Connected Mass Transit System Design Guide (Cisco Validated Design)

Last Updated: February 10, 2016

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

Connected Mass Transit System Design Guide (Cisco Validated Design)

CONTENTS

Preface

This Preface includes the following major topics:

Audience

The audiences for this document are Cisco account teams, Cisco Advanced Services teams, and Systems Integrators working with Mass Transit Agencies (MTA). It is also intended directly for use by the mass transit agencies to understand the features and capabilities enabled by the Cisco Connected Mass Transit System design.

Document Objective and Scope

This design guide provides a comprehensive explanation of the Cisco Connected Mass Transit System design. It includes information about the system's architecture, supported services, and possible deployment models. The guide also recommends best practices and potential issues when deploying the reference architecture.

The *Cisco Connected Mass Transit System Implementation Guide* is a companion document to this document, and provides guidelines for implementation and configuration of the system architecture and supported services. Please refer to the Implementation Guide at the following URL:

- https://docs.cisco.com/share/s/VPXt5hVkQ5-1541t47hQgw

Use Cases/Services/Deployment Models

This guide addresses the following technology use cases:

- Passenger and Enterprise Wi-Fi Network Services
- Vehicle Location and Telemetry Data Collection and Correlation
- Passenger Real-Time Information
- Vehicle Two-way Voice Communication

- Vehicle Video Surveillance
- Event-Triggered Video Surveillance
- Vehicle Panic Button
- Wireless Bulk Data Transfer
- Connected Passenger Stop
- Fleet Management

System Overview

The Cisco Connected Mass Transit System provides an end-to-end system design for service delivery to a Mass Transit infrastructure, including connectivity to vehicles, bus stops, and maintenance yards. The system provides a converged, multi-service, secure, and standards-based infrastructure on which passenger and operational capabilities for buses 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 mass transit.

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

The *Cisco Connected Mass Transit System Implementation Guide* is a companion document to this document, and provides guidelines for implementation and configuration of the system architecture and supported services.

System Supported Services and Models

This chapter, which details the services supported by the Connected Mass Transit System, includes the following major topics:

Service Architecture Overview

The Cisco Connected Mass Transit System implements a comprehensive infrastructure that supports multiple services. These services are typical of those required by Mass Transit fleets, and are easily extensible to other Mass Transit Agencies (MTAs) and Metro deployments.

Service Inventory/Models

Table 2-1 lists the services supported in this phase of the Connected Mass Transit System.

Table 2-1 Supported Services

Service Category	Service Definition
Wi-Fi Network Services	Provides Wi-Fi Network services to passengers, drivers, and emergency personnel and Transit Agency employees on the bus and at a bus stop. Passenger access is authorized by the passenger accepting the terms & conditions of using the service before gaining access to Internet services. Access for drivers, emergency personnel, and transit agency employees requires username/password authentication.
Vehicle Location Tracking	Relay vehicle location information to Davra RuBAN™ Management system in real-time. Vehicle location determined by Global Navigation Satellite System (GNSS) integration, such as Global Positioning System (GPS) or GLOSSNAS with the vehicle onboard infrastructure.

Table 2-1 Supported Services (continued)

Service Category	Service Definition
Vehicle Telemetry Data Collection	Relay real-time vehicle performance information, such as Speed, RPM, and Idle time from vehicle Controller Area Network (CAN) bus to Davra RuBAN Management system. Provides ongoing monitoring of bus operation, and provides information on predictive maintenance to be performed before service-affecting issues are encountered.
Vehicle Location Data Correlation	Correlation of other service performance information with vehicle location such as Received Signal Strength Indicator (RSSI) and speed. Provides historical data for understanding cellular coverage along the vehicle route, driver behavior, road congestion at certain locations. Can be used for the MTA to optimize the bus route and scheduling, and plan for crew shift schedules.
Passenger Real Time Information	Displays real-time schedule updates and other information inside the vehicle and at the bus station. This information includes vehicle ID, vehicle route, next stop, estimated arrival time, and any delays in schedule.
Vehicle Two-way Voice Communication	Two-way voice communications with Push To Talk (PTT) support between drivers, supervisors, and operations team at dispatch and maintenance centers. Enables interworking between voice over IP (VoIP) systems and legacy digital radio communications through Cisco Instant Connect integration.
Vehicle Video Surveillance	Onboard vehicle systems to support up to eight separate IP video surveillance cameras. 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 cellular backhaul is supported. Recorded video is offloaded via Wi-Fi to long-term storage for later retrieval when vehicle is parked in yard.
Event-Triggered Video Surveillance	Video recording and real-time video transmission can be triggered based on certain events and triggers, such as loud noises, driver input, door close/open, and rapid acceleration/deceleration.
Vehicle Panic Button	Concealed input from the vehicle driver to report emergencies and requests assistance at any time. Panic button integration will allow the driver to contact emergency authorities and bus operation team directly, and automatically relay relevant information from the vehicle (such as location, vehicle specifications and head-count).

Table 2-1 Supported Services (continued)

Service Category	Service Definition
Wireless Bulk Data Transfer	When parked in a maintenance yard, the vehicle establishes a high-bandwidth network connection via Wi-Fi to the infrastructure in the yard. This link facilitates the ability to offload route logs, video files, and other pertinent information from the vehicle, and to update the vehicle onboard systems. This include route information, recorded public announcements, software updates for vehicle onboard systems; ability to upload passenger information, previous route log information, credit card, and onboard video at storage from vehicle to bus operator data center.
Connected Bus Stop	Provides passenger Wi-Fi services at a bus stop while passengers are waiting for a bus. Provides Estimated Time of Arrival (ETA) updates on vehicles en route to the bus stop. Network connectivity to the bus stop is provided via wired connectivity, or via cellular uplink if no wired infrastructure is deployed to the bus stop.
Fleet Management Services	The RuBAN system from Davra Networks provides a comprehensive management platform for vehicle fleet operations which integrates essential functions for managing a vehicle fleet: location tracking, vehicle telemetry data collection, asset provisioning and monitoring, geofences, vehicle dashboard reports, policy-triggered events, and video surveillance integration.

Wi-Fi Network Services

The Cisco Connected Mass Transit System provides an integrated Wi-Fi AP infrastructure, providing wireless networking services for passengers and essential systems for the MTA and Emergency Services. The following services are supported via Wi-Fi connectivity:

- Passenger Internet Services
- Enterprise infrastructure access for Mass Transit employees
- System access for Law Enforcement and Emergency Services
- Wireless PTT endpoints

The Wi-Fi infrastructure implements a separate Service Selection Identified (SSID) for each class of service supported. This provides the ability to implement authorization mechanisms and policies specific to each service class.

For Passenger Internet services, the SSID is configured for open access. The first time a passenger attempts to access Internet services over the Wi-Fi connection, the user's device is redirected to a login page hosted by the onboard Wi-Fi infrastructure. This login page presents the Terms and Conditions to which the passenger must agree before accessing Internet services. Once the passenger clicks **Accept**, access to Internet services is permitted without further impediment. In this release of the Mass Transit system design, this function is implemented using a feature in Cisco IOS called *ip admission <name>* consent. More information on configuring this feature can be found in *Consent Feature for Cisco IOS Routers* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_auth/configuration/15-mt/sec-usr-auth-15-mt-book/sec-cons-feat-rtrs.html

All passenger Internet service traffic is transported over cellular backhaul from the onboard network infrastructure, and routed directly by the cellular provider to the Internet. The actual implementation of this function, including an example custom terms and conditions HTML page, is included in the *Connected Mass Transit Implementation Guide*.

For all other services, the corresponding SSID implements an appropriate authorization mechanism before any network access is permitted. Wi-Fi Protected Access Second Generation (WPA2) is typically deployed for these types of services, implementing either username and password or certificate-based authorization mechanisms depending upon the operator's and end point's requirements. All traffic for these services is transported via a secured infrastructure over the cellular backhaul connection, implemented via a Dynamic Multipoint Virtual Private Network (DMVPN) tunnel established between the onboard network and the back office infrastructure.

Each Wi-Fi SSID is mapped to a separate Virtual Local Area Network (VLAN) in the onboard network infrastructure, providing the required service traffic separation required by the MTA.

The Connected Mass Transit System implementation for passenger Wi-Fi network services targets supporting 25 concurrent users on a vehicle, and providing a minimum of 400 Kbps of bandwidth per user. Depending upon the actual number of concurrent users and the network usage of each user, higher bandwidth may be experienced by the passengers using the service. Service traffic for PTT voice communications and for Mass Transit employees and Emergency Service personnel is prioritized over passenger Internet services.

Vehicle Location and Telemetry Data Collection and Correlation

The Connected Mass Transit System provides integrated collection and correlation of vehicle location and telemetry data. This allows MTAs to accurately track real-time vehicle location and progress along the route, as well as real-time vehicle performance. It also allows for correlation of vehicle location with other aspects of vehicle onboard system performance, such as cellular connection strength to determine poor coverage areas along a vehicle route.

Vehicle location is determined by Global Navigation Satellite System (GNSS) integration with the vehicle onboard infrastructure, supporting such systems as GPS and Globalnaya Navigazionnaya Sputnikovaya Sistema (GLOSSNAS). The onboard system is polled by the RuBAN vehicle management system at a configurable interval, such as every five seconds, depending upon the location resolution required by the operator. The vehicle onboard infrastructure implemented in the Connected Mass Transit System provides the following location, altitude, and velocity tracking accuracy:

- **Horizontal**: < 2 m (50%); < 5 m (90%). This means that horizontal GPS data has an accuracy of greater than 2 meters 50% of the time, and greater than 5 meters 90% of the time.
- **Altitude**: < 4 m (50%); < 8 m (90%)
- **Velocity**: < 0.2 m/s

In addition to simply tracking vehicle location and progress, the vehicle location information can be made available to other systems on the vehicle that require that information, such as passenger ticketing systems. The location information is distributed in a format compliant with the National Marine Electronics Association (NMEA) 0183 standard, via streaming TCP/IP, or via a serial interface for systems that do not support TCP/IP streaming of location information.

The vehicle onboard infrastructure also integrates with the vehicle Controller Area Network (CAN) bus to collect real-time vehicle performance information such as Speed, RPM, and Idle time. This data collection enables ongoing monitoring of bus operation and provides information on predictive maintenance to be performed before service affecting issues are encountered. Similar to the vehicle location data collection, vehicle performance data is collected at a configurable polling interval and

transmitted to the RuBAN integrated vehicle management system supplied by Davra Networks. The vehicle onboard infrastructure uses a SAE J1939-compatible Heavy Duty Vehicle adapter to communicate with the CAN bus.

Correlation of other service performance information with vehicle location by the RuBAN management system provides useful information about Mass Transit operations. For example, by enabling a MTA to collect cellular backhaul performance data such as RSSI, and correlate that with vehicle location, an operator can determine geographic areas that have poor cellular performance. This information can then be relayed to the MSP for service coverage improvements. Correlation of historical route data also helps analyze other aspects such as driver behavior and road congestion at certain locations at certain times. This data enables the MTA to optimize vehicle routes and scheduling, and help plan for crew shift schedules.

Passenger Real-Time Information

For MTAs to increase ridership, one key aspect is to make use of public transit as easy as possible. One way to do that is to provide easy access to accurate real-time route and ETA information to users. The Connected Mass Transit System incorporates the collection and analysis of vehicles along transportation routes, enabling the MTA to provide this information to its users through various mechanisms, such as digital signage at bus stops and smartphone applications.

The key enabler of this service is the Davra RuBAN system's ability to integrate real-time vehicle location information with historical data on transportation route progression to provide accurate ETA predictions in real-time. This system was demonstrated at Cisco Live! in San Diego.

