



Converged Public Transportation – Mass Transit

Design Guide

October 2023



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.” ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

©2023 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Contents

Converged Public Transportation – Mass Transit Design Guide.....	5
Introduction	5
Use Cases/Services/Deployment Models	5
System Overview.....	6
System Supported Services and Models	6
Service Architecture Overview.....	6
Service Inventory / Models	6
Wi-Fi Network Services.....	8
Vehicle Location Tracking and Reporting.....	10
Vehicle Location Data Correlation.....	12
Vehicle Telemetry Data Collection.....	12
Automated Passenger Counting	13
Fare Collection	13
Passenger Information Signs	14
Vehicle Two-way Voice Communication	15
Vehicle Video Surveillance	16
Event Triggered Video Surveillance	17
Vehicle Panic Button	18
CAD/AVL	19
Wireless Bulk Data Transfer.....	20
Connected Passenger Stop.....	21
System Architecture	23
Related Efforts.....	24
Functional Description.....	24
Connected Transit Vehicle Onboard Network and Systems.....	24
IR1800 Router	29
Addressing	30
Cisco IE Switches	30
Passenger Information Signs.....	31
Automatic Passenger Counting (APC).....	31
Fare Collection.....	31
Two-way Voice Communication	31
Video Surveillance	32

CAD/AVL VLU	32
Panic Button	32
Power Management.....	32
Backhaul-WAN Interfaces for Transit Vehicles.....	32
Connected Transit Stop.....	34
Additional WAN backhaul interfaces for stops or stations.....	35
Yard Network	35
Transit Management (Operations) Center Systems.....	38
Network Management Systems	40
Traffic Flow and Security	44
System Components.....	46
Cisco Products	46
System Functional Considerations.....	48
Data Center.....	48
Cisco Connected Roadways.....	48
Cisco SD-WAN for Industrial Markets.....	48
Security, High Availability, and Scale	51
Quality of Service (QoS)	51
Security.....	52
Installation Best Practices	55
General Considerations for Vehicle Installation	55
Special Considerations for Vehicle Installation.....	56
Power Source Location and Considerations	56
Ignition Sense Location and Considerations.....	57
Power On/Off Using Vehicle Ignition.....	57
Ground and Return Location Considerations	57
Antenna Mounting Considerations.....	57
Data, Antenna, and Power Cable Routing Considerations	58
Splicing Requirements	59
Battery Connection Requirements.....	59
Glossary	60

Converged Public Transportation – Mass Transit Design Guide

The intended audience for this document is Cisco account teams, Cisco CX teams, and Systems Integrators working with Transit agencies. It may also be used by the Transit agencies directly, to understand the features and capabilities enabled by the Cisco Converged Public Transportation system design.

Introduction

This guide provides a comprehensive explanation of the Cisco Converged Public Transportation design. It includes information about the system architecture, supported services, and possible deployment models. The guide also recommends best practices and potential issues when deploying the reference architecture.

Most of the examples given are directed toward connected buses. The applicability of the solution architecture includes buses, trams, and commuter metro rail deployments based on common use cases and solutions.

Use Cases/Services/Deployment Models

This guide addresses the following technology use cases:

- Passenger, Transit Worker, and Emergency personnel Wi-Fi Network Services
- Vehicle Location and Telemetry Data Collection
- Vehicle Location Tracking
- Vehicle Location Data Correlation (value added services)
 - RSSI heat map
 - Road surface mapping*
 - Driver behavior monitoring*
 - Emissions monitoring
- Passenger Real-Time Information Signs*
- Automated Passenger Counting (APC)
- Fare Collection*
- Vehicle Two-way Voice Communication
- Vehicle Video Surveillance – Event Triggered Video Surveillance
- Vehicle Panic Button
- CAD/AVL*
- Wireless Bulk Data Transfer
- Connected Passenger Stop
- Connected Depot/Yard/Maintenance Facility

**These services were not validated as part of the CVD*

System Overview

The Cisco Converged Public Transportation System provides an end-to-end design for service delivery to a Mass Transit infrastructure, including connectivity to transit vehicles, bus/rail stops, and maintenance yards/depots. The system provides a converged, multi-service, secure, and standards-based infrastructure on which passenger and operational capabilities for transit vehicles can be delivered. It replaces redundant, proprietary, patchwork siloed application solutions with limited or no interconnectivity and lack of coordination. This results in reduced CAPEX, improved operational efficiency, better data utilization, increased ridership, and improved safety and security for mass transit riders and drivers.

System Supported Services and Models

Service Architecture Overview

The Cisco Converged Public Transportation system implements a comprehensive infrastructure which supports multiple services typical in transit fleets as well as additional value-added services supported through the Cisco architecture. These services are easily extensible to multiple forms of public transit deployments. This section details the services supported by the Converged Public Transportation system.

Service Inventory / Models

Table 1 is services supported in this phase of the Converged Public Transportation system.

Table 1 Supported Services

Service Category	Service Definition
Wi-Fi network services	<p>Provides Wi-Fi Network services to passengers, transit agency workers, emergency personnel, Wi-Fi connected devices, and for the transit vehicle to connect to the maintenance yard.</p> <p>Provides internet access to passenger and transit agency workers from bus/rail stops.</p> <p>Passenger access is authorized by the passenger accepting the terms & conditions of using the service before gaining access to Internet services.</p> <p>Access for emergency personnel and transit agency employees requires username and password authentication.</p>
Vehicle Location Tracking	<p>Relays vehicle location information to the dispatch operator system in real time. Vehicle location is determined by Global Positioning System (GPS) / Global Navigation Satellite System (GLOSNASS/GNSS) integration with the vehicle onboard infrastructure.</p>
Vehicle Location Data Correlation	<p>Correlation of other service performance information with vehicle location such as Received Signal Strength Indicator (RSSI) and acceleration/tilt.</p> <p>Provides historical data for understanding cellular coverage along the vehicle route, driver behavior, and road surface quality.</p> <p>Can be used by the transit agency to optimize the bus route and scheduling, driver training, plan for crew shift schedules, and to provide feedback to road maintenance crews concerning areas in need of repair.</p>

Vehicle Telemetry Data Collection	<p>Relays real-time vehicle performance information, such as speed, RPM, air intake and coolant temperatures, fuel level, and idle time from vehicle Controller Area Network (CAN) bus to the Fleet Management system.</p> <p>Provides ongoing monitoring of transit vehicle operation and supplies information for predictive maintenance algorithms to detect and correct impending failures before issues affecting service occur.</p>
Passenger Information Signs	<p>Displays real-time schedule updates and other information inside the vehicle and at the transit station on updatable message signs.</p> <p>This information includes vehicle route, next stop, estimated arrival time, and any delays in schedule.</p>
Passenger Counting	<p>Real-time counting of passengers on the transit vehicle with updates provided at each stop or station as passengers enter and exit an in-service vehicle.</p> <p>Information includes location of stop, passengers entering, passengers exiting, net passenger count when leaving the stop or station.</p>
Fare Collection	<p>Real-time collection of fare payment via credit, debit card, prepaid transit card or ticket. All methods of payment are verified with supporting financial systems of the transit agency.</p>
Vehicle Two-way Voice Communication	<p>Two-way voice communications with Push-To-Talk (PTT) support between drivers, supervisors, and operations team at dispatch and maintenance centers.</p> <p>Enables interworking between voice over IP (VoIP) systems and legacy digital radio communications through Instant Connect integration.</p>
Vehicle Video Surveillance	<p>Onboard vehicle systems support up to eight separate IP video surveillance cameras.</p> <p>Video recordings are stored to an onboard ruggedized server, or to integrated flash storage in the camera if an onboard server is not deployed.</p> <p>On-demand real-time video transmission over cellular backhaul is supported.</p> <p>Recorded video is offloaded via Wi-Fi to long-term storage for later retrieval when the transit vehicle is parked in maintenance yard.</p>
Event Triggered Video Surveillance	<p>Video recording and real-time video transmission can be triggered by certain events and triggers, such as door open or close, driver request, loud noises, rapid acceleration or deceleration, and other events.</p>
Vehicle Panic Button	<p>Concealed input triggered by the vehicle driver to report emergencies and request assistance at any time.</p> <p>The panic button will allow the driver to contact emergency authorities and bus operation team directly over the Instant Connect system and via alerts.</p> <p>The trigger can be used to start video recording and/or streaming to capture relevant incident information.</p>
Wireless Bulk Data Transfer	<p>When parked in a maintenance yard, the vehicle establishes a high bandwidth backhaul network connection via Wi-Fi to the infrastructure in the yard.</p> <p>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 including route information, recorded public announcements, and software updates for vehicle onboard systems.</p>
Connected Bus/Rail Stop	<p>Provides passenger Wi-Fi services at a bus stop while passengers are waiting for a bus.</p> <p>Provides Estimated Time of Arrival (ETA) updates on vehicles in route to the bus stop.</p> <p>Network connectivity to the bus stop is provided via wired connectivity,</p>

	or via cellular uplink if no wired infrastructure is deployed.
Fleet Management Services & CAD/AVL	There are many fleet management software solutions on the market today, each using data provided by onboard systems to perform location tracking, vehicle telemetry data collection, geofences, vehicle dashboard reports, policy-triggered events, video surveillance integration. The key onboard systems supporting the Fleet Management services are the CAD/AVL system and driver terminal.
Connected Maintenance Yard and Depot	Provides WAN connectivity for the transit vehicle off the cellular network to the transit network and transit management center.

Wi-Fi Network Services

The Cisco Converged Public Transportation system provides an integrated Wi-Fi access point solution with wireless networking services for passengers, transit workers, emergency personnel, and wirelessly connected onboard systems.

The following service types are supported via Wi-Fi connectivity:

- Passenger Internet Services
- Enterprise infrastructure and Internet access for Mass Transit employees
- System access for Law Enforcement and Emergency Services
- Wireless systems/devices on the transit vehicle such as VoIP Push-To-Talk (PTT) endpoints, servers, and sensors.

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

Passenger Internet Services

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 splash screen (login page hosted by the onboard Wi-Fi infrastructure or centralized controller). This login page presents the Terms and Conditions to which the passenger must agree before accessing Internet services. Once the passenger accepts the terms and conditions access to Internet services is permitted without further impediment for the duration of their trip.

Wi-Fi across the journey

Passenger Wi-Fi session persistence throughout the passenger journey is also possible, if desired by the transit agency. Here, the passenger can remain authenticated and connected to a set of changing Wi-Fi access points across their journey within the transit system.

A passenger can enter a bus or rail stop/station, connect to the local access point as described above, and then transition to the access point on the vehicle without seeing an additional login page. Similarly, if exiting the vehicle, the passenger can also transition to the access point in the stop/station without seeing an additional login page. This method requires a common WLC (wireless LAN controller), such as the C9800, to be used in the data center overseeing the access points so it can provide session awareness/continuity and requires that the access points are running in CAPWAP mode. The SSID for Passenger Wi-Fi can be configured on the WLC to use FlexConnect with local switching so that Internet traffic does not need to be tunneled back to the WLC.

If Wi-Fi session persistence is not a priority, passenger Wi-Fi services can be run entirely locally to the vehicle and stop or station. Locally the access point would be running in EWC or WGB+Hotspot mode for standalone operation.

Transporting passenger internet traffic

Passenger Internet service traffic is transported over one of the following:

- Cellular network where it is routed directly by the cellular provider to the Internet.
- CURWB backhaul where it is routed to the internet by the supporting backhaul network.
- WGB backhaul for when the vehicle is at an inter-modal station, for example.

Non-passenger traffic

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

If CURWB or WGB is the active backhaul, this non-passenger traffic could optionally be sent over the FlexVPN tunnel, or not – depending on connectivity and security requirements. This is another case where the access point operates in CAPWAP mode so that authentication can be centralized at a WLC in the back office in addition to other security products such as Identity Services Engine (ISE).

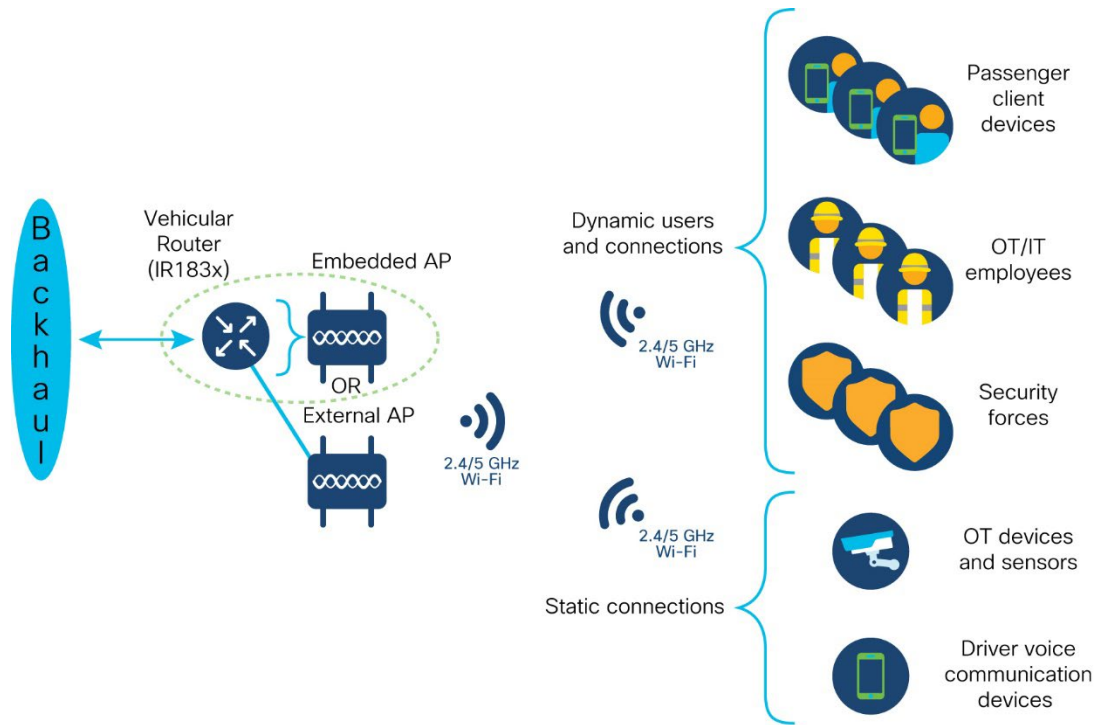
Each Wi-Fi SSID is mapped to a separate Virtual Local Area Network (VLAN) in the onboard network infrastructure, providing the required service traffic separation required by the transit operator.

The Converged Public Transport system implementation for Wi-Fi network services targets supporting 50 concurrent users on a vehicle, providing a minimum of 1 Mbps of bandwidth per user. Depending on 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 onboard systems using Wi-Fi, Transit employees, and Emergency Service personnel is prioritized over passenger Internet services.

The following diagram depicts two access points behind the IR1800 router, one internal, and one external. The different devices and users are not restricted to one AP or another. The addition of the external AP is to increase the coverage area in the case of a large vehicle such as an articulated bus or a multi-car vehicle for light rail. It can also be used to enable easier installation of antennas and cabling.

Figure 1 Wi-Fi Connectivity



388486

Vehicle Location Tracking and Reporting

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 Industrial Router obtains location data from 2 possible sources – cellular modem with integrated GPS receiver, and an optional high resolution GNSS PIM module plugged into the router.

The Cisco Converged Public Transportation system supports multiple methods and destinations for delivery of NMEA GPS coordinates.

- Automatic reporting to the SD-WAN Manager (formerly vManage) over the management tunnel at a periodic timed interval. APIs are available to export this data to a third-party application.
NOTE: Currently, coordinates from the GNSS module are not reported to SD-WAN Manager. This will be addressed in a future software release.
- Automatic reporting to the IoT Operations Dashboard over the management tunnel at timed intervals configurable from 5 seconds to 30 seconds. APIs are available to export this data to a third-party application.
NOTE: Currently, coordinates from the 5G and GNSS modules are not reported to IoT OD. This will be addressed in a future software release.
- Other options:
 - IOx docker application request for GPS coordinate updates with delivery to any reachable IP address onboard the vehicle or to any of the transit applications off the

vehicle. This solution requires a simple third-party application to perform the polling and delivery of the NMEA GPS data.

- Interval-based NMEA formatted IP packet delivery to any reachable IP address onboard the vehicle or to any of the transit applications off the vehicle. This capability is available directly via IOS configuration in the router.

Both options allow for location information to be distributed in a NMEA compliant format via streaming TCP/IP to other systems on the vehicle as well as transit applications.

The following illustration shows a solution for merging RSSI or accelerometer/gyroscope readings, respectively, as examples. Note that at the time of publishing this document, reading sensor data from the accelerometer and gyroscope on the IR1800 mainboard is not yet available, but is scheduled to be supported in the upcoming IOS-XE 17.13.1 release which is not validated for this CVD.

Figure 2 RSSI Mapping IOx Application

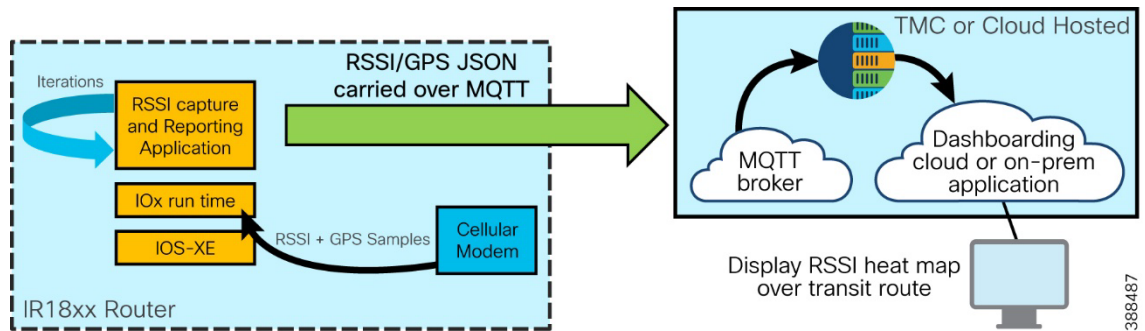
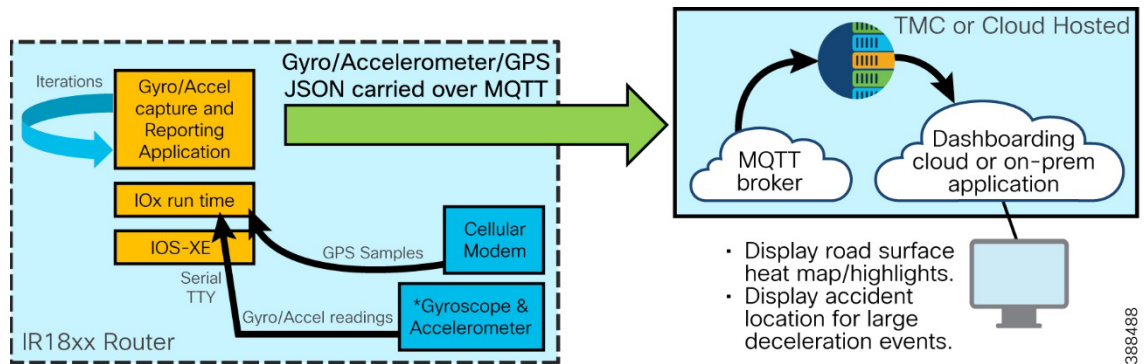


Figure 3 Road Surface Mapping / Accident Detection IOx Application



IOx Docker Application Note and Disclaimer

Several of the services and capabilities described in this document use an IOx docker application running on the IR1800 series router to perform data fusion and processing on the transit vehicle. Cisco has created sample applications as reference designs for those interested in leveraging those applications as a launching point to a tailored custom solution. Cisco does not hold any liability for the use of the sample code.

