cisco
The bridge to possible

Cisco Industrial IoT Portfolio

www.cisco.com/go/iot

The bridge to possible

Contents

Bring Cisco scale and security to industrial IoT

Stop worrying about challenges and start imagining possibilities with Cisco IoT

Deploying IoT at scale isn't easy. It requires configuring and managing countless assets and devices and dealing with complex operational and industry requirements. This increase in connected "things" can also create visibility gaps that increase security risks.

Cisco provides the most secure, dependable IoT portfolio on the market | Cisco IoT is an end-to-end IoT architecture. Built on our industry-leading networking and security capabilities, it provides

Rock-solid infrastructure

Extend the Cisco network you know and trust to scale your IoT deployment using reliable infrastructure, automation, and familiar management tools

Unparalleled visibility and control

Protect your business with Cisco's industry-leading security portfolio which gives you complete visibility and control

Trusted expertise

Partner with a trusted leader who offers continuous innovation, market-leading products, an extensive developer program, and resources like deployment blueprints to make you successful

IoT enables transformative use cases
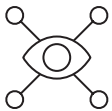
Remote monitoring

Asset tracking

Worker safety
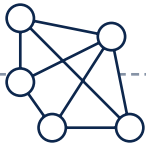
Operational agility

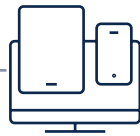Fleet management

Predictive maintenance

Cisco offers an unparalleled end-to-end IoT architecture

Interconnect assets, applications and data to uncover transformative business insights

Network connectivity

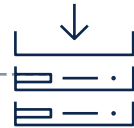Extend the network you know and trust to operational environments

Device management

Manage industrial assets and devices at scale with automated solutions

Data control and exchange

Efficiently move the right data to the right place at the right time

Edge computing

Push data processes to the edge to enable fast decision-making in the field

Security

Protect your business from end to end with Cisco's industry-leading security portfolio

Our 67,000 customers are already seeing tremendous results

> " Within a month, we increased our manufacturing floor productivity by over 10 percent.
>
> – Yair Avigdor, **COO, Lordan**

> " We gained an additional 10,000 hours of availability system-wide.
>
> – Eric Rupp, **Principal Network Engineer, Great River Energy**

Visit **www.cisco.com/go/iot** to learn more

Cisco Industrial Ethernet (IE) switching portfolio

The Cisco® Industrial Ethernet (IE) switching portfolio includes ruggedized, secure, easy-to-use switches built for extending enterprise networks to outdoor and harsh industrial environments. They provide secure connectivity across challenging operating conditions and industries such as manufacturing, utilities, transportation, oil and gas, mining, roadways, and smart cities. These Cisco switches offer best-in-class Cisco IOS® or Cisco IOS XE Software with advanced Layer 2 and Layer 3 features, along with industrial protocol support, such as PROFINET and EtherNet/IP to accelerate industries' digital transformation.

Visibility and security

Cisco IE switches are available with robust visibility and security features. Select IE switch models incorporate Cisco Cyber Vision, which provides granular visibility into connected assets and traffic flows to monitor your security posture and also helps you define rules for network segmentation. IE switches are compatible with Cisco Software-Defined Access (SD-Access), which can be used for easy segmentation, threat isolation, and building a zero-trust industrial network. Select IE switch models can also run Cisco Secure Equipment Access to enable Zero-Trust Network Access (ZTNA) and secure remote access to industrial assets.

Cisco IE switches are developed according to the **Cisco Secure Development Lifecycle** (SDL), which enforces a secure-by-design philosophy from product planning through end of life and is certified against ISA/IEC 62443-4-1. They also contain several embedded security features that provide additional layers of protection.

Easy network management

Scaling your industrial network is easy with intelligent management. You can easily manage your IoT network with the same tools that manage your IT network, such as **Cisco Catalyst™ Center**, which allows zero-touch deployments, automates configuration changes, monitors performance, and identifies and helps correct faults, reducing time and cost of deployment. You may also use other management options such as the included web management tool.

Multiple form factors

Cisco offers its IE switch portfolio in different form factors to suit a range of industries and use cases.

- **DIN rail switches:** These switches can be mounted on standard DIN rails, which are commonly used in industrial control panels. The switches are compact and take up less space in these panels, which is useful in tight spaces where there is limited room for equipment. Cisco IE DIN rail switches are available in both fixed and modular forms that can be expanded with additional ports to keep up with demand. They also offer a choice of power supplies, allowing you to match the right power capacity for your PoE needs.

- **Rack-mount switches:** These switches are designed to be mounted in a standard 19-inch equipment rack, which allows for flexibility in deployment – in industrial settings, server rooms, or even in data centers. Some of the Cisco rack-mount industrial switches are conformally coated for additional resistance against corrosion.

- **IP67-rated switches:** These switches are wall mounted and can withstand the harshest conditions, including dust, water, and extreme temperatures, as well as severe shocks and vibrations. Because they are designed to withstand harsh conditions, IP67-rated industrial switches are more reliable and less likely to fail and cause downtime. The switches are equipped with M12 connectors rather than standard RJ-45 ones. Some Cisco IP67-rated switch models also provide PoE.

- **Embedded switches:** These switches are ultra-compact and built for secure, high-bandwidth, mission-critical mobile networks. They enable integrators to build custom solutions for specialized use cases.

Built-in essential OT services

Select models of the IE switch portfolio with the open Cisco IOx-based edge-compute capabilities run a number of essential services. This differentiating feature of the switches eliminates the need for span networks and additional servers to run these applications. Note that Cisco IoT Operations Dashboard may be required to run some of these services.

These services include:

- Cyber Vision sensor to gain granular visibility into connected assets, their vulnerabilities and your security posture, increase operational efficiencies, and help define segmentation policies.

- Secure Equipment Access, which enables Zero-Trust Network Access (ZTNA) features for secure remote access to industrial assets using least privilege policies and strong security controls.

- Edge Intelligence to collect process data in real-time to improve governance and make better business decisions.

Modular DIN rail switches

Select models of the Cisco IE switch portfolio are available in a modular form factor. These switches include the base system to which expansion modules may be attached as required. This modularity gives you the freedom to add, remove, or change copper or fiber ports in the future in sync with your evolving needs without having to replace the entire switch.

Cisco Catalyst IE3400 Rugged Series

- Advanced modular DIN rail switch expandable up to 26 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 480W)
- Copper, fiber, and PoE+ expansion modules
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access policy extended node
- Advanced industrial protocols and additional security features
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
- Cisco Edge Intelligence for real-time data extraction

ılıılı
CISCO

The bridge to possible

Cisco Catalyst IE3300 Rugged Series

- Modular DIN rail switch expandable up to 26 ports
- All Gigabit Ethernet platform with available 10G uplink option, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 360W)
- Copper, fiber, and PoE+ expansion modules
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access extended node
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
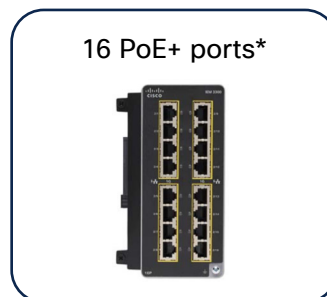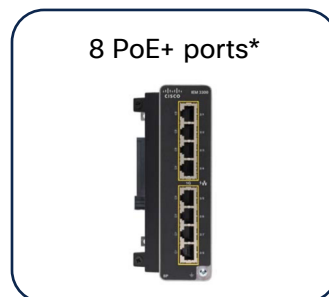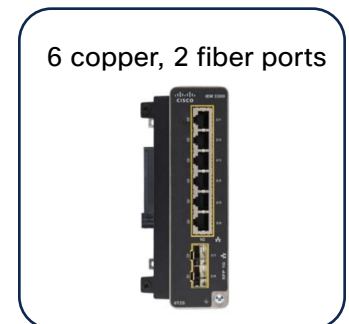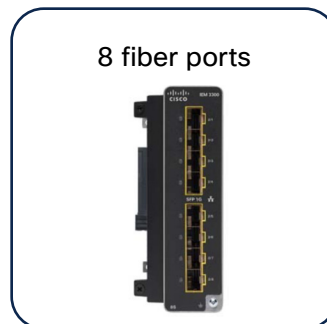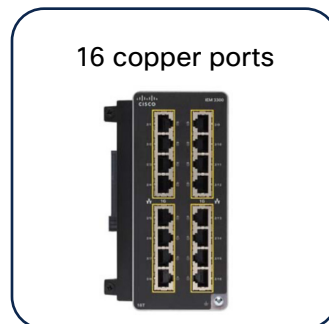- Cisco Edge Intelligence for real-time data extraction

Expansion modules for the Catalyst IE3400 and IE3300 Rugged Series

Expansion modules add versatility and flexibility to your industrial network by providing additional ports, functionalities, and features that the base switch units might not have. These modules let you customize the switch to your specific needs, allow you to accommodate future additions and changes, provide built-in scalability, and promote long-term viability and sustainability.

