Six Ways to Secure Access Connectivity for Intelligent Roadways

Achieve Secure Networking for Intelligent Roadways

Contents

With Cooperative Intelligent Transportation Systems (C-ITS), roadway ITS operators and authorities can ensure they have a strong cybersecurity posture, starting right at the edge of their networks.

Introduction

Network connectivity for roadway devices is increasingly important as civil and traffic engineers connect new devices and systems, and instrument existing ones together, as part of an Intelligent Transport System (ITS). The goals are often to reduce and ultimately eliminate road deaths (Vision Zero), and to reduce congestion and therefore reduce vehicle emissions and transit times, thus reducing environmental impact and increasing productivity.

ITS and roadway devices include traffic signal controllers, weather stations, cameras, digital/variable message signs, pedestrian detectors, and a whole lot more! These devices are often housed in metal enclosures at the side of the road. While the enclosures provide good environmental protection (usually to IP65 or better), the physical security of the enclosures/cabinets is often lacking–this makes securing the devices within them all the more important.

The era of connected and autonomous vehicles brings increasing pressures to roadway IT networks, with more advanced use cases around journey optimization and the safety of all road users, and firmly elevates the roadway devices, and their connectivity, to critical-infrastructure status. The stakes are even higher with Cooperative Intelligent Transport Systems[1] (C-ITS):

> *"As the transport system becomes more and more digitised, it may also become more vulnerable to hacking and cyber-attacks. The cyber-security of C-ITS communications is therefore critical." – European Commission[2]*

The scope of this white paper is an overview of some best practices around securing access networking for these roadway devices, and about how this impacts the cybersecurity position of the ITS and C-ITS. Roadway engineers and technicians, with their Operational Technology (OT) focus, will need to work closely with the IT team. Correspondingly, the IT team will need to gain an understanding of the unique elements of roadway systems as opposed to, for example, traditional campus networking.

[1] https://etsc.eu/wp-content/uploads/ETSC-Briefing-on-Cooperative-Intelligent-Transport-Systems-C-ITS.pdf

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=EN

Physical Connectivity and Network Protocols

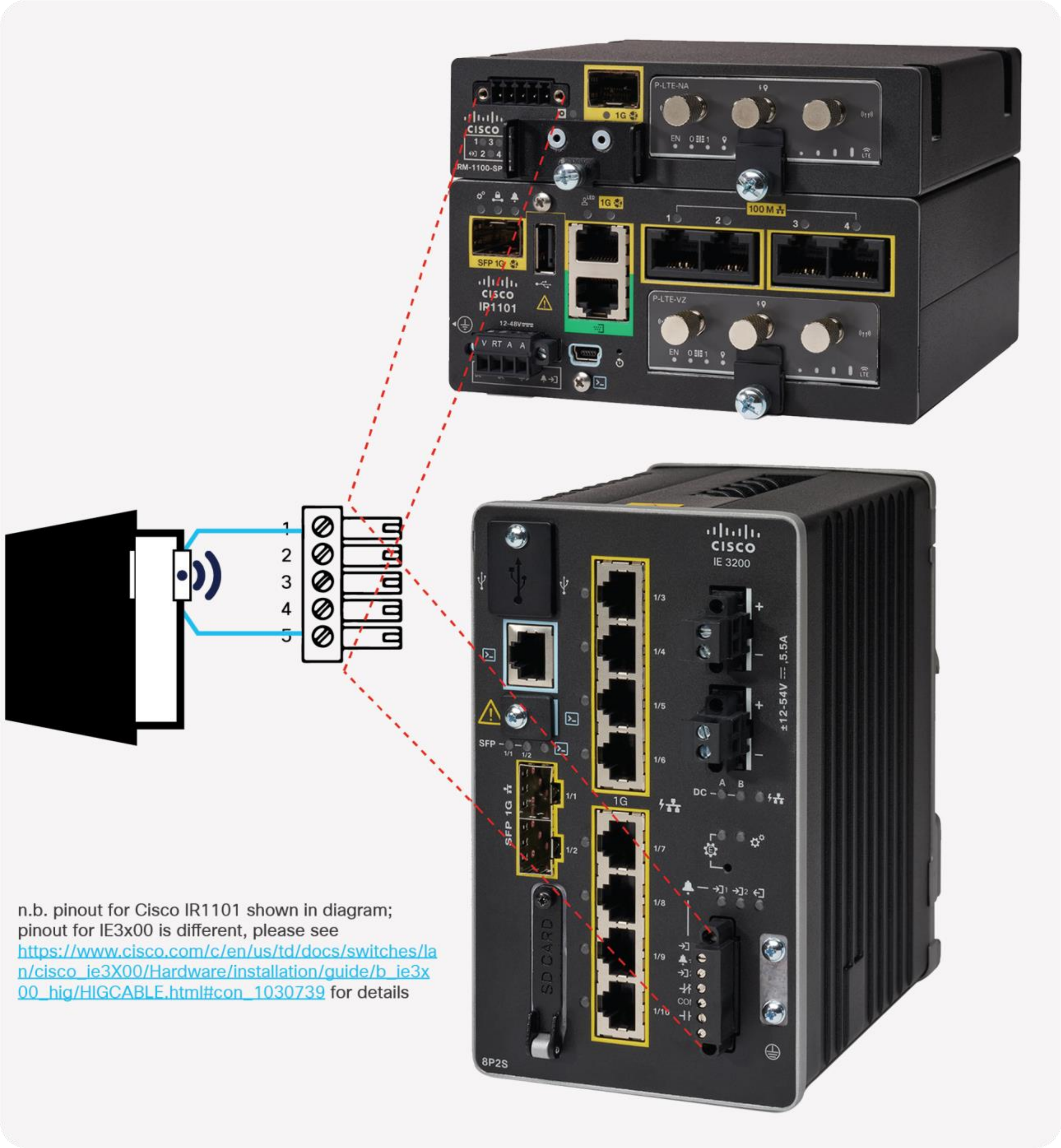
Most contemporary roadway devices offer Ethernet connectivity, with the majority of those being the common RJ-45 copper variant. However many customers have traditional roadway devices still in use, which are accessed via a serial connection (e.g. RS-232/485). Unsurprisingly, the inherent reliability of a fixed wired connection is preferred. Sometimes standards-based and proprietary wireless connections are also used; however, this is more common on the backhaul side than with the devices themselves.

