



Secure Cellular Roadways

Design Guide

June 2025



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.”

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

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

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

©2025 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Contents

Introduction..... 4

What’s new in connected roadways..... 5

Secure Cellular Roadways Architecture..... 6

Secure Cellular Roadways Reference Architecture 8

Secure Cellular Roadways - Design Considerations..... 10

LAN..... 25

LTE Timers Optimizations..... 43

Conclusions..... 44

Glossary..... 46

Introduction

Executive Summary

Cisco Industrial Routers with Cisco Catalyst software-defined WAN (SD-WAN) are the key enablers for a modern secure and scalable distributed field network – a network type commonly seen amongst roadways operators. Automated VPNs, zero-trust access, network segmentation, and getting visibility into the Operational Technology (OT) systems, as well as being ready for the next-generation of use cases in the roadways ecosystem; these are all things this Cisco Validated Design (CVD) solves for, prizing simplicity and operations at scale, without sacrificing security and digital resiliency.

Business Case

Intelligent Transportation Systems (ITS) are recognized as critical national infrastructure by the USA¹, the EU² and other developed countries and blocs. This means they are increasingly connected, instrumented and automated, allowing for optimal flow of people and goods; roadways being a cornerstone of ITS.

As roadways operators connect more ITS devices, and these ITS devices are in increasingly remote locations and/or locations that traditional WAN options (such as leased-line, MPLS), are either not available or cost-prohibitive, the use of cellular for WAN is widespread, and emerging technologies like Low Earth Orbit (LEO) satellite-based. However, connecting a large estate of ITS equipment using cellular brings challenges for both operational scalability and cyber security.

Connected Roadways

Roadways have always been connected – in the transportation sense – but connecting roadside devices in the data networking sense is relatively new. Since the 1970s the use of discrete serial connections (over copper twisted-pair wiring) has been prevalent, and in the early 2000s most of this transitioned to Ethernet and IP, aligned to the transition to ITS. This data connectivity exists to provide local synchronization between ITS elements. For example, so that a group of traffic signals/lights can effectively share information about road user volumes such that they can optimize traffic flows, but also so that ITS elements can be monitored, configured and troubleshot remotely – usually from a Traffic Management/Operations Center (TMC).

Recognizing that this data connectivity is to aid traffic engineering professionals in effectively completing their duties, for example, PTOE (https://en.wikipedia.org/wiki/Professional_traffic_operations_engineer).

¹ <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>

² https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

What's new in connected roadways

The adoption of the latest in Secure Networking

Given ITS is critical national infrastructure, the data networking that supports this is being refreshed to adopt the latest in secure networking paradigms. Cisco has seen an explosion in our ITS customers' adoption of Catalyst SD-WAN in conjunction with Cisco Catalyst Industrial Routers, and cellular being the most common WAN transport type. As discussed in detail below, the centralized policies and highly-automated nature of SD-WAN makes it the ideal foundation for a secure cellular roadways data network, for an ITS customer's distributed estate, but with low operational costs. Outside of ITS, all of the above is equally relevant for the broader roadways operations, be that Transportation Systems Management and Operations³ (TSMO) in the USA, or the local equivalent in other geographies.

Roadways ecosystem partners

Validating the architecture with key ecosystem partners ensures this design guide will deliver a solution that roadways operators will find useful, deployable and that addresses their needs.

[Q-Free](#) with their TSC, ATMS, and [Daktronics](#) with their DMS, participated with Cisco on this validated design.

Audience for Secure Cellular Roadways

This design guide is targeted at IT professionals who are tasked with designing and deploying connectivity for roadways, for system integrators and consultants, and of course for ITS professionals and Civil Engineers.

Other Relevant Documents

Cisco Catalyst SD-WAN Small Branch Design Case Study

(<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-casestudy-smallbranch.html>)

IoT Industrial Router Design Guide Extension to SD-WAN Small Branch Design Case Study

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

Six Ways to Secure Connectivity for Intelligent Roadways White Paper

(<https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/six-secure-conn-intel-roadway-wp.html>)

Robust Cybersecurity to Safeguard Roadways Infrastructure Solution Overview

(<https://www.cisco.com/c/en/us/products/collateral/security/robust-cybersecurity-safeguard-roadways-infra-so.html>)

³ <https://ops.fhwa.dot.gov/tsmo/>

Secure Cellular Roadways Architecture

Solution Requirements

High-level requirements that address the key data connectivity needs of an ITS system, while drawing from the latest Enterprise Networking and Security best practices.

Any transport, with a focus on Cellular

The solution needs to enable the use of all common standards-based WAN transports, and/or transports that present as a standards-based interface. It needs to seamlessly create VPN tunnels across these transports, with option for several in parallel. Given cellular often has usage costs, another requirement is that the data usage by the VPN is minimized, while still being fully featured.

Segmentation

Segmenting the data network into different zones has a lot of benefits, but specifically the logical segmentation to reduce the risk of contagion where a particular device or family of devices is compromised. For example, if the CCTV cameras are in a different logical network segment to the Traffic Signal Controller (TSC) – and there is no inherent reachability between these network segments – if the cameras were to be compromised (hacked), the TSCs would be separated and unreachable from the cameras. NIST SP 800-215

(<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf>) details the rationale.

The requirement is that our secure cellular WAN can support such a segmentation scheme. It does this across all the WAN transports a customer might need, and in a highly-automated and policy-based way.

Zero-trust Port Access

Also found in NIST SP 800-215 is the rationale behind adopting a zero-trust approach:

“Zero trust assumes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location (for example local area networks versus the internet) or on asset ownership (such as enterprise or personally owned). Zero trust focuses on protecting resources (such as assets, services, workflows, network accounts) rather than network segments, as the network location is no longer seen as the prime component to the security posture of the resource.”

The requirement is that our secure cellular WAN can support a zero-trust approach to port access, whereby ITS devices need to establish their identity, be permitted network access, and be placed in the appropriate network segment.

Visibility

Equally important are understanding what is connected to the ITS data network, be it ITS devices or otherwise, and understanding what these devices are communicating with. Getting this visibility ties directly back to both the network segmentation and the zero-trust port access. You can't secure what you can't see!

The requirement is that our secure cellular WAN can directly and indirectly provide the human operators and the IT systems the visibility they need to secure the ITS data network.

Cloud-connected Cabinets

Requirement that the solution has the architectural option to enable secure, specific and limited connectivity from a roadside cabinet through to the public cloud. This is in response to the emerging requirement that ITS devices are not just connected to TMCs and/or on-premises data centers and/or private clouds, but rather to

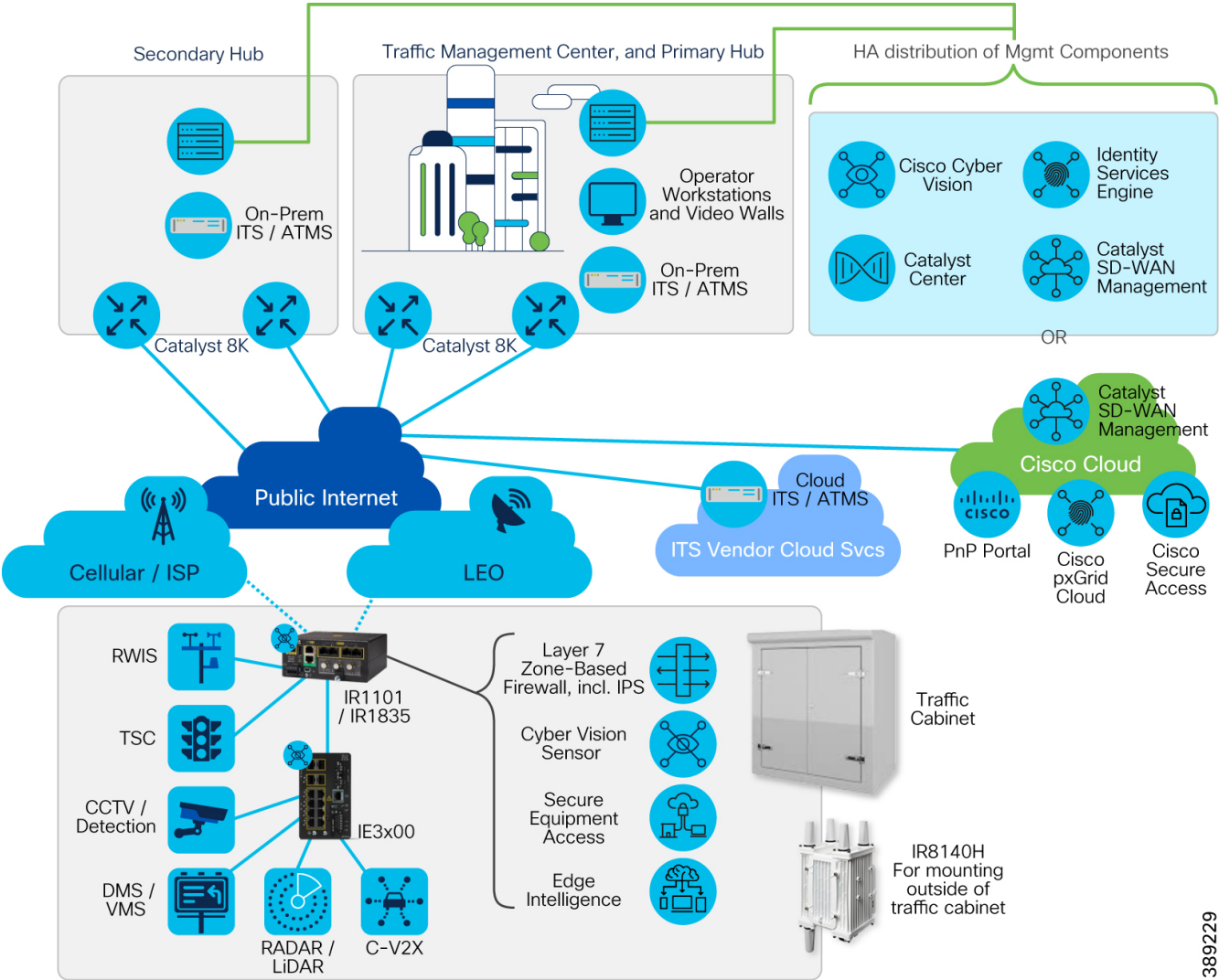
ITS backend systems and services running in public clouds, inc. cloud-delivered Advanced Traffic Management System/Intelligent Traffic Management System (ATMS/ITMS).

Technical Requirement Summary

Across segmentation, zero-trust port access, visibility and having an IT systems architecture that is ready for cloud-connected cabinets, it all starts with the need for zero-touch secure deployment of industrial secure gateways, especially on cellular networks. The industrial secure gateways must be part of an intent-based and software-defined network so that a large field network can be deployed and lifecycle-managed by a small team, and that is an overall system vs. many individual network components.

Secure Cellular Roadways Reference Architecture

Figure 1 - Reference architecture



Note: The ITS devices shown in Figure 1, for example RWS, TSC, and so on, is a non-exhaustive list. Many other ITS devices can be well-served by this architecture, with the focus being on those that are connected via wired Ethernet.

389229

Table 1 Secure Cellular Roadways Solution Components

Vendor	Model	Software Version
Cisco	IR1101	17.15.2
Cisco	IR1835	17.15.2
Cisco	IR8140H	17.15.2
Cisco	IR8340	17.15.2
Cisco	IE3400	17.15.2
Cisco	Catalyst SD-WAN	20.15.2
Cisco	Identity Services Engine	3.2
Cisco	Cyber Vision	5.2.0
Axis	3935-LR Camera	12.3.56
Daktronics	DMP-5000	20171219-v03
Q-Free	XN-1	ATC Linux 23.02.04 Maxtime 2.15.0

Secure Cellular Roadways – Design Considerations

Traffic Management Center

The TMC has traditionally been the most important site for a roadway operator, with larger operators having several TMCs, and/or a backup TMC. Operators, Technicians and Engineers can all use centralized systems at the TMC to monitor and manage the ITS. The roadways network architecture should be designed for staff located at a TMC have secure and reliable connectivity to a distributed ITS device estate, however it is also a design consideration to factor in the access for remote staff (for example, technicians in the field), consultants and vendors.

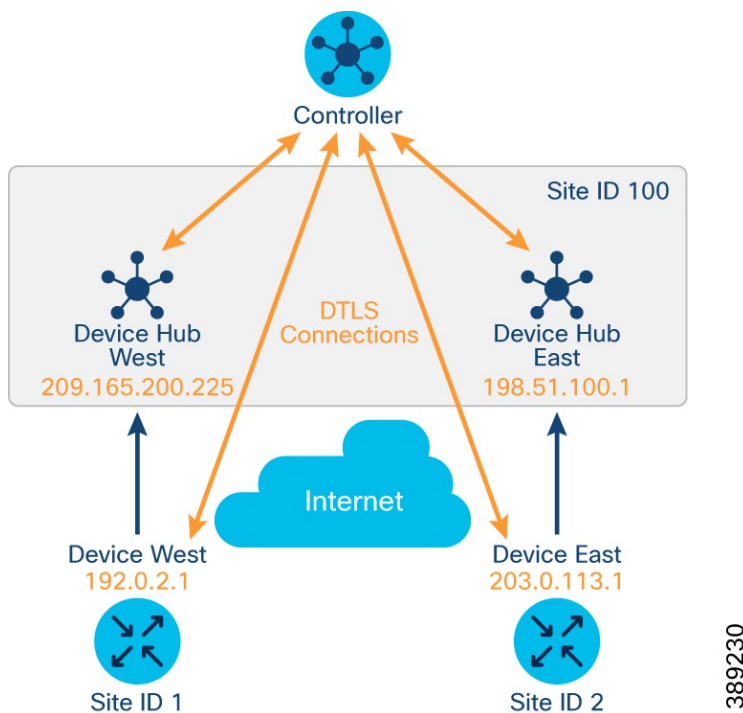
WAN Hub(s)

Choosing where to locate the WAN Hub or Hubs is often tied to the customer's disaster recovery / resiliency plan. Having a single WAN Hub location (that is where the WAN circuits from Telcos & ISPs are delivered to the customer) is acceptable, but most customers opt to have another location too. This second Hub site being significantly geographically separated from the first, helps mitigate against natural disasters and localized Telco/ISP outages.

It is common for customers to co-locate the WAN Hub with their TMC – traditionally the TMC has housed a Data Center including comms racks – but increasingly customers are disaggregating, leveraging co-location facilities and private clouds.

Fortunately, Catalyst SD-WAN simplifies this, and allows flexibility whether it is a single or multiple hubs. The WAN Edge routers can connect, as in form IPsec tunnels with, one hub at a time, or several hubs in parallel; centralized policy configuration can be used to control this (see “Creating Arbitrary Topologies” section of https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#c_Centralized_Data_Policy_Configuration_Examples_12228.xml)

Figure 2 - WAN Hubs



With dual hubs there are two main approaches:

- A. Having certain sites primarily homed to one hub or the other, with the backup path to the opposite hub, where the split between the hubs is shared (maybe 50% each).
- B. To have all sites homed to a primary hub, and the secondary hub is only used when the primary hub is not available.

In both cases the sizing of the routers at the hubs is very important, in terms of the immediate scale requirements and how these will change (often increase) over time.

For example, the Catalyst 8500 series is a good choice to aggregate many SD-WAN tunnels at a hub location, and sizing both the number of tunnels and the aggregate traffic across those tunnels is equally important, for example [Table 5a](#) of the Catalyst 8500 Data Sheet.

When there are two or more WAN Hubs the routing between them, and more specifically the advertisement of prefixes at the edge sites (reference <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-casestudy-smallbranch.html#DCtoDCRouting>)

At the Edge: One router, or Two

At the edge location/site, which is typically a traffic cabinet, one router (WAN Edge) is usually deployed. This one router may have multiple WAN transport connections, for example. two different LTE/5G modems and/or a Gigabit internet circuit, and multiple connected ITS devices. However, it is a single router, and therefore, a single point-of-failure shown in Figure 3.

