

SD-WAN for Industrial Solutions

Introduction to SD-WAN for industrial solutions

Cisco® is a global leader in data and networking solutions and provides a wide range of products to connect your enterprise sites and equipment. As networking infrastructure continues to expand in our hyper-connected world, the capabilities that businesses must deploy to secure and manage their critical Industrial Internet of Things (IIoT) devices plays an ever-increasing role in the success of their organization. Networks are expanding outside traditional office buildings and into industrial fixed and mobile use cases, resulting in more devices being connected to the internet and data centers and increased security exposure. IIoT has moved traditional networking far beyond the carpeted spaces and into industries like fleets, oil and gas, energy and water utilities, and remote condition monitoring and control—basically anything that can establish a wide area connection. Moreover, these industrial networks are increasingly being considered critical infrastructure.

In response to this expansion, Cisco has ongoing innovations advancing the ways networks operate—and at the forefront of these trends is how SD-WAN enables and supports industrial solutions.

Cisco Validated Designs

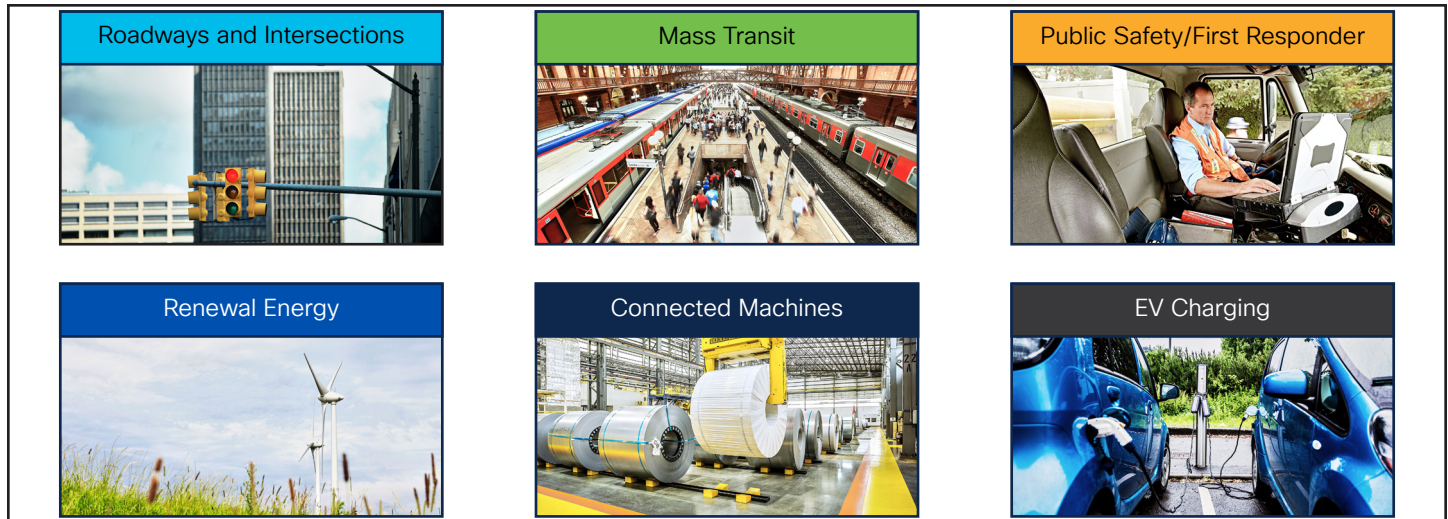
Since the inception of IP networking, Cisco Validated Designs (CVDs) have been used to validate, architect, and configure next-generation technologies. CVDs start with the vertical use cases and architect the flow from the edge device to the application, validating the key Cisco and third-party components along the way. Each aspect of the architecture is thoroughly tested and documented with sample configurations, helping to simplify integration through proven solutions.

Benefits

Manage and optimize your industrial fixed and mobile networks using SD-WAN:

- **Simplified management** using a common management tool for your Enterprise and Industrial devices
- **Multi-WAN support** for always-connected mobile use cases
- **Security** common policies are extended to the devices at your network edge
- **On-premise or cloud-hosted** architectural flexibility
- **Scalable** solution that allows thousands of assets to operate simultaneously, positioning the customer to meet future requirements

The goal is to ensure a deployment that's simple, faster, reliable, and cost effective.



This document provides an overview of Cisco's validated design to support extension of the SD-WAN fabric from the enterprise to the industrial spaces.

Benefits of SD-WAN

Cisco SD-WAN today is already an industry-leading wide area network solution. Cisco software-defined WAN enables enterprises and organizations to connect users to their applications securely. It provides a software overlay that runs over standard network transports, including Multiprotocol Label Switching (MPLS), broadband, and internet, to deliver applications and services. The overlay network supports on-premises solutions but also extends an organization's network to Infrastructure as a Service (IaaS) and multi-cloud environments, thereby accelerating the shift to the cloud.

Most industrial companies today are used to building large networks by utilizing technologies such as Internet Protocol Security (IPsec) and Dynamic Multipoint Virtual Private Network (DMVPN) to encrypt critical communications, MPLS for the underlying transport network, and public or private cellular for remote sites with no other WAN connectivity. Cisco SD-WAN brings these technologies together and enables automation to greatly simplify deployments.

