



6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: <http://www.ctclc.com>



## Installing, Configuring, Monitoring and Troubleshooting Cisco (Viptela) SDWAN (ICSDWAN-CT)

In this 5-day hands-on up-to-date course on Cisco (Viptela) SD-WAN, students will learn how to administer SD-WAN. Students will learn about deploying and configuring SD-WAN Controllers, vEdge Devices, and Cisco IOS-XE Devices. Students will learn how to manage the vManage Interface, along with the change in the interface in 20.6 and above. Students will learn about Device Template, Feature Template, Configuration Groups and CLI Templates. Student will learn how to tune OMP, BFD, TLOCs, QoS, TCP OPT, DRE, FEC, Packet Duplication. Students will learn how SD-WAN implements Security using SASE, SIG, Umbrella, FW, IPS, AMP, Threat grid, TLS Decryption and Direct Internet Access (DIA). Students will learn about Local and Central Policies. 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, MegaPort, Equinix, and SAAS application such as O365 and Webex. Students will also learn how to Monitor and Troubleshoot the SDWAN Solution.

Use this course towards your Cisco Continuing (CE) Education Credits (40)

### Why Attend with Current Technologies CLC

- Our Instructors are 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

### Objectives

- SD-WAN Overview
- Cisco SD-WAN Hardware
- Deploying the Overlay
- Configuring vManage
- Deploying using Templates
- Creating Policies
- Monitoring vManage
- vAnalytics
- Troubleshooting Tools for VManage

### Outline

#### Course Duration

5 day

#### Course Price

\$4,795.00 or 46 CLCs

#### Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

## **Module 0: Introductions**

- Module Topics
  - General Administration
  - WebEX Basics
  - Introductions
  - Questions Asked by Companies about SD-WAN
  - What is SD-WAN?
  - SD-WAN Desired Benefits
  - How does Cisco define SD-WAN?
- Module Summary

## **Module 1: Cisco SD-WAN (Viptela) Platform Overview**

- Module Topics
- Lesson 1: Legacy WAN Architecture
  - Common WAN Topologies - Design and Deployment Considerations
  - WAN needs to Support Cloud Apps
  - Cisco's SD-WAN Functionality Comparison
- Lesson 2: Cisco SD-WAN / Digital Network Architecture Integration
  - Secure Cloud Scale SD-WAN Architecture
  - SD-WAN Security
  - SD-WAN Connectivity
  - SD-WAN Application Services
  - SD-WAN Operations
- Lesson 3: Software Defined Centralized Control
  - SD-WAN - Control Plane vs Data Plane
- Lesson 4: Cisco SD-WAN Solution Overview
  - Cisco SD-WAN Solution Roles and Responsibilities
- Lesson 5: New SD-WAN Terminology
  - Cisco SD-WAN Cloud-Delivered Architecture
  - Widely Deployed SD-WAN Capabilities
- Lesson 6: Cisco DNA SD-WAN Licensing
  - Choose Licensing Type and Level
  - Cisco DNA SD-WAN Licensing
  - Bandwidth Metering
  - Cisco DNA Bandwidth Upgrades
  - Cisco Smart Licensing
  - Cisco Smart Licensing Pooling
  - Managing Smart Licenses
  - What a Smart Account is and what it isn't
  - Smart Account Structure
  - SDWAN Smart Licensing phase 2 (offline reporting and compliance notification) for SDWAN
- Module Summary

## **Module 2: Deploying Cisco SD-WAN Controllers**

- Module Topics
- Lesson 1: Cisco SD-WAN Architecture

- Lesson 2: Cisco SD-WAN Controller Deployment Models
  - Controller Deployment Models
  - From Order to Zero-Touch Deployment
  - Controllers Deployment Methodology
  - Cisco SD-WAN Architecture – vManage
  - Cisco SD-WAN Architecture – vSmart
  - Cisco SD-WAN Architecture – vBond
  - Controller Communication Principles
  - Controller Deployment in AWS
  - Cloud Hosted Deployment – Public IP Access to VPN 512
  - Management Traffic for Cloud Deployed Controllers
  - Controllers Public Cloud Deployment
  - Cloud Hosted Deployment – Recommended
  - WAN Edge Control Plane Transport
  - Cloud-Hosted Deployment – Summary
  - On-Prem Deployment Considerations
  - On-Prem Controllers Deployment
  - On-Prem Deployment – vBond / NAT Traversal
  - On-Prem Controller Access
  - On-Prem Deployment
  - Controller Proxy Access
  - Controller Deployment – vManage
- Lesson 3: Cisco SD-WAN Self Service Portal
  - Cisco SD-WAN Self-Service Portal url
  - Configure Cisco SD-WAN Self-Service Portal Components
  - Configure an IdP for the Cisco SD-WAN Self-Service Portal
  - Configure Cisco SD-WAN Self-Service Portal Roles for IdP Users
  - Create a Cisco SD-WAN Cloud-Hosted Overlay Network (1)
- Lesson 4: On-Prem Controller Deployment
  - Controller Installation Overview
  - Controller Virtual Machines Files
- Lesson 5: Create vBond VM Instance on ESXi or KVM
  - Hypervisor Compatibility for vManage, vSmart, and vBond
  - Compatibility Matrix for Cisco SD-WAN Release 20.6.x
  - Compatibility Matrix for Cisco SD-WAN Release 20.4.x
  - SD-WAN Server Sizing
  - vManage Downloads on Cisco.com
  - vManage NMS Server Recommendations 20.6.x
  - Deploy vManage VM Instance on ESXi
  - Deploy vManage VM Instance (1)
  - Change vManage VM Settings - Add Additional Hard Disk
  - Start the vManage Instance and Connect To the vManage Console
  - vManage Console Login
  - vManage – Persona
  - vManage – Add Database Storage
  - Network Interfaces
- Lesson 6: Initial vManage Setup
  - Initial Settings Set at the CLI (1)
  - Configuring vManage Interface Settings
  - Configure General System Parameters – NTP

