Cisco IoT Solution Brief

Electric Vehicle Charging Networks

Cisco Electric Vehicle Charging Networks

Benefits

Connect, manage, monitor, and secure your EV charging networks:

- Flexible deployment options
- Rugged and reliable network devices
- Automated provisioning and operational visibility
- Scalable
- Multilevel security for curbside assets
- Bring compute to the edge of the network
- Provide a platform for value-added services

Simplicity today and ready for the future

As we move toward 2030, many countries are accelerating the use of electric vehicles (EVs) and investing in EV charging networks. Public and private networks are being installed at a fast pace, with many traditional fossil fuel industries and automotive manufacturers now investing heavily in the transition to electric vehicles.

Reliable and secure connectivity is key for providing a seamless user experience, from checking charge point availability on a smartphone to paying for usage and monitoring charge status. Without a reliable and secure communications infrastructure, the user experience is poor.

From the charge point operator's perspective, the network needs to be easy to deploy, monitor, upgrade, and troubleshoot.

There are numerous ways to connect EV charge points to meet these growing needs, ranging from simple connectivity using built-in cellular modems (installed at the factory by the charge point manufacturer) to dedicated industrial gateways serving multiple charge points as well as industrial routers supporting multiple backhaul connections (DSL, fiber, cellular) and industrial switches for connecting increased numbers of EV charge points at a single location.

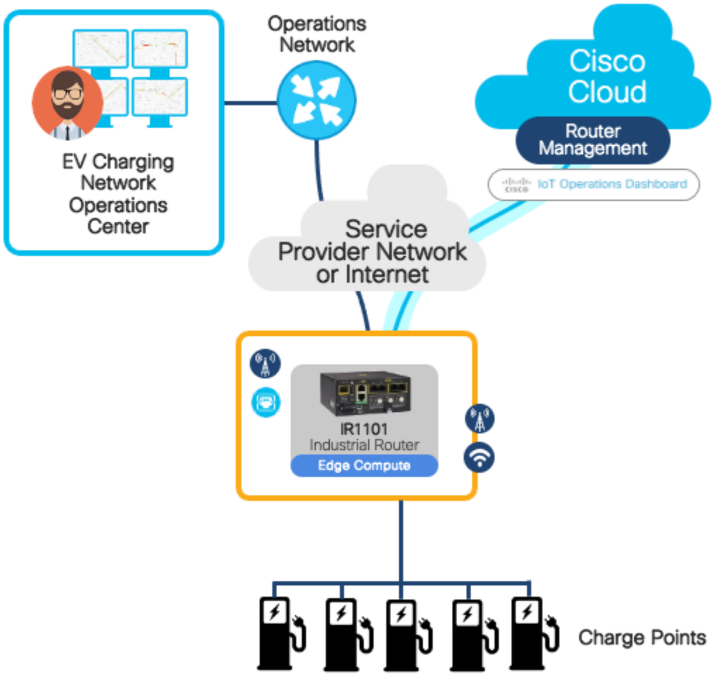
A solution is required that provides the flexibility to meet these current needs while facilitating a clear path forward as complexity and scale evolve.

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

- **Flexible deployment options:** Support simple to advanced solutions that cover various deployment options.
- **Simplified provisioning:** Enable simple onboarding, monitoring, and management of the remote equipment.
- **Simplified operations:** Increase operational visibility, minimize outages, and enable faster remote issue resolution.
- **Multilevel security:** Provide end-to-end robust security capabilities to protect the charging infrastructure and associated services.

Electric vehicle charge point connectivity

Figure 1. Cisco solution for EV charge point connectivity.



Cisco's industrial routers and gateways, paired with the Cisco® IoT Operations Dashboard platform, provide a powerful software-as-a-service (SaaS)-based solution for secure onboarding and provisioning of new deployments, plus ongoing lifecycle management of the communications infrastructure.

Cisco Catalyst IR1100 Rugged Series Routers

The modularity and expansion capabilities of the Cisco Catalyst® IR1100 Rugged Series can help extend product lifetime. Their compact, modular, ruggedized design is excellent for EV charging network use cases. They offer strong industrial router security and simplified management with support for advanced features such as SD-WAN and edge compute. The IR1100 Rugged Series is easily mounted within existing cabinets or charger enclosures.

