skilltec
training

Moving forward in knowledge and training

Cisco Training Course Brochure

☎ 01752 227330
✉ enquiries@skilltec.co.uk
⌂ www.skilltec.co.uk

skilltec training

Moving forward in knowledge and training

CiscoTraining Course Brochure

skilltec training
Moving forward in knowledge and training

Implementing and Administering Cisco Solutions

Course Code	CCNA
Duration	5 days

Overview

The Implementing and Administering Cisco Solutions course provides a broad range of fundamental knowledge for all IT careers. Through a combination of lecture and hands-on labs, you will learn how to install, operate, configure, and verify a basic IPv4 and IPv6 network. The course covers configuring network components such as switches, routers, and Wireless LAN Controllers; managing network devices; and identifying basic security threats. Network programmability, automation, and software-defined networking are also covered at a foundational level.

This course helps you prepare to take the 200-301 Cisco Certified Network Associate (CCNA) exam.

Audience

Anyone looking to start a career in networking or wishing to achieve the Cisco CCNA Certification.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Identifying the components of a computer network and describe their basic characteristics.
- Understanding the model of host-to-host communication.
- Describing the features and functions of the Cisco IOS Software.
- Describing LANs and the role of switches within LANs.
- Describing Ethernet as the network access layer of TCP/IP and describe the operation of switches.
- Installing a switch and perform the initial configuration.
- Describing the TCP/IP internet Layer, IPv4, its addressing scheme, and subnetting.
- Describing the TCP/IP Transport layer and Application layer.
- Exploring functions of routing.
- Implementing basic configuration on a Cisco router.
- Explaining host-to-host communications across switches and routers.
- Identifying and resolving common switched network issues and common problems associated with IPv4 addressing.
- Describing IPv6 main features, addresses and configure and verify basic IPv6 connectivity.
- Describing the operation, benefits, and limitations of static routing.
- Describing, implementing and verifying VLANs and trunks.
- Describing the application and configuration of inter-VLAN routing.
- Explaining the basics of dynamic routing protocols and describe components and terms of OSPF.
- Explaining how STP and RSTP work.
- Configuring link aggregation using EtherChannel.
- Describing the purpose of Layer 3 redundancy protocols.
- Describing basic WAN and VPN concepts.
- Describing the operation of ACLs and their applications in the network.
- Configuring internet access using DHCP clients and explain and configure NAT on Cisco routers.
- Describing the basic QoS concepts.
- Describing the concepts of wireless networks, which types of wireless networks can be built and how to use WLC.
- Describing network and device architectures and introduce virtualization.

- Introducing the concept of network programmability and SDN and describe the smart network management solutions like Cisco DNA Center, SD-Access and SD-WAN.
- Configuring basic IOS system monitoring tools.
- Describing the management of Cisco devices.
- Describing the current security threat landscape.
- Describing threat defense technologies.
- Implementing a basic security configuration of the device management plane.
- Implementing basic steps to harden network devices.

Pre-Requisites

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic internet usage skills
- Basic IP address knowledge

Course Contents

Modules

- Exploring the Functions of Networking
- Introducing the Host-To-Host Communications Model
- Operating Cisco IOS Software
- Introducing LANs
- Exploring the TCP/IP Link Layer
- Starting a Switch
- Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets
- Explaining the TCP/IP Transport Layer and Application Layer
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process
- Troubleshooting a Simple Network
- Introducing Basic IPv6
- Configuring Static Routing
- Implementing VLANs and Trunks
- Routing Between VLANs
- Introducing OSPF
- Building Redundant Switched Topologies
- Improving Redundant Switched Topologies with EtherChannel
- Exploring Layer 3 Redundancy
- Introducing WAN Technologies
- Explaining Basics of ACL
- Enabling Internet Connectivity
- Introducing QoS
- Explaining Wireless Fundamentals
- Introducing Architectures and Virtualization
- Explaining the Evolution of Intelligent Networks
- Introducing System Monitoring
- Managing Cisco Devices
- Examining the Security Threat Landscape
- Implementing Threat Defense Technologies
- Implementing Device Hardening

Labs

- Get Started with Cisco CLI
- Observe How a Switch Operates
- Perform Basic Switch Configuration
- Inspect TCP/IP Applications
- Configure an Interface on a Cisco Router
- Configure and Verify Layer 2 Discovery Protocols
- Configure Default Gateway
- Explore Packet Forwarding
- Troubleshoot Switch Media and Port Issues
- Troubleshoot Port Duplex Issues
- Configure Basic IPv6 Connectivity
- Configure and Verify IPv4 Static Routes
- Configure IPv6 Static Routes
- Configure VLAN and Trunk
- Configure a Router on a Stick
- Configure and Verify Single-Area OSPF
- Configure and Verify EtherChannel
- Configure and Verify IPv4 ACLs
- Configure a Provider-Assigned IPv4 Address
- Configure Static NAT
- Configure Dynamic NAT and PAT
- Log into the WLC
- Monitor the WLC
- Configure a Dynamic (VLAN) Interface
- Configure a DHCP Scope
- Configure a WLAN
- Define a RADIUS Server
- Explore Management Options
- Explore the Cisco DNA Center
- Configure and Verify NTP
- Create the Cisco IOS Image Backup
- Upgrade Cisco IOS Image
- Configure WLAN Using WPA2 PSK Using the GUI
- Secure Console and Remote Access
- Enable and Limit Remote Access Connectivity
- Configure and Verify Port Security

Exam Details

This course leads to the 200-301 - Cisco Certified Network Associate Exam (CCNA).

Implementing Cisco Advanced Call Control and Mobility Services

Course Code	CLACCM
Duration	5 days

Overview

The Implementing Cisco Advanced Call Control and Mobility Services (CLACCM) course covers advanced call control and mobility services. You will learn how to use Cisco® Unified Communications Manager features to consolidate your communications infrastructure into a scalable, portable, and secure collaboration solution. Through a combination of lessons and hands-on experiences, you will also learn about a wealth of other features such as Globalized Call Routing, Global Dial Plan Replication, Cisco Unified Mobility, Cisco Extension Mobility, Device Mobility, Session Initiation Protocol Uniform Resource Identifier (SIP/ URI) call routing, Call Admission Control, Cisco Unified Communications Manager Express and Survivable Remote Site Telephony (SRST) gateway technologies, Cisco Unified Board Element Call deployments, signalling and media protocols, call coverage, and time of day routing.

Audience

Collaboration engineers involved in the design, implementation and troubleshooting of Cisco collaboration advanced call control solutions and mobility services.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Analyzing and troubleshooting SIP, H.323, and media protocols.
- Implementing time-of-day routing, call park, call pickup, and meet-me conferences in Cisco Unified Communications Manager.
- Implementing call coverage in Cisco Unified Communications Manager.
- Configuring and troubleshooting Cisco Unified Communications Manager Device Mobility.
- Configuring and troubleshooting Cisco Unified Communications Manager Extension Mobility.
- Configuring and troubleshooting Cisco Unified Communications Manager Unified Mobility.
- Implementing Cisco Unified Communications Manager Express for SIP phones.
- Implementing globalized call routing within and between Cisco Unified Communications Manager clusters.
- Implementing Media Gateway Control Protocol (MGCP) fallback and Survivable Remote Site Telephony (SRST) in Cisco Unified Communications Manager and in Cisco IOS® XE gateways.
- Implementing Call Admission Control and Automated Alternate Routing (AAR) in Cisco Unified Communications Manager.
- Implementing URI calling in Cisco Unified Communications Manager for calls within a cluster and between clusters.
- Troubleshooting multisite Cisco Unified Communications Manager deployments.
- Implementing Intercluster Lookup Service (ILS) between Cisco Unified Communications Manager clusters and enabling General Data Protection Regulation (GDPR).
- Configuring and troubleshooting Cisco Unified Border Element.

Pre-Requisites

- Internet web browser usability knowledge and general computer usage
- Basic understanding of networking technologies
- Basic understanding of voice and video

Recommended courses:

- CLFNDU - Understanding Cisco Collaboration Foundations
- CLCOR - Implementing and Operating Cisco Collaboration Core Technologies

Course Contents

Analyzing and Troubleshooting Signalling and Media Protocols

- SIP Review
- H.323 Review
- SIP and H.323 Trunking Considerations
- SIP and H.323 Troubleshooting Tools

Implementing Cisco Unified Communications Manager Supplemental Services

- Call Park
- Call Pickup
- Meet-Me Conferences
- Time-of-Day Routing

Implementing Call Coverage in Cisco Unified Communications Manager

- Overview of Call Coverage in Cisco Unified Communications Manager
- Call Hunting
- Call Queuing

Configuring and Troubleshooting Cisco Unified Communications Manager Device Mobility

- Issues with Roaming Devices
- Device Mobility Characteristics
- Device Mobility Operation
- Device Mobility Considerations

Configuring and Troubleshooting Cisco Unified Communications Manager Extension Mobility

- Issues with Roaming Users
- Cisco Unified Communications Manager Extension Mobility Characteristics
- Cisco Unified Communications Manager Extension Mobility Components
- Cisco Unified Communications Manager Extension Mobility Considerations
- Cisco Unified Communications Manager Extension Mobility Troubleshooting.

Configuring and Troubleshooting Cisco Unified CM Unified Mobility

- Issues with Multiple Devices
- Cisco Unified CM Mobility Overview
- Cisco Unified CM Unified Mobility Operation
- Cisco Unified CM Mobility Considerations
- Cisco Unified CM Unified Mobility Troubleshooting

Implementing Cisco Unified Communications Manager Express

- Cisco Unified Communications Manager Express Overview
- Endpoint Addressing and Call Routing in Cisco Unified Communications Manager Express
- Calling Privileges and Toll-Fraud Prevention in Cisco Unified Communication Manager Express
- Hunt Groups
- Call Park
- Paging

Implementing Globalized Call Routing

- Overview of Multisite Dial Plans
- Globalized Call Routing Overview
- Globalized Call-Routing Number Formats
- Globalization of Localized Call Ingress
- Localization During Call Egress
- Calls that involve Non-DID Endpoints
- TEHO, Including Local PSTN Backup
- Class of Service in Globalized Call Routing Deployments

Implementing Remote Site Survivability

- Overview of Remote Site Survivability
- Cisco Unified SRST
- Reachability Within the Remote Site and to the Outside
- Survivability of MGCP Gateways Using MGCP Fallback

Implementing Call Admission Control in Cisco Unified Communications Manager

- CAC Overview
- Location CAC Within a Cluster
- Location CAC for Off-Cluster Calls Using Locally Configured Locations
- Intercluster Location CAC
- PSTN Backup for Intracluster Calls Denied by CAC
- PSTN Backup for Intercluster Calls Denied by CAC

Implementing URI Calling in Cisco Unified Communications Manager

- URI Call-Routing Overview
- Directory URIs in Cisco Unified Communications Manager
- URI Call-Routing Process
- SIP Route Patterns and SIP Trunks
- URI Call Routing Considerations

Troubleshooting Multisite Cisco Unified Communications Manager Deployments

- Call Routing Troubleshooting
- Calling-Party Presentation Troubleshooting
- Egress Device Selection and SIP Trunk Troubleshooting
- CAC Troubleshooting

Examining Global Dial Plan Replication

- GDPR Overview
- ILS Characteristics
- GDPR Components
- Call Routing with GDPR
- PSTN Backup

Configuring and Troubleshooting Cisco Unified Border Element

- Overview of Cisco Unified Border Element
- Cisco Unified Border Element Call Routing
- Explore Advanced Cisco Unified Border Element Dial-Peer Features
- Cisco Unified Border Element SIP Header and SDP Manipulation
- Cisco Unified Border Element Signaling and Media Bindings
- Cisco Unified Border Element Troubleshooting

Labs

- Analyze SIP, H.323, and Media Protocols
- Troubleshoot SIP and Media Protocols
- Implement Cisco Unified Communications Manager Supplemental Services
- Implement Call Hunting and Call Queueing in Cisco Unified Communications Manager
- Configure Device Mobility
- Troubleshoot Cisco Unified Communications Manager Device Mobility
- Configure Cisco Unified Communications Manager Extension Mobility
- Troubleshoot Cisco Unified Communications Manager Extension Mobility
- Configure Cisco Unified Mobility
- Troubleshoot Cisco Unified Mobility
- Implement Endpoints in Cisco Unified Communications Manager Express
- Implement Endpoint Addressing and Call Routing in Cisco Unified Communications Manager Express
- Implement Calling Privileges in Cisco Unified Communications Manager Express
- Implement Hunt Groups, Call Park, and Paging in Cisco United Communications Manager Express
- Implement Globalized Call Routing
- Implement TEHO, PSTN Backup, and CoS in a Globalized Call-Routing Deployment
- Implement MGCP Fallback and Survivable Remote Site Telephony
- Implement Call Admission Control
- Implement a URI-Based Dial Plan for Multisite Deployments
- Troubleshoot Globalized Call Routing
- Troubleshoot Call Admission Control
- Implement Global Dial Plan Replication
- Implement Cisco Unified Border Element
- Troubleshoot Cisco Unified Border Element

Exam Details

This course leads to the 300-815 - Implementing Cisco Advanced Call Control and Mobility Services (CLACCM) exam.

Successful completion of this exam, will earn you the Cisco Certified Specialist - Collaboration Call Control & Mobility Implementation certification and will satisfy the concentration exam requirement for the CCNP Collaboration professional-level certification.

Implementing Automation for Cisco Collaboration Solutions

Course Code	CLAUI
Duration	3 days

Overview

The Implementing Automation for Cisco Collaboration Solutions (CLAUI) course teaches you how to implement Cisco® Collaboration automated, programmable solutions for voice, video, collaboration, and conferencing on-premises or in the cloud. Through a combination of lessons and hands-on labs, you will combine tools and processes to tackle communication challenges using key platforms including Cisco Unified Communications Manager, Cisco IP Phone Services, Cisco Unity® Connection, Cisco Finesse®, Cisco Collaboration Endpoints, Cisco Webex Teams™, and Cisco Webex® Meetings.

Learn how to use application programming interfaces (APIs) interfaces such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP), parsing data in Extensible Markup Language (XML) and JavaScript Object Notation (JSON) formats, and leverage frameworks such as Python.

Audience

Network and software engineers interested in Cisco Collaboration and Webex automation.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Examining API and automation capabilities and concepts for Cisco Unified Communication Manager.
- Examining API and automation capabilities and concepts for Cisco Unity Connection.
- Examining API and automation capabilities and concepts for Cisco Finesse.
- Examining Experience API (xAPI) and automation capabilities and concepts for Cisco Collaboration endpoints.
- Examining API and automation capabilities and concepts for Cisco Webex Teams.
- Examining API and automation capabilities and concepts for Cisco Webex Meetings.

Pre-Requisites

- Basic knowledge of Simple Object Access Protocol (SOAP) and REST APIs
- Basic programming and scripting skills in Python
- Intermediate knowledge in managing and configuring three or more of the following Cisco Collaboration offerings: Cisco Unified Communications Manager; Cisco IP Phones; Cisco Finesse; Cisco Webex Devices (Collaboration and Video Endpoints); Cisco Webex Teams.; Cisco Webex Meetings.

Recommended courses:

- CLCOR - Implementing and Operating Cisco Collaboration Core Technologies

Course Contents

Automating Cisco Unified Communications Manager

- Cisco Unified Communications Manager: AXL API Overview
- Built-In AXL API Calls
- SQL API Calls
- Computer Telephony Integration
- CDRs and Performance APIs
- Phone Services APIs

Automating Cisco Unity Connection

- Cisco Unity Connection

Automating Cisco Finesse

- Cisco Finesse APIs
- Cisco Finesse Gadgets

Examining Cisco Collaboration Endpoint Automation

- Cisco xAPI Overview
- In-Room Control Editor Introduction
- Macro Introduction

Examining Cisco Cloud Collaboration Automation

- Cisco Webex Administration API Overview
- Cisco Webex Teams Bots Overview
- Widgets Overview
- Cisco Webex Teams SDK

Examining Cisco Conferencing Automation

- Cisco Webex Meetings API
- Cisco Meeting Server API

Labs

- Configure the Initial Collaboration Lab Environment
- Verify Phone Details
- Configure Phone Line Label
- Configure User Pin
- Configure System Forward No Answer Timer
- Configure Route Plan Report
- Deploy Basic SQL Query
- Deploy Advanced SQL Query
- Configure and Alternate Extension in Cisco Unity Connection
- Configure Voicemail Pin
- Verify Agent Settings
- Deploy Gadget
- Configure Cisco Webex Meetings User
- Configure and Record Cisco Webex Meeting
- Verify System Status
- Configure Host Access on Cisco Meeting Server Spaces

Exam Details

This course leads to the 300-835 - Automating and Programming Cisco Collaboration Solutions (CLAUTO) exam.

Successful completion of this exam will earn you the Cisco Certified DevNet Specialist - Collaboration Automation and Programmability certification, and will satisfy the concentration exam requirements for the Cisco CCNP Collaboration Certification and the Cisco Certified DevNET Professional certification.

