Cisco IoT Solution Brief

Connected Roadways and Intersections

Cisco Validated Design

Benefits

Connect, manage, optimize, and secure your roadways and intersections:

- Flexible deployment options
- Rugged/reliable network devices
- Automated provisioning and resilient operations
- Scalable
- Multi-level security for roadside assets
- Bring compute to the edge of the network

Cisco connected roadways and intersections:

Optimizing today and ready for the future

Roadways and intersections technology has evolved at an amazing pace since the first traffic lights were installed a century ago. Today, intersections number in the millions with complexity ranging from simple two-lane roads to complex multi-lane and multi-modal configurations. Moreover, interstate highways and other roadways are being connected to information and warning systems to improve highway safety and reduce congestion using data available from a host of sensors.

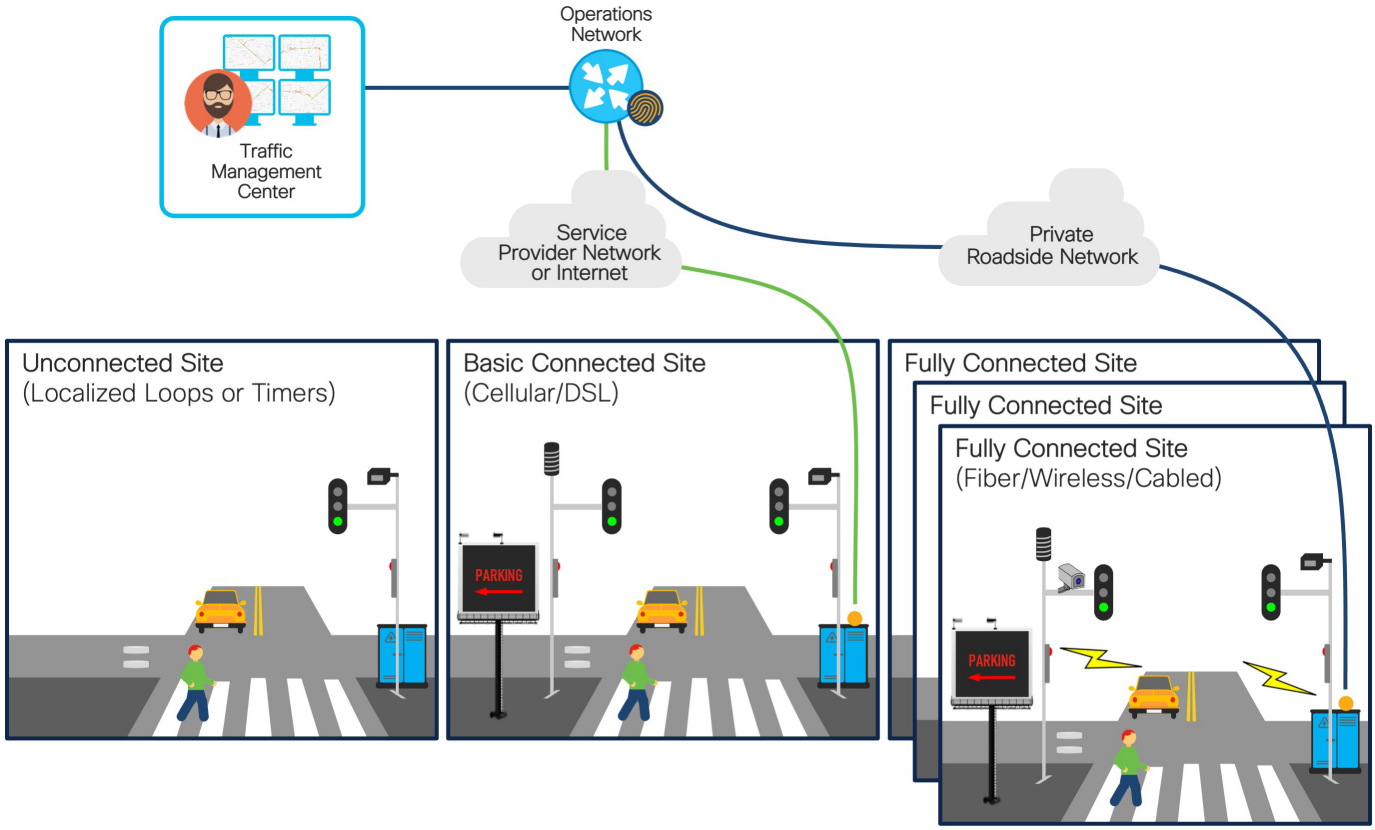
The need to connect, secure, and optimize our critical roadways and intersections infrastructure is clearer than ever. Roadways and intersections are being connected to traffic management centers allowing the collection of roadside data for analysis, real-time control, and visibility. This is the foundation of automating outcomes and improving situational awareness to improve safety, efficiency and reduce greenhouse gases. Meanwhile, increasing pressure is being placed on these systems as vehicles begin to communicate status and alerts to the roadside and other vehicles in and around the roadway. This pressure will only increase further with the growing numbers of Connected and Autonomous Vehicles (CAVs).