On the Ethernet side it is uncommon to find devices operating purely at OSI Layer-2. The majority of Ethernet-connected devices have a full TCP/IP stack, but the transport layer-4 is often unencrypted.

In denser urban locations, and along major highways, it more likely that there will be fiber optic cable available to provide connectivity upstream, often to a Traffic Management Center (TMC). For sparse urban locations and minor roadways, it is more likely that cellular backhaul will be used. However no fixed rule exists. Customers are guided by the physical locations they're providing connectivity for, and by existing communications infrastructure. When network devices come equipped with a number of different access connection types, or are modular in nature, covering copper, fiber, Wi-Fi etc., customers have significant flexibility. The same is true for access options including 4G, 5G, fiber, DSL, etc. on the backhaul; this allows customers to standardize on a few families of network devices, yet still have the flexibility to deploy these across many varied sites and requirements.

As mentioned, the physical security of roadside cabinets can be compromised, and a bad actor can gain access to the cabinets and interfere with the contents—keys for these cabinets are readily available online for as little as $10!

To mitigate these challenges, Cisco® industrial switches and routers can use native general purpose input/output (GPIO) or alarm ports through a contact-closure for cabinet doors. These methods provide an easy means of alert in the event the door is opened, through Syslog and/or Simple Network Management Protocol (SNMP) traps. When the traffic cabinet door is opened an alarm in generated; this alarm is cleared when the door closes again.



n.b. pinout for Cisco IR1101 shown in diagram; pinout for IE3x00 is different, please see https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/HIGCABLE.html#con_1030739 for details

Figure 1.
GPIO and alarm ports, on Cisco industrial routers and switches respectively

Furthermore, it is possible to use the Cisco IOS Embedded Event Manager (EEM) on the router or switch itself to take further actions when an alarm is triggered, for example, to send an email alert to the operations team, or even hook into the GPIO from an application running on the device in Cisco IOx. Please see the Appendix for more details.

Securing the Access Connection

The humble access port, be it Ethernet or serial, is the critical touchpoint between the ITS devices and the network.

Ethernet

Cisco recommends providing robust security starting right at the edge of the network, where the roadway devices physically connect. Whether this is a fiber-connected network switch or a cellular-connected router, the physical access connection is often copper Ethernet (100/1000Base-TX). The principle of "Zero Trust"[3] can be applied here, whereby a device is not granted network access merely by plugging in the cable—instead the network must be satisfied, to some degree of certainty, that this particular device is known, trusted, and is allowed access to the network:

> *"Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes." – NIST*[4]

Furthermore, a device may be given access to only a certain segment of the network, and optionally very fine-grained policies can be defined centrally and enforced at every hop in the network. The Network Access Control (NAC)[5] concept is critical here to allow customers to have network visibility and access management through policy enforcement on devices across their network.

The gold-standard for this port-based NAC is IEEE 802.1X,[6] where the roadway device is a supplicant, the Cisco switch or router is the Authenticator (reached via Extensible Authentication Protocol [EAP]), and there is a centralized Authentication Server (reached via Remote Authentication Dial-in User Service [RADIUS]). However, most roadway devices do not support the role of supplicant, and therefore MAC Authentication Bypass (MAB) is often used. MAB will use the device's MAC address as the key identifier. In conjunction with a number of other information sources, the Cisco Identity Services Engine (ISE), fulfilling the NAC role, will determine what network access this device will get, if any.