Expansion modules for the Catalyst IE3300 and IE3400 allow you to add fiber, copper, or PoE ports. These modules are listed below.

8 copper ports	16 copper ports	8 fiber ports	6 copper, 2 fiber ports

14 copper, 2 fiber ports	8 PoE+ ports*	16 PoE+ ports*	4 1G/2.5G Hi-PoE ports*

* Compatible with select models of the Catalyst IE3300 and IE3400 Rugged Series. Please consult the respective datasheets.

Fixed DIN rail switches

Cisco Catalyst IE3200 Rugged Series

- Fixed DIN rail switch, 10 ports
- All Gigabit Ethernet platform, Layer 2
- 8 ports of PoE/PoE+ (power budget up to 240W)
- Cisco IOS XE operating software
- Cisco Catalyst Center for management

Cisco Catalyst IE3100 Rugged Series

- Ultra-compact form-factor fixed DIN rail switch with 6, 10, 12, or 20 ports
- 2 or 4 dual-media or fiber uplink ports
- All Gigabit Ethernet platform, Layer 2
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- Cisco Secure Equipment Access for remote asset access

Cisco IE4000 Series Switches

- Fixed DIN rail switch, up to 20 ports
- 4x 1G combo uplinks
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 8 ports of PoE/PoE+ (power budget up to 200W)
- Advanced industrial protocols and additional security features
- Cisco Catalyst Center for management
- SD-Access extended node

Cisco IE2000 Series Switches

- Fixed DIN rail switch, up to 20 ports
- Up to 18 Fast Ethernet (FE) ports, 2x 1G combo uplinks (on select models)
- Layer 2 or Layer 3 (limited features)
- Up to 4 ports of PoE/PoE+ (power budget up to 120W)
- Conformal coating (on select model)
- Optimized for use in utilities (select models)
- Cisco Catalyst Center for management

Cisco IE2000U Series Switches

- Optimized for use in utilities
- Fixed DIN rail switch, up to 20 ports
- Up to 18 FE ports, 2x 1G uplinks
- Layer 2 or Layer 3
- Up to 4 ports of PoE/PoE+ (power budget up to 120W)
- Conformal coating (on select model)
- Cisco Catalyst Center for management

Cisco IE1000 Series Switches

- Fixed DIN rail switch, up to 10 ports
- Up to 8 Fast Ethernet (FE) ports, 2x 1G combo uplinks (on select models)
- Lightly managed Layer 2
- Up to 8 ports of PoE/PoE+ (power budget up to 180W)
- Security: Port security, TACACS, 802.1X
- Plug and Play (PnP) for easy deployment

Rack-mount switches

Cisco Catalyst IE9300 Rugged Series Switches

- 19-inch rack-mount switch
- Based on the Cisco UADP ASIC
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- 26 fiber ports, 2 combo Gigabit Ethernet ports (on select models)
- 24 copper ports with PoE/PoE+ (on select models and with power budget up to 720W)
- 4x 10G fiber uplinks (on select models)
- Multigigabit copper ports with 90W/port 4-pair PoE (on select model and with power budget up to 720W)
- GNSS/GPS antenna interface and conformal coating (on select model)
- Cisco IOS XE operating software
- Vertical stacking up to 8 members
- Advanced industrial and redundancy protocols
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Catalyst Center for management
- SD-Access fabric edge node
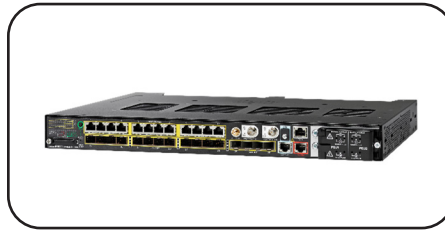
Cisco IE5000 Series Switches

- 19-inch rack-mount switch,28 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- 4x 10G fiber uplinks (on select models)
- Up to 12 ports of PoE/PoE+ (power budget 360W)
- Horizontal stacking up to4 members
- GNSS/GPS antenna interface
- Advanced industrial protocols and additional security features
- Conformal coating (on select model)
- Cisco Catalyst Center for management
- SD-Access extended node

Cisco IE4010 Series Switches

- 19-inch rack-mount switch, 28 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 385W)
- Advanced industrial protocols and additional security features
- Cisco Catalyst Center for management
- SD-Access extended node

Heavy-duty IP67 switches

Cisco Catalyst IE3400 Heavy Duty Series

- Wall-mount IP66/IP67 switch with M12 interfaces
- Up to 24 all Gigabit Ethernet or all Fast Ethernet ports, Layer 2 or Layer 3
- Cisco Catalyst Center for management
- SD-Access policy extended node
- Advanced industrial protocols and additional security features
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
- Cisco Edge Intelligence for real-time data extraction

Cisco IE2000 IP67 Series

- Wall-mount IP66/IP67 switch, up to 20 ports with M12 interfaces
- Layer 2 or Layer 3 (limited features)
- Up to 8 ports of PoE/PoE+
- Cisco Catalyst Center for management

Next steps

To learn more about the Cisco Catalyst Industrial Ethernet switching portfolio, visit **www.cisco.com/go/ie** and use the **Cisco Switch Selector** to find the best switch for your particular use case.

Cisco Industrial Router (IR) portfolio
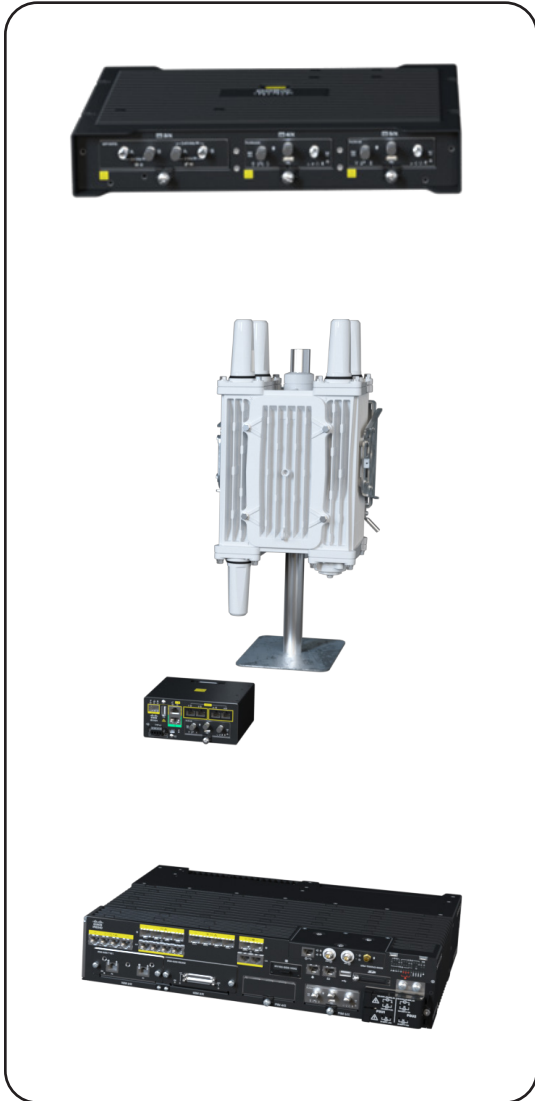
The Cisco Catalyst industrial routers are a range of ruggedized modular platforms on which you can build a highly secure, reliable, and scalable communications infrastructure.

All Cisco industrial routers share a core set of common characteristics. They are certified to meet harsh environmental standards – and have modular designs that can help extend product life and lower costs. This flexible design enables WAN redundancy and is ready to handle public and private 4G or 5G – including FirstNet and Citizens Broadband Radio Service (CBRS), as well as enhanced data throughputs and differentiated services. They are powered by Cisco IOS XE, and offer a choice of management options, allowing you to extend your network from the enterprise to the industrial edge using common security policies, tools, and management policies.

Modular design

Enjoy many pluggable module options, such as public or private 4G and 5G, Wi-Fi 6, LoRaWAN, and additional storage. The platform can adapt as your connectivity needs grow or technology evolves.

Ruggedized

Designed for industrial deployments, including harsh environments with extreme temperatures.

Scale with choice of management

Scale and simplify operations. Equip IT and operations teams with powerful management tools such as Field Network Director, Cisco Catalyst Center, and Cisco Catalyst SD-WAN Manager.

Enjoy routing and full-stack multilayer security, all in one

Easily build and manage a highly scalable and secure SD-WAN with advanced firewalling, URL filtering, intrusion prevention, malware protection, and DNS security.