- Create a Minimal Configuration for vManage – System
- Create a Minimal Configuration for vManage – VPN 0
- Display the Running Configuration: System Section
- Verify the Ethernet Interfaces
- Time and NTP
- Login to vManage Interface
- View the Dashboard
- Lesson 7: Create vBond VM Instance on ESXi or KVM
  - vBond Downloads Availability
  - Controller Deployment – vBond
  - vBond Controller Server Recommendations
  - Deploy vBond VM Instance on ESXi
  - Deploy vBond VM Instance (1)
  - vBond Console Login
  - Create a Minimal Configuration for vBond – System
  - Create a Minimal Configuration for vBond – VPN 0
  - Display the Running Configuration: System Section
  - Verify the Ethernet Interfaces
  - Time and NTP
- Lesson 8: Create vSmart VM Instance on ESXi or KVM
  - vSmart Downloads Availability
  - vSmart Controller Server Recommendations
  - Deploy vSmart VM Instance on ESXi
  - Deploy vSmart VM Instance (1)
  - Create a Minimal Configuration for vSmart – System
  - Create a Minimal Configuration for vSmart – VPN 0
  - Display the Running Configuration: System Section
  - Verify the Ethernet Interfaces
  - Time and NTP
- Lesson 9: Add Controllers to vManage
  - Integrating Controllers into SD-WAN
  - Set Organization Name in vManage
  - Add the vBond Controllers to vManage
  - Add the vSmart Controllers to vManage
- Lesson 10: Enterprise CA Configuration
  - Generate Certificates for vBond
  - Request a Certificate
  - Download the Certificate
  - Install the Certificate
  - Certificate Installed on Controllers
- Lesson 11: vManage Multitenant Mode
  - Controller Tenancy – Single Tenant
  - vManage Multi-Tenancy in 20.4 / 17.4
  - Migrate Single-Tenant Cisco SD-WAN Overlay to Multitenant
  - Controller Tenancy - Pre 20.4 Software
  - Multi-Tenancy Options
  - RBAC by VPN
  - Multitenant vManage NMS
  - Place the vManage NMS into Multitenant Mode
  - Tenant Menu

- Add Tenant
- Lesson 12: Upgrade the SD-WAN Environment
  - SD-WAN Upgrade Images – Controllers
  - Cisco vManage Upgrade Paths
  - SD-WAN Upgrade Images – WAN Edges
  - Upgrade Images Merge into Unified for IOS XE in 17.2
  - Best Practices for Software Upgrades
  - Upload Software Images to the Repository
  - Upload Images to vManage
  - Upload Virtual Images for Security on IOS-XE (1)
- Lesson 13: Upgrade vManage
  - Software Upgrade Location and Platform Version
  - vManage OS Update Scheduled (1)
  - Activation of New vManage Images
  - Activation of New Images
  - vManage Activation Complete
  - vBond Upgrades
  - vSmart Upgrades
  - vSmart Activation
  - Upgrading Devices (1)
  - SDWAN Upgrades - Set Default Image
  - SDWAN Upgrade – Delete Old Images
- Lesson 14: Upgrade Devices via CLI
  - SDWAN Upgrade – CLI – Transfer Files
  - SDWAN CLI Upgrade – Install Image
  - SDWAN CLI Upgrade – Activate Image
  - SDWAN CLI Upgrade – Verify Image Activation
  - SDWAN CLI Upgrade – Set Default Image
  - SDWAN CLI Upgrade – Delete Old Image
  - SDWAN IOS-XE Upgrade – CLI
  - SDWAN CLI IOS-XE Upgrade – Install Image
  - SDWAN CLI IOS-XE Upgrade – Activate Image
  - SDWAN CLI IOS-XE Upgrade – Verify Image Activation
  - SDWAN IOS-XE CLI Upgrade – Set Default Image
  - SDWAN IOS-XE CLI Upgrade – Delete Old Image
- Lesson 15: Check Control Plane
  - Check Control Plane – vManage
  - Check Control Plane – vBond
  - Check Control Plane – vSmart
- Lesson 16: Controller High Availability and Scale
  - High Availability and Scale
  - Horizontal Solution Scale - Data Plane
  - Using Affinity to Manage Network Scaling
  - Redundancy – vSmart Control Controllers
  - Redundancy – vManage System
  - vManage Redundancy
  - Cluster Management Status
  - vManage CLI Status Command
  - Cisco vManage Cross-DC High Availability 19.2 and above

- Understanding the vManage Cluster Messaging Interface
- Module Summary

### **Module 3: Cisco SD-WAN Allow Lists and Certificates**

- Module Topics
- Lesson 1: Certificates
  - Public Key Infrastructure
  - Types of Certificates
  - Certificate Trust Chain
  - Certificate Authority Options
  - WAN Edge and Controllers Allow Lists
  - Certificate-Based Trust Allow Lists
  - Digitally Signed WAN Edge list – Manual Download
  - Digitally Signed WAN Edge list - Smart Account
  - Control Plane Allow-Listing
  - Controllers Identity
  - Establishing IOS-XE SD-WAN Edge Router Identity
  - Cisco IOS-XE Router Certificates
  - Serial Allow Listing SDWAN WAN Edge Routers
  - Certificate Revocation - 20.7 / 17.7 and Onward
  - Secure Control Channel - WAN Edge Routers
  - Secure Control Channel: WAN Edge
  - Zero Touch Provisioning - vEdge
- Lesson 2: Certificate Configuration
  - Organization Name and vBond Configuration
  - Controller Certificate Authorization - Cisco Automated
  - Controller Certificate Authorization - Symantec Automated
  - Controller Certificate Authorization - Symantec Manual
  - Controller Certificate Authorization- Enterprise Root CA
  - Configure Hardware WAN Edge Certificate Authorization Settings
  - Configure WAN Edge Cloud Certificate Authorization Settings
  - Generate Web Server Certificate – CSR
  - Import Web Server Certificate
  - View Web Server Certificate
  - Enterprise Feature Certificate Authorization
- Lesson 3: Monitoring and Troubleshooting Certificates
  - Monitor Certificates using Dashboard
  - Ensure WAN Edge Certificates are Valid
  - Check Certificate Properties in GUI
  - Check Certificate Properties in CLI
  - Troubleshooting – View Installed Certificate
  - Troubleshooting – View the Root CA Certificate
  - Check Certificate Expiration Date
- Module Summary