[3] https://www.cisco.com/c/en/us/solutions/automation/what-is-zero-trust-networking.html

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[5] https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

[6] https://standards.ieee.org/standard/802_1X-2020.html

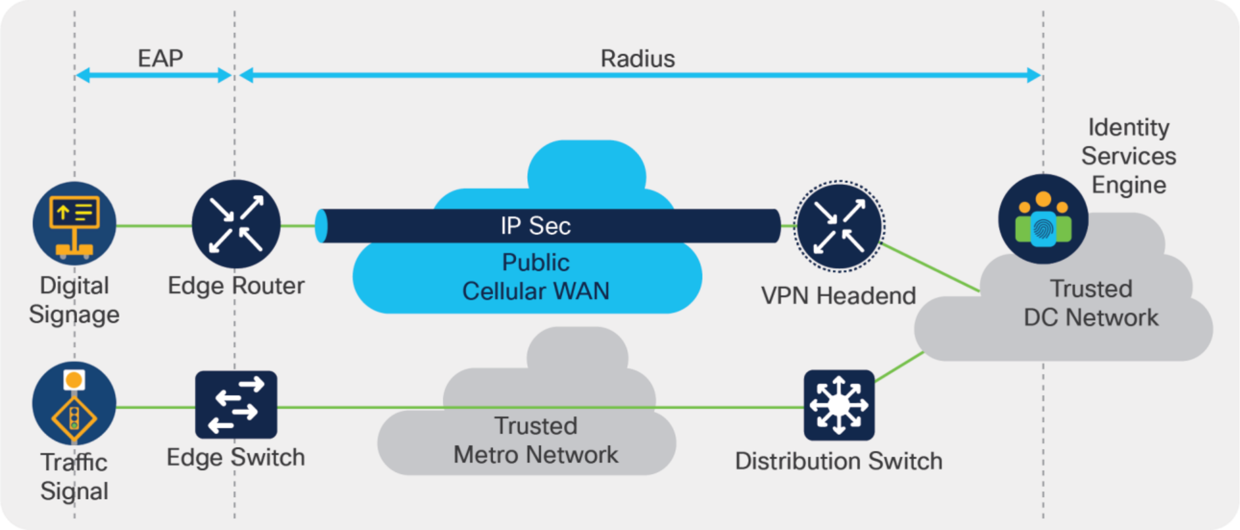


Figure 2.
Supplicant, Authenticator, and NAC

It is quite common, when using MAB, to have a device start with limited network access, and when greater confidence has been attained in the device's identity and veracity, network access will be elevated.

One way is through the use of Cisco Cyber Vision,[7] and its communication channel with ISE. Cyber Vision 4.0 added support for National Transportation Communications for ITS Protocol[8] (NTCIP), specifically the NTCIP 1200 family of standards, whereby Cyber Vision can perform deep packet inspection (DPI) of such network traffic. Cyber Vision can then help the customer determine whether a particular roadway device is communicating using valid NTCIP protocol structures, and thus this particular device is likely a genuine roadway device or an intruder. Cyber Vision communicates with ISE via Platform Exchange Grid[9] (pxGrid). Running the Cyber Vision Sensor on the network devices themselves efficiently achieves DPI, when the Sensor can be in-line with the network traffic as it transits the router or switch, and they communicate back to the Cyber Vision Center.

[7] https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

[8] https://www.ntcip.org/about/

[9] https://www.cisco.com/c/en/us/products/security/pxgrid.html

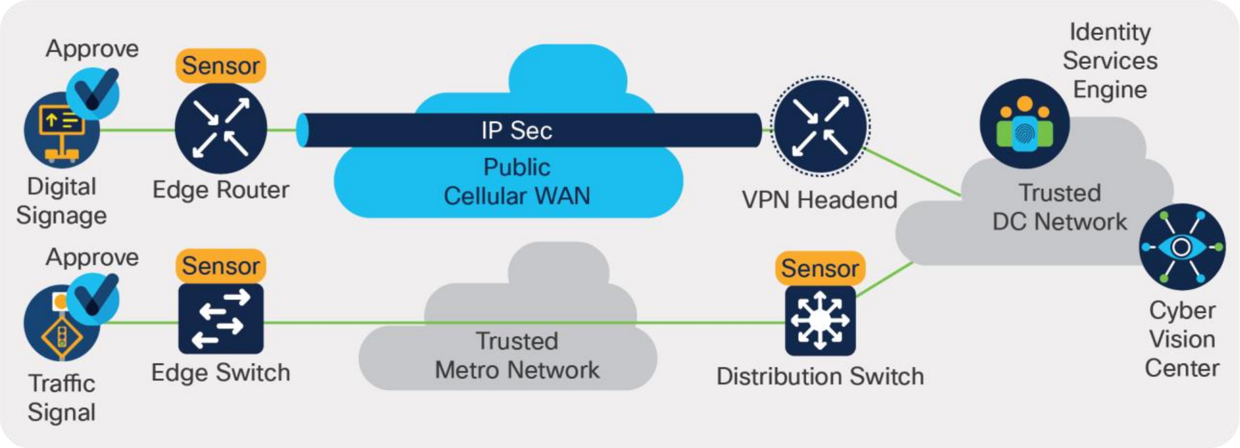


Figure 3.
Devices approved for network access

If an attacker compromised a roadway device, cloned its identity (MAC address etc.) and attempted to access the network in its place, Cyber Vision would detect this and notify ISE via pxGrid. At this point ISE would instruct the network device to remove and block the attacker’s network access, alerting the administrator.