There are numerous ways to connect roadways devices to meet these growing needs, ranging from simple connectivity of legacy and modern intersection or roadway devices, through integration with advanced city or highway multi-access networks and a spectrum in-between. A solution is required that provides the flexibility to meet current needs while facilitating a clear path forward as complexity and scale evolve.

This solution brief provides an overview of Cisco's validated solutions to support these needs and which provide the following key benefits and more:

1. **Flexible deployment options:** Support for simple to advanced as roadways digitize, including legacy device connectivity
2. **Simplified provisioning:** Enable simple Add, Moves, Changes
3. **Simplified operations:** Minimize outages, faster issue resolution, support division of labor
4. **Multi-level security:** Provide end-to-end robust security capabilities to protect critical infrastructure and services
5. **Edge compute:** Provide data and control processing capabilities for work that is best done local to the roadway

The connected roadways and intersections journey



Roadway operators may have to manage and optimize legacy deployments while also planning for the future and advanced roadway deployments. This solution brief and related material was created with the understanding that roadway installations can be at different phases of transition and provides guidance to an operator, traffic engineer or architect on a logical path to evolving their roadways digitization efforts.

This drawing 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 outcome while creating operational resilience and maintaining security.

Why Cisco connected roadways and intersections

Cisco is a global leader in networking and provides a wide range of products to address connected roadways and intersections solutions. By applying our secure and hardened industrial networking, IoT expertise, and working with industry leaders to address challenges existing in the industry, we have created innovative technology solutions which optimize and secure our critical roadways and intersections. Our goal is to future-proof your investment by providing an evolution 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 solution. CVDs start with the solution use cases and architect the flow from the edge device to the application, validating the key Cisco and 3rd party components along the way. Each aspect of the architecture is thoroughly tested and documented with sample configurations, helping to simplify integration and de-risk implementations through proven solutions.

The goal is to ensure a deployment and a solution that's simple, fast, reliable, secure, and cost effective. Cisco developed Connected Roadways and Connected Communities Infrastructure CVD's 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, while sites with bandwidth constrains may be limited to simpler use cases like remote management and monitoring. Understanding the network and technology that can be deployed at a given site will enable traffic engineers to best determine use cases and devices that can be supported.

Key use cases

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 the basic management of the traffic signal controller, this use case supports Automated Traffic Signal Performance Measures (ATSPM/SPM) functionality. This is performed via the collection and reporting of 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. With the addition of remote monitoring of intersection health and early automated fault detection, up-time will be maximized, and recovery time will be decreased making a more resilient roadway system.

Video surveillance and monitoring: The ability to monitor an intersection or roadway area is a critical capability 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 making the camera a network sensor.

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 (see earlier use case) 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. Information gathered by sensors allows for the introduction of safety improvement measures such as warning signs and traffic signal holds to allow pedestrians/cyclists to safely cross or warn vehicles of obstructions in the roadway.

Cabinet operations and resiliency: 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 attributing cabinet failures to either network or power related issues so remedial actions can be properly targeted and performed quickly.

Traffic Signal Prioritization (TSP) / 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 EMS vehicle to preempt a traffic signal to reduce response time are key capabilities of a roadway solution. Through signaling initiated from the transit or first responder vehicle directly to the intersection or via a centralized Traffic Management Center (TMC), this use case supports the public interest in a smoothly running transit system and rapid response to emergencies.

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) displaying important safety, construction or route information, remote weather sensors to detect hazardous weather or roadway conditions and alerting of road or construction site workers of oncoming traffic are all elements of this use case.

Highway tolling: Highway tolling involves detection of vehicles via RFID tags, license plate readers or tolling stations accepting various forms of payment. Ranging from single lanes to 10+ lanes, tolling stations require management, safety/lane steering messages to drivers and secure delivery of financial transactions.

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 are driving the deployment of charging stations along highways and in cities requiring visibility and management of charging resources.

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, DSRC or ITS-G5, vehicles become sensors exchanging real-time information with intersections and roadways equipment to assist with collision avoidance and congestion reduction via adaptive signal control/timing. Today's Intersections need to be ready to integrate these features to automate signal timing adjustments across a range of related intersections to optimize traffic flow dynamically improving safety and reducing emissions.

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.