Cisco Catalyst IE3100, IE3200, IE3300, and IE3400 Rugged Series Switches

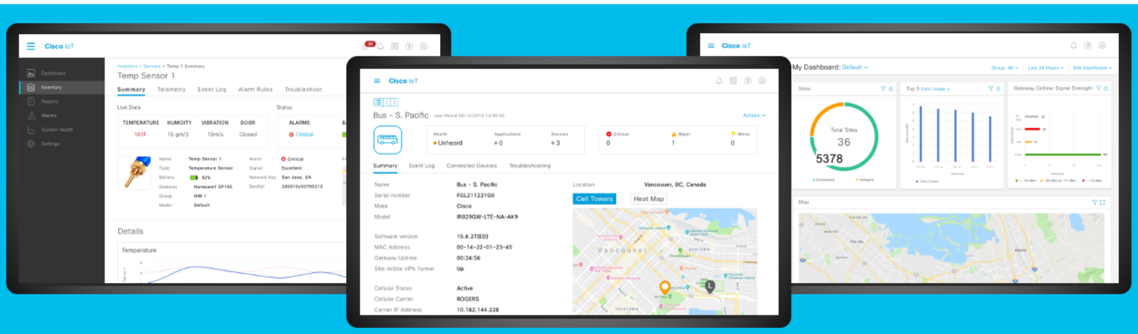
Cisco Catalyst IE3100, IE3200, IE3300, and IE3400 Rugged Series Switches feature advanced, full Gigabit Ethernet speed for rich, real-time data and a modular, optimized design. These rugged switches bring simplicity, flexibility, and security to the network edge and are optimized for size, power, and performance.

From their end-to-end security architecture to delivering centralized automation and scale with Cisco intent-based networking, the Cisco Catalyst IE3100, IE3200, IE3300, and IE3400 Series are the perfect solution to your switching needs in almost any use case.

Cisco IoT Operations Dashboard

The Catalyst IR1101 and IoT gateways are centrally managed through the same easy-to-use Cisco IoT Operations Dashboard. You can remotely deploy, monitor, and troubleshoot the gateways at scale. With the IoT Operations Dashboard, you can gain insights into network usage and carry out updates remotely without sending anyone onsite.

Cisco IoT Operations Dashboard benefits



Scale easily

- Configuration templates (eCVDs) reduce IT's pre-deployment coding
- Deploy in minutes without onsite IT support using IT-managed templates and zero touch deployment (ZTD) capabilities
- Expand your network or change existing settings with bulk actions

Simplify operations

- Get a unified view that includes the network to data visualizations
- Boost uptime with 24/7 monitoring and alerts on network devices & assets
- Simplify workflows with an intuitive web interface tailored to OT needs

Cisco Secure

- Enforce and control standard security configurations across all devices
- Support IT/OT collaboration with role-based access control
- Grant granular access down to the asset level to ensure users only touch what they need

Figure 2. Benefits of the Cisco IoT Operations Dashboard

Why Cisco for electric vehicle charging networks

Cisco is a global leader in networking and provides a wide range of products to address the EV charging market. By applying our secure and hardened industrial networking and our IoT expertise, and by working with industry leaders to address challenges existing in the industry, we have created innovative technology solutions that optimize and secure EV charging assets. Our goal is to make your investment future-ready by providing a path to evolve from today's isolated deployments to secure, connected electric charging deployments 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 start with 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 is thoroughly tested and documented with sample configurations, helping to simplify integration and de-risk implementations through proven solutions.

The goal is to help ensure a deployment and solution that are simple, fast, reliable, secure, and cost-effective. Cisco has developed EV charging network solutions to specifically address the networking and security needs of charge point operators and fleet charging owners.

Electric vehicle charging use cases

The wide-area communications options available at a given site will greatly influence the outcomes and capabilities for any use case at the curbside, parking lot, or fleet parking area. The availability of dependable lower-latency, high-bandwidth connectivity (such as fiber, LTE/5G cellular, Wi-Fi, or DSL) allows for more advanced network and data service options, while sites with bandwidth constraints may be limited to simpler use cases such as remote management and monitoring only.

Key use cases

Management and monitoring of connected EV charge points: This is the simplest use case, providing remote visibility, fault reporting, and remote access to EV charge points. From a single dashboard, operators can monitor the uptime and receive alerts for any issues. IoT Operations Dashboard provides real-time monitoring for the communications network and connected endpoints (the charge points or other devices connected to the network router or gateway).

Video surveillance and monitoring: The ability to monitor a charge point area is critical for gaining awareness of activity around the charge points. Through the use of video surveillance cameras, operators can obtain live video streams on demand, viewing them for immediate response and/or storing them 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 addition to simple video surveillance, this use case provides real-time and historical views of pedestrian and vehicle activity around a charge point focus area. Camera analytics can provide people and vehicle detection.

Secure remote access: IoT Operations Dashboard provides Secure Equipment Access via the onsite Catalyst Rugged Routers or IoT gateways. Secure remote access is provided in the remote user’s internet browser, simplifying the connectivity. Users can be restricted to only the assets they have permission to access. This simplifies troubleshooting of charge points remotely, with the aim of reducing downtime and onsite visits.

Digital signage: Value-added services such as local screens with targeted advertisements for the specific location can bring additional revenue and customer traction. Regular content updates are required and can be reliably pushed via the Cisco communications equipment.

Data offload: Local Wi-Fi access can be provided for users or vehicles. Wi-Fi has several relevant use cases:

- Connecting charge point operators’ smartphone applications (avoids relying on cellular network)
- Connecting vehicles to the charge point (for telemetry, map, or firmware uploads or downloads to vehicles)
- Connecting the charge point where fixed cabled connections are not possible to the Cisco router or gateway

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 the amount of data being delivered from the charge point location through the network relative to available capacity (bandwidth) and the real-time operational needs (latency) in receiving that data.