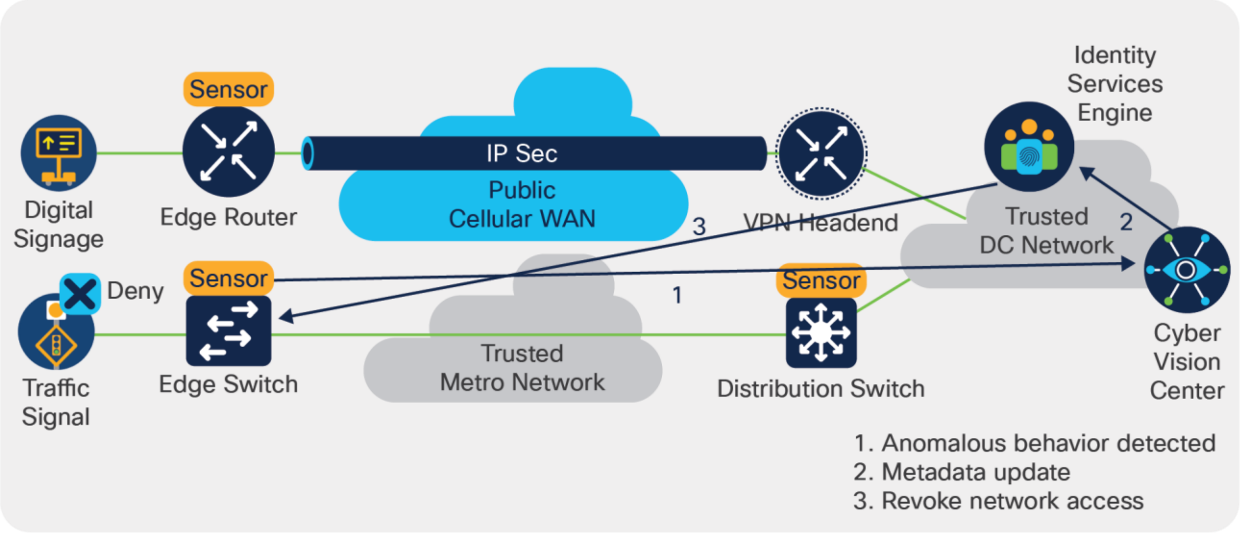


Figure 4.
Compromised device denied access

Serial

For serially connected devices, there is no port authentication model per se. Instead, Cisco industrial routers can encapsulate the serial traffic over an IP network.

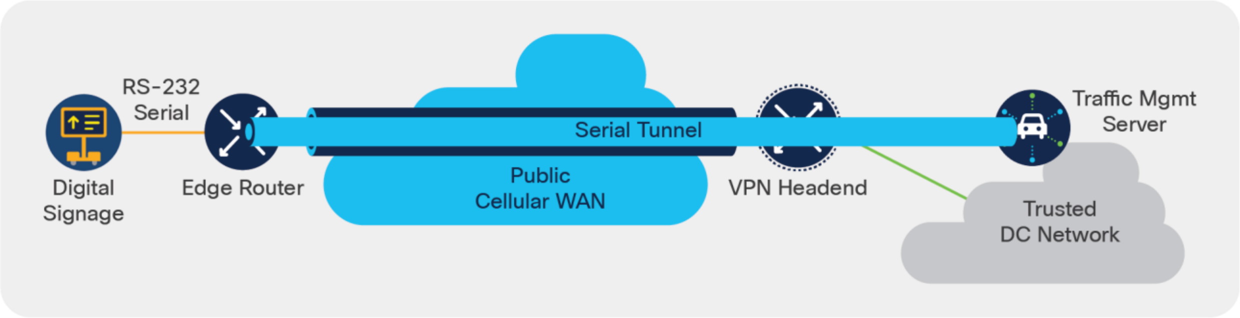


Figure 5.
Serial tunnel over IP

Although the serial port itself can't be secured, the plain-text traffic can be encrypted on the backhaul side as covered in the Backhaul section below.