Implementing Cisco Collaboration Cloud and Edge Solutions

Course Code	CLCEI
Duration	5 days

Overview

The Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI) course provides you with knowledge of Cisco® Expressway Series solutions that enable business-to-business (B2B) calls, Cisco Mobile, remote access, authentication options and additional Cisco Expressway Series features.

Though a combination of lessons and hands-on labs, you will learn how to leverage collaborative technology to access secure, collaborative work supports including video, voice, content and remote workloads.

Audience

Collaboration Engineers involved in the design, implementation and troubleshooting of Cisco collaboration technologies, as well as administrators involved in the support and troubleshooting of Cisco collaboration technologies.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Configuring and troubleshooting Cisco Unified Communications Manager and Cisco Expressway Series integration.
- Describing the Cisco Expressway-C additional features.
- Configuring and troubleshooting Cisco Collaboration solutions for B2B calls
- Describing how to secure B2B communication with Cisco Expressway Series.
- Describing the Mobile and Remote Access (MRA) feature.
- Describing the Cisco Expressway MRA security and integration options, including integration with Cisco Unity® Connection and Cisco Instant Messaging and Presence (IM&P).
- Configuring Cisco Webex® Hybrid Services.

Pre-Requisites

- Understanding of networking technologies
- Understanding of voice and video
- Knowledge of Cisco Collaboration core technologies
- SIP and XMPP signalling protocols fundamentals
- Collaboration call control fundamentals of Cisco Unified Communications Manager

Recommended courses:

- CLFNDU - Understanding Cisco Collaboration Foundations
- CLCOR - Implementing and Operating Cisco Collaboration Core Technologies

Course Contents

Configuring and Troubleshooting the Cisco Expressway Series

- Cisco Expressway Series Architecture
- Describe SIP and H.323 in the Cisco Expressway Series
- Describe Interworking in the Cisco Expressway Series
- Zones
- Digit String Manipulation
- Search Rules
- Transforms
- Troubleshoot Call Processing the Cisco Expressway Series
- Backup and Restore

Configuring Cisco Expressway Additional Features

- Describe Bandwidth Management
- Hardening Local Endpoint Registrations
- Describe Cisco Expressway Security and Clustering Features

Configuring and Troubleshooting Cisco Unified Communications Manager and Cisco Expressway Series

- Cisco Unified Communications Manager and Cisco Expressway-C Integration Overview
- Call Flow
- Dial Plan Overview
- Call Policy
- Troubleshooting Options for Cisco Unified Communication Manager and Cisco Expressway-C Integration

Configuring and Troubleshooting Cisco Collaboration Solutions for Business-to-Business

- Describe Supported Services for B2B Collaboration
- Describe Prerequisites for Business to Business Collaboration
- Call Flow Including Cisco Unified Communications Manager Endpoints
- Network Address Translation in a Collaboration Environment
- Cisco Expressway Series B2B Call Troubleshooting

Securing Business-to-Business Communication

- Firewall Traversal
- Certificates
- Secure Media
- Secure Media Between Cisco Unified Communications Manager and Cisco Expressway Series
- Toll Fraud Prevention

Configuring and Troubleshooting Mobile and Remote Access

- Describe Prerequisites for Mobile and Remote Access
- Describe Service Discovery
- Explore Expressway Settings for MRA
- Certificates
- HTTP Proxy
- Cisco Jabber Registration Procedure
- Cisco Jabber Registration in Hybrid Deployment
- Cisco Jabber Configuration File
- MRA Troubleshooting

Integrating and Securing Mobile and Remote Access

- Secure Cisco Unified Communications Integration
- Cisco Unity Connection Integration
- Cisco MRA Access Control Options
- Additional Cisco MRA Features

Configuring Cisco Webex Hybrid Services

- Cisco Webex Teams
- Describe Cisco Webex Control Hub
- Describe Cisco Webex Hybrid Media Services
- Describe Cisco Expressway Network Requirements for Using Hybrid Call Service Connect
- Explore Cisco Expressway Requirements for Using Hybrid Call Service Connect
- Describe Cisco Webex Video Mesh

Labs

- Deploy Virtualized Cisco Expressway
- Perform the Initial Cisco Expressway Series Configuration
- Register Endpoints on Cisco Expressway Series
- Call Search History and Registration
- Troubleshooting Tools
- Configure Cisco Expressway Series Bandwidth Management and Registration Restrictions
- Troubleshoot Cisco Expressway Series Endpoint Registration and Local Dial Plan
- Configure Cisco Expressway Series Security Features
- Configure Cisco Unified Communications Manager to Connect with Cisco Expressway-C
- Troubleshoot Cisco Unified Communications Manager and Cisco Expressway Series Integration
- Configure Cisco Unified Communications Manager and Cisco Expressway Series Integration (Practice Activity)
- Implement a B2B Cisco Collaboration Solution
- Troubleshoot B2B Calls on the Cisco Expressway Series
- Troubleshoot B2B Calls on the Cisco Expressway Series (practice activity)
- Secure a B2B Cisco Collaboration Communication
- Configure MRA on the Cisco Expressway Series
- Troubleshoot MRA on the Cisco Expressway Series
- Configure MRA with Additional Application Integrations
- Prepare for Cisco Webex Teams Integration
- Configure Cisco Webex Hybrid Services

Exam Details

This course leads to the 300-820 - Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI) exam.

This exam is required for one of the concentrations for the CCNP Collaboration Certification as well as the standalone Cisco Certified Specialist - Collaboration Cloud & Edge Implementation certification.

skilltec training
Moving forward in knowledge and training

Implementing and Operating Cisco Collaboration Core Technologies

Course Code	CLCOR
Duration	5 days

Overview

The Implementing Cisco Collaboration Core Technologies (CLCOR) course will provide you with the knowledge and skills needed to implement and deploy core collaboration and networking technologies, including infrastructure and design, protocols, codecs, and endpoints, Cisco IOS XE gateway and media resources, Call Control, QoS, and additional Cisco collaboration applications. The course will help you to integrate and troubleshoot Cisco Unified Communications Manager with Lightweight Directory Access Protocol (LDAP) for user synchronization and user authentication, implement Cisco Unified Communications Manager provisioning features and configure and Troubleshoot Collaboration Endpoints.

Please note that this course is a combination of Instructor-Led and Self-Paced Study; 5 days in the classroom and approximately 3 days of self-study.

Audience

Engineers involved in the implementation and operation of a Cisco Collaboration solution.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the Cisco Collaboration solutions architecture.
- Comparing the IP Phone signalling protocols of SIP, H323, MGCP and SCCP.
- Integrating and troubleshooting Cisco Unified Communications Manager with LDAP for user synchronization and user authentication.
- Implementing Cisco Unified Communications Manager provisioning features.
- Describing the different codecs and how they are used to transform analogue voice into digital streams.
- Describing a dial plan and explaining call routing in Cisco Unified Communications Manager.
- Implementing PSTN access using MGCP gateways.
- Implementing a Cisco gateway for PSTN access.
- Configuring calling privileges in Cisco Unified Communications Manager.
- Implementing toll fraud prevention.
- Implementing globalized call routing within a Cisco Unified Communications Manager cluster.
- Implementing and troubleshooting media resources in Cisco Unified Communications Manager.
- Describing Cisco Instant Messaging and Presence, the call flows and the protocols.
- Describing and configuring endpoints and commonly required features.
- Configuring and troubleshooting Cisco Unity Connection integration.
- Configuring and troubleshooting Cisco Unity Connection call handlers.
- Describing how MRA is used to allow endpoints to work from outside the company.
- Analyzing traffic patterns and quality issues in converged IP networks supporting voice, video, and data traffic.
- Defining QoS and its models.
- Implementing and Configuring classification and marking options on Cisco Catalyst switches.

Pre-Requisites

- Working knowledge of fundamental terms of computer networking, including LANs, WANs, switching, and routing
- Basics of digital interfaces, public switched telephone networks (PSTNs), and voice over IP (VoIP)
- Fundamental knowledge of converged voice and data networks and Cisco Unified Communications Manager deployment

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- CLFNDU - Understanding Cisco Collaboration Foundations

Course Contents

Describing the Cisco Collaboration Solutions Architecture

- Overview of Cisco Collaboration Solutions Architecture
- Collaboration Deployment Models
- Licensing
- High Availability
- Capacity Planning
- Security Requirements
- Disaster Recovery
- Dial Plan
- IP Network Protocols
- Codecs

Exploring Call Signalling over IP Networks Bullet

- IP Phone Initialization
- Single Site On-Cluster Calling
- Single Site On-Cluster Call Setup Troubleshooting
- Describe the Call Setup and Teardown Process
- Describe SIP Call Signalling for Call Setup and Teardown
- Compare the Call Control Protocols
- Describe DTMF Signalling over IP Networks

Integrating Cisco Unified Communications Manager LDAP

- Overview of LDAP Integration in Cisco Unified Communications Manager
- LDAP Synchronization in Cisco Unified Communications Manager
- LDAP Authentication in Cisco Unified Communications Manager
- LDAP Attribute Mapping in Cisco Unified Communications Manager
- LDAP Considerations in Cisco Unified Communications Manager
- Access Control Groups in Cisco Unified Communications Manager
- Feature Group Templates in Cisco Unified Communications Manager

Implementing Cisco Unified Communications Manager Provisioning Features

- Overview of Provisioning Options
- Self-Provisioning Prerequisites
- Self-Provisioning Components
- Self-Provisioning Authentication Modes
- Batch-Provisioning Tools

Exploring Codecs

- Define Codecs
- Compare Audio Codecs
- Compare Video Codecs
- Evaluate the Effects of Encryption on Codecs
- Describing Call Admission Control
- Configure Regions and Locations to control which codec is negotiated and how much bandwidth can be consumed

Describing Dial Plans and Endpoint Addressing

- Dial Plan Overview
- Dal Plan Components and Their Functions
- EndPoint Addressing
- Overview of Cisco Unified Communications Manager Call Routing
- Cisco Unified Communications Manager Call-Routing Logic
- Address Methods and Digit Analysis
- Variable-Length Patterns, Overlapping Patterns and Urgent Priority

Implementing MGCP Gateways

- Overview of MGCP Gateways
- MGCP Gateway Implementation
- Path Selection in Cisco Unified Communications Manager
- Route Groups
- Route Lists and Route Patterns
- Digit Manipulation in Cisco Unified Communications Manager

Implementing Voice Gateways

- Overview of Dial Peers
- Digit Manipulation Features on Cisco IOS Gateways
- Codec and DTMP-Relay Selection on Cisco IOS Gateways

Configuring Calling Privileges in Cisco Unified Communications Manager

- Calling Privileges Overview
- Partitions and CSSs
- Partition and CSS Considerations
- Time-of-Day Routing
- Client Matter Codes and Forced Authorization Codes

Implementing Toll Fraud Prevention

- Toll Fraud Prevention Overview
- Cisco Unified Communications Manager CoS for Toll Fraud Prevention

Implementing Globalized Call Routing

- Overview of Multisite Dial Plans
- Globalized Call Routing Overview
- Globalized Call Routing Number Formats
- Globalization of Localized Call Ingress
- Localization During Call Egress

Implementing and Troubleshooting Media Resources in Cisco Unified Communications Manager

- Media Resources Overview in Cisco Unified Communications Manager
- Media Resource Selection and Access Control in Cisco Unified Communications Manager
- Describing the Annunciator Feature
- Describing Unicast and Multicast MOH Characteristics
- Audio and Video Conference Bridge Devices
- Audio and Video Conference Bridge Integration Options
- MTP and Transcoder Devices
- MTP and Transcoder Requirements

Describing Cisco Instant Messaging and Presence

- Describe Cisco IM and Presence Features and Architecture
- Compare the Protocols XMPP and SIMPLE SIP
- Clustering
- Describe Cisco Unified Communications IM and Presence Components and Communication Flows

Enabling Cisco Jabber

- Cisco Jabber Deployment Modes
- Cisco Jabber Operational Modes

Configuring Cisco Unity Connection Integration

- Overview of Cisco Unity Connection Integration
- SIP Integration
- Typical Integration Mistakes
- Integration Considerations

Configuring Cisco Unity Connection Call Handlers

- Call Handler Overview
- System Call Handler
- Caller Input
- Operator Call Handler
- Goodbye Call Handler
- Directory Handler
- Interview Handler

Describing Collaboration Edge Architecture

- Describe Collaboration Edge (Expressway -C, -E)
- Describe Supported Services for B2B Collaboration
- Describe Prerequisites for Mobile and Remote Access
- Describe Service Discovery
- Explore Expressway Settings for MRA
- Describe Cisco Unified Border Element (CUBE)

Analyzing Quality Issues in Converged Networks

- Converged Networks
- Available Bandwidth
- Components of Network Delay
- End-to-End Delay Calculations
- Jitter
- Packet Loss

Defining QoS and QoS Models

- QoS Defined
- Network Traffic Identification
- Divide Network Traffic into Classes and Define Policies
- QoS Mechanisms
- QoS Models
- DSCP Encoding
- Expedited Forwarding and Assured Forwarding
- Class Selector

Implementing Classification and Marking

- Classification and Marking Overview
- Classification and Marking at the Network and Data Link Layers
- QoS Service Class
- Cisco Marking Recommendations
- QoS Markings in a SIP Call Flow
- MQC Classification and Marking Options

Configuring Classification and Marking on Cisco Catalyst Switches

- Campus Classification and Marking
- Overview of QoS Trust Boundaries
- Ingress QoS Models
- QoS Marking and Table Maps
- Internals DSCP

Labs

- Using Certificates
- Configure IP Network Protocols
- Configure and Troubleshoot Collaboration Endpoints
- Troubleshoot Calling Issues
- Configure and Troubleshoot LDAP Integration in Cisco Unified Communications Manager
- Deploy an IP Phone Through Auto and Manual Registration
- Configure Self-Provisioning
- Configure Batch Provisioning
- Explore the Cisco VoIP Bandwidth Calculator
- Configure Regions and Locations
- Implement Endpoint Addressing and Call Routing
- Implement PSTN Calling Using MGCP Gateways
- Configure and Troubleshoot ISDN PRI
- Examine Cisco IOS Gateway Inbound and Outbound Dial-Peer Functions
- Implement and Troubleshoot Digit Manipulation on a Cisco IOS Gateway
- Configure Calling Privileges
- Implement Toll Fraud Prevention on Cisco Unified Communications Manager
- Implement Globalized Call Routing
- Deploy an On-Premise Cisco Jabber Client for Windows
- Configure the Integration between Unity Connection and CUCM
- Manage Unity Connection Users
- EAI: Configure QoS

Exam Details

This course leads to the 350-801 CLCOR - Implementing Cisco Collaboration Core Technologies.

Delegates looking to obtain their CCNP Collaboration will also need to pass a CCNP Collaboration Concentration exam. Passing the 350-801 exam will also earn you the Cisco Certified Specialist - Collaboration Core certification.

Understanding Cisco Collaboration Foundations

Course Code	CLFNDU
Duration	5 days

Overview

The Understanding Cisco Collaboration Foundations (CLFNDU) course gives you the skills and knowledge needed to administer and support a simple, single-site Cisco® Unified Communications Manager (CM) solution with Session Initiation Protocol (SIP) gateway. The course covers initial parameters, management of devices including phones and video endpoints, management of users, and management of media resources, as well as Cisco Unified Communications solutions maintenance and troubleshooting tools. In addition, you will learn the basics of SIP dial plans including connectivity to Public Switched Telephone Network (PSTN) services, and how to use class-of-service capabilities.

Audience

This course is designed for individuals looking to administer and support a simple single-site Cisco Unified Communications solution.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Defining collaboration and describing the main purpose of key devices in a Cisco collaboration on-premise, hybrid, and cloud deployment model.
- Configuring and modifying required parameters in Cisco Unified Communications Manager (CM) including service activation, enterprise parameters, CM groups, time settings, and device pool.
- Deploying and troubleshooting IP phones via auto registration and manual configuration within Cisco Unified CM.
- Describing the call setup and teardown process for a SIP device including codec negotiation using Session Description Protocol (SDP) and media channel setup.
- Managing Cisco Unified CM user accounts (local and via Lightweight Directory Access Protocol [LDAP]) including the role/group, service profile, UC service, and credential policy.
- Configuring dial plan elements within a single site Cisco Unified CM deployment including Route Groups, Local Route Group, Route Lists, Route Patterns, Translation Patterns, Transforms, SIP Trunks, and SIP Route Patterns.
- Configuring Class of Control on Cisco Unified CM to control which devices and lines have access to services.
- Configuring Cisco Unified CM for Cisco Jabber and implementing common endpoint features including call park, softkeys, shared lines, and pickup groups.
- Deploying a simple SIP dial plan on a Cisco Integrated Service Routers (ISR) gateway to enable access to the PSTN network.
- Managing Cisco UCM access to media resources available within Cisco UCM and Cisco ISR gateways.
- Describing tools for reporting and maintenance including Unified Reports, Cisco Real-Time Monitoring Tool (RTMT), Disaster Recovery System (DRS), and Call Detail Records (CDRs) within Cisco Unified CM.
- Describing additional considerations for deploying video endpoints in Cisco Unified CM.
- Describing the integration of Cisco Unity® with Cisco Unified CM and the default call handler.