Table 1. Bandwidth and backhaul technology for key use cases.

Use case	Bandwidth demand	Suitable backhaul technology
Management and monitoring of EV charge points	Low	Cellular, fiber, DSL
Video surveillance and monitoring	High	Fiber, DSL
Vehicle and pedestrian safety monitoring	Medium (data) to high (video)	Fiber, DSL
Secure remote access	Very low	Cellular, fiber, DSL
Digital signage	Low	Cellular, fiber, DSL
Data offload	High	Fiber, DSL

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

Today’s connectivity challenges

As EV chargers become increasingly ubiquitous, equipment must be installed with conscious attention given to the ease of operations, management, and security. Our validated solutions are simple, scalable, and flexible, with a focus on operations processes that are field-friendly without 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 helps ensure that field technicians can easily deploy and manage these devices without the need for IT support, while both the IT and EV charging operations teams have full visibility into and control over the deployed equipment.

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 hardwired connections are not available.

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 and monitoring of system status and contributes to best operational practices and processes. An example of how a new device can be deployed with zero touch with the Cisco solution is given here.

Benefit: Add a new backhaul networking device to a charge point site.

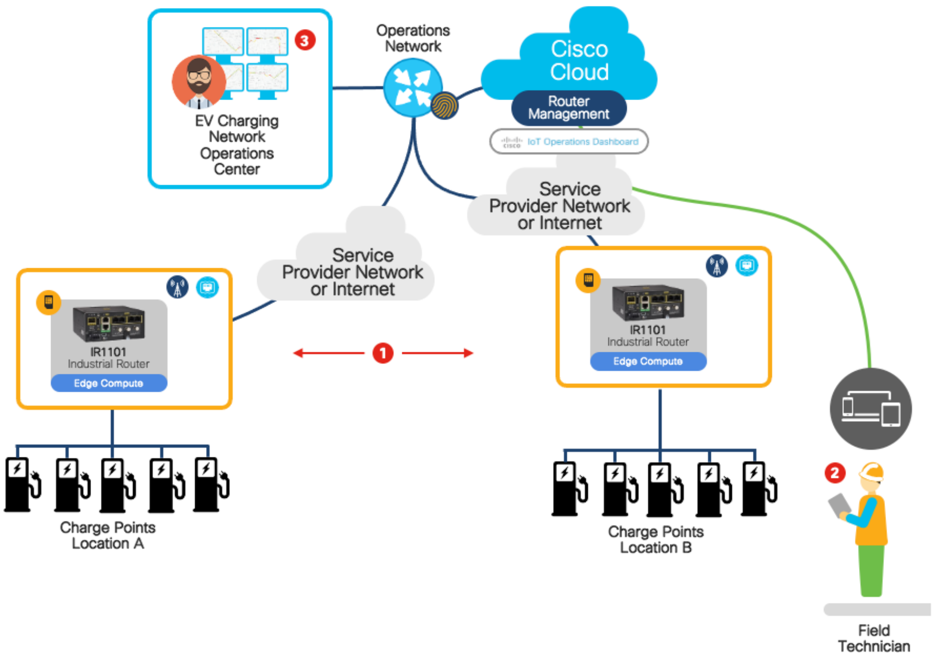
Field engineer: Easily installs and maintains the required equipment at scale without having to know about ports or network security or perform individual device configuration.

Network operations: Consistently deploys, monitors, and operates the network at any location to help ensure security policy, device operation, configuration, and consistency.

EV network operations: Responds quickly to site events to troubleshoot issues and pinpoint the problem. Quickly identifies any issue and dispatches the proper resource to resolve the issue if necessary.

Cisco building blocks: Provisioning.

Figure 3. Zero-touch deployment of network infrastructure at EV charge point locations.



1. Centrally configure the policy for consistent asset configuration and communication parameters for any location.
2. Allows a technician to deploy specific charge point location 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.

Simple operations

Removing complexity from operations leads to quicker problem resolution, higher system availability, and better outcomes for people using the charge points. Automating asset inventory, eliminating reliance on manual device tracking, and deploying policies from a central location help ensure accurate information about the status and operations of the equipment supporting the charging network. As events occur at the charging locations, such as unauthorized access to roadside cabinets, power failures, or failed equipment, it is critical to have that visibility to be able to respond quickly with the right resources to address the issue and get the charging locations operational again. Below is an example of how Cisco's EV charging solutions can benefit your operations teams.

Benefit: Minimize service outages and support faster issue resolution.