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 / 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

Today's connectivity challenges

As roadways become increasingly connected and remotely accessible, equipment has to be installed with conscious effort given to the ease of operations, management and security. Our validated solutions are simple, scalable and flexible with focus put on operations processes that are field-friendly, not requiring a technical wizard. Our centralized network device management and strong asset operation capabilities eliminate the need for manual asset tracking or inconsistencies in field deployment from one site to the next. Integration with operations ensures that field technicians can easily deploy and manage these devices without the need for IT support, while both the IT and traffic operations team (OT) have full visibility and control of the deployed equipment and critical applications. The next sections describe specific capabilities of the Cisco validated solutions.

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

Simple provisioning

It is important that a field engineer can 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. An example of how a new device can be zero-touch deployed with Cisco validated roadway solutions is given here.

Benefit: A new networking device needs to be added at the intersection.

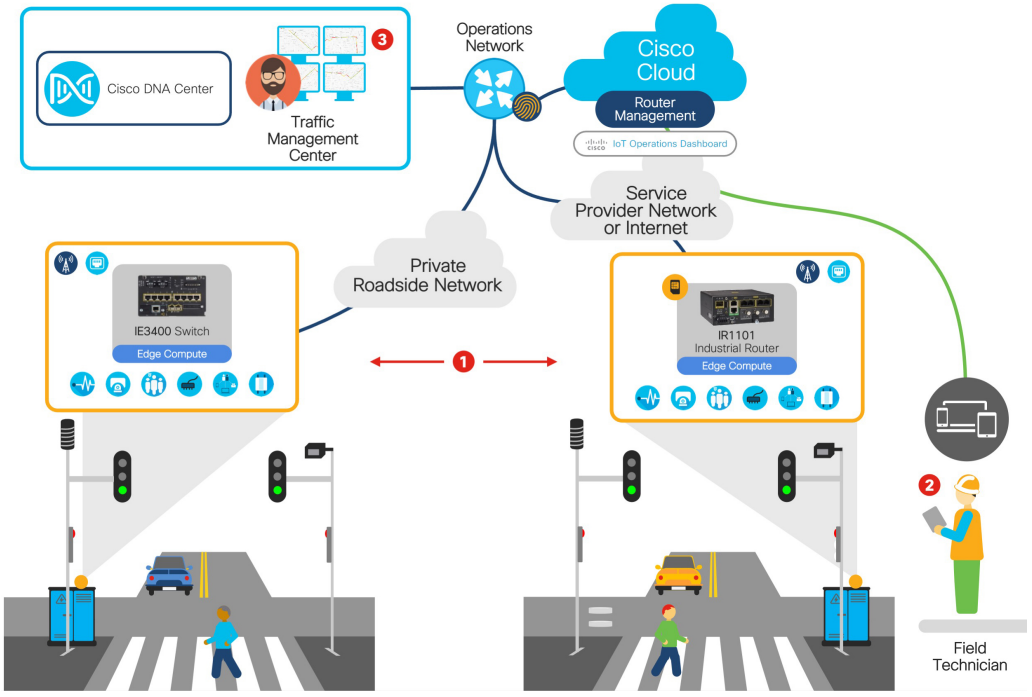
Field engineer: Make it easy for a field technician to install and maintain required roadside equipment at scale without having to know about ports, network security, or perform individual device configuration.

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 ensuring traffic related applications and outcomes are operating. Quickly identify any issue to 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

Note: Only certain IE switches support edge compute but all IE3x00 series switches can be used for Roadways.

Simple operations

Removing complexity for operations leads to quicker problem resolutions, higher system availability, and better outcomes for people using the roadways. Automating asset inventory, eliminating the reliance on manual device tracking, and deploying policies from a central location ensures accurate information about the status and operations of the equipment supporting the roadway. As events occur along the roadway, such as unauthorized access to roadside cabinets, power failures, or failed equipment, it is critical to have that operational visibility 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.

Benefit: Minimize service outages and support faster issue resolution.