Figure 3 - A single router site

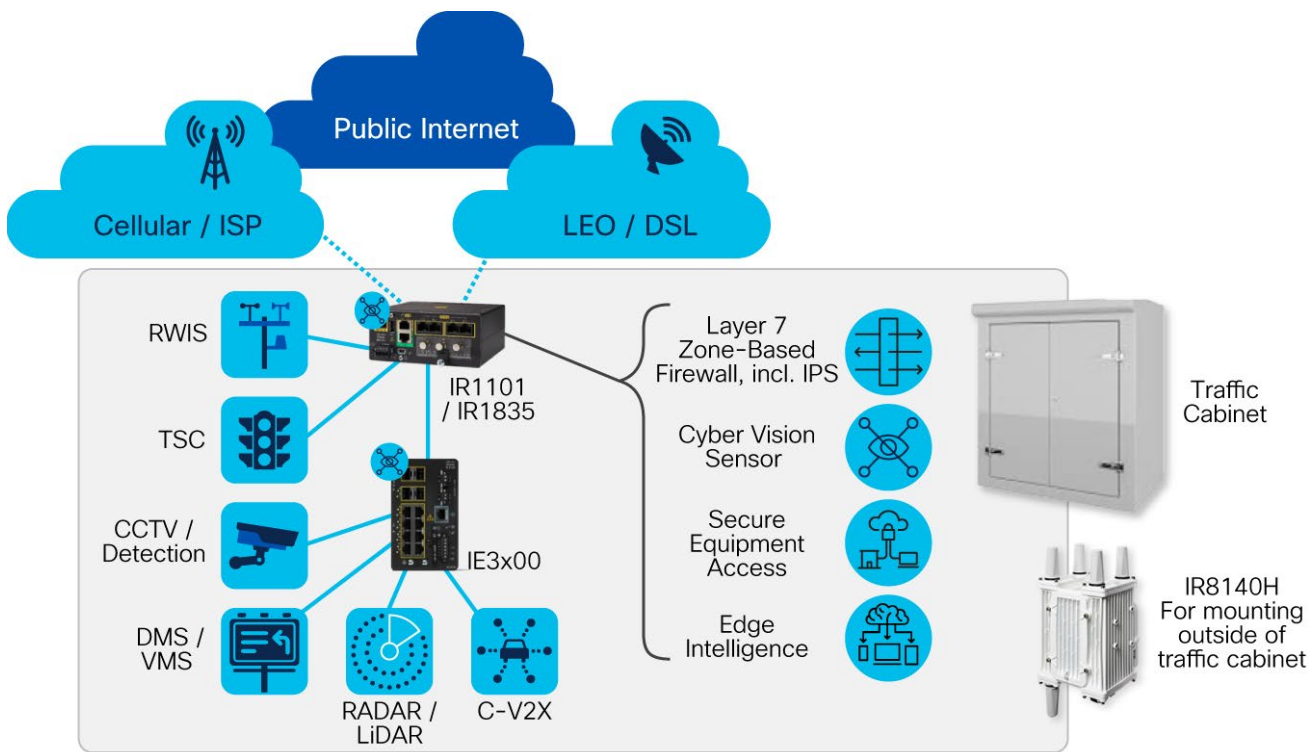
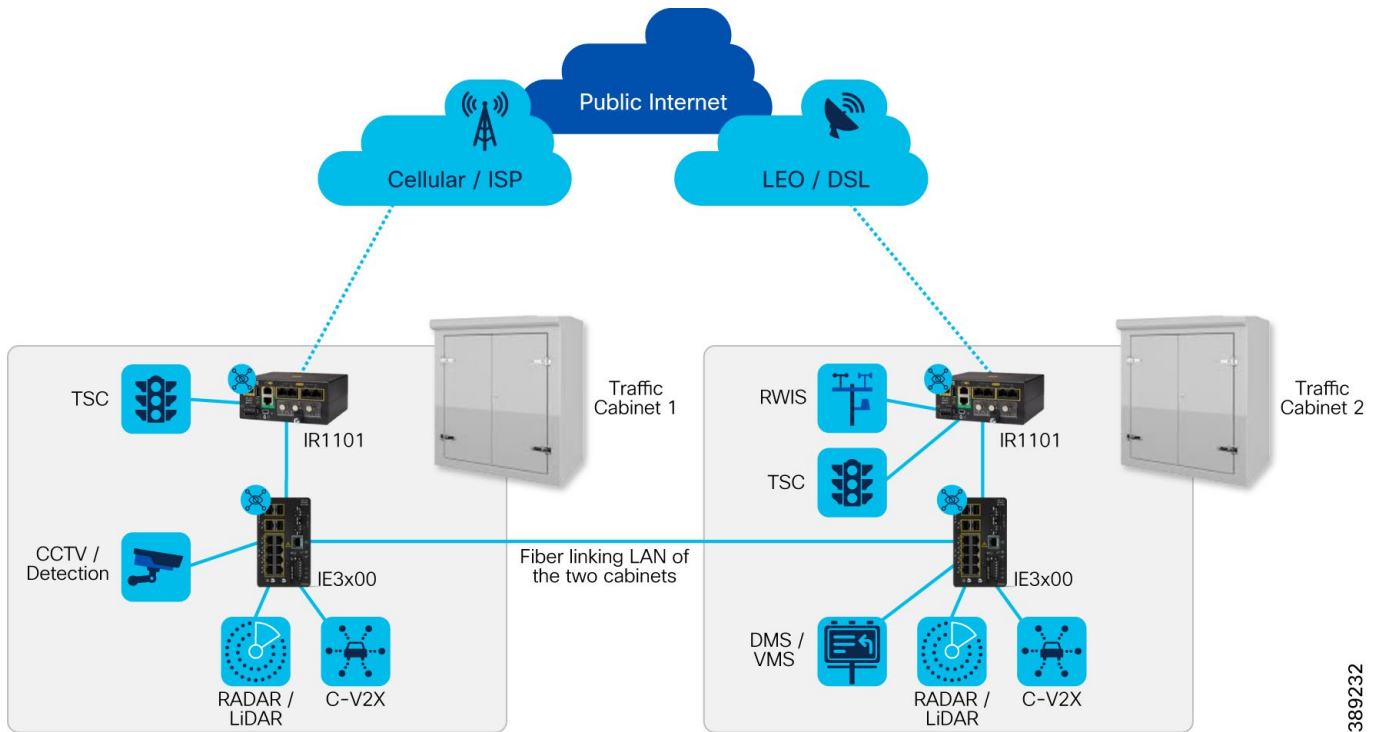


Figure 4 shows two WAN transports: Cellular and Low Earth Orbit Satellite (LEO), however many transport types are possible, and discussed in [WAN Transport options](#).

For critical locations or sites, two routers can be deployed.

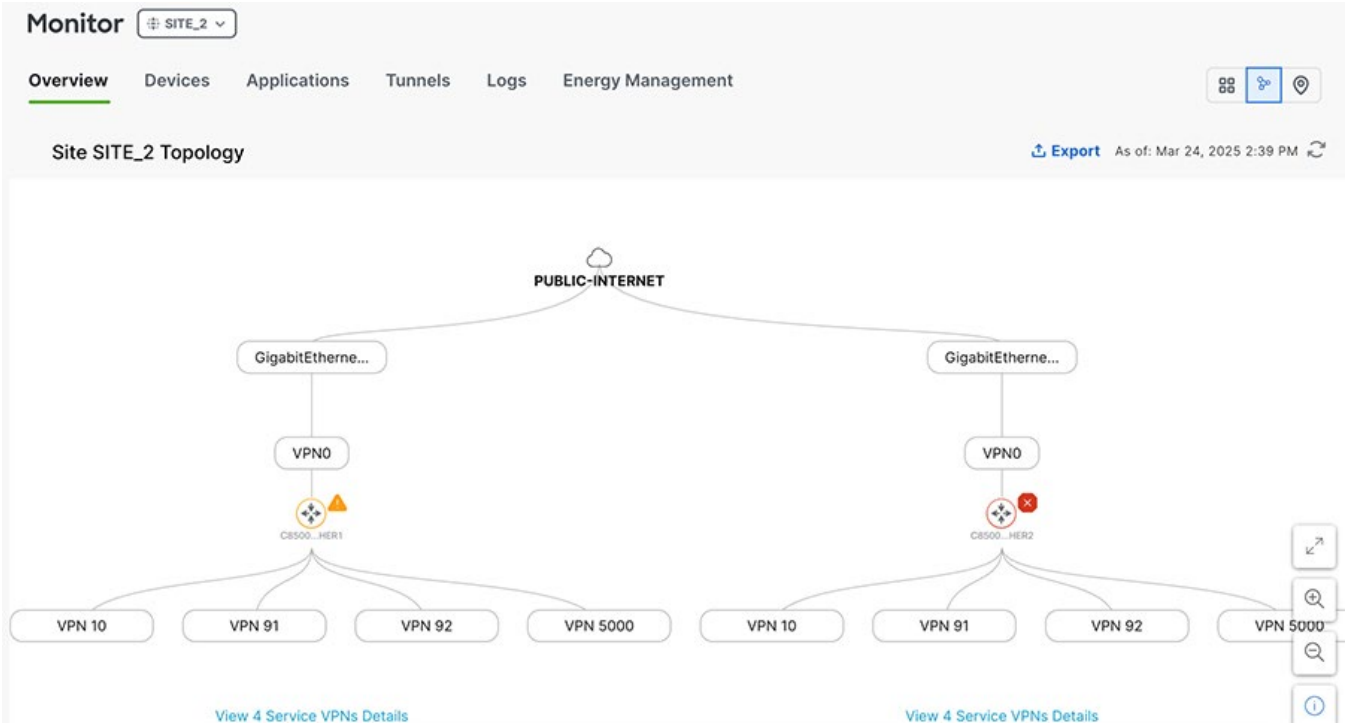
Figure 4 - A dual-router site



With a dual-router site, the LAN segment(s) is/are shared between the two routers, and a first-hop-redundancy-protocol (FHRP) is used to resiliently share the default-gateway for that LAN segment(s) between the two routers – VRRP can be configured via SD-WAN Manager. Also, the two routers can be somewhat geographically separated – they do not need to be in the same traffic cabinet; this allows for the site to be a logical vs. strictly being a physical construct.

Note: Each router can have its own Latitude and Longitude values, which can be dynamically learned if a GNSS antenna is connected and GNSS is correctly configured. Alternatively, Latitude and Longitude values can be manually specified by the administrator.

Figure 5 - A dual-router site (a Hub example), in Catalyst SD-WAN Manager



(reference <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#WANEdgeDeployment>)

For mounting inside a traffic cabinet, the Cisco Catalyst Rugged IR1101 and IR1835 are well-suited and widely deployed by customers today, with the IR8340 also being an option for larger cabinet and/or more demanding use cases. Some customers prefer to mount outside the traffic cabinet, and the Cisco Catalyst Heavy Duty IR8140H is a great fit, being IP67 rated and pole-mounted. All the Cisco secure gateways can support dual active LTE/5G connection, be Gigabit fiber connected, and so on.

Table 2 - Cisco IRs

Cisco IR model	LTE/5G	Gigabit Fiber Ethernet (via SFP ⁴)	Copper Ethernet ⁵
IR1101	Yes, up to 3 (active-active-active)	Yes, up to 2	Yes, up to 8
IR1835		Yes	Yes
IR8140H	Yes, up to 2 (active-active)	Yes	Yes
IR8340		Yes, up to 10	Yes, up to 10

⁴ SFP port can be used as an additional copper Ethernet port (e.g. 1000BASE-TX) as required, via a supported pluggable.

⁵ Ethernet ports on Cisco IRs are denoted as “WAN” and “LAN”, however there is flexibility to use a WAN port as a LAN port by configuring it as “switchport”, equally a LAN port can be used as a WAN port by configuring an SVI as the WAN interface.

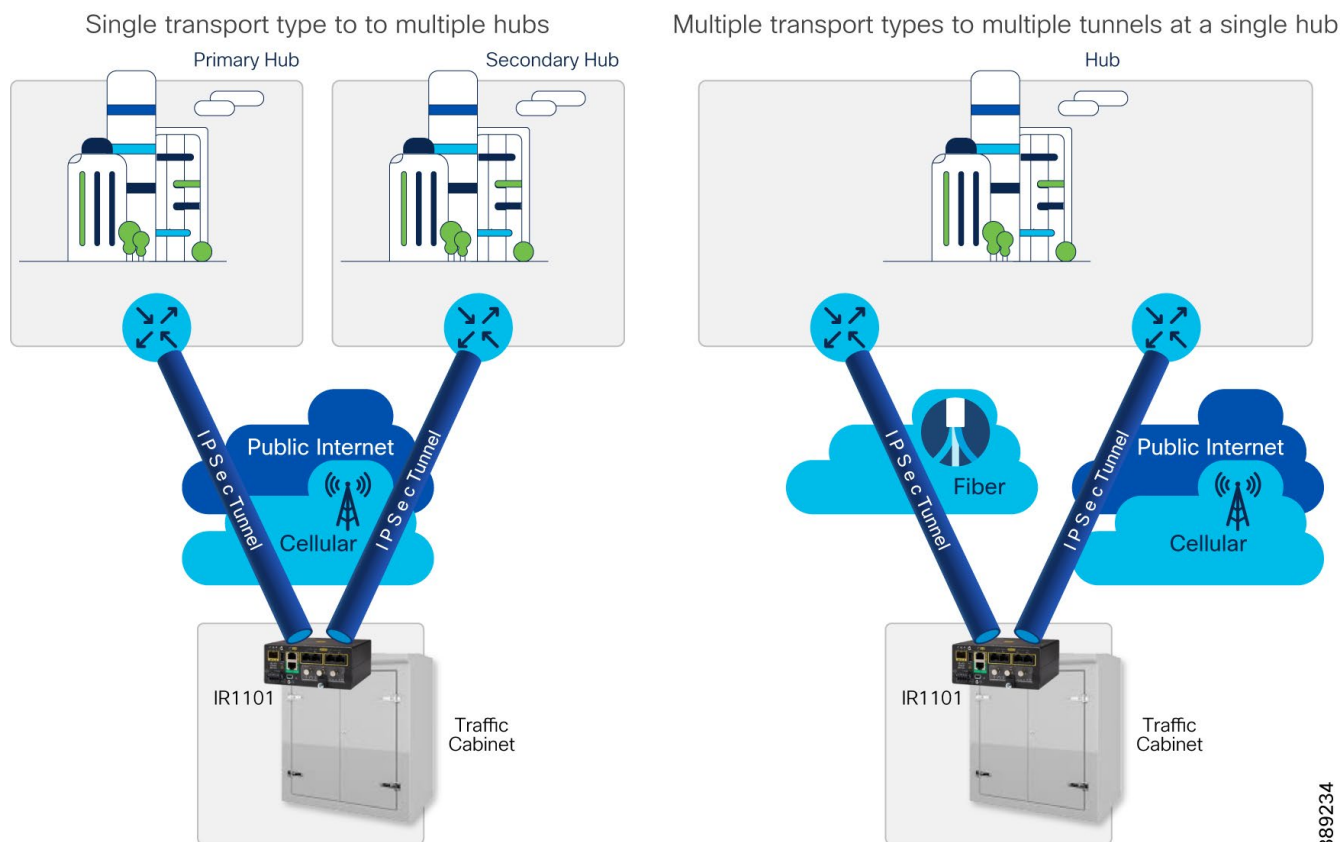
WAN Transport options

A WAN Edge router may connect back to one or more WAN Hubs via one or several so-called Transports.