To learn more about IOx applications and how to develop them, go to the Cisco Developer Network (DevNet) section at

<https://developer.cisco.com/docs/iox/#/introduction-to-iox>.

At the time of this writing, the IOx application life cycle management is not available using SD-WAN Manager.

Vehicle Location Data Correlation

Vehicle location data can be shared with other onboard systems as well as edge applications (in this case, IOx docker applications). The Converged Public Transportation solution provides some reference applications that can be used by the customer or integrator and adapted to their specific needs. The applications can be found on GitHub at the following link:

<https://github.com/keholcom/vehicle-obd2>.

Example applications include:

- Correlation of vehicle location with Received Signal Strength Indicator (RSSI). The output of this reported data produces a heat map showing the quality of cellular coverage across the route that can be used to communication coverage issues with the local cellular carrier.
- Correlation of vehicle location with acceleration/tilt to characterize and monitor road surface conditions and driver behavior.
 - The output of this reported data provides a heat map showing road surface conditions along the bus route which can be used to adjust bus routes and schedules to avoid unnecessary wear and tear as well as to provide a public service by sharing the collected data with the road maintenance crews.
 - The acceleration/tilt can also be used to monitor driver behavior such as fast turns, hard braking, or even detection of an accident.
 - Note: This application is not available to the public in Github at time of publishing but may be added in the future.
- Correlation of vehicle location with CANbus data
 - Location stamping of CANbus telemetry data is a powerful way to assess traffic patterns, driver behavior, fuel utilization, hard braking zones, etc. to optimize bus routes and schedules

Other examples include emissions monitoring along a transit route or dwell time at transit stops. There are many distinct pieces of information that can be correlated with location data to provide increased insights into one or more aspects of operational performance.

Vehicle Telemetry Data Collection

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 to capture vehicle utilization data.
- Vehicle health measurements such as oil temperature, engine temperature, and tire pressure. This data collection provides ongoing monitoring of transit vehicle operation and provides information for predictive maintenance algorithms to detect and correct impending failures before these issues occur.
- Vehicle operational data such as door open or closed, stop request, or emergency request which is information the transit operator may want to track.

Similar to vehicle location data, vehicle CANbus data (J1939 or OBD-II) is collected at a configurable polling interval and transmitted to fleet management software in the transit management center or cloud for processing. The delivery of that data is accomplished through an IOx docker application which consumes the CANbus data, filters the data to leave only

information of interest, packetizes the data and transmits it to the fleet management software. An example IOx docker application which can be tailored can be found in Github at <https://github.com/keholcom/vehicle-obd2>.

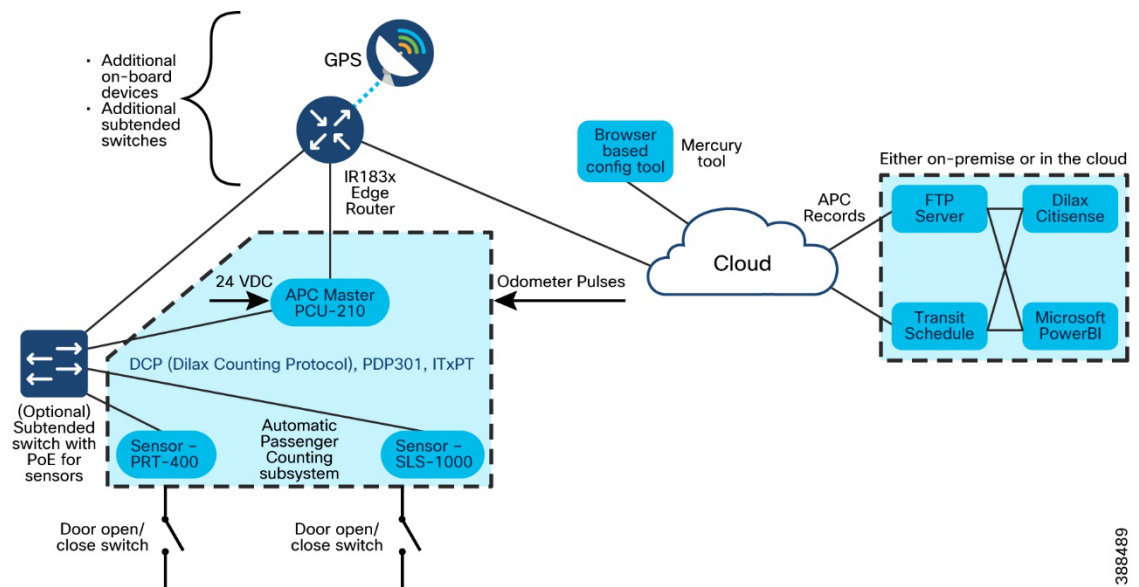
Automated Passenger Counting

Passenger counting is used to capture the key metric of ridership levels across various legs of transit routes. It is used to measure ridership levels, optimize route planning, and determine the number of transit vehicles required to support rider demand at different times of day.

Cisco is working with Dilax (www.dilax.com) to integrate their automatic passenger counting (APC) system as a key solution component.

Refer to the following diagram:

Figure 4 Dilax Automatic Passenger Counting (APC) Line-up



Operationally, the door open and close switch triggers sensors to begin counting entries and exits when the doors open and stop measuring for a final count when the doors close and the transit vehicle begins moving. The APC Master uses odometer pulses to determine when the vehicle moving (for example, leaving the station or stop) or it could use the GPS NMEA stream provided by the IR1800 industrial router to capture the same information. The APC Master pulls data from sensors at least once per stop and data stored for up to 1 month in a ring buffer.

Data is delivered to the cloud or TMC application by the APC Master in one of two ways:

- An autonomous push at a defined time of day to a configured FTP server address.
- After each stop a collection of data include the APC Master ID, passenger counts, location, and time) using JSON are delivered over HTTP/S to a configured IP address.

Citisense is the Dilax APC application used to process APC reports leveraging data from the FTP server or per-stop reports and transit agency schedules. It can be used to produce reports, graphs, and Fin-BI based analytics.

Fare Collection

Fare collection is a primary piece of the revenue stream supporting any transit operation and, therefore, carries careful consideration. Public transit vehicles will either have an onboard fare

collection system or validation device (on a bus) or require checking of proper fare payment by transit personnel (on trains).

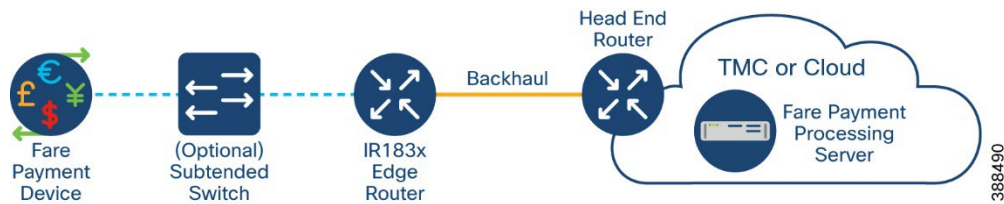
Modern options for fare payment include paper money or coins, prepaid ticket with magnetic stripe, prepaid fare for a day/week or month captured on a smartphone and scanned as riders enter the vehicle.

Given the sensitivity and privacy of financial transactions, fare collection data must be sent using a secure, encrypted link between the transit vehicle and the fare payment processing center.

The onboard fare payment validation device may use location information to correlate passenger counts with passenger payments to determine if fare evasion is taking place and at which locations.

The IR1800 industrial router provides the required secure backhaul over an IPsec tunnel as well as location information, if required, for the fare payment device. For remote updates and troubleshooting, the Secure Equipment Access service can be used to connect to the fare collection device.

Figure 5 Fare Payment System



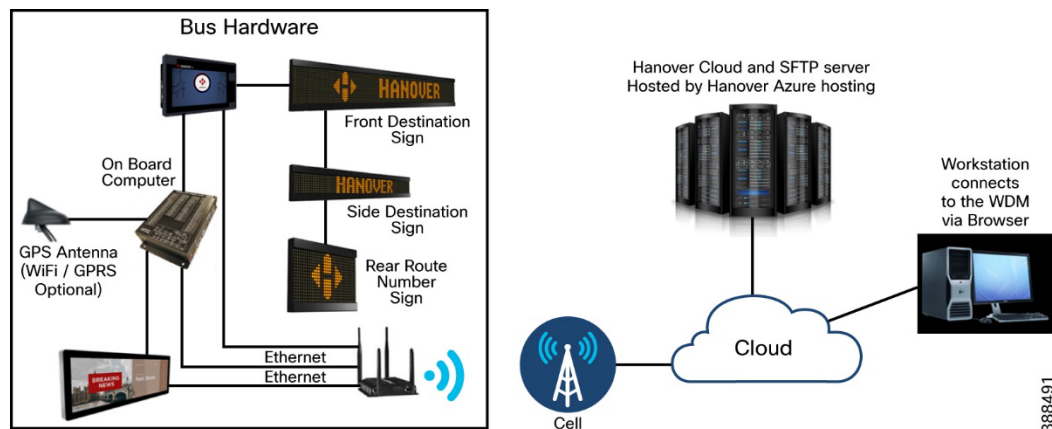
Passenger Information Signs

For Mass Transit agencies to increase ridership, one key aspect is to make the use of public transit as easy as possible. One way to do that is to provide easy access to accurate real-time route and estimated time-of-arrival (ETA) information to users.

The Cisco Converged Public Transportation system supports a passenger signage system on the transit vehicle and at the stops or stations.

On the vehicle, Cisco has partnered with Hanover Displays (<https://www.hanoverdisplays.com>) for an onboard signage solution. The Hanover solution includes the sign controller, front destination sign, side destination sign, rear route number sign and a TFT Display controller and TFT Display as well as the Hanover Central Software controlling sign messaging content and infotainment content. See the following illustration.

Figure 6. Hanover VMS System Line-up



The onboard vehicle infrastructure from Cisco provides the backhaul connectivity, location updates and maintenance/troubleshooting connectivity between the sign controller and the Hanover Cloud and SFTP server.

Note that configurations of transit vehicle message signs are downloaded onto the sign controller and are rarely changed except for when a route is modified.

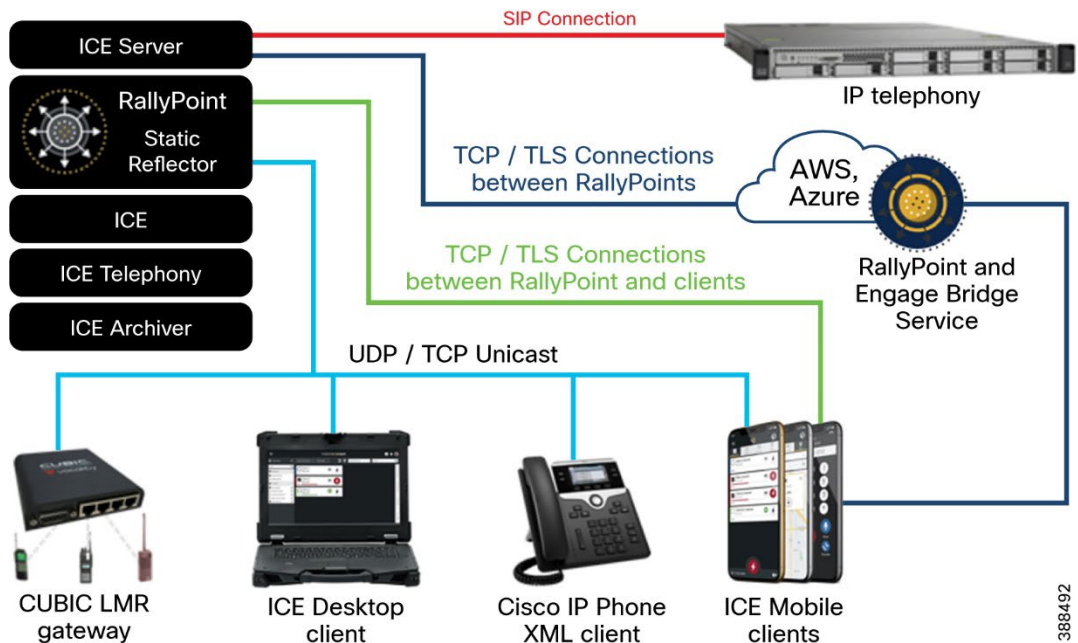
Vehicle Two-way Voice Communication

The converged network infrastructure integrated into the Converged Public Transportation system supports two-way Push-to-Talk (PTT) Voice over IP (VoIP) communications between the vehicle driver and the dispatchers in the operations center using the Instant Connect solution architecture (www.instantconnectnow.com/). This provides the flexibility to integrate VoIP-based next generation voice communications systems for new vehicle deployments with accommodation for existing vehicle retrofits through VoIP integration with existing digital radio systems. This capability allows for operators to gradually migrate away from proprietary voice communication systems.

The 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.

This CVD has fully validated the Instant Connect Enterprise server (ICE), RallyPoint, and ICE mobile clients. Client devices use a TLS connection to the ICE server for authentication and provisioning and a TLS connection to the RallyPoint for voice packet streaming. Actual voice packet payloads are delivered using the RTP protocol.

Figure 7. InstantConnect Voice Communication



The Converged Public Transportation system integrates end-to-end Quality of Service (QoS), providing proper real-time treatment for VoIP traffic throughout the network infrastructure. To avoid multicast challenges, voice packets are delivered using unicast IP but require priority over other non-real time traffic to ensure QoS, thereby avoiding disruptions. The driver PTT button on the mobile client is used to initiate a voice call with the ICE which then links in other participants, including the transit dispatcher using the RallyPoint functionality.

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 Cisco Converged Public Transportation system provides a comprehensive video surveillance system that ensures complete coverage of all assets and personnel onboard transit vehicles, at route stops, and in maintenance yards. The focus here is on the transit vehicle as video surveillance from fixed locations such as route stops, parking lots, and maintenance yards is well covered by other solutions outside of the scope of this design guide.

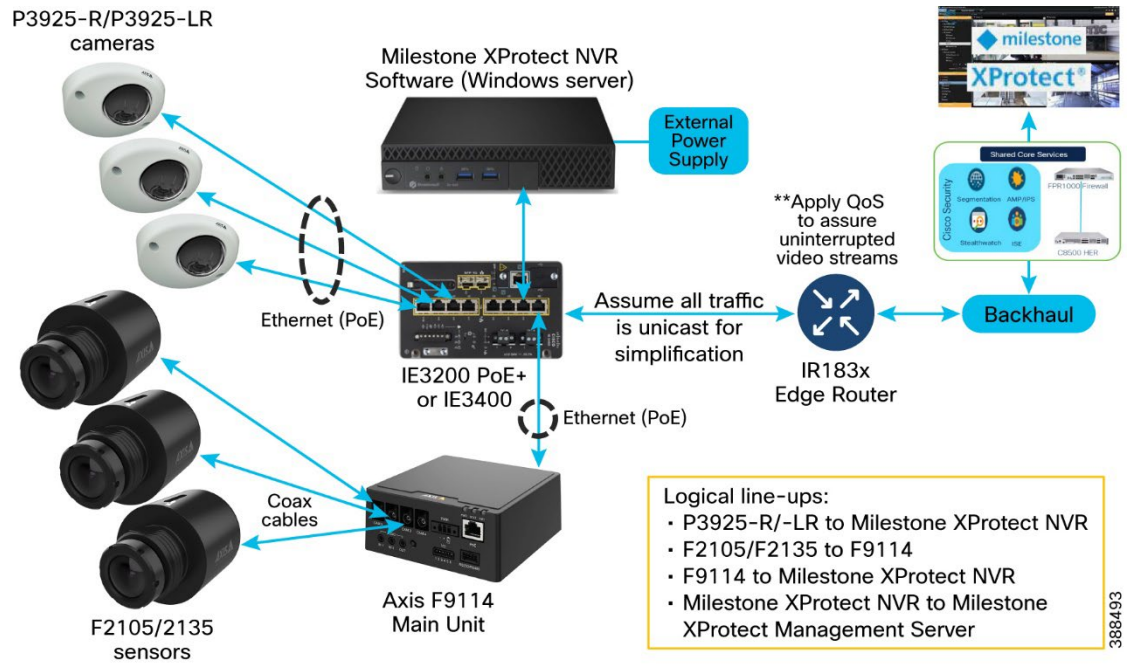
On the transit vehicle, the Converged Public Transportation system can scale video surveillance coverage to whatever number of cameras a mass transit operator requires. Typically, coverage of a vehicle like a bus will require somewhere between two to sixteen cameras although the solutions tested can scale much higher.

The system design supports two deployment options onboard the vehicle:

- A ruggedized server deployed on the vehicle with the cameras to provide storage for and real-time processing of camera video streams, as required. The server can be an off-the-shelf ruggedized Windows machine sized to the number of cameras and days of storage required. This allows for the use of different brands of servers without the worry of hardware incompatibilities.
 - The Axis Communications (www.axis.com) family of video cameras and camera sensors have been integrated and tested – models P3925 camera, P3935 camera, P2105 sensor, P2135 sensor (and F9114 Main Unit when using camera sensors).
 - The Milestone XProtect Professional+ software (<https://www.milestonesys.com/video-technology/platform/xprotect/>) running on the ruggedized server captures video from the P3925 or P3935 cameras as well as the F9114 main unit (acting as a camera back end for the P2105/P2135 sensors.) The XProtect Professional+ software exists both on the vehicle for local storage and in the Transit Management Center as a centralized video management solution for the entire transit vehicle fleet.
 - This configuration has been tested by Cisco in partnership with Axis Communications and Milestone.
- The cameras are deployed onboard without a server. Each camera has a microSD card slot which supports SD cards, enabling up to 2TB of onboard storage on each camera. In this configuration, the Milestone XProtect software directly pulls video from the cameras on the transit vehicle.
 - Cisco has not tested this configuration.