Visibility into connected assets

Assess your OT security posture and shrink your attack surface. Cisco Cyber Vision is built in to provide detailed visibility into connected assets, their vulnerabilities, and activities.

Secure access to remote assets

Take control over remote access to OT assets. Cisco Secure Equipment Access turns your Cisco industrial routers into Zero-Trust Network Access (ZTNA) gateways to simplify and secure remote access at scale.

Take action right at the edge

Use the platform's built-in edge compute and Cisco IOx support to build and run your own applications at the edge.

Cisco Catalyst IR1100 Rugged Series Routers – FirstNet Ready

- Modular and expandable hardware design to extend product life
- Choice of WAN interfaces like Ethernet, dual cellular for WAN redundancy, and DSL
- FirstNet ready
- Ruggedized and compact with low power consumption
- SD-WAN with enterprise-grade security
- Cisco IOS XE operating software
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset ccess
- Cisco Edge Intelligence for real-time data extraction
- IEC 61850-3 and IEEE 1613 certified for deployment in utility substations
- 100 GB of additional storage for edge applications

Cisco Catalyst IR1800 Rugged Series Routers – FirstNet Ready

- Highly secure, high-performance, modular routers with 5G and Wi-Fi 6
- Automotive certification and CAN-bus support
- SD-WAN with comprehensive threat protection and security features
- Cisco IOS XE operating software
- Edge compute supporting IOx applications
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
- Cisco Edge Intelligence for real-time data extraction
- FirstNet ready
- 2 cellular slots, 1 Wi-Fi slot
- 8 GB memory
- CAN bus, PoE/PoE+, ADR GNSS slot, SSD slot
- 4 digital I/O ports, advanced security features, 1 RS-232/485 combo port

Expansion modules for the Catalyst IR1101

Enjoy the very small form factor of the Catalyst IR1101, or expand with one or two modules to add more connectivity options:

- IR1101 serial expansion module adds 4 asynchronous serial ports and 2 Gigabit Ethernet LAN ports
- IR1101 cellular expansion module adds one slot for a pluggable network module and one SFP Gigabit Ethernet port as well as an optional 4 GPIO ports and one mSATA slot for data storage

Cisco Catalyst IR8100 Heavy Duty Series Routers

- Heavy duty, IP67-certified, fully modular industrial router designed for harsh outdoor environments
- 5G, public and private LTE, and more
- Multilayered cybersecurity and hardware security
- Built-in edge compute and SD-WAN-enabled
- 1 Gigabit copper with PoE output
- 1 Gigabit fiber/SFP
- 3 additional I/O slots
- PoE or AC powered with built-in battery backup
- 12V DC for external devices

Cisco Catalyst IR8300 Rugged Series Router – FirstNet ready

- Rugged, 5G, integrated routing and switching platform for many industries and use cases
- IEC-61850-3 and IEEE 1613 certified for deployment in utility substations
- Hot-swappable, fully redundant power supplies and high-availability design for maximum network uptime and redundancy
- Multiple interface options, including Ethernet switch, T1/E1, and serial (RS-232)
- Enhanced security and advanced QoS for compliance with critical infrastructure protection mandates
- SD-WAN with comprehensive threat protection and security features
- Cisco IOS XE operating software
- Edge compute supporting IOx applications
- Cisco Cyber Vision sensor with Snort IDS for Industrial Control System (ICS) visibility
- Precision timing source

Pluggable network modules for Catalyst industrial routers

Cisco Catalyst industrial routers provide flexible networking options to meet your constraints and use case requirements. Use the pluggable module that supports the technology you need and replace to adapt to technology changes or as your needs evolve.

- 4G LTE pluggable module, FirstNet ready
- Cat18 4G LTE Advanced Pro pluggable module with CBRS and private-LTE support, FirstNet ready
- 4G LTE 450-MHz pluggable module*
- 5G Standalone (SA) and Non-Standalone (NSA) sub-6-GHz cellular pluggable module
- 5G Non-Standalone (NSA) sub-6-GHz cellular pluggable module

- LoRaWAN pluggable module*
- Wi-Fi 6 pluggable module†
- 2-port T1/E1 pluggable module‡
- 8-port RS232 serial pluggable module‡

* Catalyst IR1101 only
† Catalyst IR1800 only
‡ Catalyst IR8300 only

Next steps

To learn more about Cisco Catalyst industrial routers, visit **www.cisco.com/go/iot-routers**.

ıl¡ıl¡ı
CISCO
The bridge to possible

Cisco Industrial WPAN Routers

Not available for Europe

IR510   IR530

Cisco IR510 WPAN Industrial Router

- High-performance ruggedized router with 1.2 Mbps data rate

- Provides unlicensed 915 MHz, ISM-band Wireless Personal Area Network (WPAN) communications that enable IoT applications

- Open RF mesh solution based on the following standards: IEEE 802.15.4 g/e/v, IETF 6LoWPAN, IETF Routing Protocol for Low Power and Lossy Networks (RPL), IETF Mapping of Address and Port – Translation (MAP-T, and IETF Constrained Application Protocol (CoAP)

- IOx ready

Cisco IR530 Series Resilient Mesh Range Extenders

- Extend the range of the RF wireless mesh network, providing longer reach between WPAN endpoints and other WPAN networks

- Deliver unlicensed 902 to 928 MHz, ISM-band IEEE 802.15.4g/e/v WPAN communications to diverse IoT applications

- Increases communications network uptime and grid

availability, helps ensure message delivery through a rugged industrial hardware design and highly resilient solution architecture

- Lower total cost of ownership by consolidating disparate communications networks used for AMI and distribution automation applications

Next steps

To learn more about
Cisco industrial routers, visit: **cisco.com/go/iot-routers**.

Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB)

Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) delivers fiber-like wireless connectivity for moving assets or to extend your network where running fiber isn't feasible or is too costly. It provides high-bandwidth, high-availability, ultra-low latency, seamless handoffs with zero packet loss; making it ideal to connect the most demanding applications that need uninterrupted wireless connectivity. Cisco URWB is also scalable, easy to install and uses free spectrum.

Cisco URWB can be used to create static, nomadic, and seamless roaming wireless backhaul networks for OT applications. They have been designed and successfully deployed in rail, mining, smart cities, container terminals, entertainment, smart factories, military, automotive, and video broadcasting industries. The MPLS-based secure wireless protocol that enables this technology can provide a set of benefits that surpasses other standards and industrial solutions.

High bandwidth

A multigigabit data rate makes it the ideal choice for demanding applications such as real-time video surveillance, onboard Wi-Fi for edge devices, depot telemetry download, and much more.

Seamless handoff

Handoff is one of the primary challenges in vehicle-to-wayside communications. Unlike other technologies, Cisco URWB offers seamless roaming from one base station to the next, helping ensure strong radio signals or no packet loss so moving vehicles are always connected to the application.

Ultra-low latency

When real-time interaction is required, latency must be negligible compared to the reaction time. Thanks to their wireless aware switching protocol, these radio platforms have incredibly low latency, making them the ideal choice for remote control, machine-level protocols, VoIP, and autonomous and semi-autonomous applications.

Stability and reliability

Mission-critical OT networks cannot allow downtime. Losing connection in OT means stopping machines and processes, often resulting in a huge loss of money.

Thanks to the latest technologies and dedicated network design and deployment, Cisco will help make your wireless data network smooth and seamless.

Fast failover

Sometimes stability is not enough. Applications such as Communications-Based Train Control (CBTC) require a failover system in case of communication or hardware default. To accomplish this, Cisco introduced a special algorithm that can reconfigure the network on redundant hardware in less than 500 ms.

High availability

Cisco URWB's innovative patented technology, Multipath Operations (MPO), provides uninterrupted wireless connectivity by sending high-priority packets via redundant paths. It lowers the effects of interference and hardware failures preventing packet losses, lowering latency, and increasing availability.

Next steps

To learn more about Cisco Ultra-Reliable Wireless Backhaul, visit: **www.cisco.com/go/curwb**.

