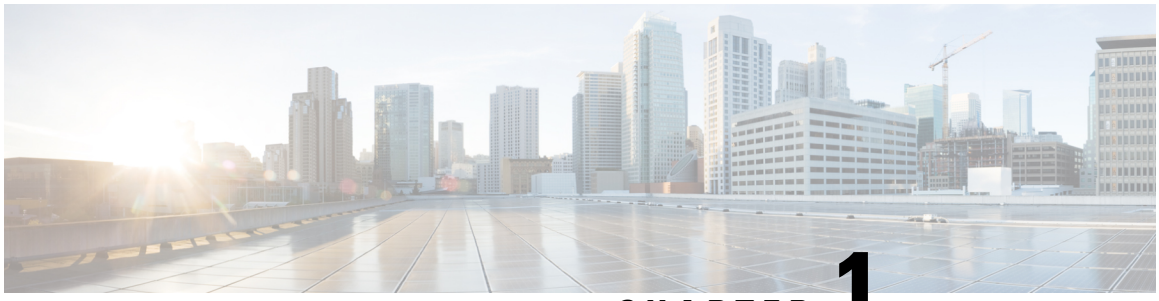
SD-WAN for Fleet and Transit Design Guide

First Published: 2023-05-02

Last Modified: 2023-05-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

SD-WAN for Fleet and Transit Design Guide

Introduction

Modern mass transit and fleet deployments today rely greatly on connectivity for both onboard devices, as well as applications in central datacenters or the cloud. The Cisco SD-WAN solution based on vManage can help extend the enterprise network to the assets in the field -- including bus stops, bus yards, maintenance yards, and even the vehicles themselves.

This document builds on other existing documents that describe the Cisco SD-WAN solution and Internet of Things (IoT) hardware offerings in detail and helps show how they can be combined to provide a scalable, secure network. While the document covers both mass transit and fleet deployments, more focus is given to mass transit as it tends to be a super set of fleet and other additional requirements.

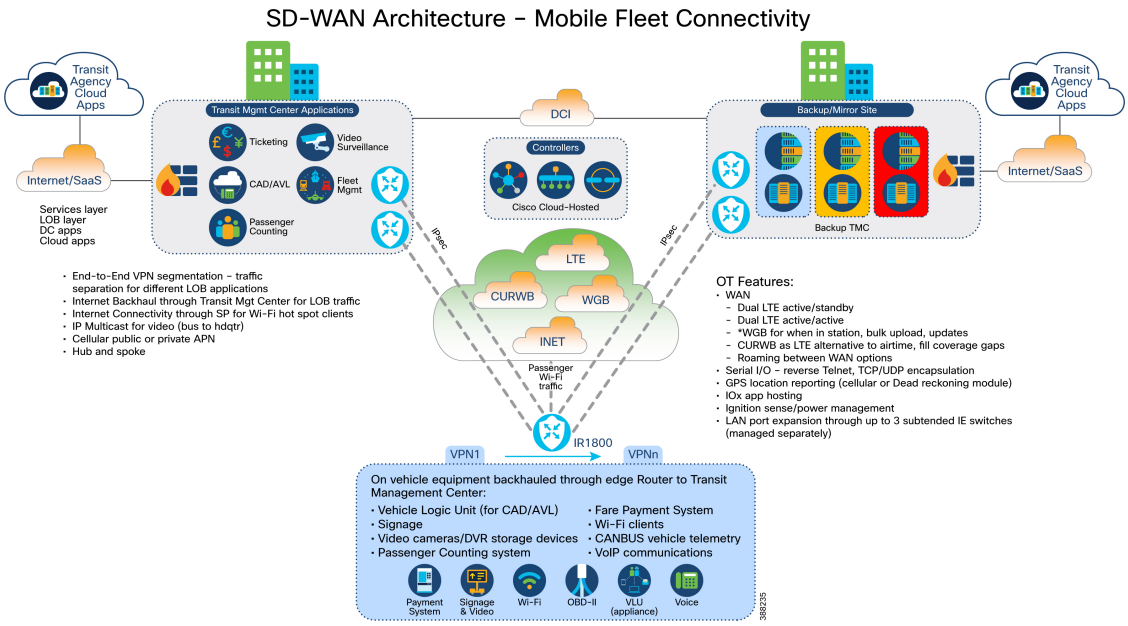
Readers should already have some familiarity with Cisco SD-WAN and IoT. Prior to reading this document, it is recommended to be familiar with the following resources:

Cisco SD-WAN Small Branch Design Case Study – This document provides a great overview of general SD-WAN concepts in the context of a “small branch” which has many commonalities with a typical IoT deployment used in a mass transit or fleet scenario.

Cisco IoT Industrial Router Extension to the SD-WAN Small Branch Design Case Study – This document builds on the previous one, with a focus on areas that are unique or at least emphasized by IoT use cases in general. This document also has detailed configuration examples for many of the IoT features.

Architecture

Figure 1: SD-WAN Architecture for Fleet and Mass Transit



Internet access for LAN devices can use different non-exclusive methods including:

- Centralized (ideally with Umbrella, or a traditional on-prem Internet security stack) – depicted here
- Local via Umbrella SIG
- Local (DIA) via ZBFW (and UTD in the future)

The network architecture for a mass transit or fleet deployment consists of the following major areas:

- Transit Management Center
- Cloud Provider
- WAN
- Mobile Vehicles
- Fixed Remote Sites

These areas are discussed in the following section.

Transit Management Center

The Transit Management Center (TMC) houses the critical applications and staff responsible for making the line of business run smoothly. This includes hosting centralized fleet management, CAD/AVL, ticketing, scheduling, dispatch, and monitoring software that ensures that drivers and vehicles are operating as expected and any issues that arise can be addressed appropriately. The TMC applications connect into the enterprise network which is equipped with proper capacity, performance, security, and resiliency to keep the applications running with minimal disruptions.