The following details the algorithm implemented in Davra RuBAN to detect and compute the ETA of the vehicles along a route:

- Virtual checkpoints are configured by the MTA on each vehicle route. The distance interval between these checkpoints is much shorter than that between the actual stops, providing a more granular analysis of vehicle progression. The stops themselves will also be treated as virtual checkpoints.
- The algorithm constantly learns and updates the baseline performance for each vehicle route, meaning the longer it runs, the more intelligent and accurate it becomes.
- The algorithm keeps track of the normal elapsed time between any two virtual checkpoints on the route for a particular time-of-day of a particular day-of-week, maintaining separate baselines for different times of the day on different days of the week. Traffic conditions vary greatly depending upon these factors, for example, what's normal at 8am on a Monday morning will be very different from what's normal at 8pm on a Sunday. This further increases the accuracy of the algorithm in RuBAN.
- Every time a vehicle reaches a virtual checkpoint, RuBAN will readjust the signs at subsequent stops down the route, based on any variation between when the vehicle arrived at the checkpoint versus when it was expected to arrive. In this way, the system constantly corrects itself, increasing ETA accuracy and preventing error propagation.
- Virtual checkpoints can be placed closer together in areas of higher variation, to give the system more opportunities to correct itself in those areas. In more stable areas, such as where traffic doesn't regularly contribute to variable delays, spacing between virtual checkpoints can be increased without affecting accuracy.
- Another important aspect is a visualization into the baseline and the accuracy of the baseline. RuBAN presents metrics on expected travel times for a particular route, and how accurate the baseline algorithm is proving to be on a per-trip and an overall fleet basis.
- The system provides special handling for a situation where a vehicle is stationary for a prolonged period of time.

The Connected Mass Transit System provides several integration points for calculating and providing ETA information:

- The RuBAN system is configured to scrape the content of the Mass Transit status system every minute or so to determine whether a change in route or an out of service announcement exist.
- RuBAN correlates the route detected with the set of stops and virtual checkpoints along the route.
- GPS info from the IR 829 onboard router is used to check if the vehicle has crossed a virtual checkpoint.
- ETAs calculated on the RuBAN server are pushed to the digital signage system using the appropriate API for the particular system.

Vehicle Two way Voice Communication

The converged network infrastructure integrated into the Connected Mass Transit System supports two-way PTT VoIP communications between the vehicle driver and the dispatchers in the operations center. This provides the flexibility to integrate next generation voice communications systems for new vehicle deployments and existing vehicle 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.

The Cisco Instant Connect system integrates support for many different endpoint devices, including dedicated VoIP endpoints, IP Dispatch turrets, wireless IP phones, and smartphones and tablets. It also provides Cisco Unified Communications integration, allowing for Cisco IP phone support.

The Connected Mass Transit System integrates end-to-end Quality of Service (QoS), providing proper real-time treatment for VoIP traffic throughout the network infrastructure. To eliminate potential disruption of voice communications, the system design recommends the routing of VoIP traffic over the cellular connection of the vehicle regardless of location, thus eliminating any loss due to connection roaming. However, the system is capable of routing VoIP traffic over the vehicle Wi-Fi connection if so desired by the MTA.

Vehicle Video Surveillance

Video surveillance for mass transit systems is an essential service for ensuring the safety and security of its passengers and employees. The Connected Mass Transit System provides a comprehensive video surveillance system that ensures complete coverage of all assets and personnel onboard vehicles, at route stops, and in parking lots and maintenance yards.

On a vehicle, the Connected Mass Transit System can scale video surveillance coverage to the number of cameras that a MTA requires. Typically, coverage of a vehicle like a bus will require between two to eight cameras, so the system has validated that range. The system design supports two deployment options onboard the vehicle:

- A ruggedized server is deployed on the vehicle with the cameras, to provide storage for and management of the cameras. The server integrates two terabytes of solid-state storage for video retention. The server is deployed with Cisco Video Surveillance Media Server (VSMS) running on top of the VSphere ESXi hypervisor from VMWare, thus using different brands of servers without concern about hardware incompatibilities, and also accommodates hosting other functions on the server in addition to VSMS. The server deployed needs to be certified to work with VSphere ESXi for this deployment model.
- The cameras are deployed onboard without a server. Each camera has a microSD card slot that supports SDXC cards, enabling up to 2TB of onboard storage on each camera.

The Connected Mass Transit System design includes two different camera designs, offering flexibility in camera location deployment and coverage:

- **The Cisco Video Surveillance 3050 IP Camera**—A dome form-factor camera which supports 720p video capture (1280x720 pixels). The camera is IP66 and IK10 rated. More information is available 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**—A high-definition video endpoint that is equipped with a 5-megapixel sensor (2560x1920 pixels) and a fisheye lens that can deliver impressive 180° panoramic views and 360° surround views. The camera is IP66 and IK10 rated. More information is available 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

Both camera models support a minimum of 25 frames per second (FPS) and a minimum resolution of 720x486 pixels for National Television System Committee (NTSC) format and 720x576 pixels for Phase Alternating Line (PAL) format. Both camera models support Motion JPEG (MJPEG) and H.264 video codecs for recording.

The Connected Mass Transit System supports event marking of video segments based on a number of triggers and inputs. The system can be configured to take different actions depending upon the particular trigger, such as only copying marked video from the vehicle, or even notifying an operator of an issue and offering live stream video over the cellular link from the vehicle. This permits the MTA to access video surveillance when needed, but not unnecessarily use cellular data for video when it's not needed. The dispatchers are also able to call up video on-demand from any vehicle's cameras via the centralized management system.

The system design supports archiving of video surveillance recordings to a centralized Long-Term Storage (LTS) system. In order to minimize the time needed to copy video surveillance files from a vehicle when parked at the end of the day, only video marked with events is offloaded to the LTS system. If all video on a vehicle is required to be offloaded to long-term storage, then special accommodations must be implemented, such as a specific video offload station within the maintenance yard combined with an extended operating window.

Event Triggered Video Surveillance

As mentioned in the previous section, the Connected Mass Transit System design supports marking of video footage by several different events and triggers. The following events are supported in the system design:

- **Contact closure triggers, which 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 propagate that trigger to other cameras as well. Examples of contact closure triggers include:
  - Door open and close
  - Panic button

- **Accelerometer-based triggers, which senses abnormal vehicle dynamics**—The system integrates with the vehicle CAN bus through the On-Board Diagnostics (OBDII) port, and can generate triggers based on events from the vehicle. Also, the Davra RuBAN management system can sense issues based on vehicle telematics, and trigger the video surveillance system. Examples of these triggers include:
  - Panic braking
  - Driver behavior
  - Accident detection, including air-bag deployment
- **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 include:
  - 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 vehicle. It is also able to include geographic information for video tagged by other events. Examples of geographic triggers include:
  - Geofence
  - Deviation of vehicle from planned route
  - Unexpected vehicle stoppages along route
  - Include geographic information with video tagged by other event triggers

Vehicle Panic Button

An essential mechanism for guaranteeing the safety of the mass transit driver and the passengers on the vehicle is for the driver to covertly alert the dispatch center if a critical situation occurs. This panic button is typically activated by a foot button or other input mechanism accessible by the driver. When the panic button is activated by the driver, the following actions are implemented by the Connected Mass Transit System:

- Two-way voice communications are opened between the driver and the dispatch center.
- Depending upon the situation, the Dispatch center can patch the audio from the vehicle directly to the relevant law enforcement agency.
- The onboard video surveillance system triggers live streaming over the cellular connection on critical cameras, so as to not overload the available bandwidth over the cellular link. The dispatch operator can select other cameras as needed through the Davra RuBAN console.
- Vehicle location information and other pertinent data is displayed on the RuBAN console.

Note Several options are supported by the Connected Mass Transit System for integration with the CAD/AVL system providing the panic button interface, but integration with a specific CAD/AVL system has not yet been validated. Those integration options are documented in this Design Guide. Inclusion and validation of this integration is targeted for a future phase of the Connected Mass Transit System.

Wireless Bulk Data Transfer

The systems onboard the vehicle responsible for handling route information and announcements, and for logging route progress throughout the day require periodic connectivity with centralized scheduling and monitoring systems to stay up-to-date. This connectivity is established when the vehicles are parked in the vehicle yard while out-of-service, via a wireless connection from the vehicle to the yard network.

When the wireless connection is established in the vehicle yard, the following types of bulk data transfers will take place between the onboard vehicle systems and the backend systems in the Operations Center:

- **Infrastructure-to-Vehicle**—Download updated route information, route audio announcements, and software updates for the onboard systems. Expected frequency of updates is no more than once per month.
- **Vehicle-to-Infrastructure**—Upload log files and video surveillance files from vehicle's previous route on a daily basis.

Table 2-2 details the types of data exchanged, the expected size, and the frequency with which the data is exchanged.

Table 2-2 Data Types for WBDT

Data Type	Estimated Size	Expected Frequency	Direction
Router Software	90 MB	2/year	To bus
IP Camera Firmware	15 MB	2/year	To bus
AP Software	20 MB	2/year	To bus
Archived Video Data	82GB for H.264 316GB for MJPEG	1/day	From bus
Automated Vehicle Announcement (AVA) Image	30 MB	12/year	To bus
Schedule Data	12 MB	12/year	To bus
Vehicle Logic Unit (VLU) Software Updates (Full Build)	15 MB	1/year	To bus
VLU Software Updates (Patches)	0.5 MB	4/year	To bus
Automatic Passenger Counting (APC) Data	154 kB	1/day	From bus
Time Point Encounters (RSA)	26 kB	1/day	From bus
AVA Logging	243 kB	1/day	From bus
Transit Signal Priority (TSP) Logs	243 kB	1/day	From bus
VLU Error Logs	30 kB	1/day	From bus

For ease of vehicle system deployment over hundreds or thousands of vehicles, identical configurations will be used for the vehicle onboard logic systems with the exception of a unique vehicle identifier. Thus, the onboard network infrastructure will be required to provide Network Address Translation (NAT) functionality to enable routing for the particular vehicle within the maintenance yard.

Nearly all required file transfers are easily accommodated within the 30 minute window proposed in this system design. The following assumptions and calculations are used to evaluate the total amount of data that can be transferred to and from a vehicle within that 30 minute window:

- The limiting factor for throughput is likely the wireless connection. An 802.11n 5GHz bridging link using 2x2 MIMO can achieve approximately 150-200Mbps bidirectionally with 40MHz channels under ideal conditions.
- At this throughput rate, a maximum of ~36GB of data can be transferred bidirectionally by one vehicle in 30 minutes. Just to clarify, bidirectional means the sum of data transferred in both directions, so if 2GB are transferred downstream, then 34GB could be transferred upstream
- As more vehicles associate to an infrastructure AP, the bandwidth available is shared between the vehicle connections. Assuming a density of 10 buses per infrastructure AP and accounting for overhead results in approximately 1.8-2.7GB of data that can be transferred in 30 minutes.

The notable exception to this are the video surveillance files. Note that the size of the video files listed are several orders of magnitude larger than any other file transfer class, and far exceed the amount of information that can be transferred from the bus to the backend systems in the 30 minute window. The Connected Mass Transit System design proposes that event-tagged video is prioritized for offloading when the vehicle is in the yard, and that non-tagged video is simply stored on the local vehicle storage to be retrieved at a later date if needed.

If a particular vehicle's video is needed in its entirety, then the Connected Mass Transit System proposes a designated video-offload location in the yard where that vehicle would make use of the entire amount of bandwidth available from an infrastructure AP. In this scenario, assuming 150Mbps of throughput to a vehicle, 82GB of video surveillance data can be copied in approximately 90 minutes, and 316GB of data can be copied in approximately 6 hours. If the MTA requires that all video had to be offloaded from every vehicle on a daily basis, then the number of cameras supported, and the resolution and frame rate of those cameras needs to be reduced to ensure that the total video surveillance data is under the ~2GB threshold.

Connected Passenger Stop

The Connected Mass Transit System seeks to provide a comprehensive end-to-end infrastructure design for all aspects of a MTA's operational scope. In addition to providing the infrastructure and services to the fleet of vehicles, the system covers connectivity and services for the passenger stops operated by the agency.

The infrastructure design for the passenger stop seeks to replicate the same service set that is provided onboard the vehicles:

- Wi-Fi services for Passengers, Employees, and Law Enforcement.
- Video Surveillance. As the passenger stop is likely to be in a public area, such as on a sidewalk next to a street, relevant privacy laws for the city/county/country must be followed when looking to deploy video surveillance.
- Vehicle ETA information is displayed at bus stop per the mechanism detailed in the section Passenger Real-Time Information, page 2-5.

Information on the infrastructure design and service delivery aspects to passenger stops is provided in Chapter 3, “System Architecture.”

