iSwitch Series

www.ieiworld.com

IIoT Wireless 4G LTE Router

ISR-2G Series

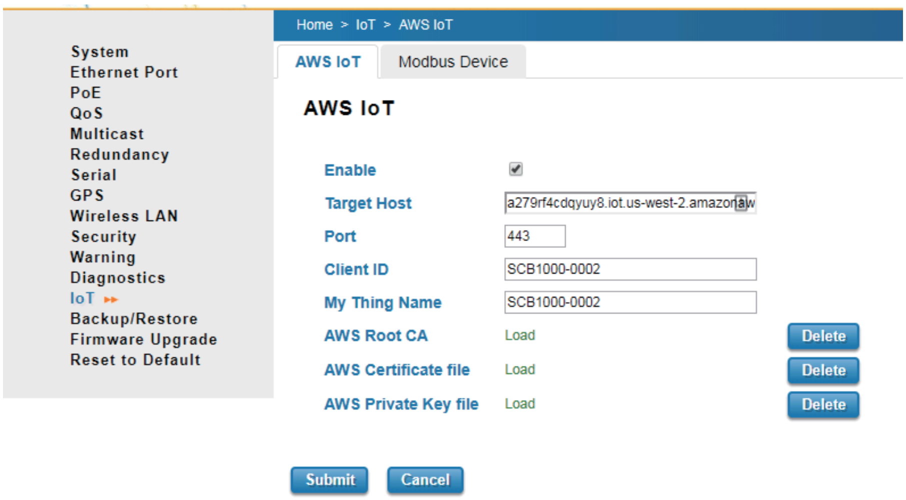
Secured and Rugged LTE Router for IIoT

- Single or dual 4G LTE Cat 4 / Cat 6* Routing
- One SIM + Micro SD or Dual SIM standby or Embedded SIM
- Wi-Fi networks (5G 802.11ac/a/n or 2.4G 802.11b/g/n)
- 2T2R Wi-Fi radio delivers up to 866Mbps high throughput
- 2-port Gigabit Ethernet Routing and Bridging
- One or Two RS232/422/485 DB9 ports for IIoT devices
- OpenVPN, IPsec for secured connection
- USB for easy field configuration and firmware upgrade
- Cellular to WAN redundancy, dual SIM backup
- Cellular to WLAN auto offload
- 1:1 NAT, port forwarding and NAPT for local traffic protection
- Support RIPv2, static routing
- Built-in Cloud AWS Agent, Azure Agent
- Support TACACS+ multi-user authentication for privileged user management
- Support OpenWRT open platform by request
- -40~75°C wide operation temperature
- EN 50121-4 railway compliance

Lte 5G 802.11ac/a/n 2.4G 802.11b/g/n IEC61000-6-2 IEC61000-6-4 EN50121-4 amazon webservices Microsoft Azure OpenWrt Wireless Freedom

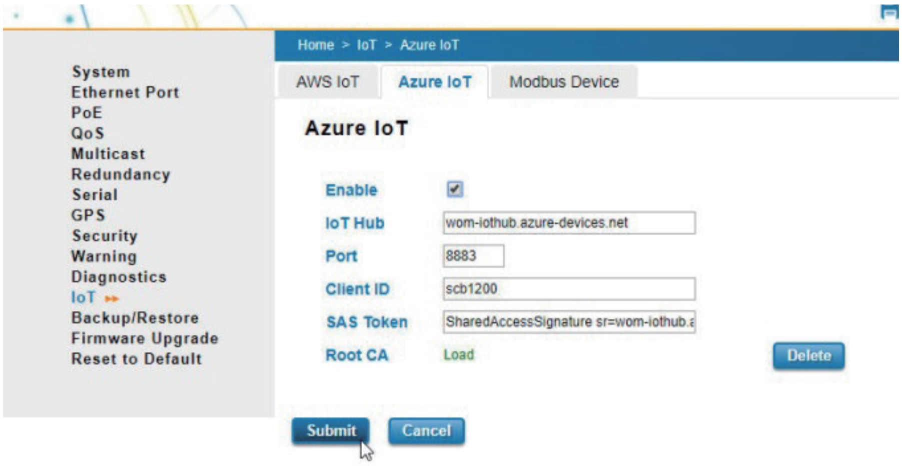
Model	OS	WAN	LAN	Serial	Radio 1	Radio 2	USB	SD	SIM	GPS	DI/DO	PW Input	Temp.	Standard
ISR-2G-R10	Embedded	1 x GE	1 x GE	2 x RS232/ 422/485	-	-	1	1	-	-	0/1	12/24/48 VDC	40~75°C	EN 50121-4 EN 301489 LVD 62368-1 Radio RED compliance
ISR-2G-WL-R10					Wi-Fi 2.4G 11n/ 5G 11ac	-	1	1	-	-	0/1			
ISR-2G-LTE-(E/CN/U)-R10					LTE Cat.4	-	1	1	1	-	0/1			
ISR-2G-LTE6-(E/CN/U)-R10					LTE Cat.6	-	1	1	1	-	0/1			
ISR-2G-LTE-(E/CN/U)-WL-GPS-R10					Wi-Fi 2.4G 11n/ 5G 11ac	LTE Cat.4	1	1	2	Yes	0/1			
ISR-2G-LTE6-(E/CN/U)-WL-GPS-R10					Wi-Fi 2.4G 11n/ 5G 11ac	LTE Cat.6	1	1	2	Yes	0/1			

AWS/Azure IoT Edge-Ready Gateway Built in AWS and Azure IoT agent



AWS IoT

Enable	☑
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaw
Port	443
Client ID	SCB1000-0002
My Thing Name	SCB1000-0002
AWS Root CA	Load
AWS Certificate file	Load
AWS Private Key file	Load



Azure IoT

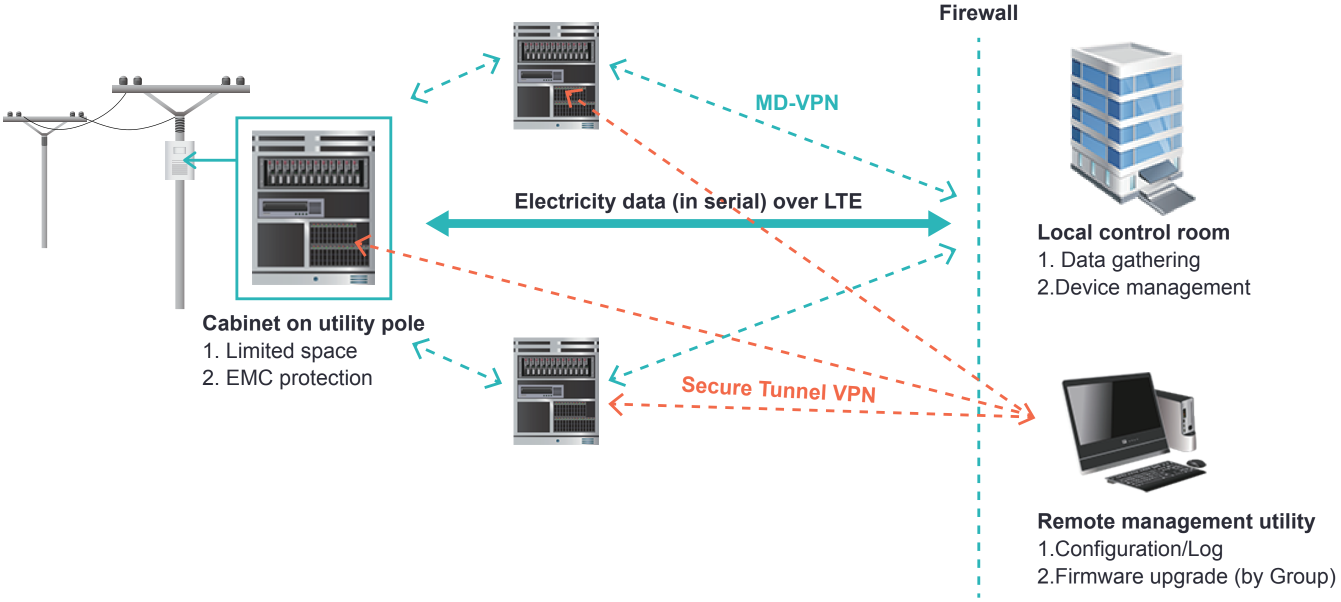
Enable	☑
IoT Hub	wom-iothub.azure-devices.net
Port	8883
Client ID	scb1200
SAS Token	SharedAccessSignature sr=wom-iothub.a
Root CA	Load

Power Distribution

An electric power distribution system is the final stage in the delivery of electric power; it carries electricity from the transmission system to individual consumers. The real time status of the system is critical to improve the efficiency of the power distribution system. As it is highly distributed throughout customer premises and is often installed in utility poles, the use of cellular network to send status report or event alarm is increasing. Rugged design for outdoor environment and support of VPN is the key factor to plan solution.

Topology description:

ISR-2G-LTE-E-R10 is installed inside the electrical power distribution cabinet on top of the utility pole. The electricity data in serial interface is transmitted over LTE to control center. The management is carried out through secured VPN tunnels.



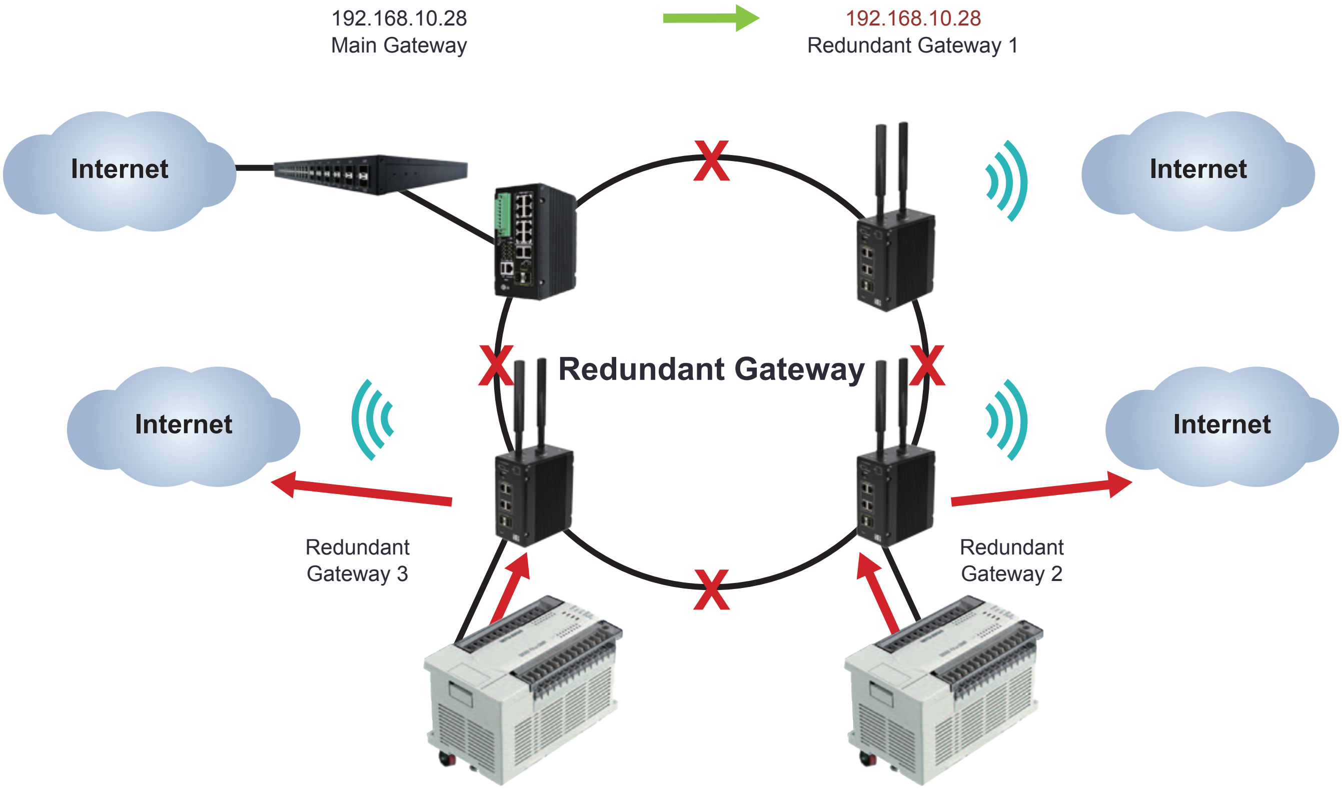
Why choose ISR-2G-LTE-E-R10 for Power Distribution networks:

- High-speed 4G LTE routing for remote monitoring
- 2-port Gigabit Ethernet Routing and Bridging and Two RS232/422/485 ports for onsite devices (IED, power meter, thermometer, etc.)
- OpenVPN, IPsec for secured connectivity, and USB for easy field configuration and firmware upgrade
- SD for field diagnostic log or extended application
- -40~75°C wide operation temperature for unfavorable conditions
- Compact size for cabinet or utility pole installation

Redundant Gateway

The open standard ITU-T G.8032 ERPS Ring topology is often deployed in industrial network applications to ensure the reliability of the network. In normal state, all traffic goes out through the main gateway. When a node in the ring network fails, the data packet will be transmitted through the redundant path to the main gateway. However, when there are multiple nodes in the ring network fail at the same time, the Ring redundant network will be cut in pieces, and cause some devices will not be able to transmit information and get on the network properly.

The Redundant Gateway technology is based on the ERPS mechanism to periodically check the main gateway status in the ERPS Ring network connection status. When the main gateway is not available, the redundant gateway will change its IP address to the main gateway's one, so the devices in the network can connect to the network in a seamless way. The multiple redundant gateway settings secures the network even when multiple nodes fail in a network.