Network component details at this level are beyond the scope of this document but would generally include some compute resources for hosting applications, resilient routing and switching design, firewalls, and internet

connectivity. Additionally, the TMC is secured by a variety of products and technologies including Identity Services Engine, AMP/IPS, and Steathwatch.

A geographically separate backup TMC is common practice, especially for larger deployments that need maximum uptime and resiliency.

Cloud Provider

It is becoming increasingly common for the transit or fleet company to leverage public cloud infrastructure for hosting various applications. Offloading applications from a local datacenter can offer efficiencies in reducing the equipment and staffing required for a traditional datacenter. In some cases, certain requirements can be met with an over-the-top approach of just providing internet connectivity to an application which will talk to a cloud provider hosting an application. When using a cloud provider, it is important to consider the security implications – such as how data from a vehicle will reach the cloud, and whether this will bypass security mechanisms that in place within the TMC/datacenter.

WAN

Fleet and transit deployments are by nature very spread out geographically, and thus very dependent on different WAN technologies. From the TMC with redundant highspeed fiber backhaul, to mobile vehicles with potentially a slow or lossy cellular connection, the requirements of each type of site needs to be analyzed carefully.

The TMC will be connected to the enterprise network with redundant, high speed wired connections. Connections between geo-redundant TMC / DC will utilize optical networking technologies such as DWDM to maximize performance over short to long distances of fiber interconnects.

Remote fixed assets like bus stops can leverage existing wired infrastructure such as ethernet or DSL, or they can rely on wireless technologies including cellular (LTE & 5G) or Cisco Ultra Reliable Wireless Backhaul (CURWB) (point to point, point to multipoint). These sites typically use relatively low bandwidth.

Mobile assets like buses and cars must rely completely on wireless connectivity such as cellular (LTE & 5G), Wi-Fi, or CURWB. In many cases redundant connections are used to provide maximum uptime in RF environments that are constantly changing due to geographic location and other environmental effects.

Mobile Vehicles

Mass Transit and fleet vehicles can leverage a single ruggedized router for connectivity of all the onboard devices to each other, the TMC, and the internet. Typical devices onboard a mass transit vehicle like a bus would include a fair payment system, passenger counter sensors, door sensors, cameras, Wi-Fi access point(s), a Computer-Aided Dispatch / Automatic Vehicle Location (CAD/AVL) system, VoIP communication device, emissions sensors, CANBUS interface to the vehicle, GPS tracking, and more. All these devices can be connected directly to the ruggedized router, or if more ports are required, a subtended ruggedized switch could be used behind the router.

Fleet vehicles such as taxi cabs, police cars, and similar typical applications will often have some overlap with mass transit vehicles in terms of onboard devices. Differences could include the type and number of sensors, cameras, and other client devices.

WAN connectivity is strictly based on wireless technologies such as cellular for on-the-move connectivity, or even CURWB in environments with a fixed infrastructure in place and strict performance requirements or where there are gaps in cellular coverage.

Fixed Remote Sites

Fixed remote sites include areas like bus stops which may be home to devices like digital signage for scheduling or route information, and potentially passenger Wi-Fi. These sites typically need connectivity back to the TMC to retrieve content for the signage, and direct internet access for Wi-Fi users. Backhaul can be provided

by existing wired infrastructure (municipal fiber network for example), wireless infrastructure like CURWB or WiFi, or cellular. For basic fixed location sites, the Cisco IR1101 provides an ideal solution for a low-power, modular router. If Wi-Fi or other advanced features are required, one of the IR1800 series routers may be more applicable.

Requirements

The requirements detailed below focus on the mobile vehicle and related devices. Details for remote fixed sites like bus stops are a similar, small subset of those described here. Details for the TMC and other areas of the network are beyond the scope of this document.

IR features Used By the Fleet Market

The Cisco IR1800 Series routers are well positioned to meet the needs of the mass transit and fleet market. The list below calls out some of the specific capabilities of these routers that make them ideal for this use case:

- Ruggedized enclosure with multiple industry certifications
- Modular design for future upgrade path
- Wi-Fi 6 access point module, with dual band, 2x2 MIMO, 2 spatial streams
- Modular cellular WAN interfaces for up to two 5G uplinks
- PoE GigabitEthernet switchports
- GPIO for digital alarm or sensor input/output
- GPS location tracking, including optional Dead-Reckoning module for calculating position during lost satellite signal
- Ignition sense and ignition power management
- Ingestion of CANBUS data from the vehicle OBD-II or J1939 port

Key Use Cases and Associated Equipment

Figure 2: Example of an Overhead Equipment Bay in a Bus Housing a Router, CAD/AVL, and More

Typical equipment inside the vehicle includes:

- Router
- Wi-Fi Access Point
- CURWB Radio
- Cellular modems
- CAD/AVL
- Passenger counting
- Fare Payment/Collection system
- IP connected cameras and video storage
- Signage
- Voice over IP transport

Router

A ruggedized router is required to act as the central device to aggregate all other devices on the vehicle and provide secure connectivity to the other applications and devices as required. The router itself must be able to withstand the physical environment encountered in a moving vehicle -- that is potentially extreme fluctuating temperatures and humidity, vibration, and dust. Related industry standards include SAE J1455, MIL STD

810G, UL 121201 Class I Div. 2 A-D, UNECE R10, CISPR25, ISO 7637-2, and ISO 11452-2/4. The router is typically mounted in a secure position in the vehicle such as in the trunk of a police car, or a dedicated rack behind or above the driver in a bus.

The router provides connectivity in the form of ethernet switch ports for LAN, one or more cellular WAN interfaces, serial and GPIO ports for sensors, a CANBUS interface for vehicle monitoring, Wi-Fi, PoE for powering connected cameras or other devices, and GPS for location tracking.