Securing the Backhaul

The first step is the access port, but then the onwards journey of the packets across the network can also be secured:

Traffic through routers

Routers are often connected with their WAN via cellular public internet. As a best practice, connections are encrypted by the network devices, in this case between the industrial router and a VPN head-end, but this is even more important given that the roadway devices often communicate using protocols that have no transport layer security. The Cisco solution here is FlexVPN,[10] leveraging IPsec with IKEv2, performing all the crypto operations in hardware with no performance hit; FlexVPN is particularly suitable where one or more network address translations (NATs) may take place.

[10] https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

Traffic through switches

Between switches MACsec[11] (IEEE 802.1AE) can be used, where up to 256-bit Advanced Encryption Standard (AES) encryption is employed (at line-rate) to encrypt all the traffic at Layer 2.

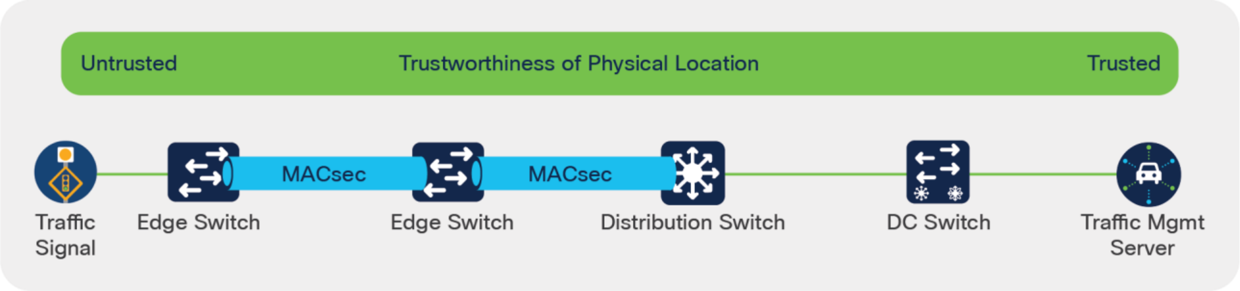


Figure 6.
Switch-to-switch MACsec

This means even if the network traffic itself is unencrypted (at the IP, TCP/UDP or Application layers), the inter-switch physical connections are practically impervious to wiretapping-like attacks, but with no throughput performance or latency impact.

As with 802.1X, certificate-based is a strong and scalable way to manage MACsec, but PSKs may also be used. Note that it may not be necessary to use MACsec for every inter-switch link. For example, in Figure 6 MACsec has been used just at the edge of the network, where physical access is more likely to be compromised.

Note that it is also possible to use MACsec to secure a device's access connection too (between the device and its access switch), but in the ITS ecosystem very few vendors have implemented this capability.

Traffic via radio link

Roadway customers are often faced with scenarios where there is no fiber available, and the use case(s) not suitable for cellular (e.g. demands either large amounts of data that would be very costly, and/or low latency which can often be challenging). Therefore a backhaul based on a high-throughput radio link, with no usage charges, could be very attractive. Cisco Ultra Reliable Wireless Backhaul offers both point-to-point and point-to-multipoint topologies, up to 500Mbps, and with 128-bit AES encryption in hardware, based on line-of-sight.

[11] https://standards.ieee.org/standard/802_1AE-2018.html

Segmentation

The Federal Trade Commission (FTC) provides guidance around network segmentation:

> *"Segmenting your network – for example, having separate areas on your network protected by firewalls configured to reject unnecessary traffic – can reduce the harm if a breach happens. Think of it like water-tight compartments on a ship. Even if one portion sustains damage, water won't flood another part of the vessel. By segmenting your network, you may be able to minimize the harm of a 'leak by isolating it to a limited part of your system" – Federal Trade Commission, US Government.*[12]

Thus by creating a segmented network, isolating groups of roadway devices that do not need to communicate together, such as CCTV cameras and Traffic Signal Controllers, the exposure of a particular group getting compromised is limited to that one group.