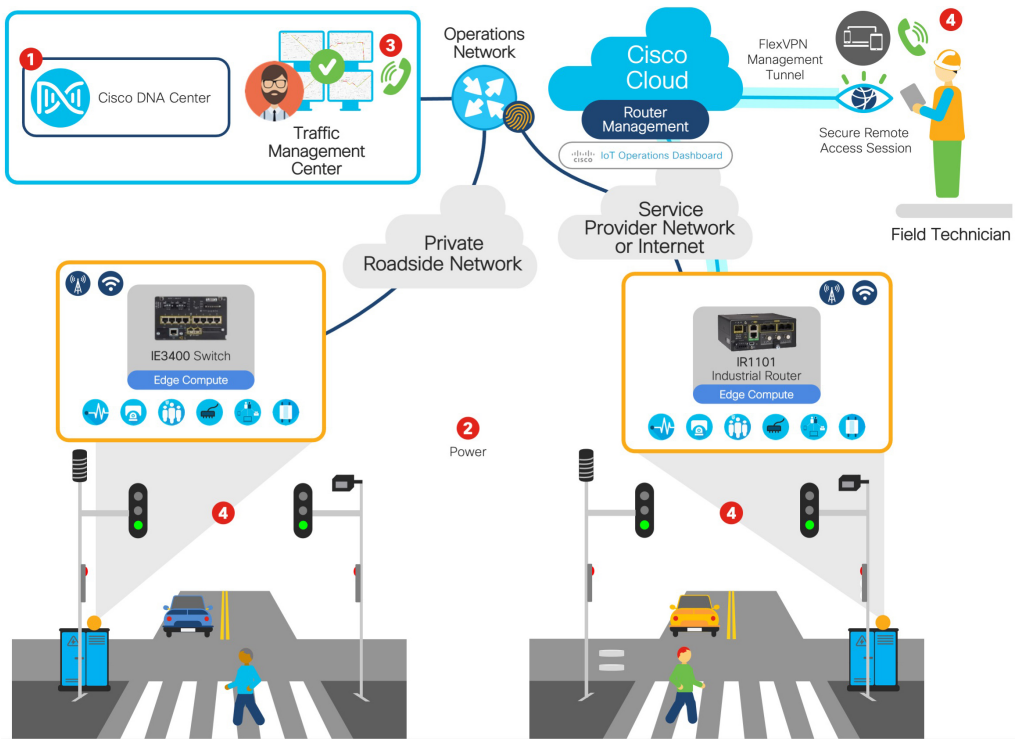
Field engineer: Dispatched to site. Connects to management tools and applications to make an impact quickly after arriving on scene.

Network operations: Automated visibility to all services operating at the intersection including the network equipment. Notify traffic operations of network status. Investigate problem; identify source.

Traffic operations: Uses remote management tools to gain visibility and investigate traffic equipment status. Quickly identifies any issues and dispatches proper resources to resolve alarms.

Cisco building blocks: Operations

Minimize downtime through remote troubleshooting and system visibility.



1. **10:00 pm:** Alert received at both the network and Traffic Management Center indicating traffic signal controller communication has been lost
2. **10:05 pm:** The traffic operation team can see:
   a. The network switch sent a dying gasp alert indicating intersection power loss **OR**
   b. 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 to temporarily control the intersection for safety while a field engineer is dispatched to locally troubleshoot the issue
4. **10:30 pm:** Technician arrives on scene and takes appropriate action to bring traffic lights back in service

Multi-level security

Roadway infrastructure is at constant cyber and physical security risk. Roadside cabinets are out in the public domain and as devices become connected the attack surface increases significantly. A secure architecture requires a multi-layer approach to ensure the physical security of the roadside cabinet, network port level security of the equipment, network segmentation, and application level traffic security. 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 to that traffic, and isolate potential security issues and breaches to a single virtual network. This is called macro segmentation. Micro segmentation provides another layer of segmentation to further isolate equipment from each other on the same segment. These features used in conjunction with port level security, like 802.1X and Mac Authentication Bypass (MAB), ensure that only known devices are allowed on the network and that policy is in place to control which devices and equipment can communicate with each other, in some cases to the protocol level.

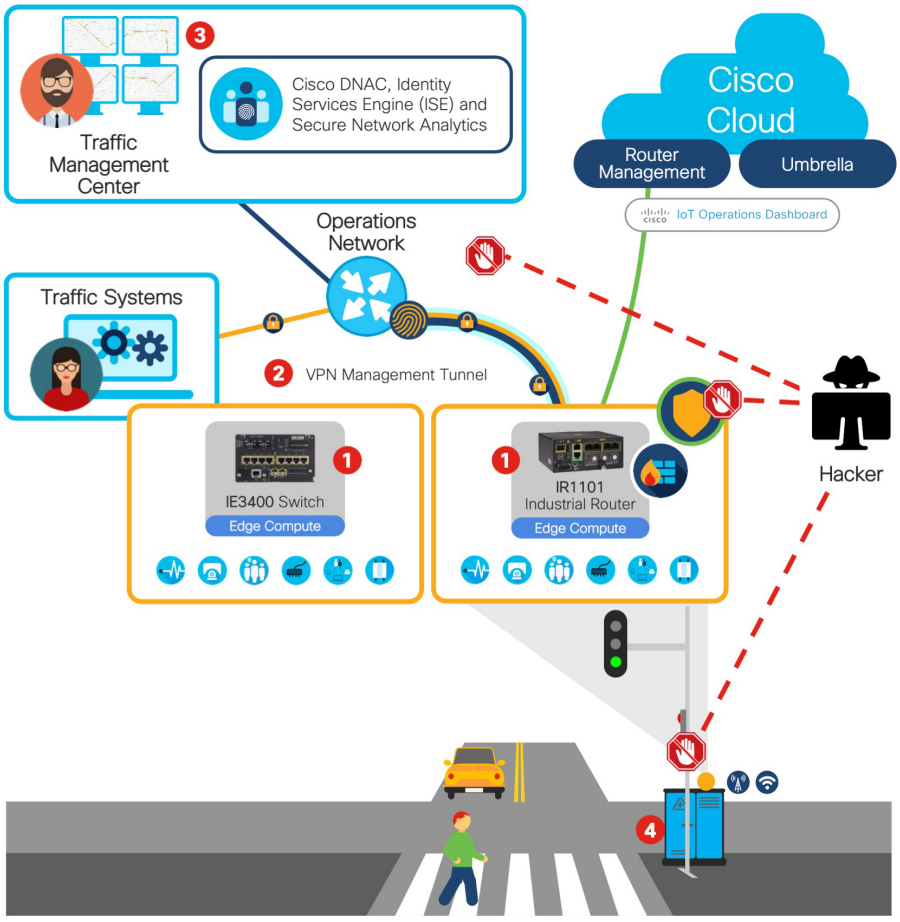
Benefit: Scalable real-time cyber security protection from external and internal threats.