Automation benefits

- Zero Touch deployment of field gateways (i.e., no field staff required to configure a gateway)
- Simple provisioning of service VPNs to segregate traffic (such as Supervisory Control and Data Acquisition [SCADA], Closed-Circuit Television [CCTV], Phasor Measurement Unit (PMU), IP Telephony, etc.)
- Templated configurations making it easy to change configuration and push it to gateways
- Application of unified security policies across a diverse range of remote sites and equipment
- Managing multiple backhaul connectivity options at the gateway, including private MPLS for critical SCADA traffic and cellular for backup, and even internet-based connections for non-critical traffic, where appropriate
- Lifecycle management of gateways (e.g., firmware updates, alarm monitoring, and statistics)

This virtualized network runs on the industry's most broadly deployed routing technology, from physical branch routers such as the Cisco Catalyst® 8000 Edge Platforms Family to virtual machines in the cloud such as the Cisco vEdge Cloud routers. Centralized controllers, which oversee the control plane of the Cisco SD-WAN fabric, efficiently manage provisioning, maintenance, and security for the entire Secure Extensible Network (SEN) overlay network.

Cisco vManage provides a highly visualized dashboard that simplifies network operations. It provides centralized configuration, management, operation, and monitoring across the entire SD-WAN fabric. Integration with Cisco Umbrella® accelerates the transition to a SASE architecture. Open programmability enables data extraction for enhanced visibility and actionable insights.

Cisco SD-WAN offers integrated security, including full-stack multilayer security capabilities on the premises and in the cloud. This integrated security provides real-time threat protection where and when it is needed—for branches connecting to multiple Software-as-a-Service (SaaS) or IaaS clouds, data centers, or the internet.

Cisco SD-WAN can be extended to any environment through its flexible architecture. Whether you deploy your product in the cloud or on-premises, Cisco SD-WAN automatically discovers, authenticates, and provisions both new and existing devices.

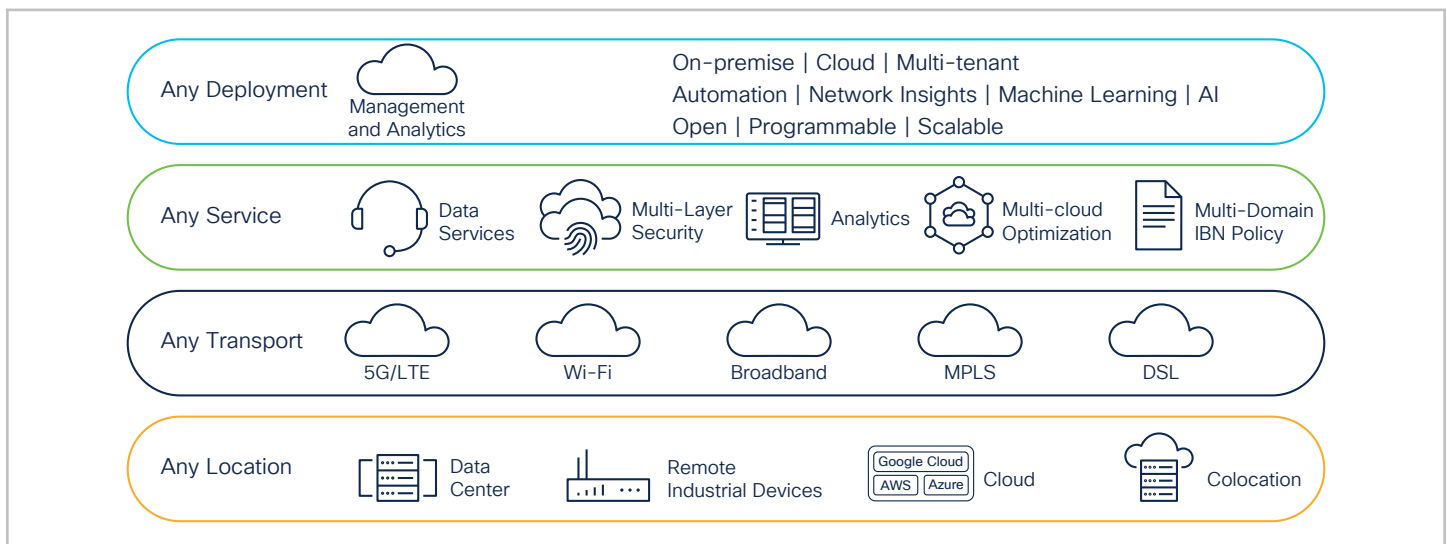


Figure 1. SD-WAN flexible architecture

Target audience

Although all stakeholders can benefit from this document, we have focused on:

- **SD-WAN users** who are expanding into industrial spaces
- **Technology buyers** responsible for selecting asset connectivity platforms
- **Industrial market leaders** evaluating connectivity

SD-WAN for industrial solutions introduces new requirements and challenges

SD-WAN has origins as an enterprise solution using fixed edge routers of various performance capabilities and predictable enterprise traffic patterns. New challenges are introduced with industrial use cases mandated by a set of industrial requirements including:

- Connectivity to legacy serial devices not supporting Ethernet/IP communications
- Mobility needs for mobile assets to ensure resilient wide area connectivity
- New WAN interfaces including dual cellular, DSL, broadband and Wi-Fi (as a WAN)
- Remote condition monitoring and control using remote sensors to collect and report critical data, and General Purpose I/O (GPIOs) to control remotely connected devices
- Vehicle interfacing for mobile use cases where the vehicle is itself a sensor

Why Cisco SD-WAN for industrial solutions

To support the unique requirements of industrial networks, the reach of Cisco SD-WAN has been expanded through a new class of devices—[Cisco Industrial Routers](#)—which provide the connectivity, mobility, and security required for critical infrastructure such as the electric grid, our streets and highways, and the fleets of transit, rail, and service vehicles that are part of many businesses.