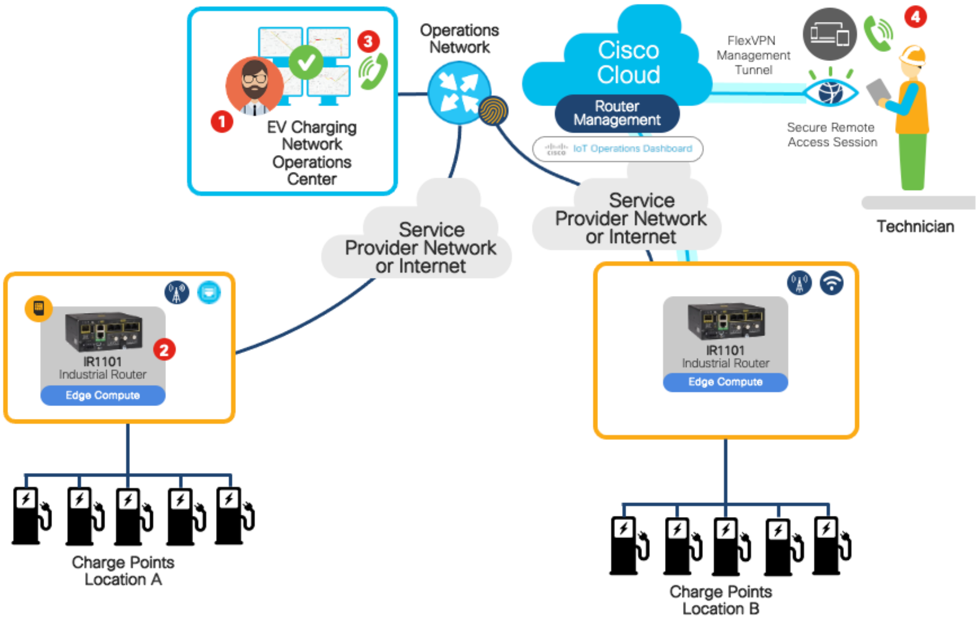
Field engineer: Connects to management tools and applications to make an impact quickly after arriving on scene.

Network operations: Has automated visibility into all services operating at the intersection, including the network equipment. Notifies field operations of network status. Investigates problems and identifies source.

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

Cisco building blocks: Operations.

Figure 4. Minimize downtime through remote troubleshooting and system visibility.



1. **10:00 pm:** Alert received at the EV network operations center indicating that charge point communication has been lost at location A.
2. **10:05 pm:** The EV operations team can see:
   - The network router or gateway is not online.

   OR

   - The networking equipment is online and has network connectivity, indicating a possible charge point problem.
3. **10:15 pm:** An engineer is tasked to troubleshoot the issue and can connect via remote access to the site and charge points.
4. **10:30 pm:** Technician takes appropriate action to bring the charge points back in service or logs a request for an onsite visit.

Multilevel security

EV charging infrastructure faces constant threats to cyber and physical security. EV charge points and associated cabinets are out in the public domain, and as devices become connected the attack surface increases significantly. A secure architecture requires a multilayer approach to help ensure the physical security of the curbside assets, network port-level security of the equipment, network segmentation, and application-level traffic security. Cisco's solution integrates all layers of security to help 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 for isolating 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 such as 802.1X and Mac Authentication Bypass (MAB), help 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.

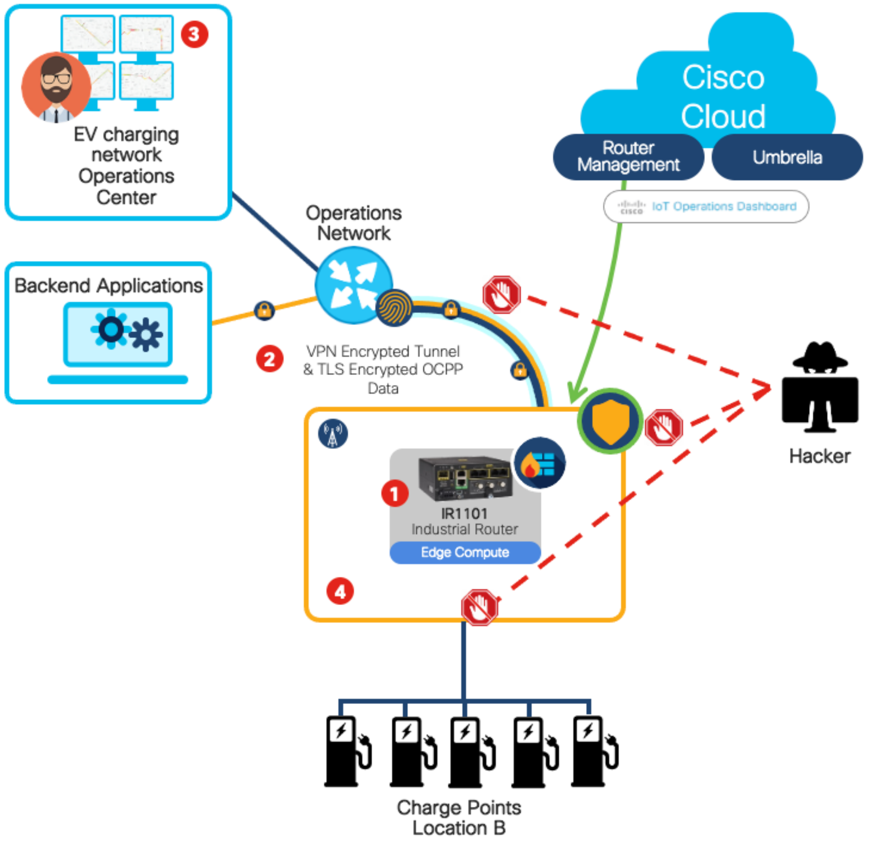
Benefit: Scalable, real-time cybersecurity protection from external and internal threats.