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

Traffic operations: Have visibility to 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

Multi-layered security enforced through a single control point; ensure data confidentiality and end-to-end encryption.



1. Device access security using port security, secured operating system, and secured device features
2. Protection of data end-to-end on and across the network using services like standards-based encrypted IKEv2 IPSEC VPN tunnels, secured firewalls, and network segmentation, where desired
3. Cyber security with 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. Physical security intrusion detection enabling visibly into cabinet access

Edge compute

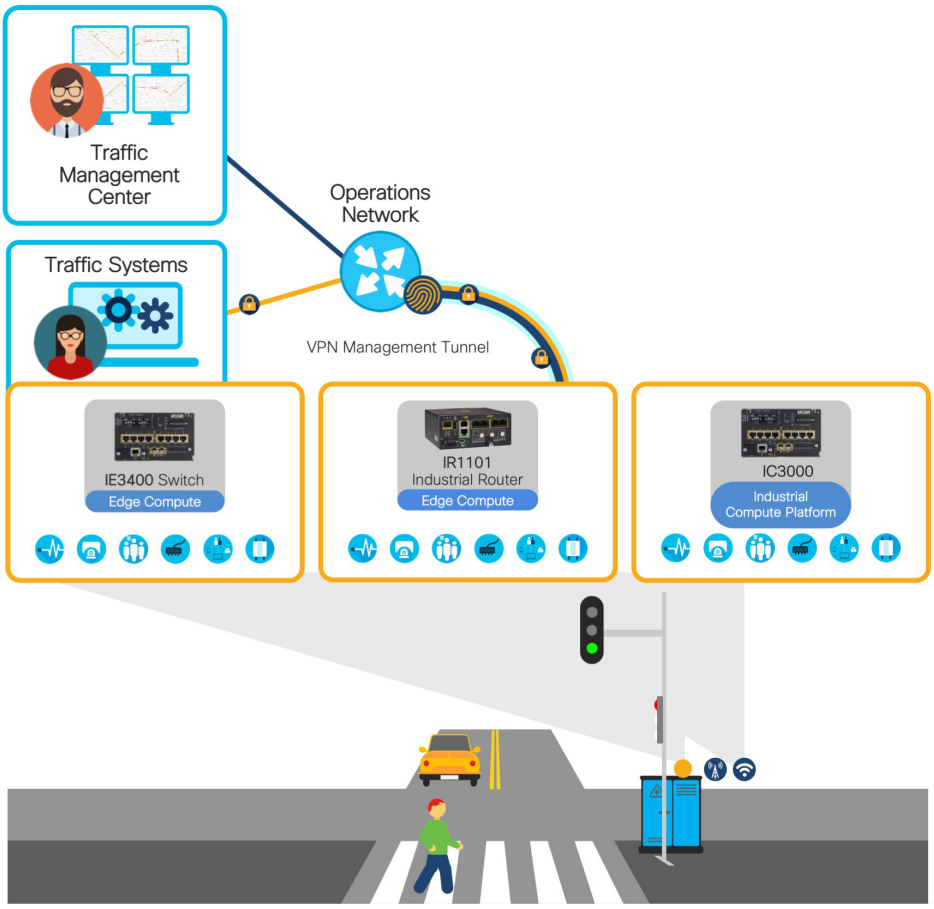
Edge compute supports a variety of applications providing local computation and decision making at the roadway and intersection site. Much of Cisco's IoT portfolio is capable of supporting edge compute applications to reduce the need for additional hardware in an already space confined location.