See the illustration that follows.

Figure 8. Video Surveillance Architecture



Event Triggered Video Surveillance

The Converged Public Transport system design supports marking of video footage by different events and triggers. The following events are supported in the system design:

- **Contact closure triggers.** These are connected to the IP Cameras. Any contact switch can be used as a trigger when connected to one of the cameras. Examples of contact closure triggers include:

- Door open and close

Upon arriving at a transit stop, the doors of the transit vehicle will open to allow passengers to both exit and enter the vehicle and then close as the vehicle departs. This time period is of most interest to transit companies due to the high content value of passenger movement.

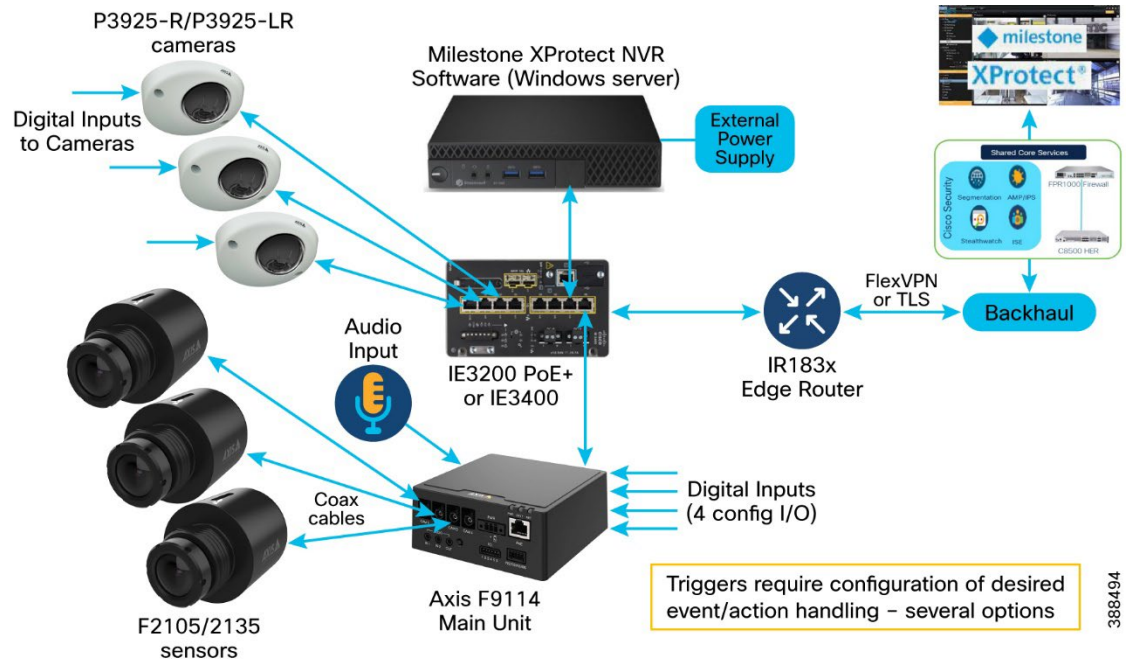
- Driver panic button

A driver panic button is typically a covert switch that can be pressed by the driver if they feel that a dangerous situation is occurring. This is intended to initiate live video streaming of the event to the video client application in the transit management center and to generate alerts to the security team.

- **Audio triggers.** The F9114 main unit from Axis, acting as a back end for onboard IP cameras incorporates a microphone for detection of audio events such as shouting, gun shots, or a crash. As with the driver panic button, these audio events are intended to initiate live video streaming of the event and sending alerts.

The illustration that follows captures these concepts.

Figure 9. Video Surveillance Action Triggering



Vehicle Panic Button

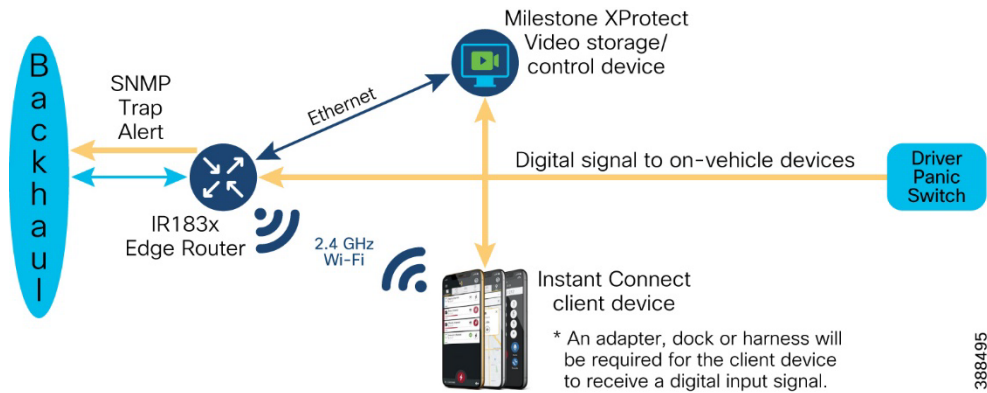
An essential idea for guaranteeing the safety of the mass transit driver and the passenger on the vehicle is for the driver to covertly alert the dispatch center if a critical situation develops. The driver panic button is an electronic device installed in the driver compartment within arm’s reach and is typically shielded from the passenger view.

In the Cisco Converged Public Transport system, the following actions will happen when the button is pushed:

- Two-way voice communications are established with an open microphone between the driver and the dispatch center using the Instant Connect product. Depending upon the situation, the Dispatch center may patch the audio from the vehicle directly to the relevant law enforcement agency.
- The onboard video surveillance system from Axis and Milestone will trigger live video streaming over the cellular connection for critical cameras. Some bandwidth compression and loss of resolution can be expected when using an LTE link or even a 5G link depending on the current coverage. The dispatch operator can select other cameras as needed through the Milestone XProtect video management solution.
- The IR1800 industrial router will send an SNMP trap/alert to the fleet management software in the TMC (requires accessible IP address) – SD-WAN only
- The router will create a syslog update
- The IR1800 industrial router will publish alerts to any IOx applications

Refer to the illustration that follows.

Figure 10. Driver Panic Button Connectivity



Some on-board cameras also come equipped with digital inputs that can be used for triggering video streaming, recording, and so on.

CAD/AVL

Computer aided dispatch/automatic vehicle location services are central to every transit vehicle. These services support the representation of transit vehicle routes and schedules to the driver, give feedback on vehicle location along the route, and report adherence to the planned schedule to dispatchers.

The CAD/AVL system is comprised of the Vehicle Logic Unit (VLU), the driver terminal, and the associated fleet management application(s) in the Transit Management Center or in the cloud.

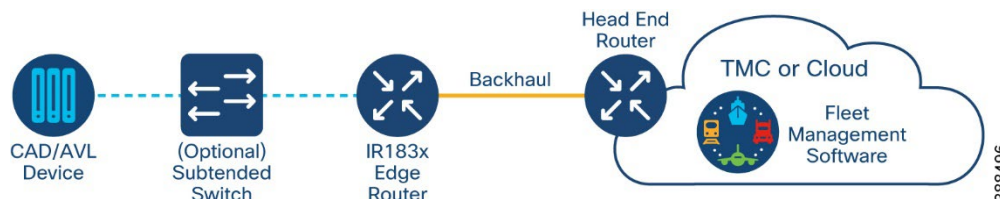
Fleet dispatchers in the transit management center continuously monitor their transit vehicles for adherence to schedule, looking for situations that require intervention or alternate planning, such as putting another transit vehicle on the route to handle capacity.

Fleet Management software, supplied by several industry software vendors provide dashboard, alerting, and initiation of voice communication with the transit vehicle driver or workers to coordinate any needed responses.

On the transit vehicle, the Vehicle Logic Unit (VLU) performs centralized dispatch coordination functions including receiving routes downloads, updates, alerts, and messages from dispatch. The VLU allows the driver to interact with dispatch using a driver interface terminal. The driver interface terminal may be a tablet or smartphone with a large screen and is mounted to allow single handed operation.

The IR1800 industrial router provides the required secure backhaul over an IPsec tunnel as well as location information for the VLU device. For remote updates and troubleshooting, the Secure Equipment Access service can be used to connect to the VLU device.

Figure 11. CAD/AVL System



Wireless Bulk Data Transfer

Wireless bulk data transfer refers to the use of high-capacity links to upload or download large amounts of data. Information downloaded would include software updates, configuration updates, router information, voice announcements, and infotainment data. Information uploaded includes any data being captured or logged by onboard systems for later use.

The connectivity for wireless bulk data transfer is established when the transit vehicles enter the depot and go out of service. This transfer is via a wireless connection from the transit 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 transit vehicle systems and the backend systems in the Operations Center:

- Vehicle-to-Infrastructure: Upload daily log files and video surveillance files from the vehicle previous shift.
- Infrastructure-to-Vehicle: Download updated route information, audio announcements, sign display messages, infotainment data and software updates for the onboard systems. Updates are expected infrequently as this information changes.

The table below details the types of data exchanged, the expected size, and the frequency with which the data is exchanged.

Table 2. Bus System Data Usage

Data Type	Estimated Size	Expected Frequency	Direction
Router Software	700 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 ¹	82GB for H.264 316GB for MJPEG ²	1/day	From bus
Vehicle Announcements (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

Most transit vehicle physical configurations and system configurations are the same, so identical configurations will be used for the vehicle onboard logic systems for ease of scaling the vehicle system deployment over hundreds or thousands of vehicles. The key exception is the unique vehicle identifier. Thus, the onboard network infrastructure will be required to provide Network Address Translation (NAT) functionality to enable routing for a specific vehicle within the maintenance yard.

Note that it is expected that the transit vehicle engine will be turned off once parked in the maintenance yard to save fuel. However, using ignition sensing and power management capabilities of the Catalyst IR1800 Industrial Router, the router can continue to operate for a configurable period with a wide range from 2 minutes to 9 days (not recommended) to complete the data transfers.

Almost all required file transfers, except for video, are easily accommodated within a 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 802.11ax 5GHz bridging link utilizing 2x2 MIMO can achieve theoretically 1.488 Gbps bidirectional with 80MHz channels under ideal conditions. Real world performance will likely be lower.
- At this throughput rate, a maximum of ~330GB of data can be transferred bidirectionally (sum of data in both directions) by one vehicle in 30 minutes.
- As more vehicles associate to an infrastructure access point, the bandwidth available is shared among the vehicle connections. Assuming a density of 10 buses per infrastructure AP and accounting for overhead results in approximately 16–25 GB (max) of data that can be transferred in 30 minutes.
- On-site testing of average wireless throughput should be conducted when determining video recording and archiving policies.

Video surveillance file sizes can be several orders of magnitude larger than any other file transfer class based upon resolution and number of cameras used. The result is that the amount of information that can be transferred from the bus to the backend systems in a 30-minute window is far exceeded by the amount of video data.

This design proposes to ensure that video data is backed up onboard for several days and to either find an extended period to upload the video data or assign a dedicated access point in the yard for uploading video with maximum bandwidth. The alternative is to upload only parts of the video tagged based upon door open/close, driver panic button or other triggered events.

If a dedicated access point is used for video transfer, 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 Mass Transit operator requires that all video must 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 ~330GB threshold.

Connected Passenger Stop

The Converged Public Transport system is designed to provide a comprehensive end-to-end infrastructure for all aspects of a mass transit agency operational scope. In addition to providing the infrastructure and services to the fleet of transit vehicles, the system includes connectivity and services for the passenger stops operated by the agency.

The infrastructure design for the passenger stop replicates a limited set of the same services that are provided onboard the transit vehicles including:

- Wi-Fi services for Passengers, Transit system employees, and Emergency Services
 - Passenger Wi-Fi is delivered directly to the Internet from the service provider or through the transit management center
 - Transit employee and emergency services Wi-Fi is routed over an IPsec tunnel to the transit management center.
 - As described in an earlier section, if the transit agency wishes to host a Wireless LAN controller (WLC) in the transit management center, the passengers exiting the transit vehicle can hand off their Wi-Fi connection to the AP at the passenger stop without the need to log in again.
- Video Surveillance to capture activities at and around the passenger stop for security purposes.
 - At the stops, the Cisco Converged Public Transport Architecture uses the Meraki family of cameras, specifically the MV72 or MV72X (<https://meraki.cisco.com/product/security-cameras/outdoor-security-cameras/mv72x/>) for surveillance.
- Information signage showing transit vehicle route and ETA information.
 - At the stops, the Cisco solution uses the Daktronics dynamic message signs (<https://www.daktronics.com/en-us/products>) and Vanguard Professional Software.

There are several architectural options for passenger stops based on the backhaul connectivity available and the presence of a city or roadway network. Information about the infrastructure design and service delivery to passenger stops is provided in the System Architecture section that follows in this document.

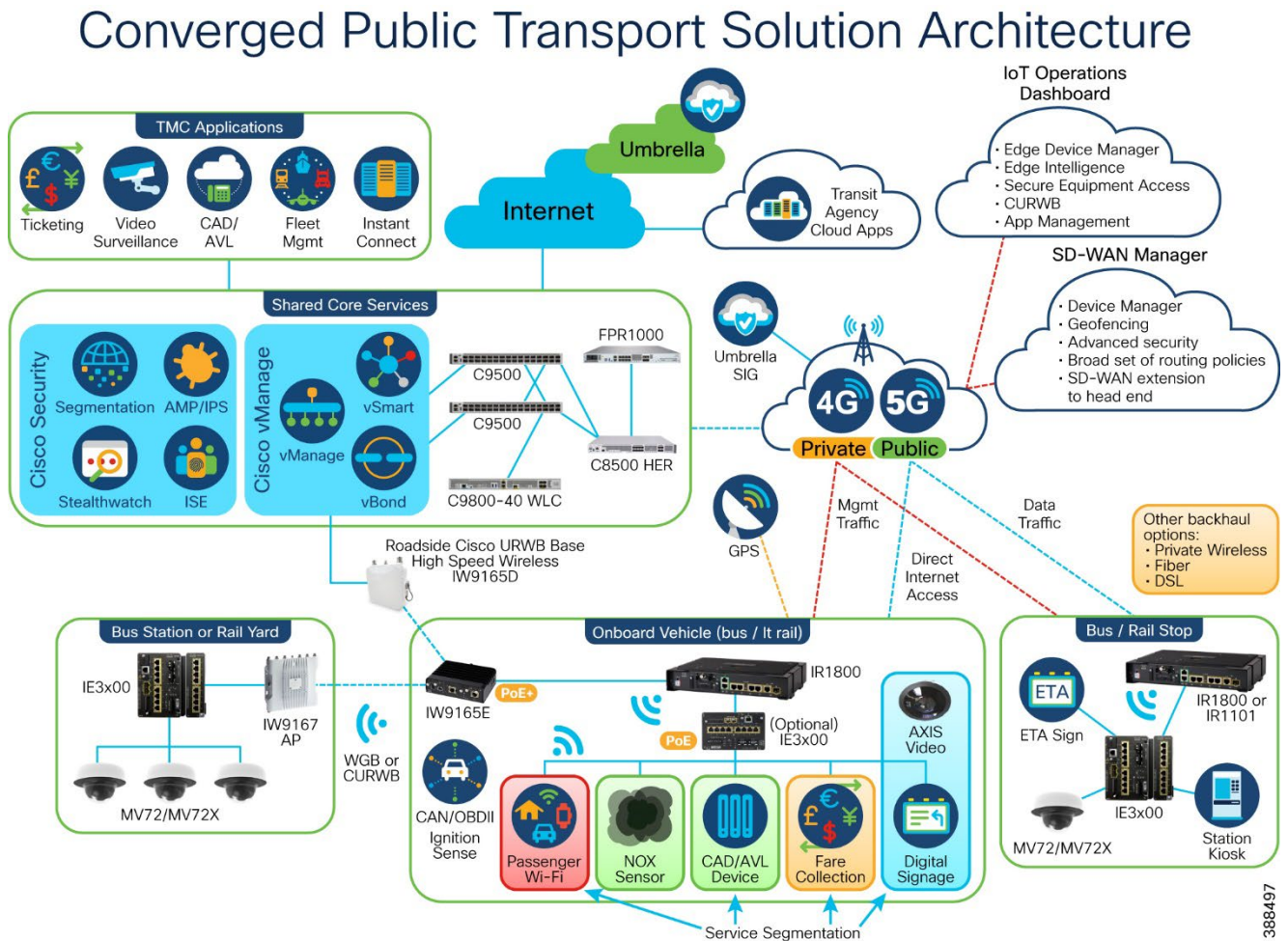
System Architecture

This release of the Converged Public Transport system proposes a scalable and resilient design for the following aspects of a mass transit operator infrastructure and services:

- Vehicle Onboard Network and Systems
- Off-boarding Wireless System
- Transit Stop Network design
- Yard Network and Transport Network designs
- Transit Management Center
- Hosted Systems and Services

The figure below illustrates the full scope of the transit system solution.

Figure 12. Converged Public Transport Solution Architecture



Note that the IE3x00 on the transit vehicle is optional and only required if the number of ethernet ports required to connect onboard systems is greater than four.

Each of these system layers is described in greater detail in this section.

Related Efforts

The Converged Public Transport system scope focuses on infrastructure and services specific to mass transit vehicle operations, safety and optimization, and passenger connectivity and services.