Fleet Management

The Connected Mass Transit System provides a comprehensive set of services essential to a MTA for managing a vehicle fleet. The set of services supported in the system include:

- Vehicle GPS tracking
- Vehicle telemetry data collection
- Asset provisioning and monitoring
- Geofence configuration and monitoring
- Customizable dashboard reports to dispatchers and operators on any vehicle
- Policy-triggered events and alerts
- Video surveillance system integration
- RuBAN management system

This set of services is supported by the RuBAN Management System by Davra Networks. The services supported and the way in which the services are managed can be tailored to meet the specific needs of a particular customer. Details are included in Management User Interface, page 3-15.

System Architecture

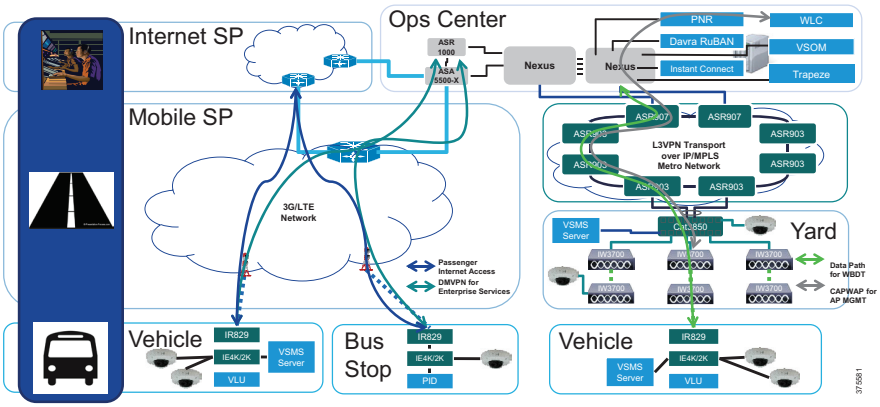
This chapter includes the following major topics:

This release of the Connected Mass Transit System proposes a scalable and resilient design for the following aspects of a MTA's infrastructure and services:

- Vehicle Onboard Network and Systems
- Off-boarding Wireless System
- Yard Network and Transport Network designs
- Operations Center criteria
- Hosted Systems and Services

Figure 3-1 illustrates the layers of the Connected Mass Transit System.

Figure 3-1 Connected Mass Transit System Overview



Each of these system layers are described in greater detail in this chapter.

Related Efforts

The Connected Mass Transit System scope focuses on infrastructure and services specific to mass transit vehicle operations, safety and optimization, as well as passenger connectivity and services.

The Connected Mass Transit design interfaces with key aspects from other Cisco Validated Designs (CVDs) for the following areas:

- **Enterprise Data Center**—Provides a scalable and highly resilient data center infrastructure necessary for hosting key service and management components.
- **Cisco Connected Roadways System**—Provides design best practices for a scalable and resilient transport network for Metro Network connectivity between MTA locations, based on the tried and tested Unified MPLS design deployed by service providers around the globe.

Inter-System Interfaces

The Connected Mass Transit System relies on LTE services provided by a MSP to enable network connectivity between the vehicles, Internet, and backend systems while the vehicle is in motion. This service must enable Layer 3 connectivity to and from the vehicles. The choice of MSP is left to the City Municipality or Metro Transit Authority, provided the service requirements outlined in this document are met.

Functional Description

Connected Vehicle Onboard Network and Systems

The vehicle onboard network design proposed in the Connected Mass Transit System consists of the components shown in Table 3-1.

Table 3-1 Connected Vehicle Onboard Components

Component	Provides
Cisco IR 829 Mobile Router	• IP routing and gateway functionality for all onboard systems • Wireless connectivity for passengers and enterprise systems • All wireless offboarding connections: LTE and Wi-Fi Workgroup Bridge (WGB) • An on-demand secure, encrypted infrastructure for transmitting data from onboard systems over data services provided by Service Providers • CAN bus integration through a serial adapter for Engine Telematics data gathering
Cisco IE4000 Ethernet Switch	• Additional gigabit Ethernet and power-over-Ethernet capacity for onboard systems • Support of up to 8 PoE devices
Cisco IE2000 Ethernet Switch	• Alternative onboard Ethernet switch 100 Megabit Ethernet connections and PoE for up to 4 devices

Table 3-1 Connected Vehicle Onboard Components (continued)

Component	Provides
Cisco Video Surveillance IP3050 Camera	• 720p HD video capability with Wide Dynamic Range (WDR) plus digital I/O and audio integration in a transportation-focused IP66/IK10 rated housing • Inclusion of integrated storage for video recordings on the camera
Cisco Video Surveillance IP7070 Camera	• 5MP video resolution with a 360 degree view capability plus digital and audio I/O integration in a transportation-focused IP66/IK10 rated housing. • Inclusion of integrated storage for video recordings on the camera
Third Party J1939 Adapter	• Converts the Onboard Diagnostics (OBDII) connection to the CAN bus of the vehicle into a serial connection to the IR 829 router

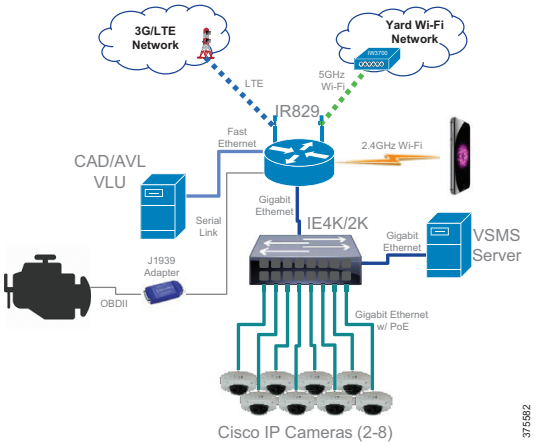
In addition, the following component is optional for the Video Surveillance system on the vehicle:

- **Ruggedized Server**—A compute platform to host the Cisco VSMS for management of the onboard IP Cameras. The Cisco Connected Mass Transit System is validated with servers from Advantech, the details of which are specified in Chapter 4, "System Components." The servers from Advantech support automotive-grade, and wide-range voltage input DC power supplies (9 Volt to 36 Volt), and are certified to perform under the vibration and shock environment of a vehicle. Other brand servers with similar specifications may also be potentially supported, as the VSMS application is hosted within VMWare VSphere ESXi on the server. Provided that the server can support the proper version of VSphere ESXi, it can be a candidate for supporting VSMS.

Finally, the following component may be present, and can make use of the communications infrastructure proposed in this system design:

- **CAD/AVL Vehicle Logic Unit (VLU)**—Provides CAD/AVL functions for the vehicle. May also provide the panic button interface for the driver.

Figure 3-2 Vehicle Onboard Network Overview



The IR829 router provides wireless connectivity for passenger devices onboard the vehicle, using the 2.4GHz radio of the integrated wireless AP. The AP implements multiple SSIDs on this radio, providing secured connectivity to MTA devices and potentially law enforcement devices as well. Each SSID is mapped to a separate VLAN that is trunked to the router portion of the IR829, to facilitate service separation and security. The 5GHz radio of the integrated wireless AP in the IR829 is dedicated as a WGB to provide high-bandwidth connectivity for the vehicle systems when the vehicle is parked in a

maintenance yard. Traffic to this radio is also on a separate VLAN, specifically the native VLAN, trunked to the router portion of the IR829. This places the routing engine of the IR829 between the Gigabit Ethernet ports, the 2.4GHz radio, and the 5GHz and LTE radios. This allows the router to perform all needed networking functions on traffic from the onboard vehicle systems and from passenger devices, and facilitate routing of traffic to the appropriate offboarding connection.

The Cisco IE4000 switch connects one Gigabit Ethernet uplink port to a LAN switchport on the IR 829 router for network connectivity. The IE4000 switch provides a maximum of 8 GE ports with up to 170 Watts of Power-over-Ethernet (PoE) capacity for IP camera connectivity. Eight additional GE ports supply connectivity to other devices, such as the onboard server for VSMS, but without providing PoE.

For deployments that require fewer PoE devices to be implemented, a Cisco IE2000 switch can be used instead. By combining the PoE capacity of the IE2000 switch with the PoE capacity of the IR829, up to 6 devices can receive PoE power.

The IP Cameras and VSM server connected to the IE4000 switch will all be configured for a Video Surveillance VLAN, to provide service separation. If other systems are also connected to the IE4000 switch, then the uplink port to the IR829 needs to be configured as an 802.1Q trunk port. Otherwise, this uplink is configured as an access port. In either case, the video surveillance traffic is attached to a separate VLAN on the IR829 router.

The OBDII port from the vehicle is connected to the Async 1 port of the IR829 router through a third party adapter. In this phase, a heavy duty vehicle interface adapter from B&B Electronics was used to validate this feature. The IR829 runs a RuBAN agent that queries the adapter through the serial port at a configured interval and collects the returned engine telematics data to forward to the RuBAN management system. The RuBAN agent uses raw-TCP socket communication with the serial port to enable efficient and reliable bi-directional communication with the vehicle interface. This method may be adapted to support integration with a wide range of sensor gateways and other equipment which communicate via serial interfaces.

The CAD/AVL VLU, if present, is assumed to have a 100Mbps Fast Ethernet interface, and is connected to a LAN switchport on the IR829 router for network connectivity. This port is configured as an access port, and should implement portfast functionality to minimize port negotiation time. This port is mapped to a VLAN interface for Layer 3 functionality and for service separation from other services.

Panic button notification from the driver, whether provided by the CAD/AVL system or another onboard system, can be integrated into the system in several different ways to accommodate a wide range of systems. The system has the ability to support network-based triggers via HTTP GET messages, serial port integration for trigger sensing with the IR829 router, or a contact closure link to one of the IP cameras. This provides effective integration between the onboard systems, video surveillance system, and Davra RuBAN management system. Connections to other desired triggers, such as door sensors, can be connected to other cameras. Alternately, the alarm input on the IE 4000 switch may be used for contact closure inputs, if combined with an Embedded Event Manager (EEM) script to generate the proper soft trigger call to the video surveillance system. Note that these are listed here as options, but have not been validated with a specific CAD/AVL vendor. This is targeted for validation in a future system phase. More information on using soft triggers with the Cisco Video Surveillance Manager system is available in Chapter 12 of the *Cisco Video Surveillance Operations Manager User Guide*, available at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/security/physical_security/video_surveillance/network/vsm/7_7/admin_guide/vsm_7_7_vsom.pdf

The IR829 router provides DHCP server functionality for all onboard systems on the vehicle that require it. The IR829 router also provides routing, gateway, and NAT functions for all onboard systems, allowing multiple systems onboard to share a single offboarding link for communications.

To facilitate ease of deployment, all onboard systems may be deployed in all vehicles with identical RFC 1918 compliant private IP address and subnets. In order to provide unique IP addressing toward the backend infrastructure and beyond, the IR 829 must implement NAT to translate the private IP address space for the onboard subnets. This translation may be to either a unique RFC 1918 IP address or a public IPv4 address, depending upon the deployment requirements of the MTA.

All components are connected to the vehicle 12 Volt DC power system, and thus power up at the same time that the vehicle is started. The system design assumes that power to the onboard networking infrastructure is maintained when the vehicle engine is turned off, to maintain connectivity for a period of time when the vehicle is parked. Power for the onboard networking infrastructure should be connected to a separate manual or automatic power isolation switch to permit this. The IR 829 supports ignition sensing management features to enable the gateway to detect the current voltage of the vehicle electrical system and the state of the engine in the vehicle. The IR 829 supports configurable timers triggered by the ignition state, allowing for graceful shutdown of systems before the power isolation removes power from the IR 829.

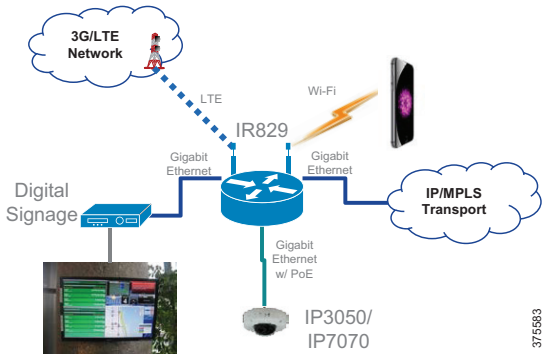
Details of the design implemented to carry all service traffic over the MSP-provided LTE service are detailed in Offboard Wireless Connection System, page 3-6.