Figure 3: Cisco IR1835 Front View

The Cisco Catalyst IR1800 Rugged Series Routers meets all these requirements and more. The IR1800 is modular for future upgradability, but today offers dual 5G modems and a Wi-Fi6 access point to address the most demanding connectivity requirements. Other innovative features include edge compute capability in the form of Cisco IOx, a 100 GB solid state drive, and an optional dead-reckoning module for computing approximately vehicle location even when there is a loss of GPS signal. For additional details, refer to the Cisco Catalyst IR1800 Rugged Series Routers Data Sheet.

Wi-Fi Access Point

Wireless connectivity on-board a vehicle can create a value-add service in the case of mass transit, or provide flexible connectivity for critical devices including laptops, VoIP endpoints, and more in both mass transit and fleet deployments. Wi-Fi6 can be implemented with the modular access point on the Cisco IR1800 router, utilizing external antennas for maximum coverage (internal or external to the vehicle). It is also possible to implement multiple SSIDs to serve, for example, passengers and transit employees simultaneously while maintaining security through traffic segmentation, centralized authentication, and other security mechanisms.

The same access point module on the IR1800 can act as a small-scale Wi-Fi controller onboard the vehicle, allowing a limited number of additional access points to register to it, expanding coverage in the case of a large vehicle such as an articulated bus.

CURWB Radio

Cisco Ultra-Reliable Wireless Backhaul (CURWB) can provide a high-speed WAN link for the Cisco IR1800, suitable for connectivity on the move at speed. For example, if a city builds out a CURWB network, a transit vehicle could take advantage of this to provide a high bandwidth, low latency for passenger Wi-Fi, streaming video, and other data intensive applications. CURWB also provides seamless handover capability as the vehicle roams between fixed infrastructure radios. The Cisco IW9165 was designed specifically to be mounted on a moving asset or vehicle like a bus or light rail train. This can be paired with a network of fixed position Cisco IW9167 radios.

Figure 4: Cisco IW9165 and Cisco IW9167 CURWB Radios

Note that the IW9165 and IW9167 are not configurable through vManage templates. Alternatives include CURWB standalone tools or IoT Operations Dashboard for off-line configuration generation and local application to the CURWB devices.

Antennas

Antennas are a critical component for a system that relies on wireless connectivity for Wi-Fi, Cellular, GPS, CURWB, and more. Typically, antennas for these applications are roof mounted and omnidirectional. For best performance, it is strongly recommended to review the Cisco Industrial Routers and Industrial Wireless Antenna Guide to find the correct antenna for a specific use case based on the required frequency bands, connectors, gain, etc. Mounting the antennas is also important to ensure there is minimal interference with other RF sources and that the antenna is secure. If multiple antennas are required, there must be a minimal distance between them, as described in the Antenna Guide. Cisco produces a variety of antenna options, including 5-in-1 and 7-in-1 dome style antennas for Wi-Fi, GPS, and Cellular.

Cameras and Video Storage

Physical security is important for both mass transit and fleet deployments, as companies try to protect their property, employees, and the general public. In addition to security applications, modern video cameras often include some level of onboard analytics and processing capabilities that can be used for tasks like people counting (number of passengers for example), or even gunshot detection (for law enforcement). Vehicle cameras can be mounted inside or outside the vehicle, depending on the intended use, and must be able to withstand vibration, dust, and even harsh weather. Camera power is typically provided through the same Ethernet cable used for data, and this is connected to a PoE port on the ruggedized router, or a subtended switch. The Cisco IR1835 router includes 4 switchports with PoE capability, providing up to 30W. If more power is required, it is recommended to use a subtended switch like the Cisco IE3200, IE3300, or IE3400 series industrial ethernet switches.

The video can be stored locally on the camera, if supported, or a dedicated Digital Video Recorder (DVR) that aggregates video from all cameras in the vehicle. To offload the video from the vehicle, it may be desirable to wait until the vehicle is back at the depot or station and within range of a high-speed wireless backhaul like Wi-Fi or CURWB. Streaming video from the cameras in real time is also an option but can use significant amounts of bandwidth which is a generally a concern for cellular backhaul.

CAD/AVL

Computer Aided Dispatch (CAD) systems on public transit vehicles connect the bus to the dispatcher or operator, providing updates to scheduling and routing, detours, service disruptions, and more. Automatic Vehicle Location (AVL) systems utilize GPS to accurately determine the transit vehicle location, and share it with the TMC for tracking, scheduling, and routing.

There is often a driver panic button for the driver to signal extreme conditions. This panic button can be integrated with the CAD/AVL inputs or could go to the router directly with GPIO alarming. See the Driver and passenger Safety & Triggers - GPIO alarming section later in this document.

Voice Communications system

Fleet and Mass Transit drivers need a way to communicate back to the office to receive and provide updates about what is happening around them. From being redirected to a new location, to a reporting an emergency, voice communication is critical in vehicle applications. Traditionally, voice communications were conducted over radio, which required expensive dedicated transceivers, antennas, and had limitations in terms of security, range, and quality. Modern Voice over IP systems can leverage the IP network, backhauling voice traffic over the same packetized data links that are used for other applications within the vehicle. Not only do VOIP systems utilize the same existing network, but they can leverage the added encryption, segmentation, and other security benefits provided by Cisco IOS-XE based ruggedized routers. Quality of service can be enabled to prioritize VOIP traffic over less critical applications, ensuring a high-quality experience.

Signage

Digital signage systems can be used to display static information like the assigned route for a bus or be updated dynamically based on the time or location to show the next stop or estimated arrival time. Dynamic updates can come from integration with the CAD/AVL system directly, or over the network from the TMC.

Fare Payment System

A fare payment system can leverage the Cisco SD-WAN network to reach the backend servers for payment authorization – whether they are in the TMC, another DC, or in the cloud. Service VPN segmentation and IPsec encryption ensures that the payment data is isolated protected end-to-end.