From an SDN perspective, the Transports are part of the underlay (see <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#UnderlayvsOverlayRouting>), and tunnels are formed over the transport connections: IPsec for an encrypted tunnel, GRE for an unencrypted tunnel. Even if the underlay network is considered as “trusted” or secure, GRE tunnels then enable the segmentation and security tagging discussed later in this design guide.

A WAN Edge router can use a single transport type to form tunnels to multiple hubs, and it can use multiple transport types to form multiple tunnels to a single hub as seen in Figure 6.

Figure 6 - Transports and Hubs



389234

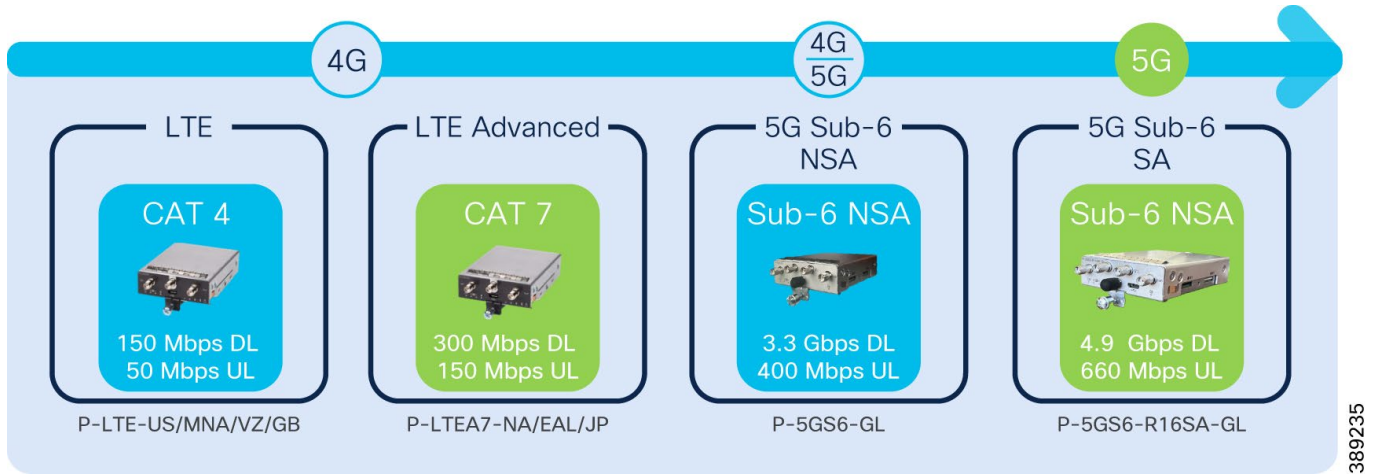
The “Color” of the transport is a static label, as is part of the Transport Locator, or TLOC (see <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#TransportLocatorsTLOCs>);

Note: there is currently no label for 5G, and even though 3G has been sunset as a cellular technology, it is still acceptable to use the “3G” TLOC color, because this is just a label.

Public cellular is ubiquitous, and often the only WAN transport type that is available consistently across the entire physical area the roadway operator covers. With the deprecation of 3G variants of cellular, the most commonly available is 4G/LTE, with increasing amounts of 5G.

Cisco has a range of cellular pluggable interface modules (PIMs), which allows the selection of modules most appropriate to the frequency bands available from local carriers, and the data rates required; plus allows for future additions and upgrades. For example, a Cisco IR can start with one lower-speed 4G PIM, add a 5G PIM, and replace the initial 4G PIM with a faster one.

Figure 7 - Cellular PIMs



Interface type: Cellular

Suggested TLOC paradigm: Public

Suggested TLOC color(s): lte, 3g

Private Cellular

Cellular is also available privately operated, although this is less common for roadways operators to have access to it; a private Access Point Name (APN) on a public cellular network is typical. The key element impacting the design is whether such a network is thought of as public or private by the customer, and whether NAT is required. If the cellular is thought of as private, and trusted, GRE could be used as the tunnel encapsulation; Cisco always recommends IPsec for increased security.

Interface type: Cellular

Suggested TLOC paradigm: Private

Suggested TLOC color(s): private1, private2

Satellite

Satellite connections, especially those based on Low Earth Orbit (LEO)-type satellites, are increasingly an option for roadways operators; providing coverage in areas that even public cellular does not cover or enabling public cellular to be used as a backup to a LEO primary.

The Cisco SD-WAN Solution Engineering team has done extensive testing using Starlink, for example, please refer to <https://community.cisco.com/t5/networking-knowledge-base/catalyst-sd-wan-quickstart-guide-for-using-starlink/ta-p/5112291> and <https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink> for specific guidance with respect to configuring Catalyst SD-WAN to work best with Starlink.

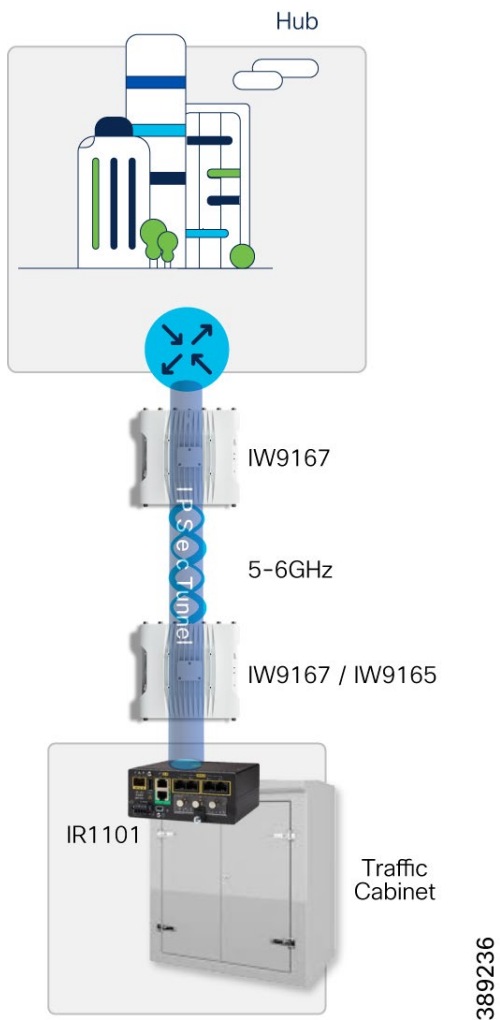
Interface type: Ethernet or SVI

Suggested TLOC paradigm: Public

Suggested TLOC color(s): biz-internet

Line-of-sight Radio

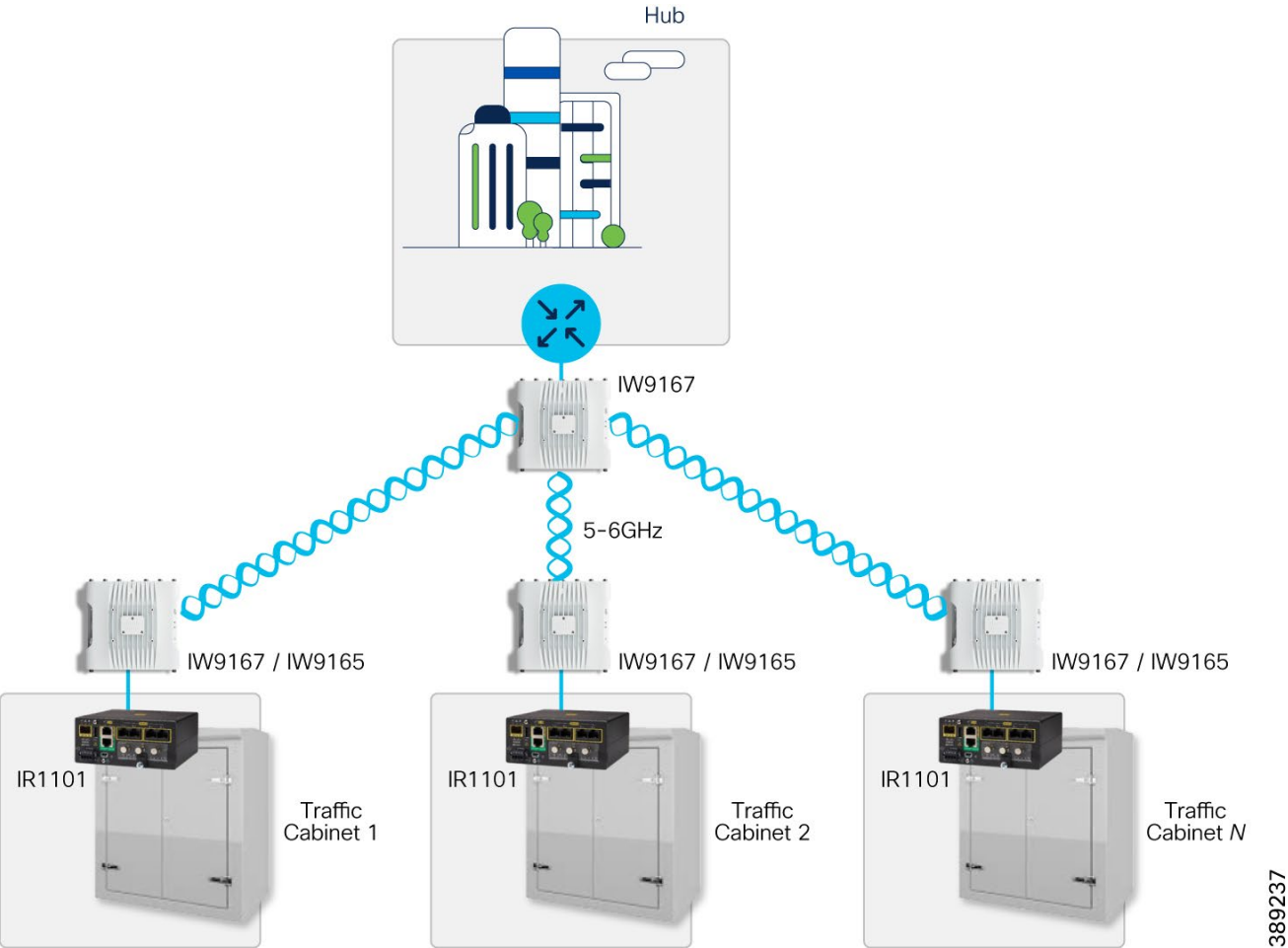
For a group of nearby intersections/junctions and/or other roadside ITS assets, in the absence of physical cabling between these locations, the use of line-of-sight radios is quite common. Here Catalyst SD-WAN can use these a line-of-sight radio as WAN Transports, as they are Ethernet-based; the Cisco Industrial Wireless portfolio (<https://www.cisco.com/site/us/en/products/networking/industrial-wireless/index.html>) has been tested in this capacity, with the IW9167E (<https://www.cisco.com/site/us/en/products/networking/industrial-wireless/catalyst-iw9167-series/index.html>) being particularly well suited.

Figure 8 - Point-to-point IW9167 radio link

Typically, a simple point-to-point topology is used, however point-to-multipoint can also be used. The multipoint network segment is typically an IP subnet in RFC1918 address space. The multipoint aggregation is typically done at a customer high-site and/or central building, which may be a TMC.

Please note that point-to-point radios can also be used between cabinets, side-to-side, as shown in Fig. 4. Here the IW9165D (<https://www.cisco.com/site/us/en/products/networking/industrial-wireless/catalyst-iw9165-heavy-duty-series/index.html>) has been tested and is well suited.

Figure 9 - Point-to-Multipoint WAN transports



Interface type: Ethernet or SVI
Suggested TLOC paradigm: Private
Suggested TLOC color(s): private1, private2

389237

Fiber

The use of fiber optic cables at the roadside, is more traditionally associated with an Ethernet Switching-based architecture, however all the Cisco Catalyst IRs support using a Fiber Ethernet connection as a WAN transport.

Table 3 - Fiber Ethernet WAN port options on Catalyst IRs

SFP	Distance	Fiber type	Classification ⁶
GLC-SX-MM-RGD	220-550 m	MMF	Industrial (-40C to +85C)
GLC-LX-SM-RGD	550m / 10 km	MMF / SMF	Industrial (-40C to +85C)
GLC-ZX-SM-RGD	70 km	SMF	Industrial (-40C to +85C)
GLC-SX-MMD	220-550m	MMF	Extended (-5C to +85C)
GLC-LH-SMD	550m / 10 km	MMF / SMF	Extended (-5C to +85C)
GLC-ZX-SMD	70 km	SMF	Extended (-5C to +85C)
GLC-BX-U	10 km	SMF	Commercial (0C to +70C)
GLC-BX-D	10 km	SMF	Commercial (0C to +70C)
GLC-LH-MMD	550m / 10km	MMF / SMF	Extended (-5C to +85C)
GLC-EX-SMD	40 km	SMF	Extended (-5C to +85C)
GLC-FE-100FX-RGD	2 km	MMF	Industrial (-40C to +85C)
GLC-FE-100LX-RGD	10 km	SMF	Industrial (-40C to +85C)
GLC-FE-100FX	2 km	MMF	Commercial (0C to +70C)
GLC-FE-100LX	10 km	SMF	Commercial (0C to +70C)
GLC-FE-100EX	40 km	SMF	Commercial (0C to +70C)
GLC-FE-100ZX	80 km	SMF	Commercial (0C to +70C)

⁶ **Note:** the Industrial rating (-40C to +85C) is typically needed for a traffic cabinet, especially to comply with NEMA TS/2 in the North American market.

SFP	Distance	Fiber type	Classification ⁶
GLC-FE-100BX-U	10 km	SMF	Commercial (0C to +70C)
GLC-FE-100BX-D	10 km	SMF	Commercial (0C to +70C)

With options for both Multi-mode (MMF) and Single-mode (SMF) fiber, and distances between 100m and 80km, there is a large range of pluggable optics available for the Catalyst IRs (please check directly with latest respective Catalyst IR datasheet on cisco.com for the latest information).

There are design options for connecting to the fiber network, where the connection can either be as a routed/WAN port, or as a Switch Virtual Interface (SVI); the former being preferred, and the latter typically being used when there is not enough available of the former.

The fiber Ethernet connection might be into the roadway operator's existing private fiber network, and here it is more likely that a static IP address will need to be applied to the interface. Conversely if the fiber Ethernet connection is to an ISP, here it is more likely that the interface will be configured to request a DHCP lease (this is also true if the ISP connection is copper-based, for example, 1000BASE-TX).