Connected Bus Stop

The network design for a Connected Bus Stop (shown in Figure 3-3) consists of the following components:

- **Cisco IR 829 Mobile Router**—Provides IP routing and gateway for all systems at the bus stop. Provides wireless connectivity for passengers via 2.4GHz and 5GHz 802.11n Wi-Fi wireless connectivity, and network connectivity for public information displays. Backhaul of all traffic is via fiber connectivity to the Metro Network, if available at to the stop, or via the integrated LTE modem if no wired connectivity is available.
- **Digital Signage System**—Displays ETA information for buses which provide service at that bus stop. Any digital signage system with an API for accepting display content can be integrated into the Connected Mass Transit System design.
- **The Cisco Video Surveillance 3050 IP Camera**—Provides 720p HD video capability with Wide Dynamic Range (WDR) plus digital and audio I/O integration in a transportation-focused IP66/IK10 rated housing. Includes integrated storage for video recordings on the camera
- **The Cisco Video Surveillance 7070 IP Camera**—Provides 5MP video resolution with a 360 degree view capability plus digital and audio I/O integration in a transportation-focused IP66/IK10 rated housing. Includes integrated storage for video recordings on the camera.

Figure 3-3 Connected Bus Stop Overview



The IR829 router provides wireless connectivity for passenger devices at the bus stop, using both the 2.4GHz and 5GHz radios of the wireless AP. The AP implements multiple SSIDs, providing secured connectivity to MTA devices and potentially law enforcement devices as well. Each SSID is mapped to a separate VLAN for interoperability with the router portion of the IR829, to facilitate service separation and security.

The Digital Signage system is connected to a LAN switchport on the IR829 router for network connectivity. This port is configured as an access port, and should implement portfast functionality to minimize port negotiation time. This port is mapped to a VLAN interface for L3 functionality and for service separation from other services.

If fiber connectivity to the Metro Network is present at the passenger stop, then it is connected to the IR829 Gigabit Ethernet WAN port. Otherwise, the LTE cellular connection is used for data backhaul. Details of the design implemented to carry all service traffic over the MSP provided LTE service are detailed in LTE, page 3-6.

Deployment of Video Surveillance at a bus stop must be done in compliance with government laws and regulations regarding privacy, as the camera view of the bus stop area will likely include surrounding public areas.

Offboard Wireless Connection System

The Cisco Connected Mass Transit System design supports two wireless communications systems concurrently for providing network connectivity to and from the vehicle:

- **Long Term Evolution (LTE)**—A contracted LTE service from a MSP is used for communication with the vehicle while the vehicle is in motion or otherwise located outside of the range of a maintenance yard or other fixed location of the MTA. In addition, LTE is used for providing wireless connectivity to a Connected Bus Stop if fiber or other wired connectivity is unavailable to that location. This is supported by the integrated LTE cellular modem in the Cisco IR829 router.
- **Wi-Fi**—When within the range of the maintenance yard or other facility for long-term parking of the vehicle, the vehicle uses a Wi-Fi bridge connection to the operator-owned Wi-Fi infrastructure at that facility. This is supported by the 5GHz radio of the integrated AP in the Cisco IR829 router.

The Connected Mass Transit System supports automatic roaming from one wireless connection to the other, implemented within the routing configuration and policies on the mobile router. Since each service and system on the vehicle has a dedicated IP subnet, this routing configuration is relatively trivial, and does not require more complex functions such as application-aware routing or Performance Routing (PfR). The rest of this section describes each wireless service implementation in detail.

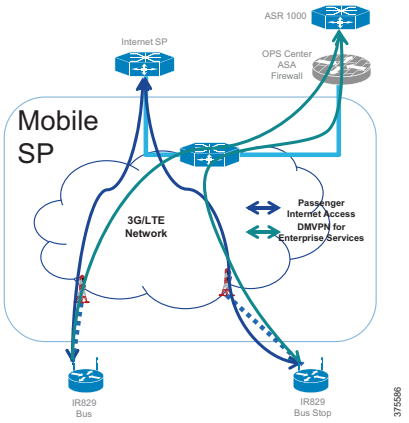
LTE

The Connected Mass Transit System uses an LTE cellular connection to provide network connectivity to the vehicles when in motion. See Figure 3-4. The design assumes these cellular services are provided by a MSP. At a minimum, this service must provide Layer 3 IP connectivity to the public Internet, over which all services will be transported. Beyond basic IP connectivity, the following services and functions are desirable:

- **Internet Access for Passengers**—The MSP should be able to route all Passenger Internet service traffic directly to the Internet, reducing the load on the MTA's network.
- **Quality of Service**—The MSP should support at least 3 classes of service on the LTE cellular service to allow for proper treatment of voice and video services required by the MTA over the best effort traffic generated by passenger internet services.

- **Direct Interconnect to Ops Center**—The MSP should support a direct connection to the MTA's data center, providing a direct path for enterprise services from the MSP's network. This prevents enterprise services from having to traverse the public Internet infrastructure, and better supports end-to-end Quality of Service.
- **VPN Service**—The MSP should offer a private L3VPN between the cellular connections from the vehicles and the MTA's data center, ensuring separation and security of all enterprise service traffic between the vehicle systems and backend systems.

Figure 3-4 LTE Connectivity via MSP



If all of these services and functions are available from the MSP, then Layer 3 routing is sufficient to transport all service traffic between the vehicles and backend systems, and an overlay mechanism is not required. However, it is currently the exception, rather than the norm, that a MSP is able to offer all of these services and functions. To accommodate this, the Connected Mass Transit System implements a secured overlay VPN mechanism to enable the MTA to deploy a secure method of service transport over any level of Layer 3 service from the MSP.

For this likely deployment scenario, the Connected Mass Transit System proposes the use of DMVPN for transport of enterprise service traffic between the vehicle infrastructure and the backend systems. DMVPN has been widely deployed in many different Enterprise and IoT network systems, including transportation systems, and thus is a well-proven technology to fulfill the transport and security requirements of the Connected Mass Transit System design. DMVPN provides a dynamic, secure VPN infrastructure over any network that provides simple IP routing between endpoints and a hub location. DMVPN is capable of providing Layer 2 as well as Layer 3 service transport, and can encrypt all traffic transported.

The network infrastructure proposed in the Connected Mass Transit System is also capable of supporting FlexVPN technology for providing a dynamic, secured, private infrastructure over the LTE services, if the customer prefers deploying it instead of DMVPN. FlexVPN is an evolution of DMVPN, supporting IKE2 by default, and consolidating multiple configuration requirements into a single comprehensible set of commands. More information on FlexVPN is available at *Cisco FlexVPN* at the following URL:

- http://www.cisco.com/c/en/us/support/security/flexvpn/tsd-products-support-series-home.html

A third potential option for providing a dynamic, secured infrastructure is Group Encrypted Transport VPN (GETVPN). GETVPN requires a private networking infrastructure on which to be deployed, so an additional abstraction layer must be implemented between the LTE service and the GETVPN transport. Location-ID Separation Protocol (LISP) can provide this additional abstraction layer. However, the added complexity of having to implement two mechanisms without providing any compelling advantage over DMVPN or FlexVPN is enough reason to not consider this approach for the Connected Mass Transit System. Information on LISP and GETVPN are included here for reference:

- LISP:
  - http://lisp.cisco.com/index.html
- GETVPN:
  - http://www.cisco.com/c/en/us/products/security/group-encrypted-transport-vpn/index.html

The router onboard the vehicle implements the role of a DMVPN spoke site, and establishes the DMVPN session to a hub router in the MTA's central network. In the interest of efficient routing and optimal service traffic flow, only those services that require connectivity to backend systems in the MTA's network, such as voice, GPS data, vehicle telematics, and on-demand video surveillance, are transported over the DMVPN tunnel. Service traffic from passengers using the wireless internet service is routed directly to the Internet over the MSP's network. This minimizes the bandwidth needed from the MSP to the MTA's network, as well as minimizes the size of the Internet-facing nodes in the MTA's network.

As each service and system on the bus is separated by VLANs with separate IP subnets on the LAN portion of the onboard network, a simple routing configuration on the onboard router handles which subnets, and thus which services, are transported by which means. All services are transported over the common LTE offboarding link through NAT. The mechanisms used by the onboard gateway are covered in Routing and Network Address Translation, page 5-3, and the exact configuration for service transport is covered in the *Connected Mass Transit Implementation Guide*.

Cellular services and systems are designed to handle roaming of endpoint devices throughout the MSP's network. Thus, once a connection is established between the onboard router on the vehicle and the MSP network, IP addressing and connectivity should remain relatively constant as the vehicle drives its prescribed route. In a situation where IP addressing on the LTE connection does change, or if the LTE connection experiences an interruption, the DMVPN service will automatically reestablish connectivity to the hub site once IP connectivity is restored. A brief interruption in traffic will be experienced during this type of event, expected to be on the order of a few seconds.

It is highly desirable, and in some cases required, to have support for multiple LTE connections to a single vehicle. This may be due to coverage gaps from a single MSP along parts of a vehicle's route, or may be due to pricing advantages of using one MSP over another at certain times of day. The mobile router in the Connected Mass Transit System design, the Cisco IR829, supports two SIM cards in the internal LTE modem. Since only one LTE modem exists, both MSPs must support the same LTE connection and bands included in the LTE modem. Only one of the SIM cards is active at any time in the IR 829 modem, and handoff from one SIM card to the other requires 45-50 seconds for the connection to be reestablished, due to the need for the IR 829 to reboot the LTE modem in order to switch SIMs.

Wi-Fi

The Connected Mass Transit System uses Wi-Fi connection to provide network connectivity to the vehicles when parked in a maintenance yard or other MTA facility. The design assumes the Wi-Fi infrastructure is owned and operated by the MTA, providing secure, higher-bandwidth connectivity to the MTA's centralized systems. This permits the MTA to update the systems onboard the vehicles when not in use via bulk data transfer, and also upload log files and video surveillance files from the vehicles to long-term storage in an automated fashion.

The mobile router on the vehicle has an integrated Wi-Fi AP, which supports 802.11n connections with 2x2 Multiple In, Multiple Out (MIMO) streams. The 2.4 GHz radio is dedicated for providing connectivity to passenger endpoint devices and MTA systems. The 5 GHz radio is dedicated to providing a WGB link to the Wi-Fi infrastructure in the maintenance yard. using 40MHz channels on the 5 GHz radio with 2x2 MIMO should yield a throughput of 150-200 Mbps bidirectional for one vehicle connection to one infrastructure AP. Authorization of vehicle access to the Wi-Fi infrastructure, as well as encryption of data passing over the wireless connection, is accomplished via WPA2 implementation. The system design recommends implementing a certificate-based authorization system for Wi-Fi

connections versus a pre-shared key (PSK) or preconfigured username and password, to ease deployment and to easily recover from compromised or leaked credentials Since the Wi-Fi infrastructure and Metro Network infrastructure are owned and under the control of the MTA, no further end-to-end encryption of data is required. This will also minimize the CPU load on the onboard router and maximize throughput, maximizing the rate of data transferred to and from the vehicle.

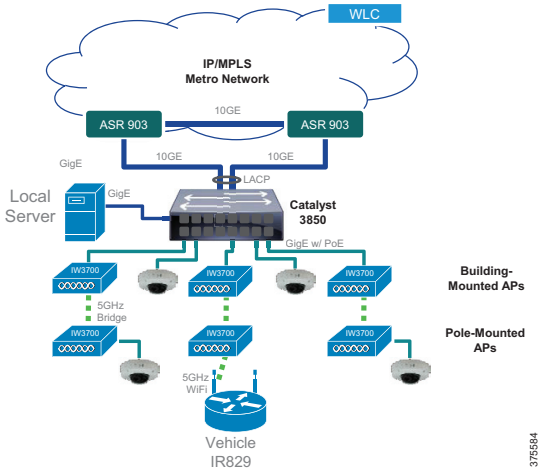
The IR 829 onboard gateway monitors the status of the Wi-Fi connection and LTE connection and manages usage of each link through the dynamic Interior Gateway Protocol (IGP) used for routing decisions. By using Enhanced Interior Gateway Routing Protocol (EIGRP) for routing management, reachability through each connection is actively monitored and service traffic is routed out the correct interface.