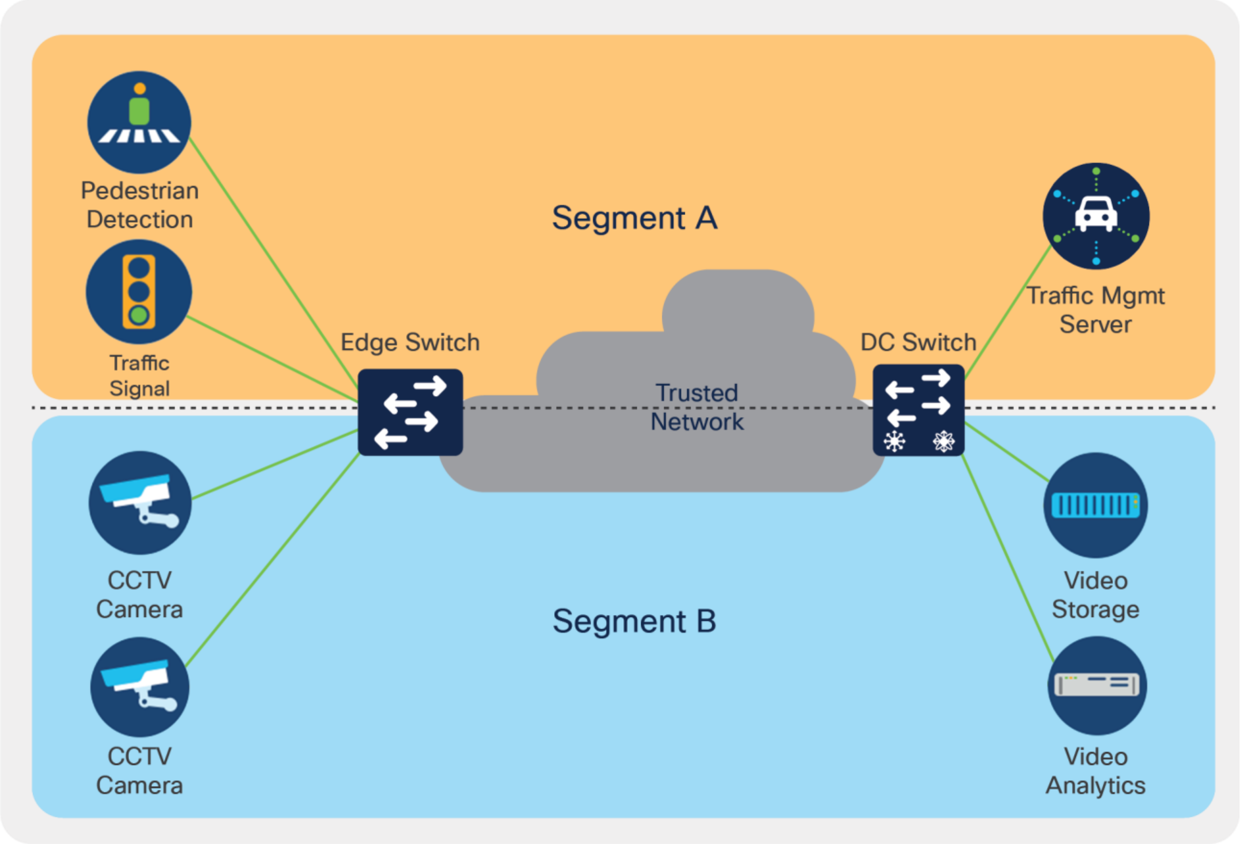


Figure 7.
Example of network segmentation by use case or department

[12] https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-segment-your-network-monitor-whos-trying-get

Network segmentation can be realized using mechanisms like VLANs, Virtual Routing and Forwarding (VRF) etc., but this can be burdensome to deploy and manage on an ongoing basis. The use of software-defined networking and automation, e.g. Cisco's Software-Defined Access solution, is a way to make a segmented network, and one that supports Zero Trust concepts, scalable and supportable. As NIST notes:

> *"Implementation could be achieved by using an overlay network (i.e., layer 7 but also could be set up lower of the OSI network stack). These approaches are sometimes referred to as software defined perimeter (SDP) approaches and frequently include concepts from Software Defined Networks (SDN) and intent-based networking (IBN)." – NIST*[13]

Segmentation can be delivered end-to-end, from edge switch to server, whether that server is across a WAN, in a DC, or even in a private cloud—all of this in a way that is transparent to the roadway devices and their backend components. Furthermore, communication between segments is possible when required, and it is recommended to use a firewall to interconnect the segments, giving fine-grained control over what traffic is allowed, and providing an audit trail of the same.

Authentication, Authorization and Accounting

Authentication, Authorization, and Accounting, more commonly known as "AAA"/triple-A, is a vital step up from having a simple admin account on network devices. Now a user's credentials are authenticated, certain admin functions are then authorized (or not), and there is an accounting audit trail of all actions this user performs while logged in to the network device. A backend AAA server is required, and Cisco ISE can fulfill this role.

[13] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Remote access to roadway devices

Roadway and ITS operators themselves, or sometimes the roadway device vendors in conjunction with the operators, often need remote access to the devices. In the case of the operators there is likely a secure connectivity path, for example if the advice detailed above has been followed. However especially when there are devices connected to an industrial router that is itself connected to the public internet, caution must be observed when granting any remote access to individuals outside the operator's own organization or network.

The Secure Equipment Access[14] (SEA) capability available for Cisco industrial routers (when deployed using Cisco IoT Operations Dashboard) means HTTP/S, SSH, Remote Desktop Protocol (RDP), and Virtual Network Computing (VNC) protocols can be used, securely tunnelled over insecure networks, with audit trail, just using a web browser (no need to install client software).

