

Cisco SD WAN Training (Viptela Training Course)

Training Available	Classroom & Online
Skill Level	Advanced
Study Material	Yes
Batches Available	Regular (Mon-Thu) & Weekend(Sat-Sun)
Enroll for a Free Demo	https://www.imatedita.com/register-for-demo/

[Need More Information? Click here to chat with our Team on Whatsapp](#)

1.0 SD-WAN Architecture

1.1 Describe Cisco SD-WAN architecture and components

1.1.a Orchestration plane (vBond, NAT)

1.1.b Management plane (vManage)

1.1.c Control plane (vSmart, OMP)

1.1.d Data plane (vEdge)

1.1.d (i) TLOC

1.1.d (ii) IPsec

1.1.d (iii) vRoute

1.1.d (iv) BFD

1.2 Describe WAN edge platform types, capabilities (vEdges, cEdges)

1.3 Describe Cisco SD-WAN Cloud OnRamp

1.3.a SaaS

1.3.b IaaS

1.3.c Colocation

2.0 SD-WAN Controller Deployment

2.1 Describe controller cloud deployment

2.2 Describe controller on-premises deployment

2.2.a Hosting platform (KVM/Hypervisor)

2.2.b Installing controllers

2.2.c Scalability and redundancy

2.3 Configure certificates and device lists

2.4 Troubleshoot control-plane connectivity between controllers

3.0 Router Deployment

3.1 Describe WAN edge deployment

3.1.a On-boarding

3.1.b Orchestration with zero-touch provisioning/plug-and-play

3.1.c Data Center and regional hub deployments

3.2 Configure and verify SD-WAN data plane

3.2.a Circuit termination/TLOC-extension

3.2.b Dynamic tunnels

3.2.c Underlay-overlay connectivity

3.3 Configure and verify OMP

3.4 Configure and verify TLOCs

3.5 Configure and verify CLI and vManage feature configuration templates

3.5.a VRRP

3.5.b OSPF

3.5.c BGP

3.5.d EIGRP

4.0 Policies

4.1 Configure and verify control policies

4.2 Configure and verify data policies

4.3 Configure and verify end-to-end segmentation

4.3.a VPN segmentation

4.3.b Topologies

4.4 Configure and verify SD-WAN application-aware routing

4.5 Configure and verify direct Internet access

5.0 Security and Quality of Service

5.1 Configure and verify service insertion

5.2 Describe Cisco SD-WAN security features

5.2.a Application-aware enterprise firewall

5.2.b IPS

5.2.c URL filtering

5.2.d AMP

5.2.e SSL and TLS proxy

5.3 Describe Cloud security integration

5.3.a DNS security

5.3.b Secure Internet Gateway (SIG)

5.4 Configure and verify QoS treatment on WAN edge routers

5.4.a Scheduling

5.4.b Queuing

5.4.c Shaping

5.4.d Policing

5.4.e Marking

5.4.f Per-tunnel and adaptive QoS

6.0 Management and Operations

6.1 Describe authentication, monitoring, and reporting from vManage

6.2 Configure authentication, monitoring, and reporting

6.3 Describe REST API monitoring

6.4 Describe software image management from vManage

LABS DURING THE TRAINING:

Our Lab sessions focus on practical aspects for Implementing & Troubleshooting SD-WAN operation of: -

Creating a SD-WAN Overlay and Underlay in the Network

Lab 1 - Interconnecting the SD-WAN components

Lab 2 - Installing the enterprise root CA server

Initializing the Controllers

Lab 3 - Performing initial configurations on **vManage** via CLI

Lab 4 - Exploring **vManage GUI** mode

Lab 5 - Performing initial configurations on **vBond** via CLI

Lab 6 - Registering and **installing certificate** for vBond in vManage

Lab 7 - Performing initial configurations on **vSmart** via CLI

Lab 8 - Registering and **installing certificate** for vSmart in vManage

Initializing the WAN Edges

Lab 9 - Performing initial configurations on **vEdge** via CLI

Lab 10 - **Registering** vEdges devices in vManage

Lab 11 - Performing initial configurations on **cEdge** via CLI

Lab 12 - **Registering** cEdges devices in vManage

Feature / Device Templates for vEdge and cEdge in vManage

Lab 13 - Configuring **System** template

Lab 14 - Configuring **Banner** template

Lab 15 - Configuring VPN 0 and VPN 512 templates

Lab 16 - Configuring VPN 0 interface and VPN 512 interface templates

Lab 17 - Configuring **AAA, BFD** and **OMP** templates

Lab 18 - Configuring device template from various feature templates

Routing for Transport Side VPN & Service Side VPNs

Lab 19 – Adding service-side VPNs in sites using CLI and template

Lab 20 - Configuring **static routing** using CLI

Lab 21 - Configuring **OSPF routing** using CLI

Lab 22 - Configuring **BGP routing** using CLI

Lab 23 - Configuring routing using templates in vManage GUI

Lab 24 - Attaching routing feature template in device template

Lab 25 – Verifying the reachability between sites using CLI and vManage

Lab 26 – Configure **TLOC extension** for site redundancy

Configuring Control Policies

Lab 27 – Configure an arbitrary **hub-n-spoke** topology for a VPN

Lab 28 – Create a control policy for **traffic engineering** using TLCOs

Lab 29 – Configuring a policy for firewall **service insertion**

Lab 30 – Perform **route-filtering** for sites using control policy

Lab 31 – Configuring **route-leaking** between VPNs for shared services

Configuring Data Policies

Lab 32 – Create a data policy to set *preferred transport* for certain traffic

Lab 33 – Implementing *application aware policies* for real-time traffic

Lab 34 – Configuring vEdges with *NAT* and *direct internet access*

Lab 35 – Configuring various *QoS concepts* using data policy

Configuring Security Policies

Lab 36 – Implementing *application-aware firewall* policy for traffic

Lab 37 – Creating an *IDS/IPS policy* for real time traffic analysis

Lab 38 – Implementing *URL Filtering* to block certain websites

Lab 39 – Verifying *AMP** for malware protection

Configuring Cloud-on-Ramp Feature

Lab 40 – Implementing *Cloud-on-Ramp for SaaS*

Lab 41 – Demonstrating *Cloud-on-Ramp for IaaS**

Verifying Day 2 Operations

Lab 42 – Using *vManage GUI* to explore various monitoring features

Lab 43 – Verifying *syslog* and *tcpdump* on vEdge devices

Lab 44 – Using *apidocs* to create a REST API call to query vManage

Lab 45 – Performing *software upgrade* for controllers and edge devices

Devices Used:

1 vManage, 1/2 vSmart, 1 vBond Controller

5 vEdges, 1 cEdge,

7 Cisco 7200 Router,

3 Cisco Catalyst Switch,

2 Cisco routers for Transport Connection – ISP and MPLS

1 Win-Host and 1 Root CA