Network operations: Consistently applies security policy, deploys security updates, and protects from unwanted devices or applications on the network. Performs ongoing monitoring and analysis of the network with automated anomalous network traffic detection and alerts and is able to instantly quarantine suspect devices or applications.

Field operations: Has visibility into cabinet access, quickly deploys equipment without having to understand complex security deployments, and knows that critical applications are available and operational at the charging locations.

Cisco building blocks: Security

Figure 5. Multilayer security enforced through a single control point to help 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 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. Cybersecurity 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

Edge compute

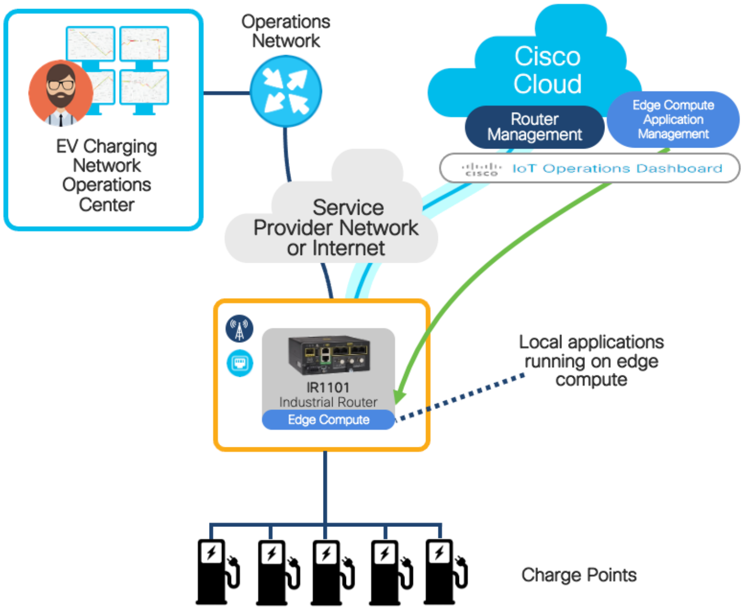
Edge compute supports a variety of applications, providing local computation and decision making at the curbside charging site. Much of Cisco's IoT portfolio is capable of supporting edge compute applications to reduce the need for additional hardware in an already space-constrained location.

Advantages of edge compute include the ability to run applications directly at the network edge for use cases such as power management or local processing of data.

Cisco building blocks: Edge compute

- 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 required.
- Centrally managed deployment and monitoring of applications to edge devices.

Figure 6. Edge compute for running local applications


EV Charging Network Operations Center
Operations Network
Cisco Cloud
Router Management
Edge Compute Application Management
cisco IoT Operations Dashboard
Service Provider Network or Internet
IR1101 Industrial Router
Edge Compute
Local applications running on edge compute
Charge Points

Deployment options

The following table shows the various charger types and the typical deployment scenarios.

Table 2. Charger types and deployment scenarios

	Level 1	Level 2 7 kW /22 kW	Level 3 DC fast charger 50 to 350 kW	Deployment scenarios
Domestic single charger	✓	✓		Uses domestic Wi-Fi or dedicated embedded cellular modem connection.
Private multiple chargers		✓		Multiple charger deployments for offices or multitenant buildings or smaller retail locations.
Public multiple chargers (e.g., curbside, mall, rest area, coffee shop, hotel, forecourt)		✓	✓	Public network operated by a charge point operator. Deployment sizes vary based on the location and charger type. One or two Level 3 chargers are common, and smaller Level 2 curbside deployments are also common (e.g., two or four chargers).
Fleet multiple chargers (office, depot, warehouse, etc.)		✓	✓	Multiple Level 2 chargers at a depot or enterprise location. Chargers connected via Ethernet or Wi-Fi with deployments common in larger groups. Large deployments of Level 2 chargers with some Level 3 fast chargers.