Pre-Requisites

- Internet web browser usability knowledge and general computer usage
- Knowledge of Cisco Internetwork Operating System (Cisco IOS®) command line

Course Contents

Modules

- **Exploring the Path to** Collaboration
- Introducing Cisco Unified Communications Manager and Initial Parameters
- Exploring Endpoints and the Registration Process
- Exploring Codecs and Call Signalling
- Managing Users in Cisco Unified Communication Manager
- Describing a Basic Dial Plan
- Describing Class of Service
- Enabling Endpoints and Features
- Describing the Cisco ISR as a Voice Gateway
- Exploring Cisco Unified Communication Manager Media Resources
- Reporting and Maintenance
- Exploring Additional Requirements for Video Endpoints
- Describing Cisco Unity **Connection**

Labs

- Configure Default Cisco Unified CM System and Enterprise Parameters
- Configure the Cisco Unified CM Core System Settings
- Configure an Access Switch for an Endpoint
- Deploy an IP Phone Through Auto and Manual Registration
- Administer Endpoints in Cisco Unified Communications Manager
- Create a Local User Account and Configure LDAP
- Implement Users
- Create a Basic Dial Plan
- Explore Partitions and Call Search Spaces
- Describe Private Line Automatic Ringdown (PLAR)
- Deploy an On-Premise Cisco Jabber® Client for Windows
- Implement Common Endpoint Features
- Configure Common Endpoint Features
- Configure Voice over Internet Protocol (VoIP) Dial Peers
- Configure Integrated Service Digital Network (ISDN) Circuits and Plain Old Telephone Service (POTS) Dial Peers
- Control Access to Media Resources
- Use Reporting and Maintenance Tools
- Explore Endpoint Troubleshooting Tools
- Examine the Integration between Unity Connection and Cisco Unified CM
- Manage Unity Connection Users

Exam Details

This course does not lead directly to a certification exam, but it does cover foundational knowledge that can help you prepare for the professional-level collaboration courses and exams.

skilltec training

Moving forward in knowledge and training

Implementing Cisco Collaboration Applications

Course Code	CLICA
Duration	5 days

Overview

The Implementing Cisco Collaboration Applications (CLICA) course provides you with the knowledge and skills required to streamline communication protocol, strengthen compliance measures and enhance your communication systems and devices. Gain an understanding of Single Sign-On (SSO), Cisco® Unified IM & Presence, Cisco Unity® Connection and Cisco Unity Express and Application clients. Through a combination of lessons and hands-on training, you will acquire the skills to maximize the agility of robust management systems.

Audience

Collaboration engineers involved in the design, implementation and troubleshooting of Cisco collaboration applications and administrators involved in the support and troubleshooting of Cisco Collaboration applications.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Configuring Cisco Unity Connection integration.
- Configuring and troubleshooting Cisco Unity Connection and Cisco Unity Connection call handlers.
- Configuring and troubleshooting Cisco Unity Express.
- Describing SSO for Cisco Unified Communications applications.
- Describing how Cisco Jabber® and Cisco Unified Communications Manager IM and Presence are integrated with other Cisco or third-party applications.
- Customizing the Cisco Unified Communications Manager IM and Presence and Cisco Jabber functionality.
- Configuring and troubleshooting chat rooms and message archiving.
- Troubleshooting Cisco Jabber and Cisco Unified Communications Manager IM and Presence.
- Integrating Cisco Unified Attendant Console Advanced with Cisco Unified Communications Manager and Cisco Unified Communications Manager IM; Presence server.
- Configuring call recording and monitoring.

Pre-Requisites

- Basic understanding of networking technologies
- Basic understanding of voice and video
- Cisco Unified Communications Manager experience including single site dial plan, single Public Switched Telephone Network (PSTN) gateway, and Session Initiation Protocol (SIP) trunks.

Recommended courses:

- CLFNDU - Understanding Cisco Collaboration Foundations
- CLCOR - Implementing and Operating Cisco Collaboration Core Technologies

Course Contents

Configuring and Troubleshooting Cisco Unity Connection Integration

- Overview of Cisco Unity Connection Integration
- SCCP Integration
- Typical Integration Mistakes
- Integration Considerations
- Clustering Options
- Deployment Options
- Networking

Configuring and Troubleshooting Cisco Unity Connection Call Handlers

- Call Handler Overview
- System Call Handler
- Caller Input
- Operator Call Handler
- Goodbye Call Handler
- Directory Handler
- Interview Handler
- Toll Fraud

Troubleshooting Cisco Unity Connection

- Overview of Cisco Unity Connection Troubleshooting Options
- Integration Troubleshooting Tools
- Cisco Unified Real-Time Monitoring Tool

Configuring and Troubleshooting Cisco Unity Express

- Overview of Cisco Unity Express Integration
- Triggers
- MWI Notification
- Cisco Unity Express Trigger Troubleshooting
- MWI Notification Troubleshooting

Configuring Single Sign-On (SSO) for Cisco Unified Communications Applications

- SSO Overview
- SSO Prerequisites
- SSO Components
- Trust Metadata File
- Identity Provider
- SAML Authentication
- OAuth
- Cisco Unified Communications Manager SSO Capabilities
- SSO for Collaboration Endpoints
- SSO and Collaboration Edge
- Session and Token Expiration Timers

Integrating Cisco Unified Communications Manager IM and Presence and Cisco Jabber

- Cisco Unified Communications Manager IM and Presence and Cisco Jabber Integration Overview
- Integration with Cisco Unified Communications Manager and IM and Presence Service
- Integration with Cisco Unity Connection
- Integration with Conferencing Servers
- Integration with LDAP
- Integration with Microsoft Exchange
- Clustering
- Cisco Unified Communications Manager IM and Presence Service Federation Overview
- Cisco Unified Communications Manager IM and Presence Multidomain Deployment
- Cisco Unified COmmunications Manage IM and Presence Interdomain Federation
- Cisco Jabber Deployment Options
- Cisco Jabber in Deskphone Control Mode
- Cisco Jabber in Softphone Mode
- Cisco Jabber Service Discovery Process

Customizing Cisco Unified Communications Manager IM and Presence and Cisco Jabber Functionality

- Cisco Jabber Customization Overview
- Cisco Unified Communications Services
- Service Profiles
- Custom Configuration Files
- Contact Sources
- Contact Photos
- Policies
- Embedded Tabs
- Cisco Jabber Extend and Connect
- Apple Push Notification Service

Configuring Cisco Unified Communications Manager IM and Presence Service Compliance and Message Archiving

- Enterprise Instant Messaging
- External Database Overview
- PostgreSQL External Database Integration
- Persisitent Chat
- Message Archiving

Troubleshooting Cisco Unified Communications Manager IM and Presence Service

- Cisco Unified Communications Manager IM and Presence System Troubleshooting Tools
- System Troubleshooter
- Cisco Unified Real-Time Monitoring Tool
- Presence Viewer
- Cisco Jabber Connection Status
- Apple Push Notifications Troubleshooting
- IM and Presence Service Multidomain Deployment Troubleshooting

Integrating Cisco Unified Attendant Console Advanced

- Cisco Unified Attendant Console Advanced Integration Overview
- Capablilities
- Platform Requirements
- Cisco Unified Communications Manager Integration
- Cisco Unified Communications Manager IM and Presence Service Integration
- Reporting

Implementing Call Recording and Monitoring

- Overview of Call Recording and Monitoring in Cisco Unified Communications Manager
- SPAN-Based Solutions
- Cisco Unified Border Element Dial-Peer Forking
- Cisco Unified Communications Manager Network-Based Recording and Monitoring

Labs

- Integrate and Set Up Cisco Unity Connection
- Configure Cisco Unity Connection Call Handlers
- Implement Toll Fraud Prevention
- Troubleshoot Cisco Unity Connection Call Handlers
- Troubleshoot Cisco Unity Connection
- Configure Cisco Unity Express
- Troubleshoot Cisco Unity Express
- Configure Cisco Unified Communications Manager IM and Presence High Availability
- Implement Cisco Jabber
- Configure Centralized Cisco Unified Communications Manager IM and Presence
- Configure Cisco Unified Communications Manager IM and Presence Service Functionality
- Enable Message Archiving and Chat Rooms
- Troubleshoot the Cisco Unified Communications IM and Presence Database Connection
- Troubleshoot Cisco Unified Communications Manager IM and Presence High Availability
- Troubleshoot Cisco Unified Communications Manager IM and Presence Service
- Integrate Cisco Unified Attendant Console Advanced
- Implement Call Recording and Monitoring Using a Switched Port Analyzer (SPAN)-based Solution
- Implement Cisco Unified Communications Manager Call Recording and Monitoring

Exam Details

This course leads to the 300-810 - Implementing Cisco Collaboration Applications (CLICA) Exam.

This exam is one of the CCNP Collaboration Certification concentrations exams as well as being the standalone exam for the Cisco Certified Specialist - Collaboration Applications Implementation certification.

skilltec training

Moving forward in knowledge and training

Implementing Cisco Application Centric Infrastructure

Course Code	DCACI
Duration	5 days

Overview

The Implementing Cisco Application Centric Infrastructure (DCACI) v1.0 course show you how to deploy and manage the Cisco® Nexus® 9000 Series Switches in Cisco Application Centric Infrastructure (Cisco ACI®) mode. The course gives you the knowledge and skills to configure and manage Cisco Nexus 9000 Series Switches in ACI mode, how to connect the Cisco ACI fabric to external networks and services, and fundamentals of Virtual Machine Manager (VMM) integration. You will gain hands-on practice implementing key capabilities such as fabric discovery, policies, connectivity, VMM integration, and more.

Audience

The course will help you to gain skills and hands-on practice implementing Cisco Nexus 9000 Series Switches in ACI mode, to prepare for the Implementing Cisco Application Centric Infrastructure (300-620 DCACI) exam, and to qualify for the professional-level and expert-level data center job roles.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing Cisco ACI Fabric Infrastructure and basic Cisco ACI concepts.
- Describing Cisco ACI policy model logical constructs.
- Describing Cisco ACI basic packet forwarding.
- Describing external network connectivity.
- Describing VMM Integration.
- Describing Layer 4 to Layer 7 integrations.
- Explaining Cisco ACI management features.

Pre-Requisites

- Understanding of networking protocols, routing, and switching
- Familiarity with Cisco Ethernet switching products
- Understanding of Cisco data center architecture
- Familiarity with virtualization fundamentals

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- DCFNDU - Understanding Cisco Data Center Foundations

Course Contents

Introducing Cisco ACI Fabric Infrastructure and Basic Concepts

- What Is Cisco ACI?
- Cisco ACI Topology and Hardware
- Cisco ACI Object Model
- Faults, Event Record, and Audit Log
- Cisco ACI Fabric Discovery
- Cisco ACI Access Policies

Describing Cisco ACI Policy Model Logical Constructs

- Cisco ACI Logical Constructs
- Tenant
- Virtual Routing and Forwarding
- Bridge Domain
- Endpoint Group
- Application Profile
- Tenant Components Review
- Adding Bare-Metal Servers to Endpoint Groups
- Contracts

Describing Cisco ACI Basic Packet Forwarding

- Endpoint Learning
- Basic Bridge Domain Configuration ****
- Introducing External Network Connectivity
- Cisco ACI External Connectivity Options
- External Layer 2 Network Connectivity
- External Layer 3 Network Connectivity

Introducing VMM Integration

- VMware vCenter VDS Integration
- Resolution Immediacy in VMM
- Alternative VMM Integrations

Describing Layer 4 to Layer 7 Integrations

- Service Appliance Insertion Without ACI L4-L7 Service Graph
- Service Appliance Insertion via ACI L4-L7 Service Graph
- Service Graph Configuration Workflow
- Service Graph PBR Introduction

Explaining Cisco ACI Management

- Out-of-Band Management
- In-Band Management
- Syslog
- Simple Network Management Protocol
- Configuration Backup
- Authentication, Authorization, and Accounting
- Role-Based Access Control
- Cisco ACI Upgrade
- Collect Tech Support

Labs

- Validate Fabric Discovery
- Configure Network Time Protocol (NTP)
- Create Access Policies and Virtual Port Channel (vPC)
- Enable Layer 2 Connectivity in the Same Endpoint Group (EPG)
- Enable Inter-EPG Layer 2 Connectivity
- Enable Inter-EPG Layer 3 Connectivity
- Compare Traffic Forwarding Methods in a Bridge Domain
- Configure External Layer 2 (L2Out) Connection
- Configure External Layer 3 (L3Out) Connection
- Integrate Application Policy Infrastructure Controller (APIC) With VMware vCenter Using VMware Distributed Virtual Switch (DVS)

Exam Details

This course leads to the 300-620 - Implementing Cisco Application Centric Infrastructure (DCACI) exam.

Successful completion of this exam will earn you the Cisco Certified Specialist – Data Center ACI Implementation certification and will satisfy the concentration exam requirement for new CCNP Data Center certification. To complete CCNP Data Center, you also need to pass the Implementing and Operating Cisco Data Center Core Technologies (350-601 DCCOR) exam or its equivalent.

skilltec training

Moving forward in knowledge and training

Implementing Cisco Application Centric Infrastructure – Advanced

Course Code	DCACIA
Duration	5 days

Overview

The Implementing Cisco Application Centric Infrastructure–Advanced (DCACIA) course shows you how to implement and use the advanced features of the Cisco® Nexus® 9000 Series Switches in Cisco Application Centric Infrastructure (Cisco ACI®) mode. The course gives you the knowledge and skills to understand, configure, and manage Cisco Nexus 9000 Series Switches in ACI mode, how to implement traditional networks in Cisco ACI, and how to implement Cisco ACI Multi-Pod and Multi-Site deployments. You will gain hands-on practice implementing advanced ACI capabilities such as Rogue Endpoint Feature, Transit Routing, VRF Route Leaking, Contracts and Zoning Rules, Policy Based Redirect to Layer 4–7 Service Node, Multi-Pod Fabric and Cisco ACI Multi-Site Orchestrator.

Audience

Engineers looking to learn advanced ACI skills for implementation on the Cisco Nexus 9000 Series Switch running in ACI Mode.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Explaining Cisco ACI advanced fabric packet forwarding.
- Explaining advanced ACI policy and tenant configuration.
- Describing Cisco ACI Multi-Pod deployment.
- Explaining the details and consideration of implementing and integrating traditional network with Cisco ACI.
- Describing Cisco ACI Service Graph Policy-Based Redirect (PBR).
- Describing Cisco ACI Multi-Site deployment.

Pre-Requisites

- Basic understanding of Cisco ACI
- Understanding of Cisco data center architecture
- Familiarity with virtualization fundamentals

Recommended courses:

- DCACI - Implementing Cisco Application Centric Infrastructure

Course Contents

Cisco ACI Advanced Packet Forwarding

- Packet Forwarding Between Leaf Switches
- Endpoint Learning
- Network Interface Card (NIC) Teaming to ACI Fabric
- Endpoint Learning Optimizations
- Endpoint Loop Protection
- Rogue Endpoint Control

Using Advanced Cisco ACI Policy and Tenant Configuration

- Layer 3 Outside Transit Routing
- Using Tenant Common for Shared Services
- Using Virtual Routing and Forwarding (VRF) Route Leaking for Shared Services
- Using Layer 3 Outside configuration policy (L3Out) VRF Route Leaking for Shared Services
- Detailed Contract Architecture with pcTag
- Contract with vzAny
- Contract Preferred Group

Implementing Traditional Network in Cisco ACI

- Integrating Switched Network with Cisco ACI
- Migrating Existing Switched Network to Cisco ACI
- Network- vs. Application-Centric Deployment Models

Cisco ACI Service Graph PBR

- Service Graph PBR Overview
- PBR End-to-End Packet Flow
- Service Graph PBR Requirements and Topologies
- Service Graph PBR Tracking Options

Cisco ACI Multi-Pod Deployment

- Cisco ACI Multi-Pod Overview
- Inter-Pod Network Overview
- Multi-Pod Provisioning and Packet Flow Between Pods
- Connectivity to External L3 Networks
- Service Node Integration Considerations
- Service Graph Considerations

Cisco ACI Multi-Site Deployment

- Cisco ACI Multi-Site Overview
- Cisco ACI Multi-Site Orchestrator
- Inter-Site Network Overview
- Tenant Configuration Deployment from Multi-Site Orchestrator (MSO)
- Packet Flow Between Sites
- Multi-Site Stretched Components
- Multi-Site vs Multi-Pod Comparison

Labs

- Examine Local and Remote Endpoint Learning
- Verify Bounce Entries
- Validate IP Learning
- Mitigate IP and MAC Flapping with the Rogue Endpoint Feature
- Enable Transit Routing
- Implement VRF Route Leaking
- Configure VRF Route Leaking with L3Out
- Examine Contracts and Zoning Rules
- Configure Policy-Based Redirect to Layer 4–7 Service Node
- Deploy Multi-Pod Fabric
- Provision Policies with Cisco ACI Multi-Site Orchestrator

Exam Details

There are no exams currently aligned to this course.