The ability of Cisco SD-WAN to support industrial routers and the incremental capabilities they possess provides the on-ramp for industrial customers to rapidly connect, view, and monitor remote industrial devices along with Enterprise routers as a unified network under common management—see the figure below.

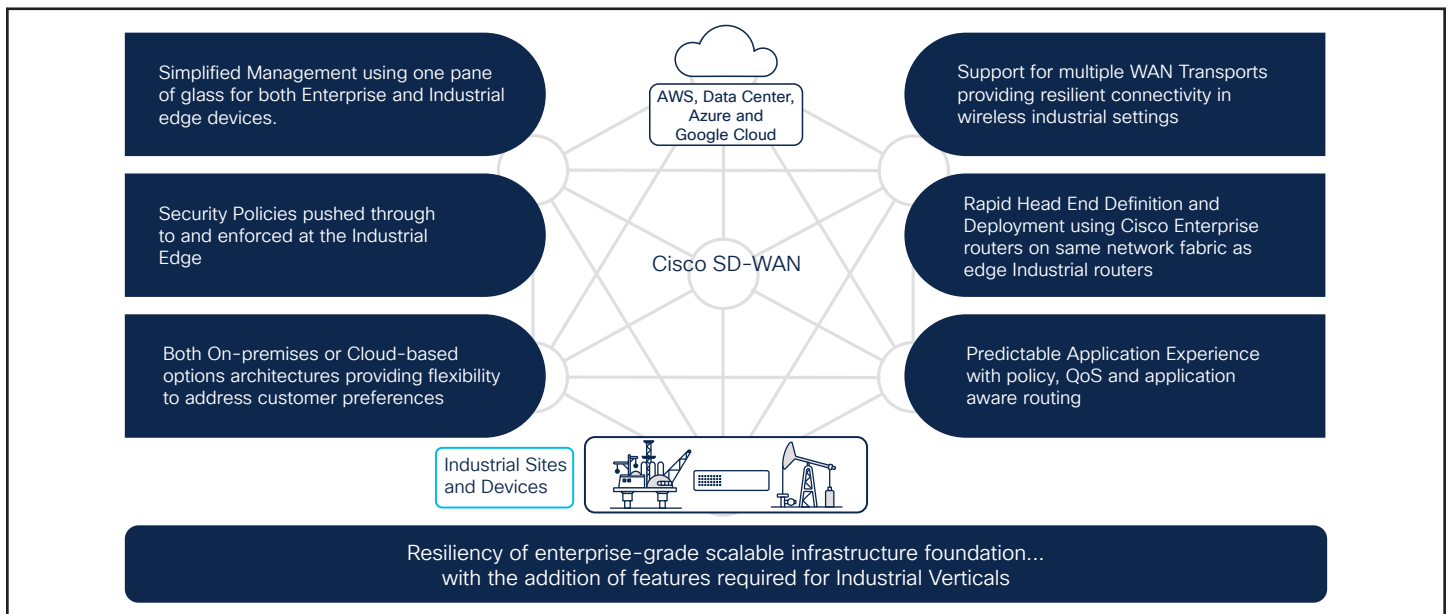


Figure 2. SD-WAN benefits

The additional multi-WAN support for mobile use cases and the capability for rapid headend deployment is available using Cisco Enterprise routers on the same network fabric as edge industrial routers. This greatly simplifies the data center creation and management and allows the system overall to be viewed as one network from edge routers to data center or cloud.

Industrial routers fill the gap for industrial needs

The Cisco industrial router portfolio was created to meet the hardened environment requirement of both fixed and mobile deployments. These routers provide industrial hardware/software features including serial communications for current and legacy devices, GPIO for remote conditioning monitoring and control, GPS location services, and vehicle interfaces for mobile deployments.

For both fixed and mobile industrial use cases, wireless WAN connectivity options are critical to providing the resiliency needed for always-connected critical remote locations and on-the-move mobile scenarios.

The WAN connectivity options supported by the Cisco Industrial Router portfolio includes:

- Ethernet—for general wired connectivity, where available
- 5G and LTE dual cellular modems (both public and private)—for resilient and flexible mobile connectivity
- Digital Subscriber Line (DSL)—for connecting to existing DSL lines deployed in cities
- Wireless private broadband networks (Cisco Ultra Reliable Wireless Backhaul)—for license-free broadband connectivity used to fill cellular coverage gaps or avoid service provider airtime costs
- Satellite links—for remote locations with no cellular or terrestrial networks

The figure below depicts the incremental features and WAN connectivity options provided by the industrial router family.

