMC), although it also leads to significantly higher network bandwidth consumption.

3. **Vehicle and pedestrian safety monitoring:** In alignment with the Vision Zero (zero roadway deaths) initiative, this use case provides real-time and historical views of pedestrian, cyclist, and vehicle activity around an intersection or other targeted roadway focus area. Through the use of video surveillance cameras, intersections can be monitored in real time and, with video analytics, radar, or lidar technologies, activity around the intersection can be classified, captured, counted, and recorded to provide data-driven analysis for roadway safety improvements, especially for vulnerable road users. Information gathered by sensors allows for the introduction of safety improvement measures such as warning signs and traffic signal holds to allow pedestrians and cyclists to safely cross or warn vehicles of obstructions in the roadway.

4. **Cabinet operations and security and resilience:** Roadside traffic cabinets host the equipment operating the intersection and are vulnerable to tampering and vandalism. This use case detects and reports physical entry and exit to the cabinet, which can be validated as authorized or unauthorized. Additionally, cabinet power monitoring and failure reporting is important to be able to attribute cabinet failures to either network or power-related issues so that remedial actions can be properly targeted and performed quickly. Another security risk is that intruders, third parties, or even employees may connect equipment to the network, either directly at the cabinet or remotely, which compromises the network. It is important to be able to limit this risk and quickly address any issues before they have an impact. For example, this may affect the integrity of traffic signaling systems or enable someone to change the messaging on traffic information or warning signs.

5. **Transit Signal Prioritization (TSP) and Emergency Vehicle Preemption (EVP):** The ability for transit vehicles to request and obtain traffic signal priority to reduce dwell time at an intersection and the ability for a responding police, fire, or emergency services vehicle to preempt a traffic signal to reduce response time are key requirements of a roadway solution. Through signaling initiated from the transit or first responder vehicle directly to the intersection or via a centralized TMC, this use case supports the public interest in a smoothly running transit system and rapid response to emergencies.

6. **Driver and work zone safety:** Promotion of safety along the roadway is a key concern for any roadway operator. Drivers need to be aware of changing road conditions due to weather or roadway work in progress. The use of dynamic or Variable Message Signs (DMS/VMS) to display important safety, construction, or route information; remote weather sensors to detect hazardous weather or roadway conditions; and sensors that can detect and alert road or construction site workers to oncoming traffic are all elements of this use case. The scenario of “all-lane running” is seeing increasing implementation by operators, in which the shoulders are used as extra lanes to allow for more traffic volume; being able to effectively communicate the state of these lanes to drivers is vital.

7. **Connected and Autonomous Vehicles (CAVs):** CAVs are rapidly becoming a reality, with large investments being made by technology leaders and trials underway. Using Vehicle-to-Infrastructure (V2I) technology such as C-V2X or ITS-G5, vehicles become sensors, exchanging real-time information with intersection and roadway

equipment to assist with collision avoidance and congestion reduction via adaptive signal control and timing. Today's intersections need to be ready to integrate these features to automate signal timing adjustments across a range of related intersections, so that they can optimize traffic flow dynamically, thus improving safety and reducing emissions.

8. **Highway tolling:** Highway tolling involves detection of vehicles via RFID tags, license plate readers, or tolling stations that accept various forms of payment. Ranging from single lanes to 10+ lanes, tolling stations require management, delivery of safety and lane steering messages to drivers, and secure handling of financial transactions.
9. **Electric Vehicle (EV) charging:** EV charging is a newly emerging use case driven by the migration to electric vehicles and environmental concerns. Funding from governments around the world is driving the deployment of charging stations along highways and in cities, requiring visibility into and management of charging resources.

Use case characteristics

The table below captures some of the performance or deployment characteristics for the key use cases and can help guide the selection of deployment models defined later in this document. The designation of high, medium, and low for bandwidth and latency characteristics reflects a scaling of the amount of data being delivered from the roadway through the network relative to available capacity (bandwidth) and the real-time operational needs (latency) in receiving that data.

Table 1. Bandwidth and latency characteristics of roadway and intersection use cases

Use case	Bandwidth demand	Latency tolerance
Connected traffic management and recovery	Low	High
Video surveillance and monitoring	High	Low
Vehicle and pedestrian safety monitoring	Medium (data) to high (video)	Low
Cabinet operations and resiliency	Very low	High
Traffic signal priority and emergency vehicle preemption	Low	Low
Driver and work zone safety	Low	Low
Highway tolling	Low to high	Low
Electric vehicle charging	Low	High
Connected and autonomous vehicles	High	Low

Provisioning of an end-to-end network and security framework is critical to all use cases.

Meeting today's digitization challenges

As roadways become increasingly connected and remotely accessible, ease of operations, management, and security must be taken into account when selecting equipment.

Our validated solutions are simple, scalable, and flexible, with a focus on operations processes that are field-friendly and do not require extensive technical expertise. By providing centralized network device management and strong asset operation capabilities we help you eliminate the need for manual asset tracking and reduce the risk of inconsistencies in field deployment from one site to the next.

