First Responder Fleet Cisco Reference Design

May 2018

Cisco
Reference
Design

Cisco Systems, Inc. www.cisco.com

Contents

First Responder Fleet Cisco Reference Design

Welcome to the First Responder Fleet Cisco Reference Design (CRD).

Audience

The intended audience for this document includes Cisco account teams, Cisco Advanced Services teams, and systems integrators working with first responder agencies, such as police and fire departments, and Emergency Medical Transport companies. It is also intended for direct use by these first responder agencies to understand the features and capabilities enabled by the Cisco Connected First Responder Fleet System design.

Introduction

This document provides a comprehensive explanation of the CRD system design for First Responder Fleet deployments. The goal of the system design is to provide a comprehensive and converged communications infrastructure and application framework to enable the deployment of multiple services for First Responder Fleets. It includes information about the system's architecture, possible deployment models, and guidelines for implementation and configuration. This guide also recommends best practices and potential issues when deploying the reference architecture.

Use Cases

This document addresses the deployment of a comprehensive and converged communications infrastructure and enables the following technology use cases:

- Dash / Passenger Video Surveillance
- Dual LTE support for WAN connectivity while vehicle is in service
- Extension of Enterprise Wi-Fi Network services to devices in and around the vehicle
- Fleet Management
- High Value Asset Tracking
- License Plate Recognition
- Vehicle Location and Telemetry Data Collection and Correlation
- Vehicle Two-way Voice Communication (Push to Talk Radio over IP)
- Wi-Fi WAN connectivity while vehicle is parked within range of agency Wi-Fi coverage

System Overview

The CRD for First Responder Fleets provides an end-to-end system design for service delivery and support for police, fire, and emergency responder vehicle fleets. The system scope includes connectivity to vehicles, an application-enablement platform for service delivery, and best practice recommendations for deployment of wireless infrastructure in vehicle parking areas such as at police and fire stations. The solution provides a converged, multi-service, secure, and standards-based infrastructure on which operational capabilities for vehicles can be delivered. It replaces redundant, proprietary, and single application solutions with limited or no interconnectivity. This results in improved safety and reduced CAPEX and OPEX for First Responders.

As mentioned above, this reference guide provides a comprehensive explanation of the First Responder Fleet System design. It includes information about the system's architecture, supported services, and possible deployment models. The guide also recommends best practices and potential issues when deploying the reference architecture. Where appropriate, the document also provides guidelines for implementation and configuration of the system architecture and supported services.

System Architecture

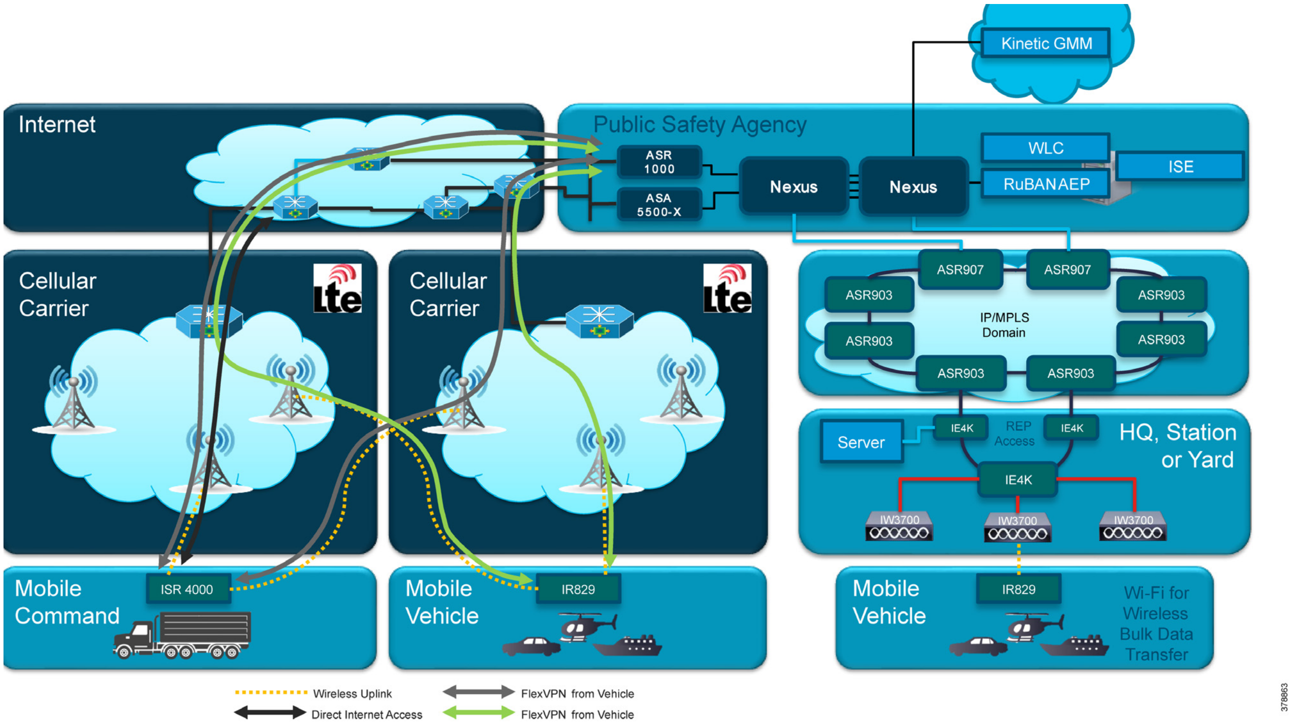
This chapter includes the following major topics:

This release of the First Responder Fleet System proposes a scalable and resilient design for the following aspects of a first responder agencies' infrastructure and services:

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

Figure 1 illustrates the layers of the First Responder Fleet System, each of which is described in greater detail in this section.

Figure 1 First Responder Fleet System Overview



Related Efforts

The First Responder Fleet System focuses on infrastructure and services specific to first responder operations, safety and optimization, and passenger connectivity and services.

The First Responder Fleet design interfaces with key aspects from other Cisco Validated Designs for the following areas:

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

Inter-System Interfaces

The First Responder Fleet System relies on Long-Term Evolution (LTE) services, which are provided by a Mobile Service Provider, to enable network connectivity between the vehicles, Internet, and backend systems while the vehicle is in motion. This service must enable Layer 3 connectivity to and from the vehicles. The choice of Mobile Service Provider is left to the first responder agency, provided the service requirements outlined in this document are met.

Functional Description

Connected Vehicle Onboard Network and Systems

The vehicle onboard network design proposed in the Connected First Responder Fleet System consists of the components shown in Table 1.

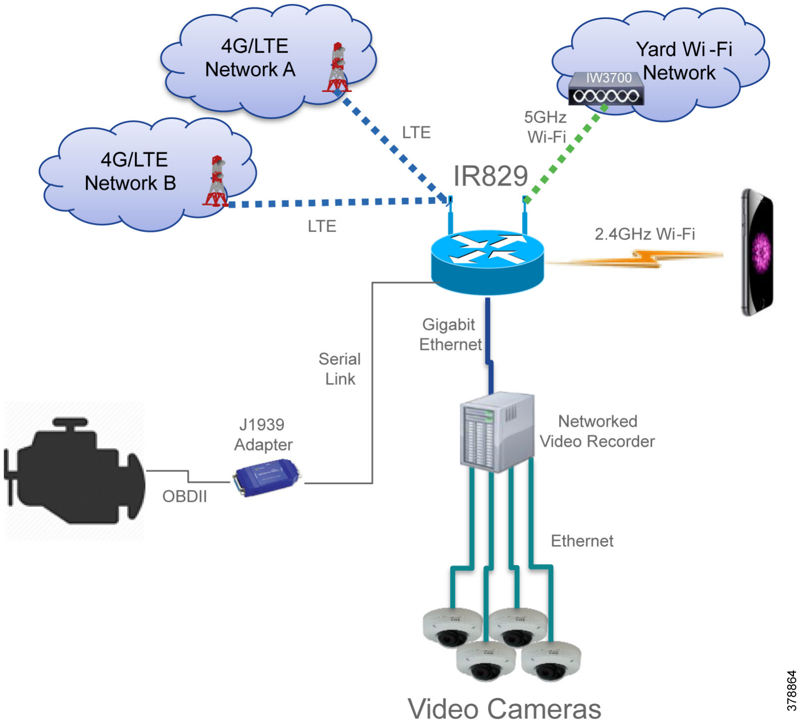
Table 1 Connected Vehicle Onboard Components

Component	Provides...
Cisco IR 829 Mobile Router	■ IP routing and gateway functionality for all onboard systems ■ Wireless connectivity for enterprise systems, both in and around the vehicle ■ All wireless off-boarding connections: Single or Dual LTE and Wi-Fi Workgroup Bridge (WGB) ■ An on-demand secure, encrypted infrastructure for transmitting data from onboard systems over data services provided by Mobile Operators ■ Engine Telematics data gathering through applications deployed onboard the Cisco IR829 Controller Area Network (CAN) bus integration (via Cisco IOx and a serial connection
Advantech B+B Smartworx ODBII / J1939 Adapter	■ Converts the Onboard Diagnostics (OBDII) connection to the CAN bus of the vehicle into a serial connection to the Cisco IR829 router
Video Surveillance System	■ System integration with popular video surveillance solutions for first responder agencies from Panasonic, WatchGuard, Axon, and Getac ■ Includes one or more cameras to provide video and audio monitoring of vehicle and employee ■ Integrates video storage, either within the camera or with a ruggedized server

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

- **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.

Figure 2 Vehicle Onboard Network Overview



The Cisco IR829 router provides wireless connectivity for devices onboard the vehicle, using the 2.4GHz radio of the integrated wireless access point. The access point is capable of implementing multiple SSIDs on this radio if that is required for the services the first responder agency wishes to deploy. Each SSID is mapped to a separate VLAN that is trunked to the router portion of the Cisco IR829 in order to facilitate service separation and security. The 5GHz radio of the integrated wireless access point in the Cisco IR829 is dedicated as a WGB to provide high-bandwidth connectivity for the vehicle systems when the vehicle is parked in a station or other agency facility. Traffic to this radio is also on a separate VLAN, specifically the native VLAN, which is trunked to the router portion of the Cisco IR829. This places the routing engine of the Cisco IR829 between the Gigabit Ethernet ports, the 2.4GHz radio, and the 5GHz WGB and LTE radios providing the WAN connections from the vehicle. This allows the router to perform all needed networking functions on traffic from the onboard vehicle systems and from passenger devices, and facilitate routing of traffic to the appropriate WAN connection.

The Cisco IR829 provides four Gigabit Ethernet LAN ports for device connectivity in the vehicle. For video surveillance, the IP camera(s) and DVR server connected to the LAN ports will be configured for a Video Surveillance VLAN in order to provide service separation. The Cisco IR829 is also able to provide up to 30 watts of Power over Ethernet (PoE), allowing for the IP cameras to be deployed without separate power connections. If more than four Ethernet LAN ports are required for onboard device connections, then a Cisco Industrial Ethernet switch can be deployed to provide the additional LAN ports.

The OBDII port from the vehicle is connected to the Serial 1 port of the Cisco IR829 router through a third party adapter. A heavy duty vehicle interface adapter from Advantech B+B SmartWorx was used to validate this feature, and a reference to this device is provided in the third party components table. The Cisco IR829 runs a data collection and management agent for RuBAN in the IOx framework that queries the adapter through the serial port at a configured interval and collects the returned engine telematics data to forward to the RuBAN management system. This agent uses raw TCP socket communication with the serial port to enable efficient and reliable bi-directional communication with the vehicle interface. This method may be adapted to support integration with a wide range of sensor gateways and other equipment which communicate via serial interfaces.

The CAD/AVL VLU, if present, is assumed to have a 100Mbps Fast Ethernet interface, and is connected to a LAN switchport on the Cisco IR829 router for network connectivity. This port is configured as an access port, and should implement portfast functionality to minimize port negotiation time. This port is mapped to a VLAN interface for Layer 3 functionality and for service separation from other services. Panic button notification from the driver, whether provided by the CAD/AVL system or another onboard system, can be integrated into the onboard vehicle system in several different ways to accommodate a wide range of systems. The system has the ability to support network-based triggers via HTTP GET messages, serial port integration for trigger sensing with the Cisco IR829 router, or through the CANBUS integration. This provides effective integration between the onboard systems, video surveillance system, and the management system.

The Cisco IR829 router provides DHCP server functionality for all onboard systems on the vehicle which require it. The Cisco IR829 router also provides routing, gateway, and Network Address Translation (NAT) functions for all onboard systems, allowing multiple systems onboard to share a common WAN link for all communications.

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

All components are connected to the vehicle 12 Volt DC power system. The Cisco IR829 incorporates ignition sensing functionality, to determine when the vehicle engine is running and not running. The Cisco IR829 supports configurable start-up and shutdown timers, which provides flexibility for the onboard system operations. Assumes that power to the onboard networking infrastructure is maintained when the vehicle engine is turned off, the shutdown timer permits the onboard systems to maintain connectivity for a configurable period of time when the vehicle is parked after the ignition is turned off.