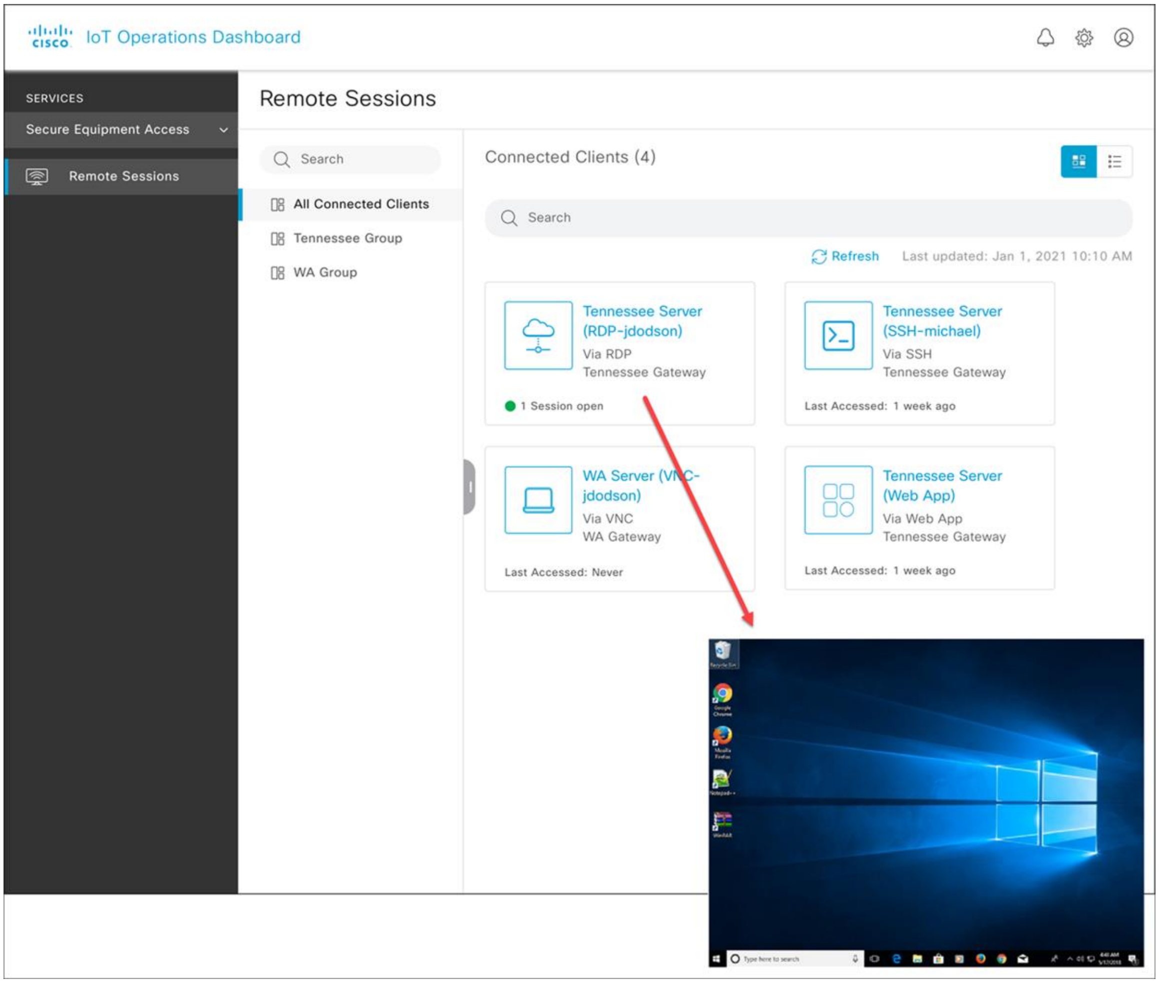


Figure 8.
And RDP session via Secure Equipment Access

Using SEA avoids the need for port forwarding from the WAN interface, thus avoiding unnecessary exposure from the public internet.

[14] https://developer.cisco.com/docs/iotod/#!secure-equipment-access-overview-secure-equipment-access-overview

Conclusion

Roadway and ITS operators and authorities should get ready for Cooperative Intelligent Transportation Systems (C-ITS) and ensure they have a strong cybersecurity posture, starting right at the edge of their networks. Here are six ways:

1. Consider using the GPIO feature on Cisco industrial routers and switches to help secure the physical cabinet—instead of being unaware if the physical security of a cabinet has been compromised.
2. Consider adopting a "Zero Trust" position for connected roadway devices, where 802.1X/MAB is available on both Cisco industrial routers and switches, leveraging Cisco Cyber Vision running on the edge network devices and Cisco ISE running back at the TMC—instead of allowing access to the network for any device that plugs in.
3. Consider encapsulating Ethernet and serial traffic, coming from roadway devices in secure encrypted tunnels, based on FlexVPN and MACsec—instead of potential exposure if a bad actor was able to capture some network traffic and see the sensitive information in plain text. Also consider Cisco Ultra Reliable Wireless Backhaul for up to 500Mbps encrypted connection, where fiber is not available and as a no-usage-charge alternative to cellular.
4. Consider a network segmentation scheme—instead of having a broad exposure if one device or group of devices is compromised.
5. Consider enabling Authentication, Authorization, and Accounting (AAA) on all the roadway network devices—instead of having a single admin password everywhere.
6. When simple and secure remote access is needed for troubleshooting/maintenance, consider using Cisco SEA—instead of punching holes in firewalls, and port-forwarding in from the public internet.