Passenger Counter

Passenger counter systems are important for getting accurate metrics on route and bus utilization. These systems typically are mounted on the doors of the transit vehicle and can use optical sensors to detect when a person enters or leaves the vehicle. Alternatively modern digital camera systems could be utilized to count passengers. The passenger count data is sent through the network to the TMC for analysis in planning future routes, or rebalancing assignments.

Emissions Sensor

Even with the shift to electric power, most of the transit and fleet vehicles today still run on fossil fuels. With a push to make these vehicles conform to emissions regulations by local, state, and federal agencies – it is helpful to have data to monitor the progress. A sensor mounted on or near the tailpipe can monitor the exhaust gases to look for levels of harmful substances. Advanced emissions sensors may also be able to work with other onboard sensors to measure things like fuel economy, driver behavior, and even identify mechanical issues with the vehicle.

Applications and Protocols

IoT use cases for mass transit and fleet utilize many types of protocols and applications. Below are a few common ones, and how they are used.

CANBUS

The Controller Area Network bus (CANBUS) is made up of a network of Electronic Control Units (ECUs) within a vehicle, connected by a 2-wire bus that provides communications between the various subsystems of the vehicle. This bus is also connected to the OBD-II (in the case of cars or smaller trucks) or J1939 (in the case of larger vehicles) connector within the vehicle that provides a diagnostic interface for external equipment. The Cisco IR1800 series router can derive power from this connector and can read the data present on the CANBUS. Once the IR1800 is configured with the correct CANBUS baud rate, it can ingest the data and send it to either an IOx application for further processing, the IRM-GNSS dead-reckoning module for approximate location calculation, or both.

IPsec

IPsec provides the basis for encrypted transport to and from the Cisco ruggedized router over the WAN. The SD-WAN network based on Cisco vManage automatically creates IPsec tunnels between the edge routers, ensuring that all traffic is protected.

Multicast

Multicast is a means of sending IP traffic from one source to many destinations in a very efficient manner, avoiding duplication of packets for each recipient. This technology can greatly reduce bandwidth utilization in the case of streaming video, for example.

NMEA

National Marine Electronics Association (NMEA) is today used as a data format for GPS location information. Various types of information can be encoded in a standardized format so that it has interoperability between various vendors hardware and software. On the Cisco industrial routers like the IR1101 and IR1800, the GPS information from the cellular modem or dead-reckoning module can be sent to a specified destination IP address and port for processing.

Typical WAN Scenarios

A mobile vehicle mounted router presents an interesting use case for WAN connectivity. The vehicle needs to rely solely on wireless communication which is inherently less reliable and lower performing than most wired options. Some level of packet loss, jitter, increased latency, and lower throughput should generally be expected and accounted for in the network design. Cisco vManage SD-WAN solution is ideal for this scenario as it can provide intelligent routing, resiliency, and monitoring – regardless of what underlying WAN technology is being used.

The simplest WAN connectivity option is a single cellular connection. This is a very cost-sensitive solution that can provide adequate connectivity in situations where maximum uptime and performance is not as critical. For example, if the IoT solution is just providing connectivity for some sensors that can tolerate momentary issues in connectivity, a single cellular connection can be sufficient. Similarly, if a vehicle primarily operates in a geographic area with great cellular signal coverage by a specific provider, this can also be a good solution.

Another option available on most of the cellular PIM modules for the industrial IoT routers is the use of dual SIM cards within a single modem. In this setup, two SIM cards from different providers are used to provide a primary and backup connection. The primary SIM (and associated carrier) are used from the time the router first boots up, until there is a complete loss of connection that triggers the modem to reboot and start using the second SIM. This can be helpful in cases where the primary concern is that the cellular network itself may go down. There is a longer failover time associated with this approach -- around 12 minutes, because the modem will by default try to recover the link once with the primary SIM, and then reboot with the second SIM as active. This can be less than ideal for an on-the-move scenario or if there are applications involved that cannot tolerate this amount of downtime.

Both the Cisco IR1101 and IR1800 can support dual cellular modems. The modems can be configured to operate in an active-active mode where dataflows are load balanced across the links, effectively doubling the

potential cellular bandwidth available to the router. Alternatively, the modems could also be configured in an active-standby manner so that the first modem will actively forward the WAN data for the router until BFD detects that the connectivity is down. Both configurations can offer quick failover times and are suitable for on-the-move applications in a vehicle. SD-WAN excels in deployments such as these where there are multiple active WAN links.

Cisco Ultra-Reliable Wireless Backhaul (CURWB) can be implemented by connecting an external CURWB radio, like the IW9165 or IW9167, to one of the onboard switchports. CURWB offers many benefits including high bandwidth and lossless resiliency. A fixed infrastructure is required to realize the benefits of CURWB but produces excellent results.

In addition to the scenarios described above, different combinations of these options can also be deployed, for example use CURWB when available around a station or depot, and switch to a load balanced dual cellular connection once on the road.

The table below summarizes the failover performance times for the different scenarios described above.