The design implemented to carry all service traffic over the Mobile SP-provided LTE service are detailed in the following section.

Offboard Wireless Connection System

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

- **LTE**-A contracted LTE service from a Mobile Service Provider is used for communication with the vehicle while the vehicle is in motion or otherwise located outside of the range of a maintenance yard or other fixed agency location. LTE is also used for providing wireless connectivity to a Connected Bus Stop if fiber or other wired connectivity is unavailable to that location. This is supported by the integrated LTE cellular modem in the Cisco IR829 router.

- **Wi-Fi-**When within the range of the maintenance yard or other facility for long-term parking of the vehicle, the vehicle uses a Wi-Fi bridge connection to the operator-owned Wi-Fi infrastructure at that facility. This is supported by the 5GHz radio of the integrated access point in the Cisco IR829 router.

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

LTE

The First Responder Fleet System uses LTE cellular connections to provide network connectivity to the vehicles when in motion, as illustrated in Figure 3. The design assumes these cellular services are provided by a Mobile Service Provider. At a minimum, this service must provide Layer 3 IP connectivity to the public Internet over which all services will be transported. Beyond basic IP connectivity, the following services and functions are desirable:

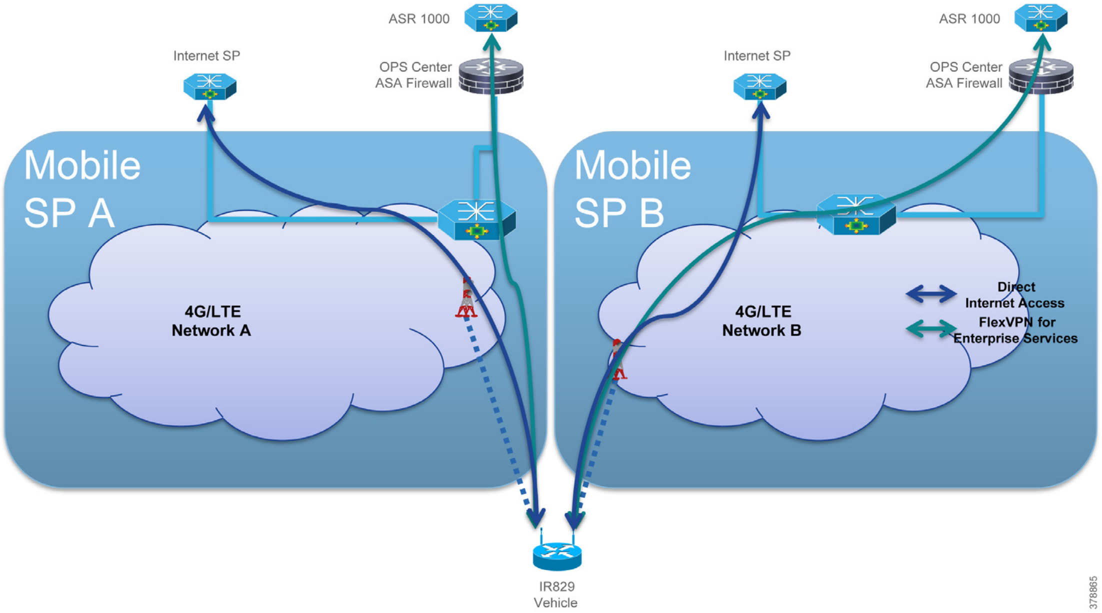
- **Internet Access**—The Mobile Service Provider should be able to route all passenger Internet service traffic directly to the Internet, which reduces the load on the First Responder Fleet operator's network.

- **Quality of Service**-The Mobile Service Provider should support at least three classes of service on the LTE cellular service to allow for proper treatment of voice and video services over more delay insensitive traffic of other services (as required by the first responder agency).

- **Direct Interconnect to Ops Center**-The Mobile Service Provider should support a direct connection to the first responder agency's data center, providing a direct path for service traffic from the Mobile Service Provider's network. This prevents service traffic from having to traverse the public Internet infrastructure, and better supports end-to-end QoS.

- **Private APN / VPN Service**-The Mobile Service Provider should offer a private APN service to the first responder agency in order to segregate that agency's traffic from other traffic traversing the mobile operator's network. For traffic transport from the mobile packet core to the agency's data center, a L3VPN should be used, which ensures separation and security of all service traffic between the vehicle systems and backend systems.

Figure 3 LTE Connectivity via Mobile SP



If all of these services and functions are available from the Mobile SP, then Layer 3 routing is sufficient to transport all service traffic between the vehicles and backend systems, and an overlay mechanism is not required. However, the first responder agency may still choose to deploy a VPN overlay network in order to simplify routing over the Mobile Operator's network. To accommodate this, the First Responder Fleet System implements a secured overlay VPN mechanism to enable the first responder agency to deploy a secure method of service transport over any level of Layer 3 service from the Mobile SP.

For this likely deployment scenario, the First Responder Fleet System design proposes the use of Cisco's Flex Virtual Private Networks (FlexVPN) for transport of enterprise service traffic between the vehicle infrastructure and the backend systems. FlexVPN, which has been widely deployed in many different Enterprise and IoT network systems, including Transportation systems, is a well-proven technology for fulfilling the transport and security requirements of this system design. FlexVPN provides a dynamic, secure VPN infrastructure over any network that provides simple IP routing between endpoints and a hub location. FlexVPN is capable of providing Layer 2 as well as Layer 3 service transport and can encrypt all traffic transported.

FlexVPN is an evolution of DMVPN, supporting IKE2 by default, and consolidating multiple configuration requirements into a single comprehensible set of commands. FlexVPN does not rely on Next Hop Routing Protocol (NHRP), which reduces management overhead traffic and thus cellular data utilization. More information on FlexVPN is available at Cisco FlexVPN at the following URL:

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

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

- LISP:
  - http://lisp.cisco.com/index.html

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

The onboard vehicle router implements the role of a FlexVPN spoke site and establishes the VPN session to a hub router in the first responder agency's central network. In the interest of efficient routing and optimal service traffic flow, only services that require connectivity to backend systems in the agency's network are transported over the VPN tunnel, such as voice, GPS data, vehicle telematics, on-demand video surveillance, and Criminal Justice Information System (CJIS) queries. Any service that just requires Internet access is routed directly to the Internet over the Mobile Service Provider’s network. This minimizes the bandwidth needed from the Mobile SP to the agency's network and the size of the Internet-facing nodes in the agency's network.

As each service and system on the vehicle is separated by VLANs with separate IP subnets on the LAN portion of the onboard network, a simple routing configuration on the onboard router handles which subnets, and thus which services, are transported by which means. All services are transported over the LTE WAN link(s) through NAT. The mechanisms used by the onboard gateway are covered in Routing and Network Address Translation (NAT), page 35.

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

It is highly desirable, and in some cases required, to have support for multiple LTE connections to a single vehicle. This may be due to coverage gaps from a single Mobile SP along parts of an agency's domain, or may be due to pricing advantages of using one Mobile SP over another at certain times of day. The mobile router in the First Responder Fleet System design, the Cisco IR829, comes in two models:

- **Cisco IR829 Dual LTE Modem Models**—This version has two LTE modems, each of which supports a single SIM card. Both LTE modems can be active simultaneously. Depending upon the agency's needs, the LTE connections can be treated as primary/secondary, or both can be treated equally and used simultaneously for increased bandwidth. The routing of traffic over the two LTE connections is managed in the router configuration on the Cisco IR829.

- **Cisco IR829 Single LTE Modem Models**—This version has a single LTE modem that supports two SIM. Since only one LTE modem exists, both Mobile SPs must support the same LTE connection and bands included in the LTE modem. Only one of the SIM cards is active at any time in the Cisco IR829 modem, and hand-off from one SIM card to the other requires 45-50 seconds for the connection to be reestablished because the Cisco IR829 has to reboot the LTE modem in order to switch SIMs.

Wi-Fi

The First Responder Fleet System uses a Wi-Fi connection to provide network connectivity to the vehicles when parked in a station or at another first responder agency facility that has an outdoor Wi-Fi network. The design assumes that the Wi-Fi infrastructure is owned and operated by the agency, providing secure, higher-bandwidth connectivity to the agency's centralized systems. This permits the agency to update the systems onboard the vehicles when not in use via bulk data transfer, and also to automatically upload log files and video surveillance files from the vehicles to long-term storage.

The mobile router on the vehicle has an integrated Wi-Fi access point, which supports 802.11n connections with 2x2 Multiple In, Multiple Out (MIMO) streams. The 2.4 GHz radio is dedicated to providing connectivity to wireless devices within and around the vehicle. The 5 GHz radio is dedicated to providing a WGB link to the Wi-Fi infrastructure in the maintenance yard. Using 40MHz channels on the 5 GHz radio with 2x2 MIMO should yield a throughput of 150-200 Mbps bidirectional for one vehicle connection to one infrastructure access point. Authorization of vehicle access to the Wi-Fi infrastructure, as well as encryption of data passing over the wireless connection, is accomplished via Wi-Fi Protected Access 2 (WPA2) implementation. The system design recommends implementing a certificate-based authorization system for Wi-Fi connections versus a pre-shared key (PSK) or preconfigured username and password, to ease deployment and to easily recover from compromised or leaked credentials. Since the Wi-Fi infrastructure and Metro Network infrastructure are owned and under the control of the first responder agency, no further end-to-end encryption of data is required. This will maximize the rate of data transferred to and from the vehicle.

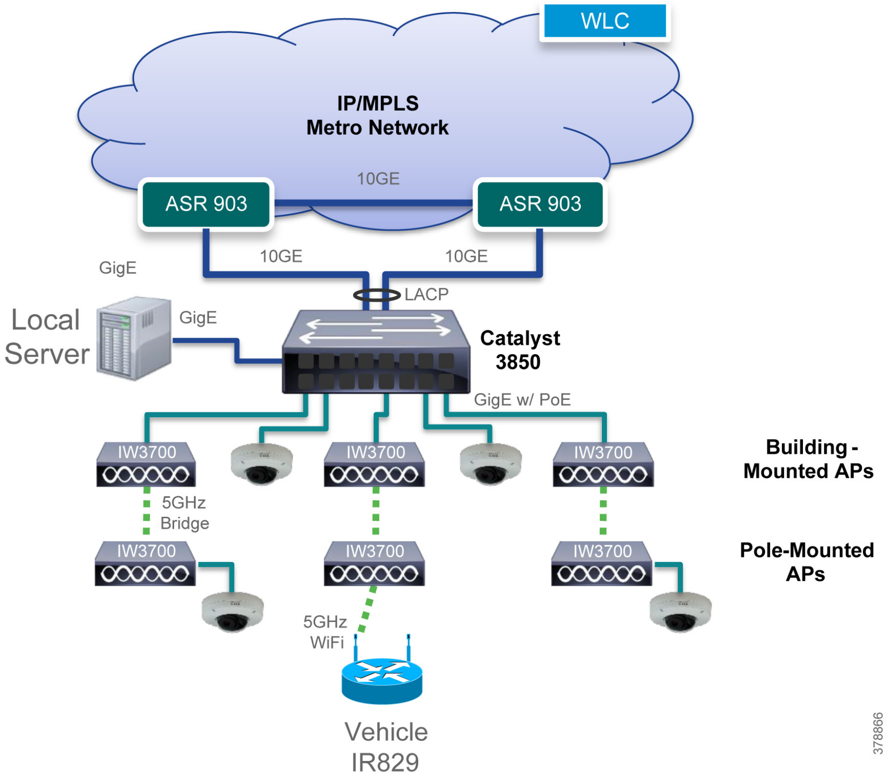
The Cisco IR829 onboard gateway monitors the status of the Wi-Fi connection and LTE connection(s) and manages use of each link through the dynamic Interior Gateway Protocol (IGP) utilized for routing decisions. By utilizing Enhanced Interior Gateway Routing Protocol (EIGRP) for routing management, reachability through each connection is actively monitored and service traffic is routed out the correct interface.

Station Wireless Network

The network in and around a station provides a scalable Wi-Fi infrastructure to deliver secure, high-bandwidth wireless connectivity to the vehicles parked at the station. The station network (shown in Figure 4) consists of the following components:

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

Figure 4 Station Network Overview



The IW3702 Access Points may be deployed with a variety of omni-directional or directional antennas, depending upon the station layout and coverage requirements. Each station 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, access points will be deployed on the sides or roof of the building(s) at the station in which resides the Ethernet switch for ease of wiring. If the area of the parking lot around the station buildings that require wireless coverage exceeds the effective range of these access points, additional access points are deployed on light standards or other pole structures throughout the parking area. If the station 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 has to be provided to the wirelessly-connected access points.

