Connected Rail Solution Design Guide

November, 2016

Cisco Systems, Inc. www.cisco.com

Contents

Connected Rail Solution Design Guide . . . 1
- Organization . . . 1
- Audience. . . . 1
- Document Objective and Scope . . . 1
- Use Cases/Services/Deployment Models . . . 2

Solution Overview. . . . 2

Solution Supported Services and Models . . . 2
- Service Architecture Overview . . . 2
- Supported Services and Models . . . 3
  - Passenger Wireless Internet Access . . . 4
  - Passenger Entertainment Services. . . . 5
  - Enterprise Wireless Network Support. . . . 5
  - Video Surveillance . . . 6
  - Communication Based Train Control . . . 7
  - Voice Communications . . . 8
  - Wireless Bulk Data Transfer . . . 8
  - Station Wi-Fi and Displays . . . 9

Solution Architecture . . . 9
- Solution Topology . . . 10
  - Connected Train . . . 10
  - Connected Trackside. . . . 14
  - Connected Station. . . . 16
- Train-to-Trackside Wireless Network . . . 18
- MPLS Backhaul Network . . . 19

Solution Components . . . 20
- Cisco Components . . . 20
- Third Party Components . . . 20

Solution Functional Considerations . . . 21
- Solution Infrastructure Design . . . 21
  - Service Transport . . . 22
  - Communications-Based Train Control . . . 23
- Passenger Wi-Fi Entitlement . . . 24
- Data Center. . . . 25
- QoS Model . . . 25
- Standards Compliance . . . 26

Network Management System 27
Management User Interface 29
Security, High Availability, and Scale 31
Security Considerations 31
High Availability Considerations 32
Scalability Considerations 33
Passenger Wi-Fi 33
Video Surveillance 33
Related Documentation 34
Cisco 35
Fluidmesh 35
Klas Telecom 35
Lilee Systems: 36
Glossary 36

Connected Rail Solution Design Guide

Welcome to the *Cisco Connected Rail Solution Design Guide*.

The document covers the solution design and best practice recommendations from Cisco for Connected Rail deployments, including the following subsystems:

- Connected Train
- Connected Trackside
- Connected Station

Organization

This guide includes the following sections:

Solution Overview, page 2	Provides an overview of the Connected Rail Solution.
Solution Supported Services and Models, page 2	Provides an overview of service architecture and supported services and models.
Solution Architecture, page 9	Describes the solution topology and functional role descriptions for the train-to-trackside wireless network and the MPLS backhaul network.
Solution Components, page 20	Provides a list of Connected Rail Solution components.
Solution Functional Considerations, page 21	Details the end-to-end Solution level functions that span across individual roles within the Solution.
Security, High Availability, and Scale, page 31	Describes considerations for security, high availability, and scalability for the Connected Rail Solution.
Related Documentation, page 34	Provides a list of documentation relevant to the Connected Rail Solution.
Glossary, page 36	Provides a list of acronyms and initialisms used in this document.

Audience

The main intended audience for this document is Cisco account teams, Cisco Advanced Services teams, and Systems Integrators working with railroad operators. It is also intended for use directly by the railroad operators in order to understand the features and capabilities enabled by the Cisco Connected Rail Solution design.

Document Objective and Scope

This design guide provides a comprehensive explanation of the Cisco Connected Rail Solution design. It includes information about the Solution's architecture, supported services, and possible deployment models. The guide also recommends best practices and potential issues when deploying the reference architecture. This document supersedes previous Cisco Connected Rail design guides.

The *Cisco Connected Rail Solution Implementation Guide* is a companion document to this document, and provides guidelines for implementation and configuration a validated subset of the Solution architecture and supported services described in this document. This guide can be found at the following URL:

- https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-11479439

Use Cases/Services/Deployment Models

The following are the technology use cases addressed by the Connected Rail Solution:

- Passenger Wireless Internet Access, page 4
- Passenger Entertainment Services, page 5
- Enterprise Wireless Network Support, page 5
- Video Surveillance, page 6
- Communication Based Train Control, page 7
- Voice Communications, page 8
- Wireless Bulk Data Transfer, page 8
- Station Wi-Fi and Displays, page 9

Solution Overview

The Cisco Connected Rail Solution provides an end-to-end Solution design for service delivery to a rail infrastructure, including connectivity onboard the train, at the trackside, and in the stations and maintenance yards. The Solution provides a converged, multiservice, secure, and standards-based infrastructure on top of which passenger and operational capabilities for the rail operator can be delivered. It replaces redundant, proprietary, and single application solutions with limited or no interconnectivity. This results in reduced CAPEX, increased ridership, and improved safety for rail Solutions.

As mentioned in the above, this design guide provides a comprehensive explanation of the Connected Rail Solution design. It includes information about the Solution's architecture, supported services, and possible deployment models. The guide also recommends best practices and potential issues when deploying the reference architecture.

Solution Supported Services and Models

This section, which details the services supported by the Connected Rail Solution, includes the following major topics:

- Service Architecture Overview, page 2
- Supported Services and Models, page 3

Service Architecture Overview

The Cisco Connected Rail Solution implements a comprehensive infrastructure that supports multiple services. These services are typical of those required by rail operators.

Supported Services and Models

Table 1 lists the services supported in this release of the Connected Rail Solution.

Table 1 Supported Services and Models

Service Category	Service Definition
Passenger Wireless Internet Access	Provides Wi-Fi Network services to passengers onboard the train. Passenger access is authorized when the passenger accepts the terms & conditions of using the service in order to gaining access to Internet services. Passenger acceptance is done through a portal page, or through a certificate loaded from a previously installed application. Subsequent access to Wi-Fi network services is transparent to the passenger within a timeout period defined by the operator.
Passenger Entertainment Services	Provides on-demand entertainment content to passenger devices such as tablets, smartphones, and laptops. Delivered over the same Wi-Fi network as passenger internet access. Content is stored on an onboard server, and security policies permitting access are implemented on the onboard gateway.
Enterprise Wireless Network support	Provides Wi-Fi Network access to Enterprise services for drivers, conductors, emergency personnel, and other operator employees to enterprise services on a separate Service Set Identifier (SSID) from Passenger Services.NEWAccess requires username/password and/or certificate-based authorization.
Video Surveillance	Onboard systems support 2 to 16 separate IP video surveillance cameras per car, depending upon the operator's requirements. Video recordings are stored to an onboard ruggedized server, or to integrated flash storage in the cameras if no onboard server is deployed. On-demand real-time video transmission over train-to-trackside and/or cellular backhaul is supported. Recorded video is offloaded via train-to-trackside wireless network or via maintenance yard network to long-term storage for later retrieval when the train is parked in yard. The Solution can be configured to offload all recorded video, or only video associated with tagged events.
Communications Based Train Control	Implements semi-autonomous to fully-autonomous control of trains from a centralized operations center via spatially-diverse parallel networks between the train and control center. Spatially-diverse parallel networks help ensure that control traffic is successfully transmitted in spite of any network disruption.

Table 1 Supported Services and Models (continued)

Service Category	Service Definition
Voice Communications	Enable two-way voice communications between personnel on the train and personnel in the control center via Voice over IP (VoIP) systems. Supports wireless handsets for onboard personnel via the onboard Wi-Fi system. Supports integration with legacy voice equipment, such as digital radios, and with desktop VoIP phones via Cisco Instant Connect.
Wireless Bulk Data Transfer	Onboard train systems are able to be updated and provide information on a continual basis over the train-to-trackside wireless network or as a bulk data transfer while in a maintenance yard. Such systems include: ■ Predictive maintenance system updates and log files ■ Ticketing and payment information ■ Video surveillance recordings ■ Software updates for other systems ■ Passenger " infotainment" systems
Station Wi-Fi and Displays	Provides high-density Wi-Fi service deployment for rail stations and platforms, using the best practices developed for deploying Wi-Fi services in large sports stadiums and other retail locations. Includes location tracking and analytics information for passengers when in the station. Also provides management and display of rich information content and videos to multiple monitors throughout the station.

Passenger Wireless Internet Access

The Passenger Wireless Internet Access service is described in this section.

The Cisco IW3702 Access Point is deployed on board for wireless connectivity. The following considerations are made for deployment:

- Both 2.4GHz and 5GHz radios are used for passenger device connections, providing the ability to support higher-bandwidth connectivity in the less congested 5GHz frequency range while maintaining backward compatibility for devices that only support 2.4GHz frequencies.
- The access points are deployed in FlexConnect mode, which transports user traffic via a locally-defined VLAN on the onboard network. This helps enable access to local resources such as an on-demand entertainment server, and eliminates the potentially inefficient routing of traffic via the centralized Wireless LAN Controller (WLC). All access points are still centrally managed via the WLC. If the tunnel from the WLC to the access point is interrupted, new client connections will not be allowed but existing authorized connections will continue to pass traffic.
- the number of access points deployed within a car depends upon several factors, including the physical topology of rail car, the number of passengers expected in the car, whether the passengers predominantly sit or stand, and suitable mounting positions. A minimum of two access points should be planned for most deployments, in order to provide infrastructure redundancy; no more than four access points are typically needed. Each access point is capable of handling up to 75 device connections efficiently.

Multiple services are supported by the onboard wireless infrastructure, with unique SSIDs for each service, providing service separation across the common onboard infrastructure. Each SSID is mapped to a separate Virtual Local Area Network (VLAN), which is then provided a separate IP subnet by the DHCP server via the onboard gateway. This provides proper service separation and service routing. Deployment considerations for the passenger wireless internet access are discussed here, and other services are discussed in the next section.

- The passenger wireless internet access SSID is configured to be open, with no authentication required. This reduces any barrier to entry for using the Wi-Fi service.

- When associating to the SSID for the first time, the passenger will be presented with a portal landing page. Depending upon the requirements of the rail operator, the passenger may simply have to accept the terms and conditions of use, or provide additional information to verify entitlement to use the service, such as a ticket number. Another option is to have the passenger install a certificate profile on the device via the rail operator's application, which then grants them secure access to the wireless internet access.

For portal-based deployments, the landing page is hosted by the Cisco Enterprise Mobility Services Platform (EMSP). Cisco EMSP provides a rich content platform for handling user authorization and entitlement, as well as serving context-aware advertisement and other content via the portal page. The WLC controlling the access point redirects the connection request to the EMSP portal. Further details on implementing Cisco EMSP are available in the *Cisco Wireless Controller Configuration Guide, Release 8.2* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_011000.html

By deploying the onboard access points in FlexConnect mode, passenger traffic from authorized sessions is switched to a locally-defined passenger Wi-Fi VLAN in order to allow for local resource access for services, such as personal device infotainment. In order to maintain security for local service access and to maintain service separation throughout the onboard network, all local service traffic access is through inter-VLAN routing implemented on onboard gateway. This provides a single place for implementing security policies for service access, such as Access Control Lists (ACLs).

Passenger Entertainment Services

On-demand entertainment services may be provided to passenger devices via the same wireless connection that is offered for passenger internet access. This service helps enable the potential for additional revenue streams to rail operators, via charging for access to on-demand content, displaying advertisements on passenger devices, or both.

On-demand content is provided via a ruggedized server onboard the train, to eliminate bandwidth utilization for this service over the train-to-trackside wireless link. The service is accessed through the same SSID as is the passenger wireless internet access. To provide secure access, the onboard server is placed in a separate VLAN and IP address range from the passenger internet users. Access to the server, and thus content, is enabled via inter-VLAN routing through the onboard gateway. ACLs restrict access to only the required IP address and ports for helping enable the entertainment service.

Entitlement to on-demand entertainment content is handled at the application layer between the onboard server and the passenger device being used to access the content. This may be facilitated via an application loaded on the passenger device, or via a web portal that is hosted by the onboard server.

The Connected Rail Solution provides the transport infrastructure and security layers for this service, supporting the requirements of any on-demand entertainment service that the rail operator wishes to deploy.

Enterprise Wireless Network Support

Enterprise services are delivered on the same onboard network and wireless infrastructure that provides passenger wireless internet access. If required, even access for law enforcement agencies may be implemented. The onboard infrastructure implements the proper service separation, security, and QoS functionality to support multiple services on a converged infrastructure.

Each service is assigned a separate SSID in the wireless infrastructure. This provides access controls, bandwidth guarantees and restrictions, and security functionality tailored to the requirements of a particular service. All SSID access, with the exception of the previously described passenger wireless internet access, is authorized by Wi-Fi Protected Access 2 (WPA2) Enterprise security functionality. Depending upon the rail operator's requirements, service authorization can be conducted through a per-user username and password, a pre-installed certificate on a wireless device, or a combination of the two.

Each SSID is mapped to a separate VLAN, which is then allocated a separate IP address subnet. This provides proper service separation and service routing through the onboard gateway device. If needed for operational workflows, such as accessing a Video Surveillance feed from another Enterprise service VLAN, inter-VLAN routing can be accommodated at the onboard gateway.

Video Surveillance

A crucial aspect of maintaining the safety and security of a rail operation is the ability to maintain visual and audio surveillance of the entire operation, including stations, trackside infrastructure, and onboard the trains. The Cisco Connected Rail Solution scope includes comprehensive video surveillance capabilities integrated into the converged networking infrastructure.

The Connected Rail validated solution design supports up to 16 cameras per car, which is more than enough to accommodate any single or double level rail car configuration with any number of doors and other spaces requiring monitoring.

In order to support video surveillance in a converged infrastructure, IP-enabled video cameras are implemented in the solution design. Two camera options exist in the solution design:

- **The Cisco Video Surveillance 3050 IP Camera**—This is a dome form-factor ruggedized, outdoor, high?definition (HD) video endpoint with IP66 / IK10 ratings. It supports up to 720p video (1280x720 pixels) at 30 frames per second (fps), and supports both Motion JPEG (MJPEG) and H.264 codecs simultaneously for recording. The 3050 provides a 90 degree diagonal field of view, and is manually adjustable from 0-90 degrees. More details are available in the *Cisco Video Surveillance 3050 IP Camera Data Sheet* at the following URL:
  - http://www.cisco.com/c/en/us/products/collateral/physical-security/video-surveillance-3000-series-ip-cameras/datasheet-c78-735497.html
- **The Cisco Video Surveillance 7070 IP Camera**—This is a ruggedized, outdoor, HD video endpoint equipped with a 5-mega-pixel sensor and a fish-eye lens that can deliver 180° panoramic views and 360° surround views with IP66 / IK10 ratings. It supports up to 1080p video (1920x1080 pixels) at 15 fps, and supports both MJPEG and H.264 codecs simultaneously for recording. More details are available in the *Cisco Video Surveillance 7070 IP Camera Data Sheet* at the following URL:
  - http://www.cisco.com/c/en/us/products/collateral/physical-security/video-surveillance-7000-series-ip-cameras/datasheet-c78-735498.html

Note that these two cameras are not fully-compliant with the European Committee for Electrotechnical Standardization (CENELEC) EN 50155 specification for onboard deployment of electrical equipment. This must be taken into consideration when choosing equipment for onboard deployment. Inclusion of a fully-compliant IP video camera is planned for a future release of the Connected Rail Solution.

