The bridge to possible

Cisco Connected Rail

Transforming passenger experiences and rail operations with secure, reliable connectivity

Rail operators must ensure the safety of workers, passengers, and the public while at the same time keeping trains running on time, providing superior service, and minimizing operational costs. To achieve these business objectives, rail equipment and infrastructure owners can take advantage of increasingly advanced technology to address safety concerns, improve asset visibility, offer new value-added services, increase ridership, and reduce operating expenses. Freight rail carriers can use remote control, automation, and new Internet of Things (IoT) data to keep workers safe, streamline operations, and minimize freight cost per mile, so they remain competitive with other modes of overland freight transportation. Passenger rail providers can offer services such as high-speed internet access, infotainment, mobile ticketing, and security systems on trains and in stations to enhance the passenger experience and increase ridership. And of course, critical signaling and control systems such as ERTMS, CBTC, and PTC are needed for safe operation. All of these capabilities can be key to business success for rail operations, and they all depend on a foundation of network capability that is secure, scalable, reliable, and resilient, and that satisfies an ever-increasing demand for data throughput. Cisco's networking products and solutions provide the necessary foundation for securely solving these networking challenges. Cisco's Industrial IoT products are proven to meet the unique demands of operating in a rail environment, and the Cisco® Connected Rail solution provides a Cisco Validated Design for reliably interconnecting high-speed trains, trackside infrastructure, stations, and operations centers across all the rail operator's sites and regions.

Benefits

A network foundation for improving the safety, efficiency, and service levels of your rail operations

- Train-to-ground wireless with an unprecedented combination of bandwidth and low latency
- In-station and onboard Wi-Fi that raises the bar for passenger services and experience
- Network segmentation to securely deliver multiple services (vital and nonvital) over the same infrastructure – lowering risk and reducing cost
- Automated network configuration and security with Cisco intent-based networking, so you can easily get the network to do what you want
- Flexibility for modern or legacy backhaul

The bridge to possible

The Cisco Connected Rail solution validates the architecture for high-speed, robust wireless connectivity between train and trackside as well as resillient, scalable access and backhaul transport infrastructure to interconnect wayside, stations, and operations centers across the rail operator's regions. As listed in Table 1, rail operators and Cisco solution partners use Connected Rail as a secure foundation on which to build their solutions to support use cases including passenger Wi-Fi, infotainment, video surveillance and analytics, operations management, maintenance, signaling, and control.

Table 1. Cisco Connected Rail customer use cases and business outcomes

Use case category	Definition	Business outcomes
Safety and compliance	▪ Connectivity for train control systems such as Communication-Based Train Control (CBTC), European Railway Traffic Management System (ERTMS), and Positive Train Control (PTC) ▪ Video surveillance for passenger safety at stations and onboard trains ▪ Faster emergency response time ▪ Real-time remote asset monitoring	▪ Improved passenger safety and security ▪ Improved situational awareness ▪ Reduced risk and more auditable compliance ▪ Optimized passenger operation ▪ Improved customer experience
Passenger experience	▪ Fast and reliable passenger Wi-Fi ▪ On-demand and bandwidth-efficient infotainment services ▪ Passenger interactive kiosks and wayfinding ▪ Real-time Estimated Time of Arrival (ETA)	▪ Increased ridership ▪ Improved customer service ▪ Revenue generation and new business models
Operational efficiency	▪ Fully resilient trackside infrastructure to support signaling and control applications ▪ High-speed train-to-ground wireless infrastructure to support service delivery even when a train moves at high speed ▪ Predictive maintenance and remote condition monitoring enabled through sensor data collection and correlation ▪ High-definition IP video surveillance for live monitoring of activity on trains, in stations, and at trackside ▪ Improved train headway and increased track utilization ▪ Support for better voice communication between train operators and passengers (VoIP)	▪ Higher utilization of track infrastructure ▪ Lowered OpEx and reduced CapEx ▪ Simplified maintenance ▪ Enhanced operational efficiency
Data management	▪ Reliable passenger Wi-Fi with seamless roaming between onboard and station locations ▪ User data management and targeted advertisements ▪ Ability to link current mode of transit to additional modes for seamless experience ▪ Video analytics for passenger counting and behavior monitoring	▪ Improved passenger experience ▪ Increased ridership ▪ Better customer service ▪ New revenue resource

Network challenges

When rail operators deploy a network foundation for their operations, they typically have to address a range of challenges. These include finding a solution for high-speed wireless connectivity to trains, establishing network services with sufficient features and reliability, ensuring cybersecurity, finding a graceful migration path from legacy to future technology, and complying with rail industry standards.