Interface type: Ethernet or SVI

Suggested TLOC paradigm: Private

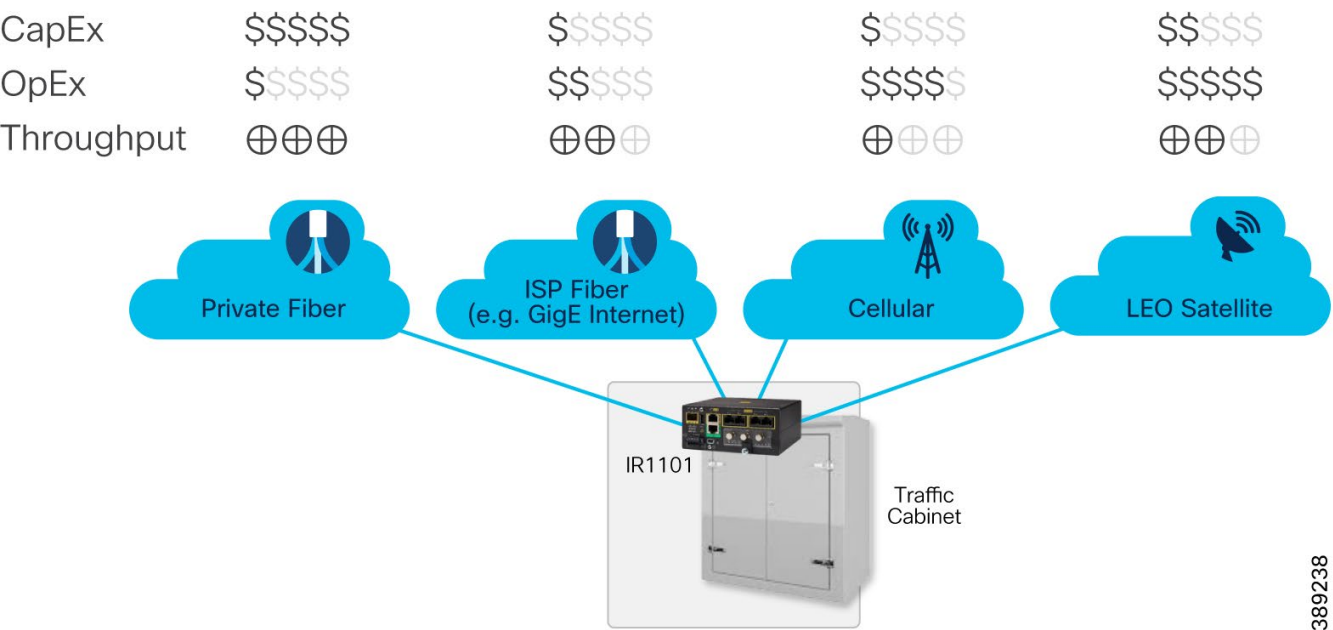
Suggested TLOC color(s): metro-ethernet

Selecting and Combining

Choosing or selecting which WAN transport(s) are the best fit for a given location is often a mixture of have some choice and having no choice. For example, fiber is often desirable, given with private fiber there is no data usage cost, and it is high throughput and low latency. If fiber is not present at the location there is a high capital cost to install and, and usually a low lead-time. Comparing this to public cellular, usually data usage costs, but just need to source a SIM card to get connected instantly.

Given Cisco Catalyst SD-WAN is transport-independent, a big benefit is that several WAN transports can be used across a deployment area. For example, some (very remote) locations using LEO, other (remote/rural) locations using cellular and some (urban) using fiber or line-of-sight radios – all are simultaneously possible within a customer installation, including several mobile carriers.

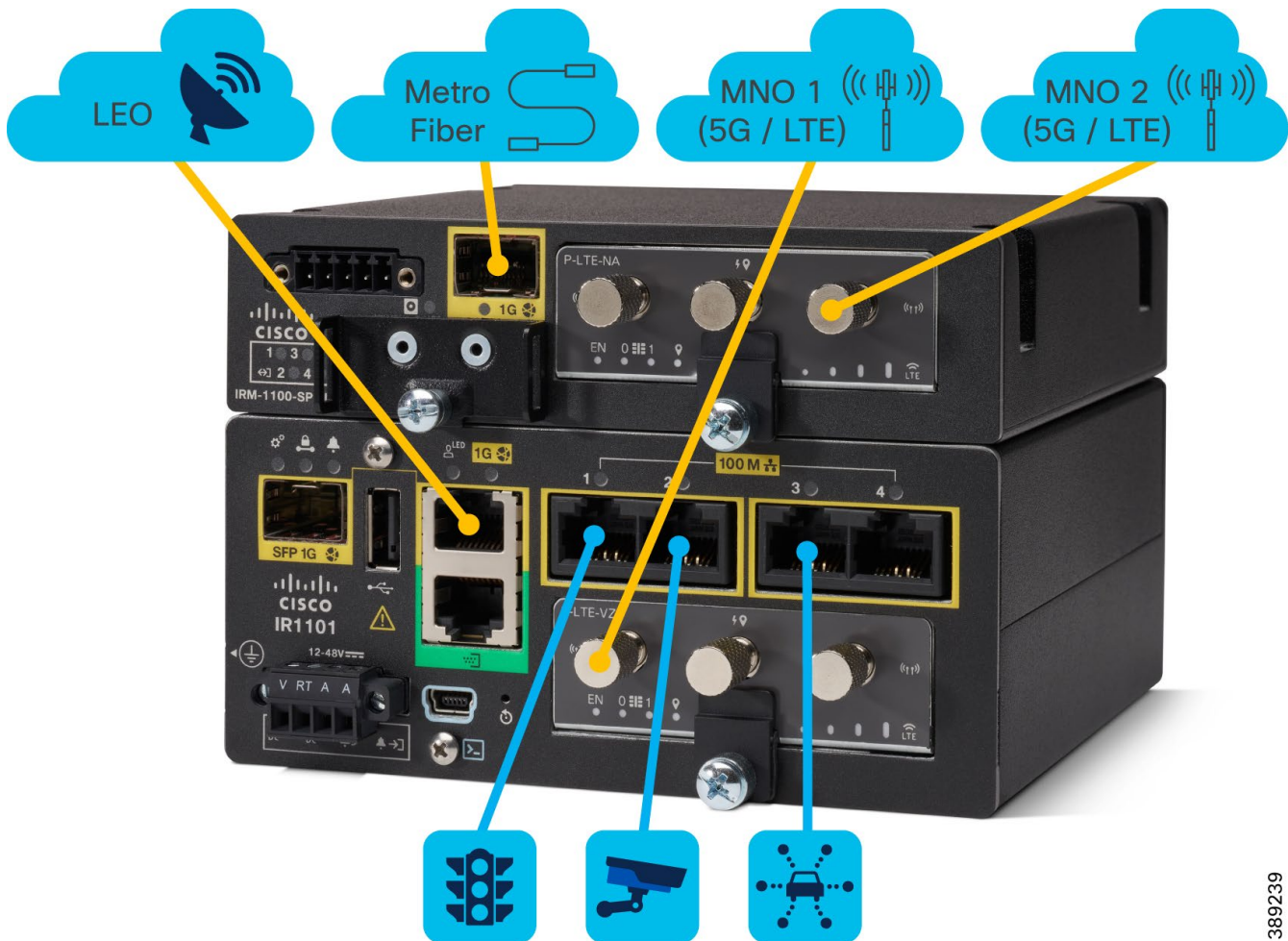
Figure 10 - WAN transport selection



389238

Additionally, Catalyst SD-WAN really shines when several WAN transports are used simultaneously at a remote location; this could be in active-backup or active-active. Active-active in particular is an area where traditional routing and VPNs struggle, as it is very complicated to configure a router to do something other than load-balance, round-robin or equal-cost-multipath (ECMP) across the multiple transports. With Catalyst SD-WAN this active-active behavior can be powerfully yet simply controlled using a centralized policy. The centralized policy is a real instantiation of software-defined networking and SD-WAN, where network traffic is classified and subject to quality measurements, and these are part of the routing/pathing decision making.

For example, at a remote location that has several ITS devices, these being of different types, and has three WAN transports shown in Figure 11.

Figure 11 - Remote location with multiple WAN connections and multiple ITS devices

389239


A centralized policy can be used to steer the CCTV traffic over the Metro Fiber connection, and the network traffic related to the TSC. If the SLA configured for the TSC fails, then the TSC network traffic can be sent over AT&T FirstNet cellular connection. At this time the CCTV traffic could be de-prioritized as it goes over FirstNet or even not sent at all.


Figure 11 shows a US-based example where MNO 1 could be Verizon Frontline, for example, the Metro fiber likely customer-owned, and MNO 2 could be T-Mobile⁷. In addition to Starlink being used for LEO satellite comms. Catalyst SD-WAN will build secure tunnels across all these three transports, with policy control to send CCTV traffic across the fiber, and ATMS traffic DIA out of MNO1 to a cloud-based ATMS. Similarly, there is policy control to route CCTV over MNO2, if fiber is disconnected, but the CCTV traffic is given a lower QoS priority, and traffic-shaped down to a lower bitrate.

Having an IR1101 with four WAN transports, all of which can be active at the same time, may be a slightly extreme example, but it should the flexibility and power of Catalyst SD-WAN to provide customers with maximum connectivity.

⁷ At time of publication Cisco has not completed certification against T-Mobile's T-Priority service for critical infrastructure – this certification is planned.

Figure 12 - SLA Policy

Policies > Application Priority & SLA
OT-Applications 

[Additional Settings](#) [Advanced Layout](#) 

SDWAN Fabric Traffic Policy Default Action ☐ Accept ☒ Drop

Gold Business Relevant	Preferred Path 1x gold	When SLA not met Fallback to Best Path	Backup Path Not Applicable
Silver Default	Preferred Path 1x silver	When SLA not met Fallback to Best Path	Backup Path Not Applicable
Bronze Business Irrelevant	Preferred Path 1x bronze	When SLA not met Fallback to Best Path	Backup Path Not Applicable

Internet Offload Traffic

Secure Internet Gateway	Application List Select Application List	Fallback to Routing <input type="checkbox"/>
Direct Internet Access	Application List Select Application List	Fallback to Routing <input type="checkbox"/>

Apply Policy

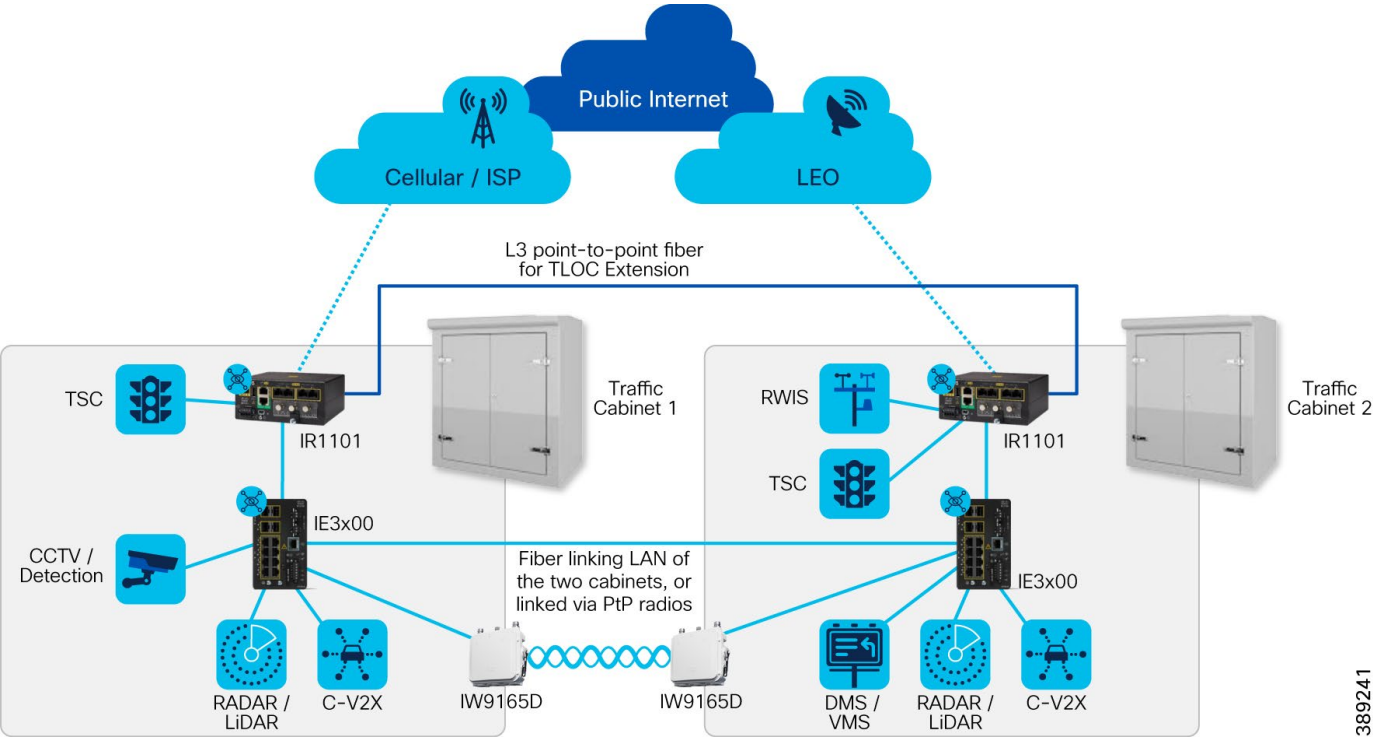
Target	Traffic Direction All	Traffic VPN(s) Service_VPN1	QoS Interface(s) Enter Comma separated QoS Interfaces <input type="button" value="Value"/> <input type="button" value="Variable"/>
--------	--------------------------	--------------------------------	--

It should be noted that the default for TLOCs is “unrestricted”, insofar as once there are two or more transports they will all try and form VPN tunnels with one another. This can lead to inefficiencies, as most transports cannot reach each other, and the WAN Edge routers will try forever to contact one another. It is recommended that most if not all TLOCs are set to “restrict”. Please see

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-casestudy-smallbranch.html#ColorRestrict> for more details.

Referring to the dual-router site example discussed in the “At the Edge: One router, or Two” section of this design guide, this can be enhanced to take advantage of the [TLOC Extension](#) concept. Here a point-to-point routed link is established between two IRs, for example, using GigabitEthernet 0/0/0 port. This allows the IR in cabinet #1 to leverage the WAN transport(s) in cabinet #2, and vice-versa. Setting this up for efficient use of WAN transports at the remote site, active-active across the two cabinets, rather than the IR and transports in cabinet #2 only being used in the event of an outage related to cabinet #1.

Figure 13 - Dual-router site, with TLOC Extension



Note: a shared fiber bundle can be used for both the L3 and L2 links between the cabinets shown in Figure13, but these are separate pairs within the bundle.

LAN

Onboard LAN

All Cisco Catalyst IRs come with at least one Ethernet LAN port, most come with four, and some IRs can be expanded with additional modules containing further LAN ports.

Table 4 - Ethernet LAN port options for Cisco IRs

Cisco IR model	Gigabit Fiber Ethernet via SFP (Max)	Copper Ethernet (Max)
IR1101	1 (3)	4 (8)
IR1835	1	4
IR8140H	1	1
IR8340 ⁸	10	10

The Max figures in Table 4 are achieved by using add-on modules. Figure 14 shows an example where an IRM-1100-4A2T module has been added to an IR1101, which results in two additional LAN ports: 2 x 10/100/1000Mbps in addition to the 4 x 10/100Mbps found in the base unit.

Figure 14 - IR1101 with an IRM-1100-4A2T module



These LAN ports are designed to connect either direct host devices, for example, ITS devices such as a TSC, RWIS, and so on, or be a trunk port to a downstream network switch where the ITS devices are connected.

⁸ Four of the IR8340s Ethernet ports are fixed Copper and four are fixed SFP, the rest are “Combo” ports that can be set to either Copper or SFP. As the Copper pluggable can be used in an SFP port, hence the IR8340 can have up to 12 Copper ports in total, although only eight of these can be used to deliver the IR8340’s 60W PoE budget.

When the devices are directly connected it is a best practice to enable port authorization, discussed further below.



It is possible to use “WAN” Ethernet interfaces (as denoted by  symbol) as LAN Ethernet interfaces (as denoted by  symbol).

Figure 15 shows an IR1101 with an IRM-1100-4A2T module, and where the WAN port is used as a LAN port. This gives a total of seven LAN ports.

Figure 15 - IR1101 with an IRM-1100-4A2T module, and WAN port used as LAN port



Figure 16 shows an IR1101 with IRM-1100-SPMI and IRM-1100-4A2T modules, and where the WAN ports are used as LAN ports. This yields a total of eight LAN ports.