Implementing Automation for Cisco Data Center Solutions

Course Code	DCAUI
Duration	3 days

Overview

The Implementing Automation for Cisco Data Center Solutions (DCAUI) course teaches you how to implement Cisco® Data Center automated solutions including programming concepts, orchestration, and automation tools. Through a combination of lessons and hands-on practice, you will manage the tools and learn the benefits of programmability and automation in the Cisco-powered Data Center. You will examine Cisco Application Centric Infrastructure (Cisco ACI®), software-defined networking (SDN) for data center and cloud networks, Cisco Nexus® (Cisco NX-OS) platforms for device-centric automation, and Cisco Unified Computing System (Cisco UCS®) for Data Center compute.

Study the current ecosystem of application programming interfaces (APIs), software development toolkits, and relevant workflows along with open industry standards, tools, and APIs, such as Python, Ansible, Git, JavaScript Object Notation (JSON), Yaml Ain't Markup Language (YAML), Network Configuration Protocol (NETCONF), Representational State Transfer Configuration Protocol (RESTCONF), and Yet Another Generation (YANG).

Audience

Individuals looking to understand how to implement automated solutions in a Cisco Data Center.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Reviewing Cisco ACI fundamental concepts and GUI workflows, and creating the case for implementing automation.
- Introducing the Cisco ACI REST API, the tools already available on the Cisco Application Policy Infrastructure Controller (APIC), and understanding basic API interaction using Postman
- Understanding the functionality provided by the Python ACI libraries and writing scripts that apply configuration and verify state on the Cisco ACI fabric.
- Understanding Cisco ACI Ansible modules, building playbooks that apply Infrastructure-as-Code concepts to Cisco ACI tenant configuration, and generating a health report using Ansible.
- Understanding Cisco ACI Apps Center integration and the benefits of integrating Kubernetes infrastructure with Cisco ACI.
- Understanding the API types and capabilities available on Cisco Nexus product family.
- Understanding Day 0 operations and how Zero Touch Provisioning (ZTP), PowerOn Auto Provisioning (POAP), and enhanced Pre-boot eXecution Environment (iPXE) fulfill these goals with their respective tooling.
- Understanding functionality provided by the on-box tooling on the Cisco Nexus series switches and implementing simple solutions to improve daily operation.
- Using Python and Ansible to leverage the NX-API to implement and verify configuration state using modern workflows.
- Understanding the paradigm shift of Model-Driven Telemetry and exploring a fully set up pipeline for data collection and analysis.

Pre-Requisites

- Basic programming language concepts
- Basic understanding of virtualization and VMware
- Ability to use Linux and command line interface (CLI) tools, such as Secure Shell (SSH) and bash
- CCNP level data center knowledge
- Foundational understanding of Cisco ACI

Recommended courses:

- DCCOR - Implementing and Operating Cisco Data Center Core Technologies
- DCFNDU - Understanding Cisco Data Center Foundations

Course Contents

- Describing the Cisco ACI Policy Model
- Describing the Cisco APIC REST API
- Using Python to Interact with the ACI REST API
- Using Ansible to Automate Cisco ACI
- Describing Cisco ACI Apps Center and Kubernetes Integration
- Introducing Cisco NX-OS Programmability
- Describing Day-Zero Provisioning with Cisco NX-OS
- Implementing On-Box Programmability and Automation with Cisco NX-OS
- Implementing Off-Box Programmability and Automation with Cisco NX-OS
- Understanding Model-Driven Telemetry
- Automating Cisco UCS Using Developer Tools
- Implementing Workflows Using Cisco UCS Director
- Describing Cisco DCNM
- Describing Cisco Intersight

Exam Details

This course leads to the 300-635 – Automating Cisco Data Center Solutions (DCAUTO) exam.

Successful completion of this exam will earn you the Cisco Certified Specialist – Cisco Certified DevNet Specialist – Data Center Automation and Programmability certification and will satisfy the concentration exam requirements for both the CCNP Data Center certification and the Cisco Certified DevNet Professional certification.

Implementing and Operating Cisco Data Center Core Technologies

Course Code	DCCOR
Duration	5 days

Overview

The Implementing and Operating Cisco Data Center Core Technologies course helps you prepare for the Cisco CCNP Data Center and CCIE Data Center certifications and for advanced-level data center roles. Learn to master the skills and technologies you need to implement data center compute, LAN and SAN infrastructure. Understand the essentials of automation and security in data centers. Gain hands-on experience with deploying, securing, operating, and maintaining Cisco data center infrastructure including: Cisco MDS Switches and Cisco Nexus Switches; Cisco Unified Computing System™ (Cisco UCS®) B-Series Blade Servers, and Cisco UCS C-Series Rack Servers.

This course, including the self-paced material, helps prepare you to take the exam, Implementing Cisco Data Center Core Technologies (350-601 DCCOR), which leads to the new CCNP Data Center, CCIE Data Center, and the Cisco Certified Specialist - Data Center Core certifications.

Audience

Individuals looking for the knowledge and skills required to implement, secure and automate network, compute and storage infrastructures.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Implementing routing and switching protocols in Data Center environment.
- Implementing overlay networks in data center.
- Introducing high-level Cisco Application Centric Infrastructure (Cisco ACI™) concepts and Cisco Virtual Machine manager (VMM) domain integration.
- Describing Cisco Cloud Service and deployment models.
- Implementing Fibre Channel fabric.
- Implementing Fibre Channel over Ethernet (FCoE) unified fabric.
- Implementing security features in data center.
- Implementing software management and infrastructure monitoring.
- Implementing Cisco UCS Fabric Interconnect and Server abstraction.
- Implementing SAN connectivity for Cisco Unified Computing System™ (Cisco UCS®).
- Describing Cisco HyperFlex™ infrastructure concepts and benefits.
- Implementing Cisco automation and scripting tools in data center.
- Evaluating automation and orchestration technologies.

Pre-Requisites

- Familiarity with Ethernet and TCP/IP networking
- Familiarity with SANs
- Familiarity with Fibre Channel protocol
- Identify products in the Cisco Data Center Nexus and Cisco MDS families
- Understanding of Cisco Enterprise Data Center architecture
- Understanding of server system design and architecture
- Familiarity with hypervisor technologies (such as VMware)

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- DCFNDU - Understanding Cisco Data Center Foundations

Course Contents

Implementing Data Center Switching Protocols*

- Spanning Tree Protocol
- Port Channels Overview
- Virtual Port Channels Overview

Implementing First-Hop Redundancy Protocols*

- Hot Standby Router Protocol (HSRP) Overview
- Virtual Router Redundancy Protocol (VRRP) Overview
- First Hop Redundancy Protocol (FHRP) for IPv6

Implementing Routing in Data Center*

- Open Shortest Path First (OSPF) v2 and Open Settlement Protocol (OSP) v3
- Border Gateway Protocol

Implementing Multicast in Data Center*

- IP Multicast in Data Center Networks
- Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD)
- Multicast Distribution Trees and Routing Protocols
- IP Multicast on Cisco Nexus Switches

Implementing Data Center Overlay Protocols

- Cisco Overlay Transport Virtualization
- Virtual Extensible LAN

Implementing Network Infrastructure Security*

- User Accounts and Role Based Access Control (RBAC)
- Authentication, Authorization, and Accounting (AAA) and SSH on Cisco NX-OS
- Keychain Authentication
- First Hop Security
- Media Access Control Security
- Control Plane Policing

Describing Cisco Application-Centric Infrastructure

- Cisco ACI Overview, Initialization, and Discovery
- Cisco ACI Management
- Cisco ACI Fabric Access Policies

Describing Cisco ACI Building Blocks and VMM Domain Integration

- Tenant-Based Components
- Cisco ACI Endpoints and Endpoint Groups (EPG)
- Controlling Traffic Flow with Contracts
- Virtual Switches and Cisco ACI VMM Domains
- VMM Domain EPG Association
- Cisco ACI Integration with Hypervisor Solutions

Describing Packet Flow in Data Center Network*

- Data Center Traffic Flows
- Packet Flow in Cisco Nexus Switches
- Packet Flow in Cisco ACI Fabric

Describing Cisco Cloud Service and Deployment Models

- Cloud Architectures
- Cloud Deployment Models

Describing Data Center Network Infrastructure Management, Maintenance, and Operations*

- Time Synchronization
- Network Configuration Management
- Software Updates
- Network Infrastructure Monitoring

Explaining Cisco Network Assurance Concepts*

- Need for Network Assurance
- Cisco Streaming Telemetry Overview

Implementing Fibre Channel Fabric

- Fibre Channel Basics
- Virtual Storage Area Network (VSAN) Overview
- SAN Port Channels Overview
- Fibre Channel Domain Configuration Process

Implementing Storage Infrastructure Services

- Distributed Device Aliases
- Zoning
- N-Port Identifier Virtualization (NPIV) and N-Port Virtualization (NPV)
- Fibre Channel over IP
- Network Access Server (NAS) Concepts
- Storage Area Network (SAN) Design Options

Implementing FCoE Unified Fabric

- Fibre Channel over Ethernet
- Describing FCoE
- FCoE Topology Options
- FCoE Implementation

Implementing Storage Infrastructure Security*

- User Accounts and RBAC
- Authentication, Authorization, and Accounting
- Fibre Channel Port Security and Fabric Binding

Describing Data Center Storage Infrastructure Maintenance and Operations*

- Time Synchronization
- Software Installation and Upgrade
- Storage Infrastructure Monitoring

Describing Cisco UCS Server Form Factors*

- Cisco UCS B-Series Blade Servers
- Cisco UCS C-Series Rack Servers

Implementing Cisco Unified Computing Network Connectivity

- Cisco UCS Fabric Interconnect
- Cisco UCS B-Series Connectivity
- Cisco UCS C-Series Integration

Implementing Cisco Unified Computing Server Abstraction

- Identity Abstraction
- Service Profile Templates

Implementing Cisco Unified Computing SAN Connectivity

- iSCSI Overview
- Fibre Channel Overview
- Implement FCoE

Implementing Unified Computing Security

- User Accounts and RBAC
- Options for Authentication
- Key Management

Introducing Cisco HyperFlex Systems*

- Hyperconverged and Integrated Systems Overview
- Cisco HyperFlex Solution
- Cisco HyperFlex Scalability and Robustness

Describing Data Center Unified Computing Management, Maintenance, and Operations*

- Compute Configuration Management
- Software Updates
- Infrastructure Monitoring
- Cisco Intersight™

Implementing Cisco Data Center Automation and Scripting Tools*

- Cisco NX-OS Programmability
- Scheduler Overview
- Cisco Embedded Event Manager Overview
- Bash Shell and Guest Shell for Cisco NX-OS
- Cisco Nexus API

Describing Cisco Integration with Automation and Orchestration Software Platforms

- Cisco and Ansible Integration Overview
- Cisco and Puppet Integration Overview
- Python in Cisco NX-OS and Cisco UCS

Describing Cisco Data Center Automation and Orchestration Technologies*

- Power On Auto Provisioning
- Cisco Data Center Network Manager Overview
- Cisco UCS Director Fundamentals
- Cisco UCS PowerTool

***These sections are self-study material that can be done at your own pace after the instructor-led portion of the course.**

Labs

- Configure Overlay Transport Visualization (OTV)
- Configure Virtual Extensible LAN (VXLAN)
- Explore the Cisco ACI Fabric
- Implement Cisco ACI Access Policies and Out-of-Band Management
- Implement Cisco ACI Tenant Policies
- Integrate Cisco ACI with VMware
- Configure Fibre Channel
- Configure Device Aliases
- Configure Zoning
- Configure NPV
- Configure FCoE
- Provision Cisco UCS Fabric Interconnect Cluster
- Configure Server and Uplink Ports
- Configure VLANs
- Configure a Cisco UCS Server Profile Using Hardware Identities
- Configure Basic Identity Pools
- Configure a Cisco UCS Service Profile Using Pools
- Configure an Internet Small Computer Systems Interface (iSCSI) Service Profile
- Configure Cisco UCS Manager to Authenticate Users with Microsoft Active Directory
- Program a Cisco Nexus Switch with Python

Exam Details

This course leads to the 300-601 - Implementing Cisco Data Center Core Technologies (DCCOR) exam.

Successful completion of this exam will earn you the Cisco Certified Specialist - Data Center Core Certification and count towards the New CCNP Data Center Certification - To achieve the new CCNP Data Center Certification you will also need a CCNP Data Center concentration.

Understanding Cisco Data Center Foundations

Course Code	DCFNDU
Duration	5 days

Overview

The Understanding Cisco Data Center Foundations (DCFNDU) v1.0 course helps you prepare for entry-level data center roles. In this course, you will learn the foundational knowledge and skills you need to configure Cisco® data center technologies including: networking, virtualization, storage area networking, and unified computing. You will get an introduction to Cisco Application Centric Infrastructure (Cisco ACI), automation and cloud computing. You will get hands-on experience with configuring features on Cisco Nexus Operating System (Cisco NX-OS) and Cisco Unified Computing System (Cisco UCS).

Audience

Individuals who want to:

- Prepare for entry-level job roles in the high-demand area of data center environments.
- Prepare for courses that support the Cisco Certified Network Professional Data Center certification exams.
- Gain knowledge and hands-on skills through Cisco's unique combination of lessons and hands-on practice using enterprise-grade Cisco learning technologies, data center equipment, and software.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the foundations of data center networking.
- Describing Cisco Nexus products and explaining the basic Cisco NX-OS functionalities and tools.
- Describing Layer 3 first-hop redundancy.
- Describing Cisco FEX connectivity.
- Describing Ethernet port channels and vPCs.
- Introducing switch virtualization, machine virtualization, and describing network virtualization.
- Comparing storage connectivity options in the data center.
- Describing Fibre Channel communication between the initiator server and the target storage.
- Describing Fibre Channel zone types and their uses.
- Describing NPV and NPIV.
- Describing data center Ethernet enhancements that provide a lossless fabric.
- Describing FCoE.
- Describing data center server connectivity.
- Describing Cisco UCS Manager.
- Describing the purpose and advantages of APIs.
- Describing Cisco ACI.
- Describing the basic concepts of cloud computing.

Pre-Requisites

- Good understanding of networking protocols
- Good understanding of the VMware environment
- Basic knowledge of Microsoft Windows operating systems

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions

Course Contents

Describing the Data Center Network Architectures

- Cisco Data Center Architecture Overview
- Three-Tier Network: Core, Aggregation, and Access
- Spine-and-Leaf Network
- Two-Tier Storage Network

Describing the Cisco Nexus Family and Cisco NX-OS Software

- Cisco Nexus Data Center Product Overview
- Cisco NX-OS Software Architecture
- Cisco NX-OS Software CLI Tools
- Cisco NX-OS Virtual Routing and Forwarding

Describing Layer 3 First-Hop Redundancy

- Default Gateway Redundancy
- Hot Standby Router Protocol
- Virtual Router Redundancy Protocol
- Gateway Load Balancing Protocol

Describing Cisco FEX

- Server Deployment Models
- Cisco FEX Technology
- Cisco FEX Traffic Forwarding
- Cisco Adapter FEX

Describing Port Channels and vPCs

- Ethernet Port Channels
- Virtual Port Channels
- Supported vPC Topologies

Describing Switch Virtualization

- Cisco Nexus Switch Basic Components
- Virtual Routing and Forwarding
- Cisco Nexus 7000 VDCs
- VDC Types
- VDC Resource Allocation
- VDC Management

Describing Machine Virtualization

- Virtual Machines
- Hypervisor
- VM Manager

Describing Network Virtualization

- Overlay Network Protocols
- VXLAN Overlay
- VXLAN BGP EVPN Control Plane
- VXLAN Data Plane
- Cisco Nexus 1000VE Series Virtual Switch
- VMware vSphere Virtual Switches

Introducing Basic Data Center Storage Concepts

- Storage Connectivity Options in the Data Center
- Fibre Channel Storage Networking
- VSAN Configuration and Verification

Describing Fibre Channel Communication Between the Initiator Server and the Target Storage

- Fibre Channel Layered Model
- FLOGI Process
- Fibre Channel Flow Control

Describing Fibre Channel Zone Types and Their Uses

- Fibre Channel Zoning
- Zoning Configuration
- Zoning Management

Describing Cisco NPV Mode and NPIV

- Cisco NPV Mode
- NPIV Mode

Describing Data Center Ethernet Enhancements

- IEEE Data Center Bridging
- Priority Flow Control
- Enhanced Transmission Selection
- DCBX Protocol
- Congestion Notification

Describing FCoE

- Cisco Unified Fabric
- FCoE Architecture
- FCoE Initialization Protocol
- FCoE Adapters

Describing Cisco UCS Components

- Physical Cisco UCS Components
- Cisco Fabric Interconnect Product Overview
- Cisco IOM Product Overview
- Cisco UCS Mini
- Cisco IMC Supervisor
- Cisco Intersight

Describing Cisco UCS Manager

- Cisco UCS Manager Overview
- Identity and Resource Pools for Hardware Abstraction
- Service Profiles and Service Profile Templates
- Cisco UCS Central Overview
- Cisco HyperFlex Overview
- Using APIs
- Common Programmability Protocols and Methods
- How to Choose Models and Processes

Describing Cisco ACI

- Cisco ACI Overview
- Multitier Applications in Cisco ACI
- Cisco ACI Features
- VXLAN in Cisco ACI
- Unicast Traffic in Cisco ACI
- Multicast Traffic in Cisco ACI
- Cisco ACI Programmability
- Common Programming Tools and Orchestration Options

Describing Cloud Computing

- Cloud Computing Overview
- Cloud Deployment Models
- Cloud Computing Services

Labs

- Explore the Cisco NX-OS CLI
- Explore Topology Discovery
- Configure HSRP
- Configure the Cisco Nexus 2000 FEX
- Configure vPCs
- Configure vPCs with Cisco FEX
- Configure VRF
- Explore the VDC Elements
- Install VMware ESXi and vCenter
- Configure VSANs
- Validate FLOGI and FCNS
- Configure Zoning
- Configure Unified Ports on a Cisco Nexus Switch and Implement FCoE
- Explore the Cisco UCS Server Environment
- Configure a Cisco UCS Server Profile
- Configure Cisco NX-OS with APIs
- Explore the Cisco UCS Manager XML API Management Information Tree

Exam Details

There are no exams currently aligned to this course.