High-speed and comprehensive wireless connectivity

Finding a cost-effective high-performance solution for wirelessly connecting trains is no trivial task. In order to provide for multiple types of application traffic, such as passenger services, video surveillance, telemetry, and control signaling, the wireless offboarding solution must support high data throughput, high-speed train mobility, full coverage of long sections of track, handoffs without data loss as a train moves along the track, and tightly controlled data latency.

Reliable network services

Rail operators want a unified network so they can provide users with a consistent experience and reduce the number of different technologies and skillsets that staff must maintain, but user groups and applications may have differing needs. Deploying a separate physical network for every application and each group of users would be impractical. For these reasons, it is important to be able to logically and virtually segment the physical network to give each class of users and applications the right network policies for access, security, priority, resilliency, and other services, while providing full physical and logical resiliency.

Network infrastructure for rail operations is highly distributed among many locations, including rail cars and locomotives, maintenance vehicles, wayside, yards, terminals, and stations. A backhaul network is needed to connect all the locations, sites, and operations centers throughout a rail operator's geographic region. Such a backhaul network needs to form a single network that supports a variety of access types and provides a variety of services so that it can all be connected in a unified manner. It needs proven end-to-end security, high reliability, high bandwidth, and scalability to many geographically distributed locations. Managing all the network policies and assuring that they are properly implemented can be overly burdensome if done manually for each network node, so good tools for automating management, orchestration, and policy are needed.

Cybersecurity

Cybersecurity attacks on rail systems can disrupt the flow of goods on freight lines, completely stop train operations, and degrade passenger services, disappointing the customers that rail operators are seeking to delight. Attacks on vital rail systems can cause shutdowns or, even worse, harm to human safety. Given the digitization of operations that rail providers must achieve in order to remain viable and competitive, the need for strong cybersecurity is only increasing. Experience has shown that a strategy of trying to simply "air-gap" and isolate operational networks does not prevent attacks. A comprehensive, systematic, coordinated approach is needed, with consideration for issues such as ensuring that only authorized users and devices are connecting to the network, users and systems are able to access only data and services for which they are authorized, users are not connecting to malicious sites, malware is not brought into systems, and only legitimate traffic is transiting the network. Robust tools are needed to manage profiles and policies at scale and monitor that users and devices on the network comply with those policies, and all this must be done in a way that enables a quick response to new threats and intrusions as they emerge.

Graceful migration

Rail businesses can benefit from the cost savings, reliability, security, and features of an advanced IP, packet-switched network, but they often have an investment in legacy Time-Division Multiplexing (TDM) and circuit-switched systems that they aren't yet ready to replace. A network solution, therefore, needs to provide a graceful migration path that allows legacy transport circuits to be used along with newer IP network services and software-defined networking automation tools so that the system can be migrated at the pace appropriate for the business.

Rail industry compliance

Equipment installed onboard trains and on the trackside must meet industry standards set out for protection against temperature variations, vibration, ingress of metallic dust and other particles, moisture, fire, electrical surges, and other challenges associated with rail operations. Equipment that doesn't meet the required specifications can result in costly system disruptions and repairs, shortened equipment lifespans, lost revenue with assets being taken out of service, lapses in passenger services, and even liability and fines.

Why Cisco?

Cisco's Intent-Based Networking (IBN) technology transforms hardware-centric, manually configured networks into controller-led networks that capture network managers' business intent and use automation to translate intent into policies that are applied consistently across the network and monitored comprehensively to assure proper ongoing operation at scale. Some of the world's largest and most vital networks have embraced Cisco IBN because it brings new levels of network performance, security, and reliability to the network at larger scale and with less effort. Cisco's Connected Rail solution combines those industry-leading IBN capabilities with the specific and distinct needs of networks used for rail operations.

Cisco Validated Designs (CVDs) provide design and implementation guides for critical portions of the rail architecture in order to validate performance characteristics needed for rail operations, such as throughput, reliable packet delivery, low latency, security, resilliency, and high availability. The validated architecture covers multiple locations involved in rail operation, including operations centers, stations, trackside, and train-to-ground wireless communications.

Cisco's rail architecture features Cisco's unique Ultra-Reliable Wireless Backhaul (formerly Fluidmesh) technology for industry-leading wireless train-to-ground communication. The Connected Rail solution gives rail operators a future-ready network, with options to implement new networking capabilities such as Cisco Software-Defined Access (SD-Access) right away or to add them in the future. The architecture takes advantage of Cisco's proven, service-provider-grade Multiprotocol Label Switching (MPLS) technology to provide a reliable backhaul connection that can scale to connect all rail sites and operational centers. The Unified MPLS backhaul provides the necessary network services, such as Layer 3 VPN and circuit emulation, so that a variety of access network types can be transported – including legacy TDM and circuit-switched technologies often found in older rail infrastructure. And the Connected Rail architecture uses Cisco's ruggedized and rail-qualified Industrial IoT products to provide network access for a wide range of devices found in rail operations.