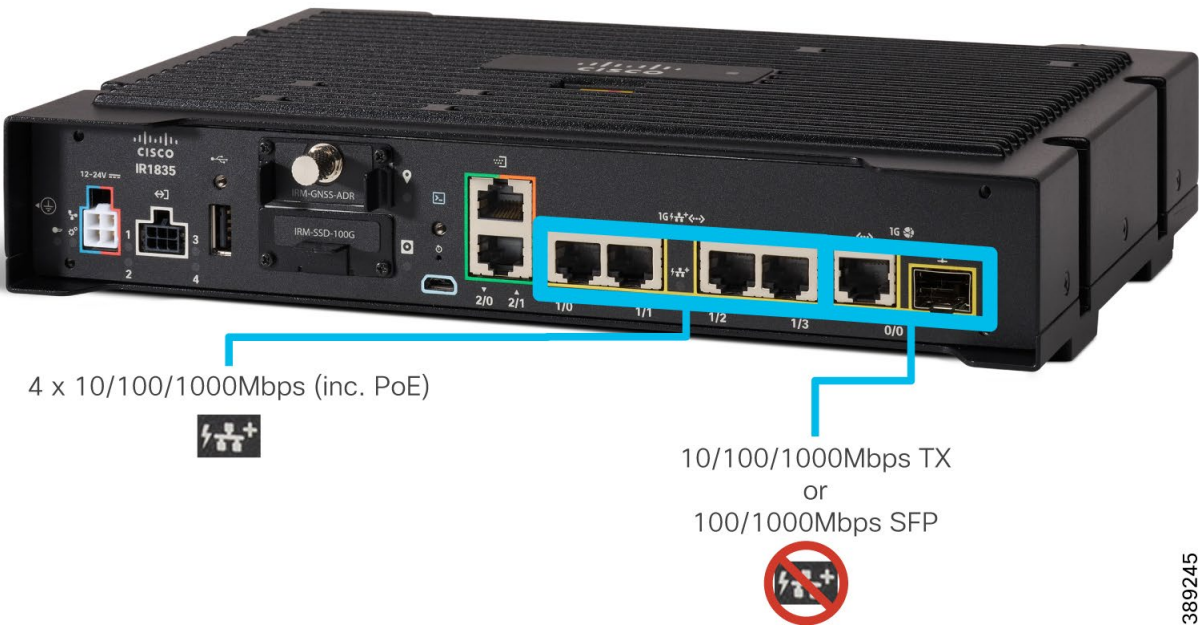
Figure 16 - IR1101 with IRM-1100-SPMI and IRM-1100-4A2T modules, and WAN ports used as LAN ports



This provides extra Ethernet ports, which can be used as access ports for hosts, or as downlink ports to a switched segment; here it is common to see the SFP port(s) being used with an SFP to give a SMF connection.

For the IR1835 note the PoE capability (30W to one port, or 15.4W to two ports) only applies to the four onboard LAN Ethernet ports (Gi0/1/0 - 3), and not to the WAN port, (Gi0/0/0) as shown in Figure 17.

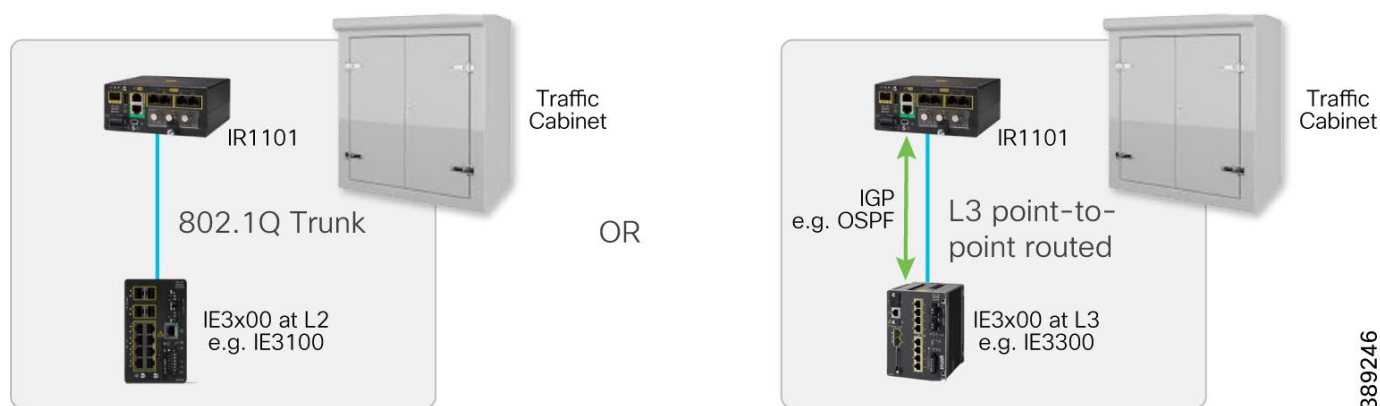
Figure 17 - IR1835



Extended LAN with IE Switches

If the number of LAN ports exceeds that on the IR itself, or for reasons of an expanded physical topology, it is quite common for one or more Cisco Industrial Ethernet (IE) switches to be added. Connectivity from the IR to IE(s) is via a “trunk” (this is based on 802.1Q tagged traffic); here the switches are usually in a Layer-2 mode helping to manage several Virtual LANs (VLANs), with the LAN gateway function running on the IR. The gateway function is realized through using an SVI, or multiple SVIs in the case of more than one VLAN.

Figure 18 - Extended LAN



It is also possible for the IE switch(es) to be in a Layer-3 mode; an interior gateway protocol (IGP) relationship is established between the IE and IR, with options for OSPF, BGP and EIGRP. Route update into and out of this IGP can be shared with the rest of the SD-WAN overlay automatically via Overlay Management Protocol (OMP) – however this is limited by default to stay within the particular Service VPN (please see [Segmentation](#) section for more details on Service VPNs, and please see

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html> for further details on configuring routing protocols in Service VPNs).

Cyber Visibility

Cisco Cyber Vision gives users an in-depth view of their operational technology (OT) security posture. It can identify all their industrial assets and see how they’re communicating. Cyber Vision builds visibility into the network infrastructure, allowing the user to know what actions to prioritize by understanding their OT security, and spotlighting devices that need immediate attention and suggested solutions.

Cisco SD-WAN now supports the deployment of Cyber Vision on edge devices via a feature profile in the SD-WAN user interface, created as “Other Profile” and adding to it “Cyber Vision” as a feature. The recommended procedure to deploy Cyber Vision in SD-WAN is as follows:

1. Create a new configuration group “A” or install it via a Catalog entry.
2. Copy the configuration group “A” creating group “B” and attach to it a Cyber Vision feature profile
3. Assign an edge device to group A and deploy the configuration.
4. Assign the same edge device to group B (forcing Cyber Vision deployment) and deploy the configuration.

The dual deployment step is needed because the device networking needs to be configured first via group “A” before Cyber Vision can be installed on the device via group “B”. Future Catalog entries will have one group without an identical one with Cyber Vision feature. User will then install both versions of the Catalog and assign the edge device to one and then the other to complete the Cyber Vision app installation. Figure 19 is an example of a Cyber Vision feature profile which must be created after first adding the Cyber Vision Center in SD-WAN UI under **Configuration>Network Hierarchy>External Services**.

Figure 19 - Screenshot from Catalyst SD-WAN Manager 20.15, for configuring Cyber Vision Sensor

Cyber Vision

Name
Cyber_vision_app

Description (optional)
Cyber Vision Feature Profile

☒ Base Configuration
 ☒ Advanced Configuration

Base Configuration

Cyber Vision Center
 CV-VPN-0

Monitoring Source Interface

Advanced Configuration

Capture Interface IP <input type="button" value="⊙"/> <system default>	Capture Interface Subnet Mask <input type="button" value="⊙"/> <system default>
Collection Interface (Sensor to Center) IP <input type="button" value="⊙"/> {{ Sensor_to_Center_IP }}	Collection Interface Subnet Mask <input type="button" value="⊙"/> {{ Sensor_to_Center_Subnet_Mask }}
VPG5 (Virtual Port Group) IP Address <input type="button" value="⊙"/> {{ Sensor_Default_Gateway_IP_aka_vpg5 }}	VPG6 (Virtual Port Group) IP Address <input type="button" value="⊙"/> <system default>

Segmentation

Delivering on the segmentation discussed earlier is easy with Catalyst SD-WAN, however the two types of segmentation available with the solution need to be chosen as appropriate to the use cases.

Macro-segmentation

Catalyst SD-WAN has a construct called a Service VPN; this is designed to host end devices, and is analogous to a Virtual Routing and Forwarding (VRF) instance for those familiar with traditional data networking. Multiple Service VPNs can be defined, with an integer identifier and a text label. Through the automation of Catalyst SD-WAN instances of these Service VPNs can be instantiated where required; for example, not every Service VPN is required everywhere, and Service VPNs can be easily added and removed over time.

In the Roadways-specific Configuration Catalogs four Service VPNs are provided, as shown in Table 5.

Table 5- Service VPN examples

Service VPN ID	Service VPN example name and use
10	ITS – for ITS equipment
20	CCTV – for IP cameras
30	Agency X – facilitating another agency
40	Management – for network management

Service VPNs are inherently separated from one another, so macro-segmentation is used. Data networking traffic in the ITS Service VPN cannot mix with traffic in the CCTV Service VPN, unless the administrator specifically configures this.

As the Catalyst SD-WAN is integrated into the rest of the ITS data network, and/or the roadways operator IT network, most customers employ a firewall at the hub location(s) to filter in to, out of and between the macro segments. The Cisco Firepower 2100 family

(<https://www.cisco.com/site/us/en/products/security/firewalls/firepower-2100-series/index.html>) is well-suited for the data traffic volumes typical of a roadways operator, up to 10Gbps, with the 4100 family (<https://www.cisco.com/site/us/en/products/security/firewalls/firepower-4100-series/index.html>) providing options for up to 50Gbps.

It is a best-practice to put data network traffic associated with “management”, into a separate Service VPN – in Table 5, VPN 40 is used for this purpose. For example, the RADIUS traffic associated with AAA for router admin access and also for port authentication will be sent via VPN 40; similarly, any custom Syslog and/or NetFlow for example, as configured by the administrator.

In the example allocation in Table 5 above, note VPN30 for Agency X. It is often the case that a roadways operator needs to facilitate network connectivity for a related agency or law enforcement, and macro-segmentation is a helpful way to deliver this connectivity without mixing the traffic.

Micro-segmentation

Building on macro, micro-segmentation allows for discrimination of traffic within a Service VPN. A Security Group Tag (SGT) is an information tag applied by the Cisco network devices, invisible to end hosts,. SGTs are kept attached to the IP packets wherever they travel throughout the Catalyst SD-WAN overlay network and can be used to make security policy decisions. SGTs can also be shared with capable downstream LAN switches, for example, the [Cisco Catalyst Rugged IE3400](#), via a process known as “inline tagging” – the Ethernet encapsulation between the IR and IE includes the SGTs⁹.

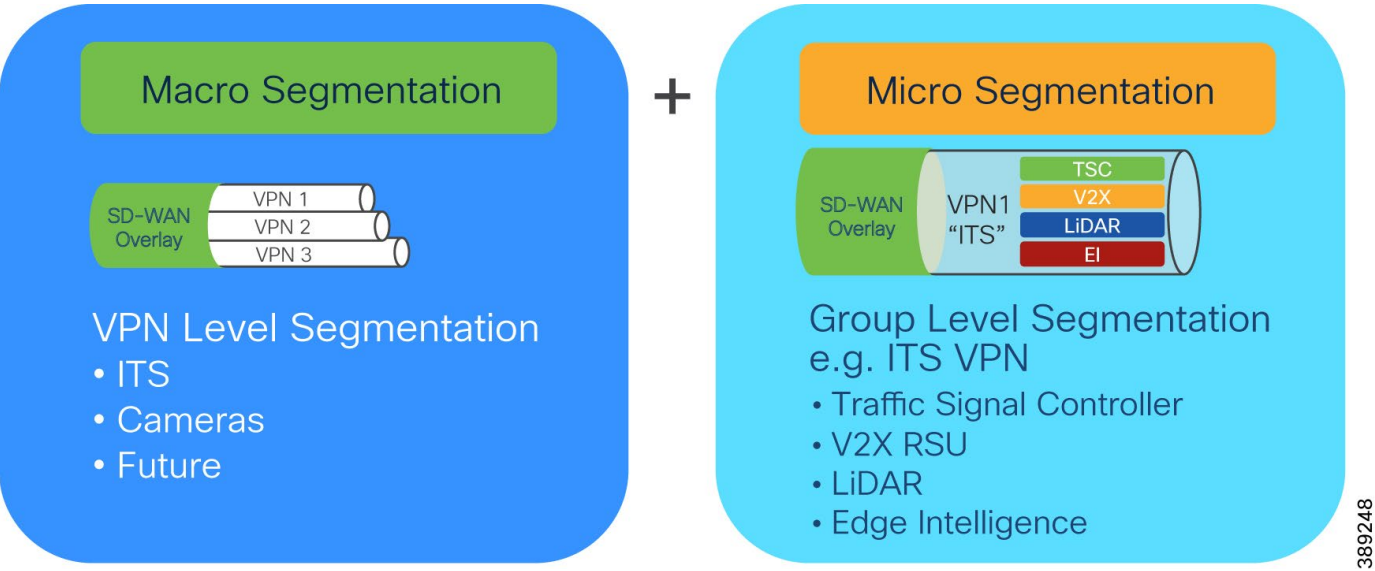
Even though ITS devices may be within a shared macro-segment, whereby default there is free and open reachability between them, an SGT-based policy can be used to put limitations in place – this helps to further mitigate risk of contagion.

Segmentation Combined

Macro and Micro go hand-in-hand. For example, there is no need for CCTV and ITS devices to mix at the edge, so they are placed within different macro segments. Within the ITS segment finer-grained control can be imposed, such that a V2X radio cannot communicate directly with a TSC – thus protecting the TSC.

⁹ Inline tagging from IR to IE is planned for an IOS-XE software update to the IRs in August 2025 (subject to change).

Figure 20 - Combined segmentation



Firewalling

With purposeful use of segmentation, firewalling at the edge is not necessarily needed, so long as there is strong firewalling at the central locations. The network traffic comes out of the SD-WAN fabric and into the rest of the network (DC, and so on.). However, if customers prefer a more defined approach then it is very feasible to enable a firewall on every router, with most models also supporting Next-gen Firewall (NGFW <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-next-generation-firewall.html>) including an IPS. See Table 6.

Table 6 - Firewall capabilities of Cisco IR models

Cisco IR model	Zone-based Firewall	Next-gen Firewall
IR1101	Yes	No
IR1835		Yes, apart from TLS decryption.
IR8140H		No ¹⁰
IR8340		Yes

In traditional Enterprise branch networking NGFW is often used to filter and protect traffic from users as it goes out from the branch towards the public internet – known as Direct Internet Access (DIA). For roadways, however, it is atypical for administrators to allow ITS devices to use DIA to go direct out to the internet, although there is an emerging trend of cloud-delivered ITS service that will change this behavior; until then the prevalent use of NGFW at the traffic cabinet will be to protect the infrastructure, primarily via IPS and AMP, in case of more traditional IT devices being connected at the edge, such as with a contractor laptop.

¹⁰ Plan to add NGFW for IR8140H in a subsequent software update.

Port Authorization

Most ITS networks have no port authorization enabled today; that means any device can be connected into an available Ethernet port and will be given network service. This is problematic because ITS networks are uniquely exposed amongst critical infrastructure, with weak physical security and often being readily accessible to the general public – and bad actors. Instead of having a “default open” posture, it moves to the best-practice of “default closed”. Any connected devices by default have no network service, and are given network service once the network can establish their identity as a trusted device. The standard-based mechanism to achieve this is IEEE 802.1X, with a fallback to MAC authentication bypass (MAB). Realistically MAB is used most of the time because the ITS industry is relatively immature on the adoption of cyber security best-practices, and most ITS devices do not have 802.1X compatibility.