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

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

Under ideal conditions, the maximum wireless throughput over the 802.11n WGB from a single vehicle to a station access point can achieve approximately 200 Mbps of bidirectional throughput although 150 Mbps is more likely. As multiple vehicles connect to a single infrastructure access point, this bandwidth will be divided more or less equally among the vehicles, so 10 vehicles simultaneously accessing a single access point will each see approximately 15 Mbps. Looking at a large-case scenario, if a station had a total capacity of approximately 400 vehicles, that station deployment will need approximately 40 access points. This ratio of vehicles to access points will allow each vehicle to transfer approximately 2GB of information on average within a 30-minute window.

The worst-case scenario for station network scaling calculations is during a shift change at the station when many vehicles at the station may be powered up nearly simultaneously, while other vehicles arrive at the end of shift. The station network must be designed to accommodate this scenario.

The station 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 station, allowing access to both local systems and centralized data center systems. Local addressing of vehicles and other wireless endpoints is handled via DHCP functionality in the Catalyst 3850 switch in coordination with PNR.

IP cameras are needed to monitor and protect assets situated within the station area. For cameras positioned on the side of the station buildings 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 station locations that do not have a wired infrastructure, the IP camera can be connected to the local Ethernet port on an IW3702 access point. The IW3702 can supply PoE power to the IP camera and wireless transport of video traffic from the camera.

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

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

Metro Network

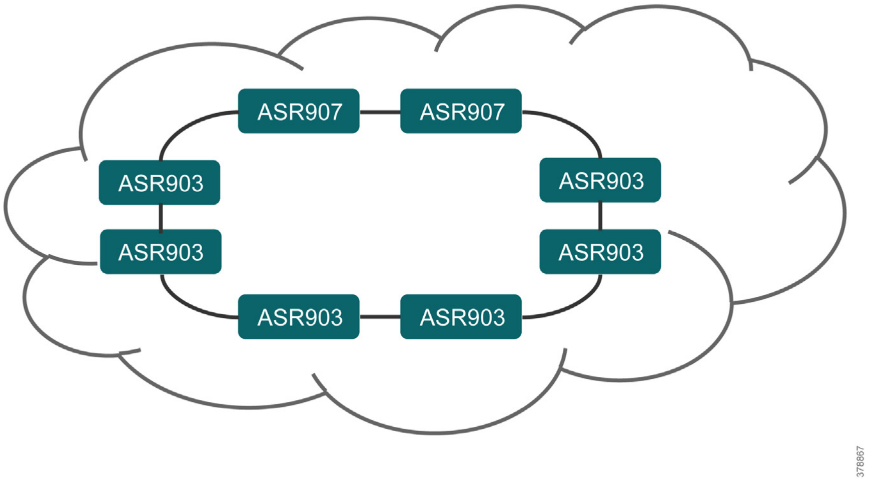
The Cisco First Responder Fleet System requires a highly scalable and resilient Metro Network infrastructure (shown in Figure 5) to facilitate service traffic transport from the distributed station networks to the Ops Center and backend systems across the first responder agency's geographic region. Cisco promotes a Unified MPLS design for this Metro Network, which easily satisfies all requirements for this network role. The Cisco Unified MPLS Transport network supports:

- Converged Architecture, a single network infrastructure that supports L3VPN services, L2VPN services, multicast services, and legacy transport with Circuit Emulation services.
- Hierarchical-QoS (H-QoS) to provide differentiated services per-hop behavior (PHB) treatment of traffic classes.
- Operations, Administrations, and Maintenance (OAM) for fault monitoring and correlation.
- Performance Management (PM) to track key Service Level Agreement (SLA) parameters such as packet-loss, packet delay, and delay variation.
- Easily deployable resiliency and high availability for both infrastructure and services with remote Loop-Free Alternate Fast Reroute (rLFA-FRR) and Border Gateway Protocol Fast Reroute (BGP FRR).

The Metro Network design used for the First Responder Fleet System is thoroughly documented in the Connected Roadways Design and Implementation Guide. A high-level overview (see Figure 5) of the design is included here for reference. The Backhaul Network design consists of the following components:

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

Figure 5 Metro Network Overview



The Unified MPLS model deployed for the Metro Network in the First Responder Fleet System implements Intermediate System to Intermediate System (IS-IS) as the Interior Gateway Protocol (IGP) in a single LAYER 1 area, with a flat LDP (Label Distribution Protocol) layer for MPLS LSP (Label Switched Path) transport. Note that if the customer is more familiar with deploying and implementing OSPF as an IGP, this is also supported for Unified MPLS networks. This network can scale up to thousands of network nodes and be deployed in both ring and hub-and-spoke topologies. The nodes in the network support Gigabit, 10 Gigabit (10GE), and even 100 Gigabit (100GE) Ethernet interfaces.

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

All service transport in the First Responder Fleet System is implemented with Layer 3 Virtual Private Networks (L3VPN). L3VPNs are deployed in the Unified MPLS design through use of Multiprotocol Border Gateway Protocol (MP-BGP) on the nodes at the edge of the Metro Network.

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

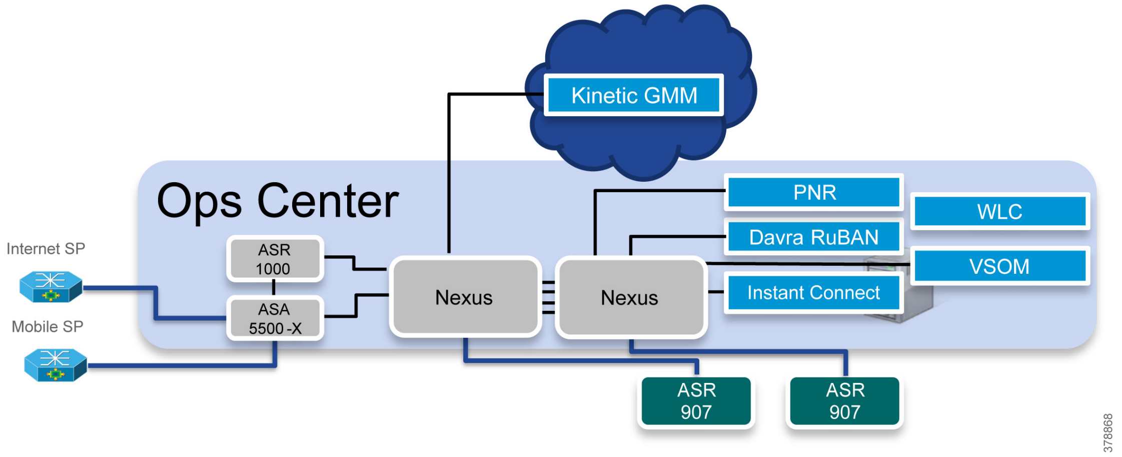
Operations Center Systems

The Operations Center in the Cisco First Responder Fleet System (shown in Figure 6) refers to the location, both logically and physically, where all centralized systems and infrastructure reside.

The following subsystems reside within the Operations Center:

- **Dispatch Center**-Location of the agency's operators and dispatchers. Incorporates management consoles for Cisco Kinetic Gateway Management Module, Davra RuBAN, and push-to-talk (PTT) voice systems through integration with Cisco Instant Connect. Cisco Instant Connect also provides compatibility with existing Land Mobile Radio Systems (LRMS).
- **Data Center**-Cisco Nexus Data Center switching and Unified Computing Systems (UCS) infrastructure for hosting all backend systems and storage for all enterprise services.
- **Internetwork Peering Gateway**-Provides connections to the Internet Service Provider and Mobile Service Provider(s) providing services to the first responder agency.

Figure 6 Operations Center Overview



First Responder agency operators in the Dispatch Center use the following systems and services:

- **Cisco Kinetic Gateway Management Module (GMM)**—A highly-scalable cloud-based gateway management platform from Cisco. Provides network element management services, including provisioning, software management, and monitoring of network functionality for the Cisco IR829 within the vehicles. Supported services include vehicle position tracking and tracking and correlation of cellular performance to vehicle location to aid in identifying LTE coverage issues.
- **RuBAN**-A comprehensive application enablement platform from Davra Networks providing vehicle telematics monitoring, driver behavior monitoring, and video surveillance integration.
- **PTT Voice**-Voice communications with drivers, which is managed by Cisco Instant Connect version 4.9.1.

The First Responder Fleet System design assumes a Data Center infrastructure is implemented in accordance with the best practices described in the Cisco Enterprise Data Center architecture. More information is available at Data Center and Virtualization at the following URL:

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

Additional infrastructure is required to facilitate the user-to-network (UNI) connections from service providers that provide contracted services to the first responder agency, namely Internet services and mobile connectivity to vehicles. The following components are utilized for these network connections:

- **Cisco ASA 5500-X Firewall**-Provides high-bandwidth gateway, firewall, and intrusion prevention services for internetwork connections up to ten Gigabit Ethernet.
- **Cisco ASR 1000 Router**-Provides hub router functionality for terminating FlexVPN tunnels originating from vehicle onboard routers over the Mobile SP provided services.

Gateway Management System

The Cisco First Responder Fleet System design uses the following platforms for management of the onboard vehicle infrastructure and secure data transport:

- **Cisco Kinetic Gateway Management Module (GMM)**—A comprehensive cloud-hosted management platform for the IR829 gateway.
- **Davra Networks RuBAN Application Enablement Platform (AEP)**—A platform enabling vehicle and driver telematics collection and analysis.

Cisco Kinetic Gateway Management Module

The Cisco Kinetic GMM is a comprehensive cloud-hosted management platform for the Cisco IR829 gateway. Kinetic GMM provides software version management and upgrades, gateway configuration and security management, and WAN and VPN interface provisioning. It also provides Global Positioning System (GPS) location tracking, and cellular health data tracking and correlation with location information for mobile service troubleshooting and improvement.

The Cisco GMM Deployment Guide is available on DevNet at the following URL:

- https://developer.cisco.com/docs/kinetic/ - gmm-deployment-guide

Initial Configuration of GMM

In order to use GMM, the gateway must be configured for the Cisco Kinetic cloud. Two ways exist to obtain a Cisco Kinetic managed gateway:

- When ordering the gateway, specify that the gateway is *cloud managed*.
- If a non-Cisco Kinetic gateway exists, that gateway can be converted to be a Kinetic managed gateway using the Gateway Provisioning Tool (GPT). Instruction and the tool is available at the following URL:
  - https://developer.cisco.com/site/dataconnect/docs/index.gsp#provision-a-gateway

The gateway must also be entitled to use Cisco Kinetic. This is done automatically when the gateway is ordered as cloud managed. For converted gateways, they must be entitled by sending a support request to Cisco Kinetic. Support can be contacted on the upper right-hand corner of the console.

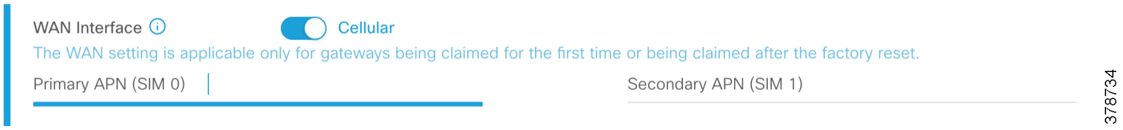
Gateways can be configured on a device by device basis. However, a template can be created if multiple devices require the same configuration. A template cannot be imported, and must be created in the GMM portal. The template consists of:

- WAN interface specification
- LAN port status
- Wi-Fi configuration for the end user
- Private subnet configuration for the Wi-Fi users
- Site-to-Site VPN configuration
- GPS status
- In order to create a template, select **Gateway** > **Templates**

WAN Interface

The WAN Interface configuration (shown in Figure 7 is only used in the Initialization process of the gateway. This is done the first time the gateway is claimed from the out of box state and is ignored in subsequent claims of the gateway. The secondary APN is only used for the Dual LTE IR829 (PID IR829-2LTE-EA-xK9).

Figure 7 WAN Interface Configuration



WAN Interface ⓘ Cellular

The WAN setting is applicable only for gateways being claimed for the first time or being claimed after the factory reset.

Primary APN (SIM 0)

Secondary APN (SIM 1)

If using the cellular interface as the uplink, select the cellular antenna that will give the best signal and connection as the primary APN.

LAN Ports

The LAN Ports configuration (shown in Figure 8) allows the gateway's Gigabit Ethernet ports to be enabled or disabled. While enabled, clients may connect via an Ethernet cable to the Gigabit Ethernet ports on the gateway. If the clients are configured for DHCP, they will receive a network configuration, as defined in **Private Subnet**. While disabled, the ports are shut down to avoid unauthorized access. Authentication protocols such as 802.1x will not be extended to the LAN ports by GMM.