Table 1: Failover Performance

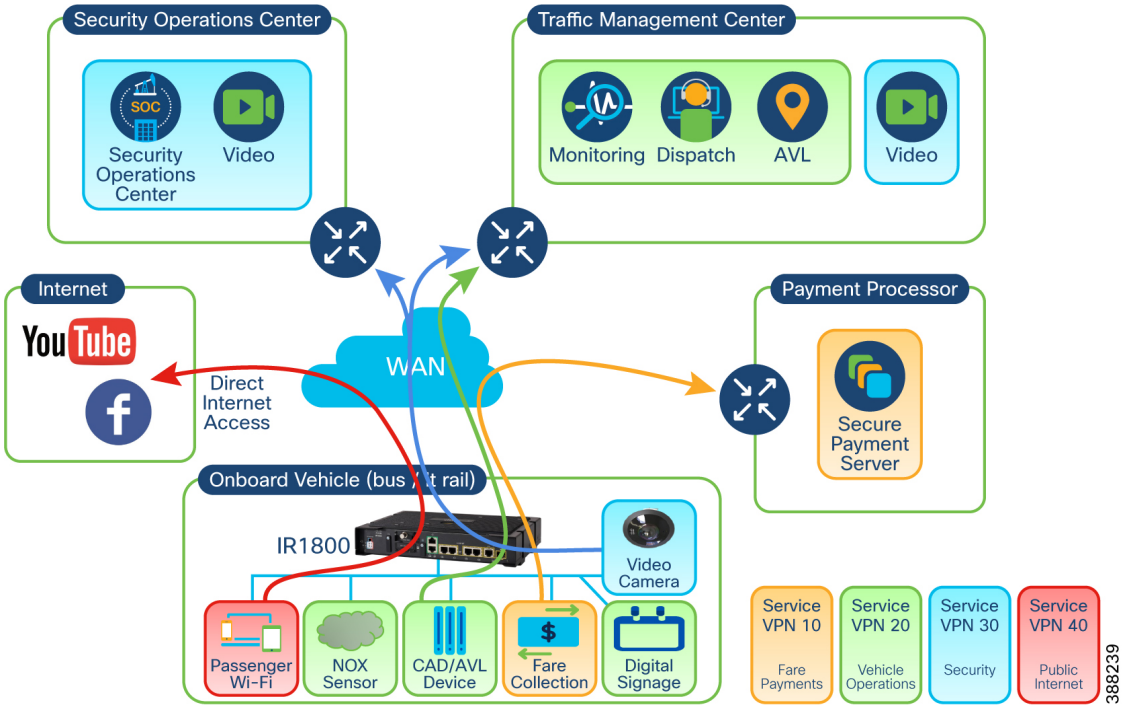
Scenario	Average Failover Time
Ethernet to Cellular (Last Resort)	7s
Cellular to Cellular (Active/active, ECMP Load Balancing)	7s
Cellular to Cellular (active/standby)	7s
Single Cellular with Dual SIM	12m
Cellular to CURWB via Ethernet	7s

In all tests, the BFD timers were left with default values of 1000 milliseconds for hello interval, and multiplier of 7.

Service VPN utilization for segmentation across different devices

Cisco SD-WAN solution provides easy-to-manage secure separation of different devices and applications. Service VPNs can be configured across the SD-WAN network, spanning one to many edge routers. The Service VPN concept is analogous to the VRF concept in traditional routing. These VPNs are extended on the LAN side toward client devices by placing them in different VLANs, each associated with a different SVI interface inside the VPN. On the WAN side, IPsec is used to extend the VPNs between edge routers – whether they are on vehicles or in a datacenter. This segmentation will prevent applications and users in different service VPNs from accessing each other. In the example below, four service VPNs have been created (10, 20, 30, 40). Depending on which locations and applications need access, some or all the VPNs can be extended to a specific location. In the case of VPN 40, it does not extend to other edge routers, but instead breaks out immediately to the internet, directly from the IR1800 router in this case.

Figure 5: Macrosegmentation Through Service VPNs



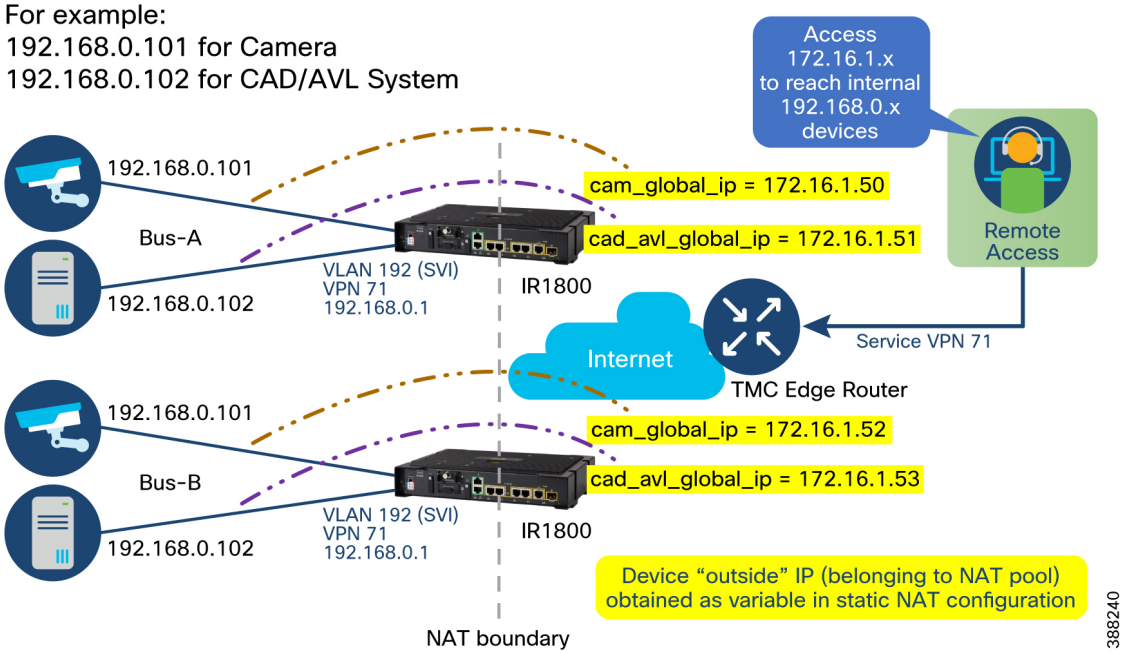
How 1:1 Static NAT Is Used and Why

In IoT deployments where there are many sites each with identical equipment, it can be helpful to use the same IP addressing scheme at each site, such as a bus. This common addressing scheme helps the OT team to deploy the end devices on the vehicle using a predefined, static IP address. Subsequently after the device is deployed, it can be accessed remotely by connecting to an NAT “outside” address which is forwarded to the inside address. If using this solution, it is important to keep careful records of the outside to inside address mapping.