Industrial Cellular PoE Routing Switch

ISR-4GP-2S-LTE-(E/CN/U)-R10

Wireless Backup for ERPS v2 Network by LTE PoE Router

- High-speed LTE Cat.4 routing and dual SIM standby
- Full-Giga: 4x 1000M RJ45 Copper + 2 100/1000M SFP Fiber
- 4-port PoE IEEE 802.3af/at 30W per port and 120W total PoE budget
- ITU-T G.8032 ERPSv2 Ring Redundancy
- Ring failure to LTE Redundancy
- VRRP redundancy
- OpenVPN, IPsec for secured connection
- USB for easy field configuration and firmware upgrade
- Built-in Cloud AWS Agent, Azure Agent
- Support TACACS+ multi-user authentication for privileged user management
- -40~75°C wide operation temperature
- EN 50121-4 railway compliance
- NMS system for individual node monitoring
- Remote configuration software utility for distributed management

802.3 at PoE+ Lte ERPS G.8032v2 VPN EN50121-4

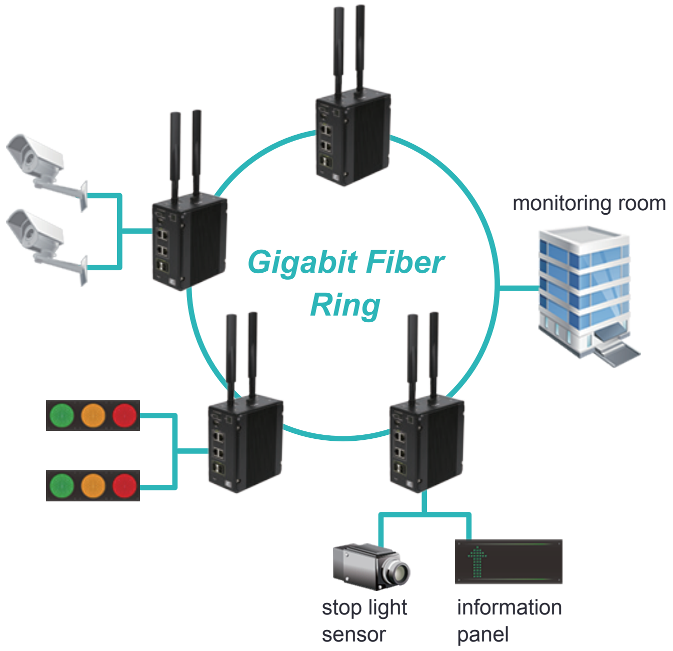
Model	Eth-LAN	PoE	Radio 1	USB	SD	SIM	DI/DO	Power Input	Temp.	Certification
ISR-4GP-2S-LTE-(E/CN/U)-R10	4 x GE 2 x GF SFP	4 x GE	LTE Cat.4	1	-	2	0/1	48/54 VDC	-40~75°C	EN 50121-4 compliance

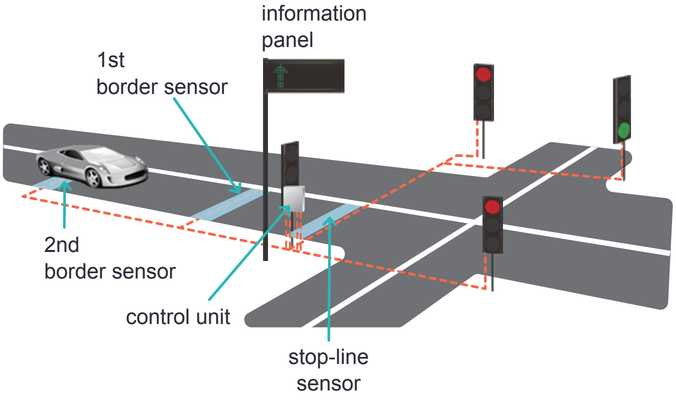
Traffic Control

Road Traffic control systems are vital for safety of all pedestrians and vehicles. Thus, it is critically important to deploy dynamic network infrastructure with strong consideration of fast data transmission, long distance of the data communication and unfavorable weather conditions. The demand is growing for rugged equipment suitable for transmitting real-time data to Monitoring Center as well as providing PoE functionality with PD fault-detection and very low to zero network recovery time.

Topology description:

- Multiple ISR-4GP-2S-LTE-E-R10 form Gigabit Fiber Ring network to connect all the traffic control devices to Control Center.
- Traffic control devices include: control units connected to road controllers, LED traffic lights, variable information signs, info screens, electronic devices for measuring vehicle movement parameters (control borders) using radio-frequency identification tools (readers).



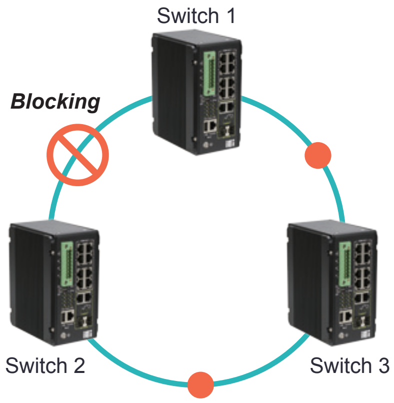


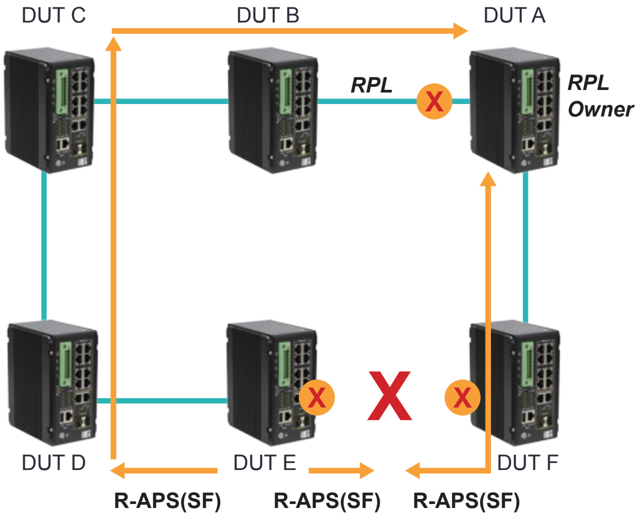
Why choose ISR-4GP-2S-LTE-E-R10:

- High-speed LTE routing for fast data transmission and dual SIM card slots for selecting the best performing network
- Up to 4-port Giga PoE Plus for delivering up to 30W per port PoE to traffic control system devices, collecting on-site data
- 2-port Giga SFP/ST/SC Fiber ports for long-distance connectivity with control center
- ITU-T G.8032 v1/v2 ERPS Ring Redundancy for interoperability, loop protection and fast network recovery
- OpenVPN, IPsec for network security
- -40~75°C wide operation temperature for operation in harsh weather conditions

ERPS

ERPS (Ethernet Ring Protection Switching) is the first industry standard (ITU-T G.8032) for Ethernet ring protection switching. It is achieved by integrating matured Ethernet operations, administration, and maintenance (OAM) functions and a simple automatic protection switching (APS) protocol for Ethernet ring networks. It provides sub-50ms protection for Ethernet traffic in a ring topology and ensures that there are no loops formed at the Ethernet layer. The first version supported a single ring architecture and the second version is expected to address multiple inter-connected rings.





The Failure Condition

When a failure is detected on a ring port, known as a Signal Fail (SF), the node detecting the failure will generate an R-APS (SF) message. The RPL nodes remove the block on the RPL link, and all the nodes perform a Forwarding Database (FDB) flush which allows traffic to quickly return. When a node on the link detects a fault, it immediately blocks the faulty node and reports the fault message (R-APS (SF)) to all the other devices in the ring. After receiving the message, all other nodes refresh the FDB. The RPL owner port receives the fault message, and the recovery port is in the forwarding state. The ERPS ring enters the protection state.

The Failure Recovery

- When the RPL Owner receives R-APS(NR) message it starts WTR timer. Once WTR timer expires, RPL Owner blocks RPL and transmits R-APS (NR, RB) message
- Nodes receiving the message – perform a FDB Flush and unblock their previously blocked ports.
- Ring is now returned to Idle state

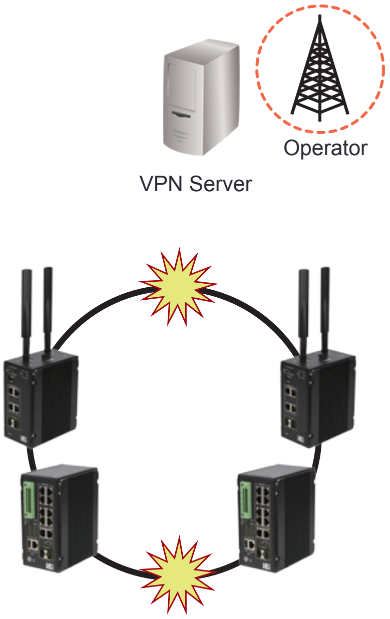
Benefits of adapting ITU-T G.8032 v2 Ethernet Ring Protection Switching

- The mechanisms and protocol defined in G.8032 v2 ERPS is tending to replace proprietary ring redundancy and standard Ethernet Ring Switching, as it provides stable protection of the entire Ethernet Ring from any loops.
- G.8032 v1 standard supported single ring topology, whilst G.8032 version 2 additionally provides recovery switching for Ethernet traffic in Multiple Ring (ladder) of conjoined Ethernet Rings by one or more interconnections which saves deployment costs by providing wide-area multipoint connectivity with reduced number of links.
- Important to note, deploying switches supporting G.8032 v2 ERPS provides economical and highly resilient Ethernet infrastructure, as they can interoperate with third party switches and still guarantee fast network recovery time without any data loss.

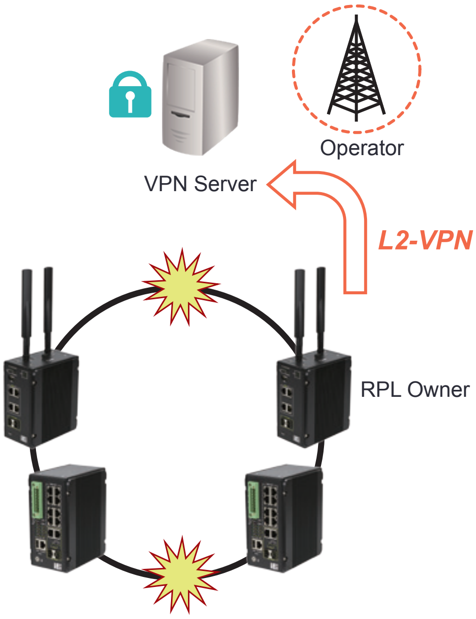
ERPS Backup by Wireless Network

G.8032 ERPS is crucial deployment in the industrial redundant network. However it can only protect in one link failure of a Ring. If there is more than one links failed, the ERPS Ring will still break. The Wireless ERPS Backup technology uses L2 VPN to provide the wireless L2 backup mechanism.

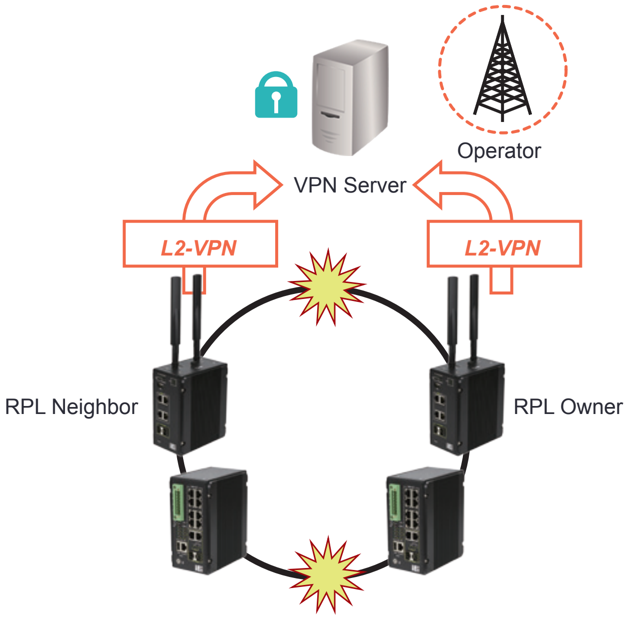
1. More than one link failure occurs



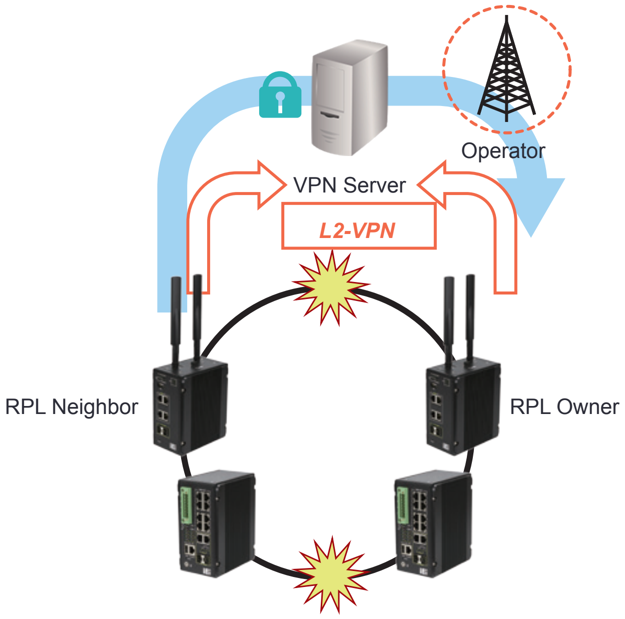
2. RPL Owner create the L2 VPN connection to VPN Server



3. RPL Neighbor creates the L2 VPN connection to VPN Server



4. The ERPS Ring is still working through the L2 VPN

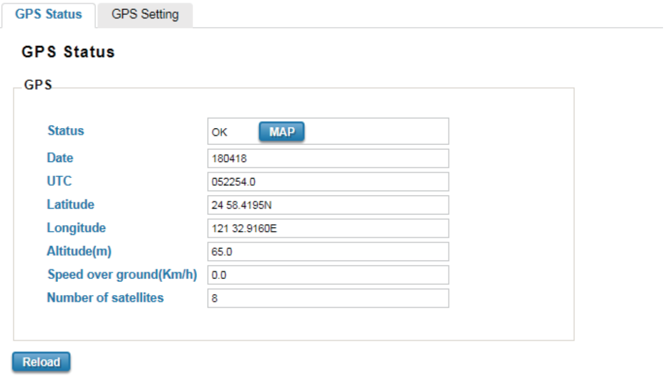


Industrial Cellular Wi-Fi Boost PoE Routing Switch

ISR-8P-1G-LTE-(E/CN/U)-WL-R10

Integrate PoE Switch + Wireless Router + (Dual radio) AP for BUS/ Vehicle

- LTE Cat.4, 2x2 MIMO, 150M downlink and 50M uplink
- 5G/2.4G Wi-Fi for local coverage, up to 866Mbps bandwidth
- 8 x Fast Ethernet PoE+ ports, up to 120W PoE power budget
- 12/24V to 54VDC Booster PoE
- 1 x Gigabit Ethernet WAN port for uplink or NVR
- WAN to LTE Redundant
- GNSS supports GPS/GLONASS/BeiDou/Galileo
- Periodically Report GPS data for Real time Location Tracking
- OpenVPN, IPsec for secure connection
- Built-in Cloud AWS Agent, Azure Agent
- Railway EMC: EN 50121-4
- EN 61000-6-2/EN 61000-6-4 heavy industrial EMC
- Vehicle: E-mark compliance