Yard Network

The network in the maintenance yard provides a scalable Wi-Fi infrastructure to deliver secure, high-bandwidth wireless connectivity to the vehicles parked in the yard. The yard network (shown in Figure 3-5) consists of the following components:

- **Cisco IW3702 Ruggedized AP**—An IP67-rated outdoor AP that provides IEEE 802.11ac Wave 1 Wi-Fi coverage for the yard.
- **Cisco Catalyst 3850 Ethernet Switch**—Provides gigabit Ethernet connectivity and PoE to the IW3702 APs and IP Cameras. Stacking capability provides redundancy and easy expansion. Router functions for all branch systems at yard. Redundant Ten-gigabit Ethernet uplinks to Metro Network.
- **Cisco WLC5520 Wireless LAN Controller**—A high-density controller for configuring and managing the IW3702 APs. Located in the data center with the other backend systems.
- **Cisco Video Surveillance IP 3050 and 7070 Cameras**—Provide video surveillance for the Yard and assets.
- **Cisco VSMS system on a Cisco Unified Computing System (UCS) Server**—Provides management of video surveillance IP cameras located in the yard, and storage capacity for recorded video. In a future release, can also serve as a repository for video files being copied from vehicles in the yard.

Figure 3-5 Yard Network Overview



The IW3702 APs may be deployed with a variety of omni-directional or directional antennas, depending upon yard layout and coverage requirements. Each yard layout will present unique criteria and challenges for wireless deployment, so a site survey is required to determine the optimal positioning and density for AP deployment. In general, for ease of wiring, APs will be deployed on the sides or roof of the building in the yard in which the Ethernet switch resides. If the area of the yard requiring wireless coverage exceeds the effective range of these APs, additional APs are deployed on light standards or other pole structures throughout the yard. If the yard has network wiring available to these poles, then the additional APs are wired to the Ethernet switch. Otherwise, wireless bridging to the APs on the side of the building is employed for traffic backhaul, and only power has to be provided to the wirelessly-connected APs.

The APs are connected to a Catalyst 3850 Universal Access Ethernet switch, as are any other local servers and branch systems located at the yard. The Catalyst 3850 switch line provides a range of configurations and port densities to accommodate any size yard deployment. Also, with PoE supplied to all ports on the switch, separate power connections are not required for each IW3702. The Catalyst 3850 switch implements stacking functionality, which provides easy network expansion and resiliency implementation. Each wired AP is connected to a gigabit Ethernet port. The yard network uplink to the metro network uses redundant ten-gigabit Ethernet connections configured in a Link Aggregation Control Protocol (LACP) port-channel bundle, enabling simplified deployment of resilient connectivity for each maintenance yard to the Metro Network.

The Catalyst 3850 switch also provides all Layer 3 addressing and routing functionality for the yard network and other branch office systems, and fulfills the CE role for the L3VPN transport over the Metro Network. All onsite IP addressing in the yard network is accomplished through Dynamic Host Control Protocol (DHCP) lease distribution. DHCP administration is managed by a centralized Cisco Prime Network Registrar (PNR) server located in the Ops Center infrastructure. The Catalyst 3850 operates as a DHCP proxy to facilitate address distribution to the infrastructure and endpoints in the yard location. Traffic patterns are almost exclusively between the yard and systems in the Ops Center infrastructure, so simple static routing can accomplish most tasks. If more complex routing patterns are required, then a routing protocol such as Open Shortest Path First (OSPF) or EIGRP can be implemented in the CE role.

Under ideal conditions, the maximum wireless throughput over the 802.11n WGB from a single vehicle to the yard AP can achieve approximately 200 Mbps of bidirectional throughput; however, 150 Mbps is more likely. As multiple vehicles connect to a single infrastructure AP, this bandwidth will be divided more-or-less equally among the vehicles, so 10 vehicles simultaneously accessing a single AP will each see approximately 15 Mbps. Assuming a total capacity of approximately 400 vehicles within a single yard, a typical yard deployment will need approximately 40 APs. This ratio of vehicles to APs will allow each vehicle to transfer approximately 2GB of information on average within a 30 minute window.

The worst-case scenario for yard network scaling is at the start of a shift, where all vehicles in the yard may be powered up nearly simultaneously. This is the scenario for which the yard network is designed to accommodate.

The Yard AP infrastructure is centrally managed by a Cisco Wireless LAN Controller (WLC). The WLC is configured to deploy and manage the APs in FlexConnect mode, transporting only control traffic via Control and Provisioning of Wireless APs (CAPWAP) tunnels to the WLC, while employing local addressing and switching of all data traffic. This provides a highly-scalable transport design for handling all data traffic from the vehicles in the yard, allowing access to both local systems and centralized data center systems. Local addressing of vehicles and other wireless endpoints is handled via DHCP functionality in the Catalyst 3850 switch in coordination with PNR.

Deployment of IP Cameras is needed to monitor and protect assets situated within the yard. For cameras positioned on the side of the yard building or in other locations with wired network access, these cameras are plugged into the same switching infrastructure as the APs. To extend the reach of the video

surveillance to yard locations that do not have a wired infrastructure, the IP Camera can be connected to the local Ethernet port on an IW3702 AP. The IW3702 can supply PoE power to the IP camera and wireless transport of video traffic from the camera.

A Cisco UCS server is located at the yard and connected to the local switching infrastructure to host VSMS for camera management and video storage. This localizes video storage to the yard network, reducing load requirements on the Metro Network for video surveillance for the yard, while still providing centralized management and monitoring capabilities via Cisco Video Surveillance Operations Manager (VSOM) and Davra RuBAN.

The WGB wireless function associates with a single SSID in the yard, transporting all wireless traffic from the vehicles. All vehicle traffic is transported by a single VLAN. This VLAN has access to locally deployed infrastructure as needed, and is mapped to a transport L3VPN within the Metro Network for access to centralized services. Video surveillance traffic from the yard camera infrastructure is carried on a separate VLAN and L3VPN. Other enterprise service traffic can be segmented as needed.

Note This same design can be deployed at Intermodal Transit Stations, to provide additional connectivity for vehicles when parked there while on daily scheduled routes.

Metro Network

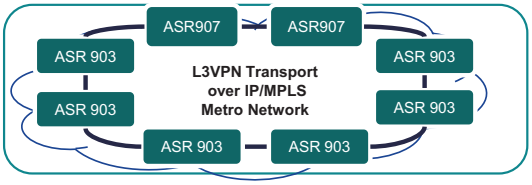
The Cisco Connected Mass Transit System requires a highly scalable and resilient Metro Network infrastructure (shown in Figure 3-6) to facilitate service traffic transport from the distributed maintenance yards to the Ops Center and backend systems across the MTA's geographic region. Cisco promotes a 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: A single network infrastructure supports L3VPN services, 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.
- Performance Management (PM) to track key Service Level Agreement (SLA) parameters such as packet-loss, packet delay, and delay variation.
- Easily deployable resiliency and high availability for both infrastructure and services with remote Loop-Free Alternate Fast ReRoute (rLFA-FRR) and BGP FRR.

The Metro Network design used for the Cisco Connected Mass Transit System is thoroughly documented in the *Connected Roadways Design and Implementation Guide*. A high-level overview of the design is included here for reference. The Metro Network design consists of the following components:

- **Cisco ASR900 Routers**—The Cisco ASR900 Aggregation Services Router (ASR) line provides both fixed and modular platforms accommodating all necessary interfaces, functionality and scalability for the Metro Network infrastructure. The ASR900 line includes the ASR902, ASR903, and ASR907 modular chassis, and the ASR920 fixed configuration routers, all using the IOS-XE system software.

Figure 3-6 Metro Network Overview



The Unified MPLS model deployed for the Metro Network in the Connected Mass Transit System implements Intermediate System to Intermediate System (IS-IS) as the Interior Gateway Protocol (IGP) in a single L1 area, with a flat LDP (Label Distribution Protocol) layer for MPLS LSP (Label Switched Path) transport. Note that if the customer is more familiar with deploying and implementing 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 Mass Transit System 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 (PAN). Connections to the Operations Center infrastructure is via multiple 10GE links configured for mLACP port-channel bundles from redundant Service Edge Nodes (SEN).

All service transport in the Connected Mass Transit System is implemented with Layer 3 Virtual Private Networks (L3VPN). L3VPNs are deployed in the Unified MPLS design through use of Multiprotocol Border Gateway Protcol (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 further enhanced with the implementation of FRR in BGP.

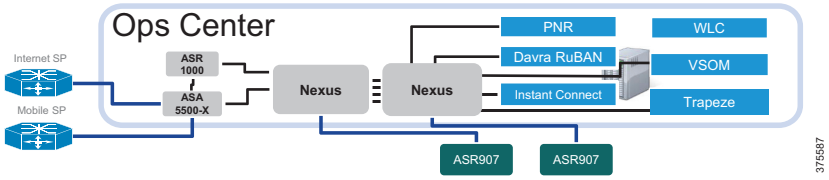
Operations Center Systems

The Operations Center in the Cisco Connected Mass Transit System (shown in Figure 3-7) refers to the location, both logically and physically, where all centralized systems and infrastructure reside.

The following sub-systems reside within the Operations Center:

- **Dispatch Center**—Location of the MTAs and dispatchers. Incorporates management consoles for RuBAN, VSOM, and push-to-talk (PTT) voice systems through integration with Cisco Instant Connect. Cisco Instant Connect also provides compatibility with legacy digital radio communications systems.
- **Data Center**—Cisco Nexus Data Center switching and Unified Computing Systems (UCS) infrastructure for hosting all backend systems and storage for all enterprise services.
- **Internetwork Peering Gateway**—Provides connections to the Internet Service Provider and MSP(s) providing services to the MTA.

Figure 3-7 Operations Center Overview



MTAs in the Dispatch Center use the following systems and services:

- **RuBAN**—A comprehensive management platform from Davra Networks providing vehicle position tracking, telematics monitoring, driver behavior monitoring, and video surveillance integration. RuBAN also provides network element management services, including provisioning, software management, and monitoring of network assets and functionality.
- **Cisco Video Surveillance Operations Manager (VSOM)**—Video surveillance system management, live streaming of video from vehicles on event triggers, vehicle alert notification, video archive access.
- **PTT Voice**—Voice communications with drivers. Managed by Cisco Instant Connect version 4.9.1.

The Cisco Mass Transit system design assumes a Data Center infrastructure is implemented in accordance with the best practices described in the Cisco Enterprise Data Center architecture. More information is available at *Data Center and Virtualization* at the following URL:

- http://www.cisco.com/go/datacenter

Additional infrastructure is required to facilitate the user-to-network (UNI) connections from Service Providers providing contracted services to the MTA, namely Internet services and mobile connectivity to vehicles. The following components are used for these network connections:

- **Cisco ASA5500-X Firewall**—Provides high-bandwidth gateway, firewall, and intrusion prevention services for internetwork connections up to ten gigabit Ethernet.
- **Cisco ASR1000 Router**—Provides hub router functionality for terminating DMVPN tunnels originating from vehicle onboard routers over the MSP-provided services.

Network Management Systems

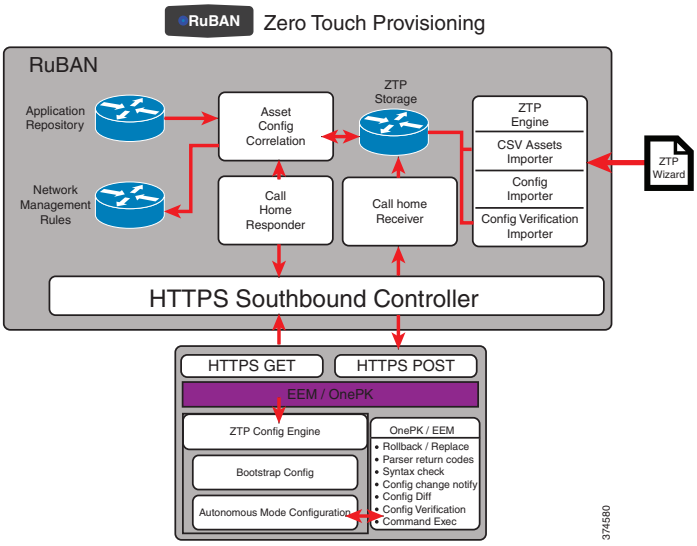
Given the transportation-specific aspects of the Connected Mass Transit System scope, the number of third party systems involved, as well as the targeted customers, a transportation-specific network management system is warranted. Cisco is partnering with Davra Networks to integrate the RuBAN IoT Management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

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

RuBAN provides integrated network element management for the Connected Mass Transit System, 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 Mass Transit System design.