Cisco Catalyst IW9167E Heavy Duty Access Point

- Tri 802.11ax radio (2.4 GHz, 5 GHz, 5/6 GHz)

- Suitable for pole installation on wayside/trackside

- 4x4 MIMO, 4 spatial streams, with a wide choice of antennas to better suit each use case

- 8 N-type antenna connectors

- 2 Multigigabit RJ-45, SFP+, optional M12 adapters

- Heavy-duty, IP67 certified enclosure to operate under extreme water, dust, and temperature conditions (-50C to +75C)

- EN50155 certified for rolling stocks

- Also available in a version with Class I Division 2, Zone 2/22, ATEX, and IECEx certifications for hazardous locations (see data sheet for more details)

Cisco Catalyst IW9165D Heavy Duty Access Point

- Dual 802.11ax radio (5 GHz, 5/6 GHz)

- Built-in directional antenna for easy backhaul network deployments

- Choice of external antennas to quickly extend network to new places when needed (2 N-type)

- 2 Multigigabit RJ-45, optional M12 adapters

- Heavy-duty, IP67-certified enclosure to operate under extreme water, dust, and temperature conditions (-50 to +75C)

Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

- Dual 802.11ax radio (5 GHz, 5/6 GHz)

- DIN rail compact form factor to enable integration in industrial vehicles, robots, cranes, trains, and more

- Wide choice of antennas to better suit each use case (4 RP-SMA)

- 2 Multigigabit RJ-45, optional M12 adapter

- Ruggedized hardware supporting high temperature ranges (-40° to +70°C)

- EN50155 certified for rolling stocks

Next steps

To learn more about
Cisco Ultra-Reliable Wireless Backhaul, visit **www.cisco.com/go/curwb**.

Industrial Wireless (IW) access points and clients

Workers, assets, and resources are becoming increasingly connected in oil and gas, mining, transportation, and manufacturing. This expansion of IoT networking and equipment interconnectivity enables new use cases and opportunities, but it also places new demands on your infrastructure. Cisco responds to these demands with range of access point specifically designed for offering extended, high-performance wireless connectivity in these outdoor and harsh industrial environments.

Cisco Catalyst IW9167E Heavy Duty Access Point

- Tri 802.11ax Wi-Fi 6/6E radio (2.4 GHz, 5 GHz, 5/6 GHz), bringing all the benefits of Wi-Fi 6/6E to the harshest environments: more spectrum, more channels, higher throughput, and improved security
- 4x4 MIMO, 4 spatial streams, with a wide choice of antennas to better suit each use case
- Designed and certified for the harshest environments with extended operating temperature ranges of –50 to +75C; vibration rated to IEC 60068-2-6 environmental standards with M12 I/O connectors; and rugged IP67- rated enclosure to protect against liquid and dust ingress
- Supports GNSS, BLE and scanning radio for spectrum management minimizing interference
- Can be powered by PoE or DC
- EN50155 certified for rolling stock
- Also available in version with Class I Division 2, Zone 2/22, ATEX, and IECEx certifications for hazardous locations (see **data sheet** for more details)

Cisco Catalyst IW9167I Heavy Duty Access Point

- Tri 802.11ax Wi-Fi 6/6E radio (2.4 GHz, 5 GHz, 6 GHz), bringing all the benefits of Wi-Fi 6/6E to the harshest environments: more spectrum, more channels, higher throughput, and improved security.
- 4x4 MIMO, 4 spatial streams, with internal omnidirectional antenna 5-6 dBi
- Designed and certified for the harshest environments with extended operating temperature ranges of -50° to +65°C
- IP67-rated enclosure to protect against liquid and dust ingress
- Supports GNSS, BLE
- Can be powered by PoE or DC

Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

- Dual 802.11ax Wi-Fi 6/6E radio (5 GHz, 5/6 GHz) Wi-Fi 6/6E access point, or enable industrial assets to connect to your network over Wi-Fi using Workgroup Bridge (WGB) mode
- Compact form factor enables integration in industrial vehicles, robots, cranes, trains, and more
- Wide choice of antennas to better suit each use case (4x RP-SMA)
- Ruggedized hardware supporting high temperature ranges (-40° to +70°C)
- EN50155 certified for rolling stocks
- Supports GNSS, BLE
- Can be powered by PoE or DC

Cisco Catalyst IW9165D Heavy Duty Access Point

- Dual 802.11ax Wi-Fi 6/6E radio (5 GHz, 5/6 GHz) Wi-Fi 6/6E access point
- Built-in directional antenna for easy deployments
- Choice of external antennas to quickly extend network to new places when needed (2 N-type)
- 2 Multigigabit RJ-45, optional M12 adapters
- Heavy-duty, IP67-certified enclosure to operate under extreme water, dust, and temperature conditions (-50° to +75°C)

Next steps

To learn more about
Cisco Industrial Wireless access points and clients, visit **cisco.com/go/iw**.

Cisco Industrial IoT embedded networks portfolio

The Cisco industrial IoT embedded networks portfolio includes access points, routers, and switches that use Cisco's networking technology packaged into highly ruggedized, low size, weight, and power networking components. Their small form factor coupled with mobile and edge-specific features make these products ideal for applications across industries such as mining, oil and gas, transportation, shipping, and defense, where highly secure, reliable performance is required during extreme conditions.

Cisco 6300 Series Embedded Services Access Points (ESW6300)

Wi-Fi integration for challenging use cases
Get access points purpose-built for integration into smart-city and industrial environments.

Intelligence beyond boundaries
Extend policy and visibility from the enterprise to the edge with Cisco's intent-based networking together with the 6300 Series Embedded Services Access Points, which streamline network management and help reduce costs. Use Cisco IOx container support to host IoT applications at the edge for faster decision making.

Enhanced connectivity and flexibility
You'll get resilient 802.11ac Wave 2, with three PoE ports, one SFP port, and one USB port.

Deployment almost anywhere
Cisco 6300 Series access points are designed for the most extreme environments and temperatures (–40 to +85C).
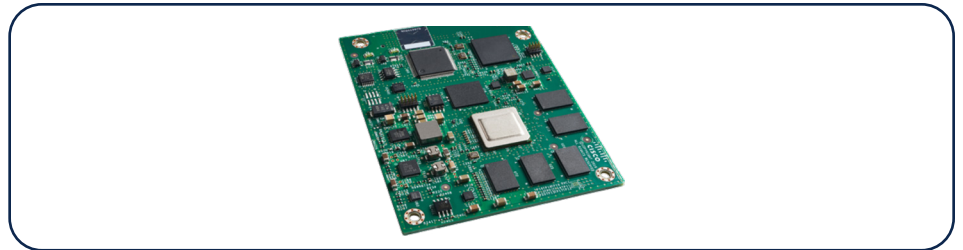
Cisco ESR6300 Embedded Services Router

Exponentially faster
The ESR6300 offers significantly faster crypto throughput than the previous generation of ESRs, to meet increased bandwidth needs arising from the rapid growth of sensor data and video streams.

Cisco trustworthy systems
The onboard Cisco Trust Anchor Module (TAM) plus image signing, secure boot, and runtime defenses help ensure that the code running on the Cisco ESR6300 is authentic, unmodified, and operating as intended.

Simplified integration
At 3 inches by 3.75 inches, the ESR6300 is smaller than its predecessors, making it easier to integrate into compact solutions. It is hardened for extreme temperatures, shock, and vibration to achieve the highest standard of reliability.

Modularity options
The ESR6300 provides two WAN ports of Gigabit Ethernet that give you a choice of media type and four LAN ports of Gigabit Ethernet with PoE/PoE+ ready options. As your needs evolve, add mSATA storage for Cisco IOx edge compute.

Streamlined management with Cisco IOS XE
Cisco IOS XE is highly programmable, with open and standards-based APIs and next-generation, multilayer security built in. This unified software stack is ideal for process and workflow automation, so you can qualify and deploy new services faster.

Software-defined WAN on the ESR6300
The ESR6300 is hardware ready to support SD-WAN so you can leverage IT expertise to a distributed network, operate at scale, and lower TCO. Cisco SD-WAN architecture delivers scale, simplicity, and unified management for extending the enterprise network to a distributed IoT deployment.
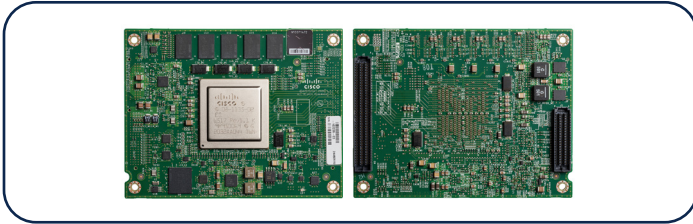
Cisco Catalyst ESS9300 Embedded Series Switch

· High-bandwidth with 10 ports of 10GE Small-Form-Factor Pluggable Plus (SFP+)
· Ruggedized for the harshest conditions, including extreme temperatures (-40° to +85°C), shock, and vibration
· Low power consumption: 35W
· RJ-45 Ethernet management port (optional)
· RJ-45 or USB micro-B console port
· Common +3.3V and 5V power inputs
· Crucial security features including secure boot and zeroization
· Advanced Cisco IOS XE operating system and WEBUI management
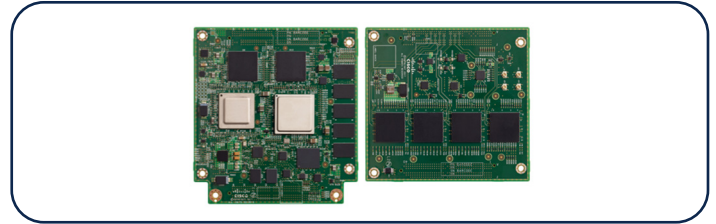
Cisco Embedded Service 3300 Series Switches

· High-speed PC 104 compact form-factor switch
· Ruggedized to operate in harsh environments (-40° to +85°C)
· Low power consumption (mainboard 16W, expansion 8W)
· 2x 10G uplink ports, 8x 1G downlink ports on mainboard
· 16x 1G downlink ports on expansion board for high port density
· Modern Cisco IOS XE operating system and WEBUI management
· PoE-ready architecture and software
· Layer 2 Network Essentials feature set

Next steps

Find out more about Cisco's **IoT embedded networks**.