The Solution design supports two options for storage of the video captured by the IP cameras onboard the train.

The first is with a ruggedized onboard server running the Cisco Video Surveillance Media Server (VSMS) software. The solution design promotes one server per consist, for up to 16 cameras. If more than 16 cameras are installed in a consist, then a server should be deployed for every 16 cameras. This facilitates the static association of cameras to the VSMS server, and ensures that the server is capable of supporting sufficient storage to ensure that retention policies are met for the associated cameras. Cisco VSMS is installed in a virtual machine within VMWare VSphere ESXi on the server. This permits the use of any VMWare and rail certified ruggedized server, without the worry of hardware incompatibilities, and also potentially permits the server to host other functions in addition to Cisco VSMS.

The other storage option is to use the microSD card storage built-in to the Cisco Video Surveillance IP cameras. Both the 3050 and 7070 IP cameras support the SanDisk Extended Capacity (SDXC) storage standard, providing up to 2TB of onboard storage per camera, depending upon the size of the microSD card installed in the camera. The microSD card slot is not accessible unless the camera is removed, providing a tamper-resistance installation.

Best practices for deployment and scaling of video surveillance in fixed locations, such as along the trackside or in a station, are well documented in existing design guides. More information is available on the Cisco IP Video Surveillance page at the following URL:

- http://www.cisco.com/c/en/us/solutions/enterprise/ip-video-surveillance/index.html

The Connected Rail Solution supports event marking of video segments based on a number of triggers and inputs. The Solution can be configured to take different actions depending upon the particular trigger, such as tagging of a particular clip to be reviewed first by an operator, or even to notify an operator of an issue and live stream video to the operations center. This permits the rail operator to access video surveillance when needed, but not unnecessarily use network resources for video when it's not needed. The operators are also able to call up video on-demand from any cameras via Cisco Video Surveillance Operations Manager (Cisco VSOM), the centralized management system for video surveillance. Video display is also integrated into Davra's RuBAN Internet of Things (IoT) management and analytics platform, which is described later in this document. Note that the RuBAN platform only supports video encoded with the MJPEG codec.

The following event triggers are supported by the Video Surveillance system:

- **Contact Closure Triggers**—These are connected to the Cisco Video Surveillance IP cameras. Any contact switch can be used as a trigger when connected to one of the cameras. The system can event tag just the video stream from the camera connected to the trigger, or can be configured to also propagate that trigger to other cameras. Examples of contact closure triggers are:
  - Door open and close
  - Panic button
- **Accelerometer-based Triggers**—These sense abnormal dynamics. The Davra RuBAN management system has APIs that can integrate train telematics and trigger the video surveillance system. Examples of these triggers are:
  - Panic braking
  - Driver behavior
- **Audio Triggers**—The Cisco Video Surveillance IP cameras incorporate a microphone for recording audio along with video. The IP camera is configured to sense the audio profile of certain events, and generate an event trigger when a profile is matched. Examples of these triggers are:
  - Gun shots
  - Shouting
  - Other loud noises
- **Geographic Triggers**—The Davra RuBAN management system is able to generate events based on the geographic location of the train. It is also able to include geographic information for video tagged by other events. Examples of geographic triggers are:
  - Geofence
  - Unexpected train stoppages along route
  - Include geographic information with video tagged by other event triggers

The system design supports archiving of video surveillance recordings to a centralized Long-Term Storage (LTS) system. If the rail operator has deployed the train-to-trackside wireless system component of this solution, then video can be copied to the LTS system on an ongoing basis. If only cellular connectivity is available to the train during normal operations, then it may be best to only copy video to the LTS system over a Wi-Fi link when the train is out of service in a maintenance yard. The configuration of the video surveillance codecs and frame rates, and the operating schedule of the train must be such as to provide sufficient connectivity time to offload the video files in the allotted time.

Communication Based Train Control

Communication Based Train Control (CBTC) is a special service case that has unique requirements on top of the other services covered in the Connected Rail Solution. CBTC provides semi-autonomous-to-fully autonomous control of train functionality from a centralized control and operations center. It also helps enable a rail operator to transition from fixed block traffic management to a moving block management system, increasing rail capacity by safely decreasing train spacing.

CBTC is enabled by implementing an onboard controller on each train that is controlled by a centralized zone controller. Moving controlling functions off of the train either partially or completely requires an *always-on* lossless network design that cannot experience any network interruption between these controllers.

Implementing a single lossless or nearly-lossless transport network is nearly impossible and prohibitively expensive. Instead of attempting to engineer a single network infrastructure with a high enough availability level to provide CBTC, the generally-accepted approach is to deploy two parallel network infrastructures. These spatially diverse parallel networks are connected to the zone controller and to the onboard controller. The controllers replicate all command packets and send these duplicate packets across these redundant traffic paths. The control center equipment and the onboard train control unit receive the traffic from both networks, recognize the redundant traffic, and implement the requested control. If one network experiences an outage, the control traffic is still carried by the other network, thus ensuring the integrity of train control and monitoring via the CBTC service.

The Connected Rail Solution design supports the transport of CBTC service traffic so that IEEE 1474.1, *Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements*, can be met. The solution infrastructure is capable of supporting the following requirements for traffic delivery:

- End-to-end network latency of <50msec between the onboard train control unit and the control center
- Differential latency of <3.5msec between the control traffic being carried over the spatially-diverse networks

Voice Communications

The converged network infrastructure integrated into the Connected Rail Solution design supports two-way Push-to-Talk (PTT) VoIP communications throughout the rail operation. This includes support for voice communications between personnel in all locations within the rail operation, such as onboard the train, trackside, within the station, and in the dispatch center. The solution provides the flexibility to integrate next generation voice communications systems for new rail deployments and existing rail retrofits. The Cisco Instant Connect communications system also provides VoIP integration with existing digital radio systems, allowing for operators to migrate from proprietary voice communication systems in a gradual manner.

Cisco Instant Connect integrates support for many different endpoint devices, including dedicated VoIP endpoints, IP Dispatch turrets, wireless IP phones, and smart phones and tablets. For rail operations personnel in the field and not tied to a specific location, a ruggedized mobile communications device is typically implemented. The solution includes the XP7 ultra-rugged LTE/Wi-Fi Android smart phone, and Cisco offers an application for other Android devices to enable VoIP. It also provides Cisco Unified Communications integration, allowing for Cisco IP phone communications support.

The Connected Rail Solution integrates end-to-end QoS, providing proper real-time treatment for VoIP traffic throughout the network infrastructure. The Solution design is capable of routing VoIP traffic over both the train-to-trackside wireless infrastructure as well as any cellular backhaul, providing comprehensive coverage for onboard the train.

Wireless Bulk Data Transfer

The systems onboard the train, such as those responsible for handling route information and announcements, as well as logging route progress throughout the day, require periodic connectivity with centralized scheduling and monitoring systems to stay up-to-date. With the constant train-to-trackside wireless connectivity implemented in the Connected Rail Solution, these transfers can happen on an as-needed basis. Some service traffic that is not passenger affecting, such as system monitoring, can be transferred on an ongoing basis. Some service updates, such as those to the passenger information system, should be coordinated for when a train is out-of-service. Lastly, if a train route has certain times or areas where cellular-only connectivity is available, system updates should be coordinated to happen when train-to-trackside wireless connectivity is available. This helps ensure that charges for cellular data usage are limited to critical or revenue-generating services, such as passenger wireless internet access.

When a trackside wireless connection is established to the train, the following types of bulk data transfers will take place between the onboard systems and the backend systems in the operations center:

- **Trackside-to-Train**—Download updated route information, route audio announcements, ticketing and payment information, and software updates for the onboard announcement system. Expected frequency of updates is needed as a train switches routes.

- **Train-to-Trackside**—Upload predictive maintenance information and log files, ticketing and payment information, and video surveillance files.

For ease of system deployment over hundreds or thousands of trains and rail cars, identical configurations may be used for onboard systems, with the exception of a unique vehicle identifier. The onboard network infrastructure then provides Network Address Translation (NAT) functionality to enable routing for the particular rail car or train.

Nearly all required file transfers are easily accommodated within a short transfer window, given the bandwidth available across the train-to-trackside wireless connection. The notable exception to this are video surveillance files and video files for infotainment services, both of which are several orders of magnitude larger than any other service. The Connected Rail Solution design proposes that video surveillance footage be moved off the train on a continual basis. Another option is to simply store the video on the local vehicle storage, to be retrieved at a later date if needed. Infotainment video source files, which may be even larger than the video surveillance files, will need to be transferred either over a long window over the wireless connection, or by swapping out the physical storage on the train.

Some other considerations to take into account when planning for bulk data transfers over wireless links are:

- Available bandwidth will be higher when passengers are not on the train, such as when parked in the station between routes or when parked in a maintenance yard.
- throughput is higher when the train is stationary versus moving, as velocity has a detrimental effect on the train-to-trackside wireless transport.
- Multiple trains connected to the same trackside base station will share the bandwidth of that base station, reducing throughput for each train.

Station Wi-Fi and Displays

Large rail stations bear a close resemblance in size, layout, and traffic flows to large retail establishments, and even sports venues. In contrast to standard Enterprise deployments, deploying Wi-Fi networking coverage in these kinds of crowded venues presents unique challenges for coverage and service delivery. In addition, having the ability to track passenger device location presents an opportunity for further monetization of that passenger through targeted advertising. Cisco has developed best practice deployment guidelines and recommendations for deploying large-scale, high-density Wi-Fi networks, which have been used in numerous venues around the world, in these venues. More details are available on the Cisco Connected Stadium Wi-Fi page at the following URL:

- http://www.cisco.com/c/en/us/solutions/industries/sports-entertainment/stadium-wifi.html

Another key method for interacting with passengers in a large rail station is through digital signage. Providing information, rich media, and targeted advertisement to passengers provides further opportunities for rail operators to improve the customer experience and potentially add further revenue opportunities. Again, Cisco has developed a system for centrally managing and targeting delivery of customized video, promotions, and relevant information to any combination of monitors throughout the station. More details are available on the Cisco StadiumVision page at the following URL:

- http://www.cisco.com/c/en/us/solutions/industries/sports-entertainment/stadiumvision.html

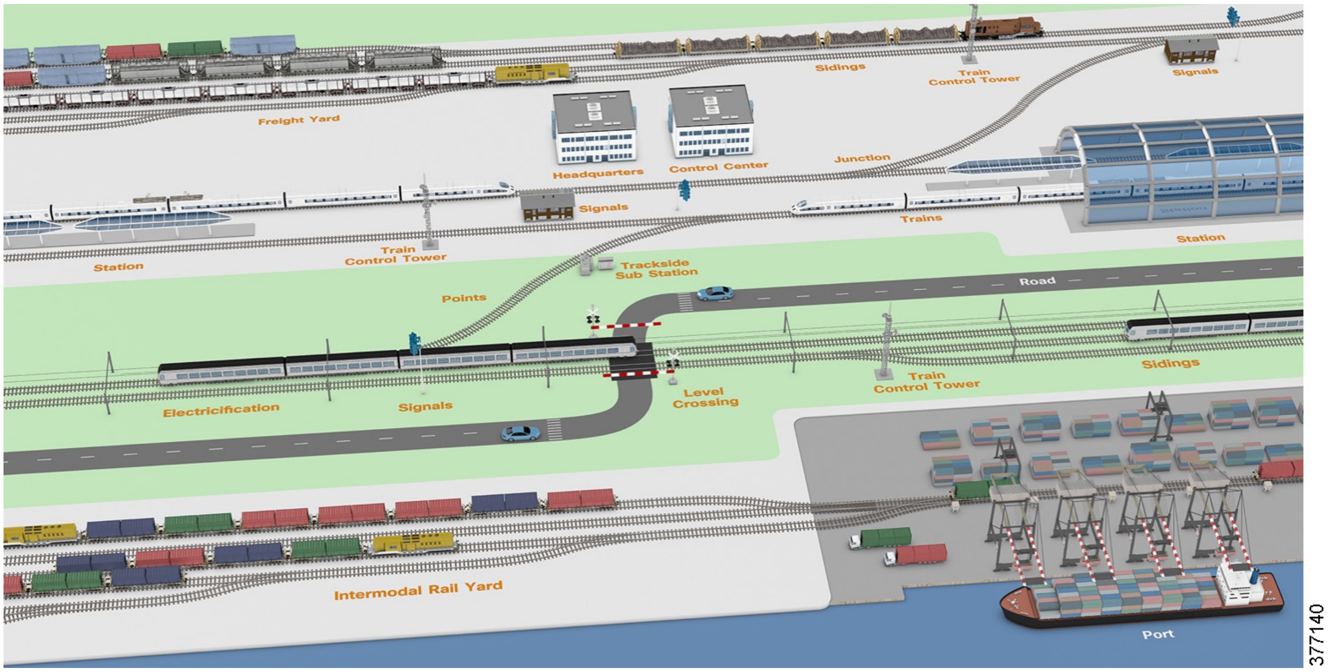
Solution Architecture

This section, which describes the high-level architecture design of the Cisco Connected Rail Solution, including functional role descriptions and end-to-end Solution functions, includes the following major topics:

- Solution Topology, page 10
- Train-to-Trackside Wireless Network, page 18
- MPLS Backhaul Network, page 19

Figure 1 shows a high-level diagram of the Cisco Connected Rail Solution.