Cisco Catalyst SD-WAN can also be integrated with Cisco Identity Services Engine for additional security. With ISE integrated we can configure MAC authentication bypass and 802.1X on our spoke sites. With MAB and 802.1X the administrator will have additional visibility and access control at the network edge. To integrate ISE the user will need to navigate to Administration in Manager and then select Integration Management and follow the details in the UI to add the integration to ISE.

There is also a configuration catalog created specifically for Roadways scenarios that adds support for ISE integration. Additional details can be found on the PDF in the description of the configuration catalog.

Enabling Port Authorization can be as simple as enabling the 802.1X toggle (and related toggles for MAB and so on) as part of a Switchport template that is associated to a Configuration Group in SD-WAN Manager.

Figure 21 - Enabling 802.1X in Catalyst SD-WAN Manager

Switchport

Name

pkavanag_Hub_IR1101_Switchports

Description (optional)

Basic Settings

Interface

Static MAC Address

Interface

+ Add Interface

Switchport Access Vlan (optional)	Allowed Vlans (optional)	Switchport Trunk Native Vlan (optional)	Voice VLAN (optional)	Enable 802.1X (optional)	Action
<div><div></div> 100</div>			<div><div></div> <system default></div>	<div><div></div> <input checked="" type="checkbox"/></div>	<div><div></div></div>
<div><div></div> 100</div>			<div><div></div> <system default></div>	<div><div></div> <input type="checkbox"/></div>	<div><div></div></div>
<div><div></div> 200</div>			<div><div></div> <system default></div>	<div><div></div> <input type="checkbox"/></div>	<div><div></div></div>
<div><div></div> 100</div>			<div><div></div> <system default></div>	<div><div></div> <input type="checkbox"/></div>	<div><div></div></div>

Static MAC Address

+ Add Static MAC Address

MAC Address	VLAN ID	Interface Name	Action
<div><div></div></div> <div>No data available</div>			

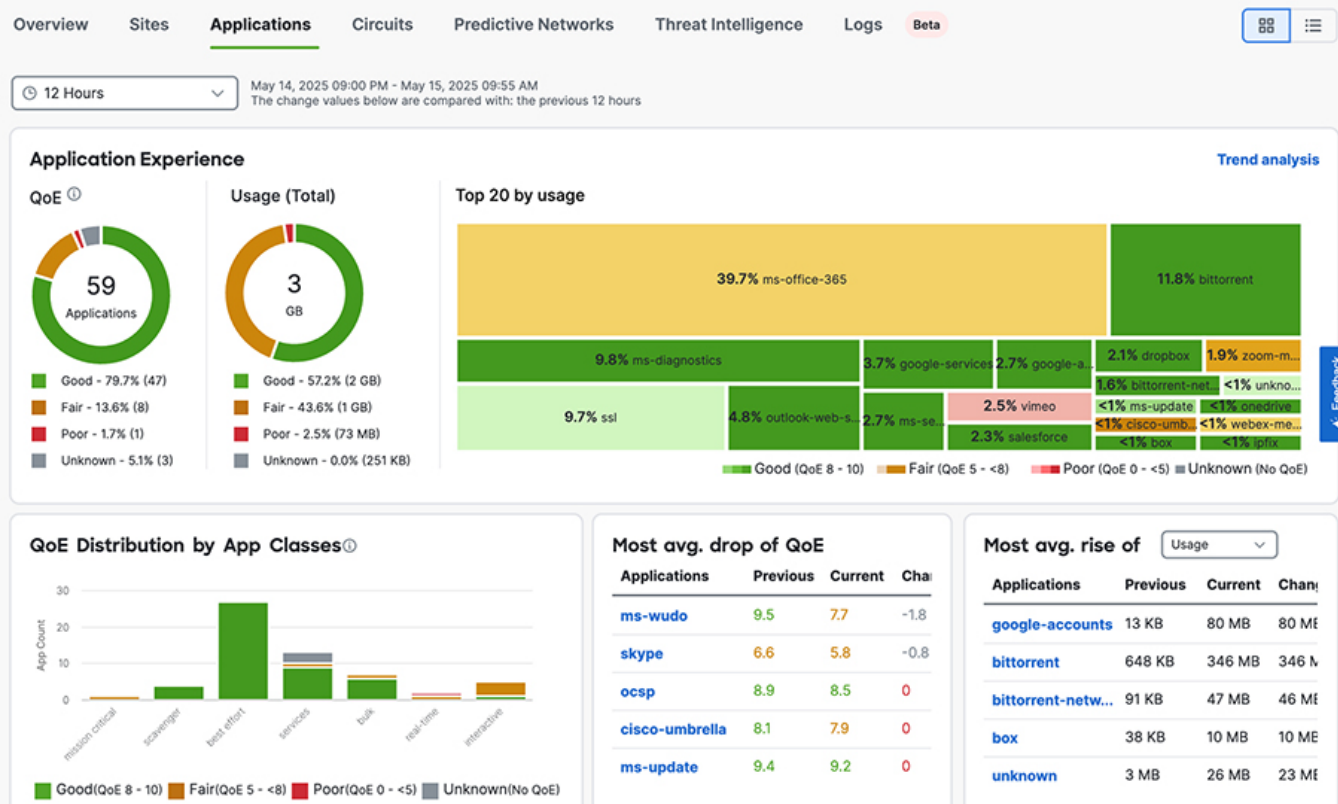
Cancel

Save

Quality of Experience

Application-centric Quality of Experience (QoE) is something that is measured automatically by Catalyst SD-WAN. Surfacing this as dashboard elements in Catalyst SD-WAN Manager allows for a quick readout on health. See Figure 22.

Figure 22 - QoE Dashboard



QoE is measured through a combination of packet loss, latency and jitter – this is in conjunction with measuring those same three elements at the VPN tunnel level. Therefore, Catalyst SD-WAN is uniquely positioned to look at QoE from the network and application perspectives.

SLAs can be defined, and specific instructions can be given on what should happen if the SLAs are not met. Figure 23 shows a Gold-Silver-Bronze breakdown.

Figure 23 - A sample Application Priority & SLA Policy – Simple View

Gold Business Relevant	Preferred Path 1x metro-ethernet	When SLA not met Backup Path
	Backup Path 1x lte	
Silver Default	Preferred Path 1x metro-ethernet	When SLA not met Fallback to Best Path
	Backup Path Not Applicable	
Bronze Business Irrelevant	Preferred Path 1x metro-ethernet	When SLA not met Strict/Drop
	Backup Path Not Applicable	

Here the example policy will route traffic over the metro-ethernet transport type (which would typically be a GRE tunnel), and if SLA for the Gold group is not met it will route the traffic over the LTE transport type (at which point it will be put inside an IPsec tunnel). For Silver the plan is to fallback to whichever best path is available, and for Bronze to actually drop the traffic completely – this could be appropriate for best-effort traffic which is not business critical and/or which could drive very high cellular costs.

Figure 24 below shows the Advanced View, which allows the administrator more fine-grained control of the policy. To the right is shown the SLA classes, for example the Transactional Data has a loss tolerance of 1%, latency and jitter both of 200ms – if any one of these elements of the SLA is exceeded, the SLA is considered broken.

Figure 24 - A sample Application Priority & SLA Policy – Advanced View

Search Traffic Policy

+ Add Traffic Policy

pkavanag_AppP+SLA_traffic (15)

Edit PolicyDelete PolicyCopy Policy+ Add RulesDelete All Rules

VPN: pkavanag_VPN100,pkavanag_VPN200Direction: AllDefault Action: Drop

Search Rule by Name or Order

NAME	MATCH	ACTION
1 rule1	Traffic Class • gold-voip-telephony	<div>Base Action • accept</div> <div>Backup Sla Preferred Color • lte,3g</div> <div>Dscp • 46</div> <div>Forwarding Class • pkavanag_AppP+SLA_1b...</div> <div>Sla Class Preferred Color • metro-ethernet</div> <div>Sla Class Sla Name • pkavana_1b4rqp1d_Voi...</div> <div>Base Action • accept</div> <div>Backup Sla Preferred Color • lte,3g</div>

pkavana_1b4rqp1d_Voice-And-Video

Loss: 2%

Latency: 300ms

Jitter: 60ms

pkav_1b4rqp1d_Transactional-Data

Loss: 1%

Latency: 200ms

Jitter: 200ms

pkavanag_AppP_1b4rqp1d_Bulk-Data

Loss: 5%

Latency: 500ms

Jitter: 500ms

pkavanag_AppP+S_1b4rqp1d_Default

Loss: 5%

Latency: 500ms

Jitter: 500ms

All these elements and thresholds are customizable, and Catalyst SD-WAN takes care of pushing the required configuration to the required network elements.

Scaling the Deployment

Scaling the Hub(s)

Configuring the hub and spoke devices in Cisco Catalyst SD-WAN is a simple process. To configure this topology, navigate to the Configuration menu and select **Topology**. From there you can add a Hub and Spoke topology and select the appropriate hub and spoke sites. Here you can also specify the primary and backup hub sites. See Figure 25 below.

Figure 25 - A hub and spoke topology

Hub and Spoke

Namepkavanag_Hub+_Spoke_CVD_TopoVPNpkavanag_VPN100

Hub Sites

Total2 sitesHubSITE_1,SITE_2

Spoke sites

+ Add Spoke Group

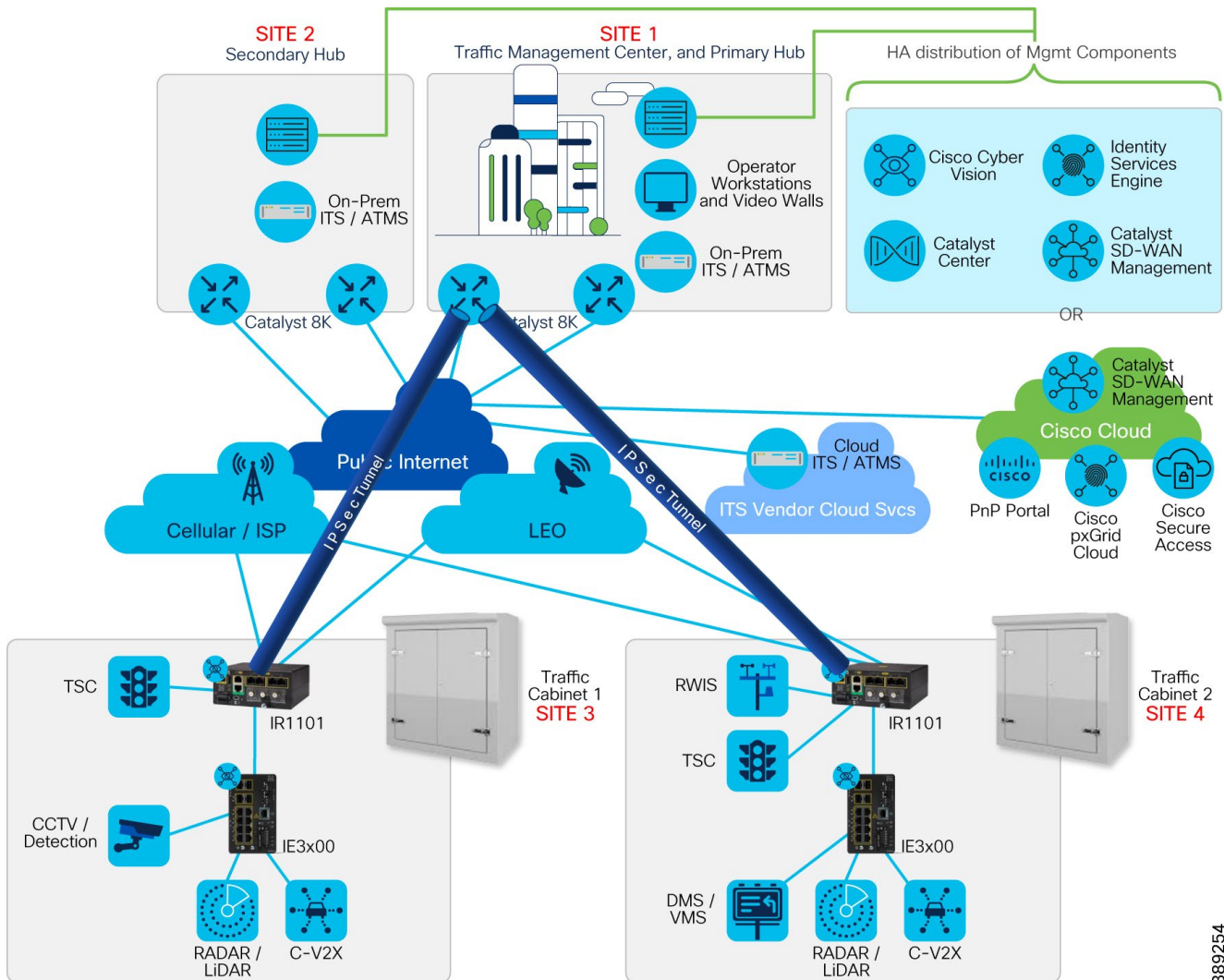
Search Table

Name	Total Sites	Spoke	Primary Hub	Backup Hub	Action
pkavanag_Spokes_CVD	3	SITE_3,SITE_4,SITE_5	SITE_1	SITE_2	...

1 RecordItems per page: 251 - 1 of 1

This makes scaling a large deployment very simple. Because Catalyst SD-WAN models the WAN as a system, as the administrator configures the respective hub and spoke elements, SD-WAN Manager knows which devices need to have their configuration modified to deliver on the administrator's intent; the administrator doesn't need to configure network devices individually – this is a huge operational benefit, and a real instantiation of intent-based and software-defined networking! Please note in Figure 25 above that the topology can be created per-VPN, in this case VPN 10; but the same topology could be applied to just VPN 10, a subset of VPNs or all VPNs, allowing for powerful and fully customizable topologies, which support all the customer use cases.

Figure 26 - Sample topology



389254

In Figure 26 this matches what we set up in Figure 25; Sites 3 and 4 (two remote traffic cabinets) have built IPsec tunnels back to Site 1 (a Hub, and the TMC). Site 2 is a backup Hub in this topology, so no tunnels are built to it currently, because Site 1 is healthy.

Configuration Groups and Configuration Catalog

In the deployment of Cisco SD-WAN for managing Industrial IoT routers like the IR1101 and IR1800 series, configuration groups serve as a powerful tool for achieving scalability and efficiency. By grouping these routers into configuration groups, network administrators can apply uniform configuration across a vast number of

devices simultaneously. This approach not only streamlines the initial deployment process but also simplifies ongoing management tasks, such as updates and configuration changes. Configuration groups ensure that all routers adhere to the same network policies and security protocols, reducing the risk of configuration drift and enhancing overall network reliability. This centralized management capability is crucial for industrial environments where maintaining consistent and secure connectivity across numerous remote sites is essential for operational success. Also, incorporating industry best practices ensures the configuration being used is reliable and secure.

A configuration group is made up of profiles such as the system, transport & management, service, and CLI-add-on profiles. In each of the profiles there are many options to select, and this can be overwhelming to develop a configuration group. To further simplify the process and ensure industry best practices are being used we have created configuration catalogs. We have developed configuration catalogs for various use cases, such as the Cellular Roadways sites. And each catalog has a detailed description and document describing the architecture of the configuration. Further detail about configuration catalogs can be found here (refer to <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/config-groups/configuration-group-guide/config-catalog.html>). The table below shows the release schedule for configurations catalogs.