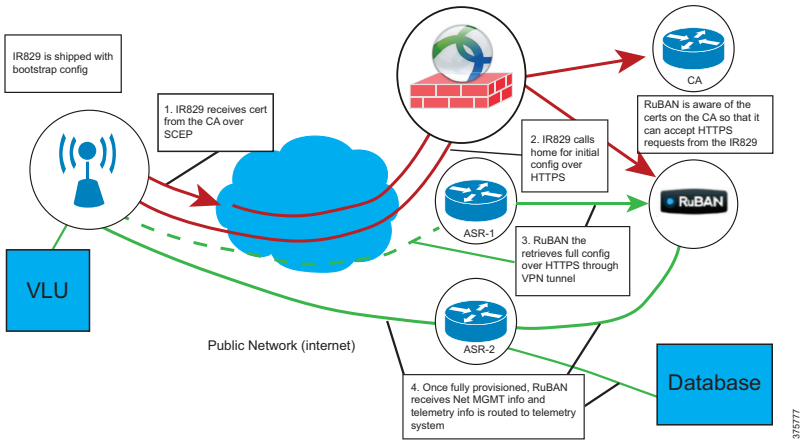
Figure 3-8 provides an overview of the southbound interface between the RuBAN system and the Cisco devices deployed in the network.

Figure 3-8 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 Cisco device to "call-home" to the RuBAN system, providing a connection for further device configuration. An overview of this workflow is illustrated in Figure 3-9.

Figure 3-9 RuBAN Network Element Management Deployment Workflow



1. The Cisco device (the IR829 router in the illustration) 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 Cisco devices.
2. The Cisco 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 Cisco 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 Cisco devices. Telemetry info is routed to the Vehicle 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 Geo Location information, so that the precise location of vehicles and other mobile components is available in real-time.

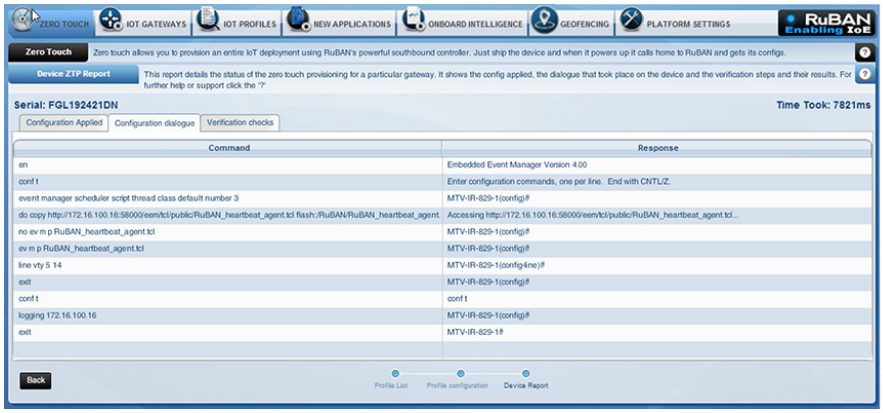
Management User Interface

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 Mass Transit Implementation Guide*.

Provisioning

The Provisioning Interface (shown in Figure 3-10) covers infrastructure and service provisioning and monitoring functions for equipment deployed on the vehicles.

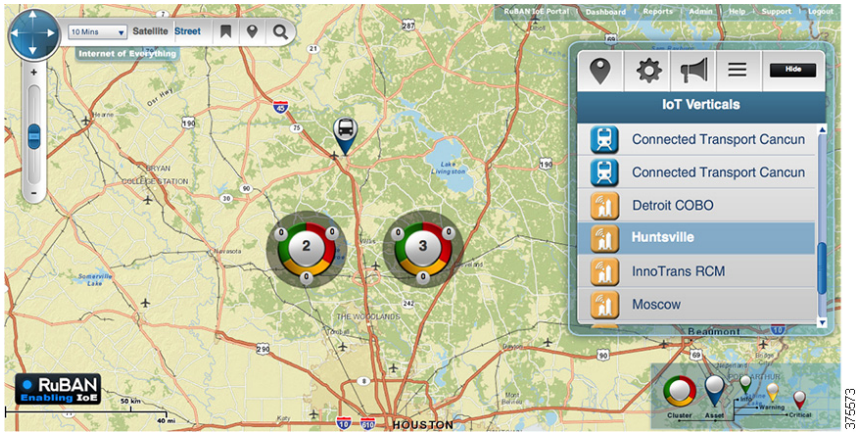
Figure 3-10 Provisioning Interface



Vehicle Tracking

The Vehicle Tracking Interface (shown in Figure 3-11) provides an overhead map view of the area covered by the MTA, with a real-time overlay of the location of all vehicles in service within that area. Clicking on a vehicle will display more detailed information and dashboards available for that vehicle, which are described in subsequent subsections. Also, integrated access is available to the VSOM system, allowing the dispatcher to pull up video surveillance within the same interface.

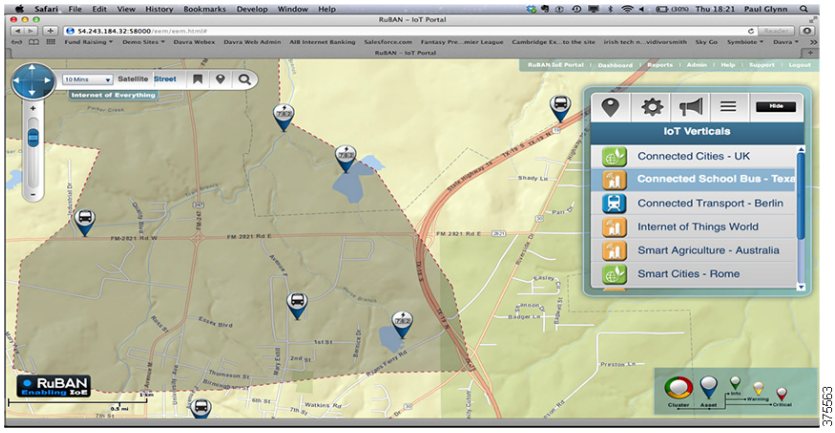
Figure 3-11 Vehicle Tracking Interface



Geofencing

The Vehicle Geofencing Interface (shown in Figure 3-12) enables the operator to set a geofence boundary for a single vehicle, a group of vehicles, or all vehicles in-service. If a vehicle covered by a geofence travels outside of that boundary, then an alert is issued to the operator.

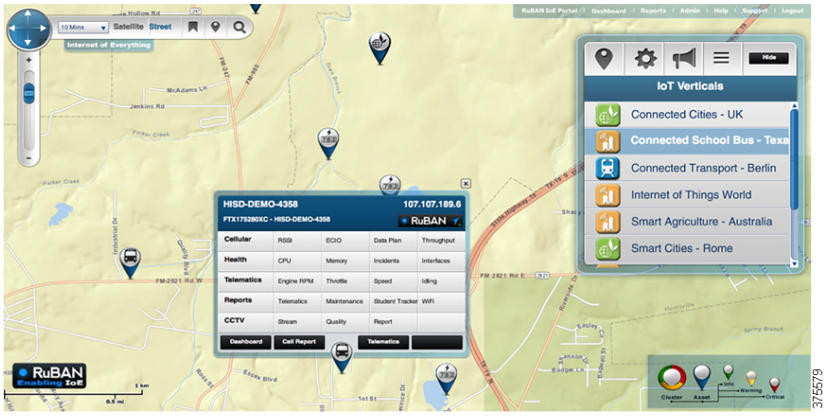
Figure 3-12 Vehicle Geofencing Interface



Vehicle Management

The Vehicle Management Interface (shown in Figure 3-13) gives the operators more specific information on a particular vehicle, and actions that can be taken for that vehicle. The information and actions can be customized to the specific requirements of the MTA.

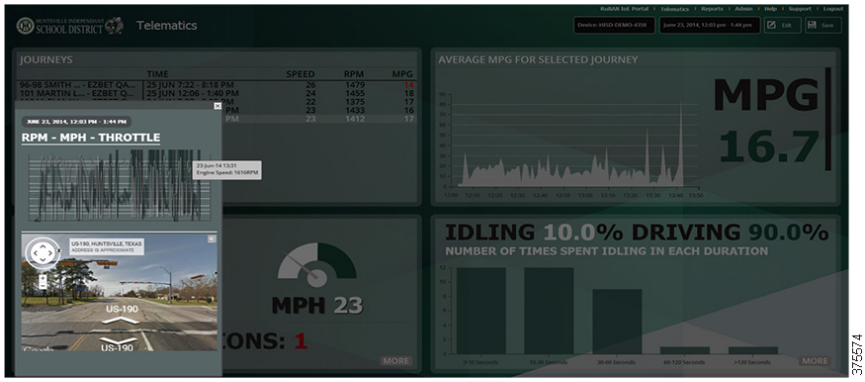
Figure 3-13 Vehicle Management Interface



Driver Management

The Driver Management Dashboard interface (shown in Figure 3-14) provides data to the operator that illustrates how the driver of a specific vehicle is performing, such as speed hysterics, acceleration and braking data, fuel efficiency, time spent driving versus idling, etc. Again, this dashboard can be customized to display whatever data the MTA requires.

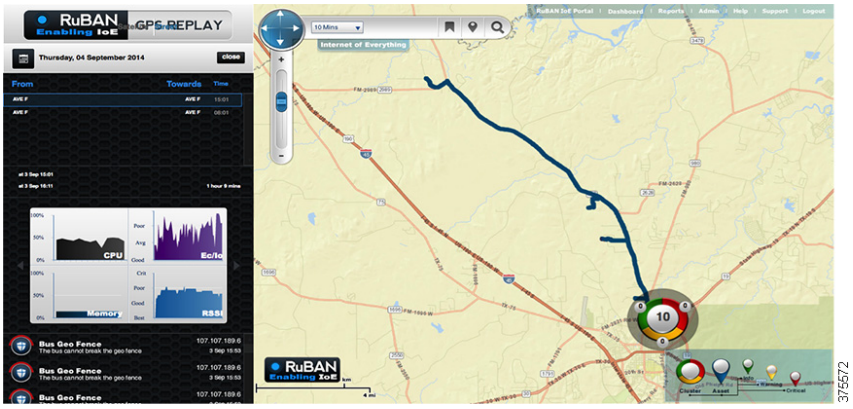
Figure 3-14 Driver Management Dashboard Interface



Route Replay

The Vehicle Route Replay Interface (shown in Figure 3-15) allows an operator to replay and review the route traveled by a vehicle during a certain day, and can correlate engine telematics information and other data to the GPS position at a particular time. This can be used to evaluate the historical performance of a particular route or a particular driver.

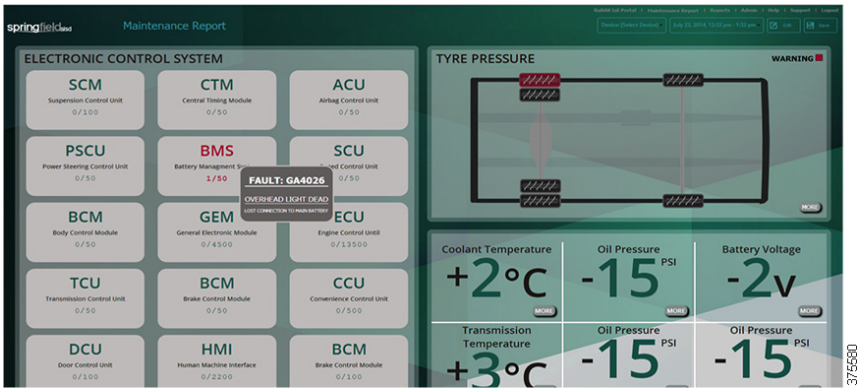
Figure 3-15 Vehicle Route Replay Interface



Vehicle Telematics

The Vehicle Telematics Dashboard interface (shown in Figure 3-16) provides a real-time display of the sensor data available from a vehicle. The data displayed can be customized to the MTA's particular requirements. It also alerts the operator to any potential performance or safety issues with a vehicle, such as low tire pressure, low oil pressure, or high engine temperature.