Figure 1 Cisco Connected Rail Solution High-Level Diagram



As shown, the Connected Rail Solution encompasses a very broad range of areas, and not all are covered in this phase of the architecture design. The three main areas of focus, or sub-systems, in this phase are:

- Connected Train
- Connected Trackside
- Connected Station

Solution Topology

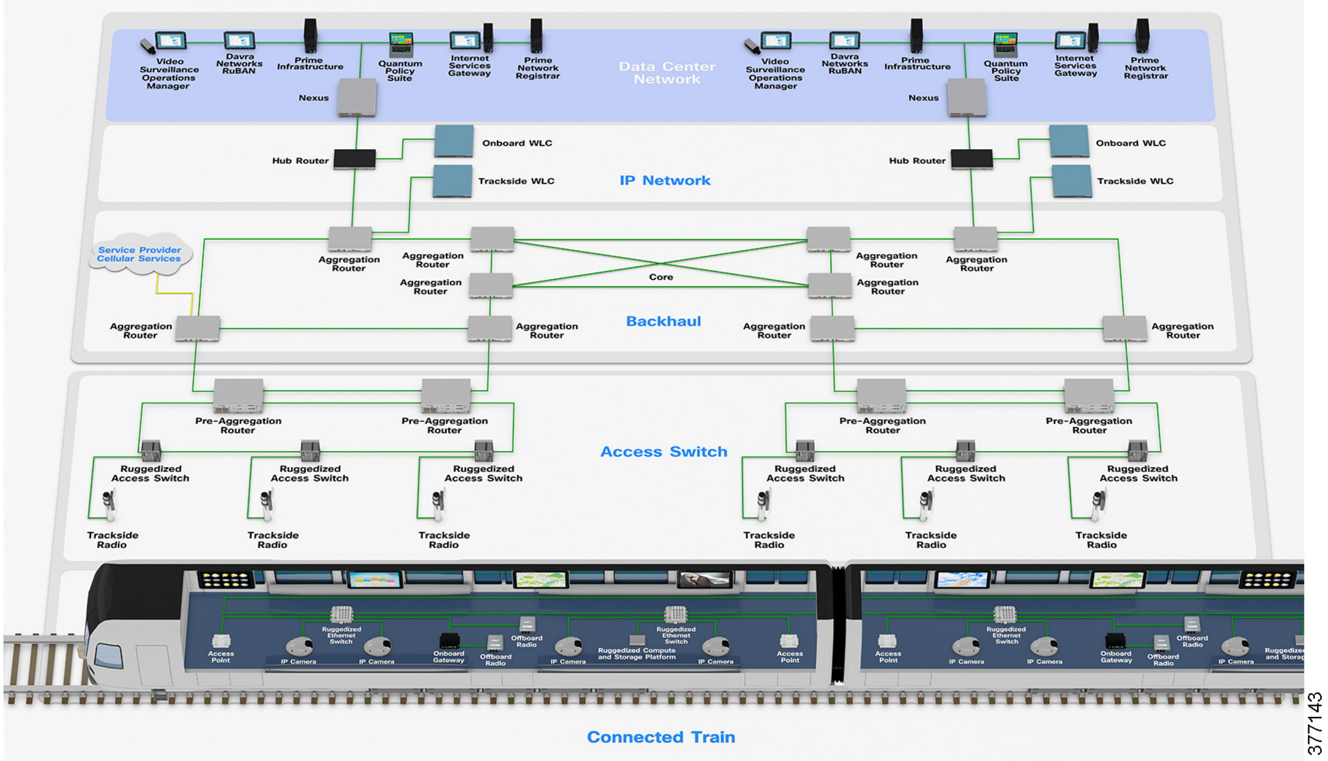
Each of the subsystems comprised by the Connected Rail Solution is described in more detail in this section.

Connected Train

The number of services offered and required onboard a train has increased over the years, and a greater number of those services are provided via a networking infrastructure. Therefore, the need for and requirements of a comprehensive, multi-service network infrastructure onboard the train has grown in recent years. The Cisco Connected Rail Solution provides for a scalable and resilient onboard network design to help enable all these services instead of requiring service-specific infrastructure deployments.

The high-level system topology of the Connected Train subsystem is illustrated in Figure 2:

Figure 2 Cisco Connected Rail High-Level System Topology



The role of each component in the Connected Train subsystem design is described in more detail in the rest of this section, along with pertinent architectural details. All devices must comply with the proper standards and certifications for installation onboard a train. These standards are referenced in Standards Compliance, page 26.

Ethernet Switch

The Ethernet switch provides the high-speed backbone network for service transport and delivery. The exact backbone network topology depends upon several operational factors, such as:

- Static or dynamic train consists
- Number and type of wired connections between rail cars
- Number of Ethernet ports required per car and how many of those require Power over Ethernet (PoE)
- Resiliency requirements

If the train consist is static, or mostly static, and if at least 2 wired connections exist between cars, then an Ethernet ring topology is recommended. If only one wired connection is available between cars, or if cars move frequently between consists, then a linear Ethernet topology may be a preferred option.

Whatever topology is deployed onboard the train, topology management and resiliency is achieved through the use of Cisco Resilient Ethernet Protocol (REP). REP is a segment-based protocol that offers rapid detection and recovery of link and node failures for any deployed Ethernet topology. If a rail operator requires that a network be deployed with only open standards protocols, then Multiple Spanning Tree Protocol (MSTP) can be used instead, but will not provide the same recovery performance as REP.

The Ethernet backbone network implements VLANs to provide secure transport of multiple services over a converged network. VLANs provide complete separation of services carried over a common Ethernet infrastructure, allowing for the coexistence of multiple services on a single network.

Deployment of the onboard infrastructure is simplified by the Ethernet switch providing PoE to connected devices such as video cameras, access points, and other devices that support PoE, Including inline power reduces the wiring required to deploy the onboard network, and also provides a centralized manner for deploying power backup systems if required.

Wireless Access Point

The wireless access point (WAP) provides high-speed wireless network access for Passenger services and Enterprise services from the onboard network. Using 802.11-based technology, the access point provides a wireless extension of the onboard network to multiple devices simultaneously. The access point is managed from a centralized WLC within the rail operator's data center or backend network, but is configured to provide local switching of service traffic. This provides the flexibility for users to access service content simultaneously from sources both remote and local to the train.

The number of access points deployed in each car and the position of those access points depends upon several factors. It is desirable to deploy at least two access points per car to avoid a single point of failure for wireless connectivity. A general guideline for Cisco access points scalability is to have no more than 75 wireless clients per access point, so the rail operator or system integrator should evaluate ridership patterns and plan accordingly. Also, single deck cars and double deck cars will have very different radio energy propagation patterns, and the latter may require access points for both decks to properly cover all areas of the car. Finally, nearly all deployment scenarios will benefit from access points with external antenna connections. External antennas permit greater flexibility in deploying the correct antenna design in the correct location within the car, since that location may not permit the installation of the access point itself and the wiring to accommodate it.

The WAPs are able to provide multiple services simultaneously through the use of SSIDs. Each service has a separate SSID to which a device entitled to use that service associates. The access point maps the traffic from each SSID to a separate VLAN tag, thus propagating service separation into the Ethernet backbone network.

Each SSID is configured with the required security and authentication features for the particular service, ranging from no security at all for services such as passenger internet access to username and password and/or certificate-based authentication for enterprise services. The access points support the numerous forms of security outlined in the 802.11 specifications governing access point functionality. A specific list of features can be found on the data sheet for the access point included in the system design, with a link found in Solution Components, page 20

The WAPs work in conjunction with the WLC to provide proper authorization functionality for all services. The WLC can also help facilitate transparent roaming of a client endpoint device for a particular service around the wireless infrastructure, allowing the client to maintain service authorization regardless of the particular access point to which that client is currently associated.

Gateway

A critical role in the Connected Train network design is an onboard gateway to facilitate service traffic routing between the onboard Ethernet network and the offboard Wide Area Network (WAN) connections to the train. This gateway serves as a network edge for onboard service traffic, including any inter-service routing that is required, implements security and QoS functionality, and manages traffic flows over one or more WAN links.

The Connected Rail Solution design implements support in this gateway for both high-speed train-to-trackside wireless networking and 4G/LTE cellular connectivity. These radios are either integrated into the gateway design, in the case of the cellular modems, or connected via Ethernet to the gateway, for the train-to-trackside offboard radios. The gateway supports multiple cellular modems, helping enable connectivity to multiple mobile operators. A rail operator's use of multiple mobile operators may be required to extend the range of network coverage by roaming from one mobile network to another, or to increase the amount of bandwidth available to a train by bonding multiple mobile networks together. A rail operator with a train-to-trackside wireless network deployed may also require cellular connectivity as a backup network mechanism, as a bridge for areas where the trackside network is not yet deployed, or to further increase the available bandwidth.

The onboard gateway works in conjunction with a hub router in the rail operator's data center or backend network to facilitate the management of multiple WAN connections. The onboard gateway and hub router implement a tunneling function that normalizes disparate WAN connections, providing the same service transport path regardless of the WAN connection currently in use. Whether the WAN links are to be used in an active/standby fashion, or bundled together in an active/active load-balancing configuration, to the service traffic it appears to be the same network. The tunneling function also monitors the status of each WAN connection via link status and heartbeat traffic, facilitating detection of any problems on a particular WAN connection.

The onboard gateway ensures that no unauthorized communication is permitted between the different services being transported. By implementing mechanisms such as VLANs, port security, ACLs, and firewall functions, only intended communications are permitted between services. This permits service flows such as access to internet destinations and streaming video from a local onboard server simultaneously to the passenger internet service, while denying any unauthorized access to any enterprise service traffic.

Another key function integrated into the gateway is a GPS receiver, which collects and relays real-time location information about the train. This can work in conjunction with or as a supplement to other location systems that the rail operator has deployed for above-ground rail systems.

Offboard Radio

Some rail operators will look to deploy a system with only Long-Term Evolution (LTE) connectivity to the train, depending upon the service bandwidth needs and cost structure for the LTE services. Many rail operators may have service bandwidth and usage needs that would make deploying LTE connections impractical or too expensive for large-scale production operations. The Connected Rail Solution scope includes a train-to-trackside infrastructure design that supports high throughput and bandwidth for trains. By deploying an Ethernet connected radio with the onboard gateway and regularly spaced trackside base station radios, the rail operator can achieve ~100 Mbps of sustained throughput to a train with no per-megabyte cost for the data transmitted.

The train-to-trackside infrastructure design is best implemented by deploying a pair of radios per gateway onboard the train for connectivity to the trackside infrastructure. The onboard radios constantly monitor the signal quality each is getting from the trackside network, and the radio with the best connection is used for transmitting and receiving. This process allows for the radios to facilitate nearly seamless hand-offs while the train is in motion.

Management of the radios onboard the train is handled through the trackside wireless infrastructure via an in-band management channel, thus facilitating control of all operational aspects from a centralized point.

Video Camera

The Connected Rail Solution design incorporates features and services to provide security monitoring of the train environment. An IP-enabled video camera is required to provide video and audio monitoring of the inside, and potentially outside of, the train. Video cameras are mounted at strategic positions within each car to provide monitoring of entry/exit points, the inside of the car, and other areas requiring security. Different styles of cameras are available to best view the area to be monitored, such directional cameras for focusing on doorways and other ingress/egress locations, and 360 degree cameras for viewing internal areas.

The video camera is connected to the onboard Ethernet switch, providing both power and connectivity to the camera with a single connection. This helps simplify installation of the cameras onboard the train, and aids in placing the cameras in the right position.

The video cameras in the Connected Rail Solution support recording video and audio to different media depending upon the requirements of the rail operator. An onboard server may be installed to provide centralized storage for all cameras within a car. The cameras also support onboard storage to a micro SD card, both as a primary and backup storage media. This assures that critical security video and audio is captured at all times.

The video cameras support the detection of many different events as triggers, such as loud noises and motion detection. These events can be used to trigger different functions in the video surveillance system, the most common of which is to tag the video for prioritized review at a later date. The cameras also support an analog input, allowing for door switches and other contact closures to act as a trigger.

Onboard Server

Several services require the resources of a server for deployment. Some services, such as Video Surveillance, have storage requirements. Others benefit from or require local computing resources for proper deployment. The Connected Rail Solution includes a purpose-built ruggedized server platform to provide these required resources for services deployed onboard the train.

Several special requirements must be designed into a server to be deployed onboard a train. The locations where equipment can be installed in a rail car will not typically be a conditioned environment, so the server must be able to withstand extended temperature and humidity ranges. Also, the environment can be quite dusty, so a fanless sealed case design is necessary. Due to the shock and vibration that can be encountered in a rail application, the server must be designed to provide isolation for components that may be susceptible to these conditions. One specific concern is that a spinning hard drive will eventually encounter faults if subjected to vibration, so the server must support solid-state storage media. Another concern is that dust and vibration will affect cabling connections to the server, so a sealed locking connector design, such as M12 connectors, is a requirement.

While not as common as in other types of vehicles, power loss can be encountered in a train car during the normal procedures of a rail operation. A server should be designed to detect a loss of power, and hibernate or shut down gracefully when power loss is detected, with the time for suspending provided either by an integrated or external battery backup.

In order to provide the capability and flexibility to host multiple services on a single server, a server virtualization environment should be implemented. The Connected Rail Solution design includes VMWare VSphere ESXi or Linux Kernel-based Virtual Machine (KVM) for server virtualization.

Digital Signage

A critical function of the rail operator is providing real-time information about the particular rail line, route progress, and upcoming stations to the passengers onboard the train. To ensure that information is conveyed to the passengers as effectively as possible, a combination of audio prompts and visual information displays is typically implemented. The network infrastructure in the Connected Rail Solution design supports the communications required for deployment and operation of these onboard displays. The design also provides real-time GPS location tracking of the train and can relay that data to the system driving the digital display, providing accurate estimated time of arrival (ETA) calculations and other information.

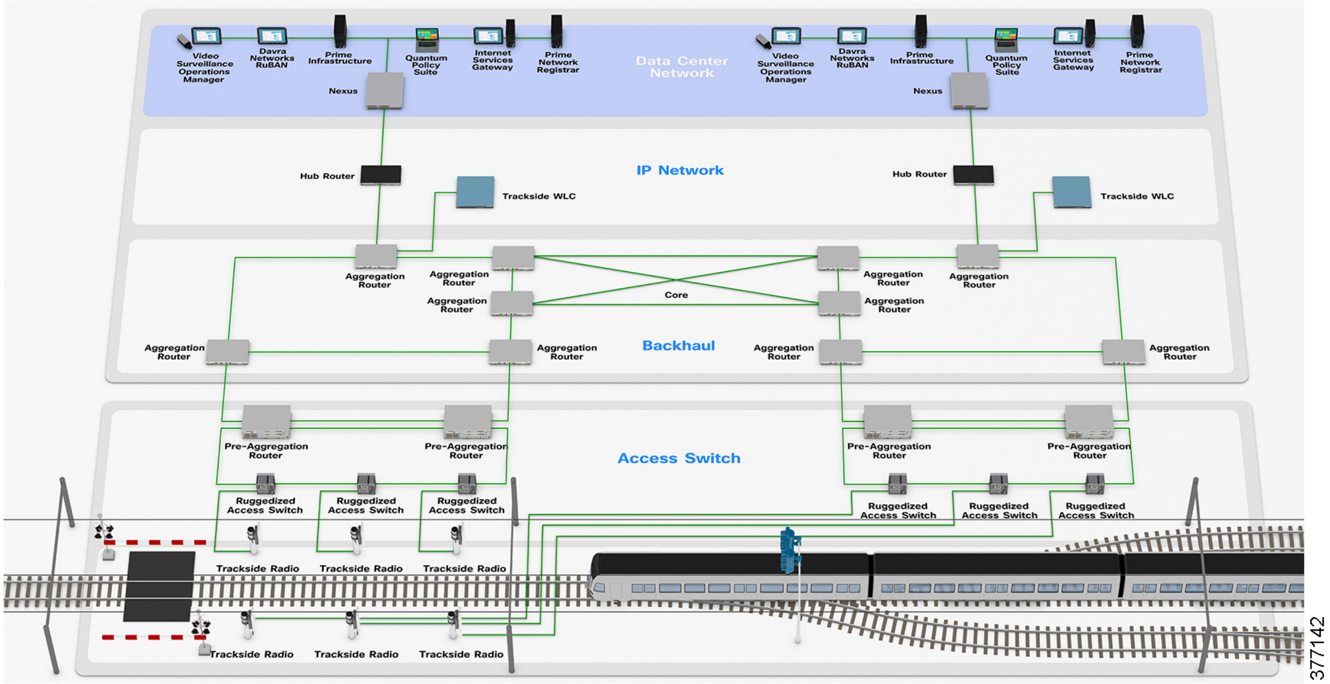
At the same time as providing route information, the digital signage system can simultaneously display advertisements, providing an additional revenue stream for the rail operator. These ads can be displayed in between stops, or can occupy a portion of the screen on a continual basis.

