



---

## Implementing and Configuring Cisco SDWAN

DURATION: 5 DAYS    COURSE CODE: ICSDWAN-CT    FORMAT: LECTURE/LAB

---

### COURSE DESCRIPTION

In this Implementation and Configuration SDWAN Course, students will deploy and configure SD-WAN Controllers, vEdge Devices, and Cisco IOS-XE Devices. Students will create Multiple Device and CLI Templates that will allow Hundreds of devices to be deployed using only a few Centralized Templates. Students will create Security Policies to enable the Enterprise Firewall, IDS/IPS, URL Filtering, and Web Layer Security to protect and allow Enterprises to deploy Cloud applications as well as Direct Internet Access (DIA). Students will also create Local and Central Policies that enable a Centralized Policy control of WAN Routing and device QOS configuration and enforcement. Students will also learn how Cisco SD-WAN allows Enterprises to deploy an effective Cloud Solutions such as Amazon AWS, Microsoft Azure, and Google Cloud. Students will also learn how to Monitor and Troubleshoot the SD-WAN Solution.

### LEARNING OBJECTIVES

- SDWAN Overview
- Cisco SDWAN Hardware
- Deploying the Overlay
- Configuring vManage
- Monitoring vManage
- vAnalytics
- Troubleshooting Tools for VManage

### COURSE OBJECTIVES

- SDWAN Overview
- Cisco SDWAN Hardware
- Deploying the Overlay
- Configuring vManage
- Deploying using Templates
- Creating Policies
- Monitoring vManage

- vAnalytics
- Troubleshooting Tools for VManage

## COURSE OUTLINE

### 1. SDWAN Overview

- Describe what a Software-Defined Wide Area Network (SD-WAN) is
- Describe the secure extensible network
- Describe the function of the virtual IP fabric created in the SD-WAN solution
- What is SDWAN
- Cisco Cloud vs On-premises vs private cloud management
- Cisco IWAN vs Viptela SDWAN
- IWAN Migration to SDWAN
- SDWAN Integration with Cisco
- Cisco SDWAN Licensing
  - DNA Essentials
  - DNS Advantage
  - DNA Premier

### 2. Cisco SDWAN Edge Devices

- vEdge Appliances
  - vEdge 100
  - vEdge 1000
  - vEdge 2000
  - vEdge 2000
- vEdge Cloud
  - ESXI
  - KVM
  - AWS
  - Microsoft Azure
- Cisco IOS-XE Platforms
  - Cisco ISR 1100 Series Routers
  - Cisco ISR 4300 Series Routers
  - Cisco ISR 4400 Series Routers
  - Cisco ASR 10XX Routers
- Cisco CSR 1000V Router
- Cisco 54xx Enterprise Network Compute System (ENCS)

### 3. Cisco SDWAN Certificates and Whitelists

- On-Prem vs Cloud Certificate deployment
- Controller Certificates
- Hardware Device Certificates
- Software Device Certificates
- Certificates
  - Export Device Data in CSV Format
  - Check the vEdge Router Certificate Status
  - Validate a vEdge Router
  - Stage a vEdge Router
  - Invalidate a vEdge Router
  - Send the Controller Serial Numbers to vBond Orchestrator
  - Install Signed Certificate
  - View the CSR
  - View the Certificate
  - Generate the CSR
  - Reset the RSA Key Pair
  - Invalidate a Device
  - View Log of Certificate Activities
- Device Whitelists