Aligning IT and operations needs helps you ensure that field technicians can easily deploy and manage these devices without the need for IT support, while both the IT and traffic Operations Teams (OT) have full visibility into, and control of, the deployed equipment and critical applications.

Additionally, Cisco provides a wide range of connectivity options, ranging from fiber and DSL in cities and along highways to cellular or high-speed wireless where a hardwired connection is not available.

The next sections describe specific capabilities supported by the Cisco validated solutions.

Simple provisioning

It is important for a field engineer to be able to deploy a piece of equipment without having to know the details of every aspect of the network or equipment operation. Asset management is key to understanding how things are connected and the impact of one system on another. Doing this in an automated way improves the tracking of resources monitoring of system status, and contributes to best operational practices and processes. Simplifying provisioning delivers the following benefits:

Action: Add a new networking device at an intersection.

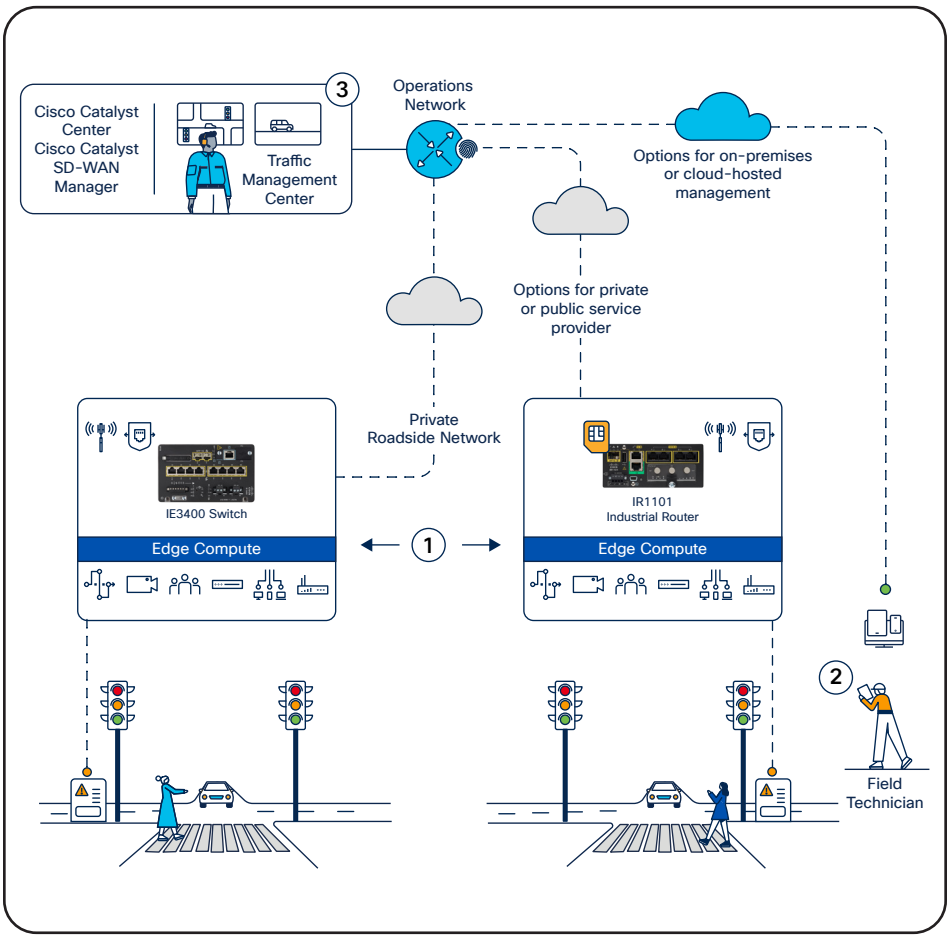
Field engineer: Make it easy for a field technician to install and maintain the required roadside equipment at scale without having to know about ports or network security, or to configure each device individually.

Network operations: Consistently deploy, monitor, and operate the network along the roadway to ensure security policy, device operation, configuration, and consistency.

Traffic operations: Respond quickly to roadside events to ensure that traffic-related applications and outcomes are operating. Quickly identify any issue and dispatch the proper resource to resolve alarms.

Cisco building blocks: Provisioning

Zero-touch deployment of network infrastructure and roadside devices.



1. Centrally configure policy for consistent asset configuration and communication.
2. Allows a technician to deploy the roadside equipment with little to no network expertise.
3. Minimizes risk by limiting field technician decision making and configuration changes. Enables device monitoring and control via a suite of centralized management tools.

Figure 2. Zero-touch provisioning of equipment

Simple operations

Removing complexity from operations leads to quicker problem resolutions, higher system availability, and better outcomes for people using the roadways. The ability to automate asset inventory, eliminate reliance on manual device tracking, and deploy policies from a central location can help ensure accurate information about the status and operation of the equipment supporting the roadway. When events occur along the roadway that may include unauthorized access to roadside cabinets, power failures, or failed equipment, it is critical to have operational visibility to be able to respond quickly with the right resources to address the issue and get the roadway operational again. Below is an example of how Cisco's validated roadway solutions can benefit your joint roadways and operations teams. Simplifying operations delivers the following benefits:

Action: Minimize service outages and support faster issue resolution.