The Converged Public Transport design interfaces with key aspects from other Cisco Validated Designs for the following areas:

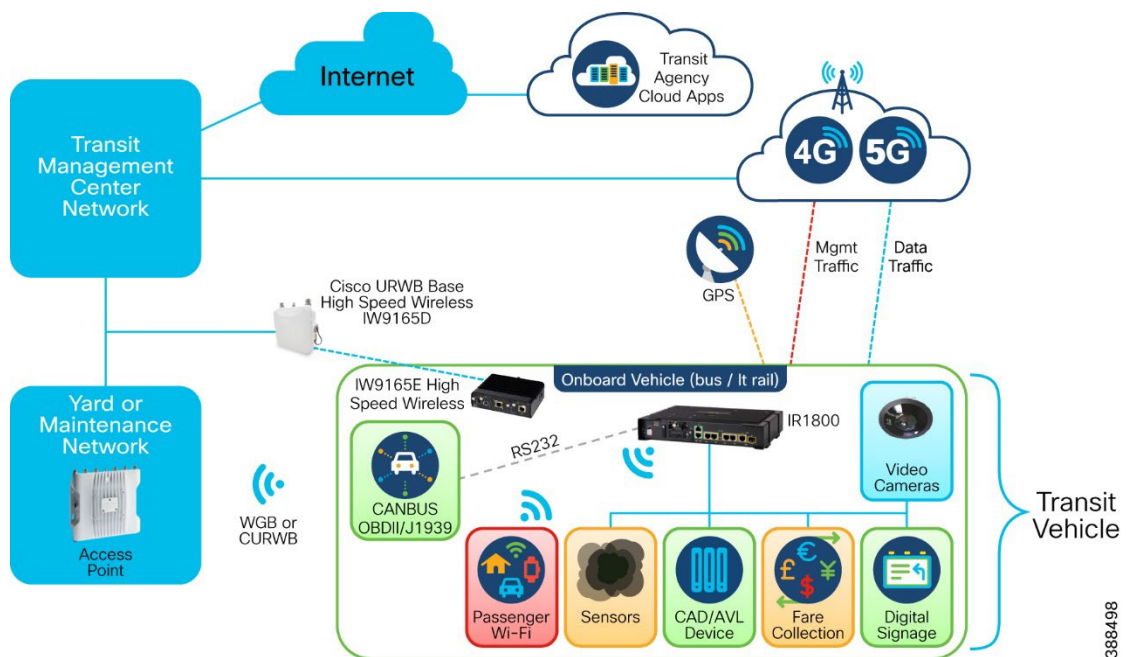
- **Cisco SD-WAN for Industrial use cases** - Provides design information on the application of SD-WAN technology and tools to industrial use cases such as fleets, utilities, and remote condition monitoring and control.
- **Cisco Connected Roadways system** - Provides design best practices for a scalable and resilient transport network for highways, roadways and intersections which provide the path of travel for bus-related mass transit vehicles.
- **Secure Equipment Access** - Provides design and implementation guidance for using Cisco Secure Equipment Access for tightly controlled remote access to industrial assets.
- **Enterprise Data Center** - Provides a scalable and highly resilient data center infrastructure necessary for hosting key service and management components.

Functional Description

Connected Transit Vehicle Onboard Network and Systems

The transit vehicle onboard network is shown in the illustration that follows.

Figure 13. Mass Transit Vehicle/Data Center Network




The transit vehicle onboard network design proposed in the Converged Public Transport system consists of the following components:

- **Cisco IR1831/33/35 Mobile Router**
 - Provides a unified IP routing function for all onboard systems, selecting the proper WAN interface for backhaul.

- Ensures traffic segmentation for different onboard systems/services.
 - Manages and terminates VPNs carrying transit traffic using IPsec tunnels.
 - Provides the linkage to OT tools like Secure Equipment Access to allow transit or external employees to remotely access onboard systems.
 - Provides wireless connectivity for passengers and enterprise systems.
 - Provides all offboarding WAN connections: LTE/5G, CURWB, Wi-Fi Workgroup Bridge (WGB), DSL, and fiber.
 - Provides GPS coordinates to onboard systems supporting the NMEA GPS data formatting and messaging.
 - Provides GPIOs to support discrete inputs such as driver panic button or door/open and close sensors.
 - Provides IOx docker run time environment for edge applications performing value added functions or edge integration.
 - Provides CANbus integration through a native CANbus port and IOx application.
 - Note: specific functionality may be limited to particular models of the IR1800 series routers. Refer to the datasheet for a breakdown of which features are supported in each.
- **Cisco IE3x00 or IE9300 Ethernet Switch**
 - Provides additional gigabit Ethernet and power-over-Ethernet capacity for onboard systems, bus stop, and yard.

Figure 14. IE Switches for Port Expansion

**IE3200
Fixed System**




1. IE3200 copper fixed
2. IE3200 PoE+ fixed

Note: No support for Expansion modules

**IE3300, IE3400
Expandable Systems**

2x1Gig SFP
and 8p Cu


2x10Gig SFP
and 8p Cu



1. IE3300 copper basic modular system
2. IE3300 PoE/4PPoE basic modular system
3. IE3400 advanced modular system
4. IE3400 Advanced PoE= modular system

IE switch selection depends upon:

- Port count
- PoE power needs
- Mounting requirements



Stackable rack-mount,
all fiber or all copper
Catalyst IE9300

388499

- **CAD/AVL Vehicle Logic Unit (VLU):** Provides Computer Aided Dispatch & Automated Vehicle Location (CAD/AVL) functions for the vehicle. May also provide the panic button interface for the driver.
- **Fare Collection:** Provides electronic fare collection and validation of prepaid cards, on-line accounts, and cash payments.

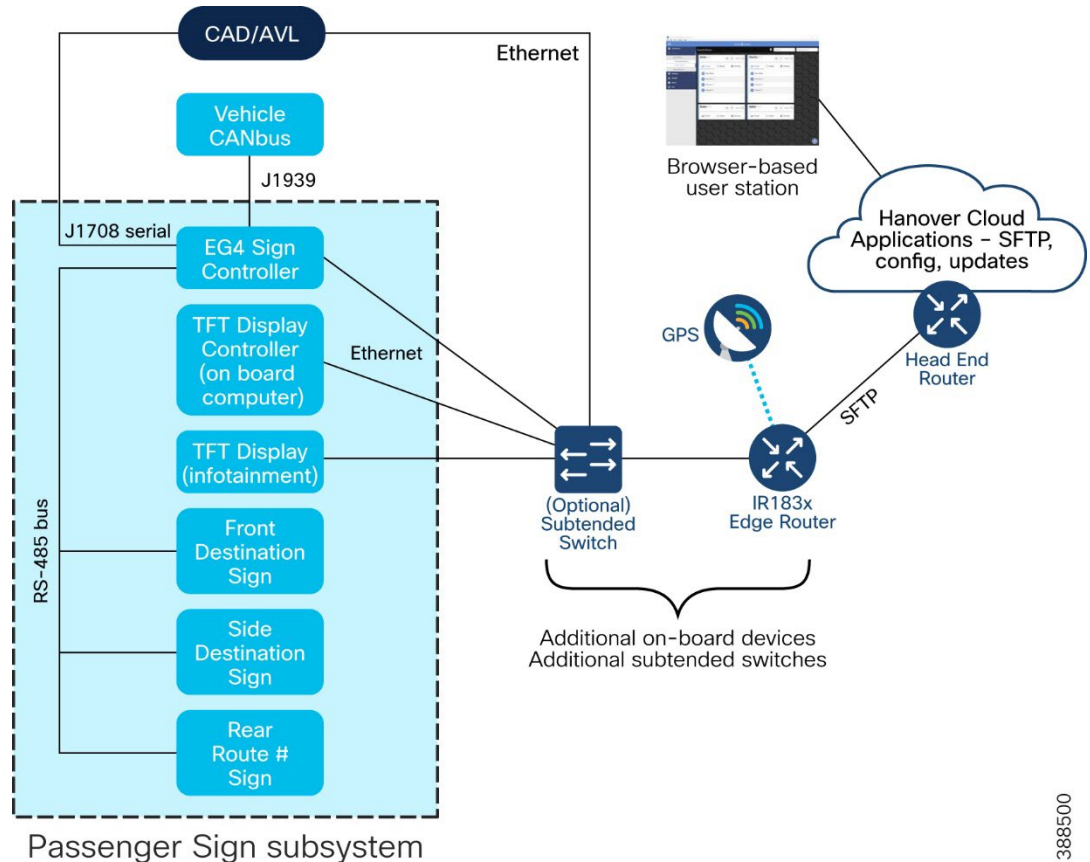
- **Video Surveillance System**
 - Surveillance cameras
 - Axis Communications model P3925-R/P3925-LR standalone dome cameras powered by POE from switch or
 - Axis Communications model F2105/F2135 camera sensors providing raw video signal with delivery via a coax cable back to the video camera back end.
 - Video camera back end: Axis Communications F9114 Main Unit which provides back-end video processing for the raw video received from the F2105/F2135 camera sensors. In essence, the combination of F2105/F2135 and F9114 are a full camera. The F9114 supports POE or a separate power feed.
 - Video recording and actioning software: Milestone XProtect NVR software which runs on a Windows server to act as a collection point for onboard video from all cameras resident on the transit vehicle. This serves as the interface back to the XProtect software in the transit management center performing overall video management services (VMS).
 - Ruggedized server: A computer platform to host the Milestone XProtect software for onboard video management storage and reporting.
- **Passenger Information System:** (see earlier illustrations)
 - Hanover EG4 sign controller:
 - Using RS-485 multi-drop interface to front, side, and rear signs on the transit vehicle, the EG4 responds to J1708 serial commands from the CAD/AVL system and updates the destination information on the front, side, and rear signs.
 - Using GPS information from either the IR1800 series router or from the CAD/AVL system, the EG4 uses location and geofencing algorithms to identify a stop and update the next stop information.
 - Additionally, as value added capability, the CANbus can be connected to the EG4 to monitor state of charge, stop requests, door open/close which is used in the logic to determine when a transit vehicle is entering or exiting a transit stop.
 - Front destination sign: Displays the next destination information for passengers facing the front of the transit vehicle.
 - Side destination sign: Displays the next destination information for passengers facing the side of the transit vehicle.
 - Rear route number sign: Displays the route number on the rear of vehicle.
 - Infotainment center:
 - TFT display controller: TFT display controller generally acts as a slave to the EG4 but launches next-up announcements through the Public Address (PA) system speaker and delivers video to the TFT display for Infotainment (VGA, DVI, HDMI).
 - TFT display: Displays route ETA information for passengers onboard the transit vehicle as well as infotainment.
 - Hanover Central Software (in transit management center): This software performs several functions including:
 - Browser-based administrative interface used to configure updated

destination lists for display.

- HELEN software used to delivery updated destination lists using the SFTP protocol.
- Creation and delivery of media content and next up announcements to the TFT Display Controller.

See the illustration that follows.

Figure 15. Physical Passenger Information Signs Line-up

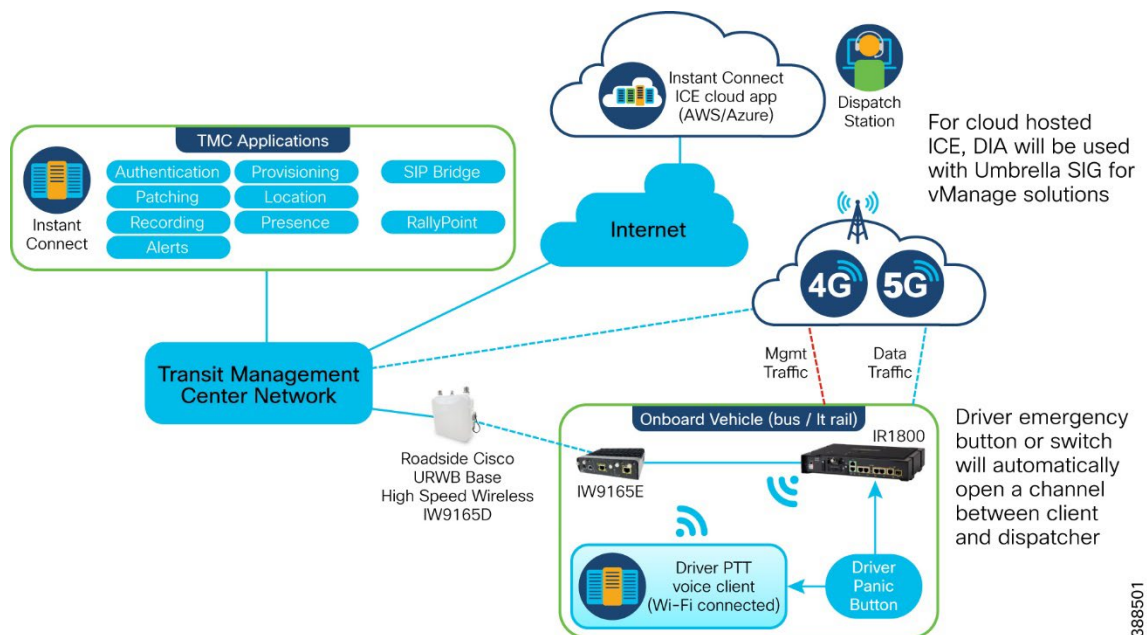


- **Passenger Counting:** Dilax provides the passenger counting system which is comprised of the following:
 - APC Master (PCU-210 model) which receives sensor input and provides the onboard passenger counting intelligence and communication to the Dilax Citisense application in the transit management center or in the cloud.
 - Sensors (PRT-400 or SLS-1000) are placed at each vehicle entry and exit door which provide counts of people entering and exiting the vehicle.
 - Additionally, the APC Master receives odometer pulses to know if the transit vehicle is in motion as well as a GPS NMEA stream from the IR1800.
 - Delivery of data from the APC Master to the cloud or on-premise application can be either:
 - An autonomous push at a configured time of day to an FTP server or
 - A push after each stop of APC Master ID, counts, location, and time using JSON over HTTP/S to a configured server ID.
 - See earlier illustration of this system.

- Two-Way Voice Communication:** Instant Connect provides two-way voice communications with Push-To-Talk (PTT) support between drivers, supervisors, and operations teams at dispatch and maintenance centers. It also enables interworking between voice over IP (VoIP) systems and legacy digital radio communications through Instant Connect integration. The following components are included in the Instant Connect solution:
 - Driver PTT voice client: also known as the ICE (Instant Connect Enterprise) mobile client which runs on a smartphone or tablet and connects to the IR1800 over Wi-Fi to deliver VoIP control and voice payload packets to the Instant Connect Enterprise (ICE) server in either the transit management center or the cloud.
 - Additionally, the client may receive a driver panic button input to automatically trigger the set up of a voice call so that dispatch can listen to events taking place on the transit vehicle.

See the illustration that follows.

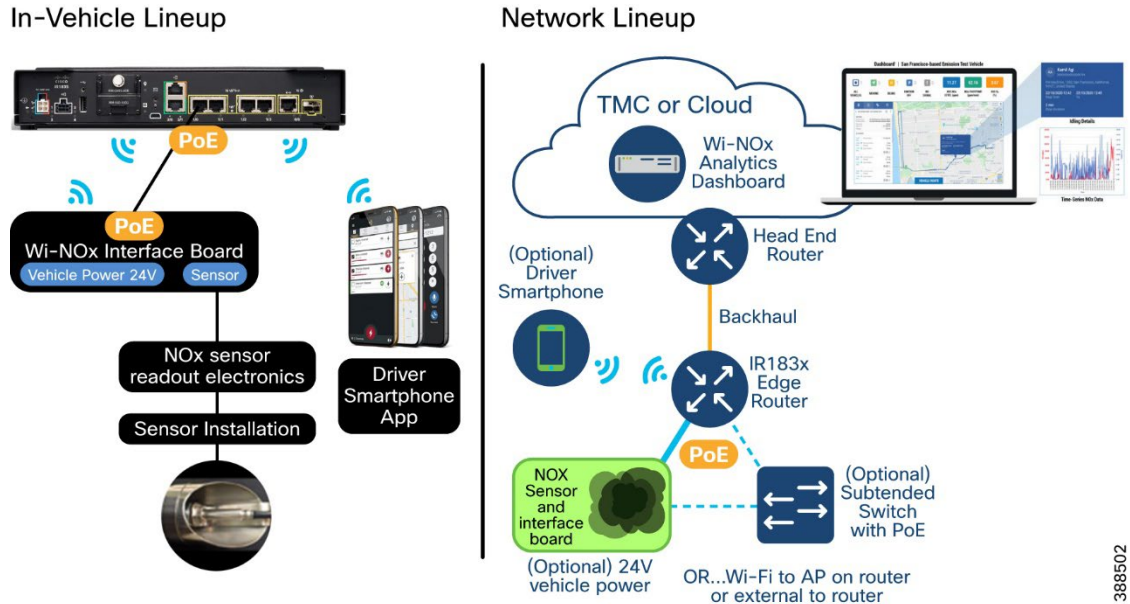
Figure 16. PTT Architecture – InstantConnect Focus



- NOX emissions measurement sensor and logic:** Sensorcomm Technologies (<https://www.sensorcommtech.com/>) Wi-NOx™ provides an onboard solution extracting, analyzing and transforming the data signature from vehicle emissions into real-time business intelligence. Wi-NOx can be used by transit authorities for emissions reduction, fuel savings, and predictive maintenance for extended asset life. The WI-NOx system is comprised of the following elements:
 - Wi-NOx sensor:** physical sensor installed in the tailpipe to capture transit vehicle emissions.
 - NOx sensor readout electronics:** circuits to transform sensor raw data into usable samples for analysis.
 - Wi-NOx interface board:** local processing of emissions samples and transformation for delivery to the Wi-NOx analytics dashboard over an Ethernet (or Serial) interface to the router or via a subtended switch. Powered by either POE from the router or switch or directly from the vehicle 24 VDC supply.
 - Driver Smartphone application:** (optional) iPhone or Android smartphone application to alert the transit vehicle driver of status and ways to improve emissions as well as fuel consumption.

See the illustration that follows.

Figure 17. NOx and Emission Monitoring – SensorComm WiNOX Line-up



IR1800 Router

The IR1800 router provides wireless connectivity for passenger devices, transit worker devices and law enforcement devices onboard or within range of the vehicle, using the 2.4GHz radio of the integrated wireless access point. Alternatively, an external access point may be used for more flexible mounting and antenna placement. The access point implements multiple SSIDs mapped to separate VLANs that are trunked to the router functions of the IR1800, providing traffic separation and security required for each user type.

The 5GHz radio of the integrated wireless access point in the IR1800 (or external AP) is dedicated as a Workgroup Bridge (WGB) to provide high-bandwidth WAN connectivity for the transit vehicle systems when the transit vehicle is parked in a maintenance yard. A separate VLAN is also used here for traffic separation.

Cisco Ultra Reliable Wireless Broadband (CURWB) may be used for WAN connectivity.

The routing function of the IR1800 is the common service point for devices connected over the Ethernet ports (directly to the router or via a subtended layer 2 switch), 2.4GHz Wi-Fi connection or the 5GHz WGB connection and the LTE, 5G, CURWB or WGB backhaul connectivity options, allowing connectivity to transit applications and services in the transit management center or the cloud.