OT and IT can collaborate and partner to reduce the cyber risks, deploying hardware with software features that IT are already experienced with, in the demanding locations and environments that OT need them. Cisco's industrial IoT portfolio and validated designs enable this!

OT and IT can collaborate and partner to reduce cyber risks, deploying hardware with software features that are already very familiar to IT teams. In the demanding locations and environments where roadway connectivity must be safeguarded, Cisco's industrial IoT portfolio and validated designs enable collaboration and achieve secure access connectivity. Secure right from the access port and right across the network, get visibility of what is on the network, use network segmentation, use network encryption where required and get ready for a successful C-ITS deployment.

Learn more

Please see the Connected Communities Infrastructure and Remote and Mobile Assets Cisco Validated Designs (CVDs) for more design and implementation guidance. Visit cisco.com/go/roadways-intersections to learn more.

Appendix

Notes on Physical Security

Different Cisco industrial switches and routers have different capabilities in terms of alarm and I/O connections:

Hardware Model	Number of GPIO ports available	Number of alarm-in ports available
Cisco IR-1101 router		1
Cisco IR-1101 router, with IRM-1101-SPMI	4	1
Cisco IR-1835 router	4	
Cisco IE-3200, 3300 & 3400 switches		2
Cisco IE-5000 switch		4

Example CLI configuration for IR-1101 router, to generate an alarm:

```
ir1101#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
ir1101(config)#alarm contact 0 description >>> Cabinet Door Opened! <<<
ir1101(config)#alarm contact 0 severity critical
ir1101(config)#alarm contact 0 trigger open
ir1101(config)#end
```

Example Syslog messages generate when alarm is triggered and then cleared:

```
Sep 7 12:43:13.978: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External alarm
asserted, Severity: Critical
Sep 7 12:43:29.237: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External alarm
cleared
```

An SNMP trap is also sent. Please see https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/b_IR1101config_chapter_010010.html#con_1106634 for more details.

Please see https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-embedded-event-manager-eem/datasheet_c78-692254.html for more details on Embedded Event Manager (EEM).

An application running on a Cisco IR-1101 or IR-1835 router in the IOx app hosting environment can hook into the GPIO ports, allowing further custom behaviors. Please see https://developer.cisco.com/codeexchange/github/repo/etychon/iox-ir1101-dio-read/ as an example.

Notes on Securing the Access Connection

```
Example CLI configuration snippet for configuring port access on an IE-3400 switch:
ie3400#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
ie3400(config)#interface GigabitEthernet0/5
ie3400(config-if)#switchport mode access
ie3400(config-if)#ip device tracking maximum 10
ie3400(config-if)#access-session host-mode single-host
ie3400(config-if)#access-session closed
ie3400(config-if)#access-session port-control auto
ie3400(config-if)#mab
ie3400(config-if)#dot1x pae authenticator
ie3400(config-if)#service-policy type control subscriber Dot1xOrMAB
ie3400(config-if)#end
```

This is an example where only if the connected device is authorized by the NAC server will it be given network access. Please see the Connected Communities Infrastructure CVD for much more implementation detail: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/IG/cci-ig/cci-ig.html.

A variety of Cisco industrial routers connect serial devices, and are commonly deployed in the ITS/roadway settings. They have different port counts and protocol support:

Router Model	Number of RS-232 ports	Number of RS-485 ports
Cisco IR-1101 router	1	
Cisco IR-1821 router	1	
Cisco IR-1831 & 1833	2	
Cisco IR-1835 router	2*	1*

* There are two serial ports total on an IR-1835, one of which can be configured as either RS232 or RS485.

An example CLI configuration for IR-1101 router, to enable serial traffic to be tunneled over a TCP/IP connection:

```
ir1101#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
ir1101(config)# line 0/2/0
ir1101(config-line)# raw-socket tcp client 192.168.100.100 4000
ir1101(config-line)# raw-socket packet-length 512
ir1101(config-line)# raw-socket tcp idle-timeout 10
ir1101(config-line)# raw-socket tcp keepalive 5
ir1101(config-line)# end
```

Notes on Securing the Backhaul

The MACsec capabilities of switches commonly deployed at the roadside and in ITS deployments:

Switch Model	Typical Role	MACsec 128-bit AES	MACsec 256-bit AES
Cisco IE-3200	Edge switch	Y	
Cisco IE-3300 & 3400		Y	Y*
Cisco IE-5000	Distribution switch	Y	
Cisco Catalyst® 9300		Y	Y
Cisco Catalyst 9500		Y	Y

* Requires Network Advantage license

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C11-2696871-00 11/21