### **Module 4: Cisco SD-WAN Platforms**

- Module Topics
- Lesson 1: Platform Positioning
  - Cisco SD-WAN Routing Portfolio

- Picking a Device Platform
- What's in a Name?
- IOS Version Images
- Cisco vEdge Routers
  - vEdge 100
  - vEdge 1000
  - vEdge 2000
  - vEdge 5000
- Scalability Considerations Data Plane and IPsec
- vEdge Cloud Virtual Routers
  - Cisco ISR1100-4G
  - Cisco ISR1100-6G
- SDWAN Throughput across ISR1100 (Viptela OS)
- XE-SDWAN for ISR1100
- Cisco ASR 1000 Series Routers: Overview
- Cisco ASR1000 Series SD-WAN Routers
- Cisco IOS XE Software Architecture
- Cisco 4000 Series ISR SDWAN Portfolio
  - Cisco ISR 4461 WAN/SDWAN Router
  - Cisco ISR 4451
  - Cisco ISR 4431
  - Cisco ISR 4351
  - Cisco ISR 4331
  - Cisco ISR 4321
  - Cisco ISR 4221
- Introducing UADP on ISR4K SDWAN IOS XE 17.4
- UADP Switch Modules
- ISR 1100 Features
- ISR 1100 Portfolio
- Cisco IR1101 – Compact and flexible
- Lesson 2: Cellular Gateways for SDWAN
  - SD-WAN Connectivity Options
    - \*G is Supposed to be WAN Tech, Right?
    - How does 5G improve on 4G?
    - Cellular Gateway Platforms
    - Why Cellular Gateway is needed for High Quality Wireless WAN
    - Deployment Connectivity
    - Cellular Gateways
    - Cellular Gateway Connections
    - Use Case for SDWAN Wireless
  - Last Resort Circuit
  - Cisco Catalyst 8000 Edge Platforms Family
    - Catalyst 8000 Edge Routers
    - Catalyst 8500
    - Catalyst 8500 Third Generation QFP ASIC Innovation
    - Catalyst 8500 for SD-WAN
    - Catalyst 8500 Series Edge Platforms
  - C8500-12X4QC Port Connectivity
    - 100GE, 40GE Connectivity Options (1)
    - High Density 10GE, 1GE Connectivity Options

- Catalyst 8500L Series Edge Platforms
  - ASR1002-HX vs C8500-12X4QC
  - ASR1001-HX vs C8500-12X
  - ASR1001-X vs C8500L-8S4X
- Catalyst 8300
  - Cisco Catalyst 8300, 8200 Edge Platforms
  - Cisco Catalyst 8300 Series Edge Platforms
  - ISR 4451 vs C8300-2N2S-xxxx
  - ISR 4431 vs C8300-1N1S-xxxx
  - Catalyst 8300 Supported Modules
- Lesson 3: Catalyst 8200 Series
  - C8200-1N-4T
  - ISR 4331 vs C8200-1N-4T
  - Catalyst 8200 vs ISR4331 Throughput
- Lesson 4: Catalyst 8000v Series Virtual Router
  - Catalyst 8000V continues to build on CSR 1000V
    - Virtual Router Convergence
    - Cisco Catalyst 8000V Edge Software
  - ENCS NVF Platforms
    - ENCS 5400 Series
- Lesson 5: Adding IOS-XE to the Fabric
  - Zero Touch Provisioning – WAN Edge Appliance
  - ZTP – WAN Edge – Static IP Support
  - One Touch Provisioning
    - One Touch Provisioning using Mobile Application
    - One Touch Provisioning Phase-1 – 17.5
    - One Touch Provisioning Phase 2 – 17.6
  - Installing the Mobile App
  - SD-WAN 20.6 - Quick Connect Onboarding
    - Quick Connect Workflow
    - Quick Connect - Getting Started
    - Quick Connect - Pre-requisites
    - Quick Connect - Process Overview
    - Quick Connect - Progress Bar
    - Quick Connect - Sync Device Inventory
    - Quick Connect - Sync Device Inventory – From Smart Account
    - Quick Connect - Sync Device Inventory – Upload Device List
    - Quick Connect - Sync Device Inventory – Skip if Already Done
    - Quick Connect - Select Devices
    - Quick Connect - View Sync Device Inventory Task Details
    - Quick Connect - Return to Workflow
    - Quick Connect - Review Workflow – at any Stage
    - Quick Connect - Add and Review Device Configuration
    - Export, Edit, and Import the Config
    - Quick Connect – Summary
    - Quick Connect - Preview CLI
    - Quick Connect – Deploy
    - Quick Connect - PnP/ZTP



- Quick Connect - Manual On-boarding
- IOS-XE SDWAN
- Cisco SD-WAN Getting Started Guide
- Cisco Smart Accounts
- WAN Edge Provisioning
- Cisco Software Central PNP Portal - [software.cisco.com](https://software.cisco.com)
- Cisco Plug and Play Portal
- Plug and Play Connect – Add Controller Profiles
- Cisco IOS-XE Router Certificates
- Add Device to the Plug and Play Portal
- Add Device – Identify Sources
- Add Device – Identify Device (1)
- Lesson 6: Manually Provision SD-WAN IOS-XE
  - Manually Provision IOS-XE (1)
  - OS Package File
  - Single Image for IOS XE and IOS XE SD-WAN
  - Operational Mode Change
  - Greenfield, Brownfield Image Upgrade Scenarios
  - Install Requirements
  - Provisioning using Bootstrap Config File
- Lesson 7: 17.X IOS-XE PnP Provisioning
  - Single Image: Boot Up Sequence
- Lesson 8: Configuration > Devices
  - Generate Bootstrap for a WAN Edge Cloud Router
  - Generate Bootstrap Configuration for a vEdge Cloud Router
  - Running Device Configuration
  - View a Device's Local Configuration
  - Template Log
  - Delete a WAN Edge Router
  - Decommission a WAN Edge Cloud Router
  - View Status of Device Bring-up
- Lesson 9: High Availability and Redundancy Overview
  - Redundancy - Site with LAN Routing
  - Redundancy - Site with LAN Bridging
  - Redundancy – Hot Standby Router Protocol (HSRP) 20.7 onward
  - Transport Redundancy – Meshed
  - Redundancy – Meshed Transports
  - Redundancy – Extended Transports
  - Transport Redundancy – TLOC Extension
  - TLOC Extension Configuration
- Module Summary