### Controller Whitelists

### 4. Deploying Cisco SDWAN Controllers

- On-Prem vs Cloud deployment
- vManage NMS
  - Deploy the vManage NMS
  - Configure the vManage NMS
  - Configure the vManage NMS Cluster
  - Configure Multitenant vManage NMS
  - Configure Certificate Settings
  - Generate vManage NMS Certificate
- vBond Orchestrator
  - Deploy vBond VM Instance
  - Configure the vBond Orchestrator
  - Add the vBond Orchestrator to the Overlay Network
  - NAT Traversal
  - Start the Enterprise ZTP Server
- Deploy the vSmart Controller
  - Deploying vSmart Controller on ESXi
  - Deploying vSmart Controller on KVM
  - Configure the vSmart Controller
  - Add the vSmart Controller to the Overlay Network
- Controller High Availability
- Cluster Management
  - Change the IP Address of the Current vManage NMS
  - Add a vManage NMS
  - Configure the Statistics Database
  - View Statistics Data

### 5. Cisco SDWAN Fabric and Overview

- Virtual Fabric Overview
- Overlay Management Protocol
- Transport Locators (TLOCs)
  - TLOC Extension
  - TLOC Colors
- Multicast
- TCP Optimization
- Opening Firewall Ports
- Software Installation and Upgrade
  - Software Version Compatibility
  - Add New Software Images to the Repository
  - Software Upgrades Best Practices
  - Activate a New Software Image
  - Redundant Software Images
- vEdge Routers
  - Deploy vEdge Cloud router
  - Deploy a vEdge 100 VM on Azure
  - Deploy vEdge Cloud VM on ESXi
  - Deploy vEdge Cloud VM on KVM
  - Deploying vEdge 100 Routers
  - Deploying vEdge 1000 Routers
  - Deploying vEdge 2000 Routers
  - Device configuration using CLI
  - Install Signed Certificates on vEdge Cloud Routers
- Deploying vEdge Routers
  - Deploy ISR 1K
  - Deploy ISR 4K
  - Deploy ASR 1K

## COURSE OUTLINE

### 5. Cisco SD-WAN Security (continued)

- Migrating IOS-XE Devices to Cisco SD-WAN
- Zero Touch Provisioning
  - Using ZTP on Non-Wireless Routers
  - Using ZTP on Wireless Routers
- Deploy AWS Gateway using the AWS Wizard

### 6. Cisco SD-WAN Security

- Solution Security
- SDWAN IOS-XE Security
  - Application Firewall
  - IDS/IPS (Snort)
  - URL Filtering
  - Web Layer Security (Umbrella/Open DNS)
- SDWAN vEdge Security
  - Application Firewall
  - Web Layer Security (Umbrella/Open DNS)
- Firewall Ports
- Control Plane Security
  - DTLS
  - TLS
- Data Plane Security
  - IPSEC
  - GRE
- Traffic Segmentation
  - VPN
  - Policies
- Service Chaining
  - Firewalls
  - IDS
- Cloud Security
  - Umbrella
  - Z-Scaler
- Enterprise Firewall

### 7. Quality of Service

- Application Visibility and Recognition
- Differentiated Services - Quality of Service
- Critical Applications SLA
- Path MTU Discovery
- TCP Performance Optimization
- Bidirectional Forwarding Detection (BFD)
  - BFD Hello Timer and Multiplier
  - BFD Measurements
- vEdge Router Queuing
  - Marking
  - Remarking
  - Shaping
  - Policing

### 8. Configuring vManage

- Using the vManage Interface
- Using the vManage Dashboard
  - Device Pane
  - Reboot Pane
  - Certificates Pane

- Control Status Pane
- Site Health View Pane
- Transport Interface Distribution
- vEdge Inventory Pane
- vEdge Health Pane
- Transport Health Pane
- Top Applications Pane
- Application-Aware Routing Pane
- Web Server Certificate Expiration Date Notification
- Maintenance Window Alert Notification

#### Administration

##### Setting

- Configure Organization Name
- Configure vBond DNS Name or IP Address
- Configure Certificate Authorization Settings
- Configure vEdge Cloud Certificate Authorization Settings
- Generate Web Server Certificate
- View Web Server Certificate Expiration Date
- Enforce Software Version on vEdge Routers
- Create a Custom Banner
- Collect Device Statistics
- Enable CloudExpress Service
- Enable vAnalytics Platform
- Enable vManage Client Session Timeout
- Enable Data Stream Collection
- Set the Tenancy Mode
- Set Interval to Collect Device Statistics
- Configure a Maintenance Window