In the example below, the administrator has setup an addressing schema so that each bus, consisting of an IR1800 router, one camera, and one CAD/AVL system uses the subnet 192.168.0.x/24 on the LAN side. This subnet will be identical on each bus, and the individual host addresses will be the same as well -- all cameras are assigned 192.168.0.101, and CAD/AVL systems are assigned 192.168.0.102. The Cisco IR1800 router performs the static 1:1 NAT function as configured using vManage feature templates and centralized policy. A unique outside address from the 172.16.0.0/16 pool is chosen to map to each individual camera or CAD/AVL system. A remote user would then be able to connect to 172.16.1.50 and be forwarded to 192.168.0.101 -- the camera on Bus-A.

LAN devices across all sites can be configured with same local subnet (192.168.0.X/24)

For example:
192.168.0.101 for Camera
192.168.0.102 for CAD/AVL System



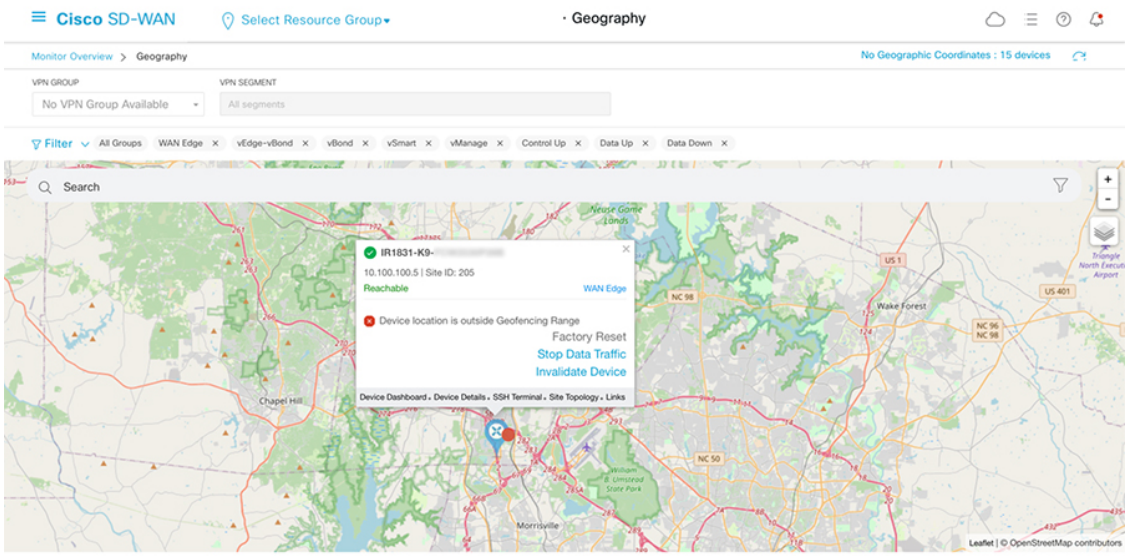
Location and Geofencing

The IoT routers equipped with supported cellular modems can be configured as GPS receivers. The GPS signal will allow the router to be located geographically based on latitude and longitude coordinates. This location can subsequently be shared with vManage and plotted on a map that is pulled from Google Maps via API. The reported location will be updated every few minutes.

Cisco vManage can also utilize a geofence around a specific location (either manually defined, or automatically detected by the router). If the router detects that it is outside the geofence area (in the shape of a circle, 100m to 10km radius around the router), it can be set to trigger an alert on the dashboard or send an SMS message. From the dashboard, if a router leaves the geofence, the administrator can quickly and easily take action by disabling data traffic or even invalidating the device certificate.

At this time, only the cellular modem GPS receiver can be used as the source for mapping and geofencing within the vManage dashboard. Either the cellular modem or the dead reckoning module can be configured with a CLI template to send a NMEA stream to a specified IP address and port number to be processed further, however it is not possible to associate the NMEA stream with a particular Service VPN, therefore the destination needs to be reachable within VPN0.

Figure 6: Cisco IR1831 Location Detected Outside the Geofence

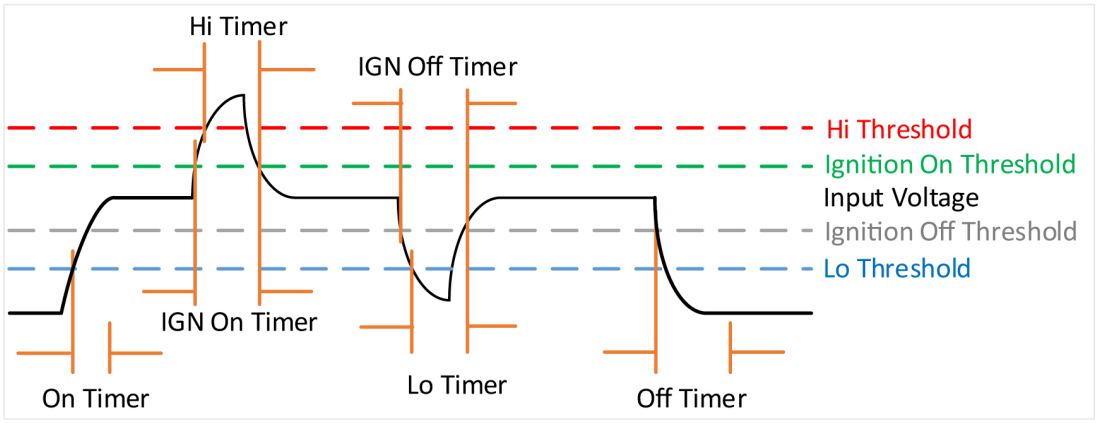


Ignition Sense/Power Management – How/Why Used

The Cisco IR1800 series routers can be powered either through the OBD-II / J1939 connector itself, or directly from the vehicle battery. In either case, it is important to prevent the router from continuing to draw power from the vehicle battery while the engine is not running so that the battery is not drained. To prevent this problem, the IR1835 offers two solutions (ignition sense, and ignition power management), while the IR1821, IR1831, and IR1833 all support ignition sense.