GPS Status

GPS

Status	OK
Date	180418
UTC	052254.0
Latitude	24 58.4195N
Longitude	121 32.9160E
Altitude(m)	65.0
Speed over ground(Km/h)	0.0
Number of satellites	8

Model	Radio 1	Radio 2	Eth-WAN	Eth-LAN	USB	SIM	eSIM (Optional)	GPS	Power Input
ISW-8-1G-L2-R10	-	-	1 x GbE	8xFE	1	0	-	-	8~32VDC
ISW-8P-1G-L2-R10	-	-	1 x GbE	8 x FE PoE	1	0	-	-	8~32VDC
IWSW-8-1G-2WL-R10	802.11ac	802.11ac	1 x GbE	8 x FE	1	0	-	-	8~32VDC
IWSW-8P-1G-2WL-R10	802.11ac	802.11ac	1 x GbE	8 x FE PoE	1	0	-	-	8~32VDC
ISR-8-1G-LTE-(E/CN/U)-WL-R10	802.11ac	LTE Cat.4	1 x GbE	8 x FE	1	2 Redundant	1	Yes	8~32VDC
ISR-8P-1G-LTE-(E/CN/U)-WL-R10	802.11ac	LTE Cat.4	1 x GbE	8 x FE PoE	1	2 Redundant	1	Yes	8~32VDC

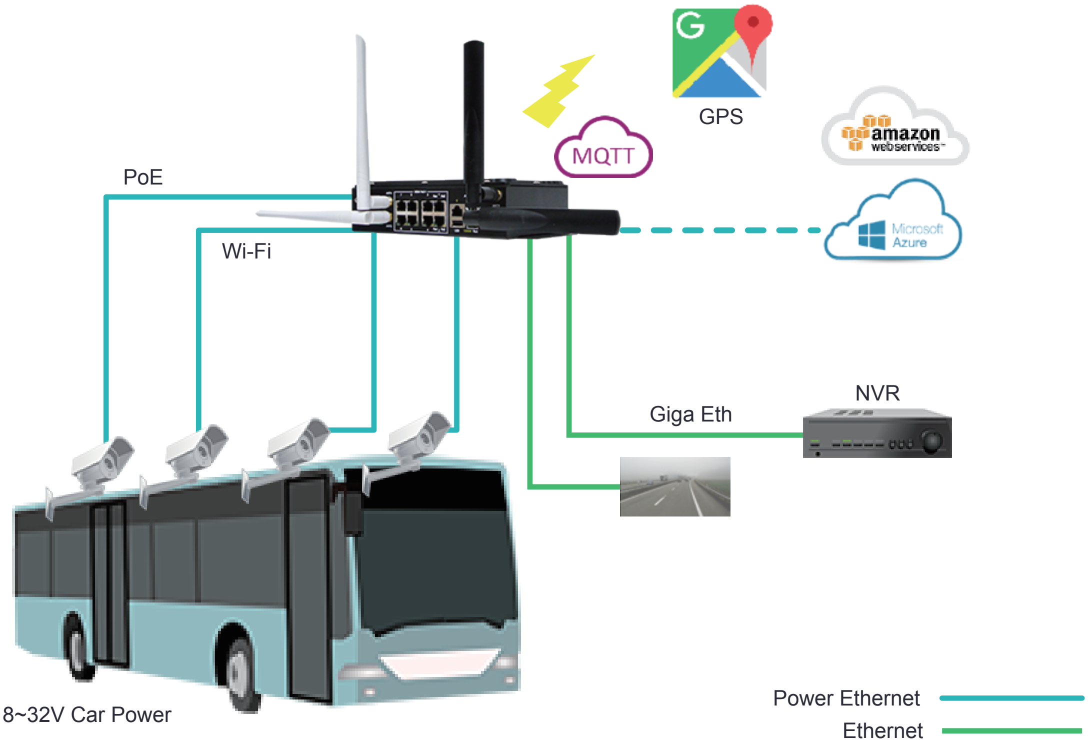
BUS

For preventing and resolving emergency situations, transport administrators deploy IP-surveillance network capable of capturing high-definition video footage.

The process of network deployment on moving vehicles encounters a variety of challenges, such as climatic conditions, extended temperatures, humidity, shock and vibration. Therefore ruggedized network devices that can perform stably over harsh environment is the only solution.

Topology description:

ISR-8P-1G-LTE-E-WL-R10 provides 8 port 10/100Mbps IEEE 802.3at PoE and 1 x Gigabit WAN for NVR/Uplink. The built-in dual radios, LTE/GPS plus Wi-Fi provide seamless routing connectivity to private or public cloud server. Dual SIM & eSIM is also supported. The 8~32V Booster PoE is suitable for BUS or vehicle power supply.

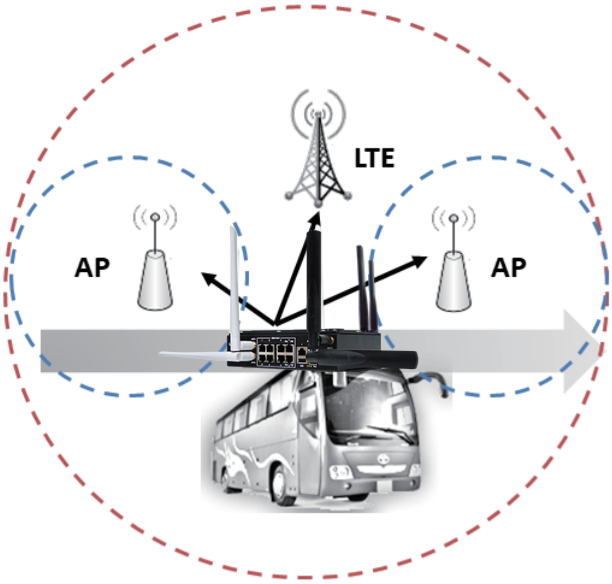


Why ISR-8P-1G-LTE-E-WL-R10 is chosen for vehicle onboard installation:

- Combine PoE Switch + Wireless Gateway
- 8 x 10/100Mbps IEEE 802.3at PoE
- 1 x Gigabit WAN for NVR/Uplink
- Dual Radio, LTE/GPS + Wi-Fi or 2xWi-Fi
- Dual SIM & eSIM supported
- 8~32V Booster PoE, max. 120W budget
- Seamless Wi-Fi and LTE Auto-offload

Auto-Offload

When the BUS approaches to the main station, it will transmit the data of surveillance videos and traffic information to the station via Wi-Fi network of the station. However if the data is big, it may not able to finish the transmission before departure. The Auto-Offload technology allows moving devices to seamlessly switch Wi-Fi network to LTE network without stopping the communication.



In the normal state, the cellular network such LTE acts as backup channel. The device will constantly detect the Wi-Fi & LTE signal strength. When the Wi-Fi signal is below the threshold, it will automatically switch to LTE and keep the data transmission.

If the vehicle stays in the single edge of Wi-Fi AP zone, the active interface of wireless will be very unstable. The wireless interface changes to LTE when Wi-Fi signal is in Low state, and prevent the frequently change problem. It continuously checks Wi-Fi connection status until Wi-Fi signal is stable (Upper state), and activates the wireless interface back from LTE to Wi-Fi.

Outdoor IEEE 802.11a/n Wireless AP

IWAP-211 Series

- Compliant with IEEE 802.11a/n with 2T2R MIMO and data rate up tp 300 Mbps
- Long wireless transmission distance up to 2km
- Built-in WPA, WPAa/ 802.1X/ Firewall security
- Multiple operating modes: Wireless AP/Client/Brige for different application
- IGMP snooping and WMM QoS ideal fro video streaming
- Outdoor waterproof IP55 enclosure
- 24V Passive PoE and Pole mount installation for wayside surveillance application
- -20~70°C operating temp. for harsh environments

WiFi 802.11a/n IP55

Model	Eth-LAN	Radio	Power Input	Temp.	Antennas	Certification
IWAP-211-R10	1 x FE PoE	Wi-Fi 5G 11a/n	24 VDC	-20~70°C	2 x Default Antennas, 5dBi	EN 301489 EN 55032 EN 60950
IWAP-211B-R10	1 x FE PoE	Wi-Fi 5G 11a/n	24 VDC	-20~70°C	11 dBi +/- 2 dBi Internal	EN 301489 EN 55032 EN 60950

Rugged L2/L3 PoE Switch

ITU-T G.8032 v1/v2 ERPS Ring Redundancy

- The ITU-T G.8032 standard for Ring redundancy Protocol
- Provide sub-50ms protection and recovery switching for Ethernet traffic
- Interoperate with 3rd party industrial switch and still remain fast recovery time
- Interoperate with commercial switch instead of STP/RSTP
- Efficient network interconnection and topology with ERPS Chain, multiple chains

Dynamic L3 Routing with Redundancy Protection

- RIPv1&v2, OSPFv1&v2 for intra-domain routing within an autonomous system
- Efficient unicast/multicast static routing
- VRRP guarantees sustainable routing in a single point of failure

NEMA TS2 EN50121-4 ERPS G.8032v2 Cyber Security

L3 PoE+

Management Features

- Various configuration paths, including WebGUI, CLI, SNMP and RMON
- IEEE 1588v1/v2 PTP time management
- LLDP topology control
- USB for easy field configuration and firmware update
- Software utility interface for LAN devices management
- NMS for individual component monitoring

Enhanced Cyber Security for Critical Applications

- L2-L7 IPv4/IPv6 Access Control List (ACL)
- DHCP Snooping, IP Source Guard, Dynamic ARP Inspection
- 802.1Q VLAN, Private VLAN, Advanced Port Security
- Multi-Level user passwords
- HTTPS/SSH/SFTP, 256-bit encryption
- 802.1X MAB for non-802.1X compliant end devices
- RADIUS/TACACS+ centralized password authentication

Rugged Design for Wayside Surveillance

- EN 50121-4 for railway trackside applications
- Top level EMC protection and excellent heat dissipation design for operating in -40~75°C environment
- EN 61000-6-2/4 Heavy Industrial Environment

Extreme PoE Capability

- 8-port IEEE 802.3af/at compliant PoE, up to 30W/port
- Up to 240W power budget
- Complete PoE management including per-port Power Budget Control, PoE Scheduling and PoE Status

Rugged Ethernet L2/L3 Switch

ERPS G.8032v2 | Cyber Security | L3 | EN50121-4 | IEC61850-3 IEEE1613

Dynamic Routing with Redundancy Protection

- RIPv1&v2, OSPFv1&v2 for intra-domain routing within an autonomous system
- Efficient unicast/multicast static routing
- VRRP guarantees sustainable routing in a single point of failure

Management Features

- Various configuration paths, including WebGUI, CLI, SNMP and RMON
- IEEE 1588v1/v2 PTP time management
- LLDP topology control
- USB for easy field configuration and firmware update
- Software utility interface for LAN devices management
- NMS for individual component monitoring

ITU-T G.8032 v1/v2 ERPS Ring Redundancy

- The ITU-T G.8032 standard for Ring redundancy Protocol
- Provide sub-50ms protection and recovery switching for Ethernet traffic
- Interoperate with 3rd party industrial switch and still remain fast recovery time
- Interoperate with commercial switch instead of STP/RSTP
- Efficient network interconnection and topology with ERPS Chain, multiple chains

Enhanced Cyber Security for Critical Applications

- L2-L7 IPv4/IPv6 Access Control List (ACL)
- DHCP Snooping, IP Source Guard, Dynamic ARP Inspection
- 802.1Q VLAN, Private VLAN, Advanced Port Security
- Multi-Level user passwords
- HTTPS/SSH/SFTP, 256-bit encryption
- 802.1X MAB for non-802.1X compliant end devices
- RADIUS/TACACS+ centralized password authentication

Rugged Design for Wayside Surveillance

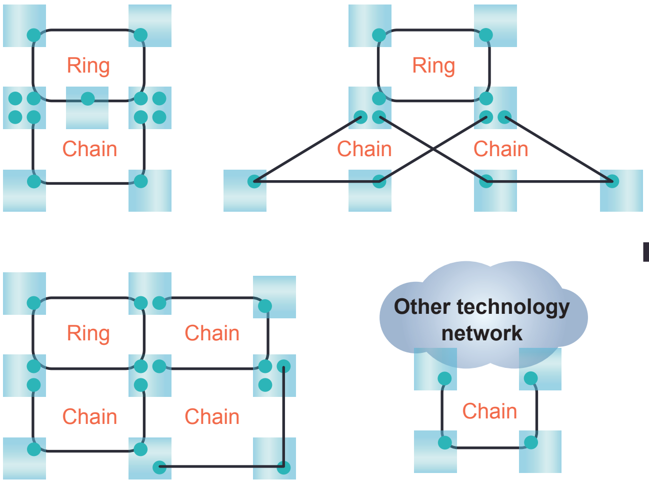
- EN 50121-4 for railway trackside applications
- Top level EMC protection and excellent heat dissipation design for operating in -40~75°C environment
- 240W extra high power budget for all kinds of power requirements
- EN 61000-6-2/4 Heavy Industrial Environment