Designing Cisco Data Center Infrastructure

Course Code	DCID
Duration	5 days

Overview

The Designing Cisco Data Center Infrastructure (DCID) v7.0 course helps you master design and deployment options focused on Cisco® data center solutions and technologies across network, compute, virtualization, storage area networks, automation, and security. You will learn design practices for the Cisco Unified Computing System™ (Cisco UCS®) solution based on Cisco UCS B-Series and C-Series servers, Cisco UCS Manager, and Cisco Unified Fabric. You will also gain design experience with network management technologies including Cisco UCS Manager, Cisco Data Center Network Manager (DCNM), and Cisco UCS Director. You can expect theoretical content as well as design-oriented case studies in the form of activities.

Audience

Engineers and Architects involved in the design of a Cisco Data Center or Cisco Data Center Solution.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the Layer 2 and Layer 3 forwarding options and protocols used in a data center.
- Describing the rack design options, traffic patterns, and data center switching layer access, aggregation, and core.
- Describing the Cisco Overlay Transport Virtualization (OTV) technology that is used to interconnect data centers.
- Describing Locator/ID separation protocol.
- Designing a solution that uses Virtual Extensible LAN (VXLAN) for traffic forwarding.
- Describing hardware redundancy options; how to virtualize the network, compute, and storage functions; and virtual networking in the data center.
- Describing solutions that use fabric extenders and compare Cisco Adapter Fabric Extender (FEX) with single root input/output virtualization (SR-IOV).
- Describing security threats and solutions in the data center.
- Describing advanced data center security technologies and best practices.
- Describing device management and orchestration in the data center.
- Describing the storage options for compute function and different Redundant Array of Independent Disks (RAID) levels from a high-availability and performance perspective.
- Describing Fibre Channel concepts, topologies, architecture, and industry terms.
- Describing Fibre Channel over Ethernet (FCoE).
- Describing security options in the storage network.
- Describing management and automation options for storage networking infrastructure.
- Describing Cisco UCS servers and use cases for various Cisco UCS platforms.
- Explaining the connectivity options for fabric interconnects for southbound and northbound connections.
- Describing the hyperconverged solution and integrated systems.
- Describing the systemwide parameters for setting up a Cisco UCS domain.
- Describing role-based access control (RBAC) and integration with directory servers to control access rights on Cisco UCS Manager.
- Describing the pools that may be used in service profiles or service profile templates on Cisco UCS Manager.

- Describing the different policies in the service profile.
- Describing the Ethernet and Fibre Channel interface policies and additional network technologies.
- Describing the advantages of templates and the difference between initial and updated templates.
- Describing data center automation tools.

Pre-Requisites

Attended courses of has existing equivalent knowledge of:

- CCNA Routing and Switching or the new CCNA
- CCNA Data Center or DCFNDU - Understanding Cisco Data Center Foundations
- DCCOR - Implementing Cisco Data Center Core Technologies

Recommended courses:

- DCCOR - Implementing and Operating Cisco Data Center Core Technologies

Course Contents

Describing High Availability on Layer 2

- Overview of Layer 2 High-Availability Mechanisms
- Virtual Port Channels
- Cisco FabricPath
- Virtual Port Channel+

Designing Layer 3 Connectivity

- First Hop Redundancy Protocols
- Improve Routing Protocol Performance and Security
- Enhance Layer 3 Scalability and Robustness

Designing Data Center Topologies

- Data Center Traffic Flows
- Cabling Challenges
- Access Layer
- Aggregation Layer
- Core Layer
- Spine-and-Leaf Topology
- Redundancy Options

Designing Data Center Interconnects with Cisco OTV

- Cisco OTV Overview
- Cisco OTV Control and Data Planes
- Failure Isolation
- Cisco OTV Features
- Optimize Cisco OTV
- Evaluate Cisco OTV

Describing Locator/ID Separation Protocol

- Locator/ID Separation Protocol
- Location Identifier Separation Protocol (LISP) Virtual Machine (VM) Mobility
- LISP Extended Subnet Mode (ESM) Multihop Mobility
- LISP VPN Virtualization

Describing VXLAN Overlay Networks

- Describe VXLAN Benefits over VLAN
- Layer 2 and Layer 3 VXLAN Overlay
- Multiprotocol Border Gateway Protocol (MP-BGP) Ethernet VPN (EVPN) Control Plane Overview
- VXLAN Data Plane

Describing Hardware and Device Virtualization

- Hardware-Based High Availability
- Device Virtualization
- Cisco UCS Hardware Virtualization
- Server Virtualization
- SAN Virtualization
- N-Port ID Virtualization

Describing Cisco FEX Options

- Cisco Adapter FEX
- Access Layer with Cisco FEX
- Cisco FEX Topologies
- Virtualization-Aware Networking
- Single Root I/O Virtualization
- Cisco FEX Evaluation

Describing Basic Data Center Security

- Threat Mitigation
- Attack and Countermeasure Examples
- Secure the Management Plane
- Protect the Control Plane
- RBAC and Authentication, Authorization, and Accounting (AAA)

Describing Advanced Data Center Security

- Cisco TrustSec in Cisco Secure Enclaves Architecture
- Cisco TrustSec Operation
- Firewalling
- Positioning the Firewall Within Data Center Networks
- Cisco Firepower® Portfolio
- Firewall Virtualization
- Design for Threat Mitigation

Describing Management and Orchestration

- Network and License Management
- Cisco UCS Manager
- Cisco UCS Director
- Cisco Intersight
- Cisco DCNM Overview

Describing Storage and RAID Options

- Position DAS in Storage Technologies
- Network-Attached Storage
- Fibre Channel, FCoE, and Internet Small Computer System Interface (iSCSI)
- Evaluate Storage Technologies

Describing Fibre Channel Concepts

- Fibre Channel Connections, Layers, and Addresses
- Fibre Channel Communication
- Virtualization in Fibre Channel SAN

Describing Fibre Channel Topologies

- SAN Parameterization
- SAN Design Options
- Choosing a Fibre Channel Design Solution

Describing FCoE

- FCoE Protocol Characteristics
- FCoE Communication
- Data Center Bridging
- FCoE Initialization Protocol
- FCoE Design Options

Describing Storage Security

- Common SAN Security Features
- Zones
- SAN Security Enhancements
- Cryptography in SAN

Describing SAN Management and Orchestration

- Cisco DCNM for SAN
- Cisco DCNM Analytics and Streaming Telemetry
- Cisco UCS Director in the SAN
- Cisco UCS Director Workflows

Describing Cisco UCS Servers and Use Cases

- Cisco UCS C-Series Servers
- Fabric Interconnects and Blade Chassis
- Cisco UCS B-Series Server Adapter Cards
- Stateless Computing
- Cisco UCS Mini

Describing Fabric Interconnect Connectivity

- Use of Fabric Interconnect Interfaces
- VLANs and VSANs in a Cisco UCS Domain
- Southbound Connections
- Northbound Connections
- Disjoint Layer 2 Networks
- Fabric Interconnect High Availability and Redundancy

Describing Hyperconverged and Integrated Systems

- Hyperconverged and Integrated Systems Overview
- Cisco HyperFlex™ Solution
- Cisco HyperFlex Scalability and Robustness
- Cisco HyperFlex Clusters
- Cluster Capacity and Multiple Clusters on One Cisco UCS Domain
- External Storage and Graphical Processing Units on Cisco HyperFlex
- Cisco HyperFlex Positioning

Describing Cisco UCS Manager Systemwide Parameters

- Cisco UCS Setup and Management
- Cisco UCS Traffic Management

Describing Cisco UCS RBAC

- Roles and Privileges
- Organizations in Cisco UCS Manager
- Locales and Effective Rights
- Authentication, Authorization, and Accounting
- Two-Factor Authentication

Describing Pools for Service Profiles

- Global and Local Pools
- Universally Unique Identifier (UUID) Suffix and Media Access Control (MAC) Address Pools
- World Wide Name (WWN) Pools
- Server and iSCSI Initiator IP Pools

Describing Network-Specific Adapters and Policies

- LAN Connectivity Controls
- SAN Connectivity Controls
- Virtual Access Layer
- Connectivity Enhancements

Describing Templates in Cisco UCS Manager

- Cisco UCS Templates
- Service Profile Templates
- Network Templates
- Designing Data Center Automation

Model-Driven Programmability

- Cisco NX-API Overview
- Programmability Using Python
- Cisco Ansible Module
- Use the Puppet Agent

Labs

- Design Virtual Port Channels
- Design First Hop Redundancy Protocol (FHRP)
- Design Routing Protocols
- Design Data Center Topology for a Customer
- Design Data Center Interconnect Using Cisco OTV
- Design Your VXLAN Network
- Create a Cisco FEX Design
- Design Management and Orchestration in a Cisco UCS Solution
- Design a Fibre Channel Network
- Design and Integrate an FCoE Solution
- Design a Secure SAN
- Design Cisco UCS Director for Storage Networking
- Design a Cisco UCS Domain and Fabric Interconnect Cabling
- Design a Cisco UCS C-Series Server Implementation
- Design Cisco UCS Fabric Interconnect Network and Storage Connectivity
- Design Systemwide Parameters in a Cisco UCS Solution
- Design an LDAP Integration with a Cisco UCS Domain
- Design Pools for Service Profiles in a Cisco UCS Solution
- Design Network-Specific Adapters and Policies in a Cisco UCS Solution

Exam Details

This course leads to the 300-610 - Designing Cisco Data Center Infrastructure (DCID) exam.

This is one of the concentration exams for the NEW CCNP Data Center Certification; to achieve the New CCNP Data Center Certification you will also need to take the 300-601 exam.

skilltec training

Moving forward in knowledge and training

Troubleshooting Cisco Data Center Infrastructure

Course Code	DCIT
Duration	5 days

Overview

Troubleshooting Cisco Data Center Infrastructure is a skills-building course focused on the troubleshooting of LAN, SAN, Cisco Data Center Unified Fabric, Cisco Unified Computing System (UCS), and Cisco Application Centric Infrastructure (ACI). The course provides rich, hands-on experience in resolving problems on Cisco MDS switches, Cisco Nexus switches, Cisco fabric extenders (FEXs), Cisco UCS and Cisco ACI.

The course is designed to help students prepare for Cisco CCNP Data Center certification and for professional-level data center roles.

Virtual and Classroom learning - V&C Select™

V&C Select™ is a simple concept and a flexible approach to delivery. You can 'select' a course from our public schedule and attend in person or as a virtual delegate. Virtual delegates do not travel to this course, we will send you all the information you need before the start of the course and you can test the logins.

Audience

Engineers involved in the troubleshooting of LAN, SAN, Cisco Data Center Unified Fabric, Cisco Unified Computing System (UCS) and Cisco Application Centric Infrastructure (ACI).

Learning Objectives

By actively participating in this course, you will learn about the following:

- Outlining the troubleshooting process and highlighting which questions to ask.
- Describing the troubleshooting tools and methodologies that are available from the CLI and are used to identify and resolve issues in a Cisco Data Center network architecture.
- Identifying and resolving issues related to VLANs and PVLANs.
- Identifying and resolving issues related to port channels and virtual port channels.
- Identifying and resolving issues related to Cisco FabricPath.
- Identifying and resolving issues related to OTV.
- Identifying and resolving issues related to VXLAN.
- Identifying and resolving issues related to LISP.
- Describing troubleshooting of routing protocols, such as OSPF, ISIS, and PIM.
- Describing troubleshooting of the AAA and RBAC.
- Identifying and resolving issues related to a single device.
- Identifying and resolving issues related to Fibre Channel interface operation.
- Identifying and resolving issues related to Fibre Channel switching when the Cisco NX-OS software switch is used in switched mode (vs. NPV mode).
- Identifying and resolving issues related to Fibre Channel switching when the NX-OS switch is used in N Port Virtualization (NPV) mode.
- Identifying and resolving issues related to FIP and FCoE, including FCoE performance.
- Describing Cisco UCS architecture, initial setup, tools and service aids that are available for Cisco UCS troubleshooting and interpretation of the output.
- Describing Cisco UCS configuration and troubleshoot related issues.
- Describing Cisco UCS B-Series operation and troubleshoot related issues.

- Describing LAN, SAN and Fibre Channel operations, including in depth troubleshooting procedures.
- Describing Cisco IMC utilities to validate performance and facilitate data-gathering activities for Cisco UCS C-Series troubleshooting, as well troubleshooting approach to hardware and firmware failures.
- Defining proper procedures to configure LAN and SAN connectivity and avoid issues with the P81E virtual interface card (VIC).
- Troubleshooting integration of Cisco UCS C-Series servers with Cisco UCS Manager.
- Identifying tools, protocols and methods to effectively troubleshoot Cisco ACI.

Pre-Requisites

Attended courses of has existing equivalent knowledge of:

- DCICN - Introducing Cisco Data Center Networking
- DCICT - Introducing Cisco Data Center Technologies
- DCII - Implementing Cisco Data Center Infrastructure
- DCVAI - Implementing Cisco Data Center Virtualization and Automation
- DCUCI - Implementing Cisco Data Center Unified Computing

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- DCFNDU - Understanding Cisco Data Center Foundations
- DCCOR - Implementing and Operating Cisco Data Center Core Technologies

Course Contents

Troubleshooting the Data Center LAN Network

- Overview of the Troubleshooting Process
- Understanding CLI Troubleshooting Tools
- Troubleshooting VLANs and Private VLANs
- Troubleshooting Port Channels and Virtual Port Channels
- Troubleshooting Cisco FabricPath
- Troubleshooting Cisco OTV
- Troubleshooting VXLAN
- Troubleshooting LISP
- Troubleshooting Routing Protocols
- Troubleshooting Data Center LAN Security
- Troubleshooting Platform-Specific Issues

Troubleshooting Data Center SAN

- Troubleshooting Fibre Channel Interfaces
- Troubleshooting Fibre Channel Fabric Service
- Troubleshooting NPV Mode
- Troubleshooting FCoE

Troubleshooting Data Center Unified Computing

- Troubleshooting Cisco UCS Architecture and Initialization
- Troubleshooting Cisco UCS Configuration
- Troubleshooting Cisco UCS B-Series Servers
- Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity
- Troubleshooting Cisco UCS C-Series Servers
- Troubleshooting Cisco UCS C-Series LAN and SAN Connectivity
- Troubleshooting Cisco UCS C-Series and Cisco UCS Manager Integration

Troubleshooting Data Center ACI

- Exploring the Tools and Methodology of Troubleshooting Cisco ACI

Labs

- Document the Network Baseline
- Troubleshoot LAN-RSTP
- Troubleshoot LAN-LACP
- Learning Lab: Troubleshoot LAN-vPC
- Troubleshoot LAN-FabricPath
- Troubleshoot LAN-OTV
- Troubleshoot LAN-OSPF
- Troubleshoot LAN-FHRP
- Troubleshoot LAN-VRF
- Troubleshoot LAN-VXLAN
- Troubleshoot LAN-CFS
- Troubleshoot LAN-FEX
- Troubleshoot SAN-FC Interfaces
- Troubleshoot SAN-FC VSANs, Zones, and Domain Services
- Troubleshoot SAN-NPV Mode
- Troubleshoot SAN-FCoE
- Troubleshoot SAN-DCB
- Troubleshoot Compute-Cisco UCS Management and Service Profile Deployment
- Troubleshoot Compute-Cisco UCS C-Series Server Boot from SAN
- Troubleshoot Compute-LAN Connectivity, Part 1
- Troubleshoot Compute-LAN Connectivity, Part 2
- Troubleshoot Compute-Cisco UCS C-Series Server Boot from SAN
- Troubleshoot Compute-Network Connectivity
- Troubleshoot ACI-Bare Metal Hosts
- Troubleshoot ACI-VMM
- Troubleshoot ACI-Contracts
- Troubleshoot ACI-External Layer 3
- Troubleshoot ACI-External Layer 2

Exam Details

This course leads to the 300-180 Troubleshooting Cisco Data Center Infrastructure (DCIT) exam; this is one of the four exams required to earn the Cisco CCNP Data Centre certification. Other exams required:

- Implementing Cisco Data Center Unified Computing (DCUCI)
- Implementing Cisco Data Center Infrastructure (DCII)
- Implementing Cisco Data Center Virtualization and Automation (DCVAI)

Configuring Cisco MDS 9000 Switches

Course Code	DCMDS
Duration	4 days

Overview

The Configuring Cisco MDS 9000 Series Switches course shows you how to implement, manage and troubleshoot Cisco MDS 9000 Series Switches, to build highly available, scalable storage networks. You will learn how to deploy and use capabilities such as virtual storage area networks (VSANs), Role-Based Access Control (RBAC), N-Port Virtualization (NPV) fabric security, zoning, automation with NX-API, Slow Drain Analysis, Fibre Channel over TCP/IP (FCIP) tunnels and more. You will learn how to configure and implement platform features and learn troubleshooting techniques pertaining to Fibre Channel (FC) domains, firmware upgrades, zones and zone mergers.