Network security should be included from day one and not as an afterthought. An effective cybersecurity strategy requires a comprehensive, systematic, coordinated approach to protect against a broad and continuously evolving set of threats. Cisco offers an ever-expanding, industry-leading portfolio of cybersecurity products to provide comprehensive protection for IT and operations networks. Cisco's portfolio includes capabilities to gain visibility into industrial devices and data traffic flows; products that use artificial intelligence to monitor data flows and detect traffic anomalies that can be used to enhance network segmentation policies; a policy platform called Cisco Identity Services Engine (ISE) that helps define and manage user profiles and access policies at scale; Advanced Malware Protection (AMP) to provide up-to-date monitoring and detection of malware threats; Cisco Umbrella® to protect against passengers or workers accessing malicious network domains; and Cisco DNA Center and SD-Access to automate and simplify security policy implementation and assurance across all network devices. Additionally, Cisco SecureX™ provides a consolidated view for simplified management of the overall security approach.

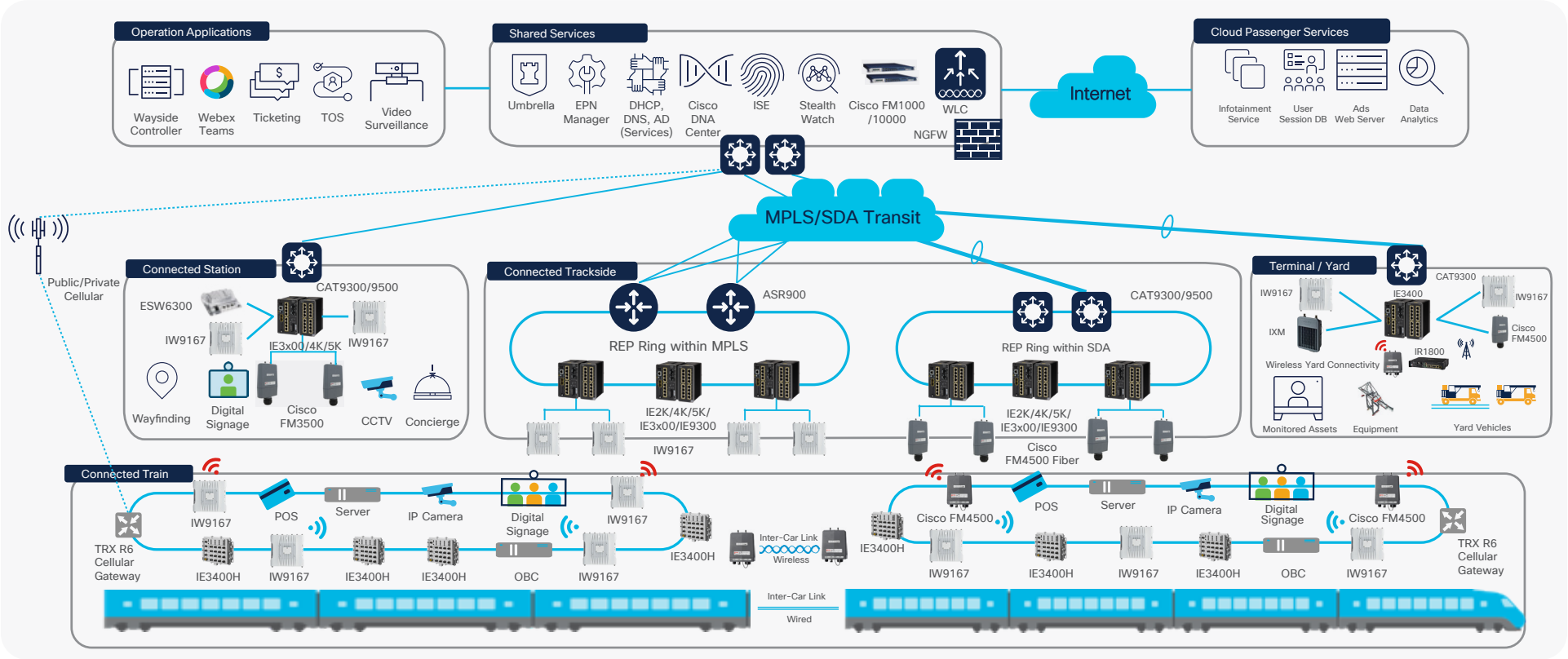
This solution brief provides a high-level overview of how to apply Cisco networking to rail operations. More detailed information about designing infrastructure for rail operations can be found in the Cisco Connected Communities Infrastructure (CCI) Solution Design Guide. With Cisco's Connected Rail solution, rail operators can lower their total cost of ownership, reduce deployment costs, manage risk, and deliver secure, high-performance networking with features that transform rail operations.