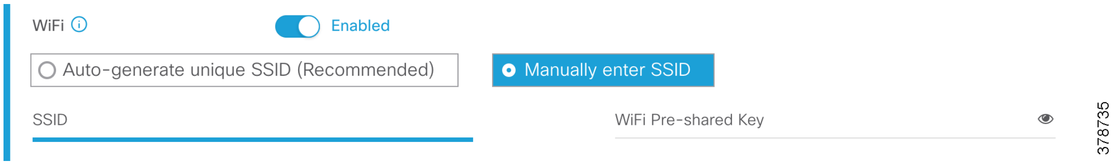
Figure 8 LAN Ports Configuration

LAN Ports ⓘ Enabled

Wi-Fi

The Wi-Fi feature (shown in Figure 9) configures the gateway to provide a Wi-Fi hotspot for local wireless devices. The Wi-Fi network is bridged to the same network as the subtended network of the LAN ports.

Figure 9 WiFi Configuration



WiFi ⓘ Enabled

○ Auto-generate unique SSID (Recommended)

● Manually enter SSID

SSID

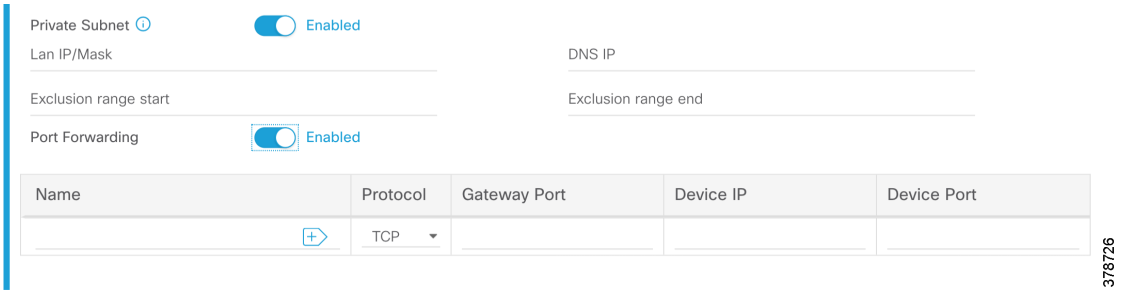
WiFi Pre-shared Key

Once a DHCP client joins this network, they will receive an IP address in the range configured in **Private Subnet**.

Private Subnet

If the Private Subnet feature (shown in Figure 10) is enabled, the user wireless network can be custom configured. In this case, the gateway will provide the DHCP service to subtended devices using the network specified in the **LAN IP/Mask** field. The LAN IP entered will be the default gateway for connected devices. The DNS IP will point to the DNS server for the DHCP clients on the subtended network.

Figure 10 Private Subnet Configuration



Private Subnet ⓘ Enabled

Lan IP/Mask

DNS IP

Exclusion range start

Exclusion range end

Port Forwarding Enabled

Name	Protocol	Gateway Port	Device IP	Device Port
	TCP			

Currently only one DNS server IP address can be configured and the **Exclusion Range** must be contiguous.

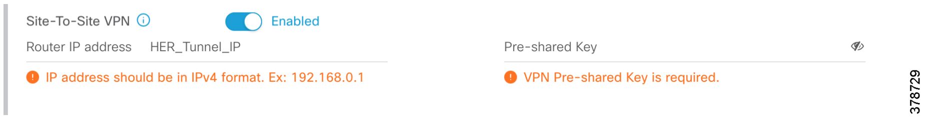
If the Private Subnet feature is disabled, then the wireless network will be given the following default configuration:

- A /28 subnet in the 10.8.0.0/16 network range
- The default router for the network will be the IP address of the gateway.
- The DNS server will be the DNS server provided to the gateway from the uplink interface.

Site-To-Site VPN

The **VPN** feature (shown in Figure 11) configures site-to-site VPN for encrypted connectivity from the gateway to the Head End Router (HER) at the corporate network or data center, using FlexVPN. In this scenario, the management traffic for Kinetic will be isolated from the user bearer traffic to the corporate network.

Figure 11 Site-to-Site VPN Configuration



Site-To-Site VPN ⓘ Enabled

Router IP address HER_Tunnel_IP

Pre-shared Key

IP address should be in IPv4 format. Ex: 192.168.0.1

VPN Pre-shared Key is required.

GPS

The GPS feature (shown in Figure 12) is used to configure the gateway to send GPS data to Cisco Kinetic in order to allow tracking of the gateway on the **Dashboard** map. For the GPS feature to work, ensure that the GPS antenna is connected and that a direct line of sight exists from the antenna to the GPS satellite.

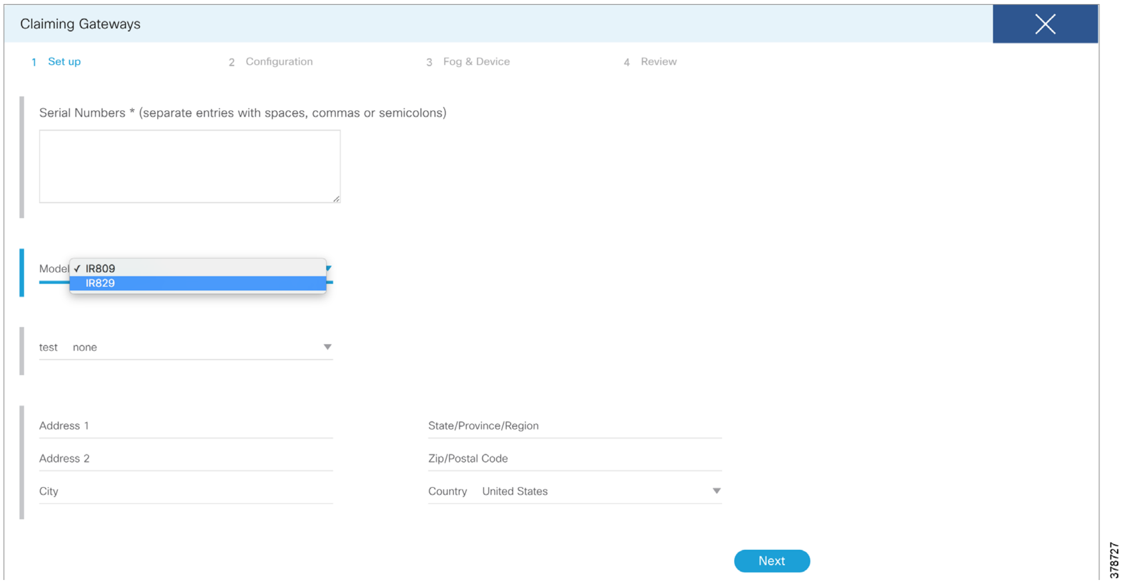
Figure 12 Site-to-Site VPN Configuration

GPS ⓘ Enabled

Claiming the Gateway

The gateway can be claimed in the GMM portal in the **Gateways** section. During this process, the serial number and model of the gateway must be provided (Figure 13) and the template selected (Figure 14). Once this is finished, GMM will start listening for the gateway.

Figure 13 Serial Number and Model Specification



Claiming Gateways

1 Set up 2 Configuration 3 Fog & Device 4 Review

Serial Numbers * (separate entries with spaces, commas or semicolons)

Model ✓ IR809
IR829

test none

Address 1

Address 2

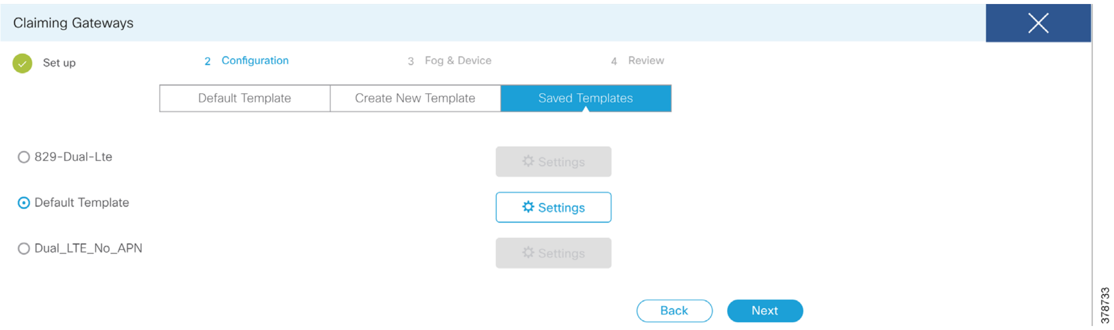
City

State/Province/Region

Zip/Postal Code

Country United States

Figure 14 Template Selection



Claiming Gateways

Set up 2 Configuration 3 Fog & Device 4 Review

Default Template | Create New Template | Saved Templates

○ 829-Dual-Lte

● Default Template

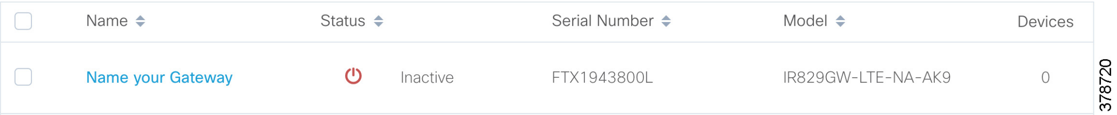
○ Dual_LTE_No_APN

Deploying a Gateway

Once the gateway is powered on and Internet connectivity is established, the provisioning process will start. The process can be followed in the GMM portal.

The call-home script on the gateway runs every two minutes, so the status may show **Inactive** for a period of time, before changing to **In Progress** (Figure 15).

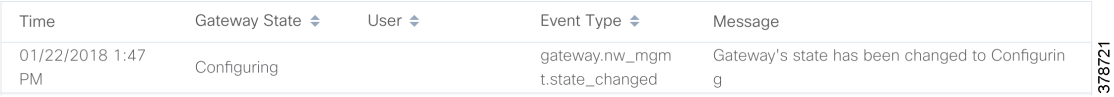
Figure 15 Gateway Inactive



□	Name	Status	Serial Number	Model	Devices
□	Name your Gateway	Inactive	FTX1943800L	IR829GW-LTE-NA-AK9	0

The first stage of the claiming process involves setting up the management FlexVPN tunnel between the gateway and GMM. Once this is successful, the event log will display a message stating that the state has been changed to **Configuring** (Figure 16).

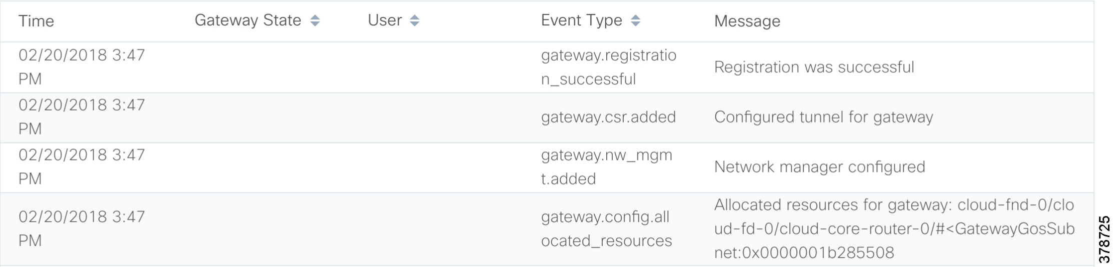
Figure 16 Gateway State Changed to Configuring



Time	Gateway State	User	Event Type	Message
01/22/2018 1:47 PM	Configuring		gateway.nw_mgmt.state_changed	Gateway's state has been changed to Configuring

Once the management tunnel has been successfully configured, the event logs will display messages for successful registration, successful resource allocation, and successful configuration of the tunnel. GMM will now start applying additional universal configuration to the gateway (Figure 17).

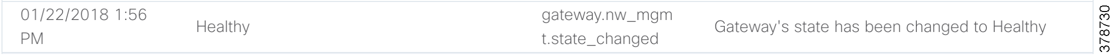
Figure 17 Management Tunnel Successfully Configured



Time	Gateway State	User	Event Type	Message
02/20/2018 3:47 PM			gateway.registration_successful	Registration was successful
02/20/2018 3:47 PM			gateway.csr.added	Configured tunnel for gateway
02/20/2018 3:47 PM			gateway.nw_mgmt.added	Network manager configured
02/20/2018 3:47 PM			gateway.config.allocated_resources	Allocated resources for gateway: cloud-fnd-0/cloud-fd-0/cloud-core-router-0/#<GatewayGosSubnet:0x0000001b285508

As soon as the universal configuration has been successfully added to the gateway, the event log will state that the gateway's state has been changed to **Healthy** (Figure 18).

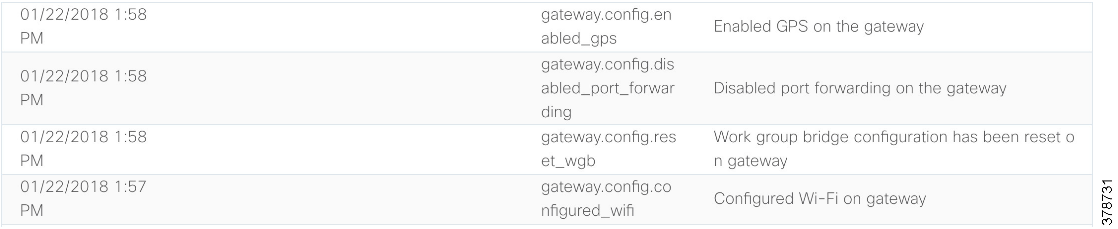
Figure 18 State Changed to Healthy



01/22/2018 1:56 PM	Healthy	gateway.nw_mgmt.state_changed	Gateway's state has been changed to Healthy

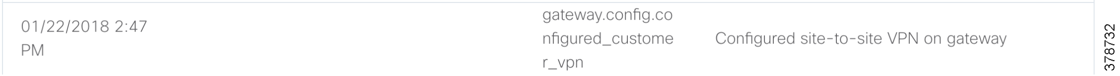
Even though the gateway now appears as **Healthy**, the configuration is not yet finished. It is at this point that GMM starts applying the template configuration. The configuration process is officially finished once all of the relevant configuration from the template can be accounted for in the event logs (Figure 19 and Figure 20).