##### Manage Users

- Add a User
- Delete a User
- Edit User Details
- Change User Password
- Add a User Group
- Delete a User Group
- Edit User Group Privileges
- View vManage Service Details
- View Devices Connected to a vManage NMS
- Edit a vManage NMS
- Remove a vManage NMS from the Cluster
- View Available Cluster Services

##### Tenant Management

- Add a Tenant
- View All Tenants
- View a Single Tenant
- Edit a Tenant
- Remove a Tenant

#### Configuration

##### Devices

- Change Configuration Modes
- Upload vEdge Authorized Serial Number File
- Generate Bootstrap Configuration for a vEdge Cloud Router
- Export Device Data in CSV Format
- View a Device's Running Configuration
- View a Device's Configuration
- Delete a vEdge Router
- Copy a vEdge Router's Configuration
- Decommission a vEdge Cloud Router
- View Log of Template Activities

## COURSE OUTLINE

### 8. Configuring vManage (continued)

- Add a vBond Orchestrator
- Add a vSmart Controller
- Edit Controller Details
- Delete a Controller
- Change Variable Values for a Device

### 9. SD-WAN Templates

#### Templates

- Describe what vManage templates are used for
- List the parameter types that are used in vManage templates
- Explain the use of the Template Variable Spreadsheet
- Summarize the configuration elements of a device
- Create a Device Template
  - Create a Device Template from Feature Templates
  - Create a Device Template from the CLI
- Describe what the system feature template is used for
- Explain how to configure logging using the logging feature template
- Describe how OMP can be configured using the OMP feature template
- Describe the function of the Security feature template
- Explain how the BFD feature can be configured using the BFD feature template
- List the other feature templates that can be configured
- Edit a Template
- View a Template
- Delete a Template
- View Device Templates Attached to a Feature Template
- View Devices Attached to a Device Template
- Perform Parallel Template Operations
- Attach Devices to a Device Template
- Copy a Template
- Edit a CLI Device Template
- Export a Variables Spreadsheet in CSV Format for a Template
- Change the Device Rollback Time and View Configuration Differences
- Configuration Rollback
- Wide Area Application Server (WAAS)
  - WAAS Integration with SDWAN
  - Service Chaining with WAAS
  - Application Optimization
  - TCP Optimization
  - Data Redundancy Elimination (DRE)
  - LZ Compression
  - Akamai Connect
- Maintenance
  - Device Reboot
  - Software Upgrade
- Configure Cisco Umbrella
- Quality of Service (QoS)

### 10. SD-WAN Policies

- Local Policies vs Central Policies
- Policies
  - Policy Construction
    - Lists
    - Policy Definition
    - Policy Application
  - Configure Centralized Policy
  - Configure Localized Policy
  - View a Policy
  - Copy a Policy
  - Edit a Policy
  - Edit or Create a Policy Component
  - Delete a Policy
  - Activate a Policy on vSmart Controllers
- Smart policies (Control, Data, AppRoute, cflowd)
  - Control Policy
    - Service Chaining
    - Traffic Engineering
    - Extranet VPNs
    - Service path affinity
    - Arbitrary VPN Topologies
    - Fabric Policies
  - Application Aware Routing Policy
    - Application SLA
      - Latency
      - Loss
      - Jitter
    - Path Determination
  - Data Policy to manipulate different traffic types
    - Shaping Policies
    - QoS Policies
    - Service Chaining
    - Traffic Engineering
    - Extranet VPNs
    - Service path affinity
    - NAT Policies
  - cFlowd Policy
    - Cflowd-template for configuring flow cache behavior and flow export
    - Data-policy for selection of traffic subject to flow data collection
  - Multi-VPN and multi-topology policy
  - Hub Mesh Policies
    - Create a VPN Membership Policy
    - Create an Application SLA Policy
  - Local Control Policy
  - Local Data Policy
    - Access Control List
    - QoS Policy
    - Mirroring