This course will help you:

- Learn how to deploy and troubleshoot the Cisco Nexus® 9000 Series Switches to support performance, resiliency, scalability, and enhanced operations for data centers.
- Gain knowledge and skills through Cisco's unique combination of lessons and hands-on practice using enterprise-grade Cisco learning technologies, data center equipment, and software.
- Succeed in today's demanding data center operations roles.
- Earn 40 CE credits toward recertification.

This course prepares you for Cisco CCNP Data Center and Cisco Certified Specialist - Data Center SAN Implementation certifications.

Audience

Engineers involved in the implementation of a storage-networking solution incorporating the Cisco MDS 9000 Series Switch platform.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Discovering and describing the Cisco Multilayer Director Switch (MDS) platform of multilayer switches and directors. Describing the MDS hardware, NX-OS operating system, Data Center Network Manager (DCNM) management software and key architectures of the platform, such as FC and Fibre Channel over Ethernet (FCoE).
- Describing key product features of the MDS platform, including VSANs, RBAC, NPV, port channels, zoning, device aliases, Interactive Voice Response (IVR) and fabric security.
- Describing and implementing state-of-the-art product features.
- Configuring and implementing the Cisco MDS switches and platform features, such as initial configuration, building a fabric, building a SAN extension and configuring inter-VSAN routing for that purpose.
- Configuring FCIP tunnels.
- Resolving issues and troubleshooting FC domains, zones and zone merges, switch boot and firmware upgrades.

Pre-Requisites

- Basic understanding of data storage hardware components and protocols, including Small Computer System Interface(SCSI) and Fibre Channel
- Basic understanding of network protocols, including Ethernet and IP
- Basic routing and switching knowledge

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- DCFNDU - Understanding Cisco Data Center Foundations

Course Contents

Describing Cisco MDS Platform

- Cisco MDS 9700/9300/9200/9100 Hardware
- 32-Gb Fibre Channel
- Cisco NX-OS
- Cisco DCNM
- Fibre Channel Architecture
- FCoE Architecture

Provisioning Cisco MDS Switches

- Power-On Auto-Provisioning
- Cisco DCNM
- Using Cisco DCNM 11.x
- RBAC and Authentication, Authorization, and Accounting (AAA)

Building the Fibre Channel Fabric with Cisco MDS Switches

- Virtual SANs
- Port Channels and VSAN Trunking
- Zoning and Smart Zoning
- Device Aliases
- Inter-VSAN Routing
- Fibre Channel Fabric Security
- Building SAN Extensions
- Inter-VSAN Routing
- Slow Drain Analysis
- SAN Analytics and Telemetry Streaming
- Cisco Secure Boot
- NPV and NPIV

Automating Cisco MDS Fabric

- Cisco MDS NX_APIPython API
- Ansible

Monitoring and Reporting Cisco MDS Features

- Cisco DCNM SAN Reports and Alarms
- SAN Analytics and SAN Telemetry Streaming

Troubleshooting Common Cisco MDS Issues

- Troubleshooting Fibre Channel Domains, Zones and Zone Merges
- Boot and Upgrade Issues

Labs

- Set Up DCNM
- Explore DCNM-SAN Client and DCNM Device Manager
- Configure and Use RBAC
- Configure and Use RBAC with DCNM-SAN Client and Device Manager
- Manage VSANs and Fibre Channel Domain
- Configure NPV and N-Port Identification Virtualization (NPIV)
- Configure Interfaces
- Configure Device Aliases and Zoning
- Explore and Automate with NX-API
- Perform Slow Drain Analysis with Cisco DCNM
- Configure SAN Analysis and SAN Telemetry Streaming
- Configure FCIP Tunnels and FCIP High Availability
- Configure IVR for SAN Extension
- Troubleshoot Zoning and Zone Merges

Exam Details

This course leads to the 300-625 - Implementing Cisco Storage Area Networking (DCSAN) exam.

This exam is one of the concentrations for the new Cisco CCNP Data Center Certification; successful completion will earn you the Cisco Certified Specialist - Data Center SAN Implementation certification.

Implementing Cisco Enterprise Advanced Routing and Services

Course Code	ENARSI
Duration	5 days

Overview

The Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) provides you with the knowledge you need to install, configure, operate, and troubleshoot an enterprise network. This course covers advanced routing and infrastructure technologies, expanding on the topics covered in the Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) course.

This course helps prepare you to take the exam, Implementing Cisco Enterprise Advanced Routing and Services (300-410 ENARSI), which leads to the new CCNP® Enterprise and Cisco Certified Specialist – Enterprise Advanced Infrastructure Implementation certifications.

Audience

Network professionals who need to install, configure, operate and troubleshoot an enterprise network using advanced routing and infrastructure technologies.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Configuring classic EIGRP and named EIGRP for IPv4 and IPv6.
- Optimizing classic EIGRP and named EIGRP for IPv4 and IPv6.
- Troubleshooting classic EIGRP and named EIGRP for IPv4 and IPv6.
- Configuring OSPFv2 and OSPFv3 in IPv4 and IPv6 environments.
- Optimizing OSPFv2 and OSPFv3 behavior.
- Troubleshooting OSPFv2 for IPv4 and OSPFv3 for IPv4 and IPv6.
- Implementing route redistribution using filtering mechanisms.
- Troubleshooting redistribution.
- Implementing path control using PBR and IP SLA.
- Configuring MP-BGP in IPv4 and IPv6 environments.
- Optimizing MP-BGP in IPv4 and IPv6 environments.
- Troubleshooting MP-BGP for IPv4 and IPv6.
- Describe the features of MPLS.
- Describe the major architectural components of an MPLS VPN.
- Identify the routing and packet forwarding functionalities for MPLS VPNs.
- Explain how packets are forwarded in an MPLS VPN environment.
- Implement Cisco IOS DMVPNs.
- Implement DHCP.
- Describe the tools available to secure the IPV6 first hop.
- Troubleshoot Cisco router security features.
- Troubleshoot infrastructure security and services.

Pre-Requisites

- General understanding of network fundamentals - CCNA or ENCOR recommended
- Basic knowledge of how to implement LANs - CCNA or ENCOR recommended
- General understanding of how to manage network devices - CCNA or ENCOR recommended
- General understanding of how to secure network devices- CCNA or ENCOR recommended
- Basic knowledge of network automation - CCNA or ENCOR

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- ENCOR - Implementing and Operating Cisco Enterprise Network Core Technologies

Course Contents

- Implementing EIGRP
- Optimizing EIGRP
- Troubleshooting EIGRP
- Implementing OSPF
- Optimizing OSPF
- Troubleshooting OSPF
- Implementing IBGP
- Optimizing BGP
- Implementing MP-BGP
- Troubleshooting BGP
- Configuring Redistribution
- Troubleshooting Redistribution
- Implementing Path Control
- Exploring MPLS
- Introducing MPLS L3 VPN Architecture
- Introducing MPLS L3 VPN Routing
- Configuring VRF-Lite
- Implementing DMVPN
- Implementing DHCP
- Troubleshooting DHCP
- Introducing IPv6 First Hop Security
- Securing Cisco Routers
- Troubleshooting Infrastructure Security and Services

Labs

- Configure EIGRP Using Classic Mode and Named Mode for IPv4 and IPv6
- Verify the EIGRP Topology Table
- Configure EIGRP Stub Routing, Summarization, and Default Routing
- Configure EIGRP Load Balancing and Authentication
- LAB: Troubleshoot EIGRP Issues
- Configure OSPFv3 for IPv4 and IPv6
- Verify the Link-State Database
- Configure OSPF Stub Areas and Summarization
- Configure OSPF Authentication
- Troubleshoot OSPF
- Implement Routing Protocol Redistribution
- Manipulate Redistribution
- Manipulate Redistribution Using Route Maps
- Troubleshoot Redistribution Issues
- Implement PBR
- Configure IBGP and EBGP
- Implement BGP Path Selection
- Configure BGP Advanced Features
- Configure BGP Route Reflectors
- Configure MP-BGP for IPv4 and IPv6
- Troubleshoot BGP Issues
- Implement PBR
- Configure Routing with VRF-Lite
- Implement Cisco IOS DMVPN
- Obtain IPv6 Addresses Dynamically
- Troubleshoot DHCPv4 and DHCPv6 Issues
- Troubleshoot IPv4 and IPv6 ACL Issues
- Configure and Verify Control Plane Policing
- Configure and Verify uRPF
- Troubleshoot Network Management Protocol Issues: Lab 1
- Troubleshoot Network Management Protocol Issues: Lab 2

Exam Details

This course leads to the 300-410 Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) exam.

Implementing Automation for Cisco Enterprise Solutions

Course Code	ENAUI
Duration	3 days

Overview

Implementing Automation for Cisco Enterprise Solutions (ENAUI) v.1.2 teaches you how to implement Cisco Enterprise automated solutions, including programming concepts, orchestration, telemetry, and automation tools.

This course highlights the tools and the benefits of leveraging programmability and automation in the Cisco-powered Enterprise Campus and WAN. You will also examine platforms including IOS XE software for device-centric automation, Cisco DNA Center for the intent-based enterprise network, Cisco Software-Defined WAN, and Cisco Meraki. Their current ecosystem of APIs, software development toolkits, and relevant workflows are studied in detail together with open industry standards, tools, and APIs, such as Python, Ansible, Git, JSON/YAML, NETCONF/RESTCONF, and YANG.

This course will help you:

- Gain high-demand skills using modern programming languages, APIs, and systems such as Python, Ansible, and Git to automate, streamline, and enhance business operations.
- Acquire the skills and knowledge to customize tools, methods, and processes that improve network performance and agility.
- Earn 24 CE credits toward recertification.

Audience

Network engineers who need to use modern programming, automation and orchestration tools such as Python, Ansible and Git to automate, streamline and enhance their Cisco enterprise network.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Getting familiar with different API styles (REST, RPC) and synchronous and asynchronous API requests.
- Learning how to use Postman software development tool in order to test the API calls.
- Learning how to automate repetitive tasks using Ansible automation engine.
- Exploring a Python programming language, Python libraries and Python virtual environments and learn how can they be used for automation of network configuration tasks.
- Getting introduced to GIT version control system and its common operations.
- Learnng how to leverage the various models and APIs of the Cisco IOS XE platform to perform day-zero operations, improving troubleshooting methodologies with custom tools, augmenting the CLI using scripts, and integrating various workflows using Ansible and Python.
- Learning about the paradigm shift of model-driven telemetry and the building blocks of a working solution.
- Learning how to leverage the tools and APIs to automate Cisco DNA infrastructure managed by Cisco DNA Center™.
- Demonstrating workflows (configuration, verification, health checking, and monitoring) using Python, Ansible, and Postman.

- Understanding Cisco SD-WAN solution components, implementing a Python library that works with the Cisco SD-WAN APIs to perform configuration, inventory management, and monitoring tasks, and implement reusable Ansible roles to automate provisioning new branch sites on an existing Cisco SD-WAN infrastructure.
- Learning how to leverage the tools and APIs to automate Cisco Meraki managed infrastructure and demonstrate workflows (configuration, verification, health checking, monitoring) using Python, Ansible, and Postman.

Pre-Requisites

- Basic programming language concepts
- Basic understanding of virtualization
- Ability to use Linux and CLI tools, such as Secure Shell (SSH) and bash
- Networking knowledge equivalent to the CCNP level
- Foundational understanding of Cisco DNA, Meraki, and Cisco SD-WAN

Recommended courses:

- ENCOR - Implementing and Operating Cisco Enterprise Network Core Technologies

Course Contents

Network Programmability Foundation

- Version Control with GIT
- Introduction to Network-Based APIs
- Characteristics of API styles (REST and RPC)
- Synchronous and Asynchronus API Requests
- Python Fundamentals
- Python Modules
- Introduction to Ansible for Network Automation
- Cisco DevNet Resources

Automating APIs and Protocols

- JavaScript Object Notation
- Extensible Markup Language
- YAML Data Serialization Standard
- Introduction to YANG
- Types of YANG Models
- Introduction to NETCONF
- Introduction to RESTCONF
- Postman for REST API Consumption

Managing Configuration with Python and Ansible

- Enterprise LAN Network Automations Overview

Implementing On-Box Programmability and Automation with Cisco IOS XE Software

- Introduction to Programmability Features on Cisco IOS XE

Implementing Model-Driven Telemetry

- Data Models on Cisco IOS XE Software
- Streaming Telemetry
- Streaming Telemetry Models
- Streaming Telemetry Transport Protocols

Day-Zero Provisioning with Cisco IOS-XE

- Day-Zero Operations
- iPXE Overview
- Cisco Network Plug and Play Overview
- ZTP Overview

Implementing Automation in Enterprise Networks

- Cisco Intent-Based Network Overview
- Cisco DNA Center Architecture
- Cisco DNA Center APIs

Building Cisco DNA Center Automation with Python

- Explore Cisco DNA Center Libraries

Automating Operations using Cisco DNA Center

- Introduction to Cisco DNA Center Assurance Workflows
- Cisco DNA Center Event Webhooks

Introducing Cisco SD-WAN Programmability

- SD-WAN Overview
- Cisco SD-WAN Architecture
- Cisco SD-WAN REST API Overview

Building Cisco SD-WAN Automation with Python

- Working with Templates in Cisco SD-WAN
- Python Workflows for Cisco SD-WAN

Building Cisco SD-WAN Automation with Ansible

- Shaping SD-WAN Overlay with Policies
- Using Ansible with Cisco SD-WAN APIs

Automating Cisco Meraki

- Cisco Meraki Architecture and Automation Capabilities
- Cisco Meraki REST API Overview

Implementing Meraki Integration APIs

- Cisco Meraki Integrations Overview
- Location Scanning APIs
- Cisco Meraki Camera APIs
- Cisco Meraki Captive Portals
- Cisco Meraki Wireless Health
- Explore Cisco Meraki Webhook Alerts

Labs

- Automate Networks with Netmiko
- Use Postman for REST API Consumption
- Use Ansible to Configure and Verify Device Configuration
- Implement On-Box Programmability and Automation with Cisco IOS XE Software
- Use Python on Cisco IOS XE Software
- Implement Streaming Telemetry with Cisco IOS XE
- Perform Administrative Task Using the Cisco SD-WAN API
- Build, Manage and Operate Cisco SD-WAN Programmatically
- Consume SD-WAN APIs Using the uri Module
- Manage Policies with Ansible
- Build Reports Using Ansible-Cisco SD-WAN Role
- Implement Cisco Meraki API Automation
- Explore Cisco Meraki Integration APIs
- Explore Cisco Meraki Webhook Alerts

Exam Details

This course leads to the 300-435 – Automating Cisco Enterprise Solutions (ENAUTO) exam.

Successful completion of this exam will earn you the Cisco Certified Devnet Specialist – Enterprise Automation and Programmability certification and will satisfy the concentration exam requirements for both the CCNP Enterprise certification and the Cisco Certified DevNet Professional certification.

skilltec training

Moving forward in knowledge and training

Implementing and Operating Cisco Enterprise Network Core Technologies

Course Code	ENCOR
Duration	5 days

Overview

The Implementing and Operating Cisco Enterprise Network Core Technologies course gives you the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. Learn how to implement security principles within an enterprise network and how to overlay network design by using solutions such as SD-Access and SD-WAN. The automation and programmability of Enterprise networks is also incorporated in this course.

This course will help you:

- Configure, troubleshoot, and manage enterprise wired and wireless networks.
- Implement security principles within an enterprise network.
- Earn 64 CE credits toward recertification.

Please note that this course is a combination of Instructor-Led and Self-Paced Study; 5 days in the classroom and approximately 3 days of self-study. The self-study content will be provided as part of the digital courseware that you receive at the beginning of the course and should be part of your preparation for the exam. Additional lab access will be provided at the end of the class, this will be valid for 60 hours or 90 days whichever is the shorter. It will be possible to complete all but 7 of the labs after the class.