## **Module 5: Cisco SD-WAN Fabric and OMP**

- Module Topics
- Lesson 1: Why Fabric Architectures?
  - Overlay Management Protocol (OMP) - Unified Control Plane

- Cisco SD-WAN Terminology – Transport / Service
- Cisco SD-WAN Terminology – OMP / Site-ID
- Cisco SD-WAN Terminology – System IP / Organization Name
- Cisco SD-WAN Terminology
- End-to-End Segmentation with Multi-Topology
- Fabric Operation Walk-Through
- Lesson 2: Overlay Management Protocol (OMP)
  - OMP Route Types and Prominent Attributes
  - OMP Routes - Routes learned from a site-local network
- Lesson 3: Transport Locators (TLOCs)
  - TLOC Route
  - TLOC Preference vs Weight
  - OMP Service Route Attributes
  - Significance of Interface (TLOC) Color
  - TLOC Colors
- Lesson 4: Overlay Routing
  - Multi-Domain Routing Fabric
- Lesson 5: OMP Service / Route Timer
  - Graceful Restart for OMP
  - Transport Independent Fabric
  - Unicast Overlay Routing Overview
  - Advertise Local Routes
  - OMP Route Redistribution
  - Administrative Distance
  - NAT Traversal
  - WAN Communication - Traffic Forwarding
- Lesson 6: Operational Commands
  - Operational Commands - vSmart Perspective
  - Operational Commands - WAN Edge Perspective
  - Operational Commands - show omp routes vpn 10 | tab
  - Operational Commands - show ip routes
  - Operational Commands
- Module Summary

## **Module 6: Cisco SD-WAN Security**

- Module Topics
- Lesson 1: Security Solutions
  - Secure SD-WAN is now Business Critical
  - Cisco's Three Cs for SASE
  - SASE Options
  - Cisco SD-WAN Security - Use Cases
  - Secure Edge
  - Secure Flows
  - SD-WAN SASE
- Lesson 2: Firewall Ports used in SDWAN
  - DDoS Protection for vEdge Routers
  - DDoS Protection for Controllers
  - Firewall Rules for Controllers

- Firewall Ports Used in Cisco SDWAN
- Firewalls Ports – DTLS
- Firewalls Ports – TLS
- Ports Used by Cisco SDWAN Devices Running Multiple vCPUs
- Administrative Ports Used by vManage NMS
- vManage Cluster Ports
- Anti-Replay Protection
- Lesson 3: SD-WAN Security and Segmentation
  - Current Challenges in Deploying Segmentation
  - WAN Edge VPNs and Security Zoning
  - VPN Labels
  - Secure Segmentation
  - Segmentation and Multi-Topology
  - Data Plane Privacy and Encryption
  - Data Plane Privacy (Pairwise)
  - Pairwise IPSec Keys for SA
  - Data Plane Integrity
  - Application Filtering
  - Application Filtering with Local Firewall
  - Layered Branch Security with SD-WAN
  - Service Based Traffic Engineering
  - Regional Secure Perimeter – Single Service
  - Regional Secure Perimeter – Multiple Services
  - L4-L7 Regional Secure Perimeter
  - Regional Internet Security
  - DIA Security
  - SD-WAN Integrated Security
  - SD-WAN Unified Security Policy (20.6)
  - Security Custom Options
  - Pre-Create Unified Security Features
  - Unified IPS Policy
  - New Unified Security Policy – Next Generation Firewall
  - NG Firewall Configuration
  - Create an Advanced Inspection Profile to be used with Rule / RuleSets
  - New Unified Firewall Rule with Advanced Inspections Profile
  - Enterprise Firewall
  - How FQDN Works?
  - Use Case: Intra-Zone Policy
  - Use Case: Self-Zone Policy
  - ZBFW: DIA/DCA Security
  - High Speed Logging (HSL)
  - Cloud Delivered Firewall
  - Intrusion Prevention
  - Snort IPS/IDS & Web Filtering Architecture
  - URL Filtering
  - URL-Filtering (URL-F) Database Profiles
  - How often URL-Filtering Database gets Updated?
  - DNS/Web-layer Security
  - DNS/Web-layer Security - Solution Overview
  - Cisco Cloud Security
  - Cloud Security with Zscaler

- Increased Throughput Capabilities per Router
- Layer7 Health Check
- Advanced Malware Protection
- TLS/SSL Decryption (MiTM Proxy)
- Lesson 4: SD-WAN Security Configuration
  - WAN Edge VPNs and Security Zoning
  - Security Configuration
  - Legacy Security Policy
  - SD-WAN Security Workflow
  - Add Firewall Policy
  - Add Rule to Firewall Policy
  - Add Rule to Deny and Log Traffic
  - Review Inspect and Deny Rules
  - Create Firewall Zones
  - Create Source Firewall Zone
  - Create Destination Firewall Zone
  - Create Firewall Zone Pair
  - Firewall Policy
  - Intrusion Prevention Policy
  - Intrusion Prevention Policy – Add Target VPNs
  - Intrusion Prevention Policy – Configuration
  - Intrusion Prevention Policy – Advanced Configuration
  - Intrusion Prevention Policy – Save IPS Configuration
  - Intrusion Prevention Policy
  - Add URL Filtering Policy
  - URL Filtering Policy – Add Target VPNs
  - URL Filtering Policy - Basic Configuration
  - URL Filtering Policy – Advanced Configuration
  - URL Filtering Policy – Save Configuration
  - URL Filtering Policy
  - Advanced Malware Protection
  - Advanced Malware Protection - Add Target VPNs
  - Advanced Malware Protection – Basic Configuration
  - Advanced Malware Protection – File Analysis Configuration
  - Advanced Malware Protection – Save Configuration
  - Advanced Malware Protection
  - DNS Security Policy
  - Umbrella API Key
  - DNS Security Policy – Add Target VPN
  - DNS Security Policy Basic Configuration
  - DNS Security Policy – Save Configuration
  - DNS Security Policy
  - TLS/SSL Decryption
  - TLS/SSL Decryption Policy Configuration
  - Configure Trusted CA
  - TLS/SSL Decryption Policy Configuration
  - TLS/SSL Decryption Policy Decryption Rule
  - Security Policy - Configuration
  - Security Policy - Preview
  - Edit Template and Apply Security Policy
  - Security Policy – Apply Security Policy to Template