## COURSE OUTLINE

### 11. SD-WAN Templates

#### OnRamp SAAS

- View Application Performance
- View Details about an Application
- Manage OnRamp Applications
- Manage OnRamp Client Sites
- Manage OnRamp Gateways
- Manage OnRamp DIA Sites

#### Cloud OnRamp IAAS

- Create a Cloud Instance
- Display Host VPCs
- Map Host VPCs to a Gateway VPC
- Unmap Host VPCs
- Display Gateway VPCs
- Add a Gateway VPC
- Delete a Gateway VPC

### 12. Monitoring vManage

#### Applications

- Display Bandwidth Utilization
- Display vQoE Values
- Display Deviations from Baseline Utilization

#### Network Availability

- Display Downtime by Site
- Display Downtime by Time

#### Network Health

- Display Latency, Loss, and Jitter on Circuits
- Display Application Performance by Carrier

#### vAnalytics Dashboard

- Network Availability Pane
- Applications Pane
  - Least Performing Applications
  - Applications Consuming Most Bandwidth
  - Anomalous Application Families

#### WAN Performance Pane

- Carrier Performance
- Tunnel Performance

### 13. Monitoring vManage

#### Network

- View List of Devices
- Export Device Data in CSV Format
- View Information about a Device
- View Device Status Summary
- View DPI Flows
- View Cflowd Flows
- View Interfaces
- View TCP Optimization Information
- View TLOC Loss, Latency, and Jitter Information
- View TLOC Loss, Latency, and Jitter Information
- View Tunnel Connections
- View Wi-Fi Configuration
  - View Client Details
  - View Client Usage
- View Control Connections
- View System Status

#### View Events

#### View ACL Logs

#### Troubleshoot a Device

- Check Device Connectivity
- Check Device Bringup
- Ping a Device
- Run a Traceroute
- View Control Connections in Real Time

#### Check Traffic Health

- View Tunnel Health
- Check Application-Aware Routing Traffic
- Simulate Flows
- Check Device Syslog Files

#### View Real-Time Data

#### ACL Log

- Set ACL Log Filters

#### Alarms

- Set Alarm Filters
- Export Alarm Data in CSV Format
- View Alarm Details
- Alarms Generated on vManage NMS

#### Audit Log

- Set Audit Log Filters
- Export Audit Log Data in CSV Format
- View Audit Log Details
- View Changes to a Configuration Template

#### Events

- Set Event Filters
- Export Event Data in CSV Format
- View Device Details

#### Geography

- Set Map Filters
- View Device Information
- View Link Information

#### Configure Geographic Coordinates for a Device

### 14. Troubleshooting Tools for vManage

#### Using vManage to Troubleshoot the environment

#### Operational Commands

- Admin Tech Command
- Interface Reset Command

#### Rediscover Network

- Rediscover the Network
- Synchronize Device Data

#### CLI Command to troubleshoot the environment.

#### SSH Terminal

- Establish an SSH Session to a Device

## DISCOVERY LABS

**1: Deploy the vManage NMS**

- Create vManage VM Instance on ESXi
- Configure Certificate Settings
- Create a vManage Cluster

**2: Deploy the vBond Orchestrator**

- Create vBond VM Instance on ESXi
- Configure the vBond Orchestrator
- Add the vBond Orchestrator to the Overlay Network
- Start the Enterprise ZTP Server

**3: Deploy the vSmart Controller**

- Create vSmart Controller VM Instance on ESXi
- Configure the vSmart Controller
- Add the vSmart Controller to the Overlay Network