Deployment example 1: Multiple Level 2 AC chargers

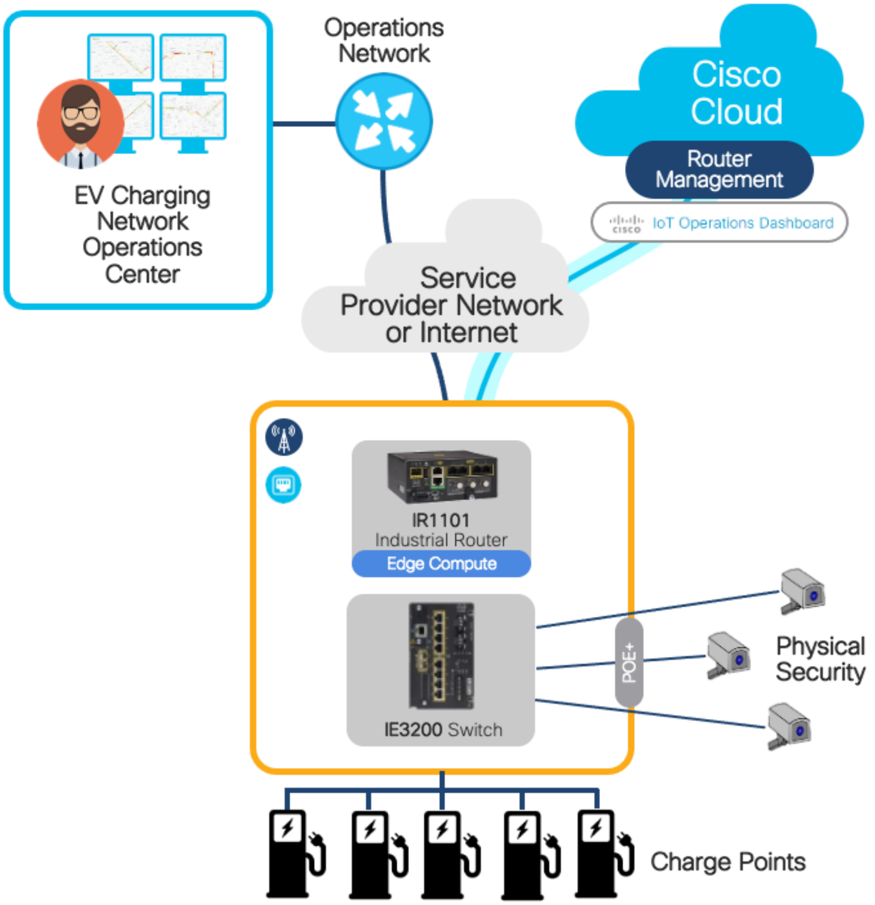
This configuration is typical for connecting multiple Level 2 chargers at either public charging locations or fleet/enterprise environments. Individual chargers can be connected to a single Cisco backhaul router or gateway via either fixed Ethernet cabling or Wi-Fi.

Backhaul is typically provided by a single cellular connection, with the option of using dual cellular (redundant or load sharing) or higher-bandwidth connections such as DSL or fiber.

Network architecture components

- Cisco Catalyst IR1101 ruggedized router or Cisco IoT Gateway
- Cisco Meraki® cameras for physical security
- Cisco Catalyst IE3200 Rugged Series switch for port fanout and Power over Ethernet (PoE) (where needed)
- Cisco IoT Operations Dashboard for centralized deployment and management

Figure 7. Deployment example 1: Multiple Level 2 AC chargers



- Centralized and automated provisioning of network elements
- Centralized and automated provisioning of security policy
- Highly reliable and redundant network connectivity
- Multilevel security for device data and management (Secure Boot, IPsec VPNs, 802.1X and MAB switch port security, Cisco Umbrella® to secure users and devices)
- Macro segmentation to isolate different services into dedicated, secure virtual networks (VLANs and VRF)
- Multiple edge compute options to enable local data processing
- Remote zero-touch deployment and ongoing operational management

Results

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

Deployment example 2: Fast Level 3 DC chargers

This configuration is typical for connecting multiple Level 3 chargers in standalone public charging locations. Individual chargers can be connected to a single Cisco backhaul router via the 4-port switch using fixed Ethernet cabling. Four chargers per router is possible without using a fanout switch.

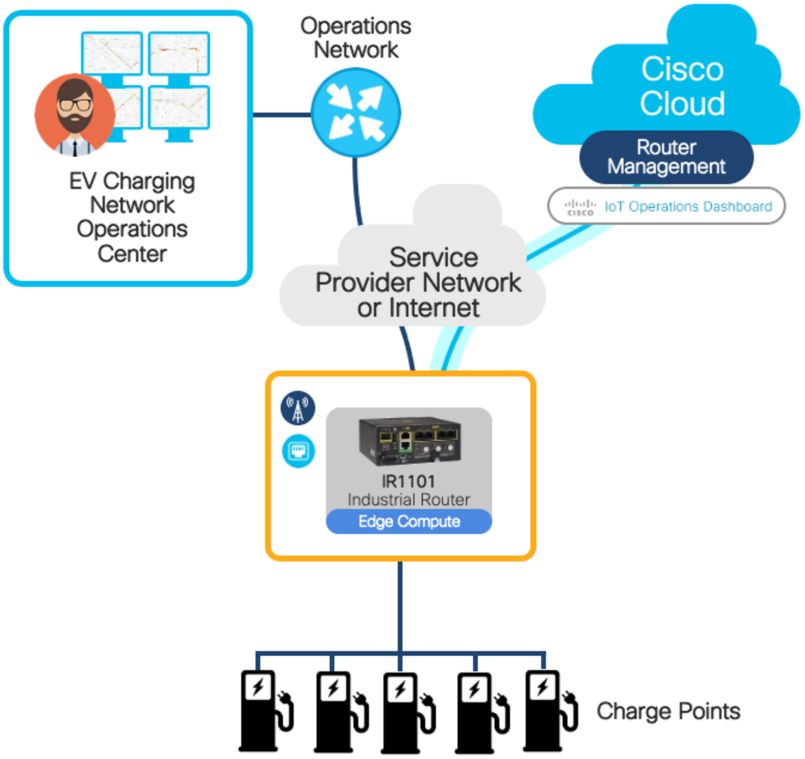
The compact size of the Cisco Catalyst IR1101 rugged router allows it to be mounted within the charge point enclosure.