Cisco LoRaWAN sensors solution

Cisco LoRaWAN gateways

LoRaWAN is unlicensed, Low-Power Wide-Area (LPWA), long-range wireless technology applicable to both private and public IoT infrastructure. It is used to connect a range of devices and environmental sensors that need low data rates and long battery lives to operate unattended for extended periods of time.

The Cisco LoRaWAN solution offers customers a fully integrated and functional architecture that supports both service providers and industrial customers and complies with the architecture and specifications defined by the LoRa Alliance.

Cisco Catalyst IR1100 Rugged Series Routers – now with LoRaWAN

- LoRaWAN module turns the Catalyst IR1101 into an 8-channel LoRaWAN gateway

- Modular and expandable hardware design supporting a wide choice of integrated WAN interfaces such as Ethernet, 4G, and 5G

- IEC 61850-3 and IEEE 1613 certified for deployment in power utility substations

Cisco Wireless Gateway for LoRaWAN (IXM)

- 16-channel LoRaWAN gateway

- GNSS support for geolocation applications and precise timestamping

- Heavy-duty IP67-rated enclosure for deployment in outdoor and harsh industrial environments

Cisco industrial sensors

Choose from a large family of LoRaWAN sensors to collect environmental and operational data. Cisco's industrial sensor options include:

- Vibration sensor
- Outdoor/Indoor temperature sensor
- Machine temperature sensor
- Refrigeration/Humidity sensor
- Water leak detection sensor

- Door/Window open/ closed sensor
- Indoor occupancy sensor
- Light detection sensor
- Geolocation sensor
- Analog/Digital Sensor Bridge

Cisco Industrial Asset Vision

Cisco Industrial Asset Vision, an all-in-one cloud-based solution to manage Cisco industrial sensors and gain centralized visibility of your sensor data so you can monitor remote facilities and industrial operations easily and securely.
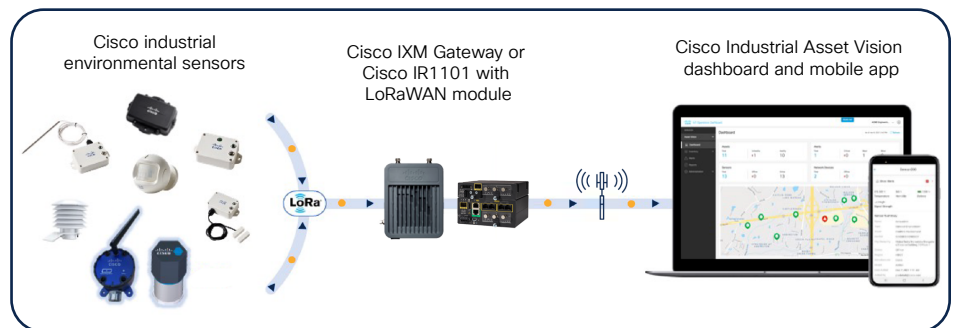
It is the ideal companion to Cisco LoRaWAN gateways, leveraging the extensive range and deep penetration capabilities of LoRaWAN to monitor and collect data from industrial assets and facilities to keep everything running efficiently.

The entire solution deploys in minutes using a simple QR code, and scaling up by adding more sensors is easy. As a cloud-based solution for management and

visualization, Industrial Asset Vision requires little technical expertise to deploy or use.

Users can view insights in one easy-to-use dashboard. For example, they can see that the temperature of an asset is outside acceptable values, or that a warehouse door has been left open. The dashboard provides a single view of asset or facility health across all connected sensors, helping operations teams identify potential issues in advance so they can optimize preventive maintenance processes.

For customers willing to deploy a LoRaWAN network server on-premises, Cisco partners with Actility to complement our LoRaWAN portfolio. Actility's ThingPark Enterprise platform is for dedicated enterprise networks, and is simple, scalable, and easy to operate. It offers a unique IoT communication infrastructure to enable an infinite number of industrial use cases.
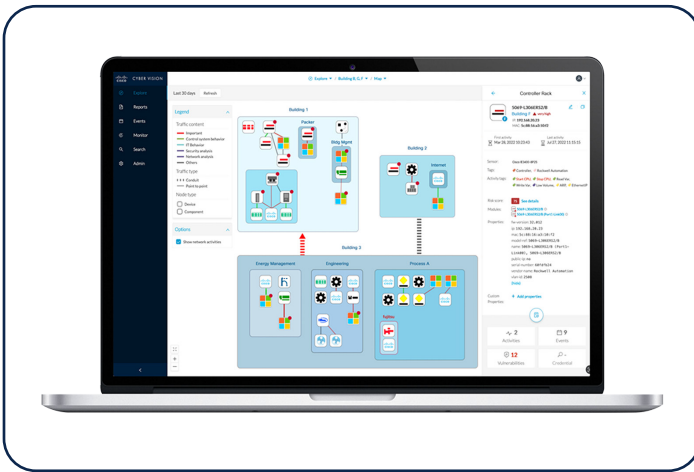

Cisco industrial environmental sensors — Cisco IXM Gateway or Cisco IR1101 with LoRaWAN module — Cisco Industrial Asset Vision dashboard and mobile app

Next steps

To find out more about Cisco's LoRaWAN solution, visit **www.cisco.com/go/lorawan**.

Industrial cybersecurity

Cisco Cyber Vision

Visibility into your OT/ICS assets and your security posture.

Cisco Cyber Vision provides asset owners full visibility into their Industrial Control System (ICS) and their OT security posture so they have the information they need to reduce the attack surface, segment the industrial network, and enforce cybersecurity policies. Its advanced OT monitoring capabilities also provide insights to improve network efficiency and enable faster troubleshooting of operational issues.

Combining a unique edge architecture that embeds OT security features into your industrial network and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale to enable IT and OT teams to work together in building innovative industrial operations while securing the global enterprise.

Benefits

Unmatched visibility into all connected assets

Know what to protect. Cisco Cyber Vision automatically builds a detailed inventory of all connected assets, including their communication patterns, vulnerabilities, rack slot configurations, vendor references, serial numbers, and more.

Visibility embedded into your industrial network

Easily deploy at scale. Cisco Cyber Vision embeds visibility capabilities into industrial network equipment. No need to source dedicated appliances or build a dedicated out-of-band network. Network managers will appreciate the unique simplicity and lower costs of Cisco Cyber Vision.

Security posture for IT

Reduce the attack surface. Cisco Cyber Vision calculates risk scores for each part of your operations to help you prioritize what needs to be fixed. Fully integrated with the Cisco security portfolio, it extends the IT Security Operations Center (SOC) to the OT domain.

Operational insights for OT

Improve network performance and reduce downtime. Cisco Cyber Vision provides insights into network issues, device misconfigurations, communication problems, unexpected changes to industrial processes, malicious traffic, and more.

Microsegmentation made simple with Cisco ISE

Implement ISA/IEC62443 zones and conduits. Cisco Identity Services Engine (ISE) leverages asset groups created by control engineers in Cyber Vision to build and enforce network access policies driving dynamic and automated segmentation of the industrial network.

**Threat investigation and remediation with Cisco Extended Detection and Response (XDR)**

Extend IT security to your OT. Cisco XDR aggregates threat intelligence from multiple security solutions, including OT context from Cyber Vision. Run investigations across the IT and OT domains in a single console. Manage cases and launch remediation with custom playbooks and workflows.

Next steps

To find out more about how Cisco can help you protect your industrial operations from cyber threats, visit **www.cisco.com/go/cybervision** or **www.cisco.com/go/iotsecurity**.