- Module Summary

## **Module 7: SD-WAN QoS**

- Module Topics
- Lesson 1: Application Visibility and Recognition (NBAR / QoS)
  - What is AppQoE?
  - SD-AVC Service
  - NBAR Agents
  - Multidimensional Application Quality of Experience
  - Application Visibility and Recognition
  - vEdge Router QoS
  - Device QoS: Queuing
  - WAN Edge Router Traffic Prioritization
  - Device QoS: Shaping
  - Device QoS: Policing
  - Policing with Packet Loss Priority
  - DSCP and COS (802.1p) Re-marking
  - Cisco SD-WAN QoS Features
  - Per-Tunnel QoS support on SD-WAN
  - Adaptive QoS on IOS-XE SD-WAN
  - IOS-XE 17.3 - Adaptive QoS
  - Per-VPN QoS Working
  - Monitor Per-Tunnel QoS
- Lesson 2: Bidirectional Forwarding Detection (BFD)
  - Bidirectional Forwarding Detection (BFD)
  - Critical Applications SLA
  - BFD Calculation App-Route Policies
  - Per-Class BFD Probing for AAR
  - Application Aware Timers - Policy Example
  - Troubleshooting BFD Session Issues
- Lesson 3: Forward Error Correction (FEC) / Packet Duplication
  - Forward Error Correction (FEC)
  - FEC and Multiple Circuits
  - Forward Error Correction (FEC) Modes & Configuration
  - Packet Duplication
  - Packet Duplication and Application Aware Routing
- Lesson 4: TCP Optimization
  - TCP Optimization Platforms
  - DRE Optimization (cEdge)
  - DRE Optimization Enhancements
  - TCP Optimization Design Considerations
  - Multiple Service Nodes for AppQoE
  - TCP Optimization on IOS-XE
  - Path MTU Discovery
  - Optimal MTU with Host PMTUD
  - Optimal MTU with TCP MSS Adjust
  - Differentiated Services - Quality of Service
  - Localized Data Policy (QoS) Configuration
  - Forwarding and QoS Example

- Module Summary

## **Module 8: Configuring vManage**

- Module Topics
- Lesson 1: vManage Dashboard
  - Cisco SDWAN Management
  - Cisco vManage Communication with External Servers via Proxy
  - vManage GUI Menu – Icon vs Expanded
  - vManage GUI Menu – 20.7 and Onward
  - vManage Main Monitor Overview
  - vManage VPN Dashboard
  - vManage Security Dashboard
  - Main Dashboard - Device Pane
  - Reboot Pane
  - Certificates Pane
  - Control Status Pane
  - Site Health View Pane
  - Transport Interface Distribution
  - WAN Edge Inventory Pane
  - WAN Edge Health Pane
  - Transport Health Pane
  - Top Applications
  - Application-Aware Routing Pane
  - Cloud Services – SAAS
  - Cloud Services – Cloud onRamp for IAAS
- Lesson 2: Monitoring
  - Monitor > Geography
  - Monitor > Network (Device)
  - Monitor > Network (Device) DC1-vEdge1 – Applications
  - Monitor > Network (Device) DC1-vEdge1 – Interfaces
  - Monitor > Network (Device) DC1-vEdge1 – WAN > TLOC
  - Monitor > Network (Device) DC1-vEdge1 – WAN > Tunnel
  - Monitor > Network (Device) DC1-vEdge1 – Control Connections
  - Monitor > Network (Device) DC1-vEdge1 – System Status
  - Monitor > Network (Device) DC1-vEdge1 – Events
  - Monitor > Network (Device) DC1-WAN Edge1 – ACL Logs
  - Monitor > Network (Device) DC1-vEdge1 - Troubleshooting
  - Monitor > Network (Device) – Real Time (Show Commands)
  - Monitor > Alarms
  - Monitor > Events
  - Monitor > Audit Log
  - Monitor > ACL Log
- Lesson 3: Tools
  - Tools > SSH Terminal
  - Tools > Rediscover Network
  - Tools > Operation Commands

- Lesson 4: Settings
  - vManage > Administration > Settings
  - Enable Email Notifications
  - Enforce Software Version on WAN Edge Routers
  - Create a Custom Banner
  - Settings > Enable Reverse Proxy
  - Settings > HTTP/HTTPS Proxy Server
  - Settings > Statistics Settings
  - Settings > Cloud Onramp for SaaS
  - Settings > Cloud Services / vAnalytics Platform
  - Settings > vManage Client Session Timeout
  - Settings > vManage Session / Server Session Timeouts
  - Settings > Enable Data Stream Collection
  - Settings > Tenancy Mode
  - Settings > Set Interval to Collect Device Statistic
  - Settings > vManage Maintenance Window
  - Settings > Single Sign-On – Identity Provider Settings
  - Settings > vManage Statistics Database
  - Settings > Google Map API Key
  - Settings > Software Installation Timeout
  - Settings > IPS Signature Update
  - Settings > Smart Account Credentials
- Lesson 5: Resource Groups / Users / Groups
  - Resource Groups / Users / Groups
  - Configuring AAA User Accounts
  - Resource Groups
  - Creating Users in CLI
  - Creating Users via vManage
  - User Account Management
  - Creating Groups
  - Basic Group Privilege
  - Operator Group Privilege
  - Netadmin Group Privilege
  - Add Group and Permissions
  - Which Policies have Granular RBAC (R/W)?
  - Creating User Groups with Policy RBAC – GUI
  - Create Users and Assign to User Groups
  - Edit Group Permissions or Delete Group
  - Configuring RADIUS
  - Configuring RADIUS Authentication
  - Configuring TACACS+ Authentication
  - Configuring the Authentication Order
  - Configuring NAS Attributes
  - Show Users Command
  - show AAA Usergroup Commands
  - Administration > VPN Groups > Add VPN Group
  - Administration > VPN Segments
  - License Management
  - License Management – Smart Account Management
  - License Management – Smart Account Management Reporting

