

COURSE OVERVIEW:

ACI for Service Providers (SPACI) is a 5-day Cisco ACI training course that provides ACI use cases for Service Provider environments including policy-driven configurations and design details, multi-tenant internal and external network integration and migration, routing protocol exploration, security implications, and disaster recovery solutions. Students in the ACI training course will perform various scenario-driven configurations and testing in lab exercises using hand-on labs. The Cisco online training course entails students learning how to simplify complex routing deployments and reduce the time and cost required to provision customer networking needs while maintaining both ACI and non-ACI networks. Students will learn to support site redundancy including disaster recovery solutions both at the customer site and public cloud provider levels while maintaining the integrity of customer data and hardening of sensitive information. This is an ideal Cisco online training course to build your skill set and prepare for Cisco ACI certification. Get the skills employers need in today's Information Technology environment and sign up for this Cisco ACI training course today.

WHO SHOULD ATTEND:

- Service providers deploying Cisco ACI

PREREQUISITES:

- Familiarity with Cisco UCS and ACI

COURSE OBJECTIVES:

Upon completing this course, the learner will be able to:

- Deploy Multi-tenant Configurations
- Configure ACI for Advanced OSPF
- Configure ACI for BGP internal environments
- Configure BGP for External reachability
- Configure ACI for Disaster Recovery
- Understand Service Graph Insertion
- Design Service Graphs



- Deploy ACI Securely

COURSE OUTLINE:

Module 1: ACI Fundamentals

- Review ACI concepts and principles
- Policy and the ACI policy model in particular
- Differentiate between the policy and the network
- Define application logic through policy
- Provider and consumer relationships
- Understand how to automate infrastructure through policy
- Review policy instantiation
- Spine/leaf single-site topology
- ACI management networks
- Extended VXLAN
- Unicast forwarding
- Multicast forwarding
- Distributed Layer 3 gateway
- ACI as a gateway
- Flowlet dynamic load-balancing

Module 2: Endpoint Groups (EPG) Usage and Design

- Current Network Definition of Applications
- ACI Endpoint Groups
- Mapping traditional network constructs to the ACI fabric
 - EPG as VLAN
 - EPG as a subnet (model classic networking using EPGs)
 - EPG as virtual extensible LAN (VXLAN)/Network Virtualization using Generic Routing Encapsulation (NVGRE) virtual network identifier (VNID)
 - EPG as a VMware port group
- Utilizing the ACI fabric for stateless network abstraction
 - EPG as an application component group (web, app, database, etc.)
 - EPG as a development phase (development, test, production)
 - EPG as a zone (internal, DMZ, shared services, etc.)

Module 3: ACI Layer 3 Connection to an Outside Network

- Border Leaves
- Route Distribution within the ACI Fabric
- OSPF Routing Protocol Peering between ACI and the External Router
 - OSPF Area Type
 - Supported Interface Type
 - OSPF Protocol Parameters Tuning
 - OSPF High-Availability Design
 - Tag Tenant Routes Using OSPF Route Policy
 - Layer 3 Outside Connection with OSPF Example
- IBGP Routing Protocol Peering between the ACI and External Router
 - BGP AS Number
 - BGP Route Policy
 - BGP Peering Consideration
 - BGP Deployment Example
- Forwarding and Policy Model with ACI Layer 3 Outside Connection
 - Inside and Outside
 - External EPG and Policy Model
- ACI Layer 2 Connection to the Outside Network
 - Extend the EPG Out of the ACI Fabric
 - Extend the Bridge Domain Out of the ACI Fabric
 - ACI Interaction with Spanning Tree Protocol (STP)
- Remote VXLAN Tunnel Endpoint (VTEP)

Module 4: Border Gateway Protocol (BGP) for External Network Reachability

- BGP Network Topology
- Fabric Setup for External Network Peering
- iBGP Peering Options with an External Network
- WAN Router Sample Configuration
- ACI BGP Sample Configuration for ISP1
- Bridge Domain
- External Routed Network
 - Create Layer 3 outside Network Profiles
 - Create Node Profiles
 - Configure a BGP Peer Connectivity Profile for ISP1

- Create an External Endpoint Group
- Route Profile
 - Create a Route Profile
 - Associate the Route Profile
 - The default-export Route Profile
- ACI BGP Sample Configuration for ISP2
- BGP Configuration and Statistic Validation

Module 5: Disaster Recovery Design

- Naming Conventions, IP Addresses, and VLANs
- Design Requirements
 - Tenant DMZ
 - Tenant Server Farm
 - Traffic Flow
- Disaster Recovery Topology and Service Flows
 - Leaf and Spine Connectivity
 - Server Connectivity with Leaf Switches
 - Layer 4 Through 7 Device Connectivity to Leaf Switches
 - Cisco ASR Router WAN Connectivity
 - Cisco APIC Connectivity
 - External Networking
- Service Architecture Design
- Traffic Flow
- Services Integration
 - Service Device Packages
 - Cisco ASA Integration with Cisco ACI
 - F5 Integration with Cisco ACI
- Virtual Machine Networking
 - VMware vSphere Integration
 - VMM Domain Configuration
- Management Network in Cisco ACI
 - Out-of-Band Management Network

Module 6: Service Insertion

- Introduction
 - Topology and Design Principles
 - Connecting Endpoint Groups with a Service Graph
 - Extension to Virtualized Servers
 - Management Model
 - Service Graphs, Functions, and Rendering
 - Hardware and Software Support
- Cisco ACI Modeling of Service Insertion
 - Service Graph Definition
 - Concrete Devices and Logical Devices
 - Logical Device Selector (or Context)
 - Splitting Bridge Domains
- Configuration Steps

Module 7: Service Graph Design

- Introduction
- When to Use the Service Graph
- Service Graphs, Functions, and Rendering
- Layer 4 Through Layer 7 Parameters
- Management Model
- Workflow
- Device Package
- Physical and Virtual Domains
- Topology Choices
 - Services Deployment Models
 - Service Graph and Contracts
 - Routed Mode (GoTo Mode)
 - Transparent Mode (GoThrough Mode)
 - One-Arm Mode
- Cisco ACI Modeling of Service Insertion
 - Concrete and Logical Devices
 - Connectivity Options, Including EPG
- Configuring vPC Connectivity at the Concrete Device Level
- L4-L7 Parameters at the Concrete Device Level

- Deployment with the Service Graph Template
- Troubleshooting

Module 8: Cisco ACI Security

- Host Virtualization-Based Software Overlay Issues
- Cisco ACI Whitelist-Based Policy Model Supports Zero-Trust Security Architecture
- Cisco ACI Policy Supports Workload Mobility
- Centralized Policy Lifecycle Management and Layer 4 Through 7 Service Automation
- Open and Extensible Policy Framework Supports Defense in Depth
- Secure Multitenancy and Built-in Stateless Layer 4 Firewall
- Automated Policy Compliance
- Deep Visibility and Accelerated Threat Detection and Mitigation

LAB OUTLINE:

- Lab 1: Initial Tenant Configuration
- Lab 2: Configure EPG for Shared Services (DNS)
- Lab 3: Configure OSPF for various situations
- Lab 4: Configure BGP for various situations
- Lab 5: Configure a Tenant DMZ
- Lab 6: Configure Complex Service Graph
- Lab 7: Deploy Multi-Tenancy Security