Field engineer: When dispatched to a site, be able to connect to management tools and applications to make an impact quickly after arriving on the scene.

Network operations: Provide automated visibility into all services operating at the intersection, including the network equipment. Notify traffic operations of network status. Investigate the problem, and identify the source.

Traffic operations: Use remote management tools to gain visibility and investigate traffic equipment status. Quickly identify any issues and dispatch proper resources to resolve alarms.

Cisco building blocks: Operations

Minimize downtime with remote troubleshooting and system visibility

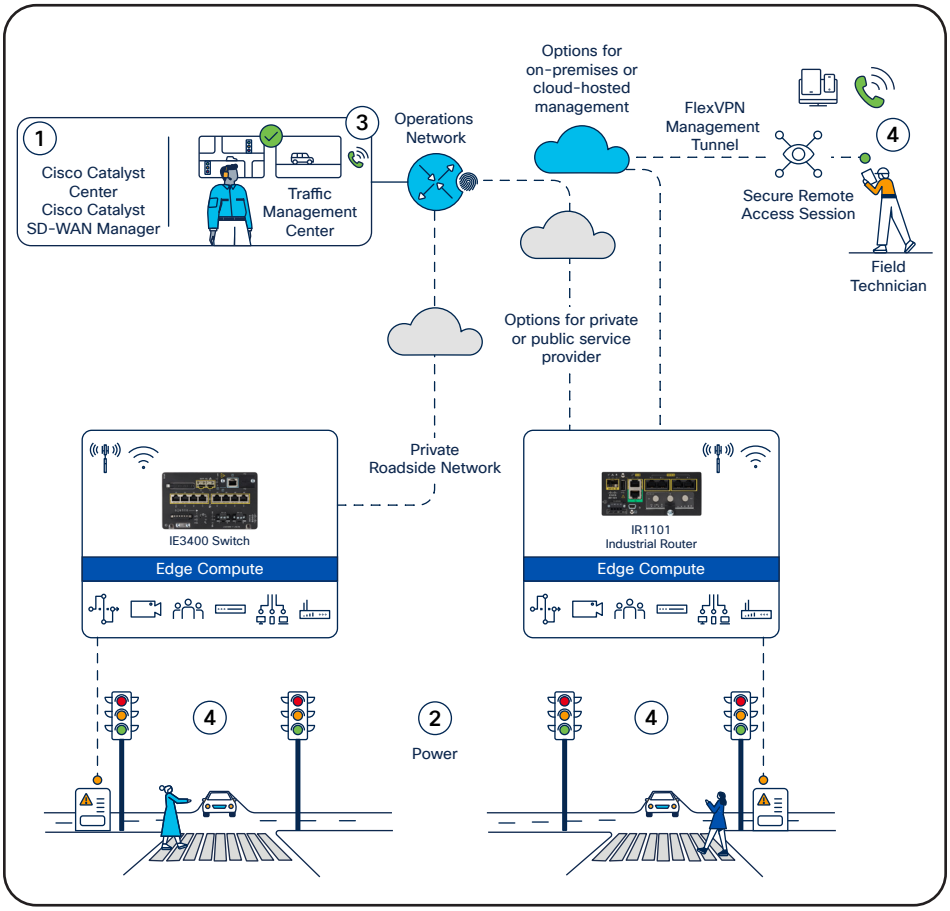


Figure 3. Responding to a communications outage

1. 10:00 pm: Alert received at both the network and traffic management center indicating that traffic signal controller communication has been lost.
2. 10:05 pm: The traffic operation team can see either:
   - The network switch sent a dying gasp alert, indicating intersection power loss OR
   - The intersection networking equipment is online and has network connectivity, indicating a traffic signal controller problem
3. 10:15 pm: Traffic operations dispatches public safety team to temporarily control the intersection for safety while a field technician is dispatched to locally troubleshoot the issue.
4. 10:30 pm: Technician uses Cisco Secure Equipment Access to securely connect to and configure the equipment to bring traffic lights back into service.

Multilevel security

Roadway infrastructure is at constant risk for cyber and physical security incidents. Roadside cabinets are out in the public domain, and as more devices are connected, the attack surface increases significantly. When organizations attempt to secure their industrial networks, they encounter two primary issues:

- **A lack of visibility:** Organizations often do not have an accurate inventory of what is on the network. Without this, they have limited ability to understand risks and build a secure communications architecture.
- **A lack of control:** A lack of visibility also means that operators are often unaware of which devices are communicating with each other or even which ones might be receiving communications from the outside. You cannot control what you cannot see.