- Network Wide Path Insight
- Module Summary

## **Module 9: Creating and Applying SD-WAN Templates**

- Module Topics
- Lesson 1: Templates
  - Build your Configuration with Templates
  - Device Templates
- Lesson 2: Feature Templates
  - Centralized Device Configuration via Templates
  - Template Editor
  - Template Options
  - Create Template
  - Centralized Device Configuration via Templates
- Lesson 3: Device Templates
  - Create a Device Template from the CLI
  - Template Parameters
  - Build a Feature Template
  - Feature Templates
  - Create Feature Templates for the Device
- Lesson 4: System Feature Templates
  - Edit Feature Templates
  - System Feature Template
  - Device Template
  - Create VPN 0 Feature Template (1)
  - Create VPN Interface Feature Template (1)
  - Device Template Management VPN 0 and VPN 512 Configuration
  - Logging Feature Template (1)
  - OMP Feature Template (1)
  - Additional Feature Templates
- Lesson 5: Apply Template to a Device
  - Attach Devices to Template (1)
  - Schedule Configuration
  - Configuration Rollback
  - Create a CLI Template
- Module Summary

## **Module 10: Creating and Applying Policies**

- Module Topics
- Lesson 1: Policy Concepts
  - SD-WAN Policy and Intent Based Networking
  - Cisco SD-WAN Policy Architecture
  - Policy Configuration Overview
  - Policy Framework - Centralized and Localized Policies
  - Cisco SD-WAN Policy Execution
  - Custom Policies
- Lesson 2: Centralized Policies (Control, Data, AppRoute, cFlowd)
  - vManage GUI Centralized Policy Wizard



- Centralized Policies
- vSmart Overlay Policy Architecture
- Centralized Policy Driven WAN Infrastructure
- Building Blocks of Centralized Policies
- Construction of SD-WAN Policies
- Centralized Policy Construction
- vSmart Policy Construction – Lists
- vSmart Policy Construction – Policies
- vSmart Policy Construction – Policy Application
- vSmart Policy Example
- Cisco SD-WAN Centralized Policy Architecture
- Where Centralized Policies are Attached
- Centralized Control Policy: Inbound vs. Outbound Route Policy
- vSmart Policy Processing
- Lesson 3: Centralized Control Policies-Multi-Domain Data Plane Case Studies
  - Control Policy Case Study
- Lesson 4: Centralized Control Policy Components
  - Centralized Control Policies
  - Centralized Control Policy
  - Centralized CLI Policy
  - vManage Configuration Procedure
  - OMP Route Match Attributes
  - TLOC Route Match Attributes
- Lesson 5: Traffic Engineering
  - Centralized Control Policy Configuration - Traffic Engineering
  - Traffic Engineering Examples
  - Traffic Engineering Example (3) – Multiple West Sites
  - Creating Arbitrary Topologies
  - Control Policy Examples - Service Chaining
  - Control Policy Service Chaining – Site 4 Service Originator
  - Control Policy Service Chaining – vSmart Policy 1
- Lesson 6: SD-WAN Policy Framework – Use Cases
  - Control Policy Case #1
  - Control Policy Example – Data Center Priority
  - Control Policy Case #2
  - Control Policy Example – Arbitrary VPN Topologies
  - Control Policy Case #3
  - Control Policy Case #4
  - Control Policy Case #5
- Lesson 7: Centralized Policy Framework - App-Route Policies
  - App-Aware Routing Policies
  - Deep Packet Inspection for Identifying Traffic
  - Enable Deep Packet Inspection via Local Policy
  - Application-Aware Routing Policy
  - Application Aware Routing
  - Application Aware Routing Policy Example
  - Application-Aware Routing Policy Configuration
  - App-Route Policies

- Lesson 8: Centralized Data Polices
  - Configuring Centralized Data Policy
  - Data Policy - Applications and Services
  - Data Policy Application
  - Centralized Data Policy Configuration
  - Data Policy NAT
  - Data Policy NAT – vSmart Policy
  - Data Policy Case #1
  - Data Policy Case #2
  - Centralized Data Policy Configuration Procedure
  - Centralized Data Policy Configuration
- Lesson 9: Centralized Data Policies –VPN Membership Policy
  - VPN Membership Policy
  - VPN Membership Policy Examples
- Lesson 10: Centralized Data Polices – cFlowd Policy
  - cFlowd Policy Example
  - cFlowd Flow Data Collection
  - Enable Netflow
  - cFlowd Example
- Lesson 11: Policy Framework – Internet Breakout / DIA
  - Internet Breakout / DIA
  - Internet Breakout Leverage
  - SD-WAN Internet Breakout Options
- Lesson 12: SD-WAN Local Policies
  - Localized Policies
  - Local Control Policy
  - Local CLI Policy
  - Local Control Policy Example
  - WAN Edge Routing Policy Architecture
  - Localized Control Policy Configuration (1)
  - Policy Management
- Module Summary