The onboard GPS receiver on the IR1800 is contained in either the cellular modem or a separate GNSS module (IRM-GNSS-ADR) (IR1833/IR1835 only) supporting high resolution GPS reception. In either case, GPS coordinates are periodically delivered to the management tool in use (SD-WAN Manager or IoT Operations Dashboard) for tracking of the transit vehicle location. Currently, in both SD-WAN Manager and IOT Operations Dashboard, location is only retrieved from 4G LTE modems on the Industrial Routers – support for 5G and GNSS module sources will be included at a future date.

Several transit applications may want to receive transit vehicle location information so the IR1800 supports delivery of NMEA GPS data over UDP to remote servers that host an application requiring GPS data.

For the router to act as the NTP source on the transit vehicle, the GPS time acts as a stratum 0

source, and the Cisco IOS NTP server acts as a stratum 1 device, which in turn provides clock information to its NTP clients (stratum 2 and 3).

The IR1800 built-in CANbus interface supports interconnection with either J1939 or OBD-II supported transit vehicles. The basic protocol data is delivered to the IOx application CAN socket and can be processed to deliver needed vehicle telemetry data to a fleet management application. See Github location <https://github.com/keholcom/vehicle-obd2> for a source code example that can be customized for a specific deployment.

Edge compute is supported on the IR1800 to address use cases leveraging multiple data sources on the transit vehicle (such as GPS, RSSI, CANbus data, and so on). Leveraging the IOx run time environment on the router, a docker application can be installed and executed. An IOx application can access the various data sources on the router, either as serial interfaces, or as IP streams and subsequently perform filtering, reformatting, and forwarding of the data to external applications.

General purpose I/O (also called Digital I/O) may be brought into the router and used to trigger the sending of SNMP traps (SD-WAN only) and events entered in syslogs which can be acted upon. Common digital I/O examples include monitoring of a driver panic button and door open/close events. Configuration of GPIO relies on adding CLI to the template in IOTOD or SD-WAN Manager.

Addressing

While the option exists for full layer 3 addressing with unique IP addresses for each device across the transit fleet, the more commonly used approach is to use a network address translation (NAT) to allow all transit vehicles to utilize the same LAN addressing map. This facilitates deployment by allowing installers the repeated operations to set up the same vehicle network across the fleet. To present a unique IP addressing toward the transit management center back end and beyond, the IR1800 must implement NAT to translate the private IP address space for onboard subnets via a unique IP address or a public IP address. The IR1800 acts as the DHCP server to support Plug-n-Play provisioning in the transit vehicles.

In some circumstances, it can be useful to use a physical Ethernet interface configured as a switchport (access or trunk) and associate it with one or more VLANs. The VLAN(s) can then be tied to a layer three SVI interface which can act as a WAN transport. This can be helpful when connected to an upstream switch or a modem (like the Cisco IW9167 CURWB radio) that supports an 802.1q trunk.


Cisco IE Switches

An IE switch will need to be deployed in scenarios where the number of connected device/subsystems exceeds the number of LAN ports on the router. Multiple switches can be deployed, each acting as a layer 2 port expansion to allow the connection of more devices and each subtended switch will consume one Gigabit Ethernet router LAN switch port.

This architecture uses an IE3100, IE3200, IE3300, IE3400 or IE9300 model switch with the selection being dependent upon the number of ports required, PoE/PoE+ power ratings, and mounting requirements.

See the figure that follows for key elements of each IE switch.

Figure 18. IE Switches Feature Overview



	IE3100	IE3200	IE3300	IE3300-10G	IE3400	IE9300
Category	DIN Rail	DIN Rail	Modular DIN Rail	Modular DIN Rail	Modular DIN Rail	Stackable Rackmount
Downlink Speeds	GE	GE	GE	GE	GE	GE /2.5GE
Uplink Speeds	GE	GE	GE	10GE	GE	10GE
PoE		PoE / PoE+	PoE / PoE+	PoE+/4PPoE	PoE / PoE+	PoE+/4PPoE
NetFlow			✓	✓	✓	✓
Layer 3			✓	✓	✓	✓
Cyber Vision			✓	✓	✓	✓
Edge Compute			✓	✓	✓	✓

388503

See the data sheets for these switches at <https://www.cisco.com/site/us/en/products/networking/industrial-switches/index.html> to learn more about maximum power budgets for PoE/PoE+ for each switch to select the most appropriate switch.

With several systems on the transit vehicle being connected to the IE switch, then the uplink port to the IR1800 needs to be configured as an 802.1Q trunk port.

Passenger Information Signs

For onboard signs, the IR1800 router provides the WAN backhaul as well as NMEA coordinates using the UDP NMEA transport described earlier. The sign controller uses SFTP for communication with the application software used for configuration and route updates. Other inputs to the sign controller include J1708 CAD/AVL interface and a J1939 CANbus interface, both running separately from the router. For the current generation of signs, the controller communicates over a dedicated RS-485 multi-drop serial interface. The router will be configured to place the sign controller on a dedicated VLAN.

Automatic Passenger Counting (APC)

The PCU-210 APC Master from Dilax provides the heart of the passenger counting system on the transit vehicle. It receives digital I/O inputs indicating when the doors open and close, counting information from sensors at each entry/exit, and odometer pulses to indicate if the transit vehicle is in motion. The IR1800 provides backhaul connectivity for reporting of APC records. The router will be configured to place the PCU-210 APC Master on a dedicated VLAN.

Fare Collection

The fare payment system on the vehicle is a standalone system utilizing the IR1800 series router for backhaul connectivity to payment and validation systems at the transit management center or in the cloud. The router will be configured to place the fare payment device on a dedicated VLAN.

Two-way Voice Communication

The only equipment onboard the transit vehicle is the driver voice client application running on a smartphone or table. The IR1800 provides Wi-Fi or Ethernet connectivity to the IR1800 for delivery and reception of SIP and RTP (VoIP) packets to/from the Instant Connect Enterprise software that patches the driver with dispatch or any other destinations. Driver voice communication is delivered with priority over passenger Wi-Fi services to ensure a QoS supporting the required voice fidelity. Should a driver panic button be used, it will be connected

to the driver smartphone or tablet and automatically initiate a voice call to dispatch. The router will be configured to place the Instant Connect voice client application on a dedicated VLAN.

Video Surveillance

The Axis IP cameras and, if used, the F9114 Main Unit are connected to the IE switch as well as the Milestone XProtect NVR server. These devices will be placed into a single VLAN for traffic separation.

Delivery of stored video from the NVR is typically done when the Milestone XProtect VMS in the transit management center is reachable by the IR1800. This will occur when the transit vehicle shifts its WAN connectivity away from cellular and onto WGB or Cisco URWB as the transit vehicle enters the maintenance yard.

Real time streaming of RTSP video streams is triggered by the driver panic button or any other desired digital input to the Axis P3925 series cameras or the Axis F9114 Main Unit. QoS is applied here to ensure uninterrupted video delivery. Notably, to fit live video streams into the available cellular bandwidth, camera resolution may need to be diminished.

CAD/AVL VLU

The CAD/AVL VLU is connected to a LAN switchport on the IR1800 router or IE switch for network connectivity. The router will be configured to place the CAD/AVL VLU on a dedicated VLAN.

Panic Button

The 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 digital signal (via contact closure) from the button depression can be routed to the IR1800, Instant Connect voice device, and the video surveillance system via a basic wired interface. The IR1800 will use SNMP traps (SD-WAN only) or syslog entries to capture and report back to the transit management center while the video system is configured to stream video and the Instant Connect voice application will establish an audio call with dispatch or emergency services.

Power Management

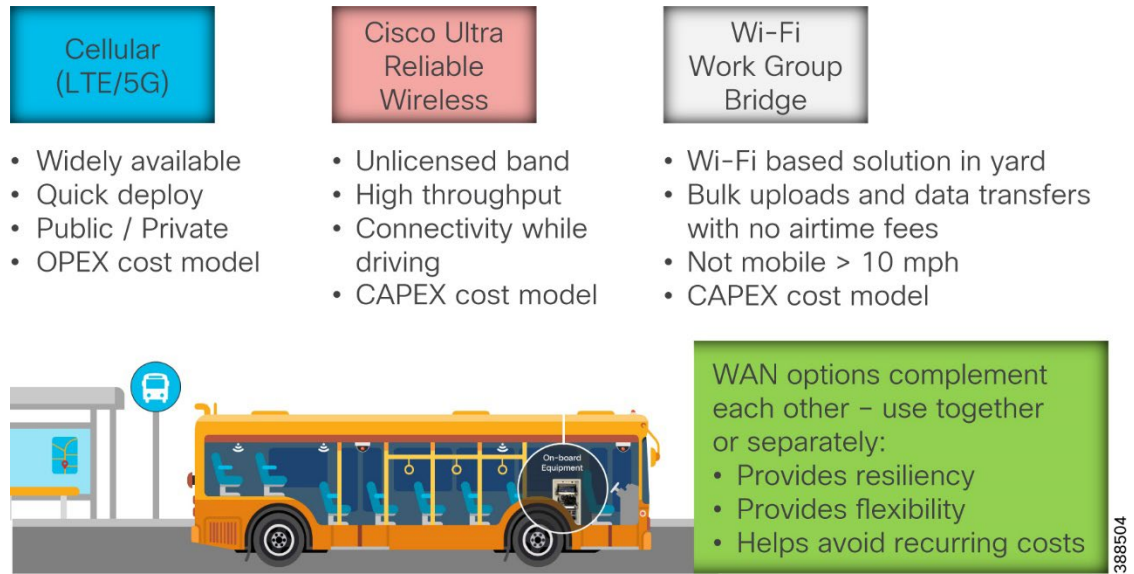
All components are connected to the transit vehicle DC power system, and thus power up simultaneously when the vehicle is started. The system design assumes that power to the onboard networking infrastructure is maintained when the vehicle engine is turned off to maintain connectivity for a period of time when the vehicle is parked in order to perform maintenance functions such as video uploads, software updates, and configuration updates. Power for the onboard networking infrastructure should be connected to a separate manual or automatic power isolation switch to permit this.

Backhaul-WAN Interfaces for Transit Vehicles

The Converged Public Transport system relies largely on LTE/5G services provided by a Mobile Service Provider (MSP) to enable network connectivity between the transit vehicles, Internet, and backend systems while the transit vehicle is in motion. However, the option exists to deploy Cisco Ultra Reliable Wideband technology (CURWB – private, unlicensed wireless) as a replacement or accompaniment to cellular connectivity to avoid recurring airtime tariffs or to fill in cellular coverage gaps. Lastly, when the transit vehicle enters the depot or maintenance yard, it will move the WAN interface to Work Group Bridge (WGB) Wi-Fi interface where the Wi-Fi AP on the transit vehicle becomes a client to the APs in the yard network. Again, this avoids cellular tariffs and supports a wider bandwidth solution for bulk uploads mentioned earlier.

Refer to the illustration that follows for characteristics of each WAN option.

Figure 19. WAN Connectivity – Resiliency & Flexibility



For edge routers operating in controller mode, managed by SD-WAN Manager, cellular roaming behavior is as follows:

- One cellular modem is active while the other cellular modem is inactive
- Active here means:
 - Connected to the cellular carrier
 - Control plane connections are established (OMP, BFD, DTLS)
- Standby here means:
 - Connected to the cellular carrier
 - Control plane connections are not established
- Operationally
 - When cellular 1 coverage fails or falls below a serviceable level (“link failure”), cellular 2 becomes the primary interface and control plane connections are established on the link.
 - Cellular 1 becomes the standby interface

In an Active-Active Configuration – both Cellular 1 and 2 are active WAN paths.

- Both cellular 1 and cellular 2 links establish control plane connections
- Traffic can be managed simply across the two cellular links by configuring a higher preference or weight to the desired primary WAN transport to pass most of the traffic through it as a preferred interface.
- Other options are:
 - Application aware routing can be used as a form of load balancing such that specific application traffic (or destination addresses) can use a designated cellular link unless that link fails.
 - This can also be based upon traffic type/class so that high priority traffic is sent over FirstNet (US only) and lower priority traffic is sent over a cellular commercial carrier

such as Verizon or T-Mobile.

- Per-packet or per-flow load balancing. For this design guide, we will ignore this load balancing method.

For edge routers on a standalone network using IoT Operations Dashboard, cellular roaming behavior operates as follows:

- The Active-Hot standby configuration is the only supported configuration – both Cellular 1 and 2 are active WAN paths
 - Both modems are configured and connected to the cellular service provider.
 - Only the currently active link is used to deliver data (both control and device data) at any time.
 - Cellular 2 is configurable as an active backup to Cellular 1 and is established control and data connections only when Cellular 1 link fails.
 - Operationally, these rules apply:
 - Control-plane connections will be established to IoT OD only on the active modem link.
 - Connected device traffic will only be carried on the active modem link.
 - Load balancing across links is not supported as data is delivered over only 1 link.
 - Data traffic is carried only on the active link.
 - SLA protocols will be used on both links to monitor link availability.

The cellular WAN links can support either a public APN or a private APN.

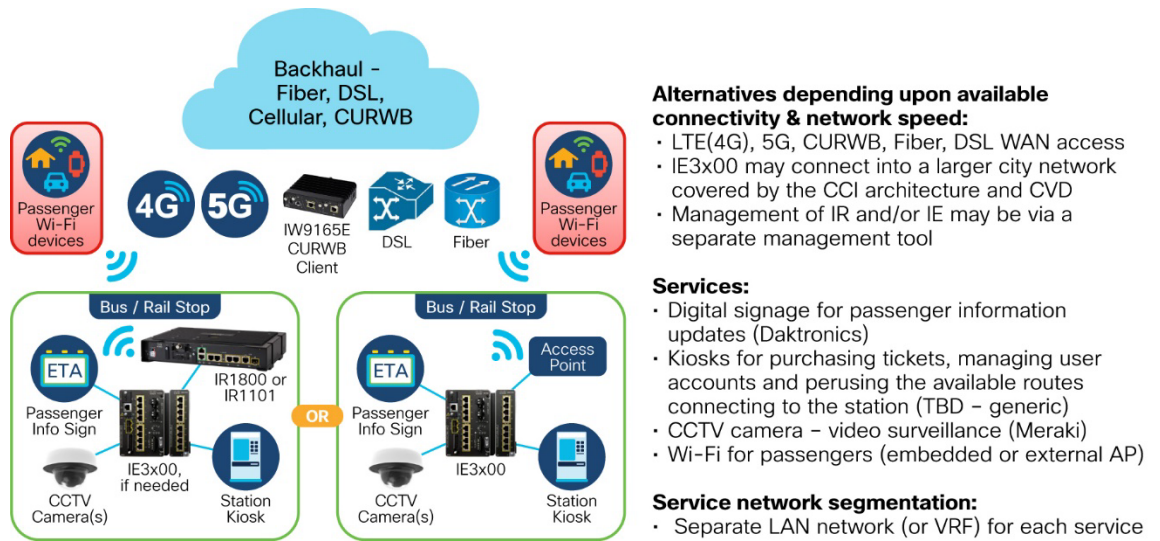
- In the case of a public APN, this assumes connectivity back to the transit management center is via an IPCP IPv4 or IPv6 address from the MSP and carrier NAT is deployed.
- In the case of a private APN, this assumes the use of an RFC1918 IPv4 address via IPCP from the MSP (optionally with static addressing) and that the handoff from MNO to transit management center is a leased-line circuit, VPN, or similar technology, so traffic never transfers over the Internet in the clear.

Connected Transit Stop

The network design for a Connected Transit Stop has several options depending upon available network backhaul connectivity. See the illustration that follows.

- For LTE/5G, or DSL backhaul, the IR1800 or the IR1101 industrial routers may be deployed to provide LAN connectivity for transit stop devices and backhaul connectivity through a carrier network.
 - Where Wi-Fi services are deployed, the IR1800 router is required.
 - If Wi-Fi is not required, the IR1101 router is sufficient.
- Where access to a smart city network or local roadways and intersections network is available, fiber connectivity to that network can be done using the IE3x00 switch with fiber SFP, and no router required.
 - For fiber networks not directly within reach, the use of Cisco URWB as a point-to-point link to bridge to a fiber access location is also an option.
 - Wi-Fi services in this configuration require a standalone AP.
- Lastly, Cisco URWB as a connection into a private wireless WAN is possible.

Figure 20. Mass Transit Stop/Station Architecture



For stop/station deployments, the Meraki MV72/MV72VX series cameras will be used. IoT OD supports integration with Meraki dashboard for these cameras. Similar to on-vehicle scenario, camera video will be captured, locally stored and uploaded to the Meraki dashboard. Signage here will be passenger ETA display from Daktronics using NTCIP 1203. Vanguard Field Controller

388505

The full list of possible components consists of:

- Cisco IR1800 Industrial Router
 - Provides IP routing and gateway for all systems at the transit stop. Provides wireless connectivity for passengers via an IR1101 with external AP provides wireless connectivity to passenger devices at the transit stop. As with the transit vehicle, the access point implements multiple SSIDs, providing secured connectivity to transit operator devices and potentially law enforcement devices as well. Each SSID is mapped to a separate VLAN on the router to facilitate service separation and security.

The Digital Signage system and video surveillance camera(s) are each connected to a LAN switchport on the IR1800 or IR1101 router for network connectivity. Each port is mapped to a VLAN interface for L3 functionality and for service separation from other services.

If connectivity to a fiber city/roadways network is present at the transit stop, then it is connected to the IE3x00 WAN port. If Cisco URWB is to be deployed for a point-to-point bridge to the fiber network, then it is connected to the IE3x00 WAN port. If connectivity to a DSL network is available, a DSL module is required in the router to act as the WAN port. Otherwise, the LTE cellular connection is used for data backhaul.

Additional WAN backhaul interfaces for stops or stations

At stops and stations, a larger number of backhaul options may exist including LTE/5G, CURWB wireless interfaces previously described. However, if the stop/station can connect into a larger city or roadways network, the fiber interfaces are viable options.