Connected Trackside

The Connected Rail Solution design incorporates a scalable and highly resilient network infrastructure for delivering the service traffic between the trackside wireless connection to the trains and the backend systems such as the Data Center network and Remote Operations Center. This network also helps enable many services to be deployed at the trackside, providing monitoring, signaling, communications and security functions. Finally, the backhaul network connecting the trackside to the backend systems also connects the station networks, providing a cohesive network design and implementation for all the rail operator's service traffic.

The high-level system topology of the Connected Trackside subsystem is illustrated in Figure 3.

Figure 3 High-Level Topology of Connected Trackside Subsystem



The role of each component in the Connected Trackside subsystem design is described in more detail in the rest of this section, along with pertinent architectural details. All devices must comply with the proper standards and certifications for installation onboard a train. These standards are referenced in Standards Compliance, page 26.

Ethernet Switch

The Ethernet switch provides the high-speed access for the trackside wireless base stations and for other trackside deployed services. The exact access network topology depends upon several operational factors such as:

- Deployed fiber layout
- Bandwidth requirements
- Resiliency requirements
- Number of devices requiring PoE

An Ethernet ring topology is recommended if supported by the deployed fiber layout. This provides resilient connectivity while requiring less fiber to be run versus a hub-and-spoke topology. The bandwidth required for each device connected to each Ethernet switch multiplied by the number of switches in a ring will determine the total bandwidth required. To ensure that all service bandwidth is transported in a failure scenario, the total bandwidth required by the services on a ring should not exceed 80% of the available bandwidth on that ring.

Topology management and resiliency in the access network is achieved using Cisco REP, which is a segment-based protocol that offers rapid detection and recovery of link and node failures for any deployed Ethernet topology. If a rail operator requires a network be deployed with only open standards protocols, then MSTP can be used instead, but MSTP will not provide the same recovery performance as REP. To ensure consistent performance, no more than 20 Ethernet nodes should be deployed in a single ring.

The Ethernet access network implements VLANs to provide secure transport of multiple services over a converged network. VLANs provide complete separation of services carried over a common Ethernet infrastructure, allowing for the coexistence of multiple services on a single network.

Trackside Base Station

The Connected Rail Solution scope includes a train-to-trackside infrastructure design that supports high throughput and bandwidth for trains. By deploying an Ethernet connected radio with the onboard gateway and regularly spaced trackside base station radios, the rail operator can achieve ~100 Mbps of sustained throughput to a train with no per-megabyte cost for the data transmitted.

The trackside base station radios are deployed along the track to be covered, and are connected to the Ethernet access network for backhaul. Proper spacing of the radios along the track depends upon several factors, including the track being above ground or subterranean, line-of-sight and obstacles that impede line-of-sight, curves in the track, and elevation of the base station radios. With respect to subterranean deployments, tunnels can often act as a wave guide for the base stations, as well as quell background radiation interference, allowing for reception distances beyond regular open-air and line-of-sight. For above ground installations, a rule of thumb is that the higher the base station radio can be mounted, the further apart the base stations can be placed while maintaining connectivity with trains. Specifically, for deploying base station radios on existing GSM-R poles, which are typically 3 kilometers apart, the radios need to be mounted at a height of 30 meters to maintain proper signal integrity. Note that these are general guidelines, and that any successful deployment along a track requires a thorough site survey to determine optimum base station placement before implementing the trackside network.

Within an access network area, the trackside base station radios will have one root radio, which facilitates communications between the trackside access infrastructure and the base stations. The radios constantly monitor the signal quality each is getting from the pair of radios on a passing train, and the radio pair with the best connection is used for transmitting and receiving. This process allows for the radios to facilitate nearly seamless hand-offs while the train is in motion. To hide this frequent switching of radio pairs from the backhaul network, all traffic is switched via Multiprotocol Label Switching (MPLS) from the active trackside base station to the root base station. With this, from the backhaul network's frame of reference, all traffic appears to be sent and received by the root base station. The root base stations work in conjunction with a hub gateway to facilitate train hand-off between base station areas, providing near seamless hand-off of a train along the entire length of track being covered.

Management of the trackside base stations is handled via an in-band management channel, thus facilitating control of all operational aspects from a centralized point.

Video Camera

The Connected Rail Solution design incorporates features and services to provide security monitoring of the trackside environment. An IP-enabled video camera is required to provide video and audio monitoring of key locations and assets along the trackside. Different styles of cameras are available to best view the area to be monitored, such directional cameras for focusing on specific areas, and 360 degree cameras for viewing wide areas.

The video camera is connected to the trackside Ethernet switch, providing both power and connectivity to the camera with a single connection. This helps simplify installation of the cameras, and aids in placing the cameras in the right position.

The video cameras in the Connected Rail Solution support recording video and audio to different media depending upon the requirements of the rail operator. For fixed position cameras connected to the trackside network, normal deployment is to record video to a centralized server in the rail operator's data center. If the deployment is quite large, distributed data centers may be used to reduce backhaul bandwidth. The cameras also support onboard storage to a micro SD card, both as a primary as well as backup storage media. This assures that critical security video and audio is captured at all times.

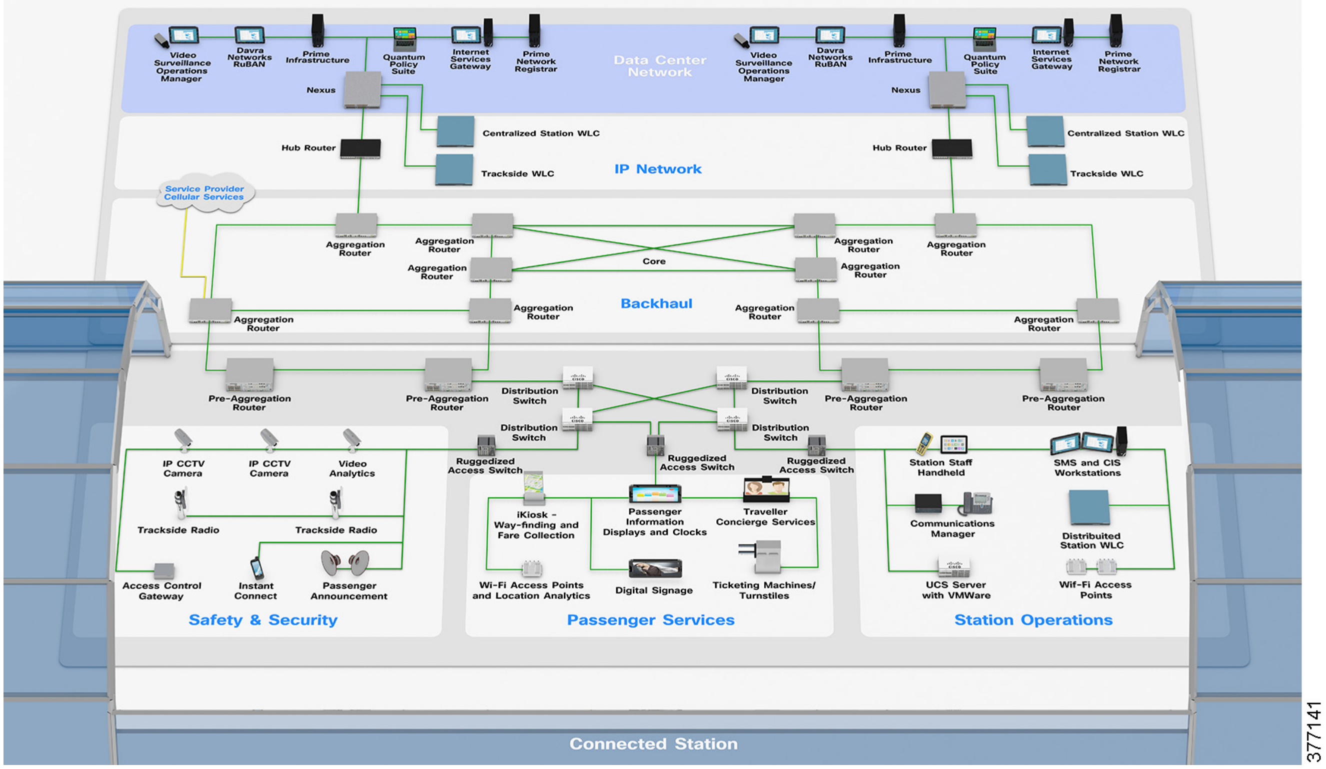
The video cameras support the detection of many different events as triggers, such as loud noises and motion detection. These events can be used to trigger different functions in the video surveillance system, the most common of which is to tag the video for prioritized review at a later date. The cameras also support an analog input, allowing for contact closures to act as a trigger.

Connected Station

The third environment addressed by the Connected Rail solution scope is the rail station. Rail stations range in size and complexity from a simple platform to a retail and transportation complex which rivals the size of large malls. The infrastructure proposed for the Connected Station is able to scale to cover the largest of these scenarios, while still addressing the requirements of smaller deployments. Rail station environments can also vary widely, from a completely outdoor space to a completely indoor space to a combination of the two, while also having requirements and standards compliances specific to rail deployments. The Connected Station incorporates products and elements to address all of these different scenarios.

The high-level system topology of the Connected Station subsystem is illustrated in Figure 4.

Figure 4 High-Level System Topology of the Connected Station Subsystem



The role of each component in the Connected Station subsystem design is described in more detail in the rest of this section, along with pertinent architectural details. All devices must comply with the proper standards and certifications for installation within a rail station environment, with the specific standards depending upon the distance from the track that the equipment is installed, and the function the equipment fulfills. These standards are referenced in Standards Compliance, page 26.

Ethernet Switch

The Ethernet switch provides the high-speed access for all components and services deployed within the Connected Station. This switch provides secure connectivity to the deployed devices, power via Power over Ethernet to devices that support it, and service separation.

If the station infrastructure has an environmentally controlled network room, then enterprise Ethernet switches can be used. In the absence of an environmentally controlled area, ruggedized switches are used.

With the relatively close proximity of equipment to Ethernet switches, a hub-and-spoke topology is usually desirable for a station network deployment. An Ethernet ring can be deployed to accommodate equipment access if needed. Topology management is handled through REP or MSTP as in the other cases.

The Ethernet access network implements VLANs to provide secure transport of multiple services over a converged network. VLANs provide complete separation of services carried over a common Ethernet infrastructure, allowing for the coexistence of multiple services on a single network.

Wireless Access Point

The WAP provides high-speed wireless network access for Passenger services and Enterprise services in the station. The access point is managed from a centralized WLC within the rail operator's data center or backend network, backhauling both control and service traffic. As a rail station has many similar parameters to other high-density public venues, the Connected Rail Solution design uses the best practices developed for Connected Stadiums for Wi-Fi deployment. Details can be found at the following URLs:

- http://www.cisco.com/c/en/us/solutions/industries/sports-entertainment/stadium-wifi.html
- https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3700-series/white-paper-c11-731923.html

Video Camera

The Connected Rail Solution design incorporates features and services to provide security monitoring of the station environment. An IP-enabled video camera is required to provide video and audio monitoring of key locations and assets within the station. Different styles of cameras are available to best view the area to be monitored, such directional cameras for focusing on specific areas, and 360 degree cameras for viewing wide areas.

The video camera is connected to the station Ethernet switch, providing both power and connectivity to the camera with a single connection. This helps simplify installation of the cameras, and aids in placing the cameras in the right position.

The video cameras in the Connected Rail Solution support recording video and audio to different media depending upon the requirements of the rail operator. For fixed position cameras connected to the station network, normal deployment is to record video to a centralized server in the rail operator's data center. If the deployment is quite large, distributed data centers may be used at the station to reduce backhaul bandwidth. The cameras also support onboard storage to a micro SD card, both as a primary as well as backup storage media. This assures that critical security video and audio is captured at all times.

The video cameras support the detection of many different events as triggers, such as loud noises and motion detection. These events can be used to trigger different functions in the video surveillance system, the most common of which is to tag the video for prioritized review at a later date. The cameras also support an analog input, allowing for contact closures to act as a trigger.

Train-to-Trackside Wireless Network

One of the most critical aspects of the Connected Rail Solution design is the train-to-trackside wireless network. Providing a scalable, converged network infrastructure for onboard the train and from the trackside to the backend systems is also important. However, no end-to-end infrastructure exists on which to deliver the services of the Connected Rail Solution without the ability to deliver consistent, high-bandwidth wireless connectivity between the trackside and a train moving at high speed.

Cisco has partnered with Fluidmesh Networks, among other companies, to fulfill this crucial role within the Connected Rail Solution. Fluidmesh Networks offers a suite of wireless products that support their proprietary FLUIDITY track-side and vehicle-to-ground communication system. The Fluidmesh wireless products are able to use existing poles along the track side such as Global System for Mobile - Rail (GSM-R) or Positive Train Control (PTC) poles, thereby reducing the cost of deploying the system. With a pair of radios deployed onboard a train, this approach is able to deliver a constant 100+ Mbps of bandwidth with near-seamless handover time of ~3ms to trains moving up to 300Km/h.

The Fluidmesh FLUIDITY approach provides near seamless roaming implements a patented MPLS-based approach to fast-roaming. The pair of radios onboard the train are configured with one radio to act as a root device. Along the trackside, a root base station is configured for every 15 to 20 base stations deployed, or for the base stations within an access network area. The radios on the train communicate constantly with the trackside base stations within range of the train, electing the best pair of train-to-base-station radios to transmit and receive. To hide this frequent switching of pairs from the wired infrastructure on either side, the current transmit/receive pair of radios uses MPLS switching to forward traffic to the root device on the train and at the trackside. Thus, all data appears to come from the root device, regardless of the radio that is actually sending and receiving at a particular instance. This allows for the best wireless reception possible while avoiding continual churn within the wired network infrastructure.