**4: Deploy the vEdge Routers**

- Create vEdge Cloud VM Instance on ESXi
- Install Signed Certificates on vEdge Cloud Routers
- Send vEdge Serial Numbers to the Controller Devices
- Configure the vEdge Routers
- Prepare vEdge Routers for ZTP

**5: Creating Device Templates**

- Explore the Interface
- Add Controllers to the Whitelist
- Add vEdge whitelist
- bfd Tuning
- Create and Update Users
- Manage the Fabric

**6: Creating Device Templates**

- Create CLI Policy Template
- Create Feature Policy Template
  - System Feature Template
  - bfd Feature Template
  - OMP Feature Template
  - VPN Feature Template
  - MPLS-TLOC Feature Template
  - Internet-TLOC Feature Template
  - OSPF Feature Template
  - VPN 10 Hub and Spoke Feature Template
  - VPN 20 Full Mesh Feature Template
  - VPN 40 Guest Feature Template
- Create vSmart Device CLI Template
- Create DC1 vEdges Device Feature Template
- Attach DC1 Devices to Template
- Create DC2 IOS-XE CSRs Device Feature Template
- Attach DC2 Devices to Template
- Create BR1 vEdges Device CLI Template using TLOC Extensions
- Attach BR1 Devices to Template
- Create BR2 IOS-XE CSRs Device Feature Template using

## TLOC Extensions

- Attach BR2 Devices to Template
- Create BR3 IOS-XE ISR4K Device Feature Template
- Attach BR3 Devices to Template
- Create REG-HUB vEdges Cloud Device CLI Template using TLOC Extensions
- Attach REG-HUB Devices to Template
- Configuration Rollback

**7: Create Policies**

- List types of policies that can be implemented in the SD-WAN solution
- Describe how policies can be implemented that affect the control plane
- Describe what affect policies can have on data traffic forwarding
- Identify the various components of the vSmart policy architecture
- Describe how different policies are enabled in different devices
- Detail how policies are processed and applied
- Control Policy Lab
  - Configure a Vpn-membership-policy
  - Configure Site-list Selection Policies
  - Configure a Service Chaining Policy
  - Configure an Extranet VPN Policy
  - Configure a Service path affinity Policy
  - Configure Fabric Policies
  - Configure Security Zones
- Data Policy Lab
  - Configure Shaping Policies
  - Configure QoS Policies
  - Configure a Service Chaining
  - Configure a Extranet VPN Policy
  - Configure Service path affinity Policy
  - Configure a NAT Policies for DIA
  - Configure a OSPF BGP Routing Policy
- Application Aware Routing Policy Lab
  - SLA Classes
  - Path Selection using Application Policies
- Create a cFlowd Policy
- Create a Local Control Policy
  - Configure OSPF and BGP
- Create a Local Data Policy
  - Create Firewall Policy
  - Configure QOS

## DISCOVERY LABS

### 8: Application Visibility

Create a Centralized Policy for Application-Aware Routing

Identify Application Groups (FTP/Office 365/Voice)

Create Lists

- Site Lists

- Application Lists

- Data Prefix Lists

- VPN Lists

Create a SLA Classes

Create Traffic Rules

Apply Policies to Sites and VPNs

### 9: Monitoring the Solution

Explore vManage Dashboard analytics

Monitor Applications

Monitor Loss, Latency, and Jitter

Monitor Individual Device

- Check system Status

- Check Control Connections

- Check OMP Status

- Check BFD Status

- Check Interfaces for Issues

### 10: API Integration

Explore the API Docs

Use Poster to connect to vManage and download Templates

### 11: Troubleshooting

Use the CLI to view and troubleshooting debug Logs

Troubleshoot BFD

Troubleshoot OMP

Use troubleshooting tools to diagnose issues

- Use the Ping tool

- Use the Traceroute tool

- Use the App Route Visualization

- Simulate traffic flows

- Take a Packet

Troubleshoot Application Routing