The bridge to possible

Connected Rail network architecture

As part of the overall Connected Rail reference architecture depicted in Figure 1, the Cisco Validated Design focuses on providing high-speed, robust wireless connectivity between train and trackside as well as resillient, scalable broadband networking infrastructure to interconnect wayside, stations, and operations centers across the rail operator's regions. Rail operators and Cisco solution partners use the Cisco Validated Design as a secure foundation on which to build their solutions for passenger services, video surveillance and analytics, operations, maintenance, and signaling and control. The figure depicts the overall scope of a rail network architecture in which Cisco products and validated designs apply and partner solutions are available.

Figure 1. Connected Rail reference architecture

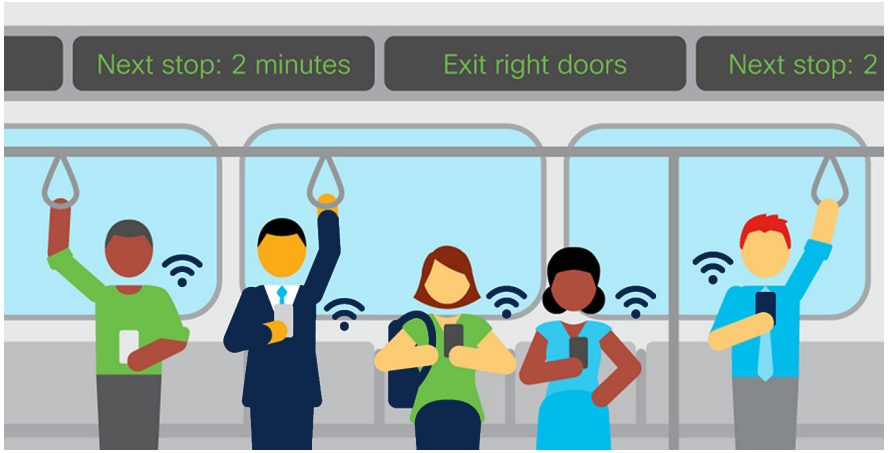


Connected Train

Cisco's Connected Train solution provides a multiservice network foundation, converging the capabilities from multiple proprietary networks in train cars onto a common IP network. The solution provides a resilient infrastructure capable of supporting numerous services and use cases.

The bridge to possible

The Cisco Connected Train onboard network is built on Cisco Catalyst IE3400 next-generation heavy duty and Cisco Industrial Ethernet 2000 series, IP67 rail-standards-compliant, small-form-factor Power over Ethernet (PoE) switches. Cisco Catalyst IW9167E Access Point provides reliable wireless connectivity for mission-critical application in a state-of-the art platform. It can operate as Wi-Fi 6 or Cisco Ultra-Reliable Wireless Backhaul (CURWB). This radio provides Wi-Fi connectivity to rail personnel and passengers within the train when it operates under Wi-Fi mode. The onboard network provides connectivity to Cisco IW9167E (CURWB) or Cisco FM4500 wireless radio that delivers fiber like train-to-ground communication for both vital and non-vital applications. As complimentary technology to Cisco wireless backhaul, a railway compliant onboard gateway equipped with multiple modems delivers a cellular based train-to-ground wireless technology for non-mission critical applications. This gateway often has compute and storage capabilities that brings additional value added services such as video surveillance and infotainment. It also enables other Cisco virtualized technologies to be integrated onboard including Cisco 5921 Embedded Service Router (ESR), Cisco Cloud Service Router (CSR) 1000v, Cisco virtual Wireless LAN Controller (vWLC), and Cisco Adaptive Security Virtual Appliance (ASAv). This cellular gateway and technology integration are delivered through Cisco connected rail solution partner's product like TRX R6 from Klas Telecom.