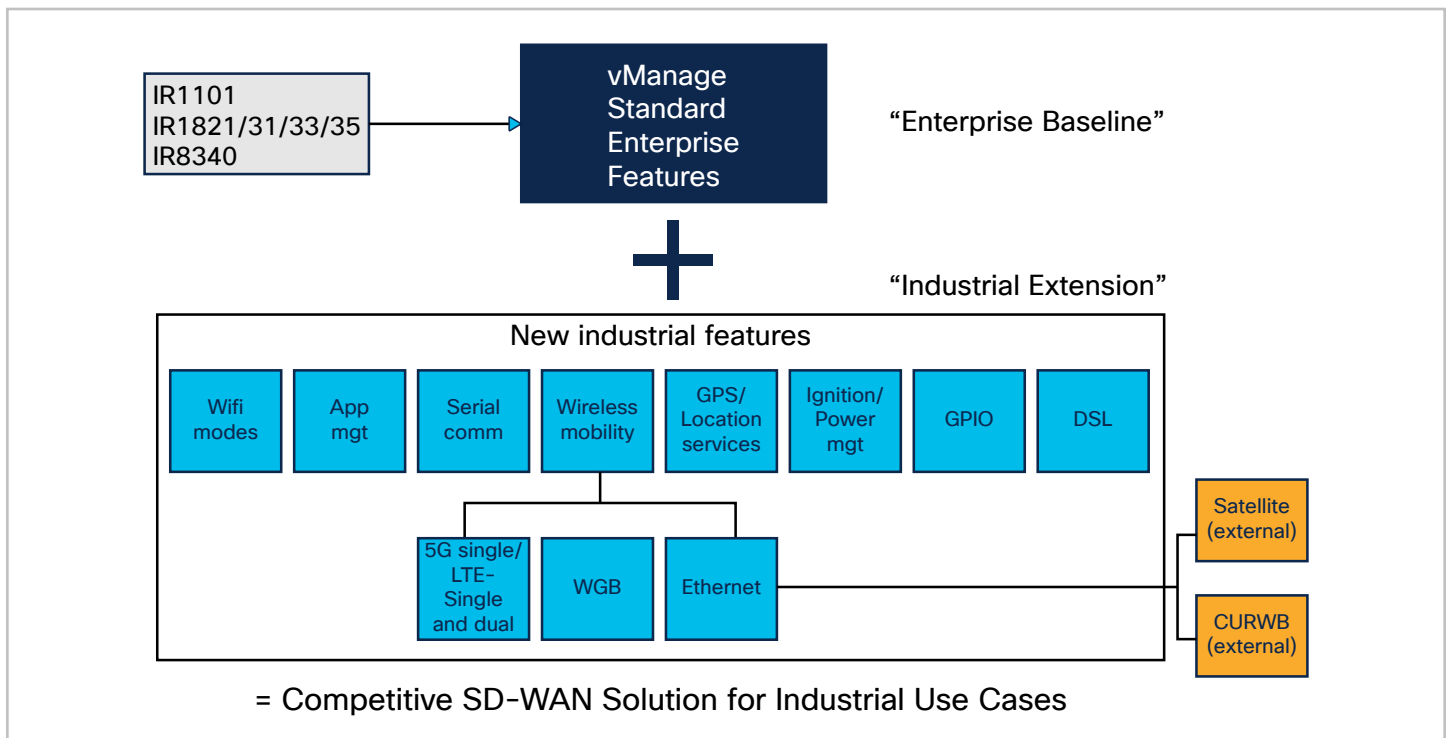


Figure 3. Industrial router family additional features and WAN connectivity options

The following figure further illustrates the application of incremental industrial router features in industrial applications.

Industrial router extension	Benefits and applicability
Wireless mobility 1	Dual 5G/LTE, WGB, CURWB roaming for transit
Ethernet extended WAN interfaces 2	Satellite, Broadband, DSL, Wifi for remote/mobile apps
Wi-Fi modes 3	Hot spot, remote office - fleet applications
DSL communications 4	Legacy wired interfaces for roadways and rail
Serial communications 5	SCADA, legacy devices - remote assets
GPS and location services 6	NMEA GPS data for location - based apps - fleet apps
Vehicle interfaces 7	Ignition Sense/Power Mgt - router power ctrl for fleets
General purpose I/O 8	Discrete sensors or external triggers - remote assets

Figure 4. Features and applications

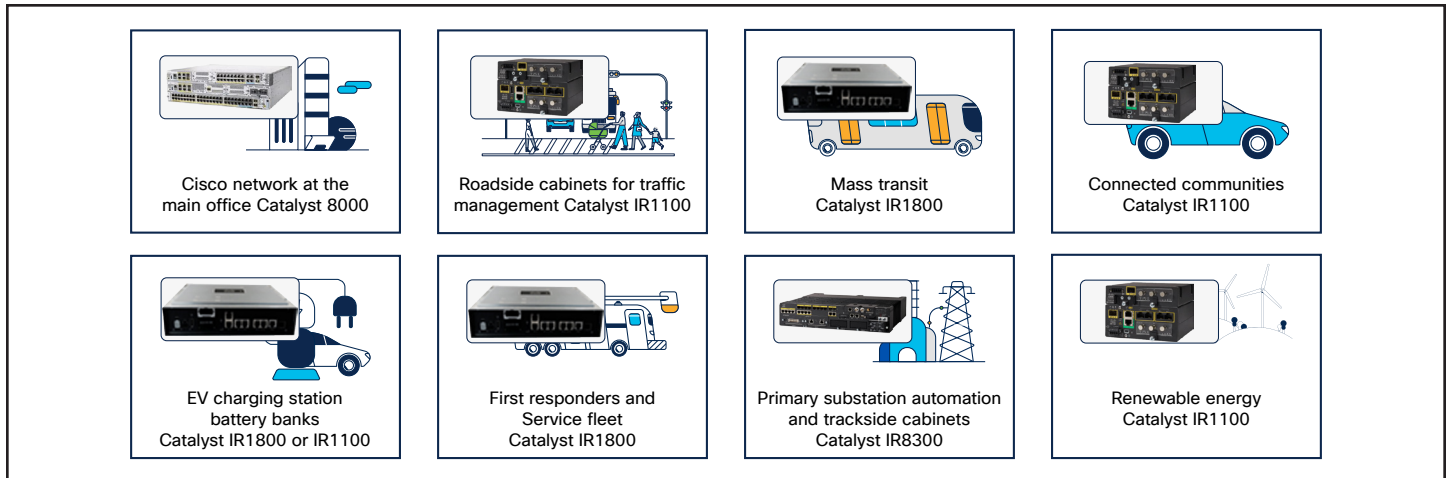


Figure 5. Industrial routers for any use case

Key markets where Cisco is a leader in industrial networking include remote condition monitoring and control, utility distribution automation, and fleets/transit. Each will be discussed briefly below and is covered more completely in the Cisco Validated Design.