For larger trackside deployments that include multiple base station areas, Fluidmesh also offers centralized gateway products. The root trackside base stations establish tunnels to the centralized gateway, and the gateway facilitates the hand-off of a train between trackside base station areas.

Cisco and Fluidmesh Networks have spent months of testing, both in the lab as well as in the field, to ensure a seamless end-to-end solution for Connected Rail. More details about this partnership can be found in the Fluidmesh Networks press release available at the following URL:

- https://www.Fluidmesh.com/Fluidmesh-cisco-wifi-trains/

MPLS Backhaul Network

The Connected Rail Solution proposes a single scalable, resilient, multiservice backhaul network design to interconnect the Connected Trackside and Connected Stations to the operator's backend systems. This Unified MPLS-based network design implements the best practices and designs developed for large service providers who have standardized on MPLS for backhaul networks for years. This design has been deployed by many rail operators, and is proven to offer the best design for large-scale network deployments.

The Cisco Connected Rail Solution requires a highly scalable and resilient Metro Network infrastructure to facilitate service traffic transport from the distributed maintenance yards to the Ops Center and backend systems across the Rail operator's geographic region. Cisco promotes a Unified MPLS design for this Metro Network, which easily satisfies all requirements for this network role. The Cisco Unified MPLS Transport network supports:

- Converged Architecture, which is a single network infrastructure supporting Layer 3 Virtual Private Network (L3VPN) services, Layer 2 Virtual Private Network (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.
- Operations, Administrations, and Maintenance (OAM) for fault monitoring and correlation.

The Metro Network design used for the Cisco Connected Rail Solution is thoroughly documented in the *Connected Roadways Design and Implementation Guide* at the following URL:

- https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-10797453

A high-level overview of the design is included here for reference. The Metro Network design consists of the following components:

- **Cisco ASR 900 Routers**—The Cisco ASR 900 line provides both fixed and modular platforms accommodating all necessary interfaces, functionality, and scalability for the Metro Network infrastructure. The Cisco ASR 900 line includes the Cisco ASR 902, Cisco ASR 903, and Cisco ASR 907 modular chassis, and the Cisco ASR 920 fixed configuration routers, all using the IOS-XE system software.

The Unified MPLS model deployed for the Metro Network in the Connected Rail Solution implements Intermediate System to Intermediate System (IS-IS) as the Interior Gateway Protocol (IGP) in a single L1 area, with a flat Label Distribution Protocol (LDP) layer for MPLS Label Switched Path (LSP) transport. Note that if the customer is more familiar with deploying and implementing Open Shortest Path First (OSPF) as an IGP, this is also supported for Unified MPLS networks. This network can scale up to thousands of network nodes and be deployed in both ring and hub-and-spoke topologies. The nodes in the network support gigabit, 10 gigabit (10GE), and even 100 gigabit (100GE) Ethernet interfaces.

The Connected Rail Solution assumes a 10GE ring deployment topology. Yard network connections employ 10 GE links configured for multichassis Link Aggregation Control Protocol (mLACP) port-channel bundles to redundant pre-aggregation nodes (PANs). Connections to the Operations Center infrastructure is via multiple 10GE links configured for mLACP port-channel bundles from redundant Service Edge Nodes (SENs).

All service transport in the Connected Rail Solution is implemented with L3VPNs, which are deployed in the Unified MPLS design through use of Multiprotocol Border Gateway Protocol (MP-BGP) on the nodes at the edge of the Metro Network.

Resiliency and high availability for the Metro Network infrastructure is achieved with the implementation of remote Loop-Free Alternate Fast Reroute (rLFA-FRR). rLFA-FRR is implemented in the IGP layer within the IS-IS configuration, and pre-calculates spatially diverse alternate routing paths for every prefix in the IGP routing table regardless of network topology, allowing for extremely rapid failover when link or node failures occur in the Metro Network. Protection at the service-level is further enhanced with the implementation of Fast Reroute (FRR) in Border Gateway Protocol (BGP).

Solution Components

This section, which lists the Cisco and third party components included in the Cisco Connected Rail Solution scope, includes the following major topics:

- Cisco Components, page 20
- Third Party Components, page 20

Cisco Components

Table 2 lists Cisco components used in the Connected Rail Solution.

Table 2 Cisco Components

Hardware	Software Release	Role
Cisco IW3702-4E-x-K9	Release 8.2	Onboard wireless access point and station wireless access point
Cisco CIVS-IPC-3050 / CIVS-IPC-7070	Release 2.8	IP video surveillance camera. These cameras are not fully EN50155 compliant, so applicability for onboard deployment must be verified first.
Cisco AIR-CT5508	Release 8.2	Wireless LAN controller for Cisco IW3702 access points.
Cisco IE-2000 IP67	IOS 15.2(4)EA1	Onboard Ethernet switch. This switch is not fully EN50155 compliant, so applicability for onboard deployment must be verified first.
Cisco ASR 1000	IOS-XE 3.16.1aS	Local Mobility Anchor (LMA) for Klas onboard mobile gateways
Cisco UCS	--	Server platform for hosting Lilee vLMC, Davra RuBAN, and other service platforms.
Cisco IE-4000	IOS 15.2(4)EA1	Ruggedized Gigabit Ethernet Trackside access switch
Cisco ASR 920	XE 3.18.0S	Unified MPLS capable fixed configuration pre-aggregation router node with GE and 10GE interface support for trackside pre-aggregation.
Cisco ASR 903	XE 3.18.0S	Unified MPLS capable modular aggregation router node with GE, 10GE, and 100GE interface support for backhaul pre-aggregation / aggregation node.

Third Party Components

Table 3 lists Third Party components used in the Connected Rail Solution.

Table 3 Third Party Components

Hardware	Software Release	Role
Klas Telecom TRX-R2/R6	ESR5921 IOS 15.6(2)T	Onboard mobile gateway
Klas Telecom TRX-S10/S26	ESS2020 IOS 15.2(4)EA1	Onboard Ethernet switch with mechanical bypass
Lilee Systems LMS-2450-ME-100	LileeOS Release 3.1	Onboard mobile gateway

Table 3 Third Party Components

Hardware	Software Release	Role
Lilee Virtual LMC (vLMC)	LileeOS Release 3.1	Lilee Mobility Controller for Lilee onboard gateways
Fluidmesh FM4200	Release 8.1	Offboarding Onboard radio for train to track communication
Fluidmesh FM3200	Release 8.1	Trackside wireless radio

Solution Functional Considerations

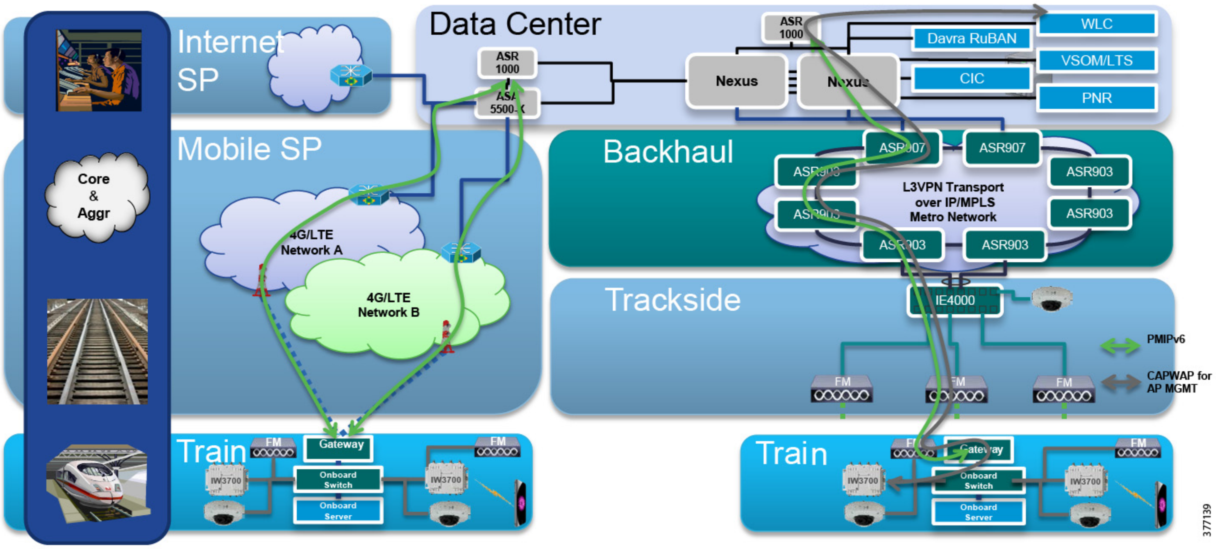
This section details the end-to-end Solution level functions that span across individual roles within the Solution.

- Solution Infrastructure Design, page 21
- Passenger Wi-Fi Entitlement, page 24
- Data Center, page 25
- QoS Model, page 25
- Standards Compliance, page 26
- Network Management System, page 27

Solution Infrastructure Design

As highlighted in Solution Architecture, page 9, the Connected Rail Solution design includes a highly-scalable and resilient end-to-end transport infrastructure, incorporating the best design practices and methodologies for each system area. This serves as the basis for delivering all the services described in Solution Supported Services and Models, page 2. Sitting between the transport infrastructure and service layers is an end-to-end abstraction design which helps deliver services across both the static areas (Station and Trackside) and dynamic areas (Trains) of the Connected Rail Solution.

Figure 5 Connected Rail High-Level Architecture



Service Transport

A critical function of the Connected Rail Solution is the efficient transport of services to and from trains. Whereas service transport from fixed assets along the Trackside and at the Station can employ standard Enterprise and MPLS network designs, as previously detailed in the Backhaul Network section, transport from the moving network infrastructure onboard the Train requires special considerations. The Connected Rail Solution implements one of two service transport mechanisms, depending upon the onboard gateway being used:

- Proxy Mobile IPv6 (PMIPv6) for the Klas Telecom TRX-R6 gateway or
- Datagram Transport Layer Security (DTLS) for the Lilee LMAS-2450-ME-100 gateway

Both mechanisms are able to deliver scalable service delivery over multiple WAN links.

Proxy Mobile IPv6 (PMIPv6)

Proxy Mobile IP version 6 (PMIPv6) provides an abstraction layer over the physical network between the onboard network and the data center by encapsulating service traffic in a tunnel. This tunnel is established between Mobile Access Gateway (MAG), a function implemented by the onboard gateway on the train, and the LMA, a function implemented in the hub router in the operator's data center. This permits the network addressing and routing design on the train to remain constant, regardless of the train location or WAN link in use, thus facilitating a seamless connectivity design to transport all service traffic.

- The Local Mobility Anchor (LMA) is the home agent for a mobile node (MN) in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol.
- The Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links, which are the onboard network infrastructure nodes in this case. MAG is the access router for the MN; that is, MAG is the first-hop router in the localized mobility management infrastructure.

A common requirement among rail operators is the utilization of multiple WAN links, in the form of multiple LTE modems and/or a private wireless network deployed along the trackside. PMIPv6 implements a feature called Dynamic Multipath that manages these multiple paths between the MAG and LMA nodes. This multipath support helps enable the MAG to select any one of the paths on priority basis, or select all the existing network paths simultaneously to create tunnels to reach LMA. The Multipath Management feature helps enable PMIPv6 to choose from multiple available links which have different access technologies. All available paths are constantly monitored using PMIPv6 heartbeat messages, which can be tuned to the operator's preferences. Link preferences can be assigned to various types of traffic by defining mobile maps.

To enable ease of segmentation of the train networks from the rest of the rail operator's network infrastructure, dynamic address pools for DHCP usage are administered on the LMA router.

Onboard networks behind the MAG are represented to PMIPv6 as Logical Mobile Nodes (LMN). This means that the MAG will advertise its direct knowledge of the onboard subnets to the LMA. The MAG also serves as the DHCP server for the devices in the onboard network.

If Layer 2 backhaul for any other services is required, then Ethernet over GRE tunneling may be implemented in conjunction with PMIPv6 to provide a Layer 2 transport path.

This PMIPv6 approach is able to support both single onboard gateway and redundant onboard gateway deployments. Special considerations are required when designing a redundant gateway deployment. If an active-standby deployment is desired, then minimal design accommodations need to be made. Virtual Router Redundancy Protocol (VRRP) is configured on the primary and standby gateways for all service VLANs requiring redundancy, which establishes a virtual gateway instance between both gateways. Heartbeat messages are exchanged between the primary and standby gateways to monitor the health of the primary gateway. If a problem is detected, the standby gateway takes over the virtual gateway instance, thus preserving service traffic transport. Once the primary gateway is reestablished, that gateway resumes service traffic transport.

For an active-active redundant onboard gateway deployment, the onboard infrastructure is configured with two VLANs for each service. One VLAN directs service traffic to one gateway, and the other VLAN directs service traffic to the other gateway. The rail operator can split the service traffic on onboard infrastructure between these two VLANs in whatever fashion best serves the operator's needs. This provides a completely deterministic division of service traffic between the two active gateways. Each gateway is configured as a VRRP standby router for the VLANs that are active on the other gateway, allowing for a single gateway to handle all service traffic in a failure scenario. In this way, both load-balancing and redundancy are achieved for the onboard network.