A secure architecture requires a multilayered approach to ensure the physical security of the roadside cabinet, network port-level security of the equipment, network segmentation, and application-level traffic security. It also requires visibility of everything on the network, and the ability to ensure that remote access to roadside equipment is always secure. Our solution integrates all layers of security to keep equipment, applications, and data secure.

Segmentation is the process of isolating certain traffic types from one another using virtual networks. This allows the administrator additional control for applying security or Quality of Service (QoS) to that traffic, and for isolating potential security issues and breaches to a single virtual network. This is termed macro-segmentation. Micro-segmentation provides another layer of segmentation to further isolate equipment from other equipment on the same segment. These features, used in conjunction with port-level security, such as 802.1X and MAC Authentication Bypass (MAB), help ensure that only known devices are allowed on the network and that policies are in place to control which devices and equipment can communicate with each other, in some cases to the protocol level. For more information on secure, ruggedized networking, check out the white paper "Harness the Power of Networking to Secure Industrial Operations."

Cyber Vision, which is embedded into Cisco industrial network devices offers full visibility into connected roadways equipment and their security posture. It enables traffic operations to maintain a detailed inventory of ITS devices so they can drive network segmentation policies and detect malicious traffic and anomalous behaviors, helping them to ensure integrity and regulatory compliance. Secure Equipment Access (SEA) is a zero-trust remote access solution, also embedded into network equipment to simplify deployment at scale without the need for extra appliances. It enforces least-privilege access controls to protect infrastructure while enabling remote technicians to access only the roadside equipment they need, and only when needed. Cisco's multi-level security solutions offer the following benefits:

Action: Deploy scalable, real-time cybersecurity protection from external and internal threats.

Network operations: Consistently apply security policy, deploy security updates, and protect the network from unwanted devices or applications. Enable ongoing monitoring and analysis of the network, with automated detection of anomalous network traffic, automated alerts, and the ability to instantly quarantine suspect devices or applications.

Traffic operations: Have visibility into roadside cabinet access, quickly deploy equipment without having to understand complex security deployments, know that critical applications are available and operational along the roadside.

Cisco building blocks: Security

Multilayered security enforced through a single control point helps ensure data confidentiality and end-to-end encryption.

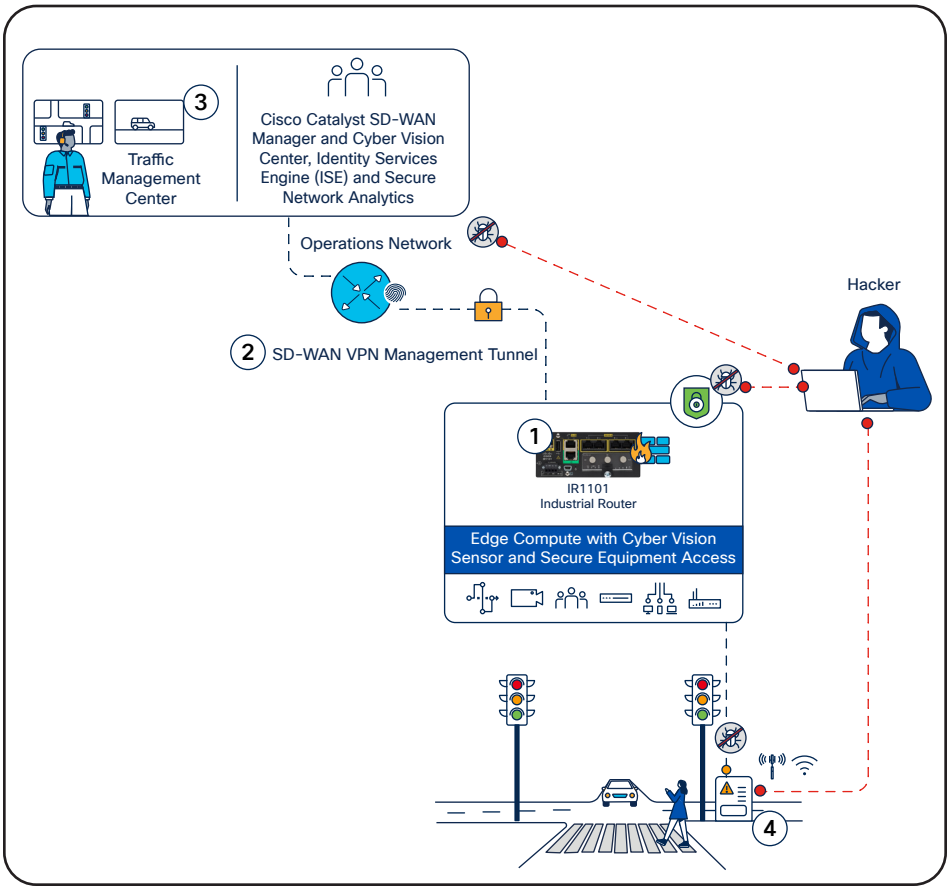


Figure 4. Multilayered security

1. Enable device access security using port security, secured operating system, and secured device features.
2. Protect data from end to end on and across the network using services such as standards-based encrypted IKEv2 IPsec VPN tunnels, secured firewalls, and network segmentation, where desired.
3. Enhance cybersecurity with visibility into connected roadways equipment, secure remote access, and security services that analyze the network traffic flow and volume as well as the device-to-device communications to detect anomalies and create a unified control point.
4. Detect physical security intrusions by enabling visibility into cabinet access.