Yard Network

The maintenance yard network provides a scalable Wi-Fi infrastructure to deliver secure, high-bandwidth wireless connectivity to the transit vehicles parked in the yard into the transit management center network which hosts the service specific transit applications, or through the

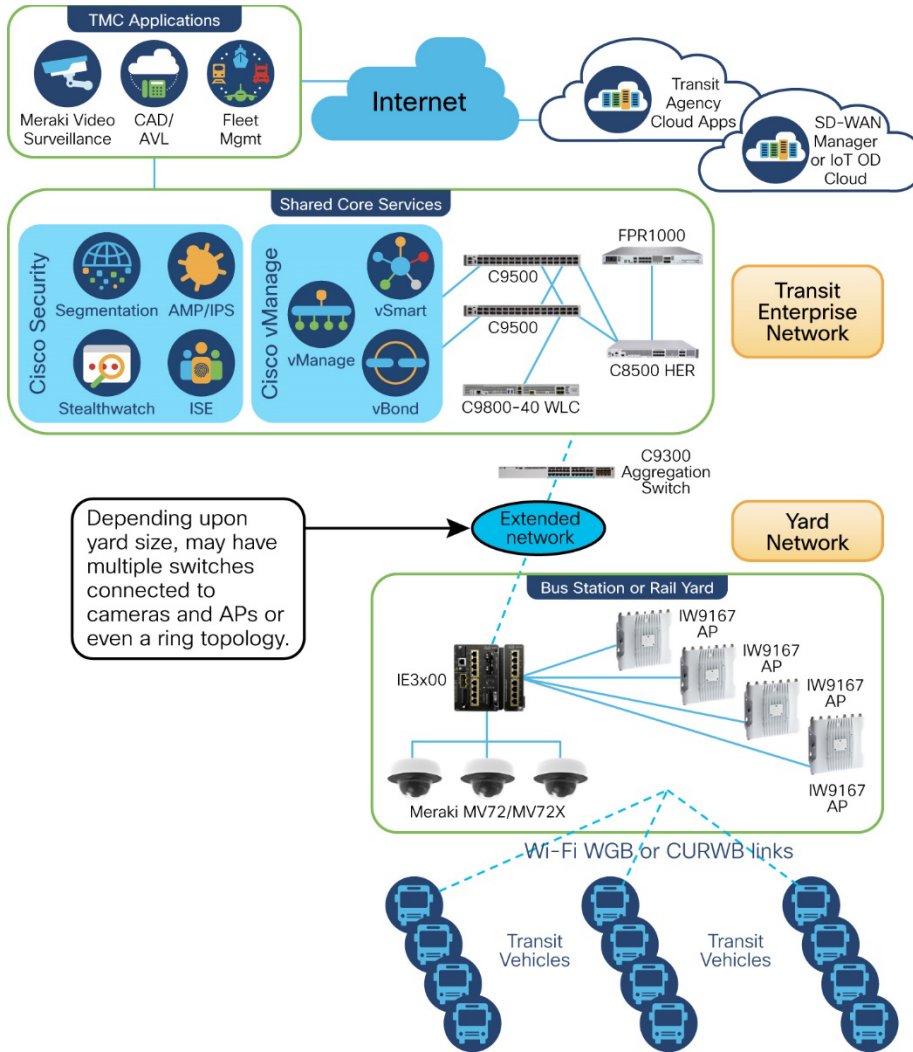
transit management center to cloud-hosted applications.

The yard network consists of the following components:

- **Cisco IW9167 Wireless Access Point:** An IP67-rated outdoor access point that provides IEEE 802.11ax Wi-Fi 6 coverage for the yard. Or, if configured as a Cisco URWB base station, provides CURWB connectivity to the yard.
- **Cisco Catalyst IE3400 Ethernet Switch:** Provides gigabit Ethernet connectivity to PoE Axis surveillance cameras in the yard as well as connectivity to the IW9167 APs. Multiple switches and configurations may be required depending upon the physical size of the yard.
- **Cisco Catalyst C9300 Stackable Ethernet Switch:** Where needed for bandwidth aggregation, provides 10-gigabit Ethernet connectivity to aggregate traffic from multiple IE3400s across the yard prior to connection to the transit management center head end router and firewall. Provides redundancy when leveraging the stackable capability.
- **Cisco C9800-40 Wireless LAN Controller:** A high-density controller for Configuring and managing the IW9167 Access Points when in Wi-Fi mode of operation. Located in the data center with the other backend systems.
- **Cisco Meraki MV72 or MV72X video surveillance cameras:** Provide high resolution CCTV video streams used to monitor yard security.

Refer to the figure that follows for an illustration of the maintenance yard line up and connection into the overall transit network.

Figure 21. Mass Transit Yard Architecture



Transit vehicle to Yard network:

- WGB (Wi-Fi) (IoT OD only), CURWB WAN access through IW9167 as Wi-Fi AP or as CURWB base station

Services:

- Bulk data offload from video system and logs
- Software/configuration updates/maintenance

Yard Network:

- Set of access points to cover the yard area OR
- Set of CURWB base stations to cover the yard area
- Access points, stations connect to the enterprise network via an industrial switch
- Aggregation switch bringing together all of the yard switching fabric into the share core/TMC
- WLC managing the access points is in the enterprise network
- Meraki MV72 video cameras connected over yard switching network for video surveillance with 802.1x authentication

Transit Enterprise network:

- As described earlier, it hosts the HER, FW, security and vManage on-prem services when used as well as the switching fabric required (beyond scope of this CVD)
- Switches and FW will be under separate management, but may share management of HER + IRs if using vManage

The IW9167 devices in the yard can be configured to operate as 802.11ax Wi-Fi6 Access Points for WGB connected transit vehicles or as Cisco URWB base stations for CURWB-connected transit vehicles. The transit agency may choose either approach based upon several factors not discussed here. Please refer to the IW9167 data sheet for more details -

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-iw9167-series/cat-iw9167e-heavy-duty-ap-ds.html>.

The IW9167 may be deployed with a variety of omnidirectional 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 access point deployment. In general, IW9167 devices are deployed on the sides or roof of the building in the yard in which resides the Ethernet switch for ease of wiring.

If the area of the yard requiring wireless coverage exceeds the effective range of these access points, additional access points 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 access points are wired to the Ethernet switch. Otherwise, wireless bridging to the access points on the side of the building is employed for traffic backhaul, and only power must be provided to the wirelessly connected access points.

The access points are connected to a Catalyst IE3400 Ethernet switches, as are any other local

servers and branch systems located at the yard. The Catalyst IE3400 switch line provides a range of configurations and port densities to accommodate any size yard deployment. Also, with Power-over-Ethernet supplied to all ports on the switch, separate power connections are not required for each IW9167 device. Each wired access point is connected to a gigabit Ethernet port.

The Catalyst IE3400 Ethernet switches are aggregated, if required to limit connections to the data center or to manage high aggregate traffic bandwidth, using the Catalyst C9300 Stackable Ethernet Switch as an aggregation switch layer into the data center.

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

The Yard Access Point infrastructure is centrally managed by a Cisco Wireless LAN Controller (WLC). The WLC is configured to deploy and manage the access points in FlexConnect mode, transporting only control traffic via Control and Provisioning of Wireless Access Points (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.

Deployment of IP Cameras is needed to monitor and protect assets situated in 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 access points. 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 IW9167 access point. However, for PoE, the camera should be connected to the IE3400 switch.

The Workgroup Bridge (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. Video surveillance traffic from the yard camera infrastructure is carried on a separate VLAN. Other enterprise service traffic can be segmented as needed.

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

Transit Management (Operations) Center Systems

The Transit Management Center in the Cisco Converged Public Transport system refers to the location, both logically and physically, where all centralized systems and infrastructure reside. There are alternatives to host some transit applications in the cloud as an option. The following sub-systems reside within the Transit Management Center (TMC):

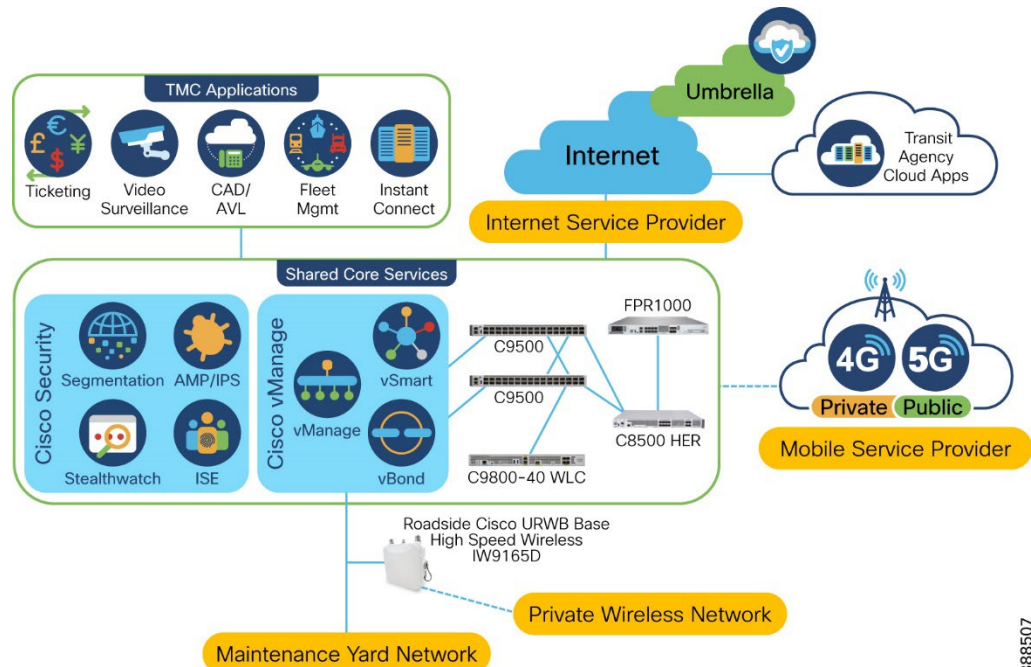
- **Dispatch Center:** Location of the Mass Transit operators and dispatchers. Incorporates management consoles for fleet management system, CAD system for dispatch, video management system, ticketing, Instant Connect voice PTT system.
- **Core Services:** The core services at the TMC provides the following functions:
 - VPN connection termination from transit vehicles, and transit stops/stations and the yard.
 - C8500 or similar Head End Router scaled to support the number of connections required based upon fleet size.
 - Firewalling for filtering out unwanted traffic from entering the TMC
 - FPR1000 class firepower firewall
 - Connect and distribute traffic from the transit vehicles, stops/station, services originating in the TMC such as SD-WAN Manager (on-premises version), Cisco

security solutions (including Umbrella, Cisco Secure Network Analytics, and ISE), transit applications and cloud-based and cloud-based transit applications.

- C9500 class stackable enterprise switch in number sized to meet the demands of the fleet size and traffic flows.
- Wireless LAN Controller (WLC) for management of APs on the transit vehicles and access control for passengers and transit workers wanting to connect over Wi-Fi assets.
 - C9800-40 class wireless LAN controller.
 - Note that passenger traffic does not require the WLC unless it is desirable for a one-time sign-on for the passenger during their journey.
- SD-WAN Manager for deployments using SD-WAN networking and desiring to use an on-premises installation.
- **Applications:** Transit applications can reside at the TMC connected into the core switches or in the cloud hosted by any cloud service connecting to the core services over the internet. Applications include:
 - Fleet management, CAD/AVL, Ticketing, video surveillance, PTT voice, passenger information sign controllers, passenger counting databases, and many more.
 - Applications running in the cloud leverage the FPR1000 firewall to allow management consoles in dispatch to connect to servers/applications through the internet.

Refer to the diagram that follows.

Figure 22. Transit Management Center



388507

Note the connections to the TMC the cellular MSP, Internet service provider, maintenance yard network and, if used, a private Cisco URWB network. All network connections will be terminated by the C8500 head end router and the FPR1000 firewall.

Network Management Systems

Network management systems provide for management of network infrastructure (in this case routers and switches on the transit vehicles, at the stops/stations and in the yard). The management includes network device configuration, security configuration, monitoring, and troubleshooting.

For the Cisco Converged Public Transport system there are two options available for network management:

- Cisco SD-WAN Manager for network devices on an SD-WAN network.
- IoT Operations Dashboard for network devices running over non-SD-WAN standalone networks.

These options each bring strengths and weaknesses with the choice being a function of what is most important to the customer.

SD-WAN Manager

This network management tool is targeted to users of existing SD-WAN enterprise networks that are adding on the mobile fleet under a common management tool. The work will be mostly IT-led as the transit network will be an extension to an existing IT network. Using a large offering of template-based configurations as well as the ability to add in low-level command line configurations make this a powerful tool.

Figure 23. Cisco SD-WAN Manager Overview



Details for leveraging SD-WAN Manager for Industrial applications can be found in the following Cisco Validated Design links. Refer to these documents for details.

[Cisco SD-WAN for Industrial Applications Design Guide](#)

[Cisco SD-WAN for Fleet Applications Design Guide](#)

Key advantages of SD-WAN Manager:

- One management tool for both Enterprise and Industrial devices in the transit fleet and stops.
- Both cloud-hosted and on-premises options
- Supports multiple WAN transports (for example, cellular, Cisco UWRB (not managed by SD-WAN Manager), WGB* (*WGB in an upcoming release) for resilience and flexibility.
- Security policies consistently pushed through the Enterprise to the transit vehicle and transit network.
- Transit Management Center head end routers and transit vehicle routers can be managed on the same network fabric, simplifying VPN creation and termination.
- Support for advanced routing features, QoS, applications-aware routing.

Disadvantages/Limitations of SD-WAN Manager:

- No inherent edge compute support at this time, limiting the use of value-added IOx applications described earlier in this document.

IoT Operations Dashboard (IoT OD)

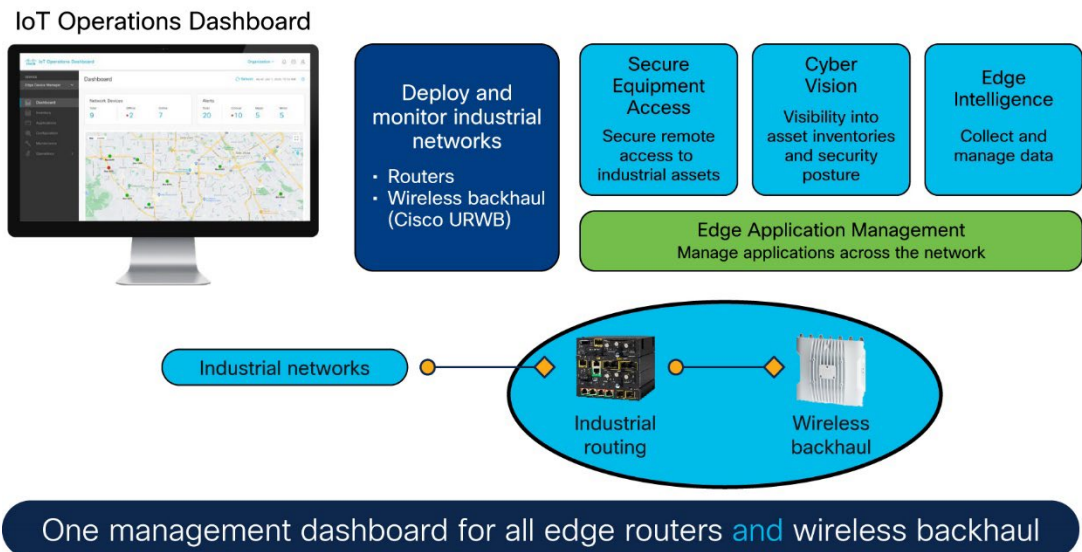
This network management tool is more targeted to OT users building a transit system as a standalone or tailored system rather than as part of an enterprise extension. Using a limited number of template-based configurations, IoT OD is a tool that still requires some IT involvement, but which can be run by OT personnel. Key to the power of IoT OD is the support of other OT services to connect, maintain and secure the transit system network assets as well as gain insights into operation.

See the figure that follows.

Figure 24. Elements of Cisco IoT Operations Dashboard

Elements of Cisco IoT Operations Dashboard

IoT OD is a cloud platform of OT services to connect, maintain and secure industrial assets and gain insights



388506

As an OT-targeted tool, IoT OD provides some additional functions beyond pure network

management. These include:

- The ability to see behind the router to connected devices on the transit vehicle. This visibility is key to monitoring and troubleshooting transit vehicle problems while still away from the yard.
- Support for secure, credentialed access to transit vehicle and transit stop devices such as cameras, signs, passenger counters, etc., remotely, and natively from any location with an internet connection. More about this is explained in a later section.
- IOx edge application lifecycle support.

Details for leveraging IoT Operations Dashboard for Industrial applications can be found in the following Cisco Validated Design link. Refer to this document for details.

[IoT Operations Dashboard Product Documentation](#)

This product documentation is in the Cisco Developer Network (DevNet) documentation cloud.

Key advantages of IoT Operations Dashboard:

- One management tool for Industrial devices and private wireless backhaul (CURWB) in the transit fleet and stops.
- Support for edge compute, support for the use of value-added IOx applications described previously in this document.
- Supports multiple WAN transports (for example, cellular, Cisco UWRB, WGB) for resilience and flexibility.
- Secure Equipment Access support for remote troubleshooting.

Disadvantages/Limitations of IoT Operations Dashboard:

- Only cloud-hosted option
- Only basic routing features
- No integration with head end routers

See the following figure for a Comparison summary.

Figure 25. IOT Operations Dashboard or SD-WAN Manager

SD-WAN Manager	IoT Operations Dashboard
<ul style="list-style-type: none"> • IT centric buyer (that already uses SD-WAN) • Cloud or on prem options • Out-of-the-box data center and edge router integration with one management tool • Feature rich, capable of addressing more complex network environments and capabilities such as segmentation, security policies, multiple WANs • Limited edge compute support 	<ul style="list-style-type: none"> • OT centric buyer (that does not use SD-WAN) • Cloud-only • Basic networking features with GUI • Supports SEA/SEA+ for secure remote access • Edge Compute application management framework • Supports both routers and wireless devices • No out of the box data center integration

388510

Management of transit vehicle devices and systems is through individual configuration tools and management tools that communicate with the transit network.

Secure Equipment Access (a service within IoT Operations Dashboard):

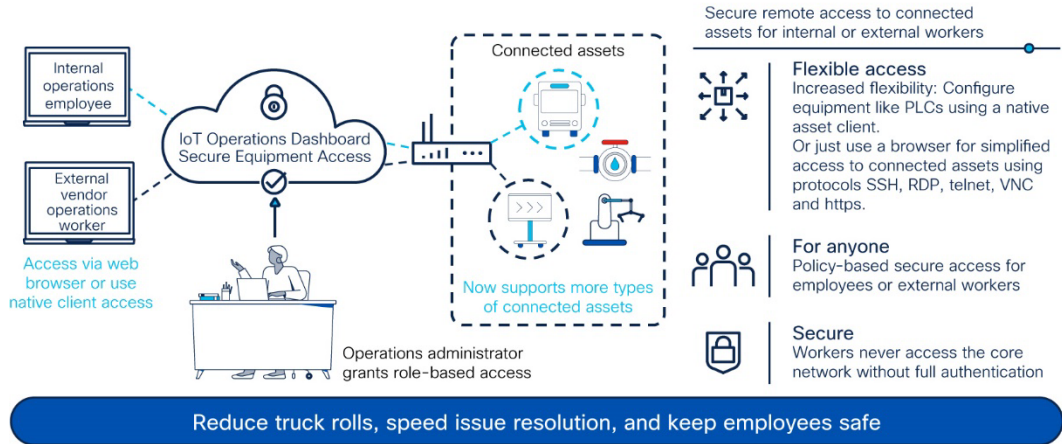
For troubleshooting, the Secure Equipment Access (SEA) service provides the means for a transit worker or external contractors to securely connected to the systems on the transit vehicle that are connected to the IR183x mobile router. It supports an industry standard set of pre-packaged protocols (HTTP/S, SSH, VNC, RDP, Telnet) as well as the ability to operate in a native application

mode where proprietary protocols are used to communicate between the vendor applications and transit vehicle subsystems. The key benefit is avoiding having to return a transit vehicle to the yard to perform troubleshooting as the SEA capability allows for remote operations.