IEC 61850-3 for Power Utility Applications

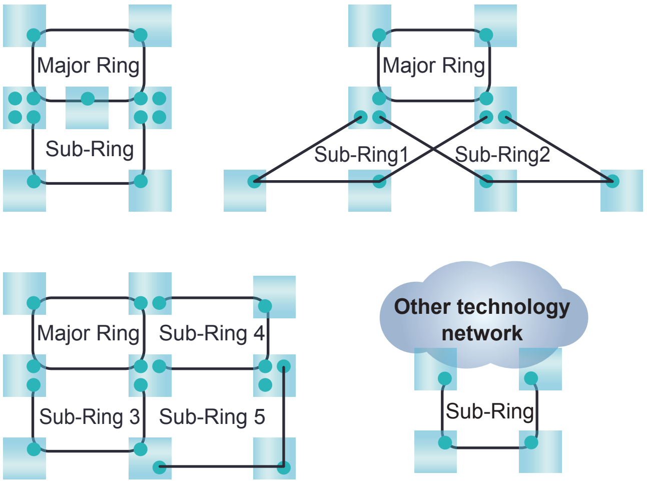
Model	PoE	Ethernet Copper	Ethernet Fiber	L3 Switch	L2 Switch	ERPS v2	USB	Power input	Vertical Standard
IDSW-1-(M/S)-SC-R10	-	1 x FE	1 x FE SC/ST*	-	-	-	-	12/24/48VDC	EN 50121-4 compliance
IDSW-5-R10	-	5 x FE	-	-	-	-	-	5/24VDC	Heavy industrial
IDSW-8-R10	-	8 x FE	-	-	-	-	-	12/24/48VDC	Heavy industrial
IDS-6-(MM/SS)-2SC-R10	-	6 x FE	2 x FE SC/ST*	-	-	-	-	12/24/48VDC	Heavy industrial
IDSW-8G-R10	-	8 x GE	-	-	-	-	-	12/24/48VDC	Heavy industrial
IDSW-8-2G-R10	-	8 x FE+ 2 x GE	-	-	-	-	-	12/24VDC	EN 50121-4
IDSW-8-2GCO-L2-R10	-	8 x FE	2 x GE Combo	-	Yes	Yes	1	24/48VDC	EN 50121-4
IDSW-4G-2GS-L2-R10	-	4 x GE	2 x GE SFP	-	Yes	Yes	1	12/24/48VDC	EN 50121-4 compliance
IDSW-6G-3GCO-L2-R10	-	6 x GE	3 x GE Combo	-	Yes	Yes	1	12/24/48VDC	EN 50121-4
IDSW-2G-2GCO-6GS-L2-R10	-	2 x GE	2 x GE Combo 6 x GE SFP	-	Yes	Yes	-	12/24/48VDC	EN 50121-4 compliance
IDSW-8G-4GS-L2-R10	-	8 x GE	4 x GE SFP	-	Yes	Yes	1	12/24/48VDC	EN 50121-4 IEC 61850-3
IDSW-8G-4GS-L3-R10	-	8 x GE	4 x GE SFP	Yes	Yes	Yes	1	12/24/48VDC	EN 50121-4 IEC 61850-3
IDSW-8GP-R10	8 x GE 802.3at	-	-	-	-	-	-	48/54VDC	Heavy Industrial
IDSW-8P-2G-R10	8 x FE 802.3at	2 x GE	-	-	-	-	-	12/24VDC	EN 50121-4
ISW-8P-1G-L2-R10	8 x FE 802.3at	1 x GE	-	-	Yes	-	1	12/24VDC	EN 50121-4
IDSW-8P-2GCO-L2-R10	8 x FE 802.3at	-	2 x GE Combo	-	Yes	Yes	1	48/54VDC	EN 50121-4
IDSW-4GP-2GS-L2-R10	4 x GE 802.3at	-	2 x GE SFP	-	Yes	Yes	1	48/54VDC	EN 50121-4 compliance
IDSW-8GP-4GS-L2-R10	8 x GE 802.3at	-	4 x GE SFP	-	Yes	Yes	1	48/54VDC	EN 50121-4
IDSW-8GP-4GS-L3-R10	8 x GE 802.3at	-	4 x GE SFP	Yes	Yes	Yes	1	48/54VDC	EN 50121-4

Advanced ITU-T G.8032 ERPSv2

Legacy Ring / Chain Solution



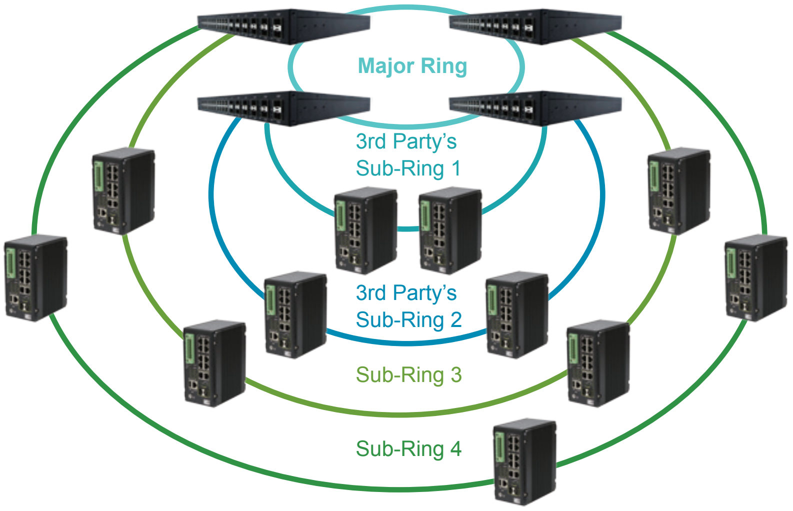
New ERPSv2 Standard



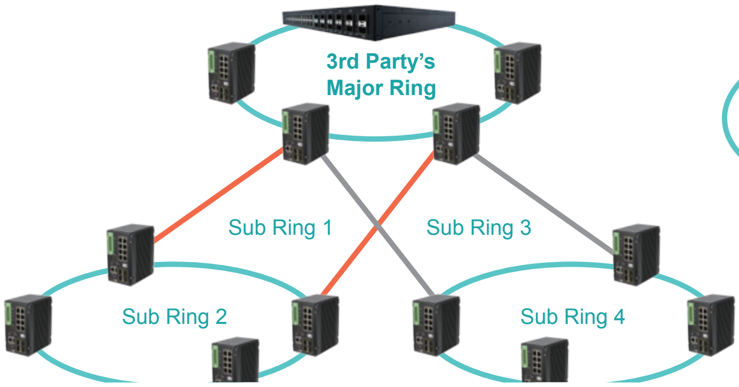
- Support ERPSv2, HW-based CCM
- Overcome GbE copper physical limitation
- Recovery time < 50ms@250pcs
- Inter-Operability with 3rd Party devices
- Replace Ring + Chain + Dual Homing

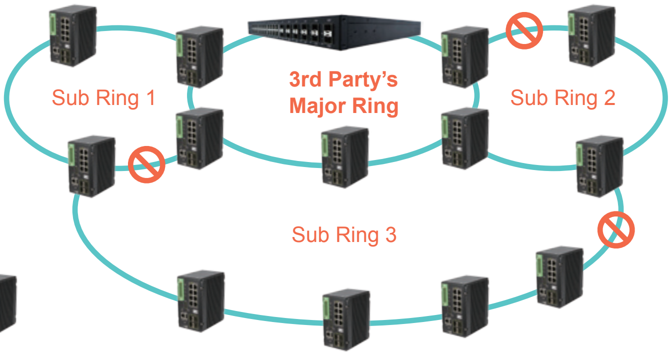
Interface	Recovery time
100M Copper/Fiber	10ms@250pcs
10GbE Copper/Fiber	20ms@250pcs
GbE Copper w.CCM	20ms@250pcs
GbE Fiber	20ms@250pcs

ERPSv2 is flexible to replace Chain



ERPSv2 can easily replace Dual Homing to 3rd party proprietary Ring



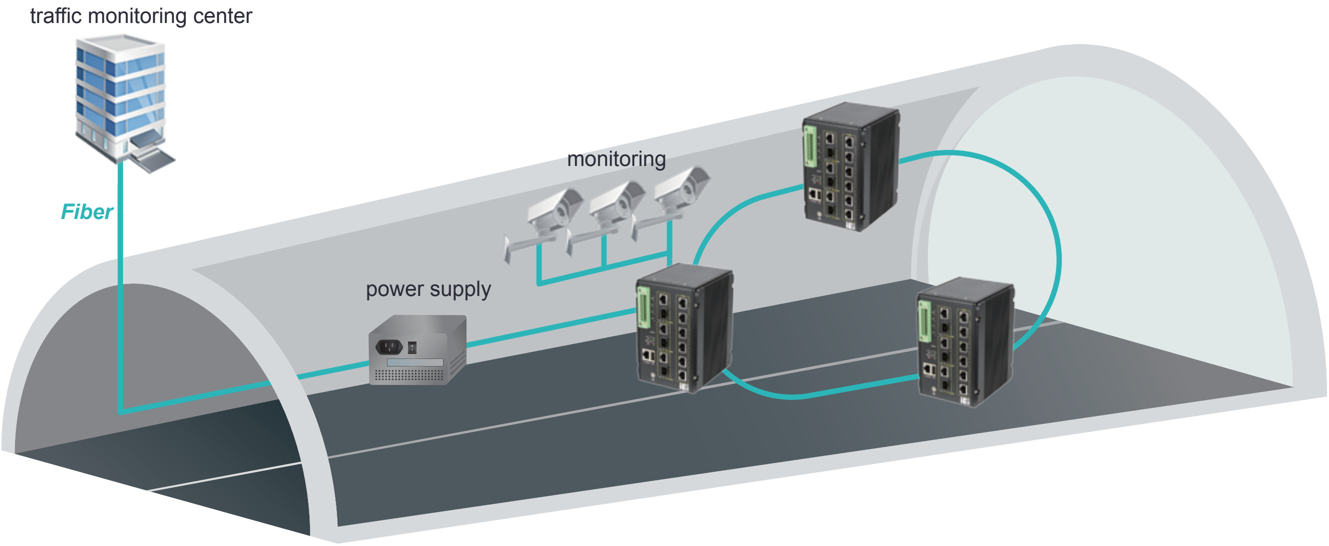


Tunnel

City Administrations widely adapt IP-surveillance for remote tunnel traffic monitoring and data driven decision making in case of accidents and other emergencies. When deploying IP-surveillance network in tunnels, system integrators encounter a number of challenges need to be addressed, such as long distances, humid and dusty environmental conditions in tunnels, as well as frequent vibrations and shock caused by moving vehicles.

Topology description:

IDSW-6G-3GCO-L2-R10 are connected in Gigabit Fiber Ring topology. They collect and further transfer the captured IP-video streams to the Traffic Monitoring Center.



Why IDSW-6G-3GCO-L2-R10 is chosen for tunnel installation:

- Ultra-high throughput for IP-video stream achieved with 9-port Full Gigabit Ethernet
- Long distance fiber connectivity through 3 SFP combo ports
- Convenient management: WebGUI, CLI, SNMP and RMON -USB for on-site configuration and firmware upgrade
- NEMA TS2 compliance for wayside traffic control assemblies
- 10~60VDC wide power range design with redundant power inputs suitable for different types of tunnel power supply equipment
- Rugged design for unfavorable tunnel environments with excellent heat dissipation for operating in -40~75°C
- High level EMC protection exceeding traffic control requirements
- Supports the latest ITU-T G.8032 v1/v2 ERPS Ring Redundancy for sub50ms protection recovery switching and high interoperability with 3rd party industrial switches

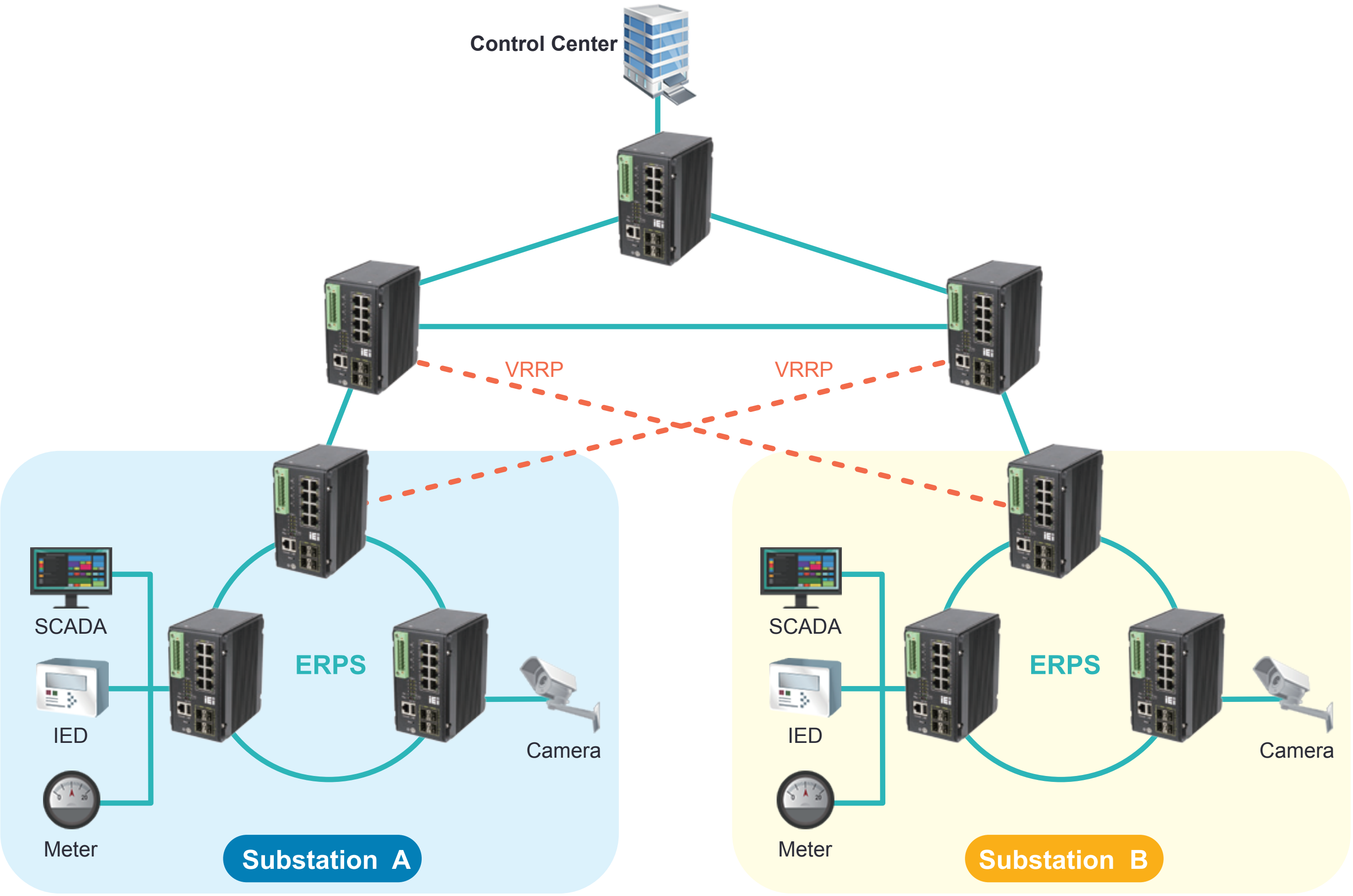
Power Substation

As Power Utilities locations are remotely distributed, DCS is usually implemented in power plant automation system for increasing working productivity as well as for smart energy production with eliminated influence on environment.