Cisco Secure Equipment Access

Zero-Trust Network Access (ZTNA) for operational environments
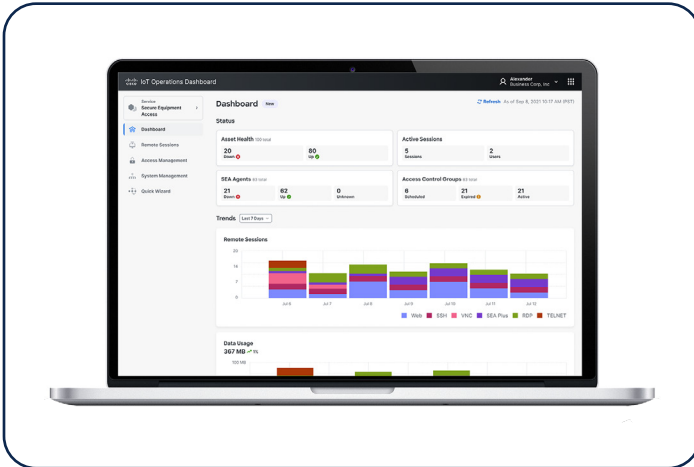
Remote access is key to being able to configure, manage, and troubleshoot OT assets without time-consuming and costly site visits. Enabling secure remote access at scale can be a daunting task: Sites might be highly distributed, and assets are often sitting behind Network Address Translation (NAT) boundaries. Configuring firewall rules and deploying dedicated gateway hardware puts an extra burden on IT and OT teams.

With Secure Equipment Access (SEA), Cisco is solving these challenges. It combines all the benefits of a ZTNA solution with a network architecture that makes it simple to deploy at scale in operational environments. There is no dedicated hardware to install and manage. No complex firewall rules to configure and maintain. The Cisco industrial switches or routers that connect your OT assets now also enable remote access to them. And it features comprehensive security capabilities, with advanced cybersecurity controls and easy-to-build policies based on identities and contexts.

Benefits

- **Boosts operational efficiency:** Empower operations teams to easily gain remote access to OT assets, even those behind NAT boundaries

- **Simple to install and scale:** Stop struggling with dedicated appliances and complex firewall setups. Cisco SEA is embedded in switches and routers

- **Offers least-privilege access:** Allow select users to access only specific devices, using only certain protocols, and only at defined times

- **Enforces strong security controls:** Authenticate users with MFA and SSO. Verify their security posture. Block asset discovery and lateral movement

- **Takes control back:** Record sessions and build audit trails for investigation and compliance. Join and terminate active sessions

Next steps

To find out more about Cisco Secure Equipment Access and ZTNA for OT, visit **www.cisco.com/go/sea** or **www.cisco.com/go/iotsecurity**.

Cisco Secure Firewall ISA3000

Developed specifically to withstand the harshest industrial environments, the Cisco Secure Firewall ISA3000 offers uncompromising end-to-end security with industrial design and operation in mind.

Featuring a compact DIN rail unit and ruggedized design, these industrial security appliances are true industrial firewalls that provide OT targeted protection based on proven enterprise-class security leveraging Cisco Firewall Threat Defense (FTD) services or Adaptive Security Appliance (ASA) with FirePOWER Services.

Key features:

- **Visibility and control of protocols**, including DNP3, CIP, Modbus, IEC 61850, IEC 104, and applications by Omron, Rockwell, GE, Schneider, and Siemens
- **Environmental hardening** for vibration, shock, surge, and electrical noise immunity
- **Compliance** with multi-industry specifications for industrial automation, ITS, and electrical substation environments
- **Multidevice management** across hundreds of devices using Cisco Secure FMC
- **Proven threat detection** with over than 25,000 rules powered Talos Threat Intelligence give the ISA3000 the widest range of operational technology protection
- **High availability** features such as hardware bypass, dual-power inputs, quality-of-service policies, and latency detection and mitigation functions help ensure traffic continuity to keep operation on track

Use cases:

Protect individual zones with network segmentation

Use the ISA3000 to separate different parts of the network in your manufacturing cells, zones, or utility substations to ensure only authorized devices or connections have access, protecting the network from malicious or unwanted activities.

Network Address Translation (NAT) ensures more efficient operations

The ISA3000 eliminates duplicate IP addresses by providing a unique IP address to each device, ensuring every device is visible on the network and able to receive commands.

Secure Remote Access

The ISA3000 provides flexible, enterprise class remote access control via Cisco AnyConnect, Site to Site VPN, Remote Access VPN, and Clientless SSL VPN offerings.

Next steps

To find out more about the Cisco Secure Firewall ISA3000,
visit **www.cisco.com/go/isa3000** or **www.cisco.com/go/iotsecurity**.

Management

[Cisco Catalyst Center](#)

Cisco Catalyst Center is a proven network management system deployed in the world's largest enterprises and most complex networks. Cisco Catalyst Center in industrial automation networks gives OT a curated view and set of functions to perform key network maintenance tasks, consistently and scalably, increasing Overall Equipment Effectiveness (OEE) and uptime, lowering operational costs, enhancing security, and helping ensure network performance.

Benefits

Network automation

- Discover existing network devices and topology
- Use network Plug and Play to provision new infrastructure
- Check for inconsistent configurations
- Deploying new images and patches at scale

Network assurance

- Collecting and analyzing network telemetry information
- Proactively identifying issues and root causes
- Helping step through remediation options

Industrial cybersecurity

- Detailed visibility into connected industrial assets and applications
- Segment communications
- Monitor and detect abnormal behaviors
- Contain malware and other attacks
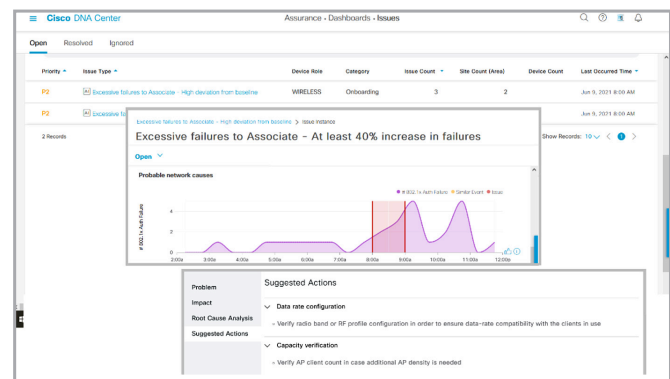- Integrate operational and enterprise security

Next steps

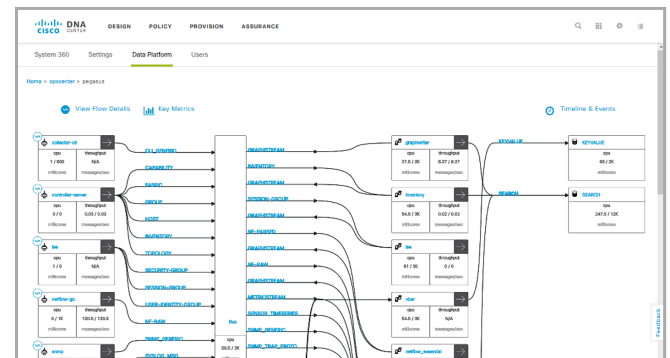To find out more about Cisco Catalyst Center, visit **www.cisco.com/go/iotmanagement**.
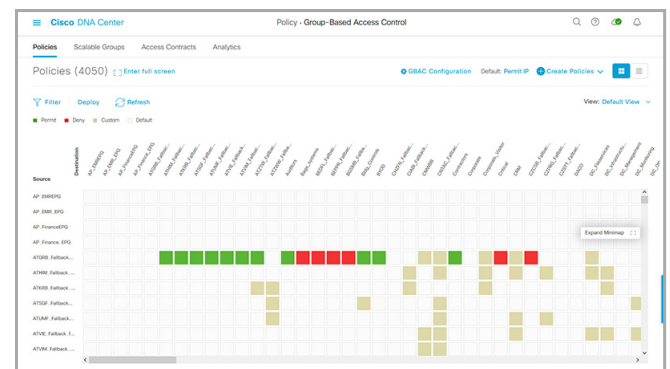
Network health
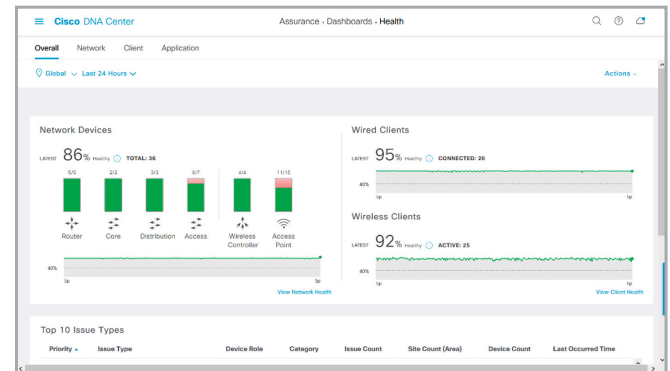
Network issues