Audience

Network engineers involved in the installation, support and troubleshooting of enterprise networks.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Illustrating the hierarchical network design model and architecture using the access, distribution, and core layers.
- Comparing and contrasting the various hardware and software switching mechanisms and operation, while defining the Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM), along with process switching, fast switching, and Cisco Express Forwarding concepts.
- Troubleshooting Layer 2 connectivity using VLANs and trunking.
- Implementation of redundant switched networks using Spanning Tree Protocol.
- Troubleshooting link aggregation using Etherchannel.
- Describing the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP).
- Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6.
- Implementing External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking.
- Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP).
- Implementing internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT).

- Describing the virtualization technology of servers, switches, and the various network devices and components.
- Implementing overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP).
- Describing the components and concepts of wireless networking including Radio Frequency (RF) and antenna characteristics and defining the specific wireless standards.
- Describing the various wireless deployment models available, include autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture.
- Describing wireless roaming and location services.
- Describing how APs communicate with WLCs to obtain software, configurations, and centralized management.
- Configuring and verifying Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC.
- Troubleshooting wireless client connectivity issues using various available tools.
- Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager.
- Explaining the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting.
- Configuring secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP.
- Implementing scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits.
- Describing the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other security features.
- Explaining the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience.
- Describing the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways.
- Defining the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane.
- Describing the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points.
- Describing the concepts and features of Quality of Service (QoS), and describing the need within the enterprise network
- Explaining basic Python components and conditionals with script writing and analysis.
- Describing network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF.
- Describing APIs in Cisco DNA Center and vManage.

Pre-Requisites

- Implementation of Enterprise LAN networks
- Basic understanding of Enterprise routing and wireless connectivity
- Basic understanding of Python scripting

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- PRNE-CPLL - Programming for Network Engineers - CPLL

Course Contents

Examining Cisco Enterprise Network Architecture

- Cisco Enterprise Architecture Model
- Campus LAN Design Fundamentals
- Traditional Multilayer Campus Layer Design
- Campus Distribution Layer Design

Understanding Cisco Switching Paths

- Layer 2 Switch Operation
- Control and Data Plane
- Cisco Switching Mechanisms

Implementing Campus LAN Connectivity

- Revisiting VLANs
- Trunking with 802.1Q
- Inter-VLAN Routing

Building Redundant Switched Topology

- Spanning-Tree Protocol Overview
- Spanning-Tree Protocol Operation
- Spanning-Tree Protocols Types and Features
- Multiple Spanning Tree Protocol
- PortFast and BPDU

Implementing Layer 2 Port Aggregation (Self-Study)

- Need for EtherChannel
- EtherChannel Mode Interactions
- Layer 2 EtherChannel Configuration Guidelines
- EtherChannel Load-Balancing Options
- Troubleshoot EtherChannel Issues

Understanding EIGRP

- EIGRP Features
- EIGRP Reliable Transport
- Establishing EIGRP Neighbour Adjacency
- EIGRP Metrics
- EIGRP Path Selection
- Explore EIGRP Path Selection
- Explore EIGRP Load Balancing and Sharing
- EIGRP for IPv6
- Compare EIGRP and OSPF Routing Protocols

Implementing OSPF

- Describe OSPF
- The OSPF Process
- OSPF Neighbor Adjacencies
- Buidling a Link-State Database
- OSPF LSA Types
- Compare Single-Area and Muliarea OSPF
- OSPF Area Structure
- OSPF Network Types

Optimizing OSPF

- OSPF Cost
- OSPF Route Summarization Benefits
- OSPF Route Filtering Tools
- Compare OSPFv2 and OSPFv3

Exploring EBGP

- Interdomain Routing with BGP
- BGP Operations
- Types of BGP Neighbor Relationships
- BGP Path Selection
- BGP Path Attributes

Implementing Network Redundancy

- Need for Default Gateway Redundancy
- Define FHRP
- HSRP Advanced Features
- Cisco Switch High Availability Features

Implementing NAT

- Define Network Address Translation
- NAT Address Types
- Explore NAT Implementations
- NAT Virtual Interface

Introducing Virtualization Protocols and Techniques

- Server Virualization
- Need for Network Virtualization
- Path Isolation Overview
- Introducing VRF
- Introducing Generic Routing Encapsulation

Introducing Virtualization Protocols and Techniques

- Server Virualization
- Need for Network Virtualization
- Path Isolation Overview
- Introducing VRF
- Introducing Generic Routing Encapsulation

Understanding Virtual Private Networks and Interfaces

- Site-to-Site VPN Technologies
- IPSec VPN Overview
- IPSec: IKE
- IPsec Modes
- IPsec VPN Types
- Cisco IOS VTI

Understanding Wireless Principles

- Explain RF Principles
- Describe Watts and Decibels
- Describe Antenna Characteristics
- Describe IEEE Wireless Standards
- Identify Wireless Component Roles

Examining Wireless Deployment Options

- Wireless Deployment Overview
- Describe Autonomous AP Deployment
- Describe Centralized Cisco WLC Deployment
- Describe FlexConnect Deployment
- Cloud Deployment and Its Effect on Enterprise Networks
- Describe the Cloud-Managed Meraki Solution
- Cisco Catalyst 9800 Series Controller Deployment Options
- Describe Cisco Mobility Express

Understanding Wireless Roaming and Location Services

- Wireless Roaming Overview
- Mobility Groups and Domains
- Wireless Roaming Types
- Describe Location Services

Examining Wireless AP Operation

- Universal AP Priming
- Explore the Controller Discovery Process
- Describe AP Failover
- Explain High Availability
- Explore AP Modes

Understanding Wireless Client Authentication

- Authentication Methods
- Pre-Shared Key (PSK) Authentication
- 802.1X User Authentication Overview
- PKI and 802.1X Certificate Based Authentication
- Introduction to Extensible Authetication Protocol
- EAP-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol
- EAP-FAST
- Guest Access with Web Auth

Troubleshooting Wireless Client Connectivity

- Wireless Troubleshooting Tools Overview
- Spectrum Analysis
- Wi-Fi Scanning
- Packet Analysis
- Cisco AireOS GUI and CLI Tools
- Cisco Wireless Config Analyzer Express
- Common Wireless Client Connectivity Issues Overview
- Client to AP Connectivity
- WLAN Configuration
- Infrastructure Configuartion

Introducing Multicast Protocols (Self-study)

- Multicast Overview
- Internet Group Management Protocol
- Multicast Distribution Trees
- IP Multicasting Routing
- Rendevous Point

Introducing QoS (Self-study)

- Understand the Impact of User Applications on the Network
- Need for Quality of Service (QoS)
- Describe QoS Mechanisms
- Define and Interpret a QoS Policy

Implementing Network Services

- Understanding Network Time Protocol
- Logging Services
- Simple Network Management Protocol
- Introducing NetFlow
- Flexible NetFlow
- Understanding Cisco IOS Embedded Event Manager

Using Network Analysis Tools

- Troubleshooting Concepts
- Network Troubleshooting Procedures: Overview
- Network Troubleshooting Procedures: Case Study
- Basic Hardware Diagnostics
- Filtered Show Commands
- Cisco IOS IP SLAs
- Switched Port Analyzer(SPAN) Overview
- Remote SPAN (RSPAN)
- Encapsulated Remote Switched Port Analyzer(ERSAPN)
- Cisco Packet Capture Tools Overview

Implementing Infrastructure Security

- ACL Overview
- ACL Wildcard Masking
- Types of ACLs
- Configure Numbered Access Lists
- Use ACLs to Filter Network Traffic
- Apply ACLs to Interfaces
- Configured Named Access Lists
- Control Plane Overview
- Control Plane Policing

Implementing Secure Access Control

- Securing Device Access
- AAA Framework Overview
- Benefits of AAA Usage
- Authentication Options
- RADIUS and TACACS+
- Enabling AAA and Configuring a Local User for Fallback
- Configuring RADIUS for Console and VTY Access
- Configuring TACACS+ for Console and VTY Access
- Configure Authorization and Accounting

Understanding Enterprise Network Security Architecture (Self-study)

- Explore Threatscape
- Cisco Intrusion Prevention Systems
- Virtual Private Networks
- Content Security
- Logging
- Endpoint Security
- Personal Firewalls
- Antivirus and Antispyware
- Centralized Endpoint Policy Enforcement
- Cisco AMP for Endpoints
- Firewall Concepts
- TrustSec
- MACsec
- Identity Management
- 802.1X for Wired and Wireless Endpoint Authentication
- MAC Authentication Bypass
- Web Authentication

Exploring Automation and Assurance Using Cisco DNA Center (Self-study)

- Need for Digital Transformation
- Cisco Digital Network Architecture
- Cisco Intent-Based Networking
- Cisco DNA Center Automation Overview
- Cisco DNA Center Platform Overview
- Cisco DNA Center Design
- Cisco DNA Center Inventory Overview
- Cisco DNA Center Configuration and Management Overview
- ONboarding of Network Devices Using Cisco DNA Center
- Cisco DNA Center Software Image Management Overview
- Cisco DNA Assurance Key Features and Use Cases
- Cisco DNA Center Assurance Implementation Workflow

Examining the Cisco SD-Access Solution (Self-study)

- Need for Cisco SD-Access
- Cisco SD Access Overview
- Cisco SD-Access Fabric Components
- Cisco SD-Access Fabric Control Plane Based on LISP
- Cisco SD-Access Fabric Control Plance Based on VXLAN
- Cisco SD-Access Fabric Control Plance Based on Cisco TrustSec
- Role of Cisco ISE and Cisco DNA Center in SD-Access
- Cisco SD-Access Wireless Integration
- Traditional Campus Interoperating with Cisco SD-Access

Understanding the Working Principles of the Cisco SD-WAN Solution (Self-study)

- Need for Software Defined Networking for WAN
- Cisco SD-WAN Components and Functions
- Cisco SD-WAN Orchestration Plane
- Cisco SD-WAN Management Plane- vManage
- Cisco SD-WAN Control Plane - vSmart
- Cisco SD-WAN Data Plane - WAN Edge
- Cisco SD-WAN Programmatic APIs
- Cisco SD-WAN Automation and Analytics
- Cisco SD-WAN Terminology
- Cisco IOS XE and IOS XE SD-WAN Software
- Fexible Controller Deployment Optins
- Cisco SD-WAN Security

Understanding the Basics of Python Programming

- Describe Python Concepts
- String Data Types
- Numbers Data Types
- Boolean Data Types
- Script Writing and Execution
- Analyze Code

Introducing Network Programmability Protocols

- Configuration Management
- Evolution of Device Management and Programmability
- Data Encoding Formats
- Understanding JSON
- Model Driven Programmability Stack
- Introduction to YANG
- Types of YANG Models
- Understanding NETCONF
- Explain NETCONF and YANG
- REST
- Understanding RESTCONF Protocol

Introducing APIs in Cisco DNA Center and vManage (Self-study)

- Application Programming Interfaces
- REST API Response Codes and Results
- REST API Security
- Cisco DNA Center APIs
- Cisco SD-WAN REST API Overview

Labs

- Investigate the CAM
- Analyze Cisco Express Forwarding
- Troubleshoot VLAN and Trunk Issues
- Tuning STP and Configuring RSTP
- Configure Multiple Spanning Tree Protocol
- Troubleshoot EtherChannel
- Implementing Multiarea OSPF
- Implement OSPF Tuning
- Apply OSPF Optimization
- Implement OSPFv3
- Configure and Verify Single-Homed EBGP
- Implementing HSRP
- Configure VRRP
- Implement NAT
- Configure and Verify VRF
- Configure and Verify a GRE Tunnel
- Configure Static VTI Point-to-Point Tunnels
- Configure Wireless Client Authentication in a Centralized Deployment (No Extended Access)
- Troubleshoot Wireless Client Cnnectivity Issues (No Extended Access)
- Configure Syslog
- Configure and Verify Flexible NetFlow
- Configuring Cisco IOS Embedded Event Manager (EEM)
- Troubleshoot Connectivity and Analyze Traffic with Ping, Traceroute and Debug
- Confiure and Verify Cisco IP SLA's
- Configure Standard and Extended ACLs
- Configure Contorl Plane Policing
- Implement Local and Server-Based AAA (No Extended Access)
- Writing and Troubleshooting Python Scripts (No Extended Access)
- Explore JSON Objects and Scripts in Python (No Extended Access)
- Use NETCONF via SSH (No Extended Access)
- Use RESTCONF with Cisco IOS XE Software (No Extended Access)

Exam Details

This course leads to the 350-401 - Implementing Cisco Enterprise Network Core Technologies (ENCOR) Exam.

skilltec training

Moving forward in knowledge and training

Cisco SD WAN Operation and Deployment

Course Code ENSDW
Duration 2 days

Overview

The Cisco SD-WAN Operation and Deployment course is designed to provide an overview of the Cisco SD-WAN solution and SD-WAN components. Students will learn how to create, manage and operate a secure extensible network using Cisco SD-WAN products. The course covers how to configure, operate and monitor overlay routing in a secure extensible network. Policies and quality of service (QoS) in the SD-WAN overlay network are also included

Audience

Engineers involved in the implementation of a Cisco SD-WAN environment.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Identifying the various components and architecture of the Cisco SD-WAN solution.
- Deploying vEdge routers in a secure extensible network.
- Creating templates to aide in the deployment and operation of the secure extensible network.
- Configuring and verifying overlay routing in the secure extensible network.
- Creating simple policies to control traffic flow in the secure extensible network.

Pre-Requisites

- Strong understanding of enterprise-wide area network design
- Strong understanding of routing protocol operation, including both interior and exterior routing protocol operation ROUTE and TSHOOT Recommended
- Familiarity with Transport Layer Security (TLS) and IP Security (IPSec) - SENSS Recommended

Course Contents

SD-WAN Solution Components

- SD-WAN Solution Overview
- SD-WAN Components
- Managing SD-WAN Components

Secure Extensible Network Deployment

- Secure Control Plane Operation
- Secure Control Plane Deployment
- Secure Data Plane Operation
- Cloud Deployments and Redundancy

SD-WAN Template Deployment

- Templates Overview
- Feature Templates
- Device Templates
- Attaching Devices to Templates

SD-WAN Overlay Routing

- Overlay Routing Overview
- OMP Route Advertisements
- OMP Route Redistribution and Network Segmentation
- Configuring and Verifying Overlay Routing

SD-WAN Policies and QoS

- Policy Overview and Framework
- Smart Policy Operation and Construction
- Forwarding and QoS Overview
- Configuring and Monitoring QoS Forwarding

Labs

- Manage and Monitor SD-WAN Components
- Deploy and Verify SD-WAN vEdge Routers
- Deploy SD-WAN Templates
- SD-WAN Overlay Routing
- SD-WAN Policies

Exam Details

There are no exams currently aligned to this course.

Designing Cisco Enterprise Networks

Course Code	ENSLD
Duration	5 days

Overview

The Designing Cisco Enterprise Networks (ENSLD) v1.0 course gives you the knowledge and skills you need to design an enterprise network. This course serves as a deep dive into enterprise network design and expands on the topics covered in the Implementing and Operating Cisco® Enterprise Network Core Technologies (ENCOR) v1.0 course.

Audience

This course also helps you prepare to learn the skills, technologies and best practices needed to design an enterprise network, to deepen your understanding of enterprise design including advanced addressing and routing solutions, advanced enterprise campus networks, WAN, security services, network services, and software-defined access SDA, and to prepare to take the exam, Designing Cisco Enterprise Networks v1.0 (ENSLD 300-420), which is part of the CCNP® Enterprise and Cisco Certified Specialist - Enterprise Design certifications.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Designing Enhanced Interior Gateway Routing Protocol (EIGRP) internal routing for the enterprise network.
- Designing Open Shortest Path First (OSPF) internal routing for the enterprise network.
- Designing Intermediate System to Intermediate System (IS-IS) internal routing for the enterprise network.
- Designing a network based on customer requirements.
- Designing Border Gateway Protocol (BGP) routing for the enterprise network.
- Describing the different types and uses of Multiprotocol BGP (MP-BGP) address families.
- Describing BGP load sharing.
- Designing a BGP network based on customer requirements.
- Decide where the L2/L3 boundary will be in your Campus network and make design decisions.
- Describing Layer 2 design considerations for Enterprise Campus networks.
- Designing a LAN network based on customer requirements.
- Describing Layer 3 design considerations in an Enterprise Campus network.
- Examining Cisco SD-Access fundamental concepts.
- Describing Cisco SD-Access Fabric Design.
- Designing an Software-Defined Access (SD-Access) Campus Fabric based on customer requirements.
- Designing service provider-managed VPNs.
- Designing enterprise-managed VPNs.
- Designing a resilient WAN.
- Designing a resilient WAN network based on customer requirements.
- Examining the Cisco SD-WAN architecture.
- Describing Cisco SD-WAN deployment options.
- Designing Cisco SD-WAN redundancy.
- Explaining the basic principles of QoS.
- Designing Quality of Service (QoS) for the WAN.
- Designing QoS for enterprise network based on customer requirements.