Vital role of data communication between various automation components is evident though it brings the problem of data protection from cyber-attacks and network redundancy as it is based on Ethernet and Internet.

Topology description:

IDSW-8G-4GS-L3-R10 is installed in power substation to ensure overcoming high level of electromagnetic interference on power plants. IDSW-8G-4GS-L2-R10 collect IP cameras, IEDs, meters and SCADAs data and transmit to the control center. Several IDSW-8G-4GS-L2-R10 in power plants connect with a ERPS ring for network redundancy.



Why IDSW-8G-4GS-L3-R10 is chosen for power substation:

- Dual redundant 10~60VDC power input
- Hi-pot isolation and operating temperature -40~75°C
- 8 Gigabit Ethernet copper ports can be connected with IP surveillance cameras
- 4 Gigabit SFP Fiber port are used for uplink data transmission to Control Center
- VRRP function provides gateway backup, keeping network avaliable

Railway M12 PoE L2/L3 Switch

2 Giga Link Bypass Ports

- Link Bypass function provides fail safe solution when the device power fails and bypasses the traffic to the onward switch

Management Features

- Various configuration paths, including WebGUI, CLI, Telnet, SNMP v1/v2c/v3 and RMON
- IEEE 1588v1/v2 PTP time management
- LLDP topology control
- Modbus/TCP, Ethernet/IP for factory automation
- M12 USB for easy field configuration and firmware update
- Software utility interface for LAN devices management
- NMS system for individual component monitoring

802.3 at PoE+ bypass ERPS G.8032v2 Cyber Security L3 EN50155

ITU-T G.8032 v1/v2 ERPS Ring Redundancy

- The ITU-T G.8032 standard for Ring redundancy Protocol
- Provide sub-50ms protection and recovery switching for Ethernet traffic
- Interoperate with 3rd party industrial switch and still remain fast recovery time
- Interoperate with commercial switch instead of STP/RSTP
- Efficient network interconnection and topology with ERPS Chain, multiple chains

Extreme PoE Capability

- 8-port IEEE 802.3af/at compliant PoE, up to 30W/port
- Up to 100W system power budget at 70°C operating temperature
- Complete PoE management including per-port Power Budget Control, PoE Scheduling and PoE Status

Enhanced Cyber Security for Critical Application

- L2-L7 IPv4/IPv6 Access Control List (ACL)
- DHCP Snooping, IP Source Guard, Dynamic ARP Inspection
- 802.1Q VLAN, Private VLAN, Advanced Port Security
- Multi-Level user passwords
- HTTPS/SSH/SFTP, 256-bit encryption
- 802.1X MAB for non-802.1X compliant end devices
- RADIUS/TACACS+ centralized password authentication

Rugged Design for Surveillance in Rail, Rolling Stock applications

- EN 50155/IEC 61373 compliance railway certification
- Railway 110VDC(77~137.5V) or 54V(46~57V) on-board power design
- Outstanding mechanical design with good heat dispassion and lightweight
- Rugged M12 connectors for harsh environments
- Wide operating temperature range from -40~70°C

Model	PoE	Ethernet Copper	L3 Switch	L2 Switch	ERPS v2	USB	Power Input	Vertical Standard
IRSW-8GP-2GB-(HV/WV)-(A/X)-L2-R10	8 x GE 802.3at	2 x GE (Bypass)	-	Yes	Yes	1	110V DC (HV) 24/48/110V DC (WV)	EN 50155 Compliance
IRSW-8GP-4G-2GB-(HV/WV)-(A/X)-L3-R10	8 x GE 802.3at	4 x GE 2 x GE (Bypass)	Yes	Yes	Yes	1	110V DC (HV) 24/48/110V DC (WV)	EN 50155 Compliance

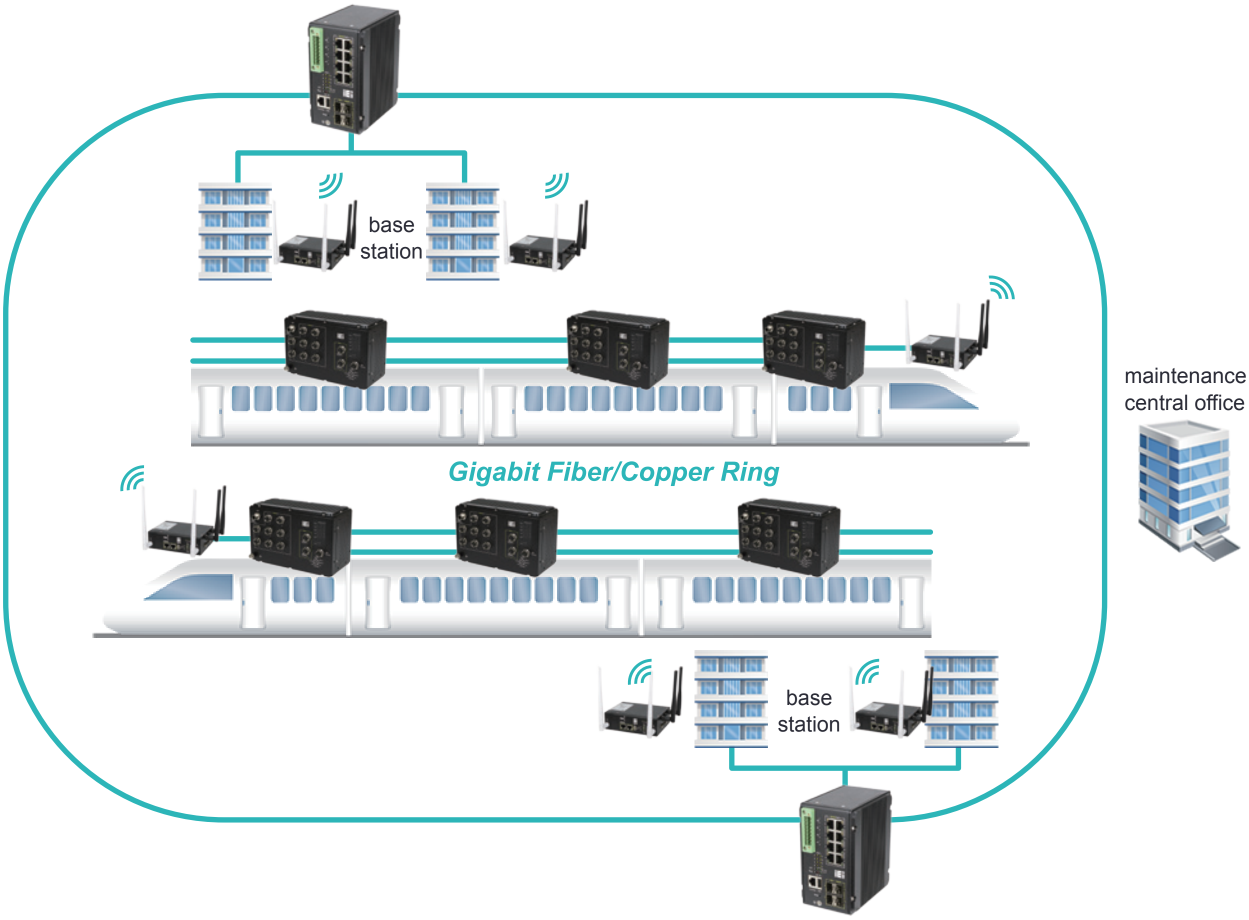
Railway

Safety for passengers and staff is provided by real-time IP video surveillance onboard and on train stations. For this purpose, reliable and secure Ethernet and wireless networks for high-speed video transmission is a must. Railway applications are composed by a number of critical requirements have to be met. All the equipment deployed on board train must comply with Railway Standard EN50155, and must sustain uniquely harsh environment, vibration, and shock

Topology description:

On-board switch IRSW-8GP-2GB-HV-A-L2-R10 collects the IP-video streaming data and sends to wireless router ISR-2G-LTE-E-R10.

IRSW-8GP-2GB-HV-A-L2-R10 installed on Base Station is equipped with 8 af/at PoE ports, transmitting 30W Power over Ethernet per port to Wireless Access Points and IP cameras, and 2 Gigabit combo ports for uplink connection with Maintenance Central Office.



Why IRSW-8GP-2GB-HV-A-L2-R10 is chosen for railway onboard installation:

- IP31 industrial hardware design with M12 rugged connectors to withstand vibration, shock, and temperature extremes
- 8-port PoE+ with 100W total power budget, including 8 Gigabit Ethernet ports, enable connected IP-cameras
- 2 Gigabit Ethernet ports with link bypass function ensure network connectivity even in case of device/power failure
- M12 USB port for field configuration and trouble shooting.

Rackmount Ethernet Switch

High Throughput Ethernet Switching

- 28-port Full GbE, by 20-port GbE RJ45 and 4-port GbE RJ45/SFP Combo, and 4 100M/1000M SFP fiber ports
- Up to 24 GbE copper RJ-45 ports
- Up to 8 100M/1000M fiber ports add more fiber links to field switches
- DDM function for high quality fiber connectivity monitoring
- 8 flexible Class of Service(CoS) queues, 512 L2 Multicast Groups for video applications
- 16K MAC address table, 9Kb Jumbo Frame

802.3 at PoE+ Cyber Security EN50121-4 IPv6

IEC 62443-4-2 Level 3/4 Cyber Security

- L2-L7 IPv4/IPv6* Access Control List (ACL)
- DHCP Snooping, IP Source Guard, Dynamic ARP Inspection
- 802.1Q VLAN, Private VLAN, Advanced Port Security
- Multi-Level user passwords
- HTTPS/SSH/SFTP, 256-bit encryption
- 802.1X MAB for non-802.1X compliant end devices
- RADIUS/TACACS+ centralized password authentication

Management Features

- Various configuration paths, including CGI WebGUI, CLI, SNMP and RMON
- IEEE 1588v2 PTP time management
- LLDP topology control
- USB for easy field configuration and firmware update

ITU-T G.8032 v2 ERPS Ring Redundancy

- ITU-T G.8032 v1/v2 ERPS Standard Ring Redundancy protocol
- Supports HW-based CFM transmission for minimum 10ms recovery time and seamless restoration time
- Provide sub-50ms protection and recovery switching for Ethernet traffic
- Interoperate with 3rd party industrial switch and still remain fast recovery time

Rugged Design for Industrial Control Room and Wayside Network Switching

- EN 50121-4 compliance for Railway Trackside, Roadside, Industrial Control Room applications
- Excellent heat dissipation design for operating in -40~75°C environments
- EN 61000-6-2/4 Heavy Industrial Environment

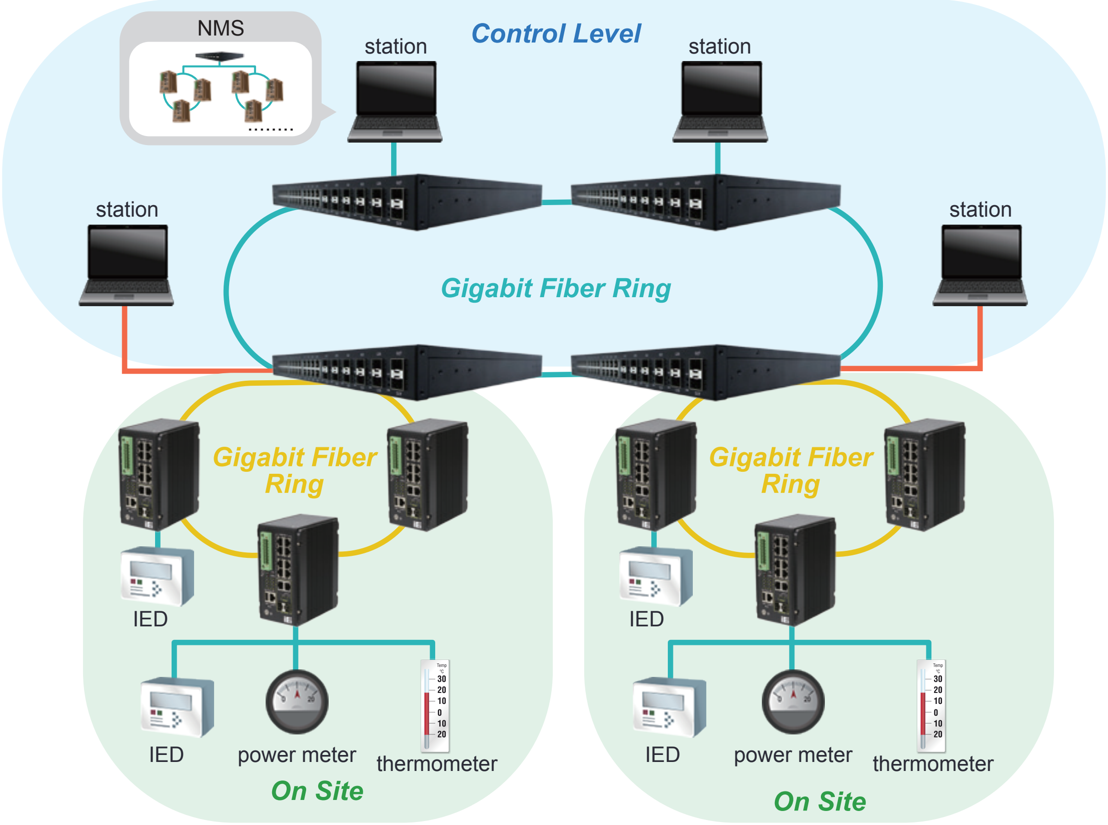
Model	Ethernet Copper	Fiber	L2 Switch	USB	Power Input	Vertical Standard
RSW-24-4GCO-L2-R10	24 x FE	4 x GE Combo	Yes	Yes	AC110/220V	-
RSW-20G-4GS-4GCO-L2-R10	20 x GE	4 x GE + 4 x GE Combo	Yes	Yes	AC110/220V or 88~300VDC	EN 50121-4 compliance
RSW-20GP-4GS-4GCO-L2-R10 (Coming soon)	20xGE 802.3at	4 x GE + 4 x GE Combo	Yes	Yes	AC110/220V or 88~300VDC	EN 50121-4 compliance

Control Center

Control centers play a vital role in large scale industrial networks. The switches in control centers collect remote data and send to backbone networks, therefore the support of resilient network is important as well as the high port density and bandwidth. To protect from network attack, comprehensive cyber security features are networkadministrators firstpriority.