Applications of edge compute include data reduction of large amounts of repetitive data that can be received or created along a roadway, normalizing data that is received along the roadway into common formats, or 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 affect local actions, such as updating variable speed and digital message signs or opening and closing roadway barriers.

Cisco building blocks: Edge compute

- Edge compute that supports standards-based microservices through an open ecosystem
- 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



Deployment options

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

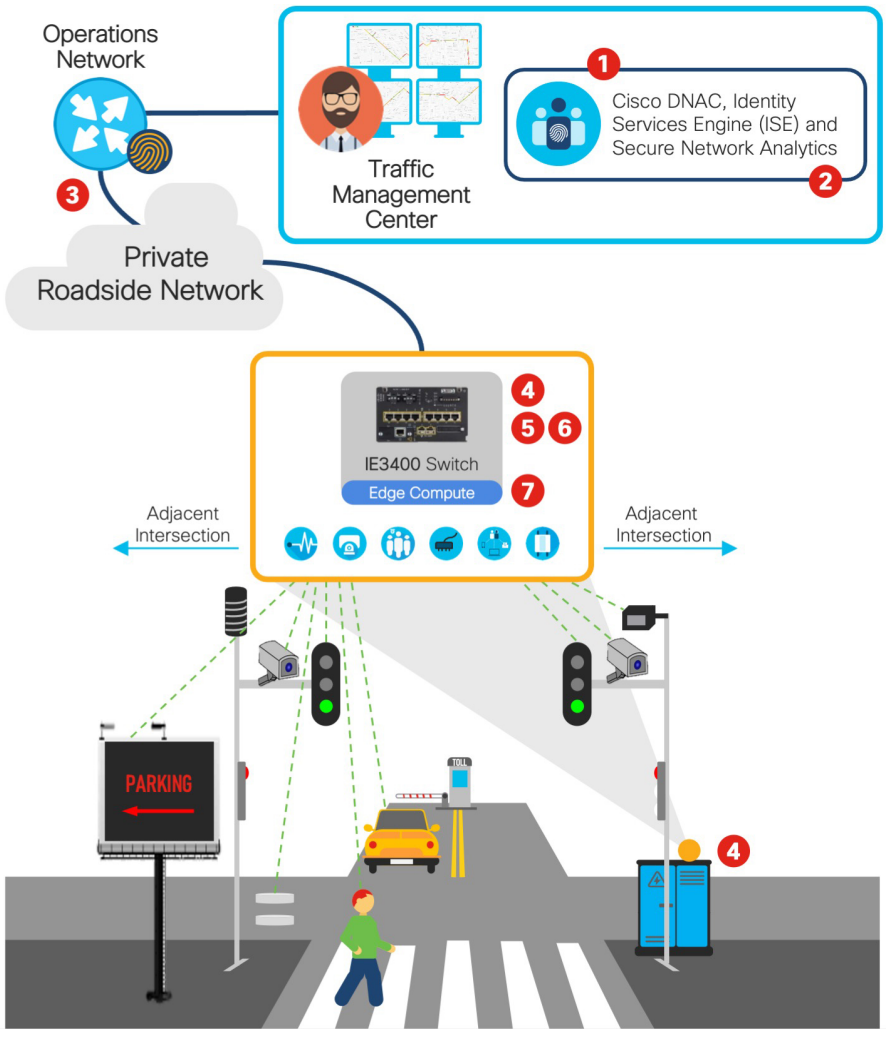
Deployment option 1: Integrated network deployment

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 of a traditional IT network but requires specialized equipment that can operate in harsher rugged and outdoor conditions. Integrated networks solution 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

Key design benefits



1. Centralized and automated provisioning **of network elements**
2. Centralized and automated provisioning **of security policy**
3. Highly reliable and redundant network connectivity
4. Multi-level security for intersection device data and management (secure boot, IPsec VPNs, 802.1X & MAB switch port security, Cisco Umbrella to 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

Results

- Simplified provisioning
- Simplified operations
- Multi-level security
- Supports current and future use cases with high bandwidth and low latency network capabilities

This deployment model is an example of the **Cisco Connected Communities Infrastructure (CCI)** validated solution and is built with Cisco Intent-Based Networking (IBN). Another solution within Cisco Digital Network Architecture (Cisco DNA) is Software Defined Access (SDA), which is built on IBN principals, providing a transformational shift in building, managing, and securing networks, making them faster to deploy, easier to operate, and improving business efficiency. CCI, using Cisco DNA-Center, allows for critical collaboration on network segmentation and security policy deployment creating consistent deployment models, easing operations, and allowing a division of labor between operational technology (OT) and information technology (IT).