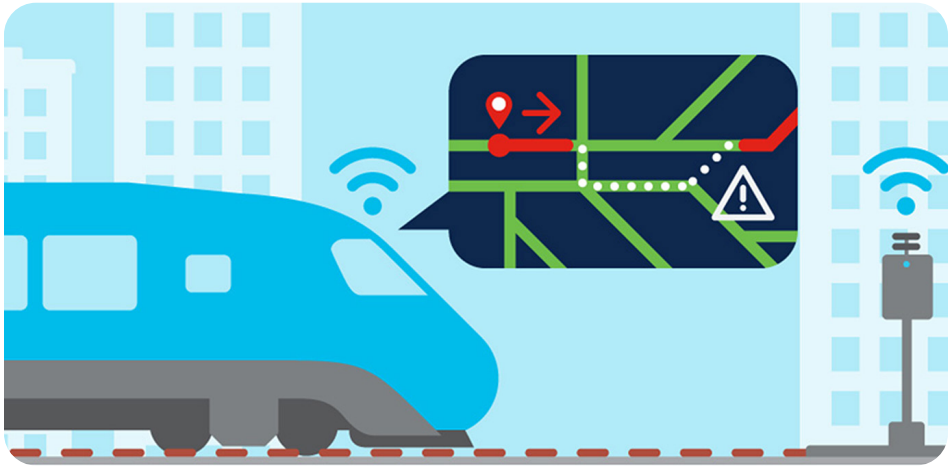
Connected Trackside

The Cisco Connected Trackside solution connects wayside controllers, I/O, and devices and provides backhaul from all rail sites to operations control centers. It provides a foundation on which Cisco customers and partners can develop end-to-end solutions for operational needs such as signaling, control, electrification, voice communication, video, and bulk data transfer. Connected Trackside uses a tiered architecture that is composed of an access layer with ruggedized IP switching infrastructure, a highly redundant and reliable backhaul transport layer, and a data center connectivity layer. The Connected Trackside infrastructure provides resilient communication paths between Connected Train, Connected Trackside, Connected Stations, and the operations control centers.

For the trackside access layer, Cisco IW9167E (CURWB), Cisco FM3500 Endo, or FM4500 Fiber trackside radio connects to the onboard radios Cisco IW9167E (CURWB) or Cisco FM4500 to provide broadband wireless connectivity between the trackside infrastructure and trains moving at various speeds. Cisco Wireless Backhaul train-to-ground solution delivers over Gigabits per second (Gbps) continuous throughput with seamless handoff and a few milliseconds latency for train speeds up to 350 km/h. Thanks to its Fluidity make-before-break technology, Cisco Wireless Backhaul can deliver zero packet loss during the handoff. Cisco ruggedized Industrial Ethernet switches connect the trackside radios and other trackside equipment to the access layer and, in turn, to the unified backhaul network and, ultimately, the data centers in the operations control centers. The ruggedized switches support fiber or copper connections to provide network connectivity and also supply power via PoE to trackside radios and other IP devices such as video surveillance cameras. The trackside switches are interconnected in either ring or hub-and-spoke topologies via fiber connections to preaggregation nodes, which form the edge of the highly scalable and converged multiservice MPLS backhaul network. Alternatively, these switches are connected in a ring topology and logically associated with CCI Points of Presence (PoP) in an SD-Access fabric that is managed by Cisco DNA Center. Cisco DNA Center is a powerful network controller appliance and management dashboard that works with Cisco's SD-Access solution to make the network more reliable, more secure, and easier to configure through policy-driven automation and assurance. Cisco DNA Center helps to automate the deployment of the network devices at scale, and can provision and configure all network devices

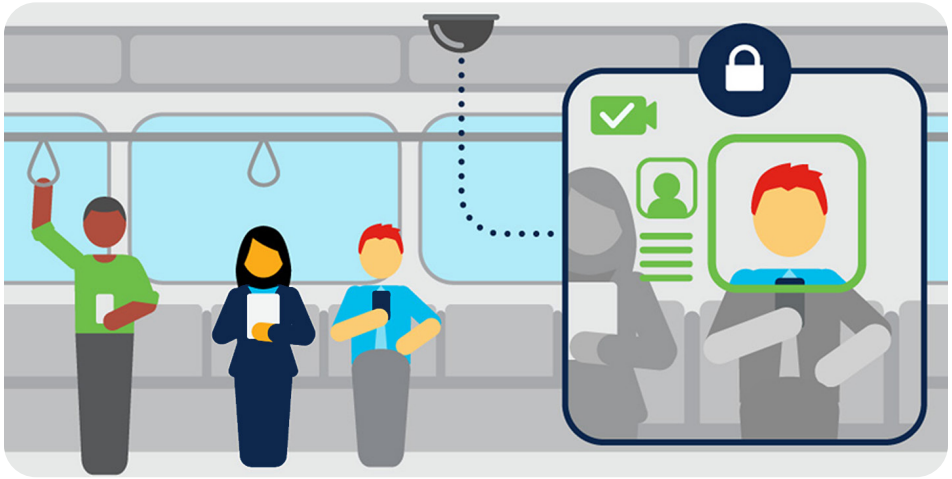
in minutes. It uses advanced artificial intelligence and machine learning to proactively monitor, troubleshoot, and optimize the network. The rail trackside access network integration with Cisco Wireless Backhaul radios has been validated and is thoroughly documented in the CCI design guide.

For network backhaul to interconnect all the rail operations sites, the Cisco Connected Rail solution uses a scalable, resilient, multiservice transport network designed to interconnect the Connected Trackside, Connected Stations, and other geographically distributed sites to centrally located operations control centers. The Connected Rail solution offers two options for the backhaul network architecture: Cisco Unified MPLS and Cisco Connected Communities Infrastructure (CCI) multiservice architecture. These two options give system designers the flexibility to choose the best alternative for their objectives and constraints. Furthemore, the CCI architecture provides options for SD-Access Transit and IP Transit backhaul (including over MPLS). More information on these options is provided below in the "Network Capabilities" section.



