Configuring, Monitoring and Troubleshooting Industrial IOT SDWAN Deployments

Configuring, Monitoring and Troubleshooting Industrial IOT SDWAN Deployments

This 5-day immersive, hands-on course is tailored for engineers and administrators deploying Cisco Catalyst SD-WAN (Viptela) environments with a specific focus on integrating Cisco Industrial IoT (IIoT) solutions. Targeting version 20.15/IOS-XE 17.15, this training emphasizes real-world use cases for Cisco IIoT Routers, the Secure Equipment Access (SEA) solution, and CyberVision as they relate to Cisco SD-WAN deployments. Students will learn to install, configure, monitor, and troubleshoot Catalyst SD-WAN environments while exploring advanced capabilities in policy management, routing, and security. Particular attention is given to enabling visibility, segmentation, and secure access for OT environments within industrial networks.

The course includes IIoT-specific modules and labs that highlight the deployment of ruggedized Catalyst IR series routers, configuration of SEA to provide secure remote access to industrial assets, and integration of CyberVision for industrial threat detection and asset visibility. Additional focus areas include centralized management through vManage, automated provisioning using Zero Touch Provisioning (ZTP), application-aware routing, and deep integration with ThousandEyes and Cisco CyberVision analytics for continuous performance and threat monitoring across industrial networks.

How you'll benefit

This class will help you:

- Learn SD-WAN and Industrial IoT Convergence
- Understand Catalyst SD-WAN and Industrial Router Platforms
- Troubleshoot SD-WAN for Industrial Environments

Course Duration
5 days
Course Price
$4,395.00 or 43 CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- IoT Network Engineers.
- IoT System Administrators
- IoT IT Professionals
- IoT Technical Support Staff
- IoT Cisco Certified Professionals

Prerequisites

- Basic Knowledge of CCNA

OUTLINE

Module 0: Course Introduction and Learning Objectives

- Overview of the training agenda and structure
- Introduction to the Cisco Catalyst SD-WAN platform and its relevance to industrial networks
- Key learning outcomes:
    - Deploying Catalyst SD-WAN with IR1100, IR1800, and IR8300 routers
    - Implementing secure access to industrial equipment using SEA
    - Integrating CyberVision to provide real-time visibility and policy enforcement
- Overview of lab topology and equipment
- Understanding IT/OT convergence in modern industrial networks

Module 1: SD-WAN and Industrial IoT Convergence

- The role of SD-WAN in industrial and remote environments
- Benefits of SD-WAN for manufacturing, energy, utilities, and transportation
- Understanding challenges in OT networks (e.g., legacy protocols, environmental constraints, intermittent connectivity)
- Overview of Cisco's Industrial Networking Portfolio:
    - IR1101 – compact and modular for mobile/field deployments
    - IR1800 – medium-scale industrial locations
    - IR8300 – modular for high-performance industrial backbones and substations
- How SD-WAN enables segmentation, redundancy, and secure remote access for OT
- Key industrial deployment use cases:
    - Remote monitoring of PLCs
    - SCADA communication optimization
    - Redundant failover paths for mission-critical data
    - Converged security posture for plant and IT environments

Module 2: Cisco SD-WAN Controller Architecture

- Functional roles of SD-WAN Validator, SD-WAN Controller, and SD-WAN Manager in the SD-WAN fabric
- Control plane and data plane separation
- High availability and redundancy planning for industrial SD-WAN controllers
- Multitenant architecture for shared OT/IT facilities
- Onboarding routers to the SD-WAN fabric through certificate-based authentication
- Controller deployment scenarios (cloud vs on-prem) for industrial environments

Module 3: Catalyst SD-WAN and Industrial Router Platforms

- Detailed overview of the following platforms:
    - IR1100 Series: Fanless, DIN-rail mountable with expansion modules, cellular-ready
    - IR1800 Series: High-throughput with support for automation protocols, dual power input
    - IR8300 series: Modular, hardened, integrated with CyberVision sensor capabilities, multiple WAN/LAN modules
- Integration with cellular gateways and public/private LTE/5G
- Use of expansion modules for serial, I/O, GPIO interfaces in OT deployments
- Managing SD-WAN features like application routing, security zones, and telemetry on rugged devices
- WAN Edge design and high availability options (Active/Standby and Active/Active) for industrial routers

Module 4: WAN Edge Provisioning and Onboarding

- Use of Plug and Play (PnP) portal and Zero Touch Provisioning (ZTP) for remote onboarding
- Manual onboarding using bootstrap CLI workflows

- Image selection, signing, and validation for IR router platforms
- Device authentication process via controller PKI
- Troubleshooting onboarding failures and connectivity tests

Module 5: Routing and Segmentation in Industrial Environments

- Configuration of SD-WAN routing protocols: OSPF, BGP, static routes
- Route advertisement between IT and OT domains
- Creating VPN segments for SCADA, video surveillance, and telemetry traffic
- Route redistribution and protocol translation between MPLS and cellular uplinks
- Planning logical segmentation between field-level and control-level networks

Module 6: SD-WAN Manager – Configuration and Access

- Navigating the SD-WAN Manager interface
- Monitoring industrial routers and remote branches
- Administrative controls: user roles, RBAC for plant engineers vs IT admins
- Central configuration workflows for remote IR routers
- Viewing device health, link status, and event logs
- Integration with external identity platforms (SSO, RADIUS, TACACS)
- Secure separation of OT domains using resource groups