Deployment option 2: Managed router connectivity

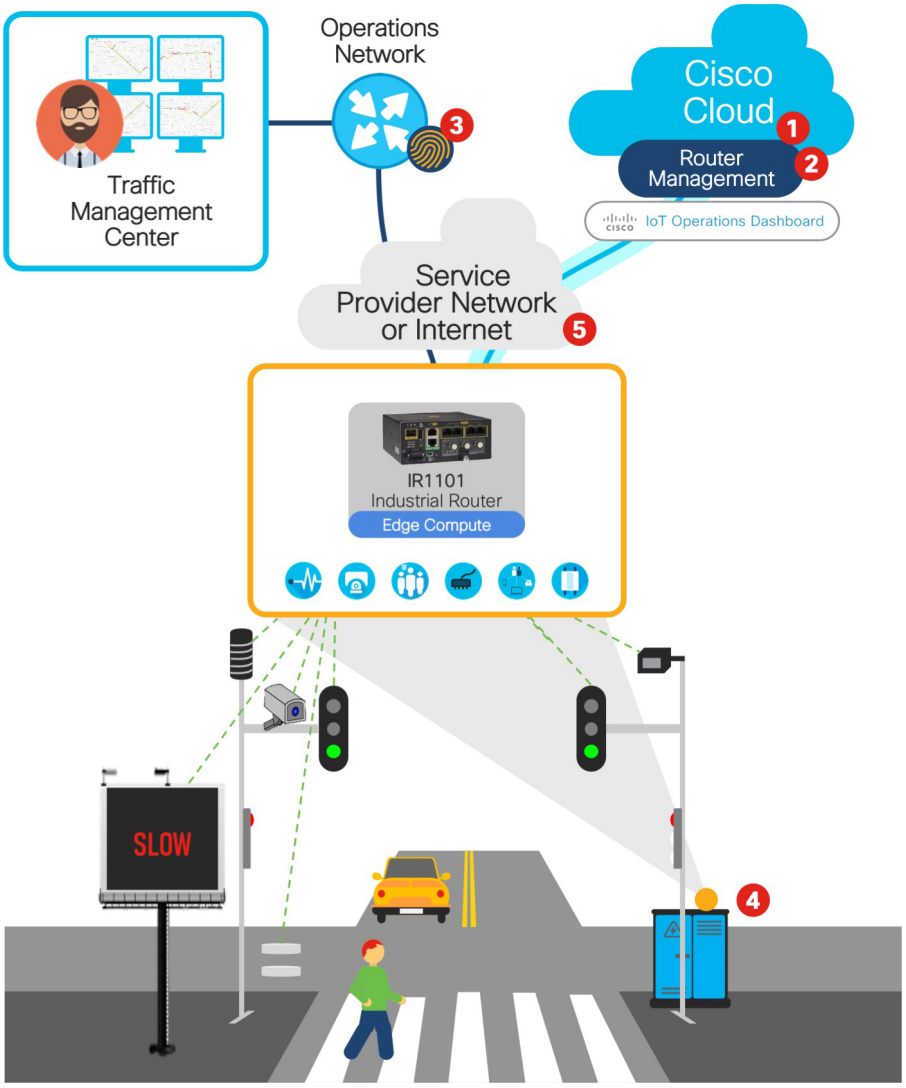
Where there is no access to wired/fiber connectivity, this basic deployment option involves the use of a cellular or DSL connected managed router to provide connectivity from the roadside cabinet to the traffic management center. Sites in isolated areas and sites in locations where private roadside network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

Managed routers that are deployed in this scenario are cloud managed to provide 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-premise or jointly with a router management strategy as described above in the other deployment options.

Network architecture components

- Cloud managed Cellular/DSL Router
- Local devices connected to router switch ports

Key design benefits



1. Centrally managed configuration templates
2. Zero-touch deployment of managed routers
3. Multi-level security for intersection device data and management (secure boot, IPsec VPNs, 802.1X & 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. Onboard edge computing to support local data processing
6. Redundancy options with multiple carriers or communications technologies

Note: For additional port count, an IE3x00 series switch can be connected to the IR1101 Industrial Router.