## **Module 11: SD-WAN Cloud Adoption**

- Module Topics
- Lesson 1: Cloud Services Adoption
- Lesson 2: Cloud OnRamp – SaaS
  - Microsoft 365 Optimization with Cisco SD-WAN
  - Cloud OnRamp for SaaS Workflow - Site Types
  - Optimize SaaS with Cloud-express Single DIA
  - Cloud onRamp for SaaS – Dual DIA
  - Cloud onRamp for SaaS (Dual ISP)
  - SaaS Cloud OnRamp – DIA and Gateways
  - Cloud onRamp for SaaS (Gateway)
  - Performance Measurement
  - vQoE – Cisco SDWAN Quality of Experience Score
  - Cloud OnRamp for SaaS via SIG

- Direct Internet Access
- DNS settings on VPN0
- NAT Settings on VPN0 Interface
- Enable Cloud On-Ramp
- Cloud On-Ramp for SaaS WorkFlow - Adding Applications
- Cloud On-Ramp for SaaS WorkFlow - Adding DIA Sites
- Cloud OnRamp for SaaS WorkFlow - Adding Client Sites
- Cloud On-Ramp for SaaS WorkFlow - Adding Gateway Sites
- Cloud On-Ramp Dashboard
- Cloud On-Ramp for SaaS QoE - Application Drill Down (1)
- Monitor > Network > Realtime > CloudExpress Applications
- Troubleshooting Cloud On-Ramp on Gateway Exit
- Troubleshooting OMP metrics
- Troubleshooting Cloud Express on Local Exit
- Lesson 3: Cloud-Onramp for IAAS / Multicloud
  - SD-WAN Landscape (Mixture of Traditional Networking and Cloud)
  - SD-WAN Evolution
  - Network Evolution at Hyper-Speed
  - SD-WAN Cloud Paths
  - SD-WAN Cloud Networking Integrations
  - Cloud OnRamp for Multicloud
  - Cisco Cloud OnRamp with AWS Transit Gateway Connect
  - Cisco SD-WAN integration with Microsoft vWAN
  - Cisco SD-WAN Cloud Hub with Google Cloud
  - SD-WAN Cloud Interconnect with Megaport and Equinix
  - Cisco SD-WAN Cloud OnRamp for Colocation
  - Cloud onRamp for Colocation and Cloud Interconnect
  - Cisco SD-WAN Cloud OnRamp Facilitates Your Multicloud Journey
  - Cisco SD-WAN Cloud Interconnect
  - Cloud Interconnect?
  - Multicloud: SD-WAN Beyond the Branch
  - SD-WAN Cloud Implementation - Site-to-Cloud
  - SD-WAN Cloud Implementation - Site-to-Site
  - Cloud Connectivity Quick Reference
  - Multi-Cloud Connectivity - Cloud On-Ramp IaaS
  - Public Cloud Connectivity Options
  - Cloud onRamp
  - Cloud onRamp for IaaS - How it works
  - IaaS and SDWAN - Multi-Cloud Deployment
  - Cloud On-Ramp for IaaS – Attached Compute
  - Cloud On-Ramp for IaaS – Gateway VPC/VNET - Fully Automated via vManage
  - Cloud on-Ramp for IaaS: Automated Azure
  - Cloud Deployment
  - Cloud Deployment – Device Template
  - Cloud On-Ramp for Multi-Cloud Dashboard
  - Associate Cloud Account
  - Cloud Global Settings
  - Host Private Networks
  - Host Private Networks / TAG
  - Create Cloud Gateway
  - Attach Host VNets

- Map VNET to VPN
- Cloud On-Ramp for IaaS Dashboard – WorkFlow
- Cloud On-Ramp for IaaS – Dashboard
- Cloud On-Ramp IaaS – Monitoring
- Module Summary

## **Module 12: vAnalytics Overview**

- Module Topics
- Lesson 1: vAnalytics Overview
  - vAnalytics Release 2.0: Better Visibility and Control
  - vManage Scalability Considerations
  - When to Consider a 3rd Party Collector
  - vManage vs vAnalytics
  - Why use vAnalytics?
  - vAnalytics Data Flow
  - Metadata Collected by vAnalytics (XML)
  - Customer Onboarding
  - Enable vAnalytics Process
  - Enable vAnalytics in vManage
  - vAnalytics – Customer Data
  - vAnalytics Menus Structure
  - vAnalytics Menu Toolbar Icons
  - vAnalytics Time Range Reporting Increments
  - vAnalytics Metrics
- Lesson 2: vAnalytics Dashboard
  - vAnalytics Summary Dashboard (1)
  - vAnalytics Application Dashboard (1)
  - vAnalytics Popular Application Dashboard (1)
- Lesson 3: vAnalytics Applications
  - Application / Flow Centric
  - Application - Performance and Usage (1)
  - Application Family - Performance and Usage (1)
  - Application Class - Performance and Usage (1)
  - Application Usage and Performance Across Network – Tunnel (1)
  - Application Usage and Performance Across Network - TLOC (1)
  - Application Usage / Performance across Network - Transport Path (1)
  - Application Usage / Performance across Network - Transport Color (1)
- Lesson 4: vAnalytics Network Availability
  - Network Centric Awareness
  - Network - Site Performance and Usage – Site (1)
  - Network - Site Performance and Usage - Edge Device (1)
  - Network - Site Performance and Usage – Carrier (1)
  - Network - Device Inventory (1)
  - Network - TLOC (Circuits) - Performance and Usage
  - Network - Transport Path - Performance and Usage
  - Network - Transport Local Color - Performance and Usage
  - Network - Tunnels - Performance and Usage

- Lesson 5: vAnalytics Flows
- Flows - Network Flow - Top Flows (Source & Destination)
- Flows - Network Flow - Top Talkers (1)
- Flows - Network Flow - Top Destinations (1)
- Module Summary