Key vertical markets and use cases

Armed with the powerful combination of Cisco SD-WAN management provided by vManage along with environmentally hardened industrial and feature rich routers, most industrial use cases requirements can be supported. Refer to the figure that follows for some example industrial applications and applicable industrial routers.

Remote condition monitoring and control

Remote condition monitoring and control is an essential IoT capability whereby data is monitored from a connected device in a remote location to assess the condition of a system, and where outbound control to turn on/off/reset resources and trigger fail-safes may be required.

Key use cases

Some example use cases for remote condition monitoring and control are shown in the table below:

Table 1. Remote condition monitoring and control use cases

Use case	Related monitoring and/or control activity
Food Industry (incl food storage and transportation)	Monitoring freezer and cold room temperature and humidity
Remote Environmental Controls	Monitoring temperature, humidity brightness
Water Management	Monitoring water tank levels, lakes/reservoir levels, water flow through distribution pipelines
Video Surveillance	Monitoring CCTV cameras with video analytics to detect over/underfill conditions and physical security breaches
Distribution Pipelines (water, gas)	Monitoring for leaks and water/gas flow through pipelines
Waste Management	Monitoring wastewater levels and starting/stopping pumping stations
Flood Management	Detecting road conditions and control of closure gates for known low lying flood areas
Industrial Process control	Remote emergency power shut off and restoration
HVAC Systems	Monitoring of rooftop AC units for temperature, and vibration for preventative maintenance
General Equipment Monitoring	Monitoring of equipment temperature, vibration, tank levels

Remote Condition Monitoring and Control quite often require collecting data from sensors connected to remote edge routers and interpreting how a connected system or device is functioning using that data alone or in conjunction with other pieces of collected data.

A conceptual diagram is shown below depicting industrial routers in cabinets supporting monitoring of a distribution pipeline sensor and sharing readings to provide visibility to warnings and imminent dangerous conditions.