Figure 19 Template Configuration Applied 1



01/22/2018 1:58 PM	gateway.config.enabled_gps	Enabled GPS on the gateway
01/22/2018 1:58 PM	gateway.config.disabled_port_forwarding	Disabled port forwarding on the gateway
01/22/2018 1:58 PM	gateway.config.reset_wgb	Work group bridge configuration has been reset on gateway
01/22/2018 1:57 PM	gateway.config.configured_wifi	Configured Wi-Fi on gateway

Figure 20 Template Configuration Applied 2

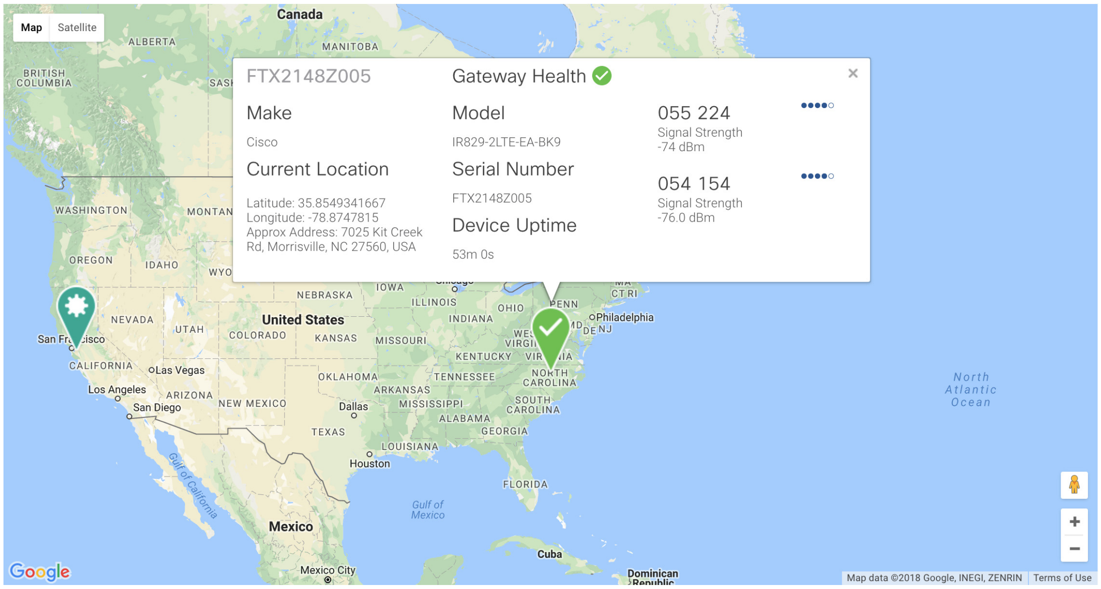


01/22/2018 2:47 PM	gateway.config.configured_customer_vpn	Configured site-to-site VPN on gateway

Monitoring a Gateway

If GPS was enabled in the template, then the gateway will appear on the map in the main page of the GMM portal (Figure 21). In addition, device information such as model, serial number, device up time, and signal strength will display. This information will be updated every thirty seconds by the gateway.

Figure 21 GPS Display in GMM



FTX2148Z005

Gateway Health ✓

Make

Cisco

Model

IR829-2LTE-EA-BK9

055 224

Signal Strength

-74 dBm

Current Location

Latitude: 35.8549341667
Longitude: -78.8747815
Approx Address: 7025 Kit Creek Rd, Morrisville, NC 27560, USA

Serial Number

FTX2148Z005

054 154

Signal Strength

-76.0 dBm

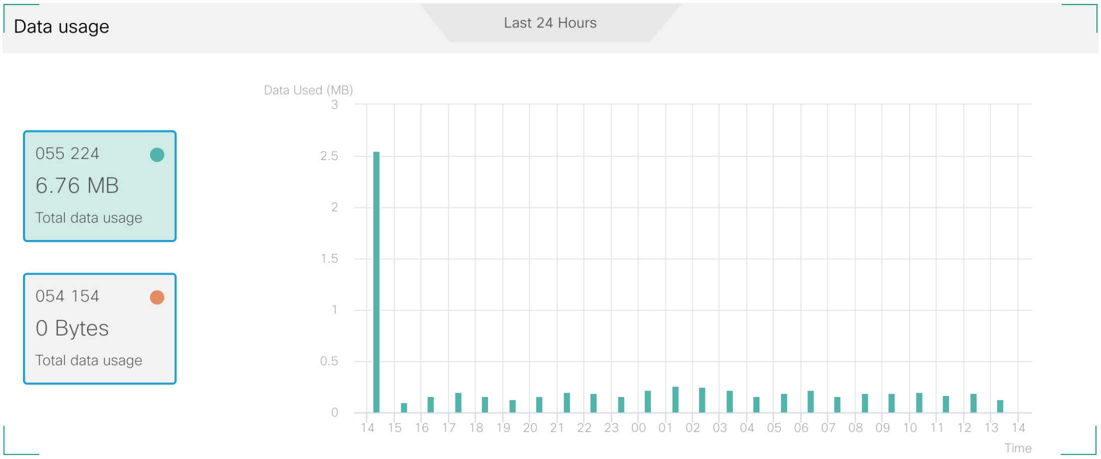
Device Uptime

53m 0s

378723

The graphical display of the data usage (Figure 22) or signal strength of the SIM cards (Figure 23) can be seen under the **Monitor** tab specific to the gateway.

Figure 22 Data Usage



Data usage

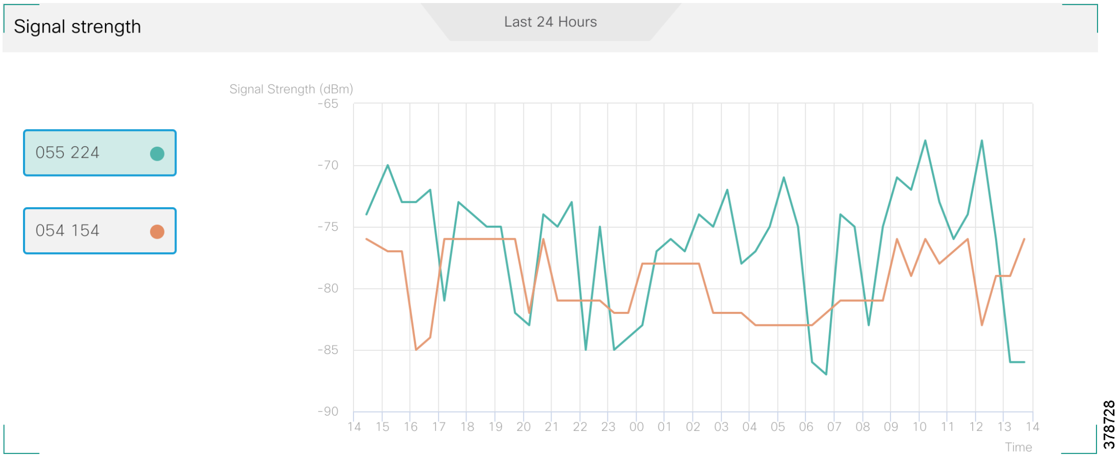
Last 24 Hours

055 224 ●
6.76 MB
Total data usage

054 154 ●
0 Bytes
Total data usage

378719

Figure 23 Signal Strength



Troubleshooting

The current troubleshooting tools are limited, but the following features will be made available in upcoming releases:

- Gateway console access:
  - When the gateway is in the Out-of-Box or Unclaimed state, the console can be accessed for troubleshooting. The default login is operator/operator. This password will be configurable from the cloud.
- A set of commands will be made available via a menu:
  - Show ip route
  - Show crypto
  - Show version
  - Show cellular/gps
  - Show interface
  - Show ip route
  - Show cryto
  - Show arp
  - Show logs
  - Ping
  - Traceroute
  - Reboot GW

Davra RuBAN

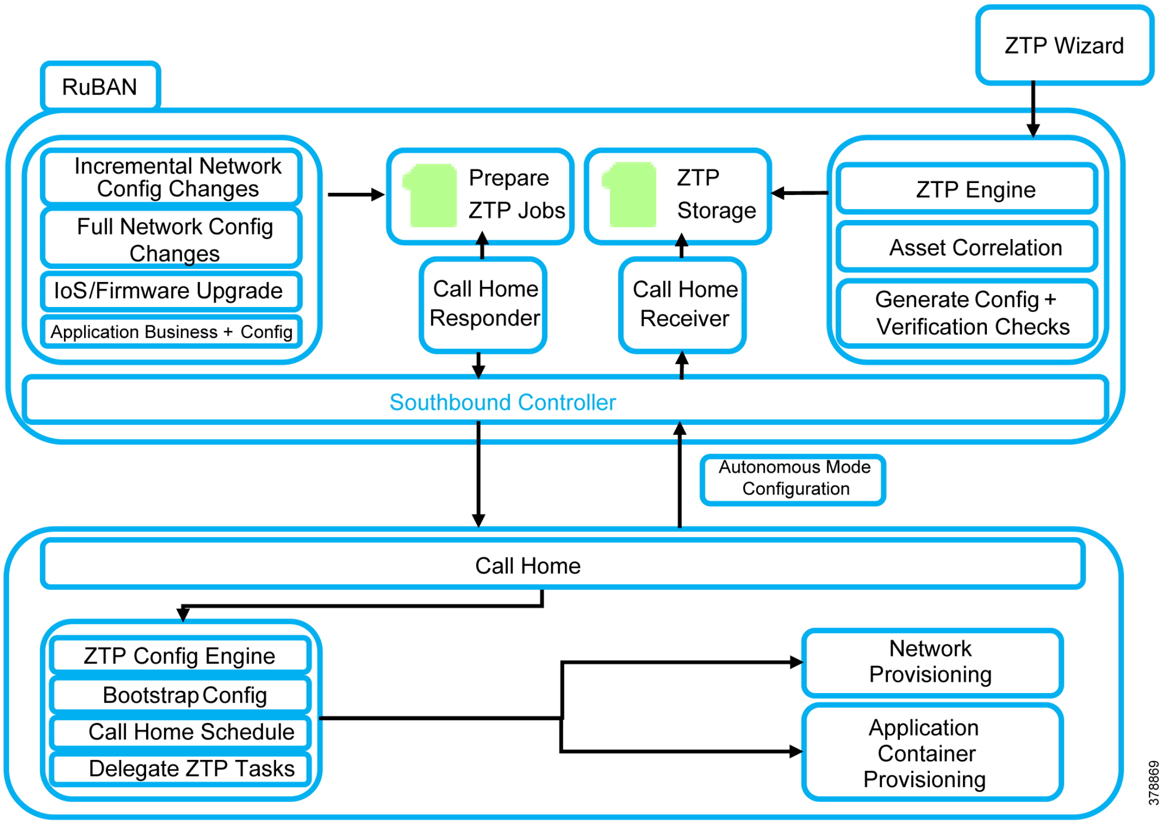
Given the transportation-specific aspects of the First Responder Fleet System scope, the number of third party systems involved, and the targeted customers, a transportation-specific Application Enablement Platform (AEP) is warranted. Cisco is partnering with Davra Networks to integrate the RuBAN IoT AEP system into the First Responder Fleet System. RuBAN provides a transportation-focused AEP that supports many services needed by first responder agencies. See the following URL:

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

RuBAN provides integrated application enablement for the First Responder Fleet System, including initial provisioning for field deployment of new services as well as **Day 2** management and monitoring. The RuBAN platform is capable of communicating with the devices under management via IPv4 and IPv6, which provides comprehensive coverage of the elements deployed in the First Responder Fleet System design.