Datagram Transport Layer Security (DTLS)

An alternative approach for deploying the onboard gateway and hub router functions is provided by Lilee Systems. This approach establishes a Layer 2 mobility tunnel between the Lilee Mobility Controller (LMC) and onboard gateway (LMAS-2450-ME-100) over each WAN link with DTLS. Link aggregation then groups all of these tunnels together into a single logical link. The LMC and onboard gateway coordinate to monitor and manage traffic flows over all WAN links to provide failover and dynamic weighted load balancing. This approach supports the following functions:

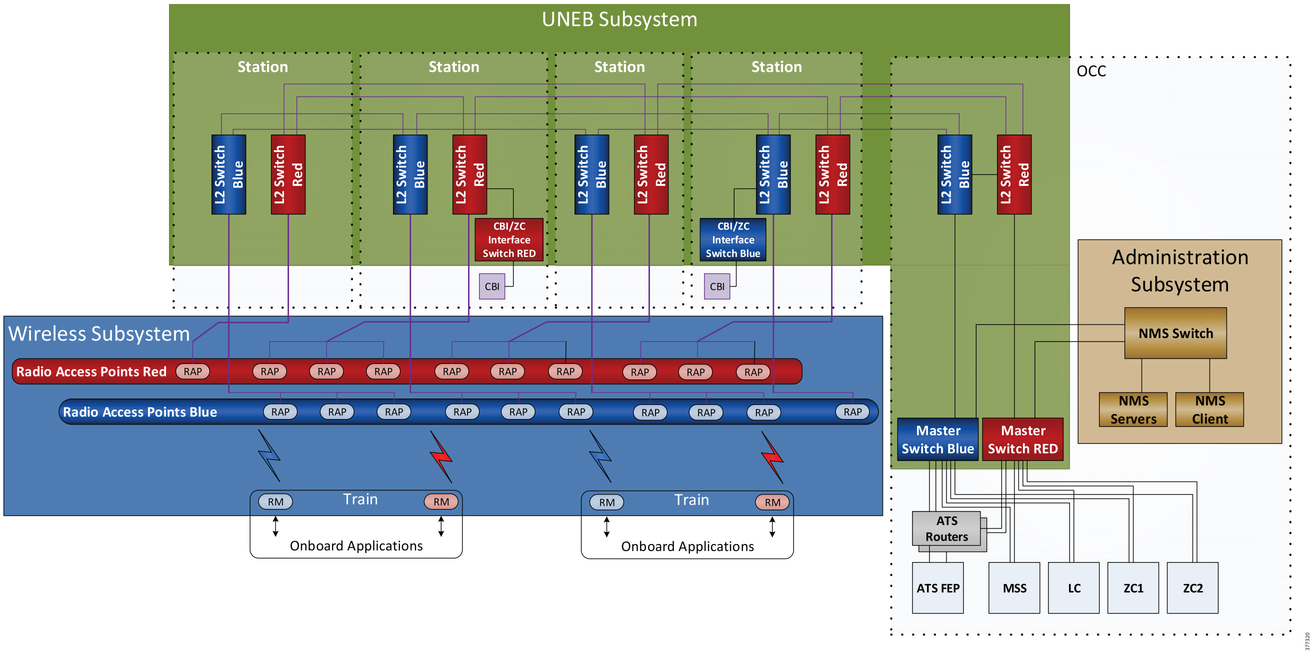
- Management of multiple WAN paths to/from a rail car or train.
- Ability to define traffic load-balance characteristics between WAN links, including proportioning of traffic loads.
- Ability to monitor WAN link availability via heartbeat packets.

This approach is suited for a single onboard gateway deployment on a train consist, or deployed per-car without redundant inter-car links. Deployments requiring redundant gateway deployments should use the PMIPv6 approach previously described.

Communications-Based Train Control

Deployment of a Communications-Based Train Control (CBTC) service requires special considerations when designing and deploying the end-to-end transport network. With the critical nature of transporting control traffic, the general consensus in the industry is that a lossless network design must be employed. While network equipment and network designs have progressed to reduce packet loss to a minimum due to link and node failures, a single network infrastructure is not able to provide lossless traffic delivery under all failure scenarios. Therefore, the design for deploying a CBTC service uses two parallel, spatially diverse networks to transport control traffic.

Figure 6 Communications-Based Train Control



The two transport networks are completely separate in this scenario, with one referred to as the "Red" network and the other as the "Blue" network. These two networks do not share any common components or links, from the Operations Control Center (OCC) to the trackside WAPs and onboard the train itself. This helps ensure that a failure of any component will only affect one network. The only components that connect to both the Red and Blue networks are the Automated Train Supervision (ATS) system in the OCC, and the Automatic Train Protection (ATP) and Automatic Train Operation (ATO) systems onboard the train. Any communications sent by the ATS, ATP, or ATO systems are replicated on both transport networks. This methodology of parallel networks for deploying CBTC ensures that, in the event of a network issue, at least one copy of the transmitted command is received by the far end.

In addition to being very sensitive to packet loss, CBTC services also have very strict latency requirements. Due primarily to these criteria, rail operators will typically deploy a dedicated network infrastructure for CBTC services, thus avoiding any chance of contention for networking resources from other service traffic. The Cisco Connected Rail Solution implements a comprehensive end-to-end QoS model that ensures the prioritization and delivery of critical service traffic such as CBTC over other services. This allows rail operators to place CBTC traffic on a network transporting other services at such time as the industry moves to being more comfortable with this concept.

The last aspect to consider in CBTC deployment is differential latency, or the difference in latency encountered by the same instruction packet traveling across each parallel network. When designing the two parallel networks, it is important to keep the designs as similar as possible to each other. The following aspects should be considered in the design:

- The number of end-to-end network nodes, and the type of each node, needs to be the same in each network, thus ensuring that the transitional latency through each node is as similar as possible.
- The length of the network connection between corresponding network nodes in each network should be as similar as possible, to ensure that propagation latency is as similar as possible. The propagation delay in both fiber optic and copper cables is typically 5-5.5 microseconds per kilometer.

Passenger Wi-Fi Entitlement

The Cisco Connected Rail solution scope provides management of subscriber authorization and entitlement for the Passenger Wi-Fi Services, both onboard a train as well as when the passenger is in the station. As previously described, due to certain service factors, the Wi-Fi infrastructure is deployed somewhat differently in each of these locations:

- For Passenger Wi-Fi Services onboard the train, the Wi-Fi infrastructure is deployed in FlexConnect mode, allowing for access to local resources onboard the train for aspects such as on-demand entertainment on personal devices. Only access point control traffic is tunneled from the train to the WLC.
- For Passenger Wi-Fi Services within a station, the best practices for high density wireless deployment from the Cisco Connected Stadium solution are implemented. This deploys the Wi-Fi infrastructure in Centralized mode, tunneling all passenger device traffic through the WLC in addition to access point control traffic.

For ease of management and for operational simplicity for each infrastructure, deploying these two different infrastructures in these two different manners dictates the use of two separate WLCs. When associating to each infrastructure for the first time, a passenger will be prompted by a portal landing page for login or other authorization credentials. Each subsequent access to each infrastructure will be remembered by the system, and the passenger will be transparently allowed access to the Wi-Fi network. The time period for which the passenger will be authorized can be controlled by the rail operator.

For portal-based deployments, the landing page is hosted by the Cisco EMSP. Cisco EMSP provides a rich content platform for handling user authorization and entitlement, as well as serving context-aware advertisement and other content via the portal page. The WLC controlling the access point redirects the connection request to the EMSP portal. Further details on implementing Cisco EMSP are available in the Radio Resource Management chapter of the *Cisco Wireless Controller Configuration Guide, Release 8.2* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_011000.html

An alternative approach to a portal-based authorization mechanism is to implement configuration profiles. The rail operator can download a configuration profile to the passenger's device through an application or a portal page, with the passenger's permission, prior to using the Wi-Fi system for the first time. This will allow the passenger's device to be pre-configured to join the Wi-Fi systems both on the train and at the station when the device is within range of either system. An added benefit of this approach is the ability to use WPA encryption to communicate with the passenger's device, thus preventing any potential wireless sniffing attacks. This type of mechanism can be implemented and managed by the Connected Rail Solution.

Data Center

All centralized Solution aspects and backend services of the Connected Rail Solution are hosted in a Data Center environment. The *Cisco Enterprise Data Center Design and Implementation Guide* provides detailed designs and best practices for deploying highly-scalable Data Center environments, and thus is the basis for any Data Center-related design considerations within the Connected Rail scope. For more information, see the following URL:

- http://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-data-center-networking/index. html

QoS Model

The Connected Rail Solution implements services that require end-to-end priority treatment to guarantee proper functionality, by ensuring that critical system traffic is prioritized for queuing and scheduling over lower priority services.

QoS classification is accomplished in several ways, depending upon the network medium:

- IP Differentiated Services Code Point (DSCP) classification for IP Layer 3 transport
- 802.1p Class of Service (CoS) classification for Ethernet Layer 2 and Fluidmesh transport
- Wi-Fi Multimedia (WMM) classification for Wi-Fi wireless transport
- LTE QoS Class Identifier (QCI) classification for LTE wireless transport

All of these QoS classification mechanisms are used in the Connected Rail Solution, with mapping between these mechanisms supported at the boundaries between the different transport mechanisms.

The classes of service shown in Table 4 are implemented in the Connected Rail solution, and are shown with mappings between representative classification markings for each type of classification.

Table 4 QoS Classifications

Traffic Class	DSCP	802.1p CoS	WMM Class	LTE QCI
Management	CS7	7	6 (Platinum)	8
Control	CS6	6	6 (Platinum)	6
Real Time (Voice)	EF	5	6 (Platinum)	1
Video	CS4	4	5 (Gold)	2
GPS/Telematics	CS2	2	0 (Silver)	6
Best Effort	CS0	0	1 (Bronze)	9

In the Connected Rail Solution, the following locations in the network are the most important to focus on for deploying queuing and scheduling, as it is at these points where congestion will be encountered:

- **LTE Cellular Connectivity to and from the Train**—In typical conditions, an LTE connection to a moving train will be expected to support 10 to 20 Mbps of throughput. Ideally, the Mobile Service Provider will support multiple LTE QCI values for the service provided to the Rail operator, and prioritization of expedited forwarding (EF) and assured forwarding (AF) classes over best effort (BE) traffic can be guaranteed in both directions. If the Mobile SP does not offer multiple QCI classes, then prioritization of EF and AF traffic can still be accomplished in the upstream direction from the Klas gateway toward the Mobile Service Provider. In either situation, the LTE connection will have less bandwidth than the other wired and wireless links feeding traffic into the gateway. A QoS policy is deployed on the interface port of the ESR 5921 router within the Klas gateway, with classes defining the proper queuing treatment for each class. Currently, the LTE interfaces in the Klas gateway map traffic to LTE QCI classes via source and destination IP address, so having service specific IP subnets and hub sites will result in proper traffic scheduling and treatment.

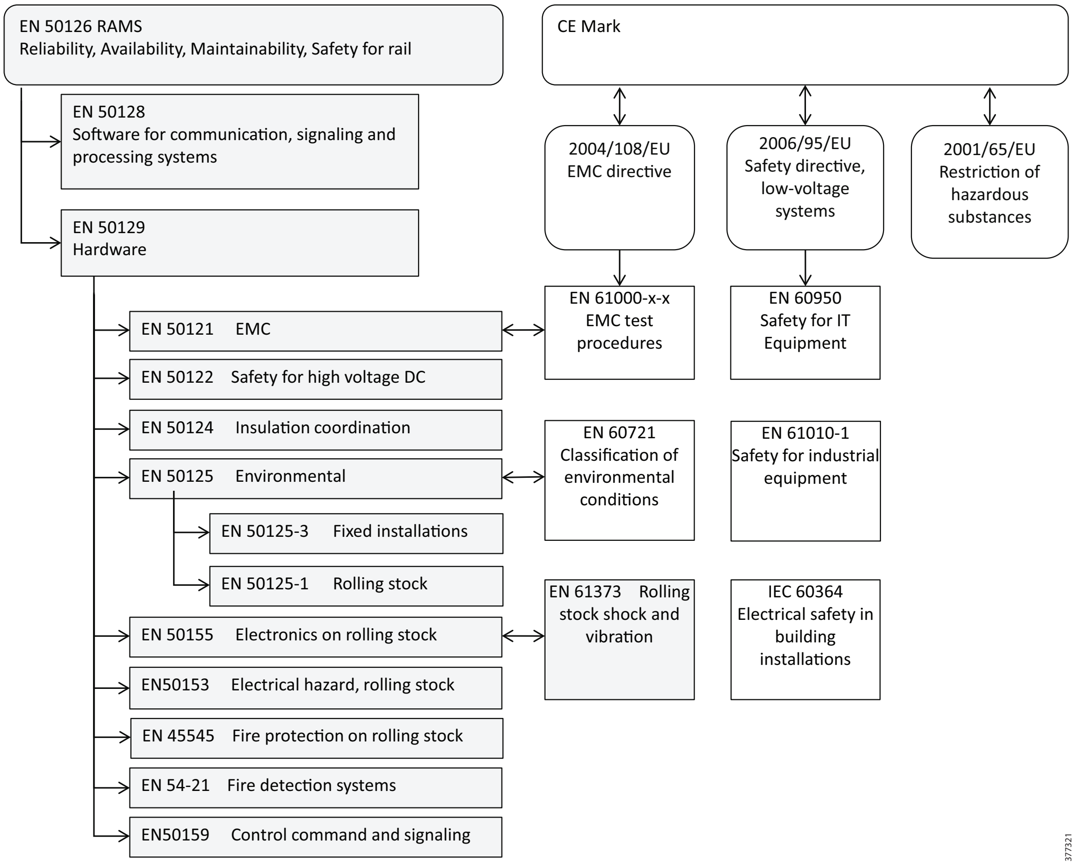
- **The Edges of the Transport Network**—The Connected Trackside network design calls for gigabit Ethernet links in the access network, and 10 gigabit Ethernet links in the aggregation network. Uplinks from the aggregation network to the data center and operations center can be 10 gigabit or 100 gigabit, depending upon scalability requirements. As such, this network will not likely encounter much congestion under normal circumstances. However, it is still important to deploy QoS to prioritize EF and AF traffic over BE traffic, to ensure that critical services such as VoIP communications and Video Surveillance function without any interference potential traffic surges. All of these links are using the available line rate of the underlying physical connection, and a flat QoS policy to define the proper queuing treatment for each class is implemented.

- **Internet Peering Connections to the Mobile SP and Internet SP**—The bandwidth of the service purchased from a service provider will often be less than the physical capacity of the link providing the service. In this case, a hierarchical QoS policy is used on the uplink connection of the peering router from the rail operator's network, with a parent shaper equal to the bandwidth of the service and child classes defining the proper queuing treatment for each class. Even in the case where the service bandwidth is equal to the physical bandwidth of the link, a parent shaper can help in smoothing traffic flow toward the SP and yielding better application throughput versus relying on the port physical layer (PHY) to indiscriminately drop excess packets.

Standards Compliance

As part of the Connected Rail Solution development, Cisco has conducted a thorough analysis of relevant rail-related standards. Figure 7 illustrates those standards and their relationship to each other.

Figure 7 Relationships of Key Rail Compliance Standards


EN 50126 RAMS
Reliability, Availability, Maintainability, Safety for rail
EN 50128
Software for communication, signaling and processing systems
EN 50129
Hardware
EN 50121 EMC
EN 50122 Safety for high voltage DC
EN 50124 Insulation coordination
EN 50125 Environmental
EN 50125-3 Fixed installations
EN 50125-1 Rolling stock
EN 50155 Electronics on rolling stock
EN50153 Electrical hazard, rolling stock
EN 45545 Fire protection on rolling stock
EN 54-21 Fire detection systems
EN50159 Control command and signaling
CE Mark
2004/108/EU
EMC directive
2006/95/EU
Safety directive, low-voltage systems
2001/65/EU
Restriction of hazardous substances
EN 61000-x-x
EMC test procedures
EN 60950
Safety for IT Equipment
EN 60721
Classification of environmental conditions
EN 61010-1
Safety for industrial equipment
EN 61373 Rolling stock shock and vibration
IEC 60364
Electrical safety in building installations
377321

Unless otherwise noted, all products proposed in this Solution are compliant with the necessary standards required for the location in which that product will be deployed, whether it be onboard the train, at the trackside, or within the station. Information regarding device compliance is available upon request.