Edge compute

Compute at the edge allows computation of data and decision making at the roadway and intersection site. However, supporting these capabilities can require additional hardware to be installed. To address this, much of Cisco's industrial IoT portfolio supports edge compute applications to reduce the need for additional hardware in an already space-confined location.

The benefits of edge compute capabilities include reduction of frequently large amounts of redundant data that may have been received or created along a roadway, normalizing data that is received along the roadway into common formats, and executing calculated responses to produce a more concise status of what is occurring along the roadside.

Additionally, edge compute can execute algorithms based on collected data to implement local actions, such as updating variable speed and digital message signs or opening and closing roadway barriers. Cisco's Edge Intelligence software, which can be installed directly onto Cisco industrial routers and switches, can natively interact with roadways/ITS devices, using, for example, NTCIP 12xx or SAE J2735.

Cisco building blocks: Edge compute

- Standards-based microservices supported through an open ecosystem.
- Cisco Edge Intelligence, a dedicated edge compute framework.
- Third-party development of edge compute microservices and applications.
- Scalable compute capacity leveraging the network infrastructure and augmented by dedicated edge compute as additionally required.

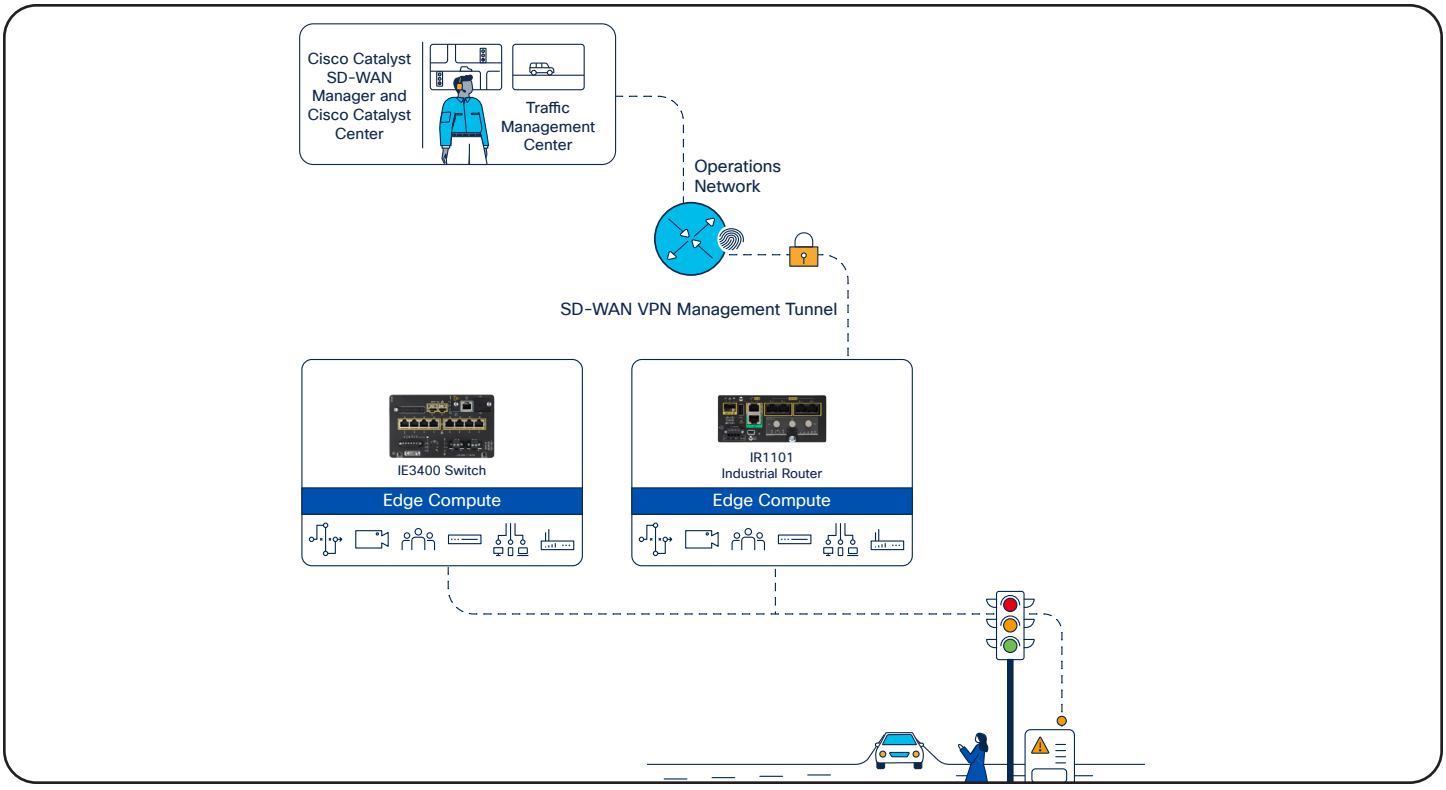


Figure 5. Edge compute capability

Deployment options

Given the complexity that exists along roadways, we next provide some examples of how to get started and scale as your roadways are digitized. Having a plan is critical to ensuring that investments are not wasted and can grow as your environment matures and has greater demands placed on it.