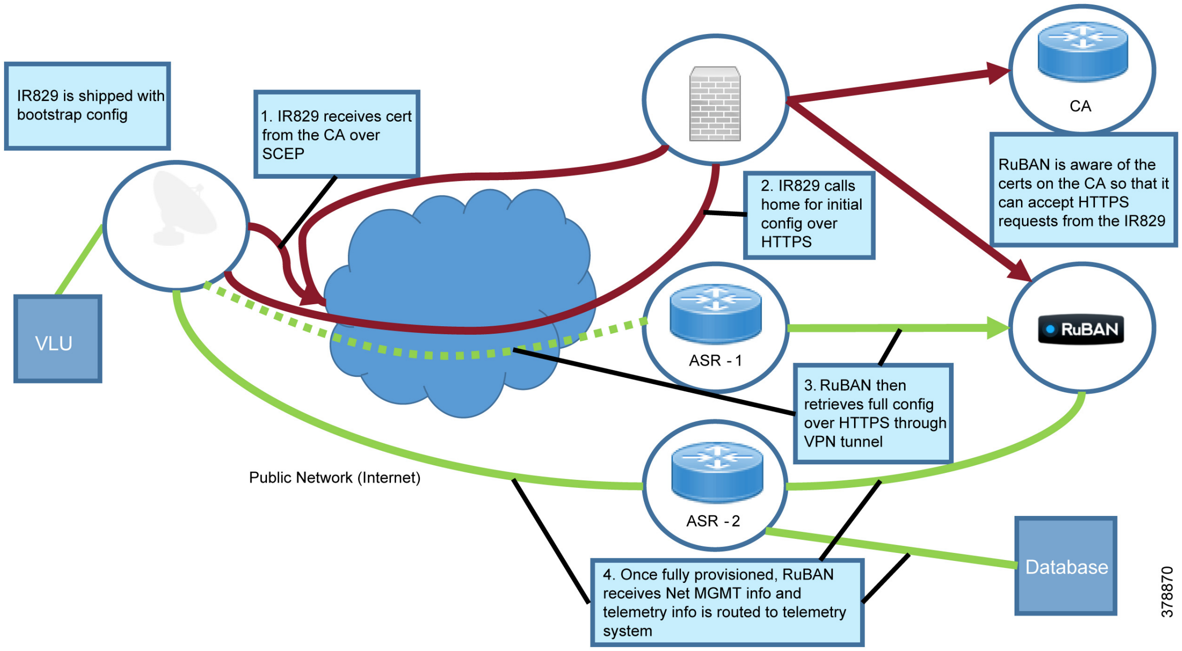
Figure 24 provides an overview of the southbound interface between the RuBAN system and the Cisco devices deployed in the network.

Figure 24 RuBAN Southbound Interface Overview



The RuBAN AEP communication with the Cisco IR829 is enabled through a software agent that runs on the Cisco IR829 IOx Guest OS. The required initial configuration for Cisco devices is loaded as part of a ConfigExpress configuration that is specified when ordering the devices. This initial configuration will enable the Cisco device to *call-home* to the RuBAN system, which provides a connection for system enablement. A workflow overview is shown in Figure 25.

Figure 25 RuBAN Service Management Deployment Workflow


IR829 is shipped with bootstrap config
1. IR829 receives cert from the CA over SCEP
CA
RuBAN is aware of the certs on the CA so that it can accept HTTPS requests from the IR829
2. IR829 calls home for initial config over HTTPS
VLU
ASR - 1
RuBAN
3. RuBAN then retrieves full config over HTTPS through VPN tunnel
Public Network (Internet)
ASR - 2
Database
4. Once fully provisioned, RuBAN receives Net MGMT info and telemetry info is routed to telemetry system
378870

1. The Cisco device (the Cisco IR829 router in the illustration) obtains a certificate from the Certificate Authority (CA) server via Simple Certificate Enrollment Protocol (SCEP). RuBAN is aware of retrieved certificates, so it can accept HTTPS connections from the Cisco devices.
2. The Cisco device *calls home* to the RuBAN system to download the initial service configuration via HTTPS
3. Once downloaded, RuBAN then downloads the remainder of the full configuration to the Cisco device over HTTPS through either the Management Network or VPN tunnel.
4. When fully provisioned, the RuBAN system receives monitoring information and alerts from the Cisco devices. Telemetry info is routed to the Vehicle Database system.

The RuBAN platform provides real-time monitoring of service traffic and alerts. In addition, the RuBAN platform integrates with the Cisco Kinetic GMM to obtain geolocation information so that the precise location of vehicles and other mobile components is available in real-time.

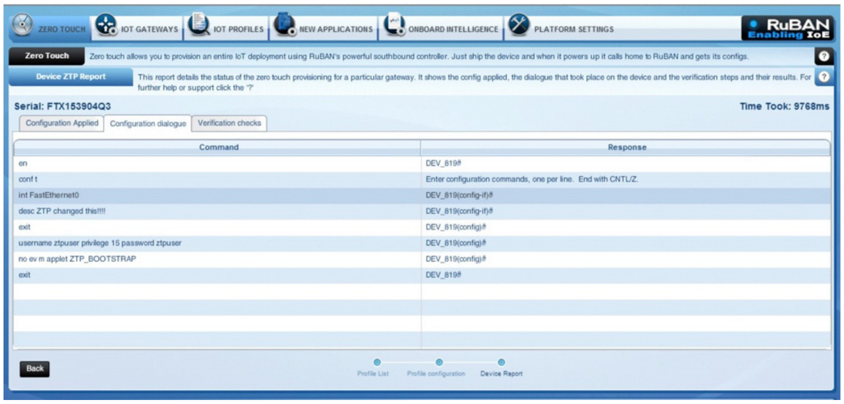
Management User Interface

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

Provisioning

The Provisioning Interface (shown in Figure 26) covers infrastructure and service provisioning and monitoring functions for equipment deployed on the vehicles.

Figure 26 Provisioning Interface



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

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

Serial: FTX153904Q3

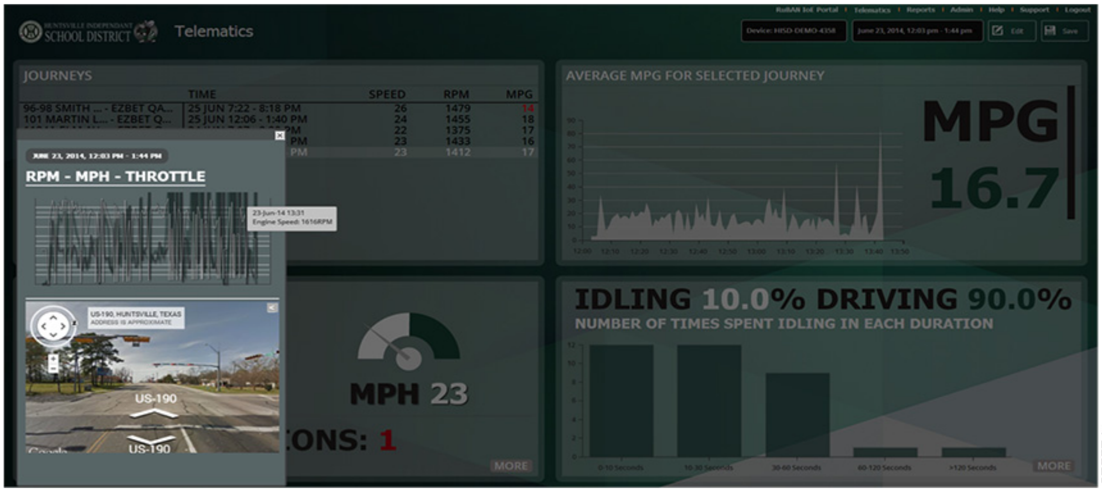
Time Took: 9768ms

Command	Response
en	DEV_819#
conf t	Enter configuration commands, one per line. End with CNTL/Z.
int FastEthernet0	DEV_819(config-if)#
desc ZTP changed this!!!!	DEV_819(config-if)#
exit	DEV_819(config)#
username ztpuser privilege 15 password ztpuser	DEV_819(config)#
no ev m applet ZTP_BOOTSTRAP	DEV_819(config)#
exit	DEV_819#

Vehicle Management

The Vehicle Management Interface (shown in Figure 27) gives the operators more specific information on a particular vehicle and actions that can be taken for that vehicle. The information and actions can be customized to the specific requirements of the First Responder Fleet operator.

Figure 27 Vehicle Management Interface

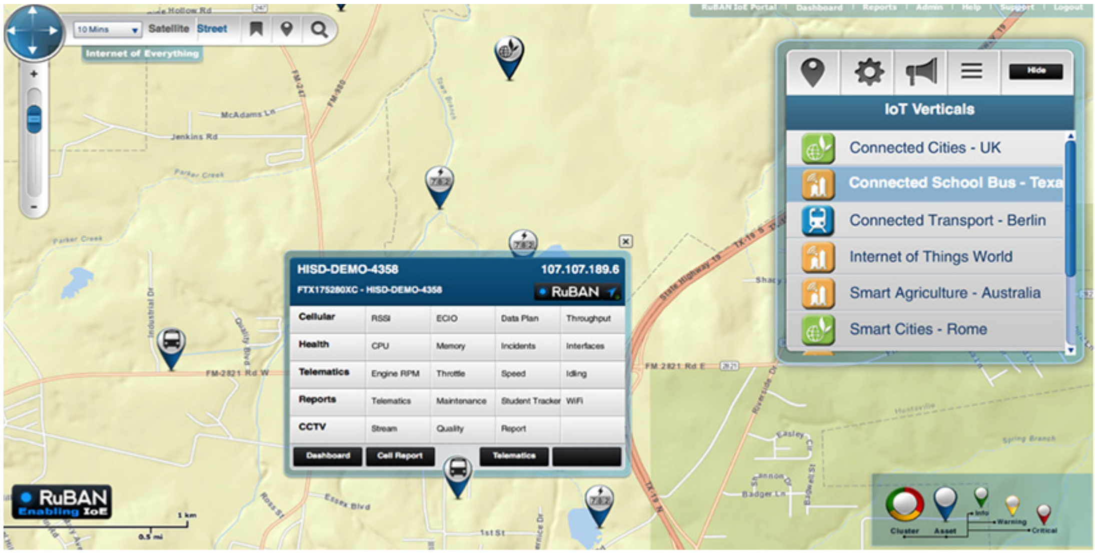


	TIME	SPEED	RPM	MPG
96-98 SMITH ... - EZBET QA...	25 JUN 7:22 - 8:18 PM	26	1479	14
101 MARTIN L... - EZBET Q...	25 JUN 12:06 - 1:40 PM	24	1455	18
	PM	22	1375	17
	PM	23	1433	16
	PM	23	1412	17

Driver Management

The Driver Management Dashboard interface (shown in Figure 28) provides data to the operator that depicts how the driver of a specific vehicle is performing, such as speed hysterics, acceleration and braking data, fuel efficiency, and time spent driving versus idling. Again, this dashboard can be customized to display whatever data the First Responder Fleet operator requires.

Figure 28 Driver Management Dashboard Interface



HISD-DEMO-4358 107.107.189.6

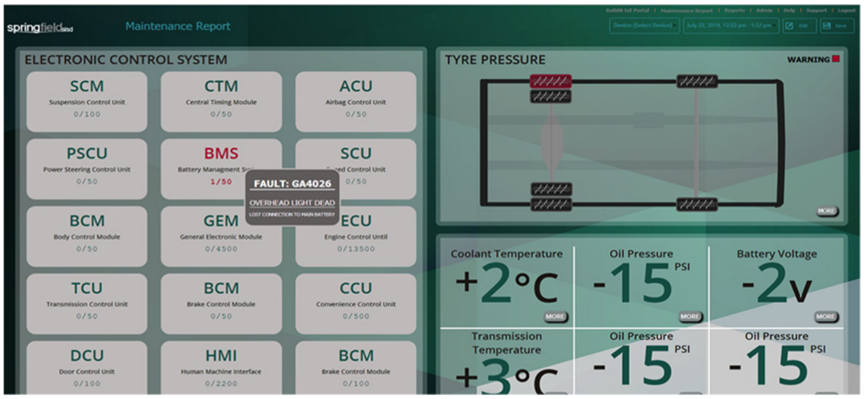
FTX175280XC - HISD-DEMO-4358 RuBAN

Cellular	RSSI	ECIO	Data Plan	Throughput
Health	CPU	Memory	Incidents	Interfaces
Telematics	Engine RPM	Throttle	Speed	Idling
Reports	Telematics	Maintenance	Student Tracker	WiFi
CCTV	Stream	Quality	Report	

Vehicle Telematics

The Vehicle Telematics Dashboard interface (shown in Figure 29) provides a real-time display of the sensor data available from a vehicle. The data displayed can be customized to the First Responder Fleet operator's particular requirements. It also alerts the operator to any potential performance or safety issues with a vehicle, such as low tire pressure, low oil pressure, or high engine temperature.