Topology description:

To constitute Distributed Control Systems of power substations, rackmount 28G L2 switch RSW-20G-4GS-4GCO-L2-R10 were deployed to provide 20 Giga copper ports to connect all network devices, and 4G SFP Fiber ports and 4G RJ45/SFP Combo ports are used to form gigabit fiber ring network topology to connect between remotely located control centers, as well as to link and collect the field data from on-site switches also equipped with fiber connectors.



Why RSW-20G-4GS-4GCO-L2-R10 is an ideal choice for installation in large-scale industrial network Control Center:

- Outstanding throughput and ultra high speed connection with high port density: 28-port Full GbE ports
- ITU-T G.8032 v1/v2 ERPS Standard Ring Redundancy protocol, Supports HW-based CFM transmission for minimum 10ms recovery time and seamless restoration time
- Data security is ensured by enhanced Cyber Security features including 802.1X/RADIUS port-based access control, Private VLAN/IP Security/Port Security , HTTPs/SSH, L2-L7 Access Control List (ACL)

ISW Cloud-Manager

ISW Cloud-Manager Agent

The ISW Cloud-Manager

agent sends data (TLS/SSL encrypted) via the cellular network or Ethernet to the ISW Cloud-Manager in the cloud.

Secure Data in Cloud

The ISW Cloud-Manager Server

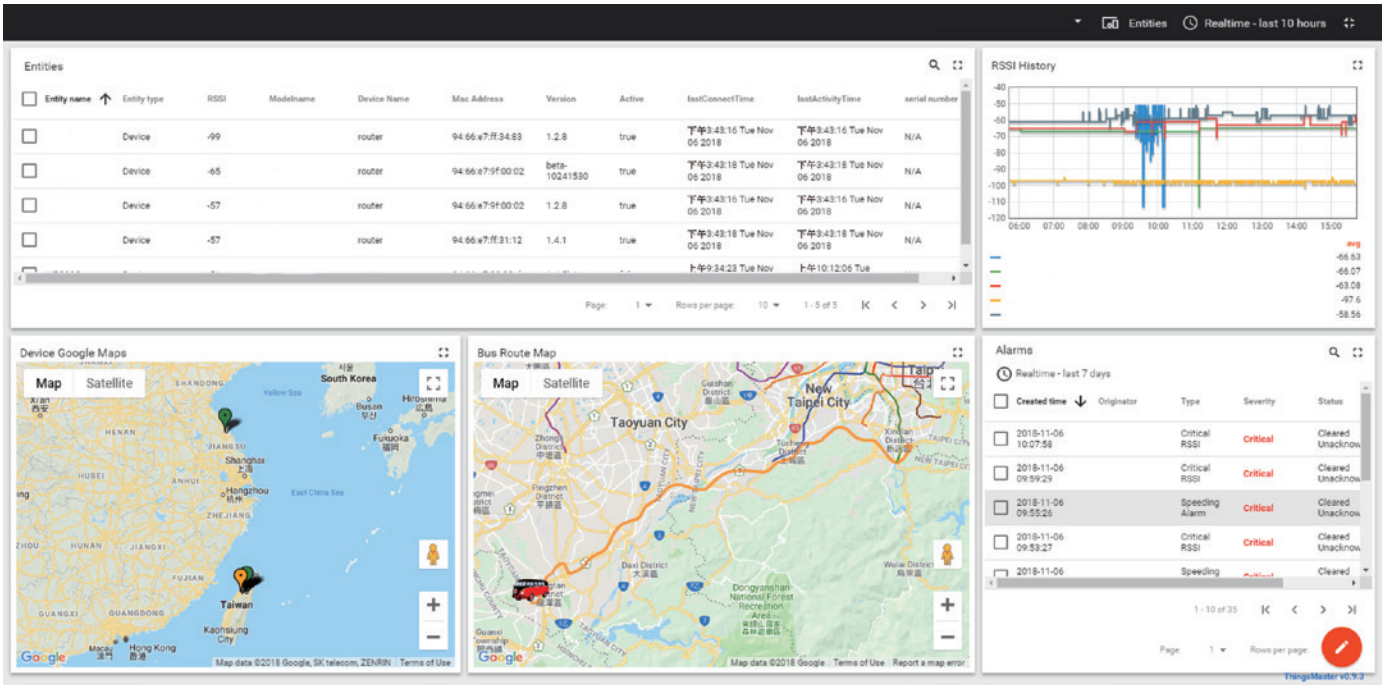
is a secured private cloud where all your data is stored and accessed. It uses the latest TLS encryption and X.509 authentication to protect the data transmission.

ISW Cloud-Manager

Interactive monitoring dashboard and map shows the status, signal strength, and location.

Set alerts on critical events to prevent downtime.

Node-RED like flow-based programming.



Entities

□ Entity name ↑	Entity type	RSSI	Modelname	Device Name	Mac Address	Version	Active	lastConnectTime	lastActivityTime	serial number
□	Device	-99		router	94:66:e7:ff:34:83	1.2.8	true	下午3:43:16 Tue Nov 06 2018	下午3:43:16 Tue Nov 06 2018	N/A
□	Device	-65		router	94:66:e7:9f:00:02	beta-10241530	true	下午3:43:18 Tue Nov 06 2018	下午3:43:18 Tue Nov 06 2018	N/A
□	Device	-57		router	94:66:e7:9f:00:02	1.2.8	true	下午3:43:16 Tue Nov 06 2018	下午3:43:16 Tue Nov 06 2018	N/A
□	Device	-57		router	94:66:e7:ff:31:12	1.4.1	true	下午3:43:18 Tue Nov 06 2018	下午3:43:18 Tue Nov 06 2018	N/A

Page: 1 Rows per page: 10 1 - 5 of 5

Alarms

Realtime - last 7 days

□ Created time ↓	Originator	Type	Severity	Status
□ 2018-11-06 10:07:58		Critical RSSI	Critical	Cleared Unacknow
□ 2018-11-06 09:59:29		Critical RSSI	Critical	Cleared Unacknow
□ 2018-11-06 09:55:26		Speeding Alarm	Critical	Cleared Unacknow
□ 2018-11-06 09:53:27		Critical RSSI	Critical	Cleared Unacknow

1 - 10 of 35

Page: 1 Rows per page:

ISW Cloud-Manager: Device Management

Interactive monitoring dashboard and map shows the status, signal strength, and location of all ISR series deployed

MAP shows devices online/offline/Warning status in **Green**/**Red**/**Orange** color, respectively

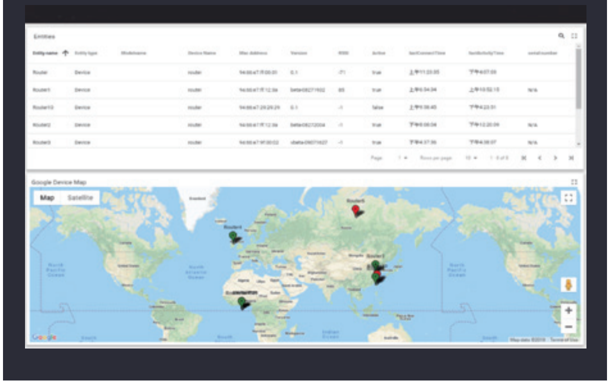
Supports over-the-air batch device configuration and firmware* update

Set alerts on critical events to prevent downtime (i.e. signal strength is too low or temperature is too high)

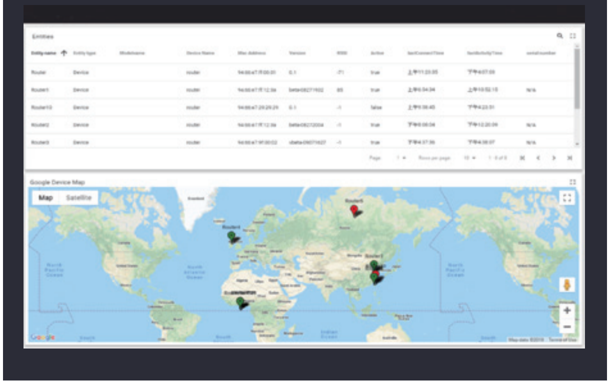
Node-RED like flow-based programming

Support the latest TLS encryption and X.509 authentication

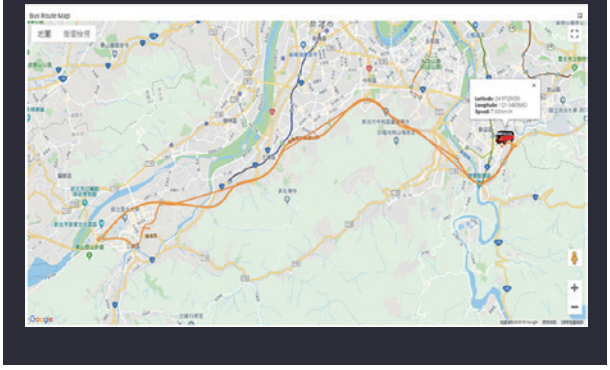
Google MAP Integration



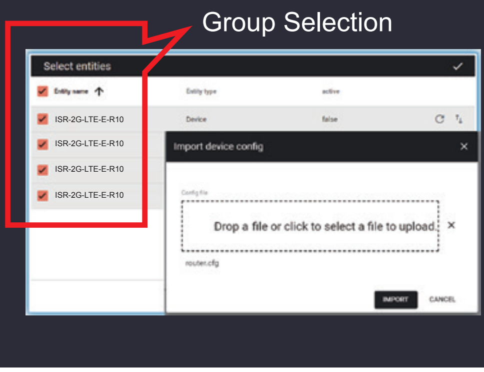
Monitor Device Information



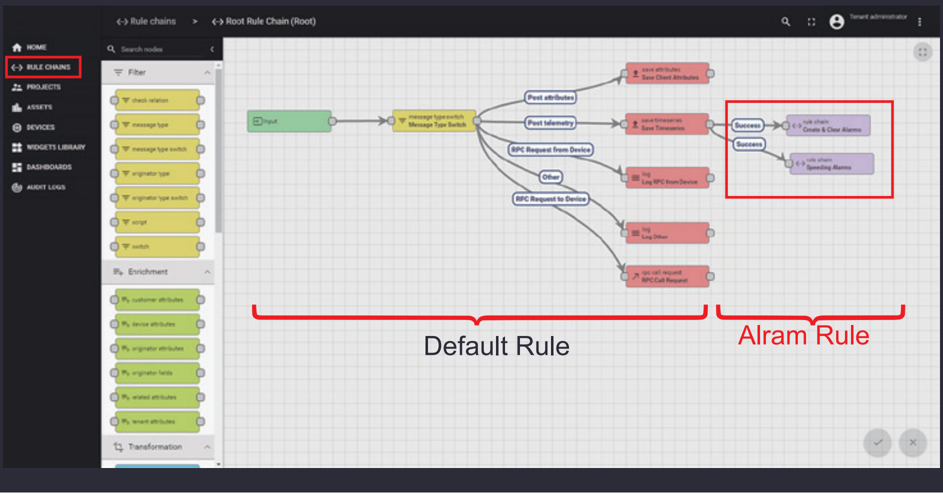
Display device location, route and speed on the Map