Network Management System

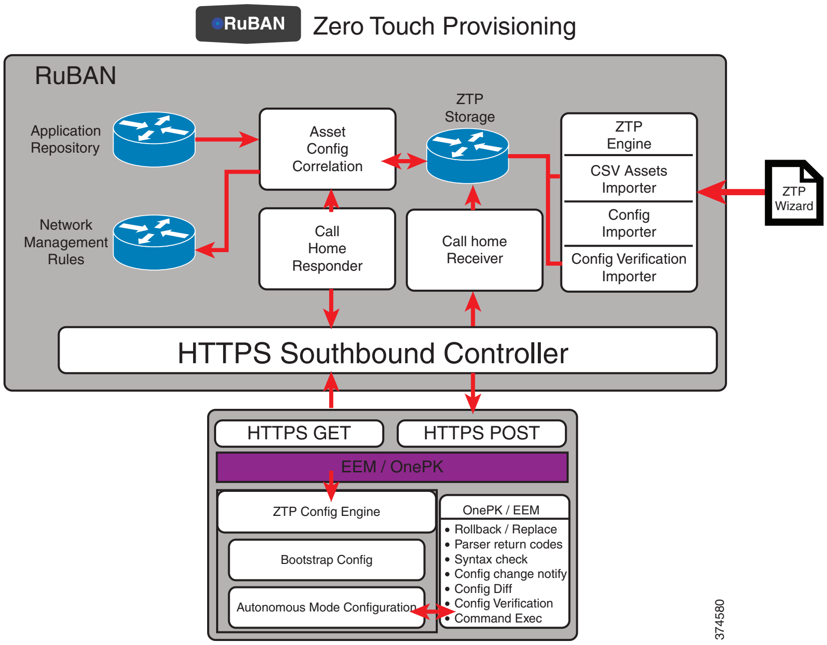
Given the transportation-specific aspects of the Connected Rail Solution scope, the number of third party systems involved, and the targeted customers, a transportation-specific network management system is warranted. Cisco is partnering with Davra Networks to integrate the RuBAN IoT Management system into the Connected Rail Solution. RuBAN provides a transportation-focused management platform which supports provisioning, monitoring, and troubleshooting of both Cisco and third party elements in the Solution scope. See the following URL:

- http://www.davranetworks.com/product/features

RuBAN provides integrated network element management for the Connected Rail Solution, including initial provisioning for field deployment of new devices as well as " Day 2" management and monitoring. The RuBAN platform is capable of communicating with the devices under management via IPv4 and IPv6, providing comprehensive coverage of the elements deployed in the Connected Rail Solution design.

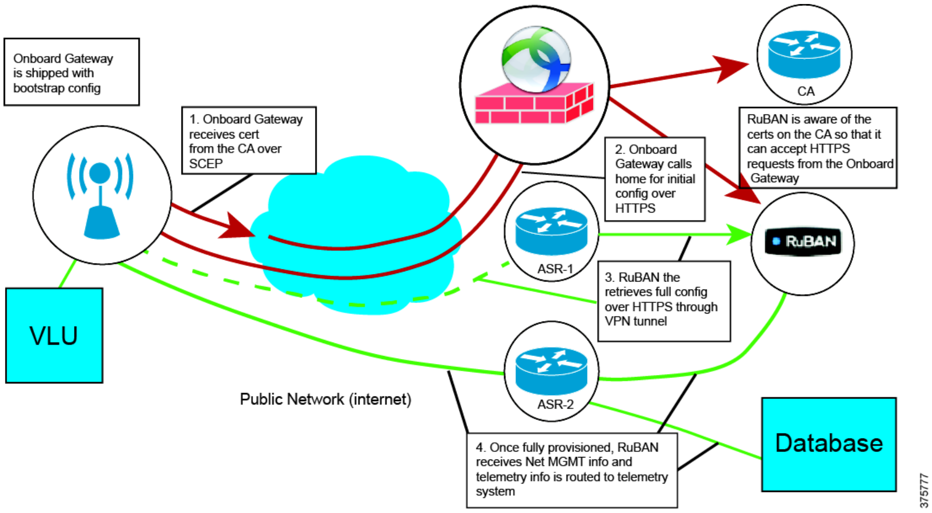
Figure 8 provides an overview of the southbound interface between the RuBAN system and the Cisco devices deployed in the network.

Figure 8 RuBAN Southbound Interface Overview



The required initial configuration for Cisco devices is loaded as part of a ConfigExpress configuration that is specified at the time of ordering the devices. This initial configuration will enable the devices to " call-home" to the RuBAN system, providing a connection for further device configuration. An overview of this workflow is illustrated in Figure 9.

Figure 9 RuBAN Network Element Management Deployment Workflow


Onboard Gateway is shipped with bootstrap config
1. Onboard Gateway receives cert from the CA over SCEP
CA
RuBAN is aware of the certs on the CA so that it can accept HTTPS requests from the Onboard Gateway
2. Onboard Gateway calls home for initial config over HTTPS
RuBAN
ASR-1
3. RuBAN the retrieves full config over HTTPS through VPN tunnel
VLU
Public Network (internet)
ASR-2
4. Once fully provisioned, RuBAN receives Net MGMT info and telemetry info is routed to telemetry system
Database
375777

1. The device to be controlled obtains a certificate from the Certificate Authority (CA) server via Simple Certificate Enrollment Protocol (SCEP). RuBAN is aware of retrieved certificates, so it can accept HTTPS connections from the devices.

2. The device " calls home" to the RuBAN system to download the initial configuration via HTTPS

3. Once downloaded, RuBAN then downloads the remainder of the full configuration to the device over HTTPS through either the Management Network or VPN tunnel.

4. When fully provisioned, the RuBAN system receives network monitoring information and alerts from the devices. Telemetry info is routed to the Telemetry Database system.

The RuBAN platform provides real-time monitoring of network performance and alerts, to help facilitate troubleshooting of any issues that arise during normal network operations. In addition, the RuBAN platform integrates Geolocation information, so that the precise location of trains and other mobile components is available in real-time.

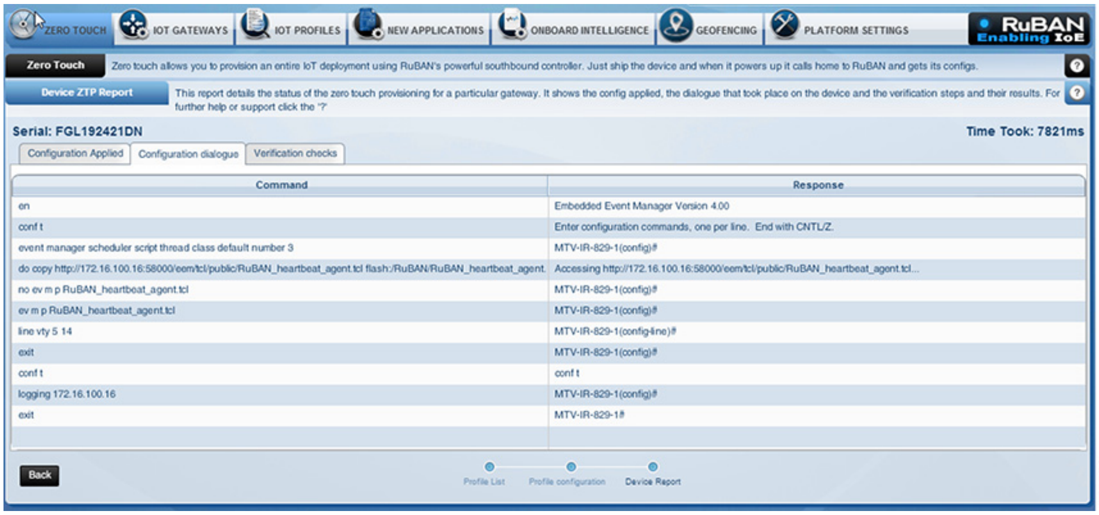
Management User Interface

This section provides examples of the different management functions and corresponding user interface screens offered by the Davra RuBAN system. Details on how each function is used is covered in the Connected Rail Implementation Guide.

Provisioning

The Provisioning Interface (shown in Figure 10) covers infrastructure and service provisioning and monitoring functions for equipment deployed on the trains.

Figure 10 RuBAN Provisioning Interface



Zero touch allows you to provision an entire IoT deployment using RuBAN's powerful southbound controller. Just ship the device and when it powers up it calls home to RuBAN and gets its configs.

This report details the status of the zero touch provisioning for a particular gateway. It shows the config applied, the dialogue that took place on the device and the verification steps and their results. For further help or support click the '?'

Serial: FGL192421DN

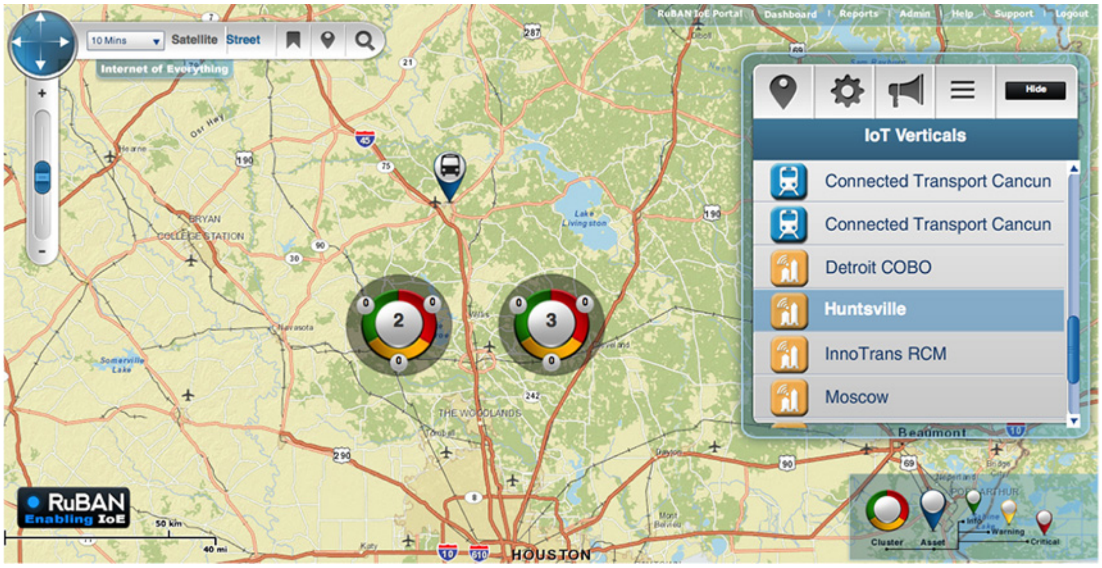
Time Took: 7821ms

Command	Response
en	Embedded Event Manager Version 4.00
conf t	Enter configuration commands, one per line. End with CNTL/Z.
event manager scheduler script thread class default number 3	MTV-IR-829-1(config)#
do copy http://172.16.100.16:58000/eem/tcl/public/RuBAN_heartbeat_agent.tcl flash:/RuBAN/RuBAN_heartbeat_agent.	Accessing http://172.16.100.16:58000/eem/tcl/public/RuBAN_heartbeat_agent.tcl...
no ev m p RuBAN_heartbeat_agent.tcl	MTV-IR-829-1(config)#
ev m p RuBAN_heartbeat_agent.tcl	MTV-IR-829-1(config)#
line vty 5 14	MTV-IR-829-1(config-line)#
exit	MTV-IR-829-1(config)#
conf t	conf t
logging 172.16.100.16	MTV-IR-829-1(config)#
exit	MTV-IR-829-1#

Train Tracking

The Train Tracking Interface (shown in Figure 11) provides an overhead map view of the area covered by the Rail operator, with a real-time overlay of the location of all vehicles in service within that area. Clicking on a train will display more detailed information and dashboards available for that train. Also, integrated access is available to the VSOM system, allowing the dispatcher to pull up video surveillance within the same interface.

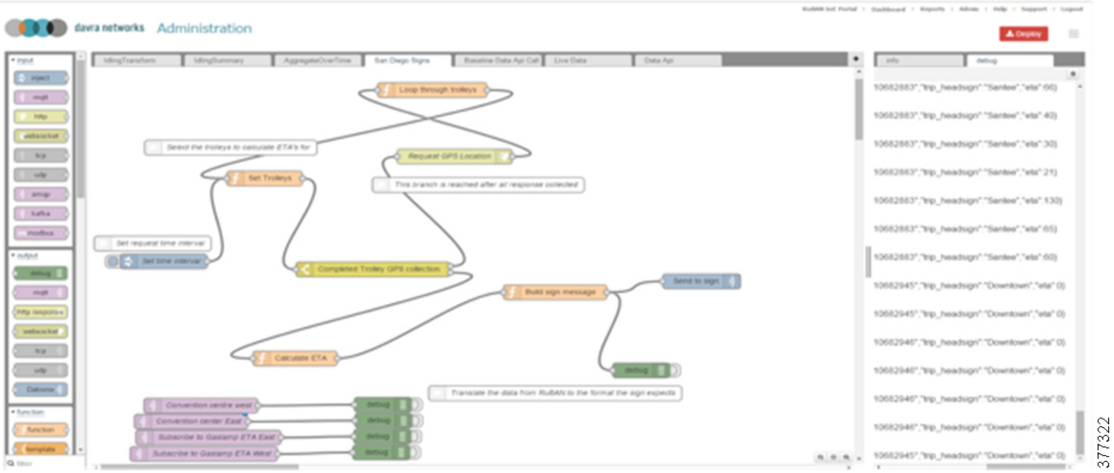
Figure 11 Vehicle Tracking Interface



Passenger Information System ETA Interface

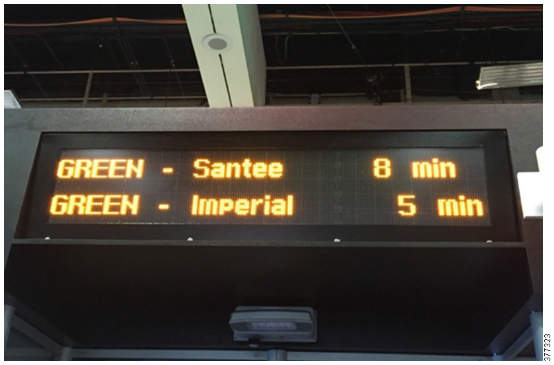
The Passenger Information System ETA interface (see Figure 12 and Figure 13) allows the Rail operator to customize the input data, data flow and criteria for ETA calculation, and output mechanism for the ETA data to the Rail operator's digital display systems at stations, at stops, and even onboard the trains.