Module 7: Software Upgrades and Maintenance

- Upgrade strategy for IR routers in live environments
- Managing mixed-image environments in large deployments
- Upgrade sequencing for SD-WAN Validator, SD-WAN Controller, and SD-WAN Manager, and IR devices
- Planning firmware upgrades across industrial routers with minimal disruption
- Rollback procedures for failed upgrade scenarios

Module 8: SD-WAN Fabric and Tunnel Operations

- Understanding OMP and TLOC concepts for IR series routers
- BFD for dynamic path selection and failure detection
- IPsec and GRE tunnels in bandwidth-constrained environments
- Tunneling for isolated sites using satellite or cellular
- Use of color and control policies to determine path selection
- Tunnel verification and failover simulation

Module 9: Quality of Service (QoS) and Application Experience (QoE)

- Prioritization of SCADA, video, VoIP, and telemetry traffic
- Application recognition and performance baselining
- Adaptive QoS for LTE/5G industrial links
- Forward Error Correction (FEC) and Packet Duplication for unreliable links
- Integration with SD-AVC and AppQoE to identify application behavior
- Compression mechanisms (DRE/LZ) to improve performance over low-bandwidth circuits

Module 10: Securing the Industrial SD-WAN Fabric

- Role of encryption in securing SCADA and automation traffic
- Lockdown strategies for remote router access
- Use of firewalls, IPS, anti-malware, and DNS security
- Implementing zone-based firewalls on IR routers
- Integration of URL filtering and threat defense into OT networks

- Securing external vendor access via SEA
- CyberVision introduction:
    - Understanding asset discovery and profiling
    - Visibility into industrial traffic patterns and anomalies
    - Ingesting data into SD-WAN for dynamic policy enforcement

Module 11: Configuration Templates and Groups

- Creating and applying Feature Templates for serial, I/O, and cellular interfaces
- Defining Device Templates for specific industrial router types
- Configuration Groups for scaling deployment across remote substations, plants, and yards
- Using the Configuration Catalog for template reuse
- Managing configuration drift and rollback in IIoT environments

Module 12: Local Policy Implementation

- Designing local data policies for isolated OT zones
- Rate-limiting and shaping on a per-port or per-VPN basis
- Access control using ACLs and data matching conditions
- Using local control policies to manipulate OMP route advertisements
- Local policy testing and validation

Module 13: Centralized Policy Enforcement

- Architecture of control and data policies in SD-WAN
- Designing control policies to prioritize field operations traffic
- Service chaining for CyberVision and firewall integration
- Path steering policies for OT traffic over cellular, satellite, and private lines
- Configuring data policies to restrict east-west and north-south traffic
- Using CyberVision data to influence policy changes dynamically

Module 14: Policy Groups for OT Traffic Management

- Grouping policies by function (e.g., Safety, Surveillance, Production)
- Creating reusable policy objects based on SCADA, HMI, or camera traffic
- Enforcing NGFW rules, SLA expectations, and telemetry requirements
- Associating policy groups to device groups in remote locations
- Leveraging UI enhancements (UX 2.0) to visualize industrial policy topology

Module 15: Secure Equipment Access (SEA)

- Overview and architecture of SEA
- Enabling secure, approved remote access to PLCs, HMIs, and sensors
- Integrating SEA with IR routers for session logging and policy enforcement
- Access control workflows, approval cycles, and compliance
- SEA use cases: vendor maintenance, emergency remote access, diagnostics

Module 16: CyberVision Deep Integration with SD-WAN

- Sensor deployment modes: embedded, external, gateway-based
- Identifying and profiling OT assets and protocols
- Monitoring flows across industrial zones
- Integrating CyberVision intelligence into SD-WAN policy decisions
- Triggering alerts and dynamic segmentation based on anomaly detection
- CyberVision dashboard walkthrough and event correlation

Module 17: Cloud OnRamp for SaaS and Enterprise Apps

- Using SD-WAN to optimize M365, ERP, and manufacturing cloud workloads
- Cloud OnRamp for Webex, O365, and custom industrial SaaS
- Traffic path monitoring and performance enforcement for SaaS
- Integration with centralized and local security policies for SaaS

Module 18: Analytics, Visibility, and Industrial Monitoring

- Using ThousandEyes agents on IR8300 and IR1835
- Digital experience monitoring for plant-to-cloud connectivity
- CyberVision-based asset health scoring
- Bandwidth forecasting and KPI dashboards
- Troubleshooting workflows using correlated data from multiple tools

Module 19: Troubleshooting SD-WAN for Industrial Environments

- Diagnosing router onboarding, routing, tunnel, and policy issues
- Real-time CLI and GUI-based troubleshooting using vManage
- Analyzing OMP, BFD, tunnel state, and control connections
- Troubleshooting configuration groups and template attachment
- Using vDiagnose, logs, and NetFlow in low-bandwidth environments
- Troubleshooting SEA sessions and CyberVision alerts

Appendix A: Controller Deployment

- Deploying SD-WAN Validator, SD-WAN Controller, and SD-WAN Manager on ESXi/KVM
- Secure controller configuration and certificates
- Linking IR routers to controllers
- Best practices for hybrid IT/OT controller deployment

Appendix B: Lab Exercises

- Lab 1–4: Controller deployment and onboarding
- Lab 5–7: Provision IR1101/IR8300 via ZTP
- Lab 8–10: Create configuration templates and groups
- Lab 11: Deploy and verify SEA access to PLCs
- Lab 12–14: Install CyberVision sensors, configure dashboards
- Lab 15–16: Create policies using CyberVision asset groups
- Lab 17: Troubleshoot SD-WAN device registration and tunnel issues
- Lab 18: Use ThousandEyes for industrial path visibility