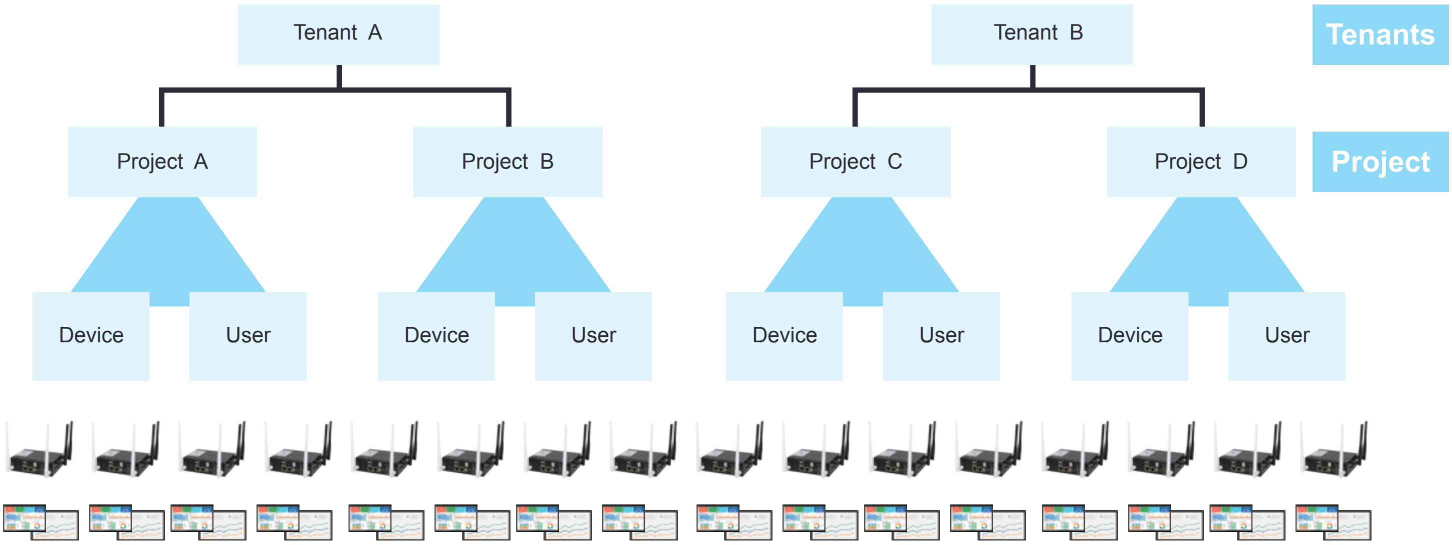
Group Configuration and Reboot



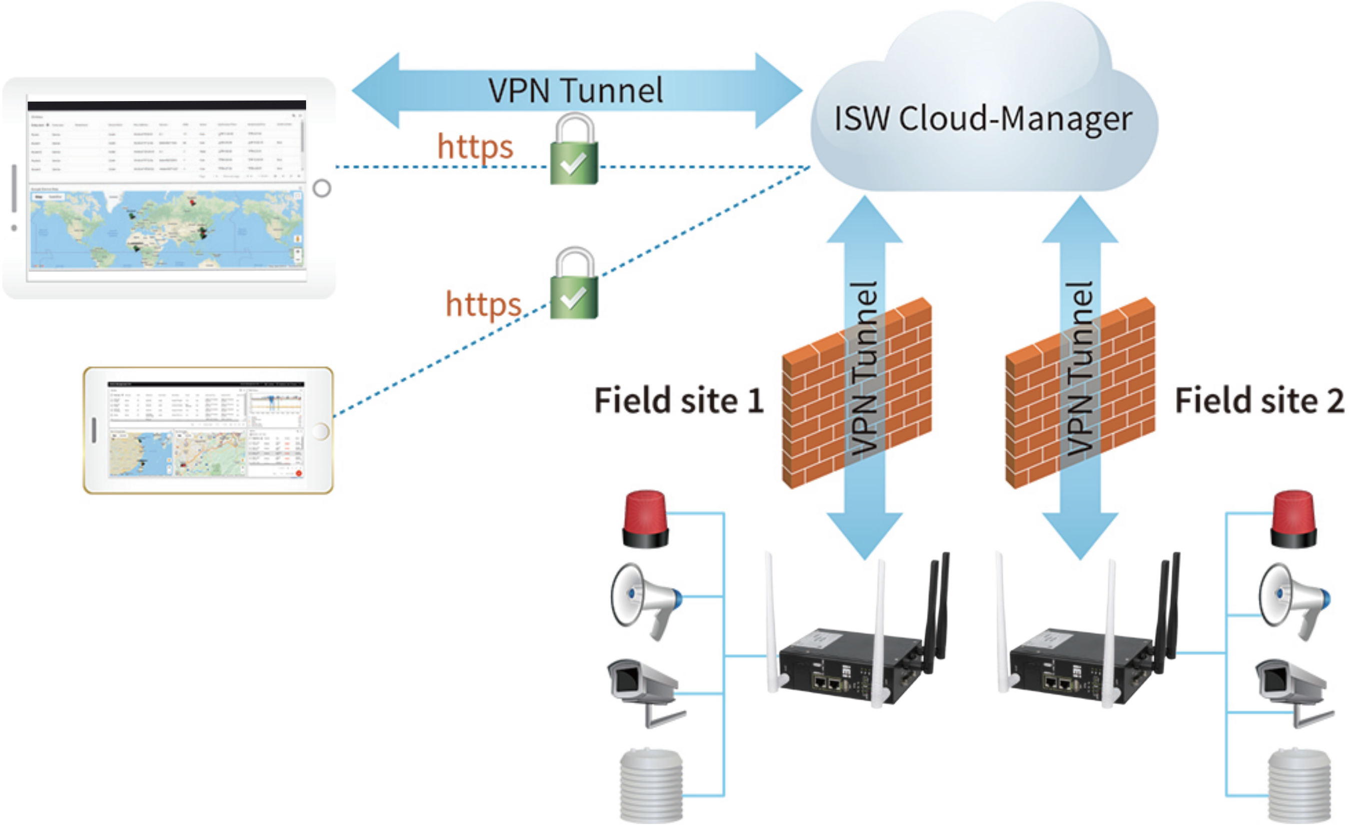
Rule Engine: Node-RED like flow-based programming



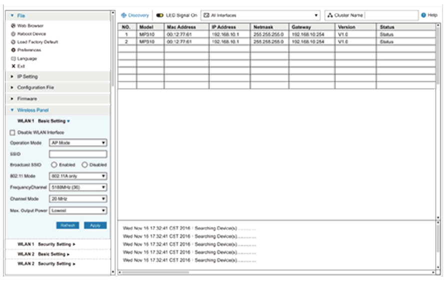
Multi-Tenant, Project based IoT deployment



Cloud Security (N to N VPN) Remote Multi-Site Management



ISW Manager Network Management Utility



□ Disable WLAN Interface
Operation Mode: AP Mode
SSID:
Broadcast SSID: ○ Enabled ○ Disabled
802.11 Mode: 802.11A only
FrequencyChannel: 5180MHz (36)
Channel Mode: 20 MHz
Max. Output Power: Lowest

NO.	Model	Mac Address	IP Address	Netmask	Gateway	Version	Status
1	MP310	00:12:77:61	192.168.10.1	255.255.255.0	192.168.10.254	V1.0	Status
2	MP310	00:12:77:61	192.168.10.1	255.255.255.0	192.168.10.254	V1.0	Status

```
Wed Nov 16 17:32:41 CST 2016 : Searching Device(s)..........
Wed Nov 16 17:32:41 CST 2016 : Searching Device(s)..........
Wed Nov 16 17:32:41 CST 2016 : Searching Device(s)..........
Wed Nov 16 17:32:41 CST 2016 : Searching Device(s)..........
Wed Nov 16 17:32:41 CST 2016 : Searching Device(s)..........
```

ISW manager is the network management utility for IEI devices. It can automatically discover network devices for batch configuration and upgrade, thus helps system integrators install the system more easily.

Manage Large and Resilient Wired/Wireless Networks for up to 2000 nodes

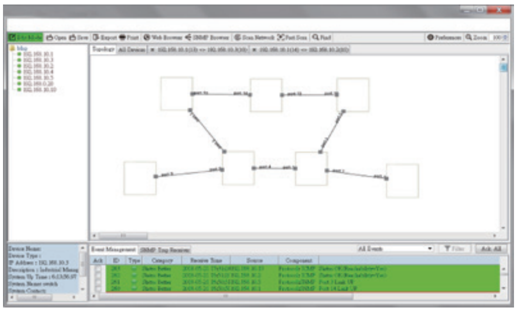
Network Discovery and Visualizationg

- Automatic discovery and intuitive visualization of network devices, wireless devices, physical link and network topology
- Real-time status of device availability and traffic performance for physical links
- Server-client operation to ensure network system reliability especially in large scale networks
- High scalability for up to 2000 network nodes by license upgrade
- Free download and permanently valid for 20 nodes trial

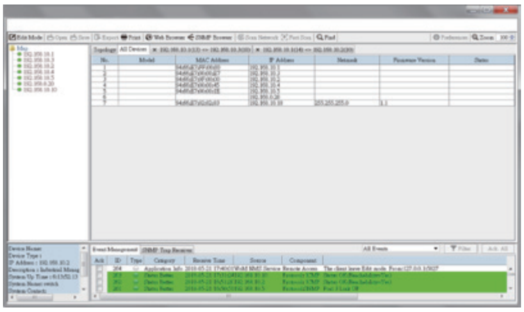
Configuration & ISW Management

- Centrally manage configurations and firmware versions
- Group IP Address assignment
- Group ERPS ring configuration & assignment *(by request)
- MIB compiler and MIB browser for private MIBs and MIBs of 3rd party device
- Fault Alert and event logs including source IP filter, network error, login record and warning
- SNMP Trap receiver for all or specific IP addresses
- Multi-language support including English, Chinese & Russian

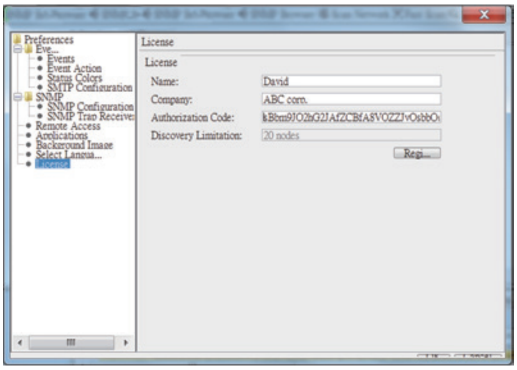
Automatic Discover and Intuitive Visualization of Network Devices and Topology



IP Device Lists, Device Information, Fault Alert and Event Logs



High Scalability for up to 2000 network nodes by license upgrade

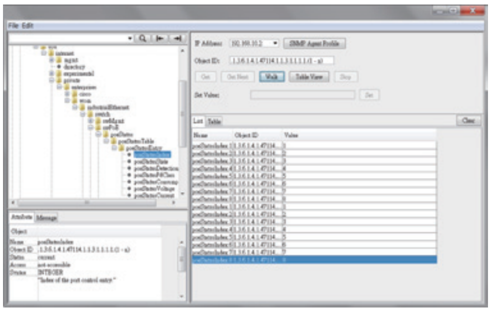


License

License

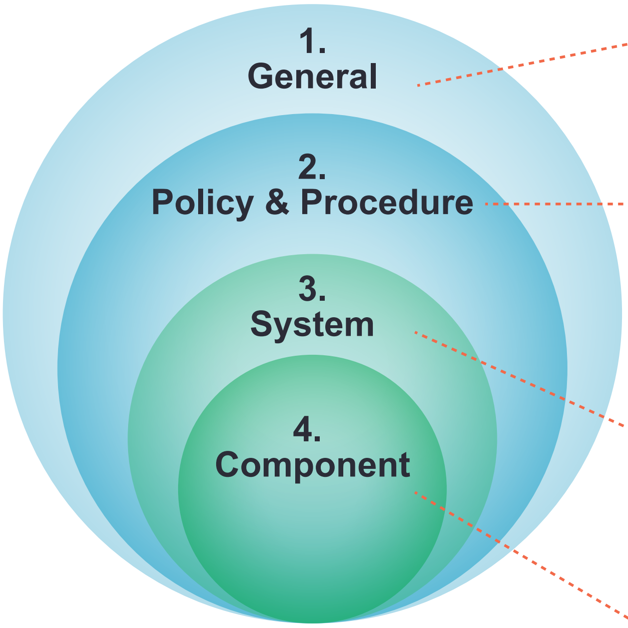
Name: David
Company: ABC corp.
Authorization Code: kBbm9JO2hG2JAfZCBfA8VOZZJvOsbbO
Discovery Limitation: 20 nodes

MIB Browser and Compiler for 3rd Party Device Management



IEC 62443 Cyber Security

Industrial Automation & Control System



The Scope of IEC 62443 standard

1-1：Terminology and concepts
1-2：Master glossary
1-3：System security compliance metrics
1-4：IACS security lifecycle and use-case

2-1：Requirements for an IACS security management system
2-2：Implementation guidance
2-3：Patch management
2-4：Installation & maintenance

✓ Apply to Asset Owner

3-1：Security technologies for IACS
3-2：Security levels for zones conduits
3-3：System security requirements and levels

✓ Apply to System Integrator

4-1：Product development requirements
4-2：Technical security requirement for IACS components

✓ Apply to Component Supplier

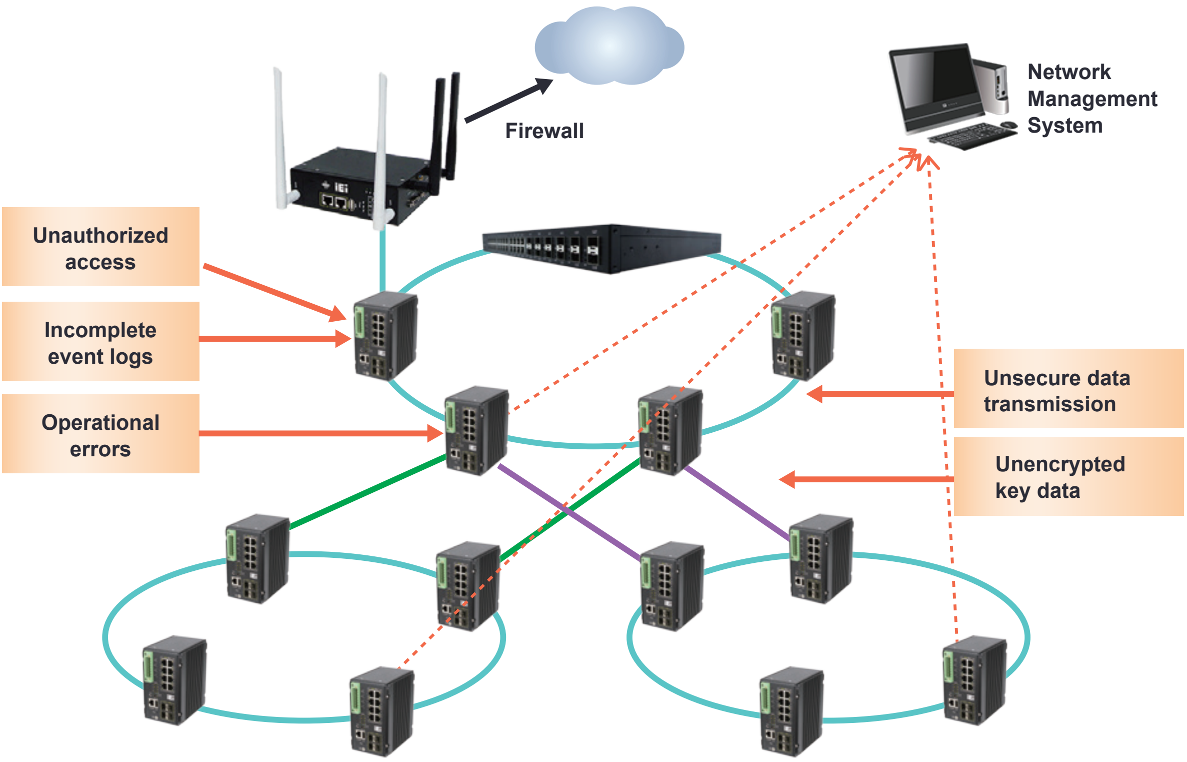
As the Industrial IoT (IIoT) demand continues growing, the closed industrial networks is facing challenges to be accessible over the public Internet. While it enhances operational efficiency, however, it brings more cyber security threats. The governments and enterprises are more concerned about the potential cyber security damages.

The IEC 62443 Standard includes up-to-date security guidelines and a list of best practices for different parts of a network. It also includes information for those who perform different responsibilities on the network in order to protect against known security leaks and unknown attacks. The ultimate goal of the standard is to help improve the safety of networks and enhance industrial automation and control settings security.