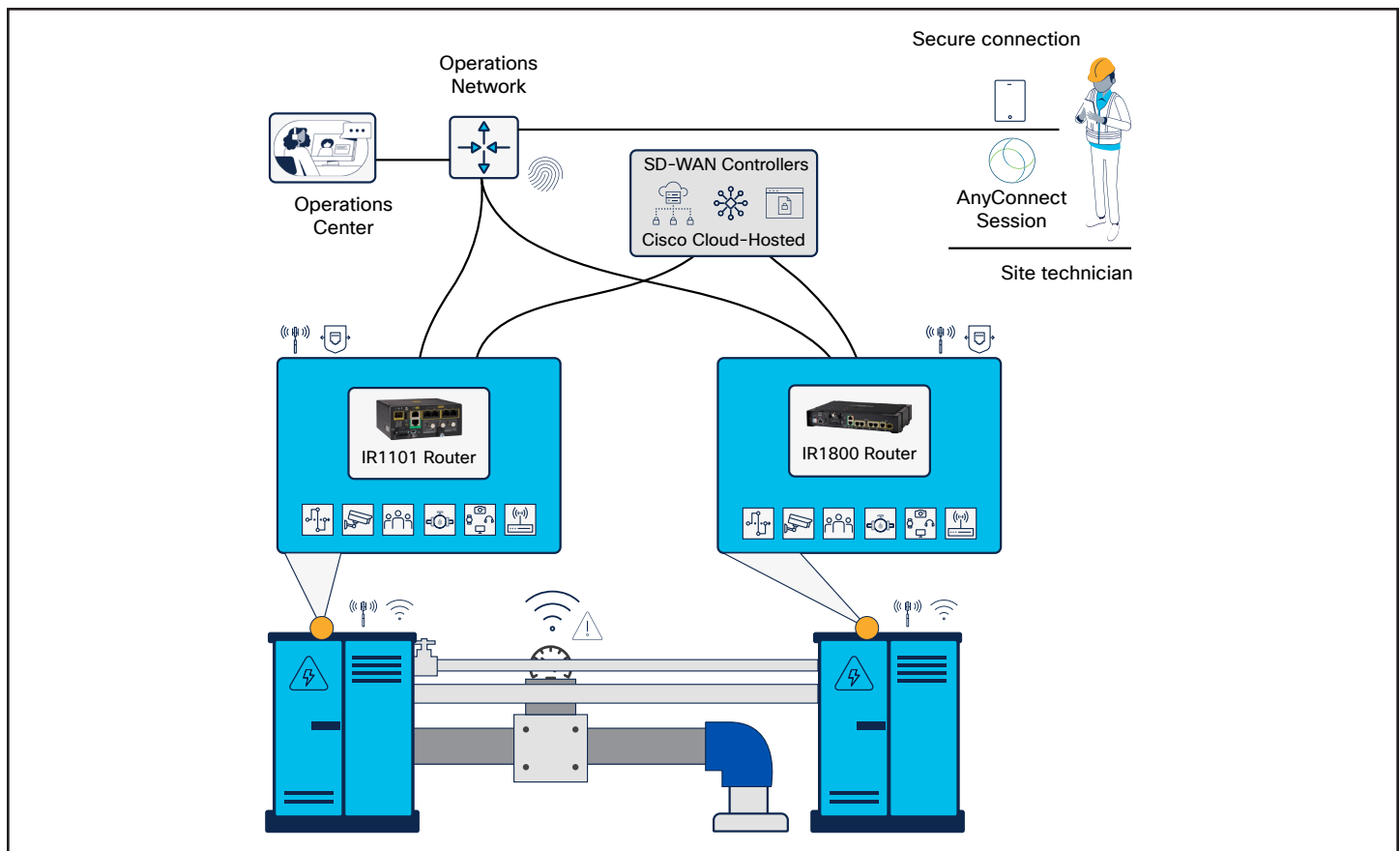


Figure 6. Remote condition monitoring architecture

Benefits

- Reliable LTE/5G or other WAN connectivity for continuous availability
- Predefined configuration templates for managing remote industrial routers
- Robust end-to-end security for business data and management
- Secure access to remote devices through the SD-WAN-managed operations network

SD-WAN is well suited to industrial deployments because it supports the needed reliable multi-WAN connectivity options, includes configuration templates for replication of consistent configurations across a large geography, and protects devices and connected sensors using end-to-end network security that extends to the edge routers.

Utility distribution automation

The goal of Distribution Automation in the Utility grid is real-time adjustment to changing load conditions, facilitating distributed generation, performing fault location identification and service restoration, and reacting to failure conditions within the Distribution grid, usually without operator intervention.

To enable such goals, multiple controller devices (referred to in this document as field devices) are deployed along the distribution feeder lines as well as at the substation premise. These controller devices can provide information to a Utility control center and also act upon control commands received from the control center. To enable this bidirectional communication between controller device and the control center, secure communication infrastructure is needed.

Key use cases

Key Distribution Automation use cases include:

Table 2. Distribution automation use cases

Use Case	
1	Advanced Metering Infrastructure (AMI) <ul style="list-style-type: none"> OPEX Reduction: Remote meter reading, Connect/Disconnect - Pre-payment, Demand Response Customer Service: Power Outage/Restoration reporting, customer portals for usage data
2	Distribution Automation (DA) - Grid Reliability Self Healing Feeder Network: <ul style="list-style-type: none"> Fault Location, Isolation and Service Restoration (FLISR)
3	Distribution Automation (DA) - Grid Efficiency <ul style="list-style-type: none"> Integrated Volt/Var Control (IVVC) Conservation Voltage Reduction (CVR)
4	Distribution Automation (DA) - Grid Visibility and Control <ul style="list-style-type: none"> Distribution - Supervisory Control and Data Acquisition (DSCADA) Remote Asset Monitoring
5	Remote Workforce Management - Secure Access from the Field to <ul style="list-style-type: none"> FAN Network Devices Remote Experts and Applications (Fixed and Mobile Hotspots)

DA
Use
Case

Please refer to the “Distribution Automation Use Cases” section of the [Distribution Automation -Secondary Substation Design Guide](#) for more details.