## **Module 13: Monitoring & Troubleshooting the SD-WAN Solution**

- Module Topics
- Lesson 1: SD-WAN Support Options
  - Contacting Cisco TAC Support
  - Contact Cisco TAC Severities
  - Cisco TAC Case Tracking
- Lesson 2: Monitoring
  - SD-WAN Monitoring Tools
  - Application Visibility with External Collectors
  - Application Visibility + ART with External Collectors
  - Network Wide Path Insight (NWPI)
- Lesson 3: ThousandEyes
  - Extended visibility with Cisco SD-WAN + ThousandEyes
  - SD-WAN + ThousandEyes Supported Platforms
  - Deployment Options
  - ThousandEyes Probing
- Lesson 4: Compliment with LiveAction
  - LiveAction – End-to-End visibility of app and network
- Lesson 5: SNMP
  - SNMP MIBs Supported on WAN Edges
  - CISCO-SDWAN-OPER-SYSTEM-MIB – Supported Attributes
  - CISCO-SDWAN-APP-ROUTE-MIB – Supported Attributes
  - CISCO-SDWAN-BFD-MIB – Supported Attributes
  - CISCO-SDWAN-POLICY-MIB – Supported Attributes (part 1)
  - CISCO-SDWAN-SECURITY-MIB – supported attributes
- Lesson 6: Controller Failures
  - Recovering from a Failure in the Control Plane
  - Recovering from a vSmart Controller Failure
  - Recovering from a vBond Orchestrator Failure
- Lesson 7: Troubleshooting Controllers
  - Troubleshooting vManage Slowness
  - Template Push failure
  - Template Push failure (Logs)
  - vManage Logs
  - Collecting Admin-Tech
  - Enable Debugs
- Lesson 8: Troubleshooting Devices When They Don't Join the Fabric
  - View Status of Device Bring-up
  - WAN Edge Requirements for Establishing Control Connections
  - WAN Edge Cannot Join the SD-WAN Overlay (Fabric)
  - Control Connections Failing
  - DTLS Connection Failure
  - TLOC Disabled

- Transient Conditions
- Serial Number(s) NOT Present
- Certificate Revoked/Invalidated
- Certificate Installation Failed
- Organization-name Mismatch
- DTLS Connection Debug
- Lesson 9: Device Configuration and Upgrades Failure
  - Self-Healing - Software Upgrade and Configuration Changes
  - Device Rejects a Template
- Lesson 10: Troubleshooting cEdge
  - Troubleshooting Data Plane on cEdge - BFD
  - Troubleshooting Data Plane on cEdge - EPC
  - Troubleshooting Data Plane on cEdge - Packet-Tracer
  - Troubleshooting Data Plane on cEdge
  - cEdge Password Discovery
  - Factory Default a cEdge
- Lesson 11: Troubleshooting using vManage
  - Check Controller Status
  - Checking Control Connections
  - WAN Edge Health
  - Reboot / Reload Services / Reset Services on Controllers / Devices
  - Reset an Interface
  - Admin Tech
  - Reset Locked Out User on a Device
  - System Alarm
  - System Events
  - System Audit Log
- Lesson 12: Device Troubleshooting
  - Troubleshoot Configuration – Change to CLI Mode
  - Monitor > Network (Device) – {device} - System Status
  - Monitor > Network (Device) – {device} - System Status – Crash
  - Checking Interface Utilization
  - Checking Transport Quality
  - Monitor > Network (Device) – {device} – Control Connections
  - Monitor > Network (Device) – {device} – Events
  - Monitor > Network (Device) – {device} – Troubleshooting
  - Troubleshooting > Ping
  - Troubleshooting > Traceroute
  - Troubleshooting > Speed Test
  - Troubleshooting > Tunnel Health
  - Troubleshooting > Visualizing Application Paths
  - Troubleshooting > Packet Capture
  - Troubleshooting > Simulate Flows
  - Troubleshooting > Debug Logs
- Lesson 13: Using the GUI for cli show command Under Troubleshooting > Real-time
  - Monitor > Network – {Device} - Real Time (Show Commands)
  - Checking BFD connections
  - Troubleshooting Routing
  - Checking OMP Peers Detail
- Lesson 14: CLI Troubleshooting

- vManage CLI Troubleshooting
- Time Issues
- Check vBond Control Connection
- show orchestrator valid-vEdges
- show orchestrator valid-vSmart
- show orchestrator valid-vManage
- CLI Troubleshooting Commands - show control connections
- CLI Troubleshooting Commands - show control connections-history
- clear orchestrator connections-history
- Log Troubleshooting
- vBond Look for Specific System IP in Logs
- vManage Log
- vManage Rest API Log
- Display the Last 10 Log Messages
- View the Root CA Certificate on vBond
- View the Server Certificate on vBond
- Using tcpdump to Capture Headers
- show configuration rollback
- Validate Command
- Lesson 15: vManage, APIs & Programmability
  - vManage REST APIs
  - REST Web Service
  - Requests and Response REST API Flow
  - Available API Calls
  - Viptela API Library and Documentation
  - REST API
  - URI Structure
  - Options for Working with REST APIs
  - REST API
  - Webhooks
  - Tools – Use the best tool you can afford
- Module Summary

## **LAB OUTLINE**

### **Lab 1: Deploy the SD-WAN Controller**

- Deploy the vManage Controllers
- Deploy the vBond Orchestrator
- Deploy the vSmart Controller
- Configure Certificate Settings

### **Lab 2: Deploy the vEdge, ISR 4K /C8000V Routers**

- Deploy WAN Edges
- Configure the WAN Edge Routers
- Prepare vEdge Routers for ZTP

### **Lab 3: vManage Configuration**

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

### **Lab 4-8: Creating Device Templates**

- Create CLI Policy Template
- Create Feature Policy 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
- Configuration Rollback

### **Lab 9: Use APIs to Import Feature Templates**

### **Lab 10: Upgrade SDWAN Environment**

### **Lab 11-13: Perform ZTP on SDWAN Environment**

### **Lab 14-17: SDWAN 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 an Extranet VPN Policy
- Configure Service path affinity Policy
- Configure a NAT Policies for DIA
- Configure an 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 ACL
  - Create Device Access Policy
  - Configure QOS
  - Configure OSPF Route Policy

### **Lab 18: 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

### **Lab 19: Cloud On-RAMP**

- Configure Cloud Onramp for SAAS

### **Lab 20: Monitoring / Troubleshooting**

- 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
- 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