Table 7 - Cisco Validated Profiles in the SD-WAN Configuration Catalog

Cisco Validated Profile	Function	SD-WAN Release	Description
CVP1/2	IR1101/1800 Single LTE	20.15.1	Single router SD-WAN configurations with wired and single LTE as last resort supporting single service VPN for horizontal ¹¹ IR deployments.
CVP3/4	IR1101/1800 Dual LTE	Target IOS-XE17.18	Single router SD-WAN configurations with wired and dual LTE in both active/active and active/standby modes, supporting single service VPN for horizontal IR deployments.
CVP5/6	IR1101/IR1800 Roadways (w/o CV)	20.15.2	Single router SD-WAN configurations with wired and single LTE as last resort supporting multiple service VPN for Roadways deployments with ISE integration and LAN port authentication.
CVP5cv	IR1101 Roadways (w/ CV)	20.16.1	Single router SD-WAN configurations with wired and single LTE as last resort supporting multiple service VPN for Roadways deployments with ISE integration and LAN port authentication.

¹¹ Horizontal refers to not being an industry or vertical-specific scenario. For example, roadways is a vertical, but industrial networking is more horizontal.

Cisco Validated Profile	Function	SD-WAN Release	Description
			Also includes profile to deploy Cyber Vision sensor in IOx.

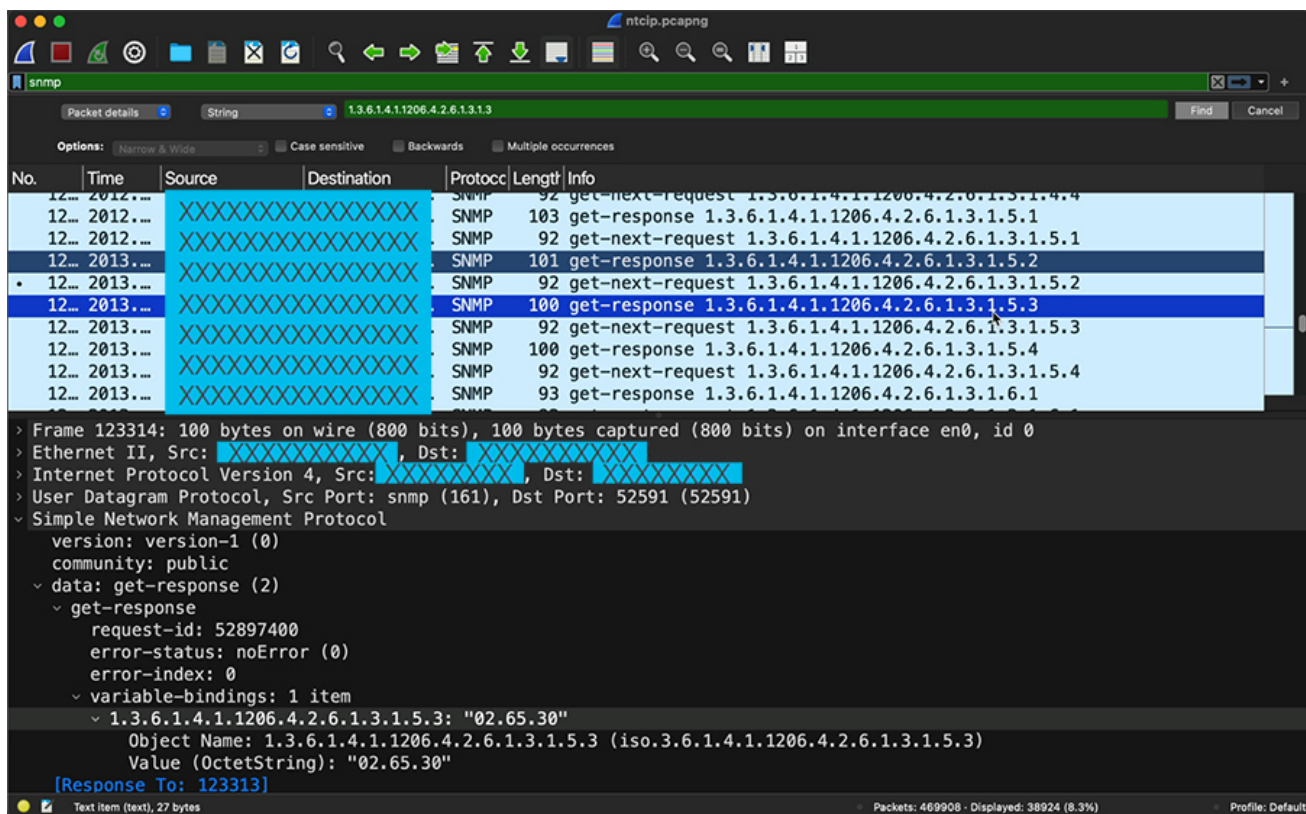
Connecting up ITS equipment

Exposures

The weak physical security of traffic cabinets has already been mentioned, but there are also weaknesses within the ITS protocols themselves; most are sent cleartext. NTCIP, for example, by default uses SNMP v1 as its transport protocol.

In Figure 27 below, please note the “02.65.30” shown towards the bottom of the image; this is the software version of a TSC. This value was found by querying an SNMP OID, as documented in NTCIP 1201 - Global Object Definitions, and was done using a read-only SNMP GET request, with the community “public”.

Figure 27 - A network capture of NTCIP traffic, viewed in Wireshark (with certain fields obfuscated).



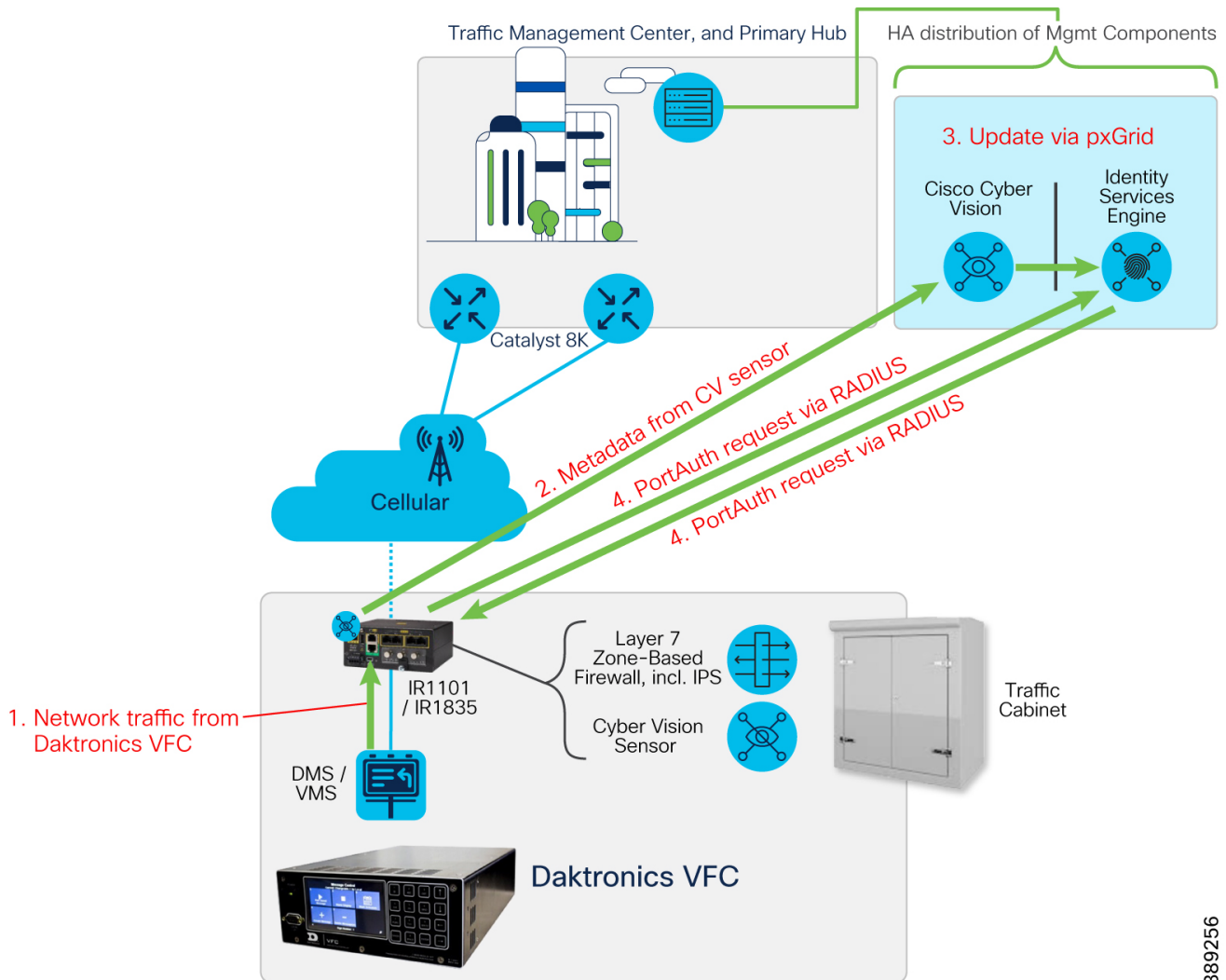
This is problematic because a bad actor can then evaluate vulnerabilities in this particular software version and may use this as an insertion point to the roadways network.

Without Catalyst SD-WAN, roadway operators often resort to port-forwarding traffic from the public internet, through simple cellular modems; with Catalyst SD-WAN instead they can avoid unnecessary exposures, use strong firewalling and advanced capabilities to connect ITS devices to this network.

Basic - with Daktronics VFC

In roadway operations, devices like the Daktronics VFC sign controller are often deployed in potentially isolated roadside cabinets. This setup poses a risk where a determined malicious actor could potentially gain physical access to the network. To mitigate such risks, Cisco's solution employs an industrial router, Identity Services Engine (ISE) with pxGrid, and Catalyst SD-WAN Manager to ensure secure connectivity through MAC Authentication Bypass (MAB); as shown in Figure 28.

Figure 28 - IR1101 with MAB for Daktronics VFC



389256

The Daktronics sign controller serves as just one example of the various roadway equipment that can benefit from MAB authentication. It physically connects to the IR1101 router which provides connectivity to the ATMS, ISE, and other parts of the network via the secure SD-WAN overlay. The IR1101 router hosts a Cyber Vision sensor application that monitors all traffic and sends metadata to the centralized Cyber Vision Center for analysis and reporting. Integration between ISE and Cyber Vision Center via pxGrid enhances the overall security framework by expanding profiling capabilities across the IT and OT domains.

The IR1101 can be configured to require 802.1X authentication on its switchports, followed by MAB as a fallback in the case that 802.1X times out. In the case of the Daktronics VFC controller, 802.1X is unsupported, so MAB will be used instead. MAB requires outbound traffic initiation from the newly connected device to reveal the source MAC address. Using DHCP for address assignment (with static bindings¹², if desired) on the roadways, equipment can be used to facilitate this, as the connected device will initiate a DHCP Discover message outbound towards the router. Specific to the Daktronics VFC controller, the MAC address contains an Organizationally Unique Identifier (OUI) belonging to Texas Instruments (the manufacturer of the NIC). Other roadways equipment vendors may have their own OUI. The IR1101 communicates with ISE using RADIUS, where policies are setup to match the MAC OUI and the source network device (IR1101), provisionally granting network access and applying a restrictive dACL to the switch port or putting it in a quarantine VLAN.

Subsequently, the Advanced Traffic Management System (ATMS) can communicate with the Daktronics controller using the NTCIP protocol. Traffic inspection by Cyber Vision aids in further device profiling. Validation through DHCP exchanges and NTCIP traffic confirms the device as a Daktronics sign controller. Upon successful confirmation, Cyber Vision Center updates ISE, prompting a revised, more permissive dACL to be applied to the IR1101 switch port via a RADIUS Change of Authorization (CoA), thus allowing full operational connectivity.

One downside of using MAB authentication is that MAC addresses can be spoofed. This is why it is important to leverage other capabilities within ISE and Cyber Vision to properly profile the newly connected device. For example, if a bad actor were to use a Raspberry Pi or similar SBC, clone the MAC address of the TSC, if MAB is the only mechanism in use the SBC gets access to the network.

Intermediate - with Q-Free Kinetic Mobility

Cisco technology ensures secure, end-to-end connectivity for roadways equipment that is increasingly interacting with cloud-based services. For example, for a Q-Free traffic signal controller interacting with the Q-Free ATMS hosted in the cloud, Cisco's solution integrates components like Cisco Catalyst SD-WAN Manager, the IR1101 router, Cisco Secure Access (CSA), Cisco pxGrid Cloud¹³, and Cisco Identity Services Engine (ISE). Leveraging Cisco TrustSec, the network enforces consistent security policies from the roadway cabinet to the cloud, safeguarding critical traffic management functions.

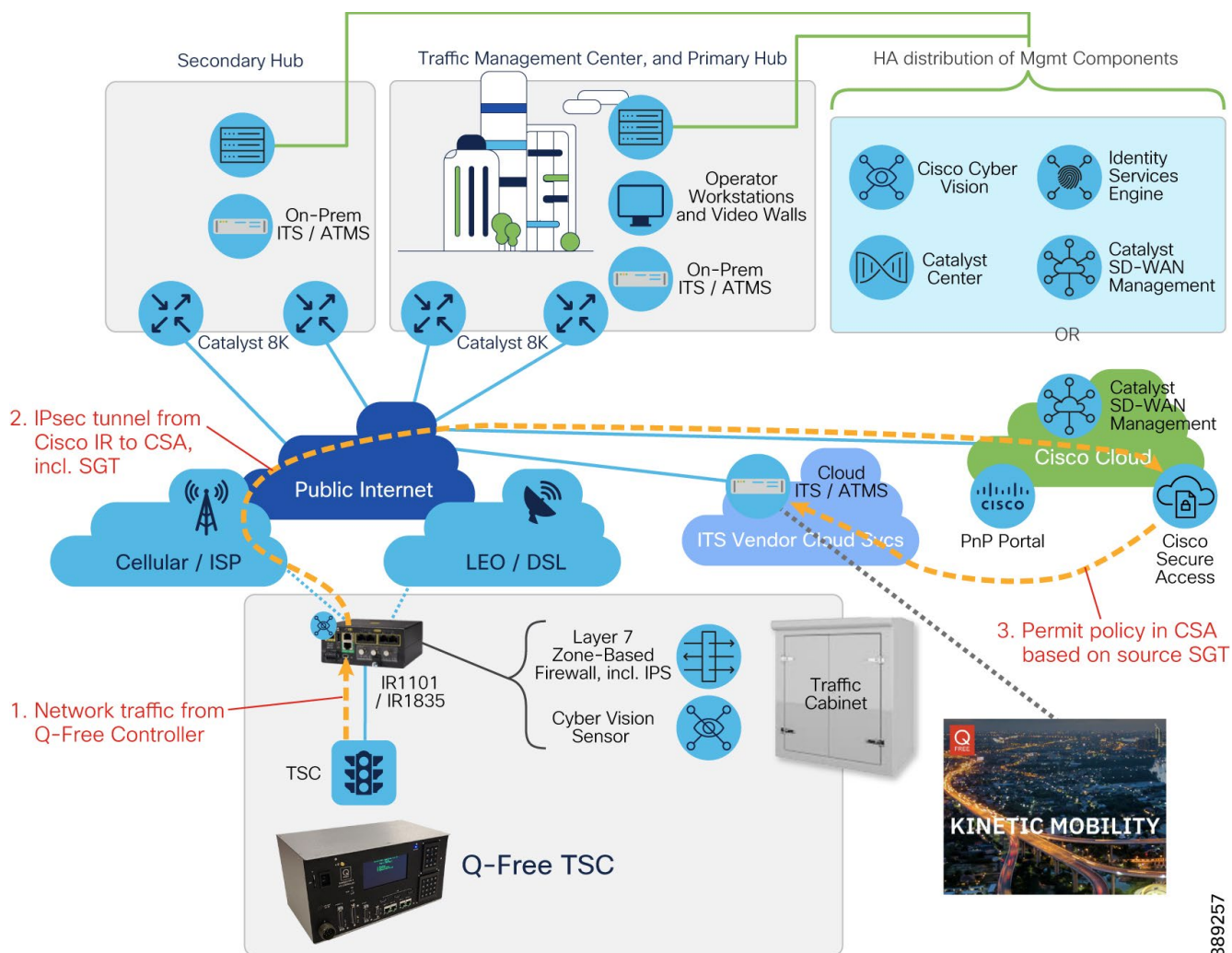
The Cisco Catalyst SD-WAN Manager plays a pivotal role by centrally managing the IR1101 router deployed at the roadside cabinet. Additionally, it integrates with Cisco Secure Access to establish IPsec tunnels—often deployed with redundancy—between the IR1101 and CSA, creating a secure pathway for traffic from one or more service VPNs on the router. At the cabinet, the IR1101 or subtended switch marks traffic from the Q-Free controller with TrustSec Security Group Tags (SGTs), which uniquely identify its source and intent. These SGTs are maintained through the IPsec tunnels, enabling CSA to use them for precise policy decisions, allowing or blocking traffic based on predefined rules to protect the ATMS. Cisco ISE and pxGrid Cloud sit in the middle of this solution and are used to share the SGTs between the other components.