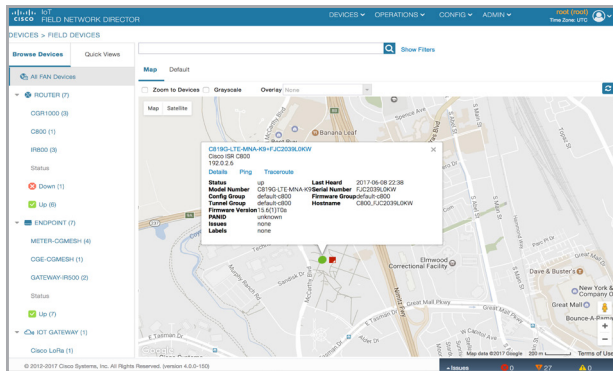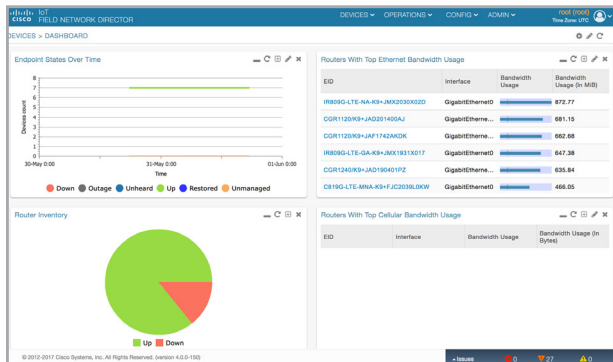**Network topology**

Access policies for segmentation
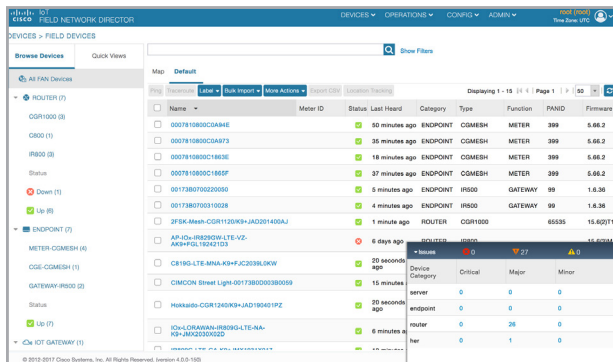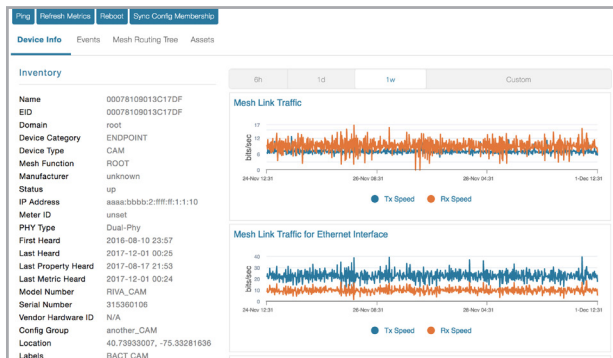
GIS map

Dashboard

Device listing

Device properties

Cisco IoT Field Network Director (FND)

The Cisco IoT Field Network Director (FND), the operating system for the multiservice Field Area Network (FAN), is a software platform that manages multiservice networks of Cisco industrial products, connected grid routers, and endpoints. Features that distinguish the IoT FND include:

- Ease of deployment at scale with Zero-Touch Deployment (ZTD) of gateways and devices
- Secure and scalable end-to-end enrollment and management of these gateways and devices
- Optimized for operation in constrained bandwidth network
- Ease of use with an intuitive web interface and GIS map visualization and monitoring
- Rich set of northbound APIs for third-party integration
- Scales to manage up to tens of thousands of routers and millions of mesh endpoints
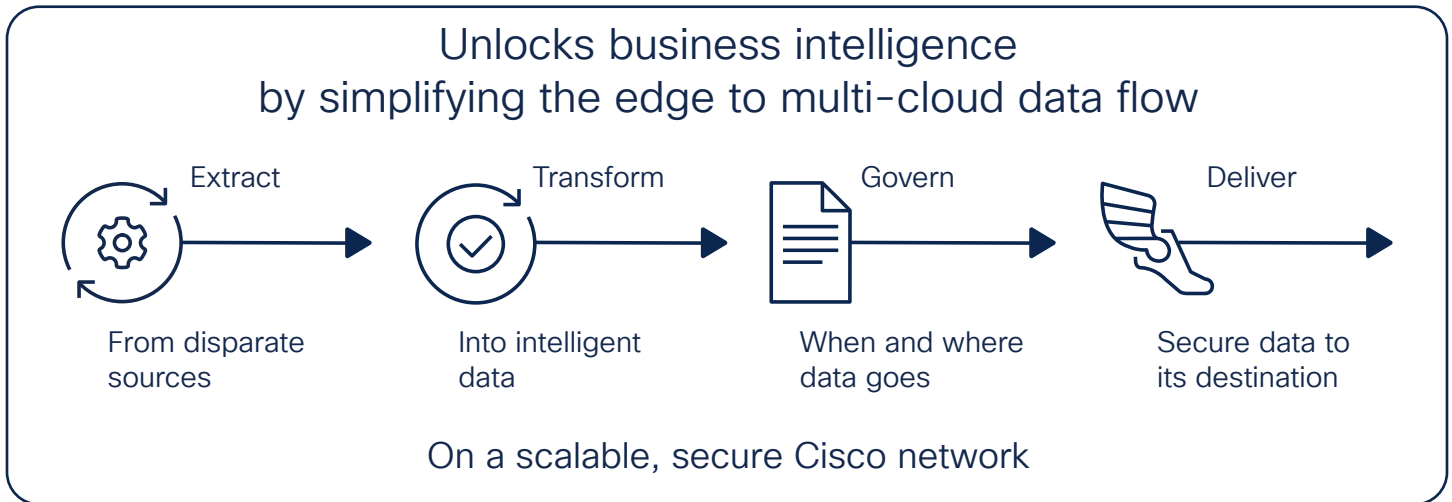
Benefits

- Comprehensive and customizable dashboard for fast, at-a-glance network health check
- Real-time GIS maps of connected devices for increased asset visibility
- Simplify troubleshooting for operators by providing customizable rules to generate custom events that matter the most
- Integrate with existing automation applications, tools, and processes through open APIs
- Supports Cisco 1000 Series Connected Grid Routers, Cisco 800 Series Industrial Integrated Service Routers, and LoRaWAN

Next steps

To find out more about Cisco IoT Field Network Director, visit www.cisco.com/go/fnd.

ılıılı
CISCO
The bridge to possible

Edge computing

Cisco Edge Intelligence

Unlocks business intelligence
by simplifying the edge to multi-cloud data flow

Extract
From disparate
sources

Transform
Into intelligent
data

Govern
When and where
data goes

Deliver
Secure data to
its destination

On a scalable, secure Cisco network

Unlock business value by simplifying the edge-to-multicloud data flow

The best decisions are made when the right people have access to the right information at the right time. The IoT has dramatically increased the volume and variety of data produced, opening the door to a wave of new possibilities. The key is to extract the data from its source, transform it so it is usable, and securely deliver the right data to the right applications to put it to work.

But most solutions today are so complicated that organizations often cannot reap the full rewards of their data-gathering projects. The most important data is often at the remote edge of the network, where the core business operates, such as in oil rigs, delivery trucks, and utility substations, and on roads. In addition, organizations lose insight into who has access to what data and often don't have the needed flexibility and simplicity to send the data everywhere it needs to go.

Cisco Edge Intelligence delivers

Cisco Edge Intelligence securely delivers data from connected assets at the network edge to multicloud application destinations. The software is integrated into Cisco's industrial networking and compute devices for an out-of-the box experience to simplify deployment and lower costs. It provides full control over and governance of IoT data, from its extraction to its transformation to its secure delivery. And because Cisco Edge Intelligence has a network- integrated approach with centralized management across the network, applications, and data, it is easy to scale and secure.

Benefits

With Cisco Edge Intelligence, you gain:

· The ability to seamlessly extract, transform, and share data from connected assets at the IoT edge to multicloud environments

· An all-in-one solution for easy deployment out of the box

· Full data ownership, control, and governance

· Cisco security

Next steps

To learn more about
Cisco Edge Intelligence,
visit **www.cisco.com/go/edgeintelligence.**

Cloud Delivered Services

Cisco IoT Operations Dashboard

A modular, cloud-based toolset to deploy, manage, and secure industrial networks at scale.
IoT Operations Dashboard provides tools to deploy OT services across Cisco industrial IoT switches and routers. This enables organizations to deploy and upgrade these services easily and at scale.