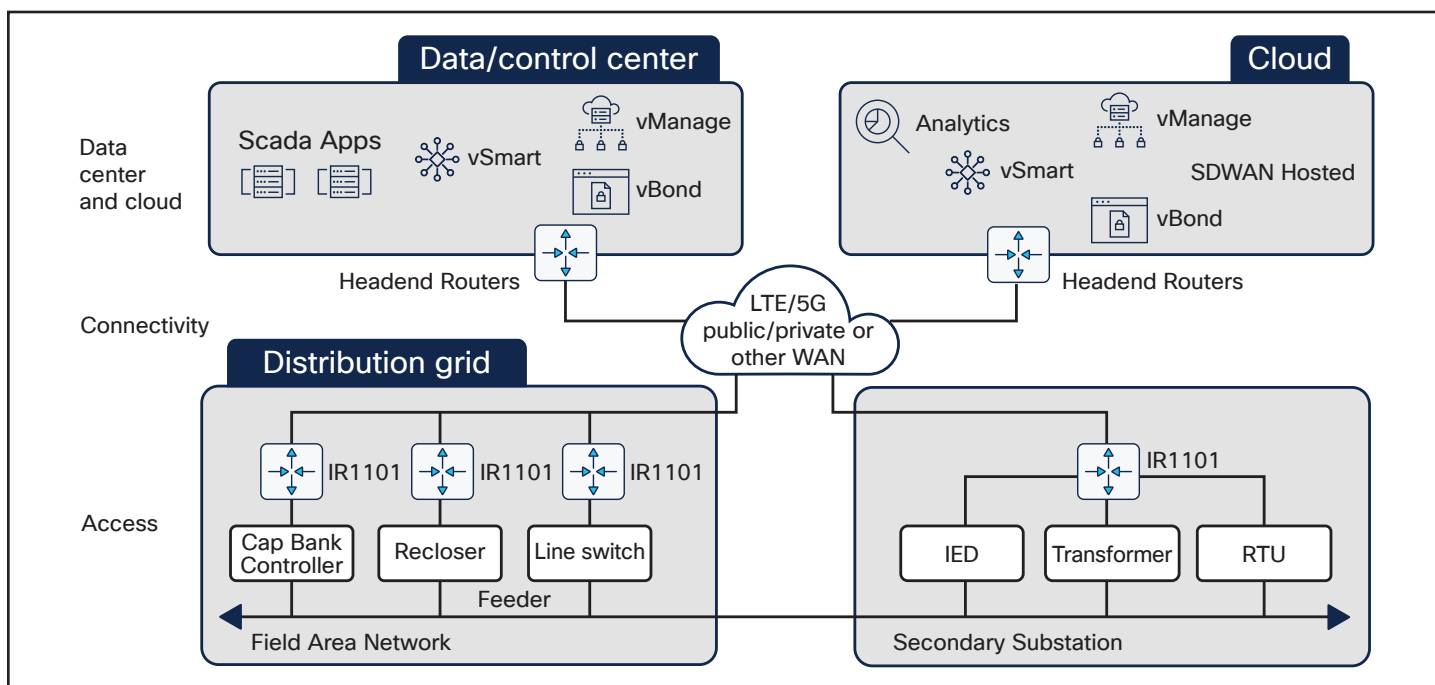


Figure 7. Distribution automation architecture

A high-level view of the Distribution Automation solution architecture is shown below for both cloud and on-premises SD-WAN deployments.

Distribution Automation leverages cellular connectivity (public or private) for LTE/5G, or utility-owned backhaul for WAN connectivity. Serial communication ports on the router communicate bidirectionally using serial-based SCADA communication protocols to Remote Terminal Units (RTU), Intelligent Electronic Devices (IED), and other sensors. Communication of data is to the SCADA system and additional application sensor monitoring applications in the operations center where the SD-WAN controllers also reside.

Benefits

- Reliable LTE/5G communications over public or private networks
- Predefined configuration templates for managing remote industrial routers
- Robust end-to-end security for business data and management
- Serial to IP conversion for interfacing with SCADA devices and controller
- Rapid head-end integration within SD-WAN fabric

Fleet and Transit

Fleet applications range broadly from public bus and light rail transit to service fleets to public safety fleets (police, fire, ambulance) and trucking fleets. Solutions require nearly all of the capability of the industrial router including GPS location services, geofencing, multiple WAN options with failovers, Wi-Fi hot spot, integration with the vehicle-as-a-sensor and connection to IP/Ethernet devices for passenger counting, fare payment, security, route updates, and passenger information signs.

Key use cases

Key Fleet and Transit Use Cases and Devices are shown in the table below:

Table 3. Fleet/Transit use cases

Operational processes	Types of use cases supported	Device and applications
Business operations	Route planning and optimization <ul style="list-style-type: none"> • Scheduling 	<ul style="list-style-type: none"> • Automatic Vehicle Location (AVL) • Dashboard
	Passenger information and management <ul style="list-style-type: none"> • Passenger Wi-Fi, advertisement • Automatic voice announcement • Fare collection • Security cameras 	<ul style="list-style-type: none"> • Displays and head signs • Text-to-speech engine • Speaker • Fare collection equipment • Safety and enforcement
	Asset utilization <ul style="list-style-type: none"> • Automatic passenger counting, driver management • Scheduled maintenance 	<ul style="list-style-type: none"> • 3D sensors • Automatic Passenger Counter (APC)
Fleet and operational management	Fleet Tracking <ul style="list-style-type: none"> • Dispatch, location, schedule adherence, safety, route compliance, vehicle predictions, vehicle headway adherence, service adjustments, rider alerts 	<ul style="list-style-type: none"> • AVL • Dashboard • Communications equipment
	Connectivity Statistics <ul style="list-style-type: none"> • Cellular, GPS, Wi-Fi 	<ul style="list-style-type: none"> • Cellular gateway • Cloud management

Operational processes	Types of use cases supported	Device and applications
Vehicle operations	Telematics <ul style="list-style-type: none"> Fuel monitoring, engine diagnostics, predictive maintenance 	<ul style="list-style-type: none"> OBD-II device CANBUS
	<ul style="list-style-type: none"> Upgrades and refreshers Vehicle ID/gateway ID alignment Hardware/firmware updates 	<ul style="list-style-type: none"> Cloud management Cisco ISE
	<ul style="list-style-type: none"> Security VPN, access control, secure boot 	<ul style="list-style-type: none"> Firewall Cisco IOS-XE configurations

A conceptual diagram is shown below depicting industrial routers in a bus or light rail deployment that represents the most comprehensive fleet configuration.