Figure 26. Secure Remote Access for All Connected Assets

Secure remote access for all connected assets

Easily enable operations teams to securely maintain connected assets and manage access



Using role-based access granted by an administrator, an internal transit employee or external vendors connect to IoT Operations Dashboard and into the SEA service using their web browser to active a secure communication link to the equipment on the transit vehicle.

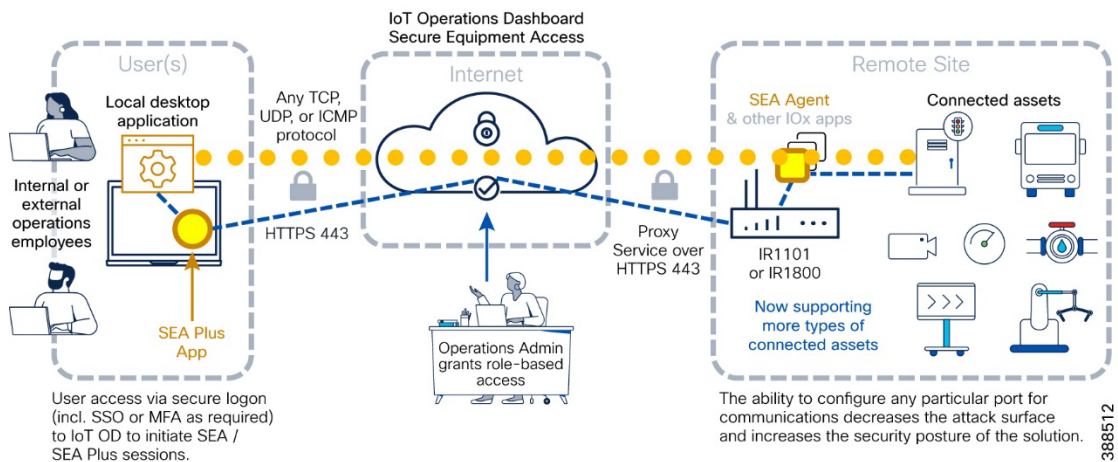
Notably, with transit vehicle devices on separate VLANs for segmentation and often connected behind a subtended switch to allow for greater port density, the SEA solution must operate in that environment.

Where a proprietary native protocol is required, provided it runs over TCP, then SEA can also be used for remote connectivity. A small SEA Plus App acting as an agent is required on the user laptop. Once in place, the same secure remote connectivity is provided using a native interface.

Figure 27. SEA Plus Solution Architecture

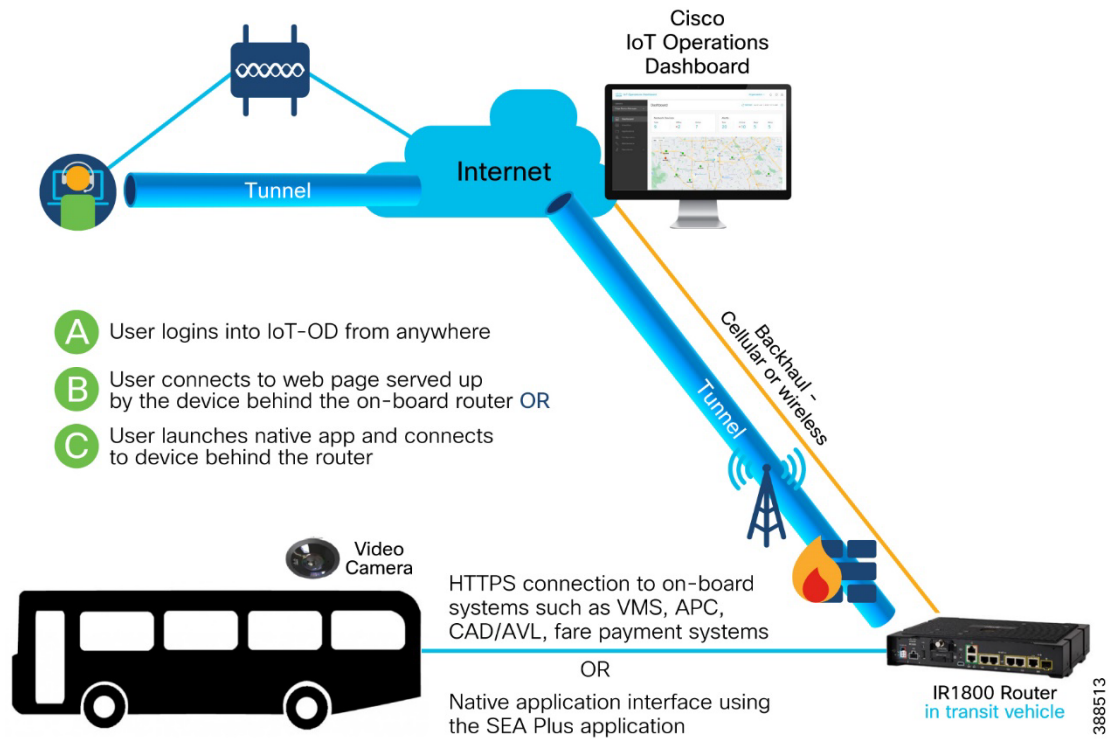
SEA Plus Solution Architecture

Use your native local application with any TCP, UDP, or ICMP protocol to access any remote equipment



The result is illustrated in the figure that follows.

Figure 28. Example: Secure Equipment Access – HTTPS/Native



Traffic Flow and Security

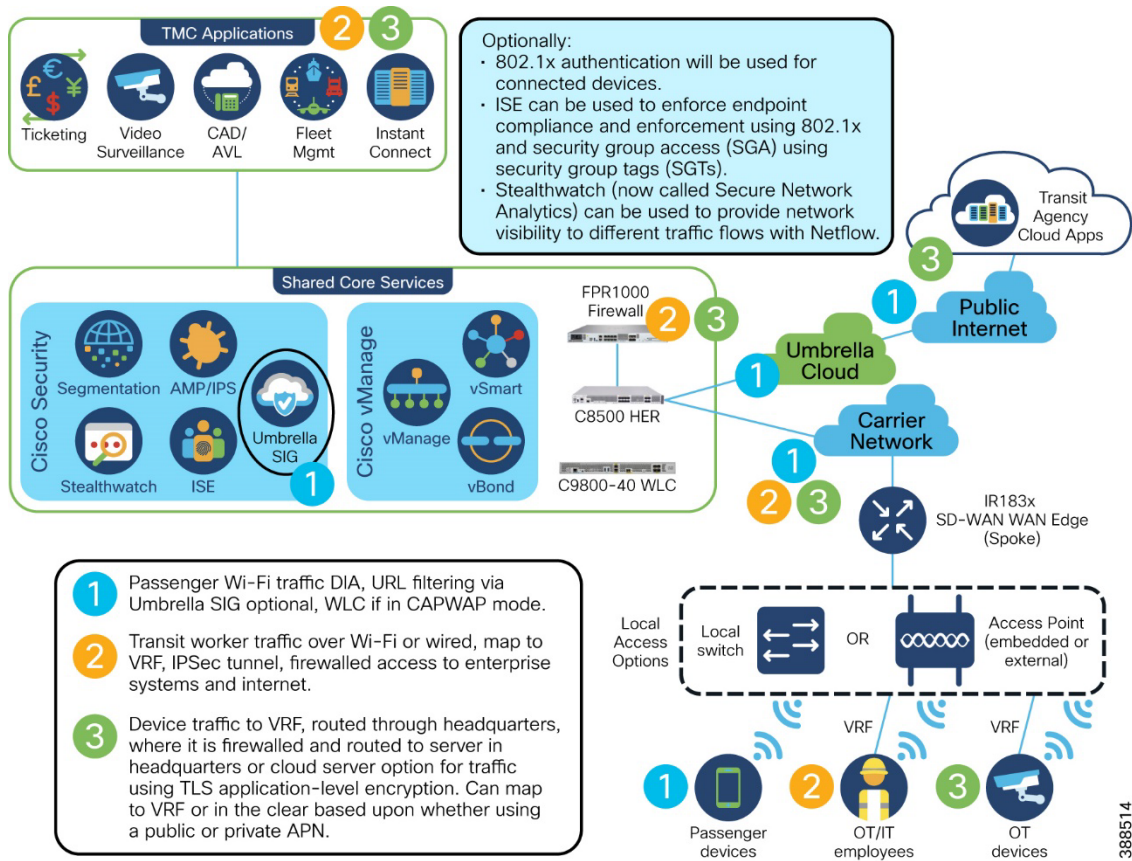
Security for SD-WAN and IoT OD connected transit vehicle routers and devices will be similar but different in important ways.

For SD-WAN managed deployments:

- Passenger Wi-Fi traffic is DIA, with potential use of Umbrella SIG for controlling access to certain URLs
- Worker Wi-Fi or wired traffic will be to Headquarters using a Service VPN
 - Traffic will flow through the firewall
 - Access to Enterprise systems is controlled
 - Access to the Internet is managed by the Headquarters network
- Device traffic will map to a Service VPN and be required to go to Headquarters (best practice)
 - Traffic terminating at a server application in Headquarters goes through the firewall
 - Traffic terminating at a server application in the cloud enters Headquarters, passes through the firewall, and traverses the Internet to reach the cloud server application

Refer to the figure that follows showing how different types of traffic flow and how security is applied in an SD-WAN deployment.

Figure 29. SD-WAN Configuration Traffic Flow/Security

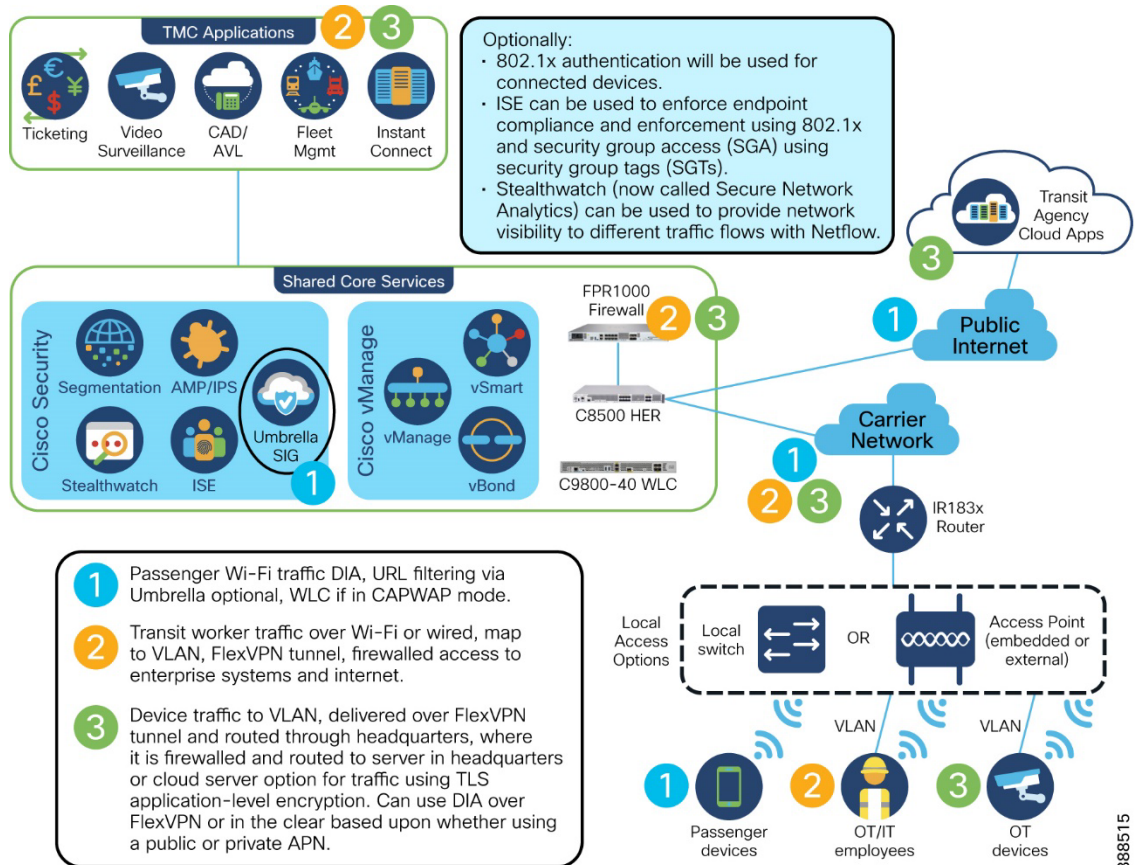


For IoT Operations Dashboard managed deployments:

- Passenger Wi-Fi traffic is DIA, with potential use of generic Umbrella for URL filtering as an additional feature
- Worker Wi-Fi or wired traffic will use macro_segmentation via VLANs and will be carried over a FlexVPN connection.
 - The VPN will terminate at the HER
 - Traffic will flow through the firewall
 - Access to Enterprise systems will be controlled
 - Access to the Internet will be managed by the Headquarters network
- Device traffic will use FlexVPN or TLS application encryption or both
 - Traffic terminating at a server application in Headquarters will go through the firewall
 - Traffic terminating at a server application in the cloud will enter Headquarters, pass through the firewall and traverse the internet to reach the cloud server application
 - Traffic requiring TLS will have the option of going directly to the internet, using a FlexVPN taking into consideration whether the routers are on a public or private APN

To illustrate this, refer to the figure that follows showing how different types of traffic flow and how security is applied in an IoT Operations Dashboard deployment.

Figure 30. IoT-OD Configuration Traffic Flow/Security



388515

System Components

This section details the Cisco and third-party components included in the Cisco Mass Transit system design.

Cisco Products

Table 3 Cisco Components

Vendor	Model	Description
Cisco	IR183x	Vehicle Onboard Mobile Router with integrated 4 port gigabit Ethernet switch with Power over Ethernet (PoE), GPS, native CANbus, GPIO, dual radio Wi-Fi6 AP and dual LTE/5G cellular modems. Also used for transit stops.
Cisco	IR1101	Stationary router with integrated 4 port fast Ethernet switch, dual LTE/5G cellular modems. Main selection for transit stops.
Cisco	IE3x00	Ruggedized gigabit Ethernet switch family with PoE for onboard vehicle and at the transit stops.
Cisco	IE9300	Alternate 24 port and stackable ruggedized gigabit Ethernet switch with PoE for onboard vehicle.
Cisco	IW9167	Industrial CURWB base station or, alternatively, an 802.11ax access point.
Cisco	IW9165D – base IW9165E – client	Industrial CURWB base station for vehicle to ground communication (IW9165D) and matching CURWB client device for on board the transit vehicle.

Cisco	Catalyst 8500	Head end router for termination of service VPNs into the transit management center network.
Cisco	Catalyst 9500	Enterprise gigabit Ethernet switch for the transit system network, residing in the transit management center.
Cisco	Catalyst 9800-40 WLC	Wireless LAN Controller for managing IW9167 APs and APs integrated in the 802.11ax/Wi-Fi6 PIM module on the IR183x vehicular router.
Cisco	FPR1000	High-capacity Firepower Firewall for protection of enterprise network infrastructure from public Internet peering connections.
Cisco	ANT-7-5G4WL2G1-0	7-in-1 Antenna for Cellular, Wi-Fi, GNSS
Meraki	MV72 or MV72X	Cameras used at transit stops or stations

3rd Party Products

Table 4 3rd Party Components

Vendor	Model	Description
Instant Connect	Rugear RG750	Ruggedized android client smartphone device for use by the driver of the transit vehicle
Hanover	Digital Sign System	Comprised of the following components: EG4 sign controller, TFT display controller/onboard computer, rear/front/side passenger information signs, optional TFT display
Axis	Camera system	Onboard vehicle cameras system comprised of the following components: P3925-R/P3925-LR ruggedized cameras; F2105/F2135 camera sensors + F9114 main unit providing camera back end processing
Milestone	Xprotect NVR	Ruggedized standard windows compute platform running Milestone XProtect software to perform NVR functions.
Dilax	APC system	Automatic passenger counting system comprised of: PCU-210 APC Master, PRT-400 passenger sensor; SLS-1000 passenger sensor
Daktronics	VFC-3000	Passenger information controller and signs for showing ETAs at transit stops and stations

Software Feature and Application Support

The following table outlines the software features and application supported in the Converged Public Transport system in this phase.

Table 5 Software Features and Applications Supported

Software Application	Function
IoT Operations Dashboard	Geographical Information System (GIS) Cisco Devices Zero Touch Provisioning 3rd Party Device access through Secure Equipment Access Vehicle GPS location tracking Group template-based configurations for fleet vehicles
SD-WAN Manager	Enterprise grade, SD-WAN network manager

	Geographic Information System (GIS) Cisco Devices Zero Touch Provisioning (ZTP) Vehicle GPS location tracking Group based templates for transit vehicle configurations
Instant Connect Enterprise software	Instant Connect PTT voice application responsible for routing, merging, repeating audio connections between driver, dispatch, transit workers, and security forces.
Hanover Sign Management Milestone XProtect	Hanover Central Software (Cloud and SFTP server hosted by Azure) XProtect video storage and management system in the transit management center or cloud
Dilax Citisense	Cloud-based passenger counting back end taking in APC records and the transit agency schedule to provide ridership analytics and reports
Wi-NOx Dashboard	Cloud or on-premises application collecting reports from transit vehicles that are WI-NOx enabled and providing analytics on emissions, fuel consumption, driver behavior and preventative maintenance
Meraki Field Controller	Meraki cloud-based video capture and analytics software for use at stops or stations. Links with IoT Operations Dashboard.
Daktronics Vanguard Field Controller	Transit Management Center or cloud-hosted software to configure and control message sign content.
CANbus IOx application	Embedded IOx docker application executing on the IR183x to capture CANbus data, filter for desired fields, format in JSON for delivery to a MQTT server for later analysis.
Web Portal	Wi-Fi User Authentication

System Functional Considerations

Data Center

All centralized system aspects and backend services of the Converged Public Transport system are hosted in a Data Center environment. The Cisco Design Zone for Data Center 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 Converged Public Transport scope. For more information:

<https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides.html>

Cisco Connected Roadways

For transit stops and stations, being in proximity to a connected roadway network is likely. This connected roadways network can be leveraged to provide backhaul transport of communications between the stop/station and transit management center.