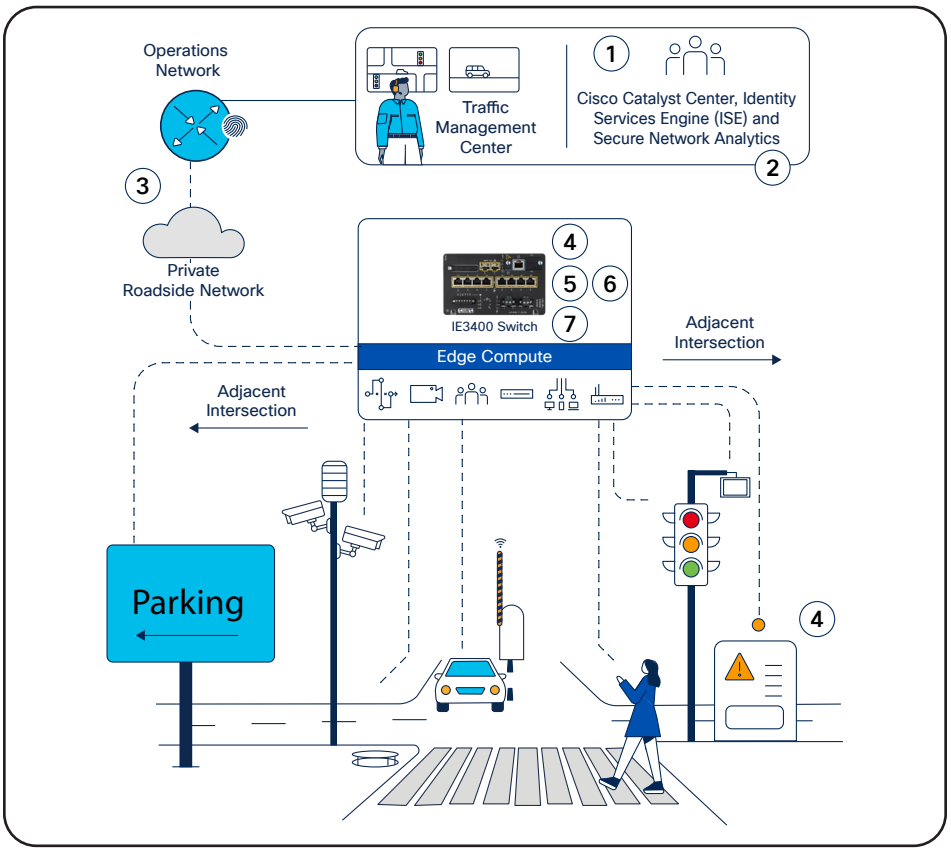


Figure 6. Key design benefits of integrated network deployment

Deployment option 1: Integrated network deployment

The typical desired configuration for connecting roadways and intersections together is over a fiber or high-speed wireless network, which we'll term an integrated network deployment. An integrated network will have the same characteristics as a traditional IT network but requires specialized equipment that can operate in harsher outdoor conditions. Integrated networks scale from flat Layer 2 networks up through full intent-based networking solutions with automated policy management and segmentation.

Network architecture components

- Robust metropolitan and regional intent-based network.
- Fiber or private connectivity supplemented with high-speed point-to-point wireless where needed.

1. Centralized and automated provisioning **of network elements**.
2. Centralized and automated provisioning **of security policy**.
3. Highly reliable and redundant network connectivity.
4. Multilevel security for intersection device data and management (Secure Boot, IPsec VPNs, 802.1X and MAB switch port security, Cisco SSE/Umbrella secure users and devices, Cisco Secure Network Analytics for traffic analysis, physical security alarms).
5. Macro-segmentation to isolate different services into dedicated, secure virtual networks.
6. Granular micro-segmentation policies to control device-to-device communication in a virtual network.
7. Multiple edge compute options to enable local data processing.
8. Visibility into all connected roadways equipment and secure remote access for remote maintenance and troubleshooting.

Benefits

- Simplified provisioning.
- Simplified operations.
- Multilevel security.
- Supports current and future use cases that require high bandwidth and low latency.

This deployment model is built with Cisco Intent-Based Networking (IBN), specifically Software-Defined Access (SD-Access); providing a transformational shift in building, managing, and securing networks, making them faster to deploy, easier to operate, and improving business efficiency.