Figure 3-16 Vehicle Telematics Dashboard Interface



Passenger Information System ETA Interface

The Passenger Information System ETA interface (see Figure 3-17 and Figure 3-18) allows the MTA to customize the input data, data flow and criteria for ETA calculation, and output mechanism for the ETA data to the MTA's digital display systems at stations, at stops, and even onboard the vehicles.

Figure 3-17 Passenger Information System ETA Interface

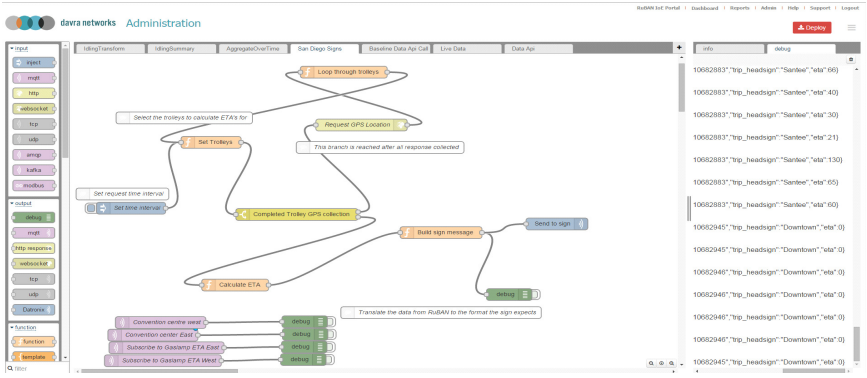


Figure 3-18 Passenger Information Display Example

System Components

This chapter, which lists the Cisco and third party components included in the Cisco Mass Transit system design, includes the following major topics:

Cisco Products

Table 4-1 describes Cisco components.

Table 4-1 Cisco Components

Vendor	Model	Description
Cisco	IR 829	Vehicle Onboard Mobile Router with integrated 4 port gigabit Ethernet switch with PoE, Wi-Fi AP and LTE cellular modem. Also used for Connected Bus Stop.
Cisco	IE 4000	Ruggedized gigabit Ethernet switch with PoE for onboard vehicle.
Cisco	IE 2000	Alternate ruggedized gigabit Ethernet switch with PoE for onboard vehicle.
Cisco	IW3702	Industrial 802.11ac Wave 1 AP to provide wireless infrastructure in Maintenance Yard.
Cisco	Catalyst 3850	Gigabit Ethernet switch with full Universal PoE support for Maintenance Yard network. Incorporates Layer 3 gateway functionality, 10 GE uplinks for connectivity to Metro Network, and stacking capability for easy expansion.
Cisco	WLC5520	Wireless LAN Controller for managing IW3702 APs with 10GE connectivity to data center. Exact model of WLC implemented should be matched to the scale of the deployment.
Cisco	ASR 903/907	Unified MPLS-capable modular aggregation router node with GE, 10GE, and 100GE interface support.
Cisco	ASR 920	Unified MPLS-capable fixed configuration pre-aggregation router node with GE and 10GE interface support.
Cisco	ASR 1000	Hub router for DMVPN termination from vehicles.

Table 4-1 Cisco Components (continued)

Vendor	Model	Description
Cisco	ASA5545-X	High-capacity firewall for protection of enterprise network infrastructure from public Internet peering connections.
Cisco	IP7070	5 Megapixel 360° IP Camera with IP66/IK10 housing rating. Includes digital I/O and audio input.
Cisco	IP3050	720p WDR IP camera with IP66/IK10 housing rating. Includes digital I/O and audio input.
Cisco	VSMS/VSOM	Cisco Video Surveillance Media Server and Operations Manager.
Cisco	Instant Connect	Cisco Instant Connect (formerly IPICS) system for PTT.
Cisco	Android Endpoint for Instant Connect	Android application providing VoIP endpoint functionality for Instant Connect PTT service. Integrates with Sonim XP7 Android smartphone.
Cisco	IP Turret	Dispatcher console for Instant Connect integration.
Cisco	Jabber	Software endpoint client for Instant Connect integration.

All onboard electronics installed in the vehicle shall comply with requirements of SAE J1455 interior environments. Details of the SAE J1455 standard are available at the following URL:

- http://standards.sae.org/j1455_201208/

All antennas and other components installed on the exterior of the vehicle shall comply with requirements of the SAE J2527 work-in-progress (http://standards.sae.org/wip/j2527/) and the exterior environment requirements of SAE J1455.

All products included in the solution shall also comply with Cisco safety requirements and product qualification guidelines.

Third Party Products

Table 4-2 describes third party components.

Table 4-2 Third Party Components

Vendor	Model	Description
Advantech	ARK-2151V	Ruggedized server option to host VSMS for Video Surveillance cameras on vehicle. Used for validation of onboard server role in Connected Mass Transit System. • http://www2.advantech.com/products/todatasheet.aspx?mod_id=dfecf53f-27c0-4200-9b71-28e8d73f0636
Nexcomm	VTC series	Ruggedized server option to host VSMS for Video Surveillance cameras on vehicle. Used for validation of onboard server role in Connected Rail system. • http://www.nexcom.com/Products/mobile-computing-solutions/in-vehicle-pc

Table 4-2 Third Party Components (continued)

Vendor	Model	Description
Davra	RuBAN	Network Management System and Data Acquisition/Analytics platform: • http://www.davranetworks.com/product/features
SONIM	XP7	Ruggedized LTE/Wi-Fi Android smartphone: • http://www.sonimtech.ca/xp7/xp7.php
B&B Electronics	HDV100A3	Heavy Duty Vehicle interface adapter to translate between the most common vehicle buses and the IR 829 Serial interface: • http://www.bb-elec.com/Products/Telematics-MRM-Solutions/Heavy-Duty-Vehicle-Converters/HDV-Vehicle-Interface-Adapters.aspx

All onboard electronics installed in the vehicle shall comply with requirements of SAE J1455 interior environments. Details of the SAE J1455 standard are available at the following URL:

- http://standards.sae.org/j1455_201208/

All antennas and other components installed on the exterior of the vehicle shall comply with requirements of the SAE J2527 work-in-progress (http://standards.sae.org/wip/j2527/) and the exterior environment requirements of SAE J1455.

All products included in the solution shall also comply with Cisco safety requirements and product qualification guidelines.

Software Feature and Application Support

Table 4-3 outlines the software features and application supported in the Connected Mass Transit System in this phase.

Table 4-3 Software Features and Applications Supported

Software Application	Function
RuBAN	Geographical Information System (GIS)
	Cisco Devices Zero Touch Provisioning
	3rd Party Device Management
	Automated Network Management (such as CPU, MEM, RSSI, Wi-Fi Traffic, and user types)
	Rules, Policies, and Alert Engines
	Vehicle Telematics
	Vehicle GPS Tracking, Geo fencing
	Vehicle Driver Management
	Physical Security Integration
	Traveler Information (arrival time)
	Route Replay

Table 4-3 Software Features and Applications Supported (continued)

Software Application	Function
Connected Safety and Security	Video Surveillance Software
	Video Analytics (such as panic button video triggering, event tagging, event recording, and event streaming)
Cisco Instant Connect System	Cisco Instant Connect Server
Web Portal	Wi-Fi User Authentication

System Functional Considerations

This chapter includes the following major topics:

Data Center

All centralized system aspects and backend services of the Connected Mass Transit System 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 Mass Transit 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

Metro Network

Cisco Connected Roadways

The Connected Mass Transit System design requires high-bandwidth, multiservice transport to be supported between the maintenance yard networks and the centralized Data Center environment hosting all the backend systems. It's likely this transport will be deployed and managed in the context of a larger city-wide Metro Network infrastructure. The Metro Network design implemented in the Connected Mass Transit System is extensively documented in the *Cisco Connected Roadways System Design and Implementation Guide*. The Connected Roadways system provides detailed recommendations and best practices for deploying a highly scalable and resilient network deployment using Unified MPLS for service transport. For more information, please contact your Cisco account team representative to obtain a copy of the Design and Implementation Guide. High level information can be found at the following URL:

- http://www.cisco.com/web/strategy/transportation/roadways.html

Quality of Service

The Connected Mass Transit System 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 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 Mass Transit System, with mapping between these mechanisms supported at the boundaries between the different transport mechanisms.

The classes of service shown in Table 5-1 are implemented in the Connected Mass Transit System, and are shown with mappings between representative classification markings for each type of classification.

Table 5-1 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 Mass Transit System design, 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:

- **The LTE cellular connection to and from the vehicle**—In typical conditions, an LTE connection to a moving vehicle will be expected to support 10 to 20 Mbps of throughput. Ideally, the MSP will support multiple LTE QCI values for the service provided to the MTA, and prioritization of expedited forwarding (EF) and assured forwarding (AF) classes over best effort (BE) traffic can be guaranteed in both directions. If the MSP does not offer multiple QCI classes, then prioritization of EF and AF traffic can still be accomplished in the upstream direction from the IR 829 router toward the MSP. In either situation, the LTE connection will have less bandwidth than the other wired and wireless links feeding traffic into the router, a hierarchical QoS policy is deployed on the cellular uplink of the IR 829 router, with a parent shaper equivalent to the uplink bandwidth on the LTE link, and child classes defining the proper queuing treatment for each class.
- **The edges of the Metro Transport network**—The uplinks from each Maintenance Yard to the Metro Transport network are 10 Gbps Ethernet links, and as such, will not likely encounter much congestion under normal circumstances. However, it is still important to deploy QoS to prioritize EF and AF traffic from local sources over the WBDT traffic generated by the vehicles parked in the yard, to ensure that critical services such as VoIP communications and Video Surveillance function without any interference from traffic due to vehicle system updates and file offloads. Likewise, a

bottleneck may occur at the uplinks from the Metro Transport network into the data center and operations center. As all of these links are using the available line rate of the underlying physical connection, a flat QoS policy to define the proper queuing treatment for each class is implemented.

- **Internet peering connections to the MSP and Internet SP**—Often, the bandwidth of the service purchased from a Service Provider will 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 MTA'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 PHY to indiscriminately drop excess packets.

Routing and Network Address Translation

The Connected Mass Transit System design provides a flexible, dynamic, and extensible routing infrastructure, with the ability to accommodate the requirements of all services enabled in a converged system. This section focuses on explaining the mechanisms implemented in the onboard gateway located on the vehicle and how it interacts with backend systems. The exact configurations for implementing these mechanisms is described in the *Connected Mass Transit Implementation Guide*.

The onboard gateway implements the following functions to enable the services supported in the Connected Mass Transit System:

- **Dynamic Client IP Addressing**—By using DHCP, the onboard gateway enables dynamic IP addressing for onboard systems, simplifying the provisioning and maintaining of those systems. Also, by combining this with NAT, the onboard configuration can use identical private IP subnets for all vehicles, further simplifying system deployment. DHCP address pools can be configured on the onboard gateway for multiple IP subnets and managed on a per-interface or per-subinterface basis. The DHCP server function on the onboard gateway supports static mapping of IP addresses to MAC addresses or DHCP identifiers, allowing for devices to receive persistent IP addressing. Alternately, IP address ranges can be reserved in any pool to accommodate devices which require static addressing to be configured on the device. Finally, the DHCP server on the onboard gateway supports all DHCP options, allowing for additional information, such as the IP addresses of Domain Name Server (DNS) and Trivial File Transfer Protocol (TFTP) servers, to be passed to other systems onboard.
- **Dynamic Routing**—The onboard gateway implements an IGP to dynamically configure routing of traffic between onboard systems and backend systems and manage traffic over the wireless offboard connections. The Connected Mass Transit System implements EIGRP for this function. By establishing EIGRP adjacencies with hub routers in the Ops Center, the onboard gateway is able to automatically maintain optimal data routing to and from the onboard systems. EIGRP timeouts and other parameters can be tuned to optimize performance given the specific criteria of a particular deployment.
- **Policy-Based Routing**—Routing decisions by the IGP implemented on the onboard gateway can be influenced by several mechanisms, including static routes injected into the routing table, routing metrics to adjust link preference, and route-maps to control the treatment of routing information within the IGP. The system design uses all of these mechanisms in implementing the services supported.