Backhaul is typically provided by a single cellular connection, with the option of using dual cellular (redundant or load sharing) or higher bandwidth connections such as DSL or fiber.

Network architecture components

- Cisco Catalyst IR1101 ruggedized router
- Cisco IoT Operations Dashboard for centralized deployment and management

Figure 8. Deployment example 2: Fast Level 3 DC chargers



- Centralized and automated provisioning of network router
- Centralized and automated provisioning of security policy
- Highly reliable and redundant network connectivity
- Multilevel security for device data and management (Secure Boot, IPsec VPNs, 802.1X and MAB switch port security, Cisco Umbrella to secure users and devices)
- Macro segmentation to isolate different services into dedicated, secure virtual networks (VLANs and VRF)
- Multiple edge compute options to enable local data processing
- Remote zero-touch deployment and ongoing operational management

Results

- Simplified provisioning
- Simplified operations
- Multilevel security

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

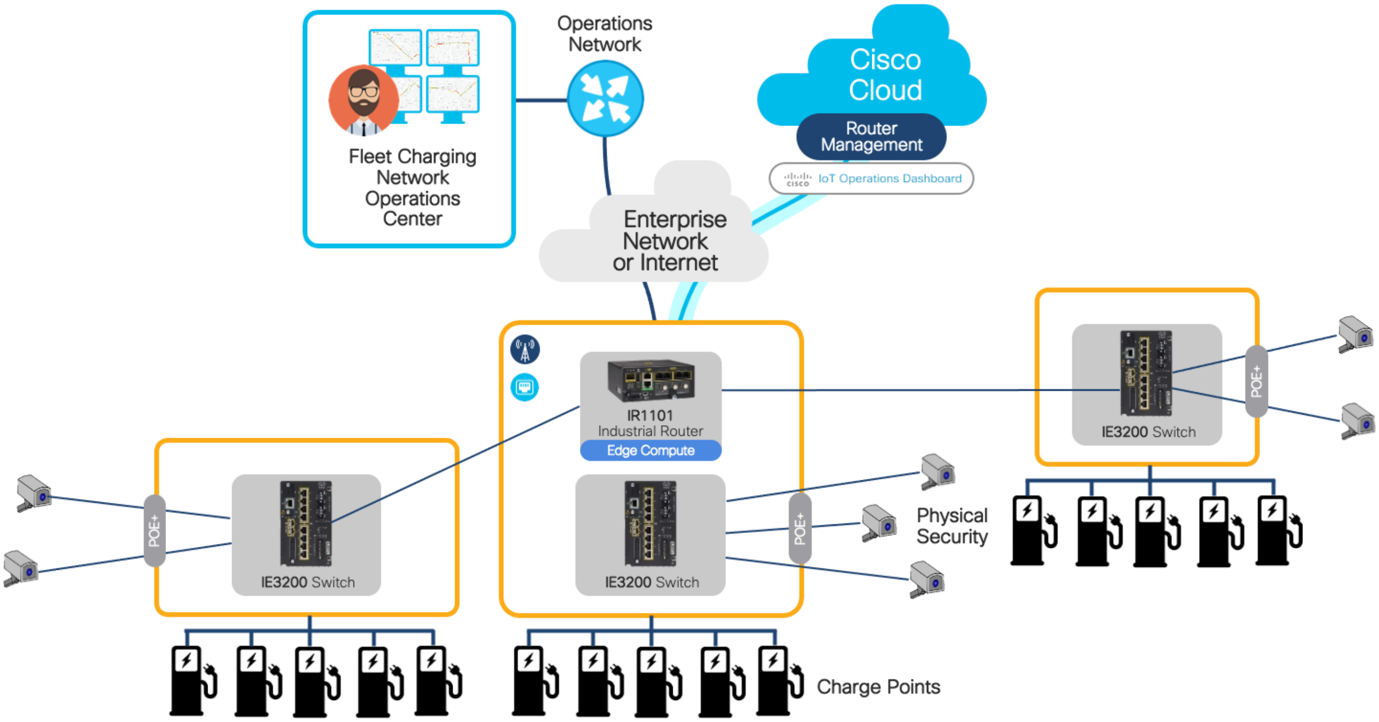
Deployment example 3: Fleet, office, or multitenant building

This configuration is typical for connecting multiple Level 2 chargers and a small number of Level 3 charge points in a typical standalone private fleet or office charging location spread over a wide area (such as multiple parking lots). Individual chargers can be connected to a Cisco switch, which then connects to a single backhaul router using fixed Ethernet fiber cabling. It is possible to have many chargers per router using multiple fanout switches.