Connected Station

The Cisco Connected Station architecture supports innovative services for passengers, helps deliver safety and security for workers and passengers within a station, simplifies operations, and provides station staff with more efficient communications. With a Cisco Connected Station architecture, stations can evolve from multiple proprietary station networks into one manageable, unified, multiservice network that can be used to securely support solutions for passenger and information systems, ticketing, voice communications, and physical security systems. In addition, the network infrastructure supports deployment of physical safety and security capabilities such as emergency help points and video surveillance cameras to enhance station safety and monitoring systems. The Cisco Connected Station network supports dynamic displays and enables new streams of ad revenue for rail operators and compelling experiences for passengers, with such capabilities as Wi-Fi access in densely populated stations, wayfinding, mobile ticketing, and mobile and fixed digital content delivery.



Data center and operations control center

The Cisco Data Center design guides deliver design principles for data center infrastructure, storage, and application solutions. The Cisco Data Center infrastructure provides the high-speed networking capabilities needed for hosting applications and services related to rail operations and passenger services and connecting distributed sites and highly mobile users to those services. The data center houses a highly scalable and virtualized server infrastructure that hosts all applications for the Cisco Connected Rail solution. These application servers may run directly on physical servers or be virtualized through the use of a hypervisor.

Network capabilities

The Connected Rail network architecture described above features some important capabilities that make for a secure, reliable network that is trusted by rail operators around the world. Key capabilities include support for the CCI architecture that brings Cisco's intent-based networking to highly reliable and resillient operational networks; Cisco's proven, service-provider-grade Unified MPLS backhaul capability to connect all of the rail operation's geographically distributed sites; and Cisco's suite of cybersecurity products that work together to provide comprehensive protection for critical rail infrastructure.

Cisco CCI with SD-Access Transit and IP Transit backhaul

The CCI solution transforms a hardware-centric, manually deployed network into a controller-led network that captures business intent into policies that can be automated and applied consistently across the network. The solution delivers a simplified, scalable, and secure infrastructure that can be deployed over a large geographical area with a single policy plane, supports multiple access technologies, and provides highly controllable segmentation capabilities to keep user groups and service classes separated and protected from end to end.

CCI brings intent-based networking to access networks that connect to fiber-connected Points of Presence (PoPs) and VPN-connected Remote Points of Presence (RPoPs); each of the PoPs and RPoPs then connect back to centralized locations via a backhaul. This backhaul can provide either SD-Access Transit or IP Transit services to each PoP. For SD-Access Transit, the backhaul becomes part of the SD-Access fabric. To support SD-Access Transit, the backhaul network should be created with campus like connectivity: high speed, low latency, and jumbo Maximum Transmission Unit (MTU) support. IP Transit, on the other hand, provides flexibility so that a backhaul network can still be used when it does not meet all of those requirements. With IP Transit, the traffic leaves the SD-Access fabric domain at the PoP, where it is transported on an IP Transit network, such as an IP MPLS network. It can then come back into the SD-Access fabric domain at the far side.

Empowered by Cisco IBN, CCI delivers the following benefits:

- Enhanced visibility and segmentation: Cisco DNA Center provides insights into network and security status and end-to-end macro- and micro-segmentation
- Simplified device onboarding, including zero-touch provisioning of Industrial Ethernet (IE) switches
- Centralized policy control: Policies are created and maintained by Cisco DNA Center to continuously align network performance and security to business intent, streamline operations, and enable business innovation
- Support for a zero-trust security posture and zero-trust device onboarding
- Adaptive operations: Keeps an active inventory of devices and, as new devices are added, automates the connection, policy, and security of those devices, avoiding manual updates
- Modularity: Allows standalone or modular solutions in an overall long-term strategic solution
- Network High Availability (HA): Every critical component and link in the overall architecture has HA or redundancy designed in

Cisco Unified MPLS backhaul

Cisco Unified MPLS-based network design implements the best practices and designs developed for large service providers who for years have standardized on MPLS for backhaul networks. The MPLS backhaul design has been used by many rail operators and is proven to support reliable, large-scale network deployments. Cisco Unified MPLS backhaul infrastructure allows for nearly any access technology to be integrated into the architecture to meet service requirements and operator preferences. It supports legacy circuit-switched (TDM) network and packet-based (Ethernet) access technologies and easily enables virtualization of multiple services, including Layer 2 and Layer 3 VPNs, over a single infrastructure. It employs a hierarchical approach to solve scaling and convergence issues associated with a large-scale MPLS deployment, while ensuring ease of end-to-end service provisioning and monitoring. A Cisco Unified MPLS transport network supports:

- Legacy circuit-based transport infrastructure support (PDH, SONET/SDH) to preserve existing investments via MPLS-based Circuit Emulation over Packet (CEoP) services
- Converged architecture, which is a single network infrastructure supporting Layer 3 VPN (L3VPN) services, Layer 2 VPN (L2VPN) services, multicast services, and legacy transport with circuit emulation services

- Hierarchical QoS (H-QoS) to provide differentiated services Per-Hop Behavior (PHB) treatment of traffic classes
- IP Transit for Cisco SD-Access architectures such as CCI
- Operations, Administration, and Maintenance (OAM) for fault monitoring and correlation
- Utilization of multiple technologies to meet stringent availability SLAs
  - Transport layer: Loop Free Alternate (LFA) and Remote LFA (rLFA) Fast Reroute (FRR), Bidirectional Forwarding Detection (BFD) at the Interior Gateway Protocol (IGP) for fast recovery
  - Multichassis Link Aggregation Groups (MC-LAG) and pseudo MC-LAG for multihomed Ethernet access nodes in hub-and-spoke topologies; Resilient Ethernet Protocol (REP) protection for Ethernet access nodes in ring topologies
  - Border Gateway Protocol (BGP) edge protection and BGP Fast Reroute (FRR) edge protection mechanisms for L3VPN services
  - Multirouter Automatic Protection Switching (MR-APS) for TDM pseudowire-based services

Cisco's Connected Rail solution gives rail operators flexibility to choose a migration path that is right for them. They can continue to leverage existing Unified MPLS backhaul networks that deliver both legacy and IP services over a converged infrastructure that meets operational SLA requirements. They can also leverage that investment to deploy the CCI SD-Access architecture to enable secure and reliable access services such as passenger Wi-Fi and station services, additionally using the MPLS network as IP Transit for the CCI architecture. This provides a simple and robust migration path to new, modern, and secure networking capabilities such as IBN and SD-Access for customers who are currently still relying heavily on MPLS to deliver their day-to-day operations.

Security

The Connected Rail solution implements layered and integrated security technologies throughout the design to provide an end-to-end secure framework, process, and network infrastructure that addresses all needs for secured operation and passenger safety. The following are four major factors needed in a secure railway network.

Asset visibility: Visibility into the operation and security conditions of devices, sensors, endpoints, networking components, and applications is foundational to designing a secure communications architecture and formalizing a secure strategy. Cisco Stealthwatch® is a comprehensive visibility and network traffic analysis solution that leverages NetFlow data from network infrastructure devices. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the network so they can quickly and effectively respond to threats.

Network segmentation: The ability to separate the Operations Network (OT) from the enterprise IT network, and the capabilities of segmenting various parts of these networks for different types of services and applications, are imperative to securing the network. Cisco Secure Firewall can be implemented to separate the operations network from the enterprise network and prevent unauthorized access from the internet to the operations and enterprise networks. Cisco ISE is a next-generation identity and access control policy platform that enables rail operators to enforce compliance, enhance infrastructure security, and streamline their service operations. The CCI solution accomplishes traffic segmentation through macro- and micro-segmentation. Macro-segmentation defines different Virtual Network (VN) instances, each of which maintains a separate routing table to keep different types of traffic completely separate. Micro-segmentation leverages ISE to classify and associate a device with a Security Group Tag (SGT) and enforce the policy with Security Group Access Control Lists (SGACLs). This provides further traffic segmentation within each VN. Additionally, L3VPN can be implemented to deliver service separation and multitenant deployments over a converged MPLS infrastructure.

Threat detection: Cisco Stealthwatch delivers an advanced network detection and response solution. By leveraging multilayer machine learning and entity modeling, it constantly monitors not only the traffic going in and out of the network, but also lateral flows within the network, enabling detection of a wide range of attacks such as zero-day malware, Distributed Denial of Service (DDoS) attempts, inside threats, and others. Cisco AMP continuously analyzes file activity across the network, enabling the security operations teams to quickly detect, contain, and remove advanced malware. Cisco Umbrella, a cloud-based security solution, blocks malicious and unwanted domains, IP addresses, and cloud applications. It prevents phishing, malware, and ransomware attacks.

The bridge to possible

Threat investigation and response: With the integrated Cisco security portfolio and open security platform, the security operations teams will have deeper and better visibility across the network, accelerating the threat detection and investigation process and enabling faster response and threat remediation.

Ecosystem Partners

Ecosystem partners are vital in the successful deployment and operation of connected rail solutions. BAI Communications (BAI), a Cisco ecosystem partner for rail, is a world leader in shared communications infrastructure, pioneering the future of advanced connectivity for customers in transport, telecommunications, government, enterprise, and venues. The BAI Group companies include Mobilitie, Signal Point, Transit Wireless, and Vilicom—and together they serve rail operators, mobile network operators, venues, and residents around the globe.