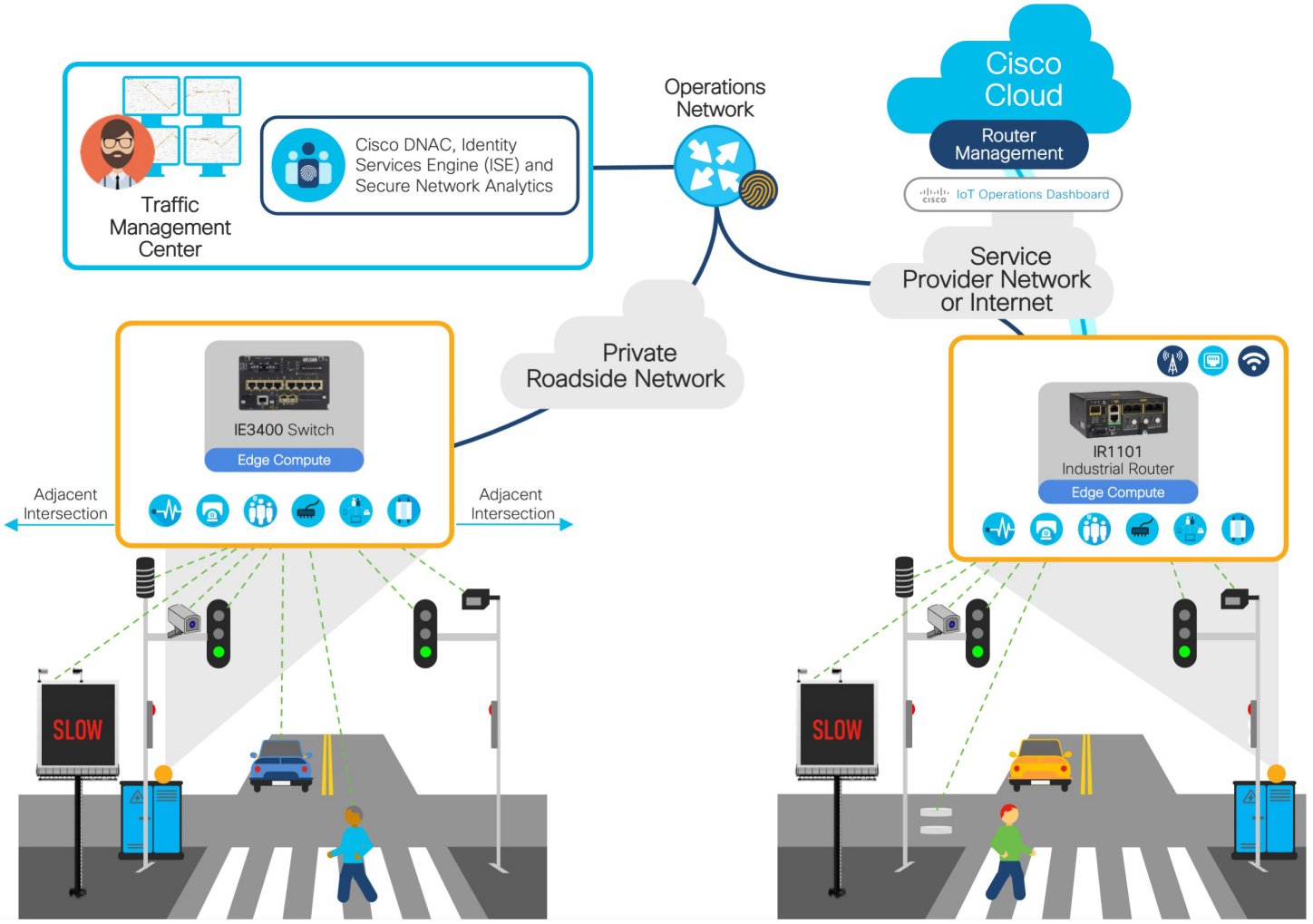
Results

- Simplified provisioning
- Simplified operations
- Multi-level security
- Use cases supported may be restricted by the available service provider service level (bandwidth, connection reliability, latency, QoS)

This deployment model is a specific example use case of the Cisco Remote and Mobile Asset (RaMA) validated solution using IoT management templates and tools targeted to OT staff to quickly and easily configure, onboard, and operate routers in a consistent fashion, helping ensure security policies are uniform and providing asset inventory and status information, all from a single pane of glass.

Deployment option 3: Hybrid network deployment

Cisco recognizes that you will likely have combinations of both deployment models in your system. No matter what you have in place, Cisco's designs for connected roadways provide 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.



Results

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

Conclusion

The demands for robust and connected solutions on simple to manage and operate network infrastructure are becoming essential to digitally transform roadways. Operating technology (OT) that were commonly owned and operated by the roadway operators are becoming more information technology (IT) dependant. Deploying Cisco Validated Designs (CVDs) reduces risk and, through deployment of a validated architecture, helps promote resilient operations and automation while guiding converstations with suppliers and partners toward outcomes, security and scalability to ensure the longevity of the solution and good stewardship of public funding.

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

Cisco connected roadways and intersections benefits

- Pre-validated, proven multi-service network for all your present and future goals
- Ruggedized network for robust and effective movement of data
- 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 Connected Roadways

Cisco Remote and Mobile Assets CVD

Cisco Ultra Reliable Wireless Broadband

Cisco DNA-Center

Cisco IoT Operations Dashboard

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.