The compact size of the Cisco Catalyst IR1101 router allows it to be mounted within the charge point enclosure.

Backhaul is typically provided by a single cellular connection, with the option of using dual cellular (redundant or load sharing) or higher bandwidth connections such as DSL or fiber.

Figure 9. Deployment example 3: Fleet charging network operations center



Results

- Simplified provisioning
- Simplified operations
- Multilevel security

- Macro segmentation
- Support for all connectivity options
- Support for all current and future use cases

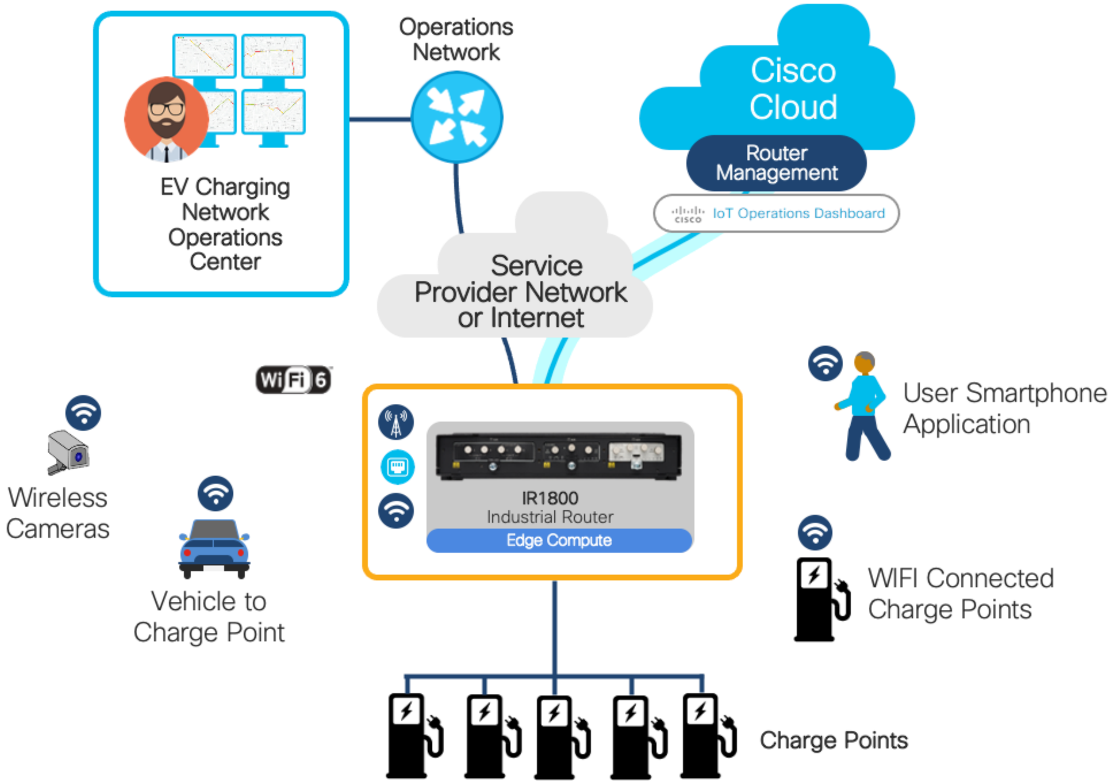
Deployment example 4: Inclusion of Wi-Fi

Wi-Fi can be added to any of the previous deployment options via external access points or via a Cisco Catalyst IR1800 Rugged Series Router with the Wi-Fi 6 module.

The Wi-Fi 6 module provides built-in wireless controller or standalone modes.

Backhaul is typically provided by a single cellular connection, with the option of using dual cellular (redundant or load sharing) or higher bandwidth connections such as DSL or fiber.

Figure 10. Deployment example 4: Inclusion of Wi-Fi



Conclusion

Robust and connected solutions on network infrastructure that is simple to manage and operate are becoming essential to support EV charging networks at scale. Cisco IoT platforms provide the capability to address different deployment options while maintaining a single provisoning and management application.

Cisco electric vehicle charging network benefits

- Pre-validated, proven multiservice network for all your present and future goals
- Ruggedized network for robust and effective movement of data
- Automated service segmentation to 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 IoT Operations Dashboard]

[Cisco Catalyst Rugged Routers]

[Cisco Catalyst Rugged Switches]

[Cisco Remote and Mobile Assets CVD]

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**.