Figure 29 Vehicle Telematics Dashboard Interface



springfield
Maintenance Report
ELECTRONIC CONTROL SYSTEM
SCM Suspension Control Unit 0/100
CTM Central Timing Module 0/50
ACU Airbag Control Unit 0/50
PSCU Power Steering Control Unit 0/50
BMS Battery Managment S 1/50
SCU Control Unit 0/50
FAULT: GA4026
OVERHEAD LIGHT DEAD
LOST CONNECTION TO MAIN BATTERY
BCM Body Control Module 0/50
GEM General Electronic Module 0/4500
ECU Engine Control Until 0/13500
TCU Transmission Control Unit 0/50
BCM Brake Control Module 0/50
CCU Convenience Control Unit 0/500
DCU Door Control Unit 0/100
HMI Human Machine Interface 0/2200
BCM Brake Control Module 0/100
TYRE PRESSURE
WARNING
MORE
Coolant Temperature +2°C
Oil Pressure -15 PSI
Battery Voltage -2v
Transmission Temperature +3°C
Oil Pressure -15 PSI
Oil Pressure -15 PSI
375580

Supported Services and Models

This section includes the following major topics:

Service Inventory / Models

Models that need to be included:

- Dual LTE support for WAN connectivity while vehicle is in service - covered in System Architecture, page 2
- Wi-Fi WAN connectivity while vehicle is parked within range of agency Wi-Fi coverage
- Extension of Enterprise Wi-Fi Network services to devices in and around the vehicle
- Vehicle Location and Telemetry Data Collection and Correlation
- Vehicle Two way Voice Communication (Push to Talk Radio over IP)
- Dash / Passenger Video Surveillance
- License Plate Recognition
- Fleet Management
- High Value Asset Tracking

Table 2 lists the services supported in this phase of the First Responder Fleet System design.

Table 2 Services Supported by First Responder Fleet System

Service Category	Service Definition
Wi-Fi Network Services	■ Provides extension of Enterprise Wi-Fi Network services to First Responder personnel and devices both in and around the vehicle.
Vehicle Location Tracking	■ Relays vehicle location information to Cisco Kinetic GMM system in real-time. ■ Vehicle location determined by Global Navigation Satellite System (GNSS) integration, such as GPS or GLOSSNAS with the vehicle onboard infrastructure.
Vehicle Telemetry Data Collection	■ Relays real-time vehicle performance information, such as Speed, RPM and Idle Time from vehicle CANBUS to Davra RuBAN Management system. ■ Provides ongoing monitoring of vehicle operation, and provides information on predictive maintenance to be performed before service-affecting issues are encountered.
Vehicle Location Data Correlation	■ Correlates other service performance information with vehicle location such as RSSI and Speed. ■ Provides historical data for understanding cellular coverage along the vehicle route, driver behavior, road congestion at certain locations. ■ Can be used for the First Responder Fleet operator to optimize the bus route and scheduling and to plan for crew shift schedules.
Vehicle Video Surveillance	■ Onboard vehicle systems to multiple IP video surveillance cameras. ■ Video recordings are stored to an onboard ruggedized server or, if no onboard server is deployed, to integrated flash storage in the cameras. ■ Supports on-demand real-time video transmission over cellular backhaul. ■ Recorded video is offloaded via Wi-Fi to long-term storage for later retrieval when vehicle is parked in yard.
Fleet Management Services	■ The Cisco Kinetic GMM is a cloud-based system that provides comprehensive vehicle gateway management, including provisioning, secure remote access, Wi-Fi management, GPS information and tracking, and cellular health tracking. ■ The RuBAN system from Davra networks provides a comprehensive application enablement platform (AEP) for vehicle fleet operations that integrates essential functions for managing a vehicle fleet: Vehicle telemetry data collection, driver behavior tracking, asset provisioning and monitoring, vehicle dashboard reports, policy-triggered events, and video surveillance integration.
Wireless Bulk Data Transfer	■ When parked within range of a Station Wireless Network, the vehicle establishes a high-bandwidth network connection via Wi-Fi to the infrastructure at the station. ■ This link facilitates the ability to offload route logs, video files, and other pertinent information from the vehicle, and to update the vehicle onboard systems. ■ This include software updates for vehicle onboard systems, offloading of log files, and onboard video offload to agency data centers.

Table 2 Services Supported by First Responder Fleet System (continued)

Service Category	Service Definition
High Value Asset Tracking	■ Tracks high value assets carried onboard the vehicle. ■ Warns the vehicle driver if any tracked asset is not onboard when returning from an incident response.
License Plate Recognition	■ Automatic tracking of vehicle license plates within view of the vehicle video surveillance camera. ■ Alerts law enforcement officer of any issues with a recognized license plate.
Vehicle Two-way Voice Communications	■ Two-way voice communications with Push To Talk (PTT) support between first responders, supervisors, and dispatchers at operation centers. ■ Enables interworking between voice over IP (VoIP) systems and Land Mobile Radio Systems (LMRS) through Cisco Instant Connect integration.

Wi-Fi Network Services

The First Responder Fleet System provides an integrated Wi-Fi access point infrastructure, providing wireless networking services for passengers and essential systems for the First Responder Fleet operator and Emergency Services. The following services are supported via Wi-Fi connectivity:

- Enterprise infrastructure access for first responders in and around the vehicle
- Wireless PTT endpoints

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

For each service, 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 agency's and end point's requirements. All traffic for these services is transported via a secured infrastructure over the cellular backhaul connection(s), which is implemented via a FlexVPN tunnel established between the onboard network and the back office infrastructure.

Each Wi-Fi SSID is mapped to a separate VLAN in the onboard network infrastructure, providing the required service traffic separation required by the agency's requirements.

Vehicle Location Tracking

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

Vehicle location is determined by GNSS integration with the vehicle onboard infrastructure, supporting such systems as GPS and GLOSSNAS. The onboard system reports position information to the Kinetic GMM system at a configurable interval, such as every five seconds, depending upon the location resolution required by the agency. This information can also be sent to Davra if desired. The vehicle onboard infrastructure that is implemented in the first responder fleet system provides the following location, altitude, and velocity tracking accuracy:

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

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

Vehicle Location Data Correlated with LTE Performance

The First Responder Fleet System provides correlation of LTE cellular connection performance data to vehicle location data within the Kinetic GMM system. This permits the first responder agency to track LTE connection performance across the geographic region it serves, allowing the agency to easily pinpoint and report coverage issues to the Mobile Service Provider.

Data tracked includes:

- dBm

Vehicle Telemetry Data Collection

The vehicle onboard infrastructure also integrates with the vehicle CANBUS to collect real-time vehicle performance information such as Speed, RPM, and Idle Time. This data collection enables ongoing monitoring of the vehicle operation, and provides information on predictive maintenance to be performed before service affecting issues are encountered. Similar to the vehicle location data collection, vehicle performance data is collected at a configurable polling interval and transmitted to the RuBAN AEP system supplied by Davra Networks. The vehicle onboard infrastructure uses a SAE J1939-compatible Heavy Duty Vehicle adapter to communicate with the CANBUS.

Vehicle Video Surveillance

Widely used vendors in first responder fleets include:

- **Panasonic Arbitrator**: http://business.panasonic.com/arbitrator/evidence-collection-systems.html
  - Supports up to 5 cameras.
- **WatchGuard**: https://watchguardvideo.com/
- **Axon**: https://www.axon.com/solutions/law-enforcement
- **Getac**: http://us.getac.com/solutions/video/video.html

Video surveillance for first responder agencies is an essential service for ensuring the safety and security of first responders and the public they serve. The Cisco First Responder Fleet System integrates with popular first responder agency video surveillance systems, ensuring complete coverage of all assets and personnel within and around vehicles.

The video surveillance systems can support one or more cameras on a vehicle, depending upon the agency's requirements. The following components are typically deployed on the vehicle:

- A ruggedized server to server as a DVR and control system.
- One or more High-Definition High Dynamic Range (HDR) video cameras. Typical locations and angles are front view, side view, and for law enforcement deployments, a rear seat view.
- Specific to law enforcement, on-body microphone systems with long-range wireless communication between the officer and vehicle. The agency may deploy on-body video cameras as well.

The cameras typically included in these video surveillance solutions have the following specifications:

- A minimum of 25 frames per second (FPS).

- High definition recording, with a minimum resolution of 720x486 pixels for National Television System Committee (NTSC) format and 720x576 pixels for Phase Alternating Line (PAL) format.
- Support for both Motion JPEG and H.264 video codecs for recording. H.264 video encoding offers smaller file sizes, while MJPEG offers reduced susceptibility to corruption.
- HDR video capture, allowing for clearer video recording in low and adverse light scenarios.
- A wide-angle lens to capture a broader view of the scene around the vehicle. Some cameras may even support 360 degree recording capabilities.

These video surveillance systems support event marking of video segments based on a number of triggers and inputs. The system can be configured to take different actions depending upon the particular trigger, such as prioritization of a particular clip to be copied off the vehicle first, or even to notify an operator of an issue and live stream video over the cellular link from the vehicle. The systems will also typically support pre-recording, which enables the capture of a pre-configured amount of time before the triggering event. This permits the agency to access video surveillance when needed, but not use cellular data for video when it's not needed. The dispatchers are also able to call up video on-demand from any vehicle's cameras via the centralized management system.

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

Fleet Management Services

The Cisco Kinetic GMM is a cloud-based system that provides comprehensive vehicle gateway management, including provisioning, secure remote access, Wi-Fi management, GPS information and tracking, and cellular health tracking.

The RuBAN system from Davra networks provides a comprehensive AEP for vehicle fleet operations which integrates essential functions for managing a vehicle fleet: Vehicle telemetry data collection, driver behavior tracking, asset provisioning and monitoring, vehicle dashboard reports, policy-triggered events, and video surveillance integration.

Wireless Bulk Data Transfer

The various systems onboard the vehicles and the logging route progress require periodic connectivity with centralized monitoring systems to stay current. When the vehicles are inactive and parked at the station, this connectivity is established via a wireless connection from the vehicle to the station network.

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

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

Table 3 details the types of data exchanged, the expected size, and the frequency with which the data is exchanged.

Table 3 Data Types for WBDT

Data Type	Estimated Size	Expected Frequency	Direction
Router Software	90 MB	2/year	To vehicle
IP Camera Firmware	15 MB	2/year	To vehicle

Table 3 Data Types for WBDT

Data Type	Estimated Size	Expected Frequency	Direction
AP Software	20 MB	2/year	To vehicle
Archived Video Data	82GB for H.264 316GB for MJPEG	1/day	From vehicle
Onboard system logs	30 kB	1/day	From vehicle

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

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

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

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

If a particular vehicle's video is needed in its entirety, then the First Responder Fleet System proposes a designated video-offload location in the station, where that vehicle would make use of the entire amount of bandwidth available from an infrastructure AP. In this scenario, assuming 150Mbps of throughput to a vehicle, 82GB of video surveillance data can be copied in approximately 90 minutes, and 316GB of data can be copied in approximately 6 hours. If the first responder agency requires that all video had to be offloaded from every vehicle on a daily basis, then the resolution and frame rate of the onboard camera(s) needs to be reduced to ensure that the total video surveillance data is under the ~2GB threshold.

Vehicle Two-Way Voice Communication

The converged network infrastructure integrated into the First Responder Fleet System supports two-way PTT VoIP communications between the vehicle driver and the dispatchers in the operations center. This provides the flexibility to integrate next generation voice communications systems for new vehicle deployments and existing vehicle retrofits. The Cisco Instant Connect communications system also provides VoIP integration with the existing Land Mobile Radio System (LMRS), allowing for operators to integrate proprietary voice communication systems from other operational areas.

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

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

High Value Asset Tracking

Omni-ID can be used to track high value assets carried onboard the vehicle, and warn the vehicle driver if any tracked asset is not onboard when returning from an incident response. Information on Omni-ID can be found at the following URL:

- https://www.omni-id.com/tool-rental-equipment/

License Plate Recognition

Automatic tracking of vehicle license plates within view of the vehicle video surveillance camera. Alert law enforcement officer of any issues with a recognized license plate. License Plate recognition and optical character recognition should be conducted onboard the vehicle, so that only the decoded license plate information is transported over the cellular link.

System Components

This section, which lists the Cisco and third party components included in the Cisco First Responder Fleet System design, includes the following major topics:

Cisco Products

Table 4 describes Cisco components.

Table 4 Cisco Components

Model	Description
IR 829	Vehicle Onboard Mobile Router with integrated 4 port Gigabit Ethernet switch with Power over Ethernet (PoE), Wi-Fi AP and one or two LTE cellular modems
IW3702	Industrial 802.11ac Wave 1 Access Point to provide wireless infrastructure in Station network.
Catalyst 3850	Gigabit Ethernet switch with full Universal PoE support for station network. Incorporates Layer 3 gateway functionality, 10 GE uplinks for connectivity to Metro Network, and stacking capability for easy expansion.
WLC5520	Wireless LAN Controller for managing IW3702 APs with 10GE connectivity to data center. Exact model of WLC implemented should be matched to the scale of the deployment.
ASR 903/907	Unified MPLS capable modular aggregation router node with GE, 10GE, and 100GE interface support.
ASR 920	Unified MPLS capable fixed configuration pre-aggregation router node with GE and 10GE interface support.
ASR 1000	Hub router for FlexVPN termination from vehicles
ASA5545-X	High-capacity Firewall for protection of enterprise network infrastructure from public Internet peering connections.
Instant Connect	Cisco Instant Connect (formerly IPICS) system for push-to-talk (PTT)
Android Endpoint for Instant Connect	Android application providing VoIP endpoint functionality for Instant Connect PTT service. Integrates with Sonim XP7 Android smartphone.
IP Turret	Dispatcher console for Instant Connect integration
Jabber	Software endpoint client for Instant Connect integration

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

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

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

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

Third Party Products

Table 5 describes third party components.