The Connected Roadways system design is documented here:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Roadways/cci-dg_roadways/cci-dg_roadways.html

Cisco SD-WAN for Industrial Markets

The Converged Public Transport system design described in this document may operate on an SD-WAN enterprise class network which involves many levels of complexity not repeated here.

The SD-WAN for Industrial Markets Cisco Validated Design provides guidance on how to use SD-WAN for industrial applications.

The Cisco SD-WAN for Industrial Markets CVD can be found here:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-case-study.pdf>

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-fleet.pdf>

Cisco Secure Equipment Access

The Secure Equipment Access system design described in this document capture many of the details of how SEA works for various system architectures and how to configure and set up for its use.

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/Secure-Remote-for-IA-Networks/Secure-Remote-Access-for-Industrial-Networks-design-guide.pdf?ccid=cc002176&dtid=odicdc000509

Caveats

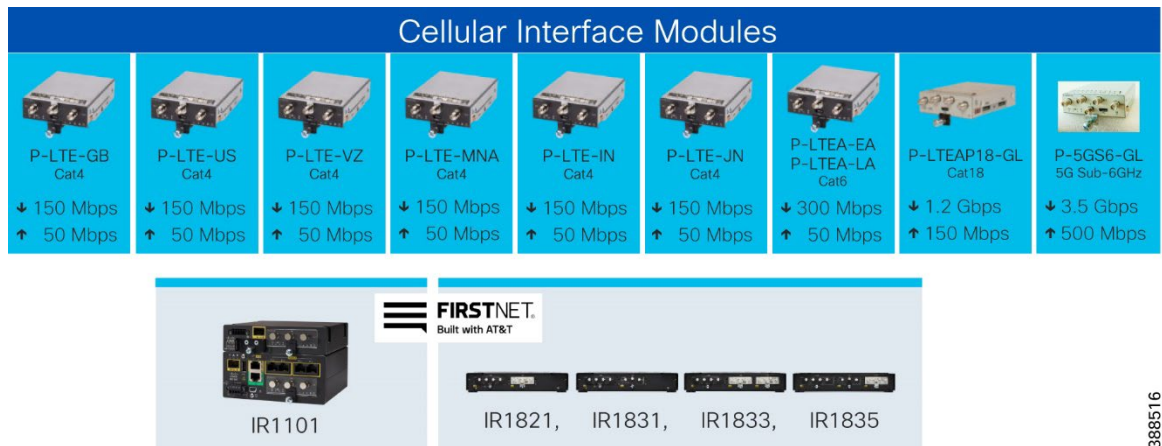
In the Converged Public Transport solution, there are some notable limitations that need to be considered in selecting among different paths.

This list represents current limitations. All items on the list are on the roadmap for full support in the near future.

Cellular module GPS support

This illustration shows the cellular PIM modules supported on the IR1800 mobile router and the IR1101 industrial router.

Figure 31. Cellular Pluggable Interface Modules for Industrial Routers



388516

Table 6 GPS Support on Cellular Modules

Cell Model Category	GPS Capable
Cat 4 LTE	Yes
Cat 6 LTE	Yes
Cat 18	No
5G sub-6GHz	Yes

Table 7 GPS Reporting to management tools

GPS Source	SD-WAN Manager	IoT Operations Dashboard
Cat 4 or 6 LTE modem	Yes	Yes
5G modem	Yes	No
Dead Reckoning module	No (roadmap)	No (roadmap)

Wi-Fi Work Group Bridge (WGB)

- This feature is currently not supported by SD-WAN Manager but is under development.

GPIO SNMP traps

- This feature is not supported by devices managed by IoT Operations Dashboard.
- This feature is fully supported by the SD-WAN network and SD-WAN Manager.

IOx docker application lifecycle management

- SD-WAN Manager does not support the downloading, starting/stopping, or updating of IOx docker applications. This function must be performed manually through the router console-based management interface or IOX Local Manager GUI.
- This capability is fully supported in an IoT Operations Dashboard environment.

ITxPT specifications support

- Cisco recognizes the growing demand for products compliant with the ITxPT specifications (IT for Public Transport). Compliance is a roadmap item and is planned for a future update to this document.

Security, High Availability, and Scale

Quality of Service (QoS)

The Converged Public Transport 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 utilized in the Converged Public Transport system, with mapping between these mechanisms supported at the boundaries between the different transport mechanisms.

The following classes of service are implemented in the Converged Public Transport system, and are shown with mappings between representative classification markings for each type of classification.

Table 8 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 Converged Public Transport 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 50 to 200 Mbps of throughput. Ideally, the Mobile Service Provider will support multiple LTE QCI values for the service provided to the Mass Transit

operator, and prioritization of expedited forwarding (EF) and assured forwarding (AF) classes over best effort (BE) traffic can be guaranteed in both directions. If the Mobile SP does not offer multiple QCI classes, then prioritization of EF and AF traffic can still be accomplished in the upstream direction from the IR1800 router toward the Mobile SP. 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 1800 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, there is the potential for a bottleneck to 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 Mobile SP and Internet SP:** Often times, 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 utilized on the uplink connection of the peering router from the mass transit operator's network, with a parent shaper equal to the bandwidth of the service and child classes defining the proper queuing treatment for each class. Even in the case where the service bandwidth is equal to the physical bandwidth of the link, a parent shaper can help in smoothing traffic flow toward the SP and yielding better application throughput versus relying on the port PHY to indiscriminately drop excess packets.

Security

The Converged Public Transport 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 access points implement WPA2 security, which includes enterprise level authorization and encryption of traffic. The Wi-Fi sub-system also supports EAP, LEAP, PEAP, EAP-TLS, and TKIP.

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 authorization. Cisco provides full Mobile Device Management (MDM) functionality for secure mobile device deployment, which is fully compatible with the Converged Public Transport system.

Outside access to the operations center infrastructure via UNI connections to the Mobile SP and Internet SP is protected by a Cisco FirePower security node. The FirePower_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:

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

The Converged Public Transport 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 IPsec tunnels. The IPsec implementation in the onboard router is capable of supporting many different encryption standards: DES, 3DES, AES 128, AES 192, and AES 256. The Converged Public

Transport system recommends implementing the strongest standard and largest keys supported to provide the most secure connection. The only traffic not transported in the IPsec tunnel is passenger Internet traffic, which is routed directly to the Internet through the Mobile SP. 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 mass transit agency data center.

As the IPsec 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.

VPN Headend Redundancy & Reliability/Availability Models (HA)

The headend routers at the enterprise datacenter provide centralized termination of all spoke VPN tunnels from the industrial routers in the field – on buses, at bus stops, and so on. This centralized headend should be deployed with redundancy and resiliency in mind, as a single router could create a single point of failure, causing serious issues for remote applications and devices that depend on secure connectivity via the VPN tunnels.

Redundancy can be deployed at various levels:

- Within a single hardware platform: redundant power supplies, route processors, and interfaces provide resiliency in the event of failure of a single subsystem of the platform, or an upstream WAN failure.
- Multiple hardware platforms at a single site: an additional hardware platform (router) within a datacenter can provide failover resiliency if the other router goes down completely. Multiple routers also have the added benefit of increasing scalability in terms of being able to balance the load of large numbers of VPN tunnels across the headends. It is important to not oversubscribe the headend routers so that the failure of one headend does not result in all tunnels reconnecting to the remaining headend and overloading it.
- Geo-redundancy: deploy headend routers at disparate geographical locations to help minimize impact of natural disasters, power outages, and more. This option provides similar scalability benefits as well.

Initial Scalability/Performance Assessment

The systems and platforms proposed in the Converged Public Transport system design are geared to easily handle a vehicle fleet of 4000 vehicles and can be scaled to handle even larger fleets.

Cellular 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
- 10 Mbps minimum throughput available to each user

Using these assumptions, each vehicle requires approximately 250 Mbps of bandwidth for passenger internet traffic. A single 5G link from a vehicle should accommodate approximately 300 Mbps (or more) of bandwidth, leaving 50 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. In case of the Mass Transit operator needing 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.

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 Workgroup Bridge (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 there are no video surveillance files to be transferred at this point, so bandwidth requirements are greatly reduced.

The Converged Public Transport system design targets a ratio of vehicles to yard access points of approximately 10 to 1. If greater throughput is needed, then more yard access points can be deployed. The number of vehicles connected to a single access point receive an equal ratio of bandwidth from the access point 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 access point, 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.

Installation Guidance and Parameters

A key benefit of the Converged Public Transportation solution is the simplicity of onboarding gateways, which allows non-IT users in the field to deploy the gateway with little to no IT support. This also significantly speeds up bulk gateway deployments across geographically dispersed locations. Leveraging SD-WAN Manager or -IOT Operations Dashboard template based configurations, office staff can define the desired feature set and fill in relevant details all at once allowing field technicians to focus on installing the hardware with without worrying about software configuration details. Once the devices are deployed in the field, monitoring and remote access capabilities help identify and resolve any issues that appear after installation.

It is recommended that prior to installing routers in the field, it is recommended to do a proof-of-concept deployment in a lab environment so that the desired configuration can be easily verified on a small number of devices before rolling out a large production network. Physical installation is just as important as the software configuration because it determines how the router stands up to the surrounding environmental conditions, as well as backhaul connectivity performance and reliability (especially in the case of cellular technologies).

Installation Best Practices

In addition to the best practices described in this document, refer to the product installation guides below for official recommendations on mounting, power, antennas, and more.

Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide:

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_01.html

Cisco Catalyst IR1800 Rugged Series Router Hardware Installation Guide:

<https://www.cisco.com/c/en/us/td/docs/routers/access/IR1800/hig/b-ir1800-hig/m-install.html>

Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide:

<https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide.html>

General Considerations for Vehicle Installation

Before starting, plan the installation carefully so it will meet the following requirements:

- The installation must be safe for the operator and passengers within the vehicle.
- The installation allows for convenient access by the operator, as applicable (i.e., the Ethernet ports, console cable, sim cards, ability to view LEDs).
- The equipment is mounted in a location assuring the vehicle occupants' safety and out of the way of passengers and auto mechanics.
- The equipment is installed away from the airbag deployment areas.
- The equipment is protected from water damage.
- The installation is neat and allows easy service access.
- Before starting the installation, it is imperative to determine the exact location in the vehicle where the equipment is to be installed. This action prevents hours of rework and reinstallation.

In addition to the considerations described in the previous paragraph, the mounting location for the router and any cables and antennas should account for the desired use case in terms of RF coverage for each radio and power source (battery or OBD-II).

Figure 32. IR1835 Mounted In Test Vehicle



Special Considerations for Vehicle Installation

Power Source Location and Considerations

Verify that the location chosen is a main power source and allows the addition of added terminals.

If an auxiliary fuse block is to be used, check that the location chosen for the block guards against possible short circuits.

Some vehicles, trucks, will have studs on the firewall that may be used to pass power without the need for a through hole. These can be used only if verified that they are not used to connect data cables or wires.

Ignition Sense Location and Considerations

Choose an ignition sense voltage source that will not interfere with the safety-related systems of the vehicle.

The ignition sense wire (white or blue wire) connection determines how or when power is applied to the mobile router. The white wire is sometimes referred to as the “white ignition switch wire” or the “ignition sense input wire”. Regardless of the configuration, the router main DC power input (red A+ wire) must be connected through an in-line fuse to unswitched vehicle DC power. The red wire must be connected to raw battery power (positive battery terminal) via the supplied fuse.

It is important to use the proper crimp tool for crimping any terminals or fuse holder.

Power On/Off Using Vehicle Ignition

The IR1800 can be powered directly by the OBD-II interface that provides a 12V (or 24V) power source in addition to the CANBUS interface. This installation allows for the use of the Ignition Sense feature to intelligently shutdown the router after a timer has expired when the detected input voltage drops, as is typical when the ignition turns off. Similarly, the router will turn on when the input voltage increases after ignition start.

Alternatively, the IR1800 can be connected directly to the vehicle battery and leverage Ignition Power Management to turn the router off and on based on the voltage on digital input pin 5 which should be connected to the vehicle ignition wire.

Ground and Return Location Considerations

Care should be taken to ensure the location chosen is truly to vehicle ground.

The location chosen should not be in an area that is prone to moisture retention.

Ensure that the location will protect the terminal from being bumped and allow the connection to loosen.

The location must allow a through bolt with a nut and lock washer or be at a factory ground.

Choose a location that will allow the ground lead to be as short as possible.

Antenna Mounting Considerations

Antenna location must be chosen based on the installation instructions and in consideration of other items installed on the vehicle's roof.

There must be at least a 24” separation between the antenna and any other roof mounted equipment (see the following figure).

If the antenna being used requires a ground plane, the location chosen must provide an acceptable ground.

Figure 33. Antennas mounted on test vehicle



Data, Antenna, and Power Cable Routing Considerations

Cables should not be routed under vehicle carpeting where the occupants' feet rest.

Plan the cable runs to protect the cables from chafing, crushing, moisture, or overheating.

Routing under the dash should not interfere with, or pass through, the steering column, brake pedal, clutch pedal, or the accelerator mechanisms.

Carefully chose the location where the wiring will exit the passenger compartment and enter the engine compartment.

In situations in which RF extension cables are utilized, be sure to mark the ends of the extension cable to correspond to the similar markings on the Cisco antenna side before hiding the cables behind the liner of the vehicle. For many of the antennas, each lead from the antenna needs to connect to a specific port on the router. But the extension cables are generic and will not natively have the markings required to identify which antenna lead is connected to it. If the connection between the antenna lead and RF extension cable is hidden behind the liner and the extension leads are not marked, the liner would have to be removed again to identify each antenna lead. So, carrying-over the markings can avoid the need to do this.

Splicing Requirements

Splicing the 12 VDC (A+) wire is not allowed. For other wires, if a splice must be installed such as to extend the wire, the following requirements must be followed:

When wire is routed through hidden locations such as door jams, under the dash or, otherwise hidden from view use a solid run.

Any splice installed must be visible to future service technicians. The best way to accomplish this is to cut off the wire back near the equipment connector and splice on a new wire.

The splice wire used must have insulation rated for use in an engine compartment.

Estimate the length of the run and determine required wire gauge.

The gauge of the wire used must be based on the length of cable run for a load of approximately 5 Amps and maximum allowable voltage drop of 200 mV at peak load. If larger gauge wire is not required the same gauge shall be used, but never a smaller gauge.

When splicing a wire that could be exposed to moisture use a butt splice encased within heat shrink tubing to seal the connection.

Battery Connection Requirements

The 12 VDC power source should be the battery if possible. Other sources may be used if a battery connection is not available or feasible. Acceptable sources are the input to the main relay/fuse panel in the engine compartment, other main 12 VDC terminal, or installation of an auxiliary fuse block.

An inline fuse holder is used for the mobile router to protect the equipment and the vehicle from a possible short circuit or excessive current draw. The fuse amperage must be according to the manufacturer's specifications. The fuse holder is water resistant to protect the fuse from the elements and avoid the possibility of corrosion. For optimum safety, the fuse should be placed as close to the battery as possible.

If an auxiliary fuse block is being installed, the conductor used to connect it to 12 VDC should be gauged large enough to support the current flow of all the equipment that is fed by the block. The gauge of the cable to be used must be based on the length of cable run for a load of approximately 40 Amps and maximum allowable voltage drop of 200mV at peak load. In most cases this conductor consists of #6 AWG or #8 AWG wire. The insulation of this conductor must be properly rated for engine compartments. An inline fuse holder must be installed on this wire near the battery. The fuse holder must be water resistant, and the amperage of the fuse installed should be rated large enough to handle the total current flow of the block. In most cases the fuse rating is 40 or 50 amps.

Glossary

Term	Description
AAG	At A Glance
AP	Wi-Fi Wireless Access Point
APC	Automatic Passenger Counting
API	Application Programming Interface
APTA	American Public Transport Association
ATMS	Automatic Traffic Messaging System
AVL	Automatic Vehicle Location
BGP	Border Gateway Protocol
BOT	Build Operate and Transfer
BU	Business Unit (for example, entity which develops products)
CAD	Computer Aided Dispatch
CAN Bus	Controller Area Network Bus
CC	Concept Commit
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
DMVPN	Dynamic Multipoint Virtual Private Network
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EC	Execute Commit
EEM	Embedded Event Manager
EFT	Engineering Field Trial
EPN	Evolved Programmable Network
ETA	Estimated Time of Arrival
FCAPS	Fault, Configuration, Accounting, Performance and Security
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema, a Russian version of GNSS
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSMA	Groupe Spéciale Mobile Association
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol, Secure
IGP	Interior Gateway Protocol
IoE	Internet of Everything
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
IVSG	IoE Vertical Solutions Group
IVU	In-Vehicle Unit
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LDP	Label Distribution Protocol
LTE	Long Term Evolution (4G)
MIMO	Multiple Input, Multiple Output
MODEM	Modulator-Demodulator
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NFC	Near Field Communication
NDP	Neighbor Discovery Protocol
OBE	On Board Equipment
OSPF	Open Shortest Path First
PA	Public Address
PEAP	Protected Extensible Authentication Protocol
PIS	Public Information System
PSK	Pre-shared Key
QoS	Quality of Service
RFID	Remote Frequency Identification
RSSI	Received Signal Strength Indication
RTPI	Real-time Passenger Information
S+CC	Smart and Connected Cities
SAE	Society of Automotive Engineers
SAS	System Architecture Specification
SEVT	Systems Engineer Virtual Team (bi-annual technical team meetings)
SNMP	Simple Network Management Protocol
SP	Service Provider
SR	System Release
SRC	System Readiness Commit
SRD	System Requirement Document
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TME	Technical Marketing Engineer
TSS	Transportation Smart Solution
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLU	Vehicle Logic Unit

VLUS	Vehicle Logic Unit System
VMDC	Virtualized Multitenant Data Center
WBDT	Wireless Bulk Data Transfer
WGB	Workgroup Bridge
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access, Second Generation