- **Multiple Loopback Addresses**—A Loopback interface on a router is used to provide a virtual gateway address for element management or for an individual service. The onboard gateway is able to support multiple Loopback interfaces, providing gateway functionality for multiple services simultaneously. Each Loopback interface is advertised into the IGP dynamic routing table, and is combined with NAT to support multiple onboard devices for a particular service.
- **Network Address Translation (NAT)**—The onboard gateway implements NAT to translate the address information between onboard "private" IP address spaces and routable "public" IP address spaces in real-time. NAT mapping between IP addresses is handled dynamically by the onboard gateway as it receives traffic originated onboard that is destined for an offboard IP address. If the traffic pattern for a particular service requires a data connection to be originated initially by an offboard system, such as the case with Video Surveillance, then a static NAT entry is configured on the onboard gateway to allow for that traffic flow.
- **Network Address/Port Translation (NAPT)**—Also known as "overloaded NAT" or simply "Port Address Translation (PAT)." NAPT enables multiple devices in a private IP address space to use a single routable public IP address. Each private IP address and port with an active data connection is mapped to a unique public IP address and port combination, allowing multiple devices to share a single routable IP address effectively. As with NAT, NAPT allows for static mapping entries as well.

The Connected Mass Transit System design strives to maximize operational simplicity. From a design best practice perspective, both for initial deployment as well as ongoing maintenance and management, keeping the configuration of the system as dynamic as possible supports this goal. Supporting dynamic addressing, routing, and other gateway functions on the onboard gateway speeds initial deployment and simplifies component replacement. Only in cases where systems require static configuration for proper function should static mechanisms be used.

CHAPTER 6

Security, High Availability, and Scale

This chapter includes the following major topics:

Security

The Connected Mass Transit System implements security mechanisms through the design to provide proper service traffic protection, separation, and system authorization. The various mechanisms and methodologies implemented are described in this section.

The Wi-Fi connections between the vehicle workgroup bridge and yard APs implement WPA2 security, which includes enterprise level authorization and encryption of traffic. The Wi-Fi subsystem 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).

All network nodes in the Connected Mass Transit System 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 interface that could be exposed to physical access by untrusted persons, such as the router and switch onboard the vehicle, has port security with 802.1X authorization enabled to prevent unauthorized access to 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 MTA. Cisco provides full Mobile Device Management (MDM) functionality for secure mobile device deployment, which is fully compatible with the Connected Mass Transit System.

Outside access to the operations center infrastructure via UNI connections to the MSP 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

The Connected Mass Transit System supports network layer security between the vehicle onboard router and hub router at command control center for all enterprise applications and services by implementing DMVPN tunnels. The DMVPN implementation in the onboard router is capable of supporting many different encryption standards: DES, 3DES, AES 128, AES 192, and AES 256. The Connected Mass Transit System recommends implementing the strongest standard and largest keys supported to provide the most secure connection. The only traffic not transported in the DMVPN tunnel is passenger Internet traffic, which is routed directly to the Internet through the MSP. This further separates any passenger traffic from enterprise application traffic, and has the added benefit of reducing the bandwidth requirement for the peering connection to the MTA's data center.

As the DMVPN tunnels are terminated on a hub router situated in a DMZ behind the security node, this requires certain inbound ports, namely UDP 500 and 4500, to be opened on the security node, potentially allow traffic in from any source. To protect the hub router from possibly becoming an attack vector to the rest of the network, VRF-lite is configured in conjunction with the DMVPN configuration. This configuration prevents any traffic not encapsulated within a DMVPN tunnel from gaining access to any infrastructure behind the hub router.

System Redundancy and Reliability/Availability Models

The network infrastructure on the vehicle has no resiliency requirements. The network infrastructure components used on the vehicle 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 vehicle. If the server hosting VSMS on the vehicle encounters issues, or if no server is deployed, then recording of video is stored on local solid-state storage on the individual IP cameras.

- The Yard Network design requires load-balancing and failover functionality between Wi-Fi APs in the yard, to facilitate an equitable distribution of vehicle workgroup bridge connections between APs, and to provide handoff of WGB connections from one AP to another if an AP is taken out-of-service. Load-balancing and resiliency of connections to the Wi-Fi infrastructure is controlled by the WLC.

  Redundancy for the switching infrastructure of the Yard network is accomplished by implementing switch stacking using two or more Catalyst 3850 routers. Redundancy for the uplinks to the Metro Network pre-aggregation nodes is accomplished by implementing LACP.

- The Metro Network design implements ring topologies, providing resilient connectivity to nodes within the network in the case of a single link or node failure. Uplink connections from any yard network are terminated on two different nodes in the Metro Network using mLACP to provide link and node redundancy. Uplink connections from the Metro Network to the Operations Center infrastructure uses two different nodes, again implementing mLACP. All resiliency design mechanisms are covered in detail in the *Connected Roadways Design and Implementation Guide*.

Redundant UNI links from the MSP and Internet Service Provider may be implemented. Typical uptime SLAs for these UNI connections will exceed the uptime requirements for the Connected Mass Transit System, so the cost versus the benefit of redundant UNI links must be analyzed by the MTA. 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 Mass Transit System.

Initial Scalability/Performance Assessment

Scalability and performance criteria for individual service areas are contained within the service descriptions in this document in Chapter 2, "System Supported Services and Models." The systems and platforms proposed in the Connected Mass Transit System design are geared to easily handle a vehicle fleet of 4000 vehicles, and can be scaled to handle even larger fleets.

LTE Service Scalability

The following assumptions are made in calculating the scalability requirements of the services enabled over LTE cellular connections from vehicles:

- 25 passengers per vehicle using Wi-Fi internet access
- 400Kbps minimum throughput available to each user
- 90% of buses are in operation simultaneously

Using these assumptions, each vehicle requires approximately 10 Mbps of bandwidth for passenger Internet traffic. A single LTE link from a vehicle should accommodate approximately 15 Mbps of bandwidth, leaving 5 Mbps for Voice communications, GPS location, engine telematics, and other Enterprise service traffic. This far exceeds the amount of traffic expected for all these services, which should be on the order of well under 1 Mbps. If the MTA needs access to live streaming of video surveillance traffic during an incident, which may require greater than 5 Mbps, available bandwidth for passenger Internet traffic is temporarily reduced through the QoS service policies implemented on the cellular uplink.

With 90% of vehicles in operation simultaneously, approximately 90000 users exist across the Mass Transit system. The total bandwidth utilization of all these users toward the MSP network is approximately 36 Gbps. MSP networks are typically scaled to handle an order of magnitude larger number of users, so this is not an issue for the MSP. As only the Enterprise service traffic needs to be carried to the Mass Transit Operations Center, and this traffic is expected to be on the order of around a gigabit per second, then either two gigabit Ethernet links or a 10 gigabit Ethernet link with a sub-linerate service is more than sufficient for the UNI connection from the MSP to the MTA's data center.

Maintenance Yard Scalability

The following assumptions are made in calculating the scalability requirements of the services enabled over Wi-Fi connections to the vehicles parked in a maintenance yard or agency parking lot:

- 200 to 400 vehicles in a yard at the beginning or end of a shift
- Vehicle communication systems remained powered on for 30 minutes after parked
- The WGB Wi-Fi link of a single vehicle is capable of 150Mbps of throughput

Not all vehicles in the yard are connected and transmitting simultaneously. At the end of shift, vehicle arrival at the yard is staggered to prevent traffic jams. At the beginning of shift is likely be the greatest number of simultaneous vehicle connections as the vehicles are started, however no video surveillance files exist to be transferred at this point, so bandwidth requirements are greatly reduced.

The Connected Mass Transit System design targets a ratio of vehicles to yard APs of approximately 10 to 1. If greater throughput is needed, then more yard APs can be deployed. The number of vehicles connected to a single AP receive an equal ratio of bandwidth from the AP when all vehicles are transferring data simultaneously, so expected throughput for planning is approximately 15 Mbps. This level of throughput supports approximately 2.5 GB of data transfer in a 30 minute window.

At 150 Mbps of aggregate throughput per yard AP, under the worst case of start of shift when all vehicles may be transmitting simultaneously, the switching infrastructure in the yard, and the uplinks to the Metro Network, could experience an aggregate throughput load of 6 Gbps. This is easily handled by the switching nodes and 10GE uplinks to the Metro Network.

Acronyms and Initialisms

Table A-1 lists the acronyms and initialisms used in this document.

Table A-1 Acronyms and Initialisms

Term	Description
AP	Access Point
ASA	Cisco Adaptive Security Appliance
ASR	Cisco Aggregation Services Router
AVL	Automatic Vehicle Location
BGP	Border Gateway Protocol
CAD	Computer Aided Dispatch
CAD/AVL	Computer-Aided Dispatch/Automatic Vehicle Location
CAN Bus	Controller Area Network Bus
COS	Class of Service (802.1p)
CPE	Customer Premise Equipment
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Connected Transportation System
CVD	Cisco Validated Design
DHCP	Dynamic Host Control Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EEM	Embedded Event Manager
EIGRP	Enhanced Interior Gateway Routing Protocol
ETA	Estimated Time of Arrival
FPS	Frames Per Second
GETVPN	Group Encrypted Transport VPN
GIS	Geographical Information System

Table A-1 Acronyms and Initialisms (continued)

Term	Description
GLOSNASS	Globalnaya Navigazionnaya Sputnikovaya Sistema, a Russian version of GNSS
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSMA	Groupe Spéciale Mobile Association
IGP	Interior Gateway Protocol
IoT	Internet of Things
IPICS	Cisco IP Interoperability and Collaboration System
IPSec	Internet Protocol Security
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
IVU	In-Vehicle Unit
L3VPN	Layer 3 Virtual Private Network
LACP	Link Aggregation Control Protocol
LEAP	Lightweight Extensible Authentication Protocol
LDP	Label Distribution Protocol
LISP	Location-ID Separation Protocol
LSP	Label-Switched Path
LTE	Long Term Evolution (4G)
LTS	Long Term Storage
MDM	Mobile Device Management
mLACP	multichassis Link Aggregation Control Protocol
MIMO	Multiple Input, Multiple Output
MP-BGP	Multiprotocol Border Gateway Protocol
MTA	Mass Transit Agency
MSP	Mobile Service Provider
NAPT	Network Address/Port Translation
NAT	Network Address Translation
NMEA	National Marine Electronics Association
OAM	Operations, Administration, and Maintenance
OBDI	On-Board Diagnostics
OBE	On Board Equipment
OSPF	Open Shortest Path First
PAL	Phase Alternating Line
PEAP	Protected Extensible Authentication Protocol
PfR	Performance Routing
PHB	Per Hop Behavior

Table A-1 Acronyms and Initialisms (continued)

Term	Description
PNR	Cisco Prime Network Registrar
POE	Power over Ethernet
PSK	Pre-shared Key
PTT	Push-to-Talk
QCI	QoS Class Identifier
QoS	Quality of Service
rLFFA-FRR	remote Loop-Free Alternate Fast Reroute
RSSI	Receive Signal Strength Indicator
RTPI	Real-time Passenger Information
SAE	Society of Automotive Engineers
SCEP	Simple Certificate Enrollment Protocol
SEN	Service Edge Nodes
SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TSL	Transit Signal Priority
UCS	Cisco Unified Computing System
UDP	User Datagram Protocol
UNI	User-to-Network
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VLU	Vehicle Logic Unit
VOIP	Voice over Internet Protocol
VSOM	Cisco Video Surveillance Operations Manager
VSMS	Cisco Video Surveillance Media Server
WBDT	Wireless Bulk Data Transfer
WDR	Wide Dynamic Range
WGB	Workgroup Bridge
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WMM	Wi-Fi Multimedia

Table A-1 Acronyms and Initialisms (continued)

Term	Description
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access, Second Generation