Table 5 Third Party Components

Vendor	Model	Description
Davra	RuBAN	Application Enablement Platform for Data Acquisition/Analytics platform - http://www.davranetworks.com/product/features
SONIM	XP7	Ruggedized LTE/Wi-Fi Android smartphone - http://www.sonimtech.ca/xp7/xp7.php
Advantech B+B SmartWorx	HDV100A3	Heavy Duty Vehicle interface adapter to translate between the most common vehicle buses and the IR 829 Serial interface - advdownload.advantech.com/productfile/PIS/BB-HD3-A3/Product%20-%20Datasheet/HD3-A3_4717ds20171215230254.pdf

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

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

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

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

Software Feature and Application Support

Table 6 outlines the software features and application supported in the First Responder Fleet System in this phase.

Table 6 Software Feature and Application Support

Software Application	Function
Gateway Management Module	- Cisco Gateway Zero Touch Provisioning - Geographical Information System (GIS) - Vehicle GPS Tracking - Automated Network Management (such as CPU, MEM, RSSI, Wi-Fi Traffic, and User types) - LTE Performance Tracking and GPS correlation
RuBAN	- Rules, Policies, and Alert - Engines Vehicle Telematics - Vehicle GPS Tracking, Geo fencing - Vehicle Driver Management - Physical Security Integration
Cisco Instant Connect System	- Cisco Instant Connect Server
Web Portal	- Wi-Fi User Authentication

System Functional Considerations

This section includes the following major topics:

Data Center

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

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

Metro Network

Cisco Connected Roadways

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

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

Quality of Service

The First Responder Fleet System design 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 First Responder Fleet System, with mapping between these mechanisms supported at the boundaries between the different transport mechanisms.

The classes of service shown in Table 7 are implemented in the First Responder Fleet System, and are shown with mappings between representative classification markings for each type of classification.

Table 7 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 system design, the following locations in the network are the most important to focus on for deploying queuing and scheduling, as it is at these points where congestion will be encountered:

- The LTE cellular connection to and from the vehicle-In typical conditions, an LTE connection to a moving vehicle will be expected to support 10 to 20 Mbps of throughput. Ideally, the Mobile Service Provider will support multiple LTE QCI values for the service provided to the agency vehicles, 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 IR 829 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 829 router, with a parent shaper equivalent to the uplink bandwidth on the LTE link, and child classes defining the proper queuing treatment for each class.
- The edges of the Metro Transport network-The uplinks from each station network to the Metro Transport network are Gigabit or 10 Gbps Ethernet links, depending upon bandwidth needs, and as such, will not likely encounter much congestion under normal circumstances. However, it is still important to deploy QoS to prioritize EF and AF traffic from local sources over the WBDT traffic generated by the vehicles parked in the yard, to ensure that critical services such as VoIP communications and Video Surveillance function without any interference from traffic due to vehicle system updates and file offloads. Likewise, a bottleneck may occur at the uplinks from the Metro Transport network into the data center and operations center. As all of these links are using the available line rate of the underlying physical connection, a flat QoS policy to define the proper queuing treatment for each class is implemented.
- Internet peering connections to the 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 First Responder Fleet 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.

Routing and Network Address Translation (NAT)

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

The onboard gateway implements the following functions to enable the services supported in the system design:

- **Dynamic Client IP Addressing**-By using Dynamic Host Control Protocol (DHCP), the onboard gateway enables dynamic IP addressing for onboard systems, simplifying the provisioning and maintaining of those systems. Also, by combining this with Network Address Translation (NAT), the onboard configuration can use identical private IP subnets for all vehicles, further simplifying system deployment. DHCP address pools can be configured on the onboard gateway for multiple IP subnets and managed on a per-interface or per-subinterface basis. The DHCP server function on the onboard gateway supports static mapping of IP addresses to MAC addresses or DHCP identifiers, allowing for devices to receive persistent IP addressing. Alternately, IP address ranges can be reserved in any pool to accommodate devices which require static addressing to be configured on the device. Finally, the DHCP server on the onboard gateway supports all DHCP options, allowing for additional information, such as the IP addresses of DNS servers and TFTP servers, to be passed to other systems onboard.
- **Dynamic Routing**-The onboard gateway implements an Interior Gateway Protocol (IGP) to dynamically configure routing of traffic between onboard systems and backend systems and manage traffic over the wireless offboard connections. This system implements Enhanced Interior Gateway Routing Protocol (EIGRP) for this function. By establishing EIGRP adjacencies with hub routers in the Ops Center, the onboard gateway is able to automatically maintain optimal data routing to and from the onboard systems. EIGRP timeouts and other parameters can be tuned to optimize performance given the specific criteria of a particular deployment.
- **Policy-Based Routing**-Routing decisions by the IGP implemented on the onboard gateway can be influenced by several mechanisms, including static routes injected into the routing table, routing metrics to adjust link preference, and route-maps to control the treatment of routing information within the IGP. The system design utilizes all of these mechanisms in implementing the services supported.
- **Multiple Loopback Addresses**-A Loopback interface on a router is utilized to provide a virtual gateway address for element management or for an individual service. The onboard gateway is able to support multiple Loopback interfaces, providing gateway functionality for multiple services simultaneously. Each Loopback interface is advertised into the IGP dynamic routing table, and is combined with NAT to support multiple onboard devices for a particular service.

- **Network Address Translation (NAT)**-The onboard gateway implements NAT to translate the address information between onboard "private" IP address spaces and route-able "public" IP address spaces in real-time. NAT mapping between IP addresses is handled dynamically by the onboard gateway as it receives traffic originated onboard that is destined for an offboard IP address. If the traffic pattern for a particular service requires a data connection to be originated initially by an offboard system, such as the case with Video Surveillance, then a static NAT entry is configured on the onboard gateway to allow for that traffic flow.
- **Network Address/Port Translation (NAPT)**-Also known as “overloaded NAT" or simply "Port Address Translation (PAT)." NAPT enables multiple devices in a private IP address space to utilize a single route-able public IP address. Each private IP address and port with an active data connection is mapped to a unique public IP address and port combination, allowing multiple devices to share a single route-able IP address effectively. As with NAT, NAPT allows for static mapping entries as well.

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

Security

The First Responder Fleet 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 WGB and station 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, WPA, and TKIP.

All network nodes in the First Responder Fleet System support being managed and monitored remotely from the operations center via the following secure methods: SNMP v2/v3, SSH, and HTTP/HTTPS. The Cisco Kinetic GMM system utilizes a FlexVPN tunnel for communication with the Cisco IR829 gateways onboard the vehicles. The Davra RuBAN system utilizes HTTPS for communication with the network nodes in the system design, providing for secure management of the network infrastructure.

Any interface that could be exposed to physical access by untrusted persons, such as the router and switch onboard the vehicle, has port security with 802.1X authorization enabled to prevent unauthorized access to network infrastructure. All wireless access to enterprise infrastructure is secured by WPA2 username/password and/or certificate-based authorization, depending upon which mechanism is implemented by the First Responder Fleet agency. Cisco provides full Mobile Device Management (MDM) functionality for secure mobile device deployment, which is fully compatible with the First Responder Fleet System.

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

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

The 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 FlexVPN tunnels. The FlexVPN implementation in the onboard router is capable of supporting many different encryption standards: DES, 3DES, AES 128, AES 192, and AES 256. The system recommends implementing the strongest standard and largest keys supported to provide the most secure connection.

Since the FlexVPN tunnels are terminated on a hub router situated in a DMZ behind the security node, certain inbound ports are required to be opened on the security node. To protect the hub router from possibly becoming an attack vector to the rest of the network, VRF-lite is configured in conjunction with the FlexVPN configuration. This configuration prevents any traffic not encapsulated within a FlexVPN tunnel from gaining access to any infrastructure behind the hub router.

For FlexVPN between the hub router and vehicle gateway, as well as Kinetic GMM communication, the ports listed in Table 8 must be open:

Table 8 Required Open Ports

Port	Protocol	Description
53	UDP	Domain Name System (DNS)
123	UDP	Network Time Protocol (NTP)
500	UDP	Bidirectional access is required for the Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
4500	UDP	Bidirectional access is required for IPSec NAT Traversal
8883	TCP	Secure MQTT (MQTT over TLS) for the data pipeline
9123	TCP	Call-home registration

GMM also allows for the configuration of VRFs in order to separate GMM management traffic from service traffic.

System Redundancy & Reliability / Availability Models

The network infrastructure on the vehicle has no resiliency requirements. The network infrastructure components utilized on the vehicle all incorporate ruggedized design and construction, resistance to shock and vibration effects, and extended temperature range functionality to ensure reliable performance in the harsh operating environment of a vehicle.

- The station wireless network design requires load-balancing and failover functionality between Wi-Fi access points in the yard, to facilitate an equitable distribution of vehicle WGB connections between access points, and to provide hand-off of WGB connections from one access point to another if an access point is taken out-of-service. Load-balancing and resiliency of connections to the Wi-Fi infrastructure is controlled by the Wireless LAN Controller.

  Redundancy for the switching infrastructure of the station network is accomplished by implementing switch stacking utilizing two or more Catalyst 3850 routers. Redundancy for the uplinks to the Metro Network pre-aggregation nodes is accomplished by implementing Link Aggregation Control Protocol (LACP).

- The Metro Network design implements ring topologies, providing resilient connectivity to nodes within the network in the case of a single link or node failure. Uplink connections from any yard network are terminated on two different nodes in the Metro Network utilizing multichassis LACP (mLACP) to provide link and node redundancy. Uplink connections from the Metro Network to the Operations Center infrastructure utilizes two different nodes, again implementing mLACP. All resiliency design mechanisms are covered in detail in the *Connected Roadways Design and Implementation Guide*, which can be found at the following URL:

  — https://www.cisco.com/c/dam/en_us/solutions/industries/docs/conn-roadways.pdf

  Redundant User-to-Network Interface (UNI) links from the Mobile Service Provider and Internet Service Provider may be implemented. Typical uptime Service Level Agreements (SLAs) for these UNI connections will exceed the uptime requirements for the Connected First Responder Fleet System, so the cost versus the benefit of redundant UNI links must be analyzed by the First Responder Fleet operator.

Implementation of this kind of redundancy is well understood and has been validated in many systems, so is considered outside the scope of this First Responder Fleet System document.

Initial Scalability / Performance Assessment

Scalability and performance criteria for individual service areas are contained within the service descriptions in this document in Supported Services and Models, page 24. The systems and platforms proposed in the First Responder Fleet System design are geared to easily handle a vehicle fleet of 4000 vehicles, and can be scaled to handle even larger fleets.

LTE Service Scalability

A single LTE link from a vehicle should accommodate approximately 15 Mbps of bandwidth. Voice communications, GPS location, Engine telematics, and other Enterprise service traffic should be on the order of well under 1 Mbps. In case of a first responder dispatcher or supervisor needing access to live streaming of video surveillance traffic during an incident, there is plenty of bandwidth available on the LTE link (an additional 4Mbps for HD video), and the QoS service policies implemented on the cellular uplink ensure proper service delivery.

Since the number of vehicles in operation simultaneously will fluctuate, potential bandwidth utilization has been calculated using three different values (assuming 400 total vehicles in the fleet, and all vehicles are accessing live video):

- 0With 25% of vehicles in operation simultaneously, the total bandwidth utilization of all these vehicles toward the Mobile Service Provider network is approximately 500 Mbps
- With 50% of vehicles in operation simultaneously, the total bandwidth utilization of all these vehicles toward the Mobile Service Provider network is approximately 1 Gbps
- With 100% of vehicles in operation simultaneously, the total bandwidth utilization of all these vehicles toward the Mobile Service Provider network is approximately 2 Gbps

Mobile Service Provider networks are typically scaled to handle orders of magnitude larger amount of traffic, so this is not an issue for the Mobile Service Provider. Since only the Enterprise service traffic needs to be carried to the agency's Operations Center, and this traffic is expected to be on the order of around 2 Gbps per second in the most extreme case, then either two Gigabit Ethernet links or a 10 Gigabit Ethernet link with a sub-linerate service is more than sufficient for the UNI connection from the Mobile SP to the agency's data center.

Station Wireless Network 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 station parking lot:

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

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

The First Responder Fleet 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.

Glossary

Table 9 lists the acronyms and initialisms used in this document.

Table 9 Acronyms and Inititalisms

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 (i.e. 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
GLOSNASS	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

Table 9 Acronyms and Inititalisms (continued)

Term	Description
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	Receive Signal Strength Indicator
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

Table 9 Acronyms and Inititalisms (continued)

Term	Description
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