Although DIA could be used from each IR at the roadside, Q-Free's solution benefits from a centralized server (typically located at the TMC or Hub location), and this server aggregates application traffic towards the public cloud, as shown in Figure 29.

Figure 29 - CSA for Q-Free Kinetic Mobility

¹² A static binding for a DHCP lease is a useful middle-ground for customers, because the security benefits helped by DHCP can be realised, but the simplicity of having consistent IP addresses (like they have with static IPs) for the OT/operations team is kept.

¹³ https://www.cisco.com/c/en/us/td/docs/security/pxgrid_cloud/solution_guide/b_pxgrid_cloud_solution_guide_2024.html



This solution benefits transportation agencies with enhanced security and streamlined operations. The TrustSec SGT-based enforcement prevents unauthorized access to traffic systems, while the centralized management and secure tunneling ensure reliable, scalable connectivity from the roadside to the cloud.

Note: When configuring the Catalyst SD-WAN Manager policy for CSA access, it is required to put a Tracker Source IP address, even if no trackers are configured. There is also an open issue preventing using Endpoint Tracking for Cellular interfaces. It is recommended to source the primary CSA IPsec tunnel over Ethernet WAN (with a tracker) and secondary tunnel over Cellular. If Cellular is the only WAN link, then it is still required to put a Source IP address for the tracker, but you will need to edit the advanced options in the tunnel and disable Tracking.

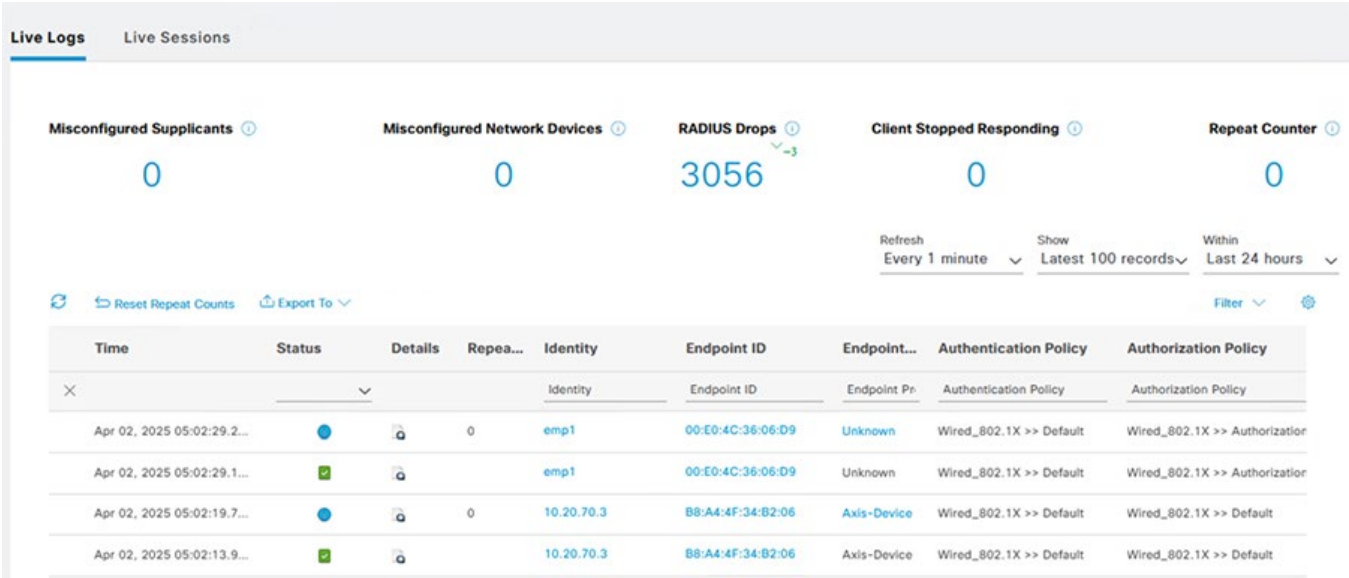
Advanced - with Axis video camera

Leveraging 802.1X authentication on supported devices can help alleviate some of the disadvantages of using MAB by itself, such as MAC spoofing. Some roadways devices like AXIS cameras, or the Q-Free traffic signal controllers, support an 802.1X client that can use EAP-TLS (certificate based) and/or EAP-MD5 (username and password based) authentication in conjunction with Cisco ISE. While 802.1X can provide more confidence in the identity of the device (versus just a MAC address, for example), ISE policies can also utilize additional profiling information from Cyber Vision, as was the case with MAB. After authentication succeeds, the device can be granted network access from ISE, via RADIUS messaging to the IR1101. If desired, ISE can assign or modify (via CoA) a dACL or VLAN to the switchport associated with the newly authenticated device.

Using 802.1X is recommended when the devices on the network support the functionality. It is important to factor in a method for initial configuration of the 802.1X client (ITS devices) – either adding credentials or a certificate – into the workflow for deploying new devices in the field.

Figure 30 that follows shows the logs in ISE for an Axis camera completing an 802.1X authentication process to access the network, as facilitated by Catalyst SD-WAN.

Figure 30 - Authentication in ISE



LTE Timers Optimizations

All “IoT” Catalog entries have optimized timer values from the defaults to reduce cellular usage per month, while still providing functional SD-WAN environment with properly exchanged OMP routes and proper BFD behavior. The list below are all the modified timer values and their default equivalent. These modified values are hard coded in all Catalog entries and the user is not allowed to modify them to ensure proper tested behavior in the Cisco Validated Profile (CVP) Catalog. These optimizations have reduced cellular data usage drastically from nearly 3.6GB monthly usage to less than 500MB¹⁴.

Table 8 - CVP Catalog Optimizations for Cellular Transport

Category	Default SD-WAN Value	CVP Catalog Optimized Value
System -> OMP		
Advertisement Interval	1 sec	60 sec
Hold Time (keepalive-hold/3)	300 sec	5,400 sec
System -> BFD		
Color LTE Hello Interval	1,000 ms	10,000 ms (10 sec)
Poll Interval	600,000 ms	1,200,000 ms
Transport -> Cellular -> Tunnel		
Hello Interval	1,000 ms	60,000 ms (1 min)
Hello Tolerance	12 sec	300 sec (5 min)

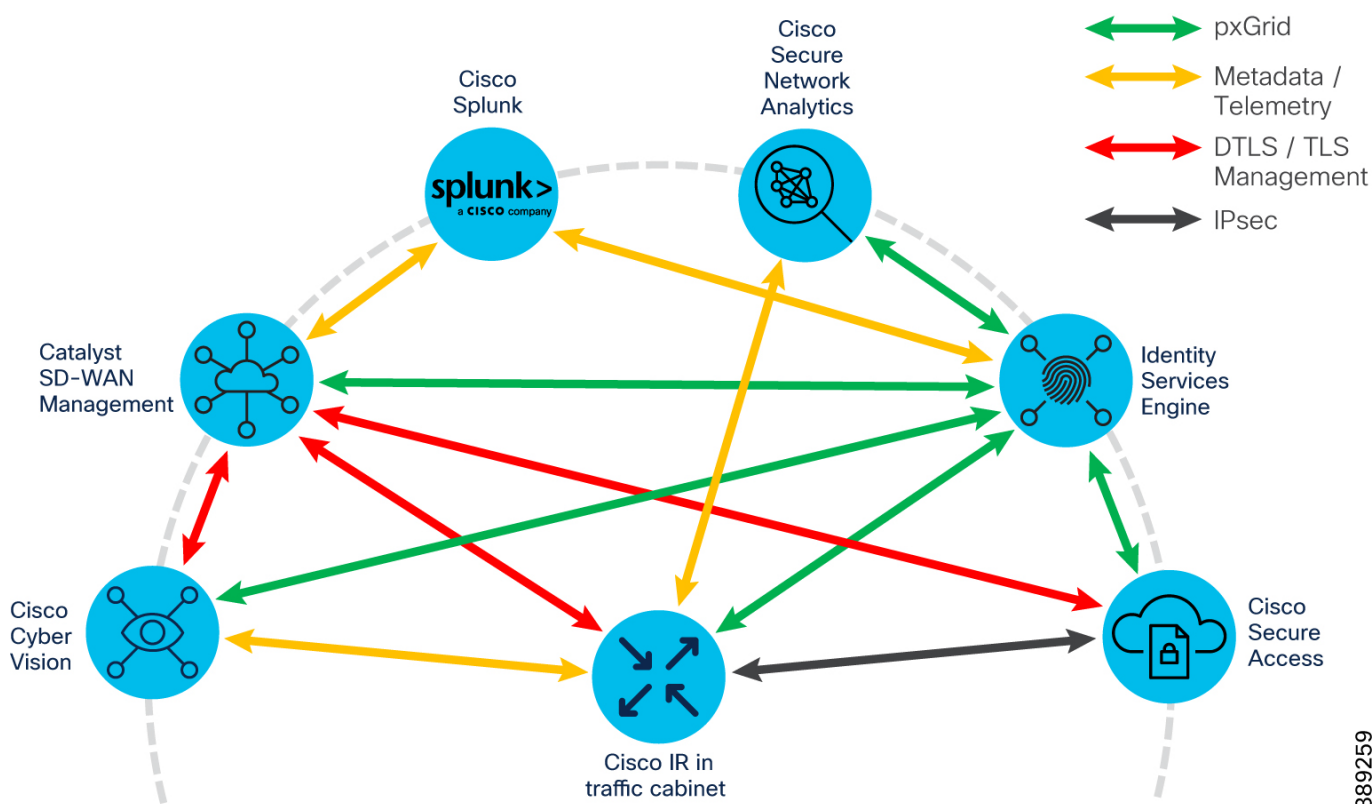
Please note that for other non-Cellular Transport interfaces the default Catalyst SD-WAN values are used, which are appropriate for transports without usage charges. For example, a typical Gigabit Ethernet public internet connection; however, for LEO connections, which present as Ethernet, some optimized values are recommended (please see [LEO section](#)).

¹⁴ This is for the combined management and control plane traffic. Customer data plane traffic will be in addition to this, and entirely dependent on the use cases involved.

Conclusions

Many system components can come together, sharing metadata to provide customers with enhanced visibility, anomaly detection and a platform for the next generation of ITS use cases, all while prizing simplicity, and that scales to thousands of traffic cabinets. Figure 31, below, shows some of the ecosystem interaction; important to note that these are enabled either by a one-time administrator setup, or enabled automatically.

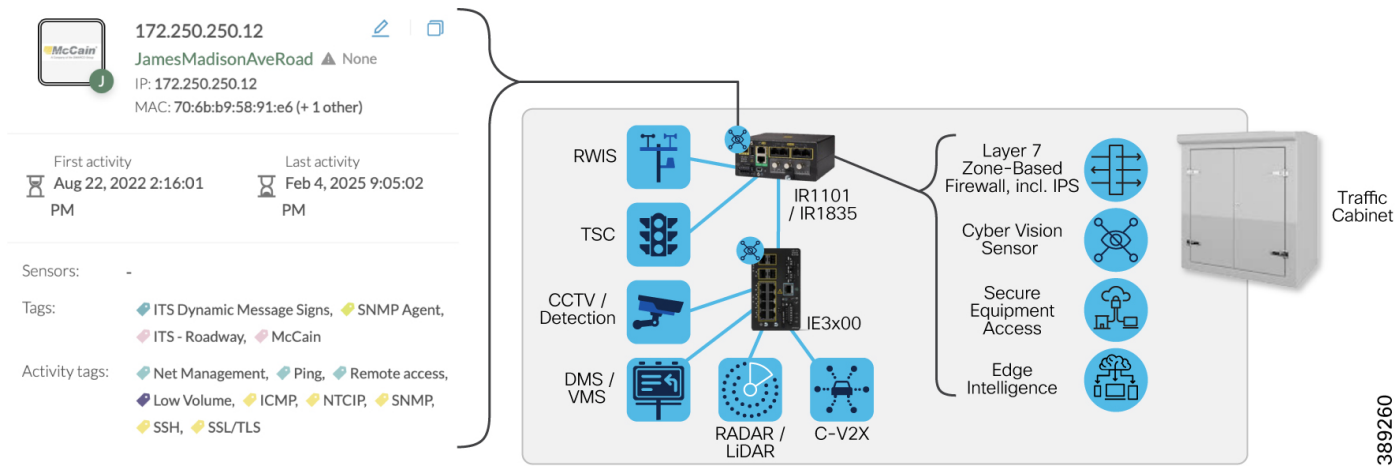
Figure 31 - Interaction with solution components



The scalability of Catalyst SD-WAN is more than enough for roadways operators – scaling to 12,500 WAN Edge routers in a single management domain – and how SD-WAN helps scale the operations has been well discussed, but the constant throughout this CVD is security:

- Best-in-class security of the WAN transports, enabling the use of more cost-effective public internet connections, but without compromising on securing those transports.
- Native Zone-based Firewall, inc. NGFW in IR1835 and IR18340
- Cisco Cyber Vision deployed via Catalyst SD-WAN Manager, to bring OT visibility of common ITS protocols, and to share context via pxGrid into ISE, enabling enhanced port authentication (see Figure 32 that follows).

Figure 32 - Cyber Vision on IR1101 deployed as part of Catalyst SD-WAN



Cisco Industrial Routers with Catalyst SD-WAN are the ideal secure foundation for your ITS network.

Glossary

AMP = Advanced Malware Protection

ATMS = Advanced Traffic Management System (aka Intelligent Transportation Management System, ITMS)

CSA = Cisco Secure Access

dACL = Dynamic Access Control List

DIA = Direct Internet Access

IPS = Intrusion Prevention Sensor

ISE = Cisco Identity Services Engine

ITS = Intelligent Transportation System

LAN = Local Area Network

LEO = Low Earth Orbit (Satellite)

MAB = MAC Authentication Bypass

NIC = Network Interface Card

NTCIP = National Transportation Communications for ITS (Intelligent Transportation Systems) Protocol

OMP = Overlay Management Protocol

OT = Operational Technology

OUI = Organizationally Unique Identifier

pxGrid = Cisco Platform Exchange Grid

QoE = Quality of Experience

RADIUS = Remote Authentication Dial-In User Service

SBC = Single Board Computer

SFP = Small form-factor pluggable

SLA = Service-Level Agreement

SMF = Single-mode Fiber

SVI = Switched VLAN Interface

TLOC = Transport Locator

TMC = Traffic Management Center (aka Traffic Operations Center, TOC)

TSC = Traffic Signal Controller

TSMO = Traffic System Management and Operations

VLAN = Virtual LAN

VPN = Virtual Private Network

VRF = Virtual Routing and Forwarding

WAN = Wide Area Network