Ignition sense utilizes the two DC power input wires to monitor the voltage feeding the router. When the vehicle engine is running (and the alternator is charging the battery), the input voltage will be slightly higher than if the engine is stopped, and power is coming directly from the battery only. This change in voltage is used to determine whether the vehicle is on or not. When the ignition sense feature detects the vehicle is off, it will start a configurable timer. When the timer expires, the router will be gracefully powered off. This delay introduced by the timer is helpful in situations where the driver needs to turn off the vehicle for a few minutes to fill up on gas, etc. If the timer has not expired, the router remains on and there is no downtime.

Figure 7: Ignition Sense – Analog Input



Input Voltage (DC)	
Min	9.6V
Max	36V
Nominal	12V or 24V

Ignition Sense Voltage		
	12V Battery	24V Battery
On	13V + 2%	26V + 2%
Off	13V -2%	26V - 2%

Battery Voltage		
	12V Battery	24V Battery
Undervoltage	11.5V	23V
Overvoltage	36V	36V

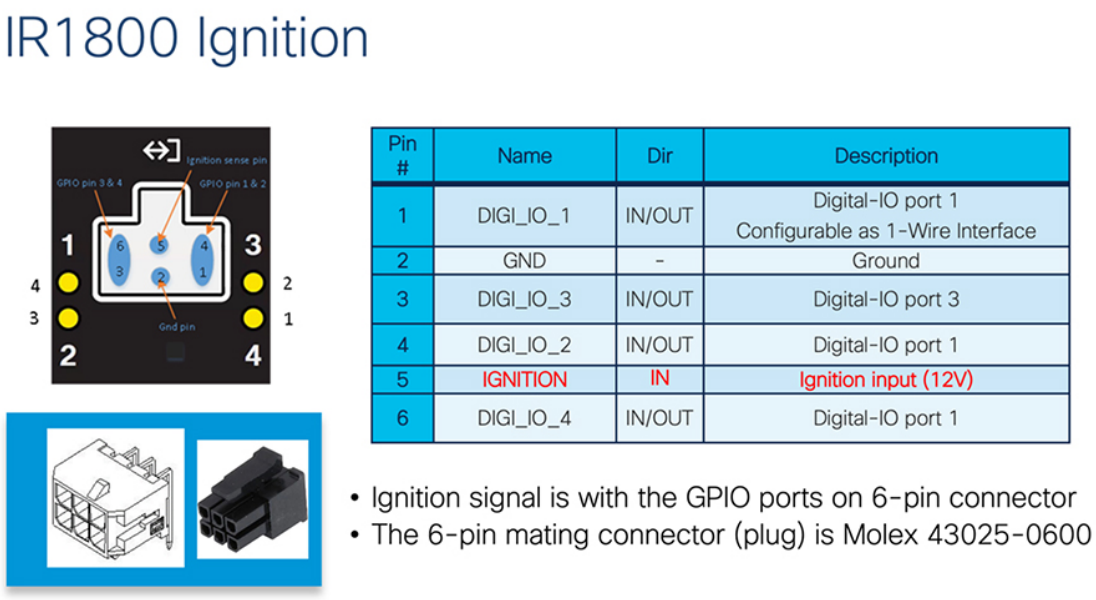
```
IR1800_FCW2445P8H8#show run | s ignition
ignition off-timer 300
ignition undervoltage threshold 9 000
ignition battery-type 12v
ignition sense-voltage threshold 13 000
ignition sense
ignition enable

IR1800_FCW2445P8H8#show ignition status
Ignition management: Enabled
Input voltage: 13.3 V
Ignition status: Power on
Ignition Sense: Enabled
Shutdown timer: 0.0 s to off [will begin power
down at ~100 sec]
Thresholds:
Undervoltage: 13.000 V
Overvoltage: 37.0 V
Undervoltage timer: 20.0 s
Overvoltage timer: 1.0 s
Ignition-Off timer: 300.0 s
```

388242

Ignition power management offers a similar experience to the end user, but instead of monitoring the input voltage (an analog value), the IR1835 router will look for a digital input on pin 5 of its GPIO port, that should be connected to the vehicle ignition signal.

Figure 8: Ignition Power Management – Digital Input



Pin #	Name	Dir	Description
1	DIGI_IO_1	IN/OUT	Digital-IO port 1 Configurable as 1-Wire Interface
2	GND	-	Ground
3	DIGI_IO_3	IN/OUT	Digital-IO port 3
4	DIGI_IO_2	IN/OUT	Digital-IO port 1
5	IGNITION	IN	Ignition input (12V)
6	DIGI_IO_4	IN/OUT	Digital-IO port 1

Fleet LAN and Subtended Switch for Port Expansion

Depending on the type and quantity of equipment that is installed on the vehicle, it may be necessary to add an additional industrial ethernet switch to expand the number of ports available. A subtended switch can also add more available PoE power for cameras, access points, and more. Cisco has a full line of industrial ethernet switches intended for a variety of industrial environments, and each model offers different port configurations, speeds, PoE power, and other features.

Figure 9: Cisco Industrial Ethernet Switches

An industrial ethernet switch can be connected to the upstream router LAN switchport. Both sides of the connection would typically be configured as trunk ports, assuming more than one VLAN (and corresponding service VPN) are required. The industrial ethernet switch itself is not managed or configured by vManage, but instead needs to be managed out-of-band which could include prestaging the switch with the required configuration, before it is physically installed.