Deployment option 2: Managed router connectivity

Where there is no access to wired or fiber connectivity, this basic deployment option involves the use of a cellular or DSL-connected managed router to provide connectivity from the roadside cabinet to the traffic management center. Sites in isolated areas and locations where private roadside network connectivity has not matched roadway growth are optimal scenarios for managed router connectivity.

Managed routers that are deployed in this scenario are cloud managed to enable simplified device installation, monitoring, and management on a service provider network. When connected to a service provider network, the possible variations in bandwidth, connection reliability, and latency, as well as recurring usage costs, should be considered in order to receive maximum benefit. Routers can also be managed as part of an integrated network model on-premises or jointly with a router management strategy as described in the other deployment options.

Network architecture components

- Cloud-managed cellular or DSL router
- Local devices connected to router switch ports

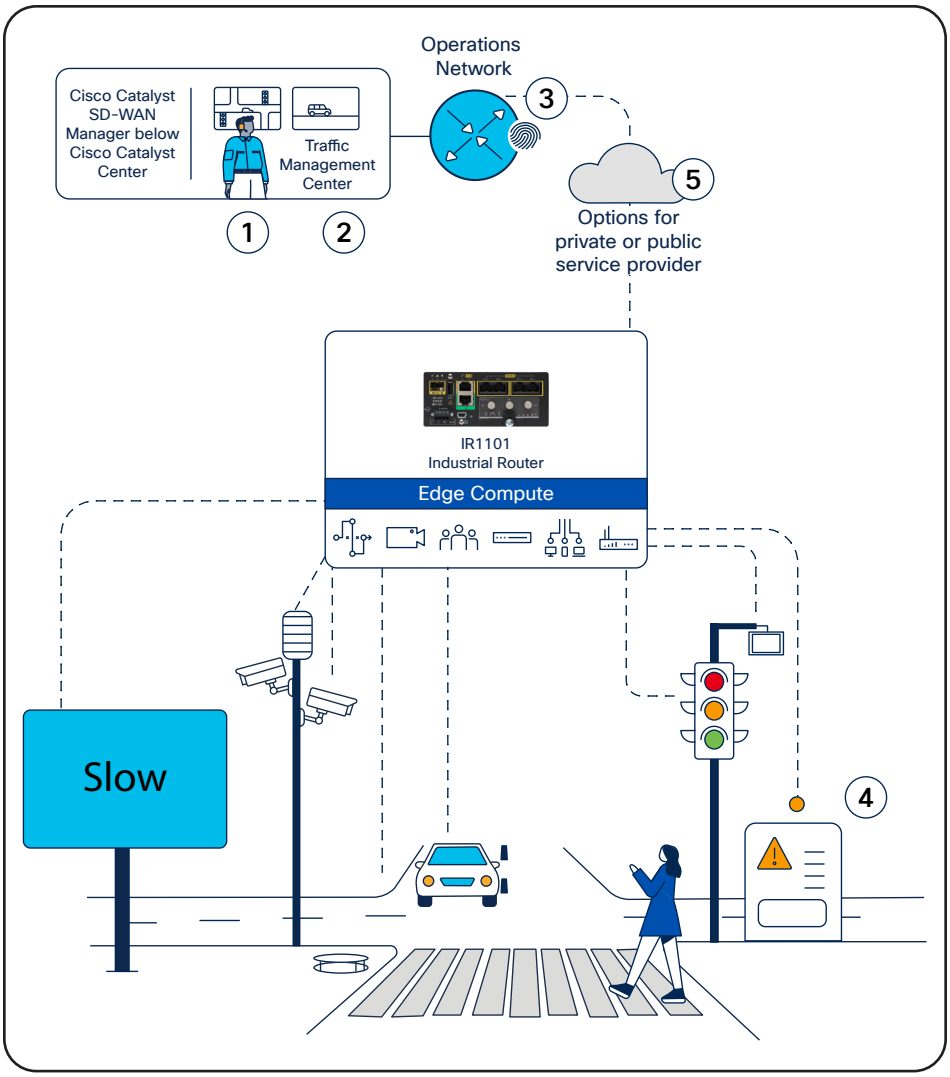


Figure 7. Key design benefits of managed router connectivity

1. Centrally managed configuration templates.
2. Zero-touch deployment of managed routers.
3. Multilevel security for intersection device data and management (Secure Boot, IPsec VPNs, 802.1X and MAB switch port security, Cisco Umbrella to secure users and devices, Cisco Secure Network Analytics for traffic analysis, physical security alarms).
4. Macro-segmentation to isolate different services into dedicated, secure virtual networks.
5. Visibility into all connected roadways equipment and secure remote access for remote maintenance and troubleshooting.
6. Onboard edge computing to support local data processing.
7. Redundancy options with multiple carriers or communications technologies.