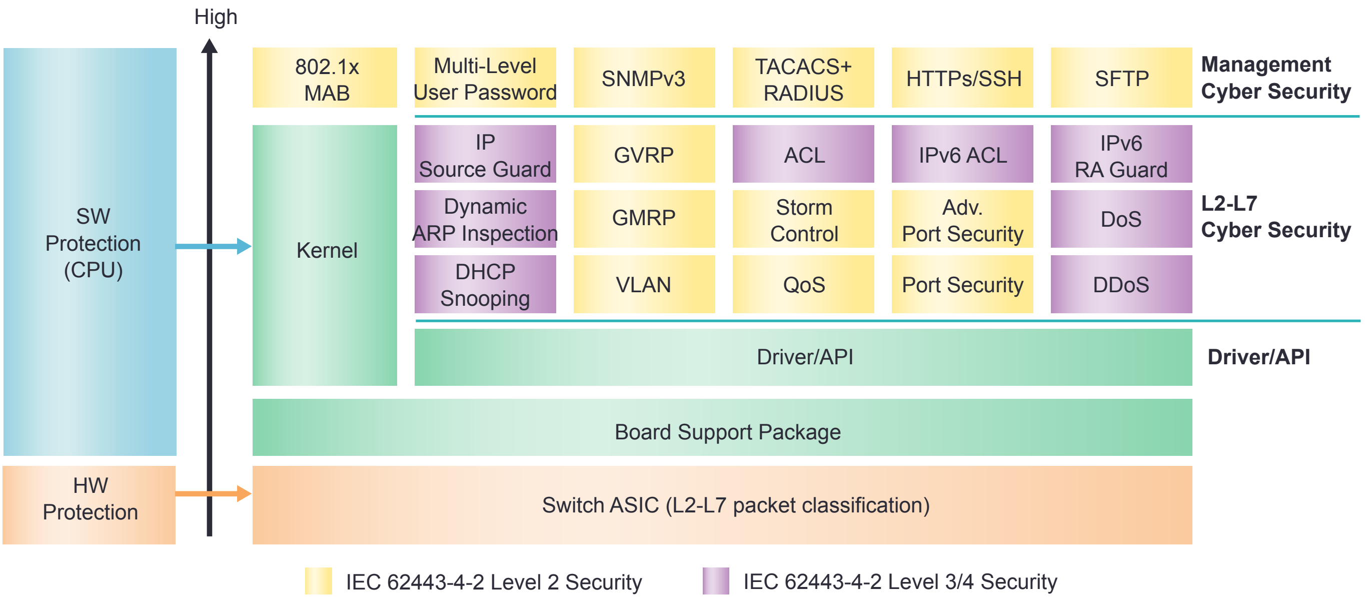
At present, many system integrators, such as Siemens and ABB, require component suppliers to comply with the IEC 62443-4-2 subsection that specifically pertains to the security of end devices. This subsection defines four security threat levels.

- Level 1 is to protect against accidental and unauthenticated access
- Level 2 is the baseline requirement of the automation industry. It relates to cyber threats posed by hackers, which is the most common attack experienced by system integrators
- Levels 3 and 4 are against intentional access by hackers who utilize specific skills and tools

Cyber Security Solutions



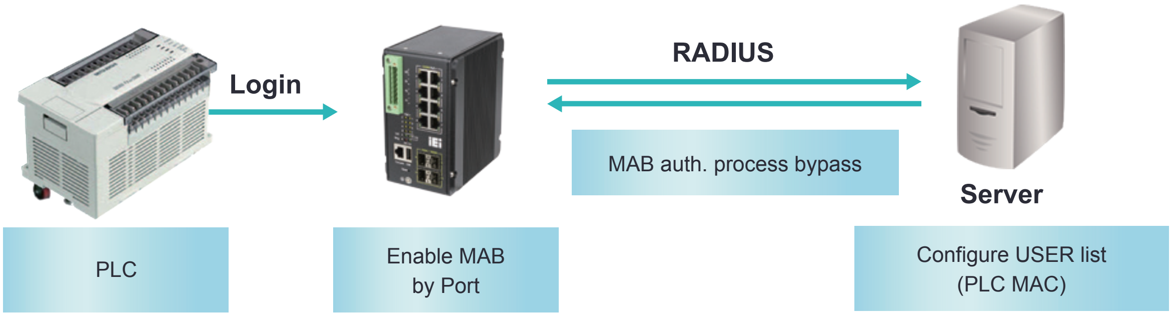
From the viewpoint of cyber security experts, the major cyber security threats that can affect internal networks include unauthorized access, unsecured data transmission, unencrypted key data, incomplete event logs, and operational errors.



provides SW & HW(ASIC) integrated protection mechanism, which applies the latest Application-Specific Integrated Circuit (ASIC) secure technology (L2-L7 packet classification), that covers from level 1 to level 4 of IEC 62443-4-2 range.

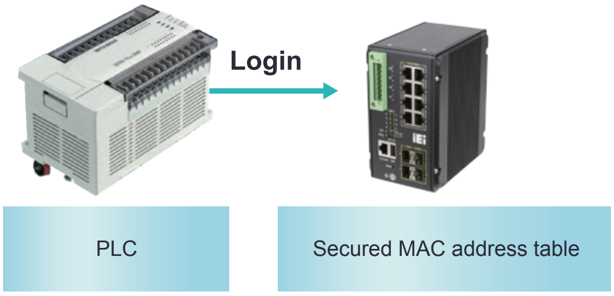
Level 2 Security

IEEE 802.1X MAB (MAC Authentication Bypass)



MAB enables port-based access control by bypassing the MAC address authentication process to RADIUS Server. Prior to MAB, the endpoint's (ex. PLC) identity is unknown and all traffic is blocked. The switch examines a single packet to learn and authenticate the source MAC address. After MAB succeeds, the endpoint's identity is known and all traffic from that endpoint is allowed. The switch performs source MAC address filtering to help ensure that only the MAB-authenticated endpoint is allowed to send traffic.

Advanced Port Based Security



In addition to MAB, the authentication can also be done by the pre-configured static or auto-learn MAC address table in the switch.

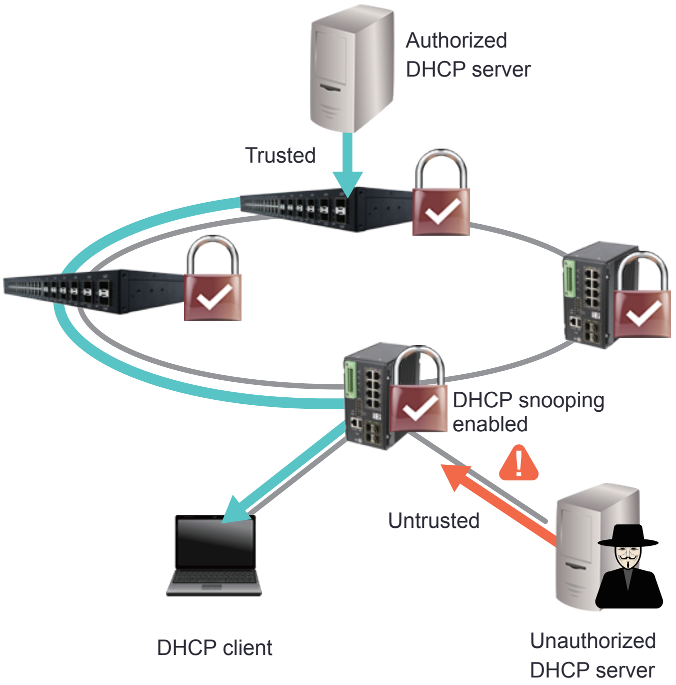
- MAC address Auto Learning enables the switch to be programmed to learn (and to authorize) a pre-configured number of the first source MAC addresses encountered on a secure port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses are automatically inserted into the Static MAC Address Table and remain there until explicitly removed by the user.
- The port security is further enhanced by Sticky MAC setting. If Sticky MAC address is activated, the MACs/evices authorized on the port 'sticks' to the port and the switch will not allow them to move to a different port.
- Port Shutdown Time allows users to specify for the time period to auto-shut down the port, if a security violation event occurs.

Level 3/4 Security

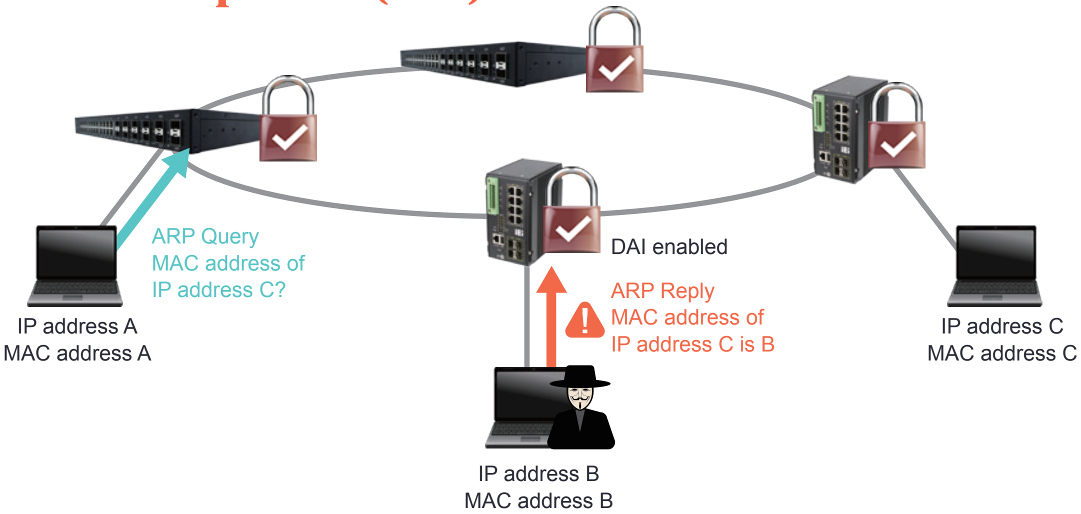
DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. It performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.
- DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.



Dynamic ARP Inspection (DAI)



DAI validates the ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

DAI ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

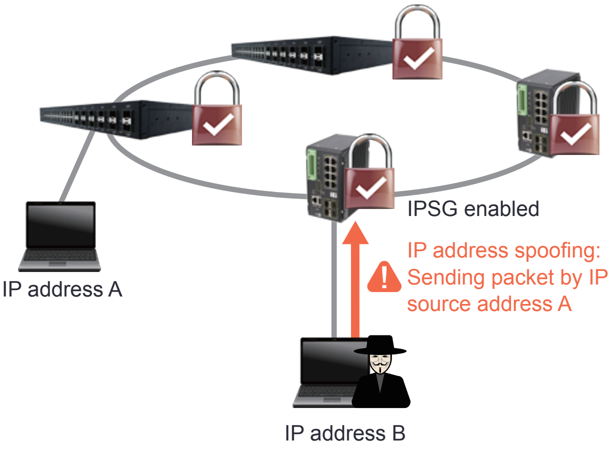
- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

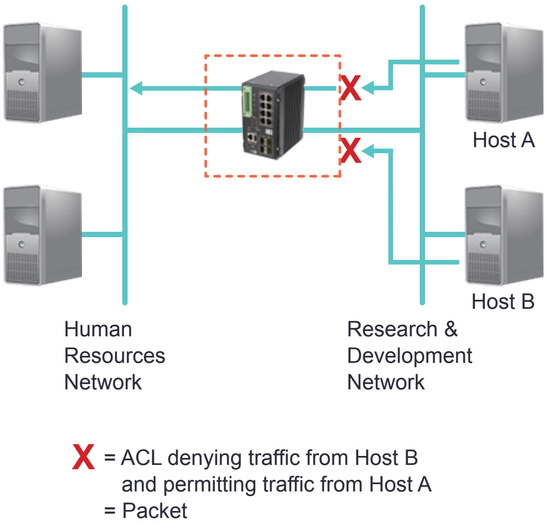
DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

IP Source Guard (IPSG)

IP source guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.




Host A
Host B
Human Resources Network
Research & Development Network
X = ACL denying traffic from Host B and permitting traffic from Host A
= Packet

IPv4 / IPv6 Access Control List (ACL)

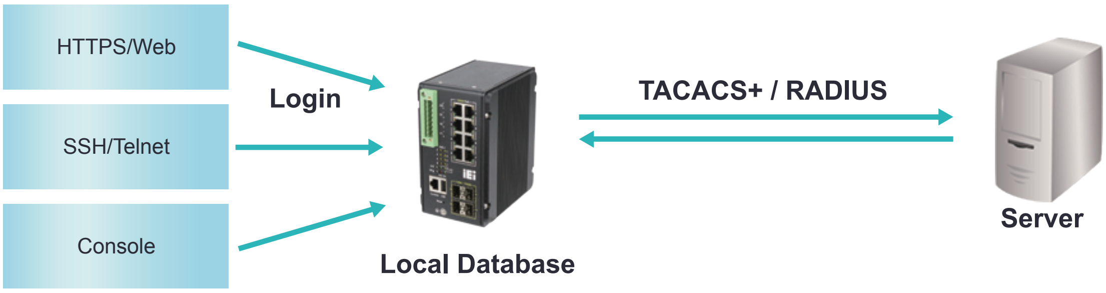
Packet filtering limits network traffic and restricts network use by certain users or devices. ACLs filter traffic as it passes through a switch and permits or denies packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists.

Supports L2-L7 ACLs, parsing up to 128 bytes/packet and L2-L7 packet classification and filtering IPv4/IPv6 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).

Multi-Level User Passwords

Different centralized authentication server is supported such as RADIUS and TACACS+. Using a central authentication server simplifies account administration, in particular when you have more than one switch in the network.

Authentication Chain is also supported. An authentication chain is an ordered list of authentication methods to handle more advanced authentication scenarios. For example, you can create an authentication chain which first contacts a RADIUS server, and then looks in a local database if the RADIUS server does not respond.



2019

*Specifications are subject to change without prior notice.

Headquarters
威強電工業電腦 IEI Integration Corp.
No. 29, Zhongxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL : +886-2-86916798 / +886-2-26902098 FAX : +886-2-66160028
sales@ieiworld.com www.ieiworld.com

America
IEI Technology USA Corp.
138 University Parkway, Pomona, CA 91768
TEL : +1-909-595-2819 FAX : +1-909-595-2816
sales@usa.ieiworld.com usa.ieiworld.com

China
威强电工业电脑 IEI Integration (Shanghai) Corp.
上海市闵行莘庄工业区申富路515号
515, Shen Fu Rd., Xin Zhuang Industrial Develop Zone, Shanghai, 201108, China
TEL:+86-21-3116-7799 FAX:+86-21-3462-7797
sales@ieiworld.com.cn www.ieiworld.com.cn

2019.03