Figure 12 Passenger Information System ETA Interface



```
10682883","trip_headsign":"Santee","eta":66}
10682883","trip_headsign":"Santee","eta":40}
10682883","trip_headsign":"Santee","eta":30}
10682883","trip_headsign":"Santee","eta":21}
10682883","trip_headsign":"Santee","eta":130}
10682883","trip_headsign":"Santee","eta":65}
10682883","trip_headsign":"Santee","eta":60}
10682945","trip_headsign":"Downtown","eta":0}
10682945","trip_headsign":"Downtown","eta":0}
10682946","trip_headsign":"Downtown","eta":0}
10682946","trip_headsign":"Downtown","eta":0}
10682946","trip_headsign":"Downtown","eta":0}
10682946","trip_headsign":"Downtown","eta":0}
10682945","trip_headsign":"Downtown","eta":0}
```

Figure 13 Passenger Information Display Example



Security, High Availability, and Scale

This chapter includes the following major topics:

- Security Considerations, page 31
- High Availability Considerations, page 32
- Scalability Considerations, page 33

Security Considerations

The Connected Rail Solution implements security mechanisms throughout the design to provide proper service traffic protection, separation, and system authorization. The various mechanisms and methodologies implemented are described in this section.

Service separation is maintained via the use of 802.1q VLAN tags within native Ethernet networks, and MPLS tags within MPLS networks. These tags maintain total separation between services being carried on a converged transport network. All inter-service routing, such as that required for access to on-demand video entertainment onboard the train from passenger smart devices, should be restricted via ACLs to only permit specific IP addresses and ports required to enable the service. This limits potential attack vectors from other services. In general, the rule of ACL implementation is to filter traffic as specifically as possible, and as close to the edge of the network as possible.

The Wi-Fi SSIDs for enterprise and law enforcement access implement WPA2 Enterprise security, which includes enterprise level authorization and encryption of traffic. The Wi-Fi sub-system also supports Extensible Authentication Protocol (EAP), Lightweight Extensible Authentication Protocol (LEAP), Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Wi-Fi Protected Access (WPA), and Temporal Key Integrity Protocol (TKIP). Passenger wireless internet access deploys that is deployed with an open SSID employs a centralized system to manage authorization and entitlement.

All network nodes in the Connected Rail Solution support being managed and monitored remotely from the operations center via the following secure methods: SNMP v2/v3, SSH, HTTP/HTTPS. The Davra RuBAN system uses HTTPS for communication with the network nodes in the system design, providing for secure management of the network infrastructure.

Any network interface that could be exposed to physical access by untrusted persons, be it located on the train, along the track, or in the station, has port security with 802.1X authorization enabled to prevent unauthorized access to the network infrastructure. All wireless access to enterprise infrastructure is secured by WPA2 username/password and/or certificate-based authorization, depending upon which mechanism is implemented by the rail operator. Cisco provides full Mobile Device Management (MDM) functionality for secure mobile device deployment, which is fully compatible with the Connected Rail solution.

Outside access to the operations center infrastructure via user-to-network (UNI) connections to the Mobile SP and Internet SP is protected by a Cisco Adaptive Security Appliance (ASA) series security node. The ASA node prevents any unauthorized access and attacks from external networks by implementing the security designs and best practices recommended by Cisco for Enterprise Networks. More details are available at the following URL:

- http://www.cisco.com/c/r/en/us/internet-of-everything-ioe/security/technology/index.html

If required, the Connected Rail Solution supports network layer security between the train onboard gateway and hub router at in the data center for all enterprise applications and services. The Klas model implements IPSec VPN tunnels within the PMIPv6 infrastructure, and the Lilee model implements tunnels with DTLS. The IPSec approach is capable of supporting many different encryption standards: DES, 3DES, AES 128, AES 192, and AES 256. The Connected Rail solution recommends implementing the strongest standard and largest keys supported to provide the most secure connection.

High Availability Considerations

The network infrastructure onboard the train implements an Ethernet ring design that uses Cisco REP to manage topology changes. This protocol supports ~50msec detection and failover in the case of a link or node failure. If the operator requires a standards-based approach to the onboard train network, then MSTP is implemented instead, albeit with slower failure detection and failover performance. The network infrastructure components used on the train all incorporate ruggedized design and construction, resistance to shock and vibration effects, and extended temperature range functionality to ensure reliable performance in the harsh operating environment of a train. If the server hosting VSMS on the train encounters issues, or if no server is deployed, then recording of video is stored on local solid-state storage on the individual IP cameras.

In addition, the Klas deployment model is able to support redundant onboard gateways for further resiliency. The two ways in which the redundant gateways can be deployed are:

- **Active/Standby Gateways**—In this model, one gateway is designated the primary path for all traffic, and the other gateway is in a standby role, only carrying traffic in the case of a failure in the primary gateway. The redundancy between the two gateways is handled by VRRP.
- **Active/Active Gateways**—In this model, both gateways actively pass traffic from the onboard infrastructure, effectively increasing the amount of bandwidth available to a train. The onboard infrastructure is logically split with VLANs between the two gateways, allowing each gateway to be the primary path for half of the onboard infrastructure and traffic. Each gateway serves as the standby path for the other gateway's traffic by using VRRP, ensuring service survivability in the case of a gateway failure.

Similar to the onboard network, the Connected Trackside network is deployed in an Ethernet ring topology, using REP for network topology and failover management in the access rings, and Unified MPLS in the aggregation network. This subtended ring topology design provides resilient connectivity to nodes within the network in the case of a single link or node failure. Uplink connections from the Connected Trackside backhaul network to the Operations Center infrastructure uses two different nodes, implementing mLACP. All resiliency design mechanisms are covered in detail in the *Connected Rail Solution Implementation Guide*, and further covered in the *Connected Roadways Design and Implementation Guide*.

Redundant UNI links from the Mobile Service Provider and Internet Service Provider may be implemented. Typical uptime SLAs for these UNI connections will exceed the uptime requirements for the Connected Rail solution, so the cost versus the benefit of redundant UNI links must be analyzed by the rail operator.

Implementation of this kind of redundancy is well understood and has been validated in many systems, so is considered outside the scope of the Connected Rail Solution.

Scalability Considerations

Passenger Wi-Fi

Scalability for Passenger Wi-Fi services depends upon several factors, including bandwidth per user, the amount of bandwidth available to a train, and the total users active on a system at one time. In the Connected Rail Solution, the following guidelines are assumed:

- ~400Kbps minimum bandwidth available to a user
- ~100Mbps bandwidth available via the train-to-trackside wireless link.

With those two parameters, each train would be capable of supporting ~250 simultaneous users with no other service traffic on the train-to-trackside link. Assuming a 4:1 over-subscription ratio, since many users will be engaging in transactional-type data usage, allows for ~1000 users per train for a single gateway.

Video Surveillance

The biggest limiting factor for number of onboard video surveillance cameras is the process of transferring the video archives off the train to long-term storage.

- The VSF has the following limits:
  - 500 VSOM servers
  - 2000 regions
  - 200 client workstations
- Each VSOM can support the following:
  - 200 VSMS/LTS
  - 10,000 cameras (Cisco and non-Cisco)
  - 100 DP servers
- Default licensing includes:
  - A single VSMS
  - Up to 10,000 Cisco cameras
  - Up to 10 non-Cisco cameras

Long Term Storage Transfer

Company policy and/or government regulations may require video archives be available for a minimum amount of time. This could be a matter of days, weeks, or months of video archives which will require many terabytes, if not petabytes, of storage space. Depending the number of cameras and the amount of storage on the onboard VSMS, two options may exist for long term video archive storage:

- The archives may be transferred off of the VSMS to a LTS server offboard the train. This transfer can be scheduled to happen during periods of low network traffic and while the train is connected to the trackside network over a high speed Wi-Fi connection.
- The archives may be kept on the VSMS on which the archives are created. For this option, sufficient storage space must be available on the VSMS to meet the requirements of storage durations. Configuration of this option can be accomplished within the camera template as was covered in the VSOM section.

Configuring offboard LTS first requires the offboard server(s) to be configured as storage servers. An LTS is essentially a VSMS configured with the LTS server type.

A critical factor that must be taken into consideration when designing and implementing the system is the amount of time it will take to transfer the video archives from each onboard VSMS to LTS. Transfer time will be affected by the following data points:

- **Number of Cameras**—The VSMS can only transfer a single camera's archive at a time and will transfer all camera archives sequentially. Therefore, the more camera archives to be transfer, the longer the transfers will take to complete.
- **Size of Archives**—The larger a camera's video archive is, the longer it will take to transfer. The size of the archives is directly impacted by the bitrate of the video stream that is being archives. Higher bitrates create larger archives.
- **Offboard Link Speed**—The speed of the wireless link between the onboard and offboard network, which will be the slowest segment in the path, will directly impact the time it takes to transfer the archives.

Table X offers an estimate of how long it will take to transfer the video archives of a single camera feed based on the variable factors of video feed bitrate and offboard link speed.

Table X. Archive Transfer Times Per Camera

Table 5

		Transfer Time Based on Offboard Link Speed		
Video Bitrate (Kbps)	Archive Size (GB)	15 Mbps	25 Mbps	100 Mbps
128	1.39	12 min	7.2 min	1.8 min
256	2.76	24 min	14.4 min	3.6 min
384	4.15	36 min	21.6 min	5.4 min
512	5.53	48 min	28.8 min	7.2 min
768	8.29	72 min	43.2 min	10.8 min
1024	11.06	96 min	57.6 min	14.4 min
1536	16.59	144 min	86.4 min	21.6 min

Related Documentation

The *Connected Rail Solution Implementation Guide* provides detailed implementation and validation details for the solution scope. The Connected Rail Solution scope incorporates products from Cisco and from ecosystem partners. Links to relevant product documents are included in this section.

Any documentation that is not listed here can be obtained through your Cisco Sales contact.

Cisco

- ESR 5921 Software Embedded Router:
    - http://www.cisco.com/c/en/us/support/routers/5921-embedded-services-router/model.html
- Cisco ASR1000 PMIPv6 Configuration Guide:
    - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmipv6/configuration/xe-16/mob-pmipv6-xe-16-book/imo-pmipv6-multipath-support.html
- Cisco Unified MPLS on ASR Products:
    - http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/118846-config-mpls-00.html

Fluidmesh

- FM1000 Gateway:
    - https://Fluidmesh.box.com/s/tt5gu26g6oc0r43g24w3td6jx348vske
- FM10000 Gateway:
    - https://Fluidmesh.box.com/s/turvxz3jobx62oiair21x21dpzkrzem5
- FM4200 MOBI:
    - https://Fluidmesh.box.com/s/ky60o1a69ookpe4igc4rxt59fb78yt1o
- FM3200 BASE:
    - https://Fluidmesh.box.com/s/uma7b9f3gh2jw55utc9gtu7cjjl6958e
- FM3200 ENDO:
    - https://Fluidmesh.box.com/s/ugxwfxjwfa0c18ojiq0w7jpd36o5kuba
- FM PONTE 50:
    - https://Fluidmesh.box.com/s/ro894dttfroxfoqvxxfz79wj5zvj72v3
- FM SHARK 16:
    - https://Fluidmesh.box.com/s/teq0l5uqa0y5hkeo70njc3ebunjl1xzz
- FM TUBE:
    - https://Fluidmesh.box.com/s/ld1ju0n9eu9yecdiwbyf8qmjju5fvdtx
- FM Fluidity:
    - https://Fluidmesh.box.com/s/ff64mo4d0ym40sjmnwx40q9qlu3gjvk8

Klas Telecom

- TRX-R2 Gateway:
    - http://klastelecom.com/trx-r2/

- TRX-R6 Gateway:
  - http://klastelecom.com/trx-r6/
- TRX-S10 Switch:
  - http://klastelecom.com/trx-s10/
- TRX-S26 Switch:
  - http://klastelecom.com/trx-s26/

Lilee Systems:

- LMS-2450-ME-100 Gateway:
  - http://www2.lileesystems.com/lilee-transair-lms-2450-me-100_datasheet
- Virtual LMC:
  - http://www2.lileesystems.com/lileeos-vlmc_datasheet

Glossary

Table 6 lists acronyms and initialisms used in this document.

Table 6 Acronyms and Initialisms

Term	Definition
ACL	Access Control List
AF	assured forwarding
ASA	Cisco Adaptive Security Appliance
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automated Train Supervision
BGP	Border Gateway Protocol
CA	Certificate Authority
CENELEC	European Committee for Electrotechnical Standardization
CoS	Class of Service
CTBC	Communications Based Train Control
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EF	expedited forwarding
EMSP	Cisco Enterprise Mobility Services Platform
ETA	estimated time of arrival
fps	frames per second
FRR	Fast Reroute
GRE	Generic Route Encapsulation

Table 6 Acronyms and Initialisms (continued)

Term	Definition
GSM-R	Global System for Mobile - Rail
H-QoS	Hierarchical-QoS
IGP	Interior Gateway Protocol
IoT	Internet of Things
IS-IS	Intermediate System to Intermediate System
KVM	Linux Kernel-based Virtual Machine
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LDP	Label Distribution Protocol
LEAP	Lightweight Extensible Authentication Protocol
LMA	Local Mobility Anchor
LMC	Lilee Mobility Controller
LMN	Logical Mobile Nodes
LSP	Label Switched Path
LTE	Long-Term Evolution
LTS	Long-Term Storage
MAG	Mobile Access Gateway
MDM	Mobile Device Management
MJPEG	Motion JPEG
mLACP	multichassis Link Aggregation Control Protocol
MN	mobile node
MP-BGP	Multiprotocol Border Gateway Protocol
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
OAM	Operations, Administrations, and Maintenance
OCC	Operations Control Center
OSPF	Open Shortest Path First
PAN	pre-aggregation node
PEAP	Protected Extensible Authentication Protocol
PHY	physical layer
PMIPv6	Proxy Mobile IPv6
PoE	Power over Ethernet
PTC	Positive Train Control
PTT	Push-to-Talk
QCI	QoS Class Identifier
REP	Cisco Resilient Ethernet Protocol
rLFA-FRR	Remote Loop-Free Alternate Fast ReRoute
SCEP	Simple Certificate Enrollment Protocol

Table 6 Acronyms and Initialisms (continued)

Term	Definition
SDXC	SanDisk Extended Capacity
SEN	Service Edge Node
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UNI	user-to-network
VLAN	Virtual Local Area Network
vLMC	Lilee Virtual LMC
VoIP	Voice over IP
VRRP	Virtual Router Redundancy Protocol
VSF	Video Surveillance Federator
VSMS	Cisco Video Surveillance Media Server
VSOM	Cisco Video Surveillance Operations Manager
WAN	Wide Area Network
WAP	wireless access point
WLC	Wireless LAN Controller
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2