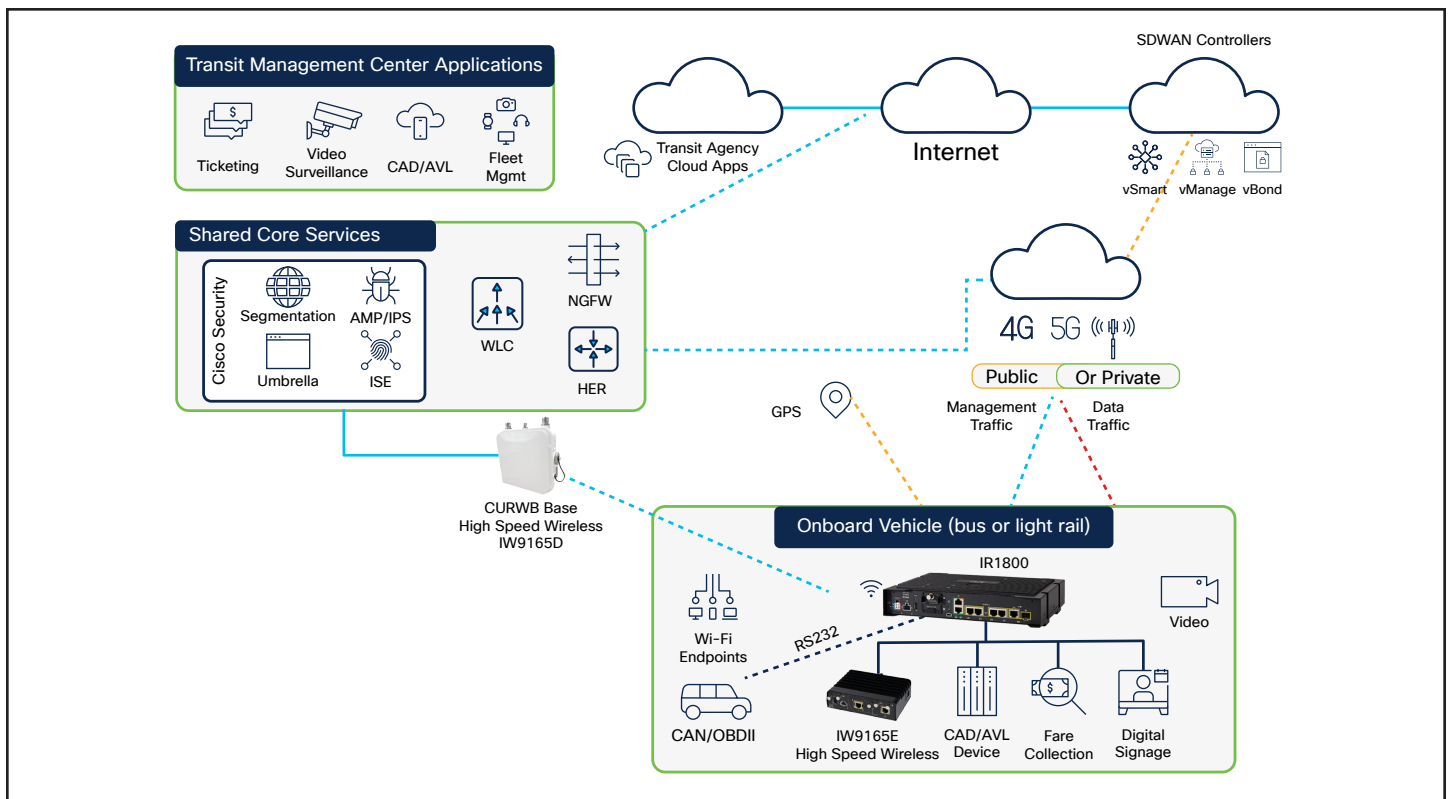


Figure 8. Transit system architecture

Fleet solutions leverage the ability of SD-WAN for any combination of transport services with configurable, dynamic routing policies to ensure that traffic is flowing over the correct primary, secondary, or tertiary wide area connections as the vehicles in motion experience RF signal fades and dropouts.

For any fleet application, location tracking is paramount. SD-WAN captures initial location as well as location updates, which allows vManage to render the vehicle location on a map and apply geofencing rules to alert if a vehicle has gone outside of defined boundaries.

Vehicle integration to monitor the ignition switch and battery levels exist in the Cisco IR1800 Rugged Series Routers to provide alerting and controlled or delayed shutdowns when a fleet vehicle is turned off.

Lastly, Wi-Fi hot spot operation for transit agencies is important for passenger internet access to improve the passenger experience while keeping this traffic segmented from other transit agency traffic and ensuring that enough bandwidth is reserved through QoS policies for agency traffic.

Benefits

- Multiple WAN transports connectivity for continuous availability
- Predefined configuration templates for managing remote industrial routers
- Secure segmentation of transit vehicle services
- Support for vehicle integration and passenger Wi-Fi
- Rapid head-end integration within SD-WAN fabric

Conclusion: SD-WAN + industrial routers

Industrial markets deploy IoT devices that are often considered mission-critical, which means the ability to stay connected for visibility while securely extending security policies into the industrial spaces is essential. Cisco SD-WAN provides solutions for common challenges for industrial spaces by supporting multiple transports with configurable dynamic routing policies while leveraging the same security features and management tools for both the enterprise and industrial network extensions. SD-WAN enables encryption and segmentation of data from industrial devices to be applied so that the right personas or applications with the right credentials are able to access critical information at the right time.

With the introduction of industrial routers, a new set of functionality has been introduced that captures the unique requirements of industrial markets greatly extending the reach of SD-WAN networks and easing the costs of deployment into industrial spaces. With SD-WAN embracing those new industrial router capabilities, Cisco is able to bring the richness of SD-WAN to industrial markets and applications.



Cisco SD-WAN benefits for industrial markets

- **Simplified management** using a common management tool for your Enterprise and Industrial devices
- **Multi-WAN support** for always-connected mobile use cases
- **Rapid head-end deployment** within the SD-WAN network fabric
- Common **Security** policies are extended to the devices at your network edge
- **On-premise or cloud-hosted** architectural flexibility
- **Scalable** solution that allow thousands of assets to operate simultaneously, positioning the customer to meet future requirements

Resources

- [Cisco SD-WAN](#)
- [Cisco SD-WAN For Industrial Markets](#)
- [Cisco Industrial Routers](#)
- [Cisco Catalyst IR1100 Rugged Series Router Data Sheet](#)
- [Cisco Catalyst IR1800 Rugged Series Routers Data Sheet](#)
- [Cisco Catalyst IR8300 Rugged Series Router Data Sheet](#)
- [Cisco Ultra Reliable Wireless Backhaul](#)