The rail networks deployed by BAI support many important services, not only for passenger entertainment, but for operational enhancements as well. Their unique model also opens new avenues for transport partners to deliver neutral hosted infrastructure at low or no cost, while advancing additional use cases such as advertising or infotainment to establish a profitable service.

Cisco Validated Designs provide solution partners with a foundation for a secure, segmented, multiservice network, which is ideal for operating a neutral host environment like this. The Connected Rail architecture provides flexibility for various technologies, enabling the broadest possible adoption of compelling use cases. For BAI, each potential use case built on Cisco's rail architecture represents a new opportunity for a financially advantageous solution that can be offered to our mutual rail customers.

"We have been working with Cisco for several years to deliver robust transport connectivity solutions around the world. The end-to-end testing, global experience, and proven products that Cisco offers the rail industry made the choice easy. With the integration of the Fluidmesh product line into Cisco's portfolio, it's clear that they are making the important investments the rail industry expects."

Josh MacKinnon
Engineering Systems Director, BAI Communications

Cisco Customer Experience

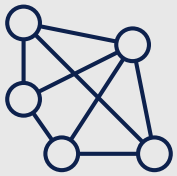
In today's rapidly evolving OT and industrial spaces, customers and systems integrators are challenged to keep pace with new technology trends to ensure that projects are delivered in a cost-effective manner. With Cisco's suite of Industrial Networking and Security services, our partners and customers can reduce solution implementation risk on projects that leverage Cisco IoT technologies in a true model of partnership with Cisco. With simplified packaging, a flexible consumption model, and advisory services covering each key project milestone, this suite of services can allow you to enter new markets with confidence to expand and grow your business.

Cisco's CX Industrial Networking and Security services help rail and transportation operators accelerate the digitization of their existing operations using a unique architecture-based approach to service delivery. Cisco CX leverages strategy development, architectural assessments, network design, migration and deployment assistance, and support services to help Cisco's key ecosystem partners plan, build, and manage solutions. These solutions focus on business outcomes that result in improved worker and passenger services and safety, risk mitigation, higher productivity, improved operational efficiency, and deeper intelligence and insights, with security at the core of the end-to-end solution.

The bridge to possible

Overview of CX Services

Advisory services around key project milestones

Design Reviews	Testing and Validation	Outdoor Wireless Planning and Design	Outdoor Wireless Tuning and Optimization
			
Cisco will help validate your designs	FAT, SAT, SIT and UAT Advisory	Predictive Modeling + Wireless Design Document Development	Optimize RF deployment

Enable Cisco Partners in Model of True Partnership

Numerous options available within each service, with and without document development

With more than 30 years of industrial networking experience, Cisco is uniquely positioned to address these new demands on industrial networks, which require a greater need for improved interconnectivity across industrial equipment and enterprise networks. Our proven processes and tools deliver consistent results based on best practices and strong communication. Our experts deliver services that allow organizations to accelerate the integration and transformation of their current infrastructure to the next-generation network, capable of evolving operations to continue to meet the evolving demands of the business.

Conclusion

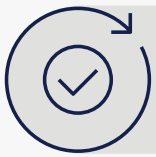
Cisco supports many of the world's largest passenger and freight rail infrastructure and train operators and understands the unique demands and challenges that rail operators face. This solution brief has provided an overview of Cisco's Connected Rail solution, which gives rail operators and rail solution providers a proven approach for meeting their needs. The Connected Rail solution incorporates Cisco networking innovations such as intent-based networking and tools such as Cisco DNA Center so that the rail operator's networking intent can be easily specified in understandable policies that are then implemented using automation and monitored using artificial intelligence to give operators assurance that their network is secure and performing as intended. Innovations like IBN are made easily adoptable for rail operations through the Connected Rail solution, which includes Cisco Validated Designs comprising design guides and implementation guides supported by Cisco. The Connected Rail solution securely and reliably connects users and devices onboard trains, in stations, at trackside, and in operations control centers so that solution providers can support use cases including passenger internet access, infotainment, infrastructure monitoring and maintenance, and signaling and control. Cisco's ecosystem of partners and Cisco professional services are available to help rail operators design, deliver, and even operate the Connected Rail solution as part of an end-to-end solution that meets your specific needs.

What we make possible

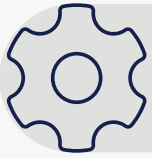
Prevalidated, proven multiservice network for all your present and future goals

Automated service segmentation to reduce the scope of compliance and simplify security policies

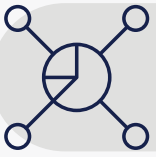
Ruggedized network for robust and effective movement of data



Automated uniform policy deployment for one redundant and resilient network



Plug-and-play device deployment for simplicity and efficiency



Flexible network topology and backhaul options for future cost security and growth opportunities