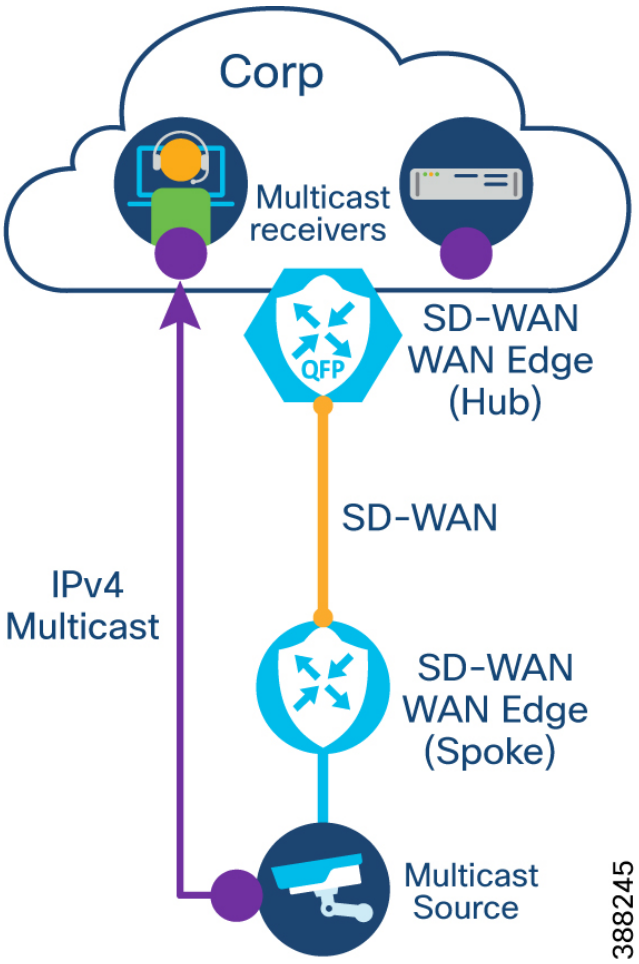
Video Security Cameras - Multicast Video

Physical security of the vehicle and other transit and fleet assets should include video cameras and the corresponding systems and software to record, manage, and view the video footage. The cameras, mounted

inside or outside, are wired back to the ruggedized router or subtended switch for data connectivity and power through the ethernet cable.

The video from the cameras can either be recorded on the camera or on an onboard DVR for later access, or it can be streamed over the network to various locations for live viewing. The video content is a valuable resource that could have potential use in security, analytics, or capacity planning, therefore it is recommended to setup the cameras to use multicast streaming based on RTSP or similar protocol. Multicast IPv4 relies on the underlying IGMP and PIM technologies to build the connectivity from source (camera) to destination (viewers, storage, etc.). A single video stream is sent from the camera to the SD-WAN Edge router acting as a multicast replicator – this router could be the hub in the hub-and-spoke topology, or another nearby router in the central location. The replicated streams are then sent to all hosts that indicate they are interested in receiving this video. This can greatly reduce WAN bandwidth utilization, especially if there are many video receivers, as only one stream needs to traverse the WAN.

Figure 10: Multicast Video from Spoke to Hub



For additional design and implementation details on multicast in an SD-WAN environment, refer to the Multicast Overlay Routing Overview:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-multicast-routing.html

Passenger Wi-Fi – Hotspot

The Cisco IR1800 series router supports a modular Wi-Fi6 access point that can be used to provide wireless connectivity for passengers, drivers, and any sensors or similar devices that are not connected via ethernet. In a typical mass transit deployment, it will be common to deploy multiple SSIDs, associated with different Service VPNs, to keep different types of devices and traffic segmented and secure. The passenger Wi-Fi service VPN could be setup for direct internet access, to offload the traffic from having to traverse the central hub router.

The access point module in the IR1800 router will operate in Embedded Wireless Controller (EWC) mode, when used with the Cisco SD-WAN solution. This mode allows the module to act not only as an access point, but as a small wireless controller as well. As a controller, other Cisco IOS-XE based wireless access points can register to it to expand wireless coverage in the case of a very large vehicle, for example.

Authentication for Wi-Fi clients can be done through WPA2 with pre-shared key (PSK), WPA2 with external RADIUS server, or open authentication. When deciding on an authentication method for Wi-Fi users in a mobile vehicle, the centralized control and IT system integration provided through RADIUS based authentication needs to be weighed against the potential for authentications to fail if the WAN connection is down.

Driver and Passenger Safety and Triggers - GPIO Alarming

Various digital sensors, panic alarms, and similar systems with a digital output can be connected to the GPIO interface in Cisco industrial routers. When triggered, the digital input could be used to generate an alert to be sent upstream to the security operations center. The router can also use the embedded event manager (EEM) or edge compute (IOx) resources for further processing of the input and take other action.

Cellular Artime Optimization

Mass transit and fleet vehicles need to rely on wireless connectivity exclusively, typically in the form of cellular (LTE or 5G). Cellular plans can be expensive and limited by monthly data caps. To minimize cellular bandwidth, there are several methods that can be used to reduce the management overhead required by Cisco vManage. These methods include using a hub and spoke design, increasing timers on BFD for link monitoring, and reducing statistics monitoring. For details, refer to the IoT Industrial Router Extension to SD-WAN Small Branch Design Case Study document.

Specific Design Considerations

Static NAT

When deploying static NAT mappings on the spoke routers, as described in detail in the “IoT Industrial Router Extension to SD-WAN Small Branch Design Case Study”, make sure that the SD-WAN Edge router at the central site that acts as the “hub” in a “hub-and-spoke” design can scale to the level required. Each static NAT entry will create a host route that is advertised by OMP to the hub router, this can quickly grow to thousands of routes in the routing table.