IoT Operations Dashboard includes the following services:

- Secure Equipment Access for Zero-Trust Network Access (ZTNA) to assets deployed in remote locations

- Cisco Cyber Vision (new) for automated discovery of connected assets, their vulnerabilities, and your cybersecurity risks

- Cisco Industrial Asset Vision to monitor assets and facilities using Cisco industrial sensors

- Cisco Edge Intelligence to enable edge to multicloud data orchestration

In addition to being able to deploy and manage their industrial networks, operations teams can use IoT Operations Dashboard to inform business decision-making by leveraging data from the edge. To enable this capability, edge Intelligence provides ready-built connectors to support a wide range of connectivity protocols to collect data from connected assets, transform and correlate that data, and forward it to upstream, multicloud environments for further processing or presentation.

Next steps

To find out more about Cisco IoT Operations Dashboard, visit **www.cisco.com/go/operationsdashboard**.

Cisco IC3000 Industrial Compute Gateway

Transforms businesses by capturing data from legacy assets and deriving business intelligence at the network edge
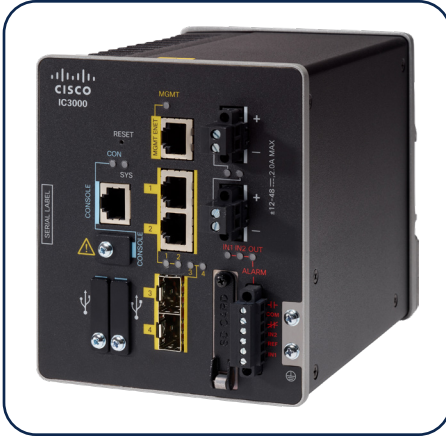
Key features:

- **Zero-touch provisioning:** Reduces the cost of deploying the IoT edge infrastructure

- **Application development tools:** Provides flexibility for developers to use any programming language or operating system, powered by Cisco IOx

- **Device and app lifecycle at scale:** Enables IT and OT admins to easily manage, monitor, troubleshoot, and upgrade IoT applications centrally using Cisco IoT Field Network Director

- **Brings intelligence to the edge:** It has two Ethernet ports and two SFP fiber ports in a DIN rail-mounted, ruggedized appliance that provides the widest range of applications for the harshest and most demanding industrial environments

- Enables application developers to unleash their creativity in developing apps that harness the wealth of IoT data, such as smart roadway applications with applications for traffic pattern detection, hazardous weather warnings, and road condition detection

Optional applications

- **Cisco Edge Intelligence:** IoT software integrated with Cisco's industrial networking portfolio to securely and simply extract, transform, govern, and deliver data from the edge to multicloud environments.

- **Cisco Cyber Vision Hardware Sensor:** Gain visibility into your industrial control network to assess your OT security posture and protect your operations from cyber risks. The Cisco IC3000 collects traffic from network equipment that does not support the embedded Cyber Vision sensor software to extract the needed information to build asset inventories, map application flows, detect vulnerabilities, malware, and intrusions (IDS)

Next steps

To find out more about the Cisco IC3000 Series,
visit **www.cisco.com/go/ic3000**

## Cisco IOx

Edge compute application framework

Fast. Simple. Secure. Scalable.

Cisco IOx is a simple yet powerful infrastructure framework allowing developers and operators to securely onboard legacy and greenfield applications to their IoT edge infrastructure at massive scale, creating business value from previously untapped data.

Benefits

- **Transformation of IoT data into new digital business value:** Build new business with the ability to process high volumes of data at the edge and deliver closed loop system control in real time

- **Rapid time to value:** Achieve business outcomes associated with IoT initiatives more rapidly with application execution at the edge and scale with the Cisco partner ecosystem

- **Broad scope of impact:** Reach production deployment rapidly with edge application management and execution at IoT scale

Docker developer tool EMU
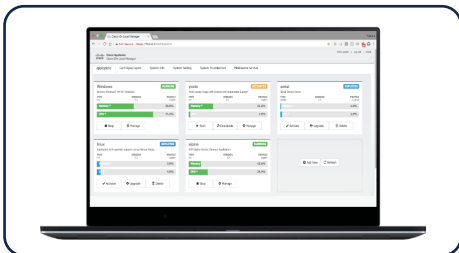
- Execute container or virtual machine concurrently
- Run Windows or Linux applications
- Easily consumable IOx system services

Management tool
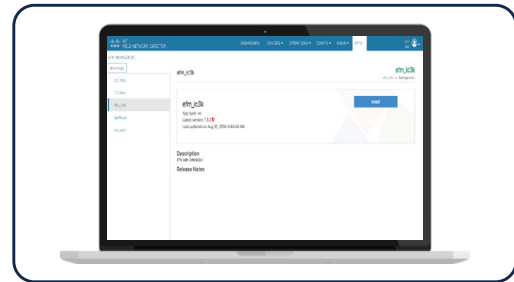
- Zero touch deployment of devices
- Centralized device and application lifecycle management at scale
- End-to-end security

Cisco IOx components

- **Cisco IOx enabled edge network devices:** The Cisco IOx edge application framework provides uniform and consistent hosting capabilities for applications across Cisco IoT network infrastructure. The Cisco IOx edge application environment brings together Cisco IOS Software, the industry-leading and highly secure networking operating system, and Linux, the leading open-source platform

- **Cisco IOx developer tools and documentation:** SDKs, command-line and web-based UI tools, and Cisco DevNet documentation on how to build, package and deploy edge applications to Cisco IOx enabled network devices

- **Cisco IOx edge application management:** Deploy and manage IOx edge applications at scale from centralized device and edge application management software. Support for both on-premises and cloud based management. These edge applications may be supplied by an ecosystem partner and Cisco or developed with a range of common programming languages

Next steps

The Cisco IOx application framework offers consistent management and hosting across network infrastructure products. To find out more about Cisco IOx, visit **www.cisco.com/go/iox** and **developer.cisco.com/docs/iox/**.

Cisco IoT Validated Designs

We know our products have proven to be the industry's best "ingredients" for IoT networks. But we also know there can be complexity in designing, deploying, and managing those products into a "meal" – a complete solution to support all courses of a real-world use case.

That's why we have Cisco Validated Designs (CVDs). They are used to validate, architect, and configure next-generation technologies. Each is designed to help you accelerate digital transformation, innovate faster, and stay competitive.

Think of them as blueprints to your successful implementation. For every CVD, our engineers create detailed design and implementation guides that use Cisco and our partners' products to address critical business needs. We then engineer, test, and validate each design for our customers' industry-specific requirements, to guide their own deployments.

Next step

To see how Cisco Validated Designs can help you, visit **www.cisco.com/go/iotcvd**.

Featured design guides

Extended enterprise
Securely extend your IT network to rugged and outdoor spaces.

Manufacturing
Improve business operations by digitizing production environments.
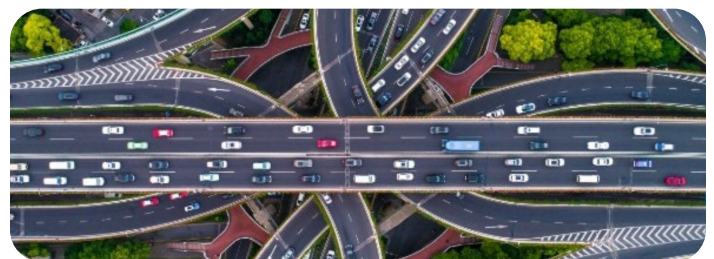

Utilities and renewables
Modernize the power grid to improve reliability, security, and distributed renewable resources.

Roadways and intersections
Improve public safety, operational efficiency, and traffic management.

CISCO

The bridge to possible

Cisco industrial IoT solutions

Connected Factory

Factory Wireless

Site Asset Management

Substation Automation

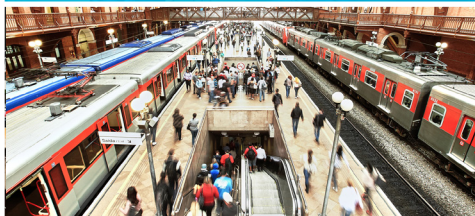**Utility WAN**

Field Area Network (AMI)

Connected Renewables

Industrial Security

Smart Cities

Roadways and Intersections

Connected Rail

Connected Mass Transit

Connected Fleet

Connected Pipeline

Connected Refinery

Cisco IoT accelerates digital transformation, delivering insight and action from your data.

www.cisco.com/go/iot

ı‖ı‖ı
CISCO
The bridge to possible

Cisco Industrial IoT portfolio

Deploy. Accelerate. Innovate.

Cisco industrial IoT is an end-to-end architecture that enables you to digitize your business and drive better business results. It offers rock-solid infrastructure, unprecedented visibility, security, and control, and trusted expertise to help ensure the success of your IoT deployment.

www.cisco.com/go/iot