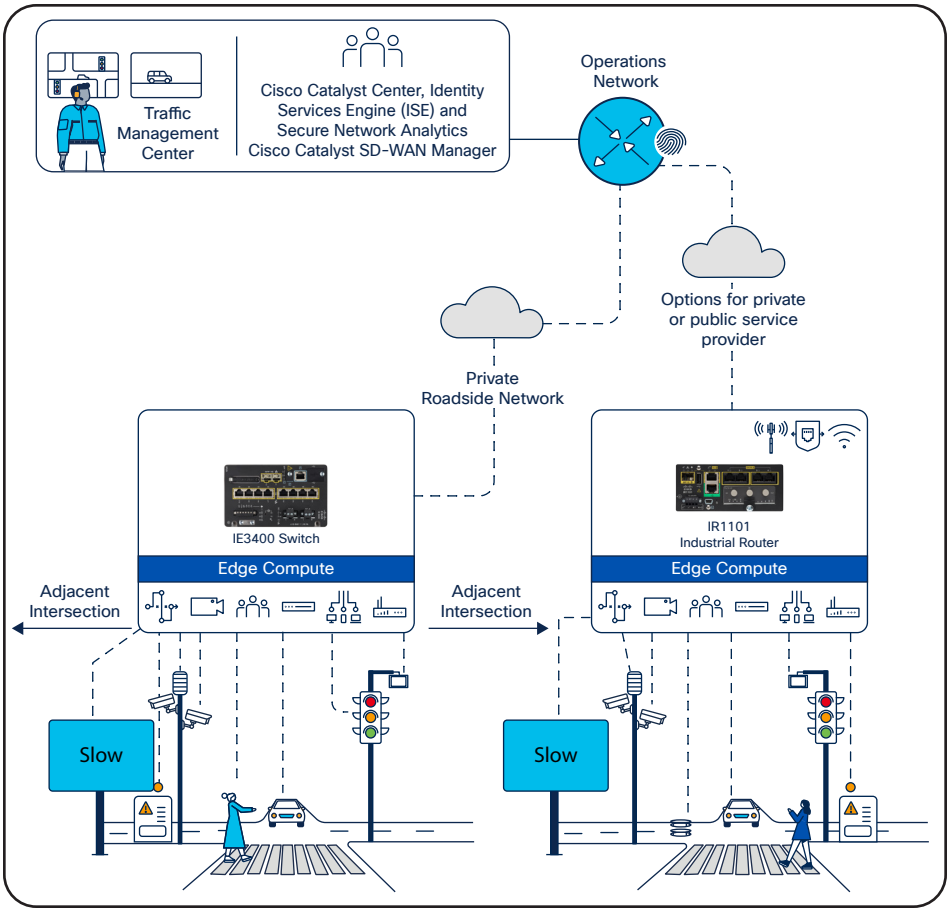
Note: Only certain Industrial Ethernet (IE) switches support edge compute, but all IE3x00 series switches can be used for roadways. For additional port count, a Cisco Catalyst IE3x00 series switch can be connected to the Cisco Catalyst IR1101 industrial router.

Benefits

- Simplified provisioning and automatic VPN creation.
- Simplified operations.
- Multilevel security (including IPS with the Cisco Catalyst™ IR1835 and IR8340 Rugged Routers).
- Use cases supported may be restricted by the available service provider service level (bandwidth, connection reliability, latency, QoS).

Deployment option 3: Hybrid network deployment

Cisco recognizes that you will likely have combinations of both deployment models described above in your system. No matter what you have in place, Cisco's designs for connected roadways provide the flexibility to connect fiber or high-speed wireless networks and managed router deployments into a completely integrated network, creating a robust single architecture that scales with you while retaining key design benefits.



Benefits

- Simplified provisioning.
- Simplified operations.
- Multilevel security.
- Macro- and micro-segmentation.
- Support for all connectivity options.
- Support for all current and future use cases.

Figure 8. Hybrid network deployment

Conclusion

Robust and connected solutions that can be deployed on network infrastructure that is simple to manage and operate are becoming essential to digitally transform roadways. Traffic/ITS assets that were previously commonly owned and operated by the roadway operators are becoming more dependent on IT support. Using Cisco Validated Designs as described in this solution brief reduces risk and, through deployment of a validated architecture, helps promote resilient operations and automation while guiding conversations with suppliers and partners toward outcomes, security, and scalability to help ensure the return on investment of the solution and good stewardship of public funding.

Cisco's roadway solutions validate many of the common use cases roadway operators wish to deploy and go beyond Cisco infrastructure components to include leading third-party industry partner devices and solutions.

Benefits of Cisco connected roadways and intersections solutions

- Prevalidated, proven, secure multiservice network for all your present and future goals.
- Ruggedized network for robust and effective movement of data in harsh environments.
- Automated service segmentation to reduce the scope of compliance and simplify security policies.
- Plug-and-play device deployment for simplicity and efficiency.
- Automated uniform policy deployment for one redundant and resilient network.
- Flexible network topology and backhaul options for future cost security and growth opportunities.

Resources

Cisco Communities Infrastructure CVD

Cisco Remote and Mobile Assets CVD

Cisco Catalyst Center

Cisco Connected Roadways

Cisco Ultra-Reliable Wireless Backhaul