- Explaining the basic principles of multicast.
- Designing rendezvous point distribution solutions.
- Describing high-level considerations when doing IP addressing design.
- Creating an IPv6 addressing plan.
- Planning an IPv6 deployment in an existing enterprise IPv4 network.
- Describing the challenges that you might encounter when transitioning to IPv6.
- Designing an IPv6 addressing plan based on customer requirements.
- Describing Network APIs and protocols.
- Describing Yet Another Next Generation (YANG), Network Configuration Protocol (NETCONF), and Representational State Transfer Configuration Protocol (RESTCONF).

Pre-Requisites

- Basic network fundamentals and building simple LANs
- Basic IP addressing and subnets
- Routing and switching fundamentals
- Basic wireless networking concepts and terminology

Course Contents

- Designing EIGRP Routing
- Designing OSPF Routing
- Designing IS-IS Routing
- Designing BGP Routing and Redundancy
- Understanding BGP Address Families
- Designing the Enterprise Campus LAN
- Designing the Layer 2 Campus
- Designing the Layer 3 Campus
- Discovering the Cisco SD-Access Architecture
- Exploring Cisco SD-Access Fabric Design
- Designing Service Provider-Managed VPNs
- Designing Enterprise-Managed VPNs
- Designing WAN Resiliency
- Examining Cisco SD-WAN Architectures
- Cisco SD-WAN Deployment Design Considerations
- Designing Cisco SD-WAN Routing and High Availability
- Understanding QoS
- Designing LAN and WAN QoS
- Exploring Multicast with Protocol-Independent Multicast-Sparse Mode
- Designing Rendezvous Point Distribution Solutions
- Designing an IPv4 Address Plan
- Exploring IPv6
- Deploying IPv6
- Introducing Network APIs and Protocols
- Exploring YANG, NETCONF, RESTCONF, and Model-Driven Telemetry

Exam Details

This course leads to the 300-420 – Designing Cisco Enterprise Networks (ENSLD) exam.

Successful completion will earn you the Cisco Certified Specialist - Enterprise Design certification and will satisfy the concentration exam requirement for the new CCNP Enterprise certification. Other exams required for the CCNP Enterprise certification:

- Implementing Cisco Enterprise Network Core Technologies (ENCOR)

Designing Cisco Enterprise Wireless Networks

Course Code	ENWLSD
Duration	5 days

Overview

The Designing Cisco Enterprise Wireless Networks course gives you the knowledge you need to design Cisco wireless networks. The course covers design specifics from scenario design concepts through the installation phase and into post-deployment validation.

This course, including the self-paced material, helps prepare you to take the exam, Designing Cisco Enterprise Wireless Networks (300-425 ENWLSD), which leads to to the new CCNP Enterprise and Cisco Certified Specialist – Enterprise Wireless Design certifications.

Audience

Individuals interested in gaining the knowledge needed to plan advanced designs of Cisco Wireless Products.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing and implementing a Cisco-recommended structured design methodology.
- Describing and implementing industry standards, amendments, certifications, and RFCs.
- Describing and implementing Cisco enhanced wireless features.
- Describing and implementing the wireless design process.
- Describing and implementing specific vertical designs.
- Describing and implementing site survey processes.
- Describing and implementing network validation processes.

Pre-Requisites

- General knowledge of networks - ICND1 or CCNA
- General knowledge of wireless networks - WIFUND or WLFNDU
- Routing and switching knowledge - ICND1 or CCNA

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- WLFNDU - Understanding Cisco Wireless Foundations
- ENCOR - Implementing and Operating Cisco Enterprise Network Core Technologies

Course Contents

Describing and Implementing a Structured Wireless Design Methodology

- Importance of Planning Wireless Design with a Structured Methodology
- Cisco Structured Design Model
- Cisco Design Guides and Cisco Validated Designs for Wireless Networks
- Role of the Project Manager When Designing Wireless Networks

Describing and Implementing Industry Protocols and Standards

- Wireless Standards Bodies
- IEEE 802.11 Standard and Amendments
- WFA Certifications
- Relevant IETF Wireless RFCs
- Practice Activity

Describing and Implementing Cisco Enhanced Wireless Features

- Hardware and Software Choices for a Wireless Network Design
- Cisco Infrastructure Settings for Wireless Network Design
- Cisco Enhanced Wireless Features

Examining Cisco Mobility and Roaming

- Mobility and Intercontroller Mobility in a Wireless Network
- Optimize Client Roaming in a Wireless Network
- WGB and WGB Roaming in a Wireless Network

Describing and Implementing the Wireless Design Process

- Overview of Wireless Design Process
- Meet with the Customer to Discuss the Wireless Network Design
- Customer Information Gathering for a Wireless Network Design
- Design the Wireless Network
- Deployment of the Wireless Network
- Validation and Final Adjustments of the Wireless Network
- Wireless Network Design Project Documents and Deliverables

Describing and Implementing Specific Vertical Designs

- Designs for Wireless Applications
- Wireless Network Design Within the Campus
- Extend Wireless Networks to the Branch Sites

Examining Special Considerations in Advanced Wireless Designs

- High-Density Designs in Wireless Networks
- Introducing Location and CMX Concepts
- Design for Location
- FastLocate and HyperLocation
- Bridges and Mesh in a Wireless Network Design
- Redundancy and High Availability in a Wireless Network

Describing and Implementing the Site Survey Processes

- Site Survey Types
- Special Arrangements Needed for Site Surveys
- Safety Aspects to be Considered During Site Surveys
- Site Survey Tools in Cisco Prime Infrastructure
- Third-Party Site Survey Software and Hardware Tools

Describing and Implementing Wireless Network Validation Processes

- Post-installation Wireless Network Validation
- Making Post-installation Changes to a Wireless Network
- Wireless Network Handoff to the Customer
- Installation Report

Labs

- Use Cisco Prime Infrastructure as a Design Tool
- Create a Predictive Site Survey with Ekahau Pro
- Perform a Live Site Survey Using AP on a Stick
- Stimulate a Post-installation Network Validation Survey

Exam Details

This course leads to the 300-425 - Designing Cisco Enterprise Wireless Networks (ENWLSD) exam.

Successful completion will earn you the Cisco Certified Specialist - Enterprise Wireless Design Certification and count towards the New CCNP Enterprise Certification - To achieve the new CCNP Enterprise Certification you will also need the CCNP Enterprise Core Exam.

Implementing Cisco Enterprise Wireless Networks

Course Code	ENWLSI
Duration	5 days

Overview

The Implementing Cisco Enterprise Wireless Networks course gives you the knowledge and skills needed to secure wireless network infrastructure and troubleshoot any related issues. You'll learn how to implement and secure a wireless network infrastructure and use Cisco Identity Service Engine (ISE), Cisco Prime Infrastructure (PI), and Cisco Connect Mobile Experience to monitor and troubleshoot network issues.

The course provides hands-on labs to reinforce concepts including deploying Cisco Prime Infrastructure Release 3.5, Cisco Catalyst 9800 Wireless Controller Release IOS XE Gibraltar 16.10, Cisco Digital Network Architecture (DNA) Center Release 1.2.8, Cisco CMX Release 10.5, Cisco MSE Release 8.0 features and Cisco Identity Services Engine (ISE) Release 2.4.

This course also helps you prepare to take the Implementing Cisco Enterprise Wireless Networks (300-430 ENWLSI) exam, which is part of the new CCNP Enterprise certification. Passing the exam will also provide you with the Cisco Certified Specialist - Enterprise Wireless Implementation certification.

Audience

Individuals needing to understand how to implement, secure and troubleshoot a Cisco Enterprise Wireless Network.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Implementing network settings to provide a secure wireless network infrastructure.
- Troubleshooting security issues as it relates to the wireless network infrastructure.
- Implementing a secure wireless client and troubleshoot wireless client connectivity issues.
- Implementing and troubleshooting QoS in wireless networks.
- Implementing and troubleshooting advanced capabilities in wireless network services.

Pre-Requisites

- General knowledge of networks
- General knowledge of wireless networks
- Routing and switching knowledge

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- WLFNDU - Understanding Cisco Wireless Foundations
- ENCOR - Implementing and Operating Cisco Enterprise Network Core Technologies

Course Contents

Securing and Troubleshooting the Wireless Network Infrastructure

- Implement Secure Access to the WLCs and Access Points
- Configure the Network for Access Point 802.1X Authentication
- Use Cisco DNA Center for Controller and AP Auto Install
- Implement Cisco Prime Infrastructure
- Define Network Troubleshooting Techniques
- Troubleshoot Access Point Join Issues
- Monitor the Wireless Network

Implementing and Troubleshooting Secure Client Connectivity

- Configure the Cisco WLC for Wireless Client 802.1x Authentication
- Configure the Wireless Client for 802.1X Authentication
- Configure a Wireless LAN for FlexConnect
- Implement Guest Services in the Wireless Network
- Configure the Cisco WLC for Centralized Web Authentication
- Configure Central Web Authentication on Cisco ISE
- Implement BYOD
- Implement Location-Aware Guest Services
- Troubleshoot Client Connectivity
- Describe Issues that Affect Client Performance
- Monitor Wireless Clients

Implementing and Troubleshooting QoS in Wireless Networks

- Implement QoS in the Wireless Network
- Configure the Cisco WLC to Support Voice Traffic
- Optimize Wireless Utilization on the Cisco WLC
- Implement Cisco AVC in the Wireless Network
- Implement Multicast Services
- Implement mDNS Service
- Implement Cisco Media Stream
- Troubleshoot QoS Issues in the Wireless Network
- Troublehoot mDNS Issues
- Troubleshoot Media Stream Issues

Implementing and Troubleshooting Advanced Wireless Network Services

- Implement Base Location Services on Cisco Prime Infrastructure
- Implement Hyperlocation in the Wireless Network
- Implement Detect and Locate Services on Cisco CMX
- Implement Analytics on Cisco CMX
- Implement Presence Services on Cisco CMX
- Monitor and Locate Rogue Devices with Cisco Prime Infrastructure and Cisco CMX
- Monitor and Detect Wireless Clients with Cisco CMX and Cisco DNA Center
- Run Analytics on Wireless Clients
- Troubleshoot Location Accuracy with Cisco Hyperlocation
- Monitor and Manage RF Interferers on the Cisco WLC
- Monitor and Manager RF Interferers on Cisco Prime Infrastructure and Cisco CMX

Labs

- Lab Familiarization (Base Learning Lab)
- Configure Secure Management Access for WLCs and APs
- Add Network Devices and External Resources to Cisco Prime Infrastructure
- Capture a Successful AP Authentication
- Implement AAA Services for Central Mode WLANs
- Implement AAA Services for FlexConnect Mode WLANs
- Configure Guest Services in the Wireless Network
- Configure BYOD in the Wireless Network
- Capture a Successful Client Authentications
- Configure QoS in the Wireless Network for Voice and Video Services
- Configure Cisco AVC in the Wireless Network
- Capture Successful QoS Traffic Marking in the Wireless Network
- Configure Detect and Locate Services on the Cisco CMX
- Identify Wireless Clients and Security Threats

Exam Details

This course leads to **300-430** - Implementing Cisco Enterprise Wireless Networks (ENWLSI) exam.

Implementing Cisco SD-WAN Solutions

Course Code	SD-WAN300
Duration	4 days

Overview

The Implementing Cisco SD-WAN Solutions course gives you deep-dive training about how to design, deploy, configure, and manage your Cisco® Software-Defined WAN (SD-WAN) solution in a large-scale live network, including how to migrate from legacy WAN to SD-WAN. You will learn best practices for configuring routing protocols in the data center and the branch, as well as how to implement advanced control, data, and application-aware policies. The course also covers SD-WAN deployment and migration options, placement of controllers, how to deploy and replace edge devices, and how to configure Direct Internet Access (DIA) breakout.

Audience

Technical individuals looking to understand how to design, configure and manage a Cisco Software Defined SD-WAN including how to migrate from a legacy WAN to a SD-WAN.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the Cisco SD-WAN overlay network and how modes of operation differ in legacy WAN versus SD-WAN.
- Describing options for SD-WAN cloud and on-premises deployments, as well as how to deploy virtual vEdge and physical cEdge devices with Zero Touch Provisioning (ZTP) and device templates.
- Describing best practices in WAN routing protocols, as well as how to configure and implement transport-side connectivity, service-side routing, interoperability, and redundancy and high availability.
- Describing dynamic routing protocols and best practices in an SD-WAN environment, transport-side connectivity, service-side connectivity, and how redundancy and high availability are achieved in SD-WAN environments.
- Explaining how to migrate from legacy WAN to Cisco SD-WAN, including typical scenarios for data center and branch.
- Explaining how to perform SD-WAN Day 2 operations, such as monitoring, reporting, logging, and upgrading.

Pre-Requisites

- Completion of the Cisco SD-WAN Operation and Deployment (ENSDW) course or equivalent experience
- Knowledge of Software-Defined Networking (SDN) concepts as applied to large-scale live network deployments
- Strong understanding of enterprise wide area network design
- Strong understanding of routing protocol operation, including both interior and exterior routing protocol operation
- Familiarity with Transport Layer Security (TLS) and IP Security (IPSec)

Recommended courses:

- Cisco SD WAN Operation and Deployment (ENSDW)

Course Contents

Cisco SD-WAN Overlay Network

- Examining Cisco SD-WAN Architecture

Cisco SD-WAN Deployment

- Examining Cisco SD-WAN Deployment Options
- Deploying Edge Devices
- Deploying Edge Devices with Zero-Touch Provisioning
- Using Device Configuration Templates
- Redundancy, High Availability, and Scalability

Cisco SD-WAN Routing Options

- Using Dynamic Routing
- Providing Site Redundancy and High Availability
- Configuring Transport-Side Connectivity

Cisco SD-WAN Policy Configuration

- Reviewing Cisco SD-WAN Policy
- Defining Advanced Control Policies
- Defining Advanced Data Policies
- Implementing Application-Aware Routing
- Implementing Internet Breakouts and Network Address Translation (NAT)

Cisco SD-WAN Management and Operations

- Performing Day-2 Operations
- Performing Upgrades

Labs

- Deploying Cisco SD-WAN Controllers
- Adding a Branch Using Zero Touch Provisioning (ZTP)
- Deploying Devices Using Configuration Templates
- Configuring Controller Affinity
- Implementing Dynamic Routing Protocols on Service Side
- Implementing Transport Location (TLOC) Extensions
- Implementing Control Policies
- Implementing Data Policies
- Implementing Application-Aware Routing
- Implementing Internet Breakouts
- Migrating Branch Sites
- Performing an Upgrade

Exam Details

There are no exams currently aligned to this course

Understanding Cisco Wireless Foundations

Course Code	WLFNDU
Duration	5 days

Overview

The Understanding Cisco Wireless Foundations (WLFNDU) v1.0 course gives you the knowledge and skills you need to position, plan, implement, operate, and manage a Cisco WLAN network. This course teaches you how to design, install, configure, monitor, and conduct basic troubleshooting tasks on a Cisco WLAN network of any size.

Audience

This course will help you to learn the skills, technologies and best practices needed to manage a Cisco WLAN network, to understand and implement a Cisco wireless network architecture, and to design and implement WLAN maintenance and troubleshooting solutions.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing and implementing foundational wireless theory.
- Describing and implementing basic wireless security and client access.
- Describing and implementing a Cisco wireless network architecture.
- Configuring Cisco centralized wireless networks.
- Describing and implementing WLAN maintenance and troubleshooting.

Pre-Requisites

- General knowledge of networks
- General knowledge of wireless networks
- Routing and switching knowledge

Course Contents

- Describing and Implementing Foundational Wireless Theory
- Describing and Implementing Foundational Wireless Math and Antennas
- Describing and Implementing Foundational Wireless Operation
- Describing and Implementing Basic Wireless Security
- Describing and Implementing 802.1X and EAP
- Implementing Wireless Guest Access and Configuring Wireless Security
- Describing and Implementing Cisco Wireless Network Architecture
- Describing and Implementing Cisco Wireless Network
- Describing and Implementing Cisco Wireless Network Wired Support
- Configuring Cisco Centralized Wireless Networks

Labs

- Explore the Physics of Wi-Fi
- Explore the Wi-Fi Environment
- Analyze Wireless Frames
- Configure Client Access
- Configure the Wired Infrastructure
- Configure a Centralized Cisco WLC Deployment
- Configure a Centralized WLAN Deployment
- Configure an IPv6 Operation in a Centralized WLAN Deployment
- Optimize RF Conditions and Performance for Clients
- Perform Centralized Controller Maintenance
- Use Troubleshooting Tools

Exam Details

There are no exams currently aligned to this course.

skilltec training

Moving forward in knowledge and training

Implementing Automation for Cisco Security Solutions

Course Code	SAUI
Duration	3 days

Overview

The Implementing Automation for Cisco Security Solutions (SAUI) course teaches you how to design advanced automated security solutions for your network. Through a combination of lessons and hands-on labs, you will master the use of modern programming concepts, RESTful application program interfaces (APIs), data models, protocols, firewalls, web, Domain Name System (DNS), cloud, email security, and Cisco® Identity Services Engine (ISE) to strengthen cybersecurity for your web services, network, and devices. You will learn to work within the following platforms: Cisco Firepower® Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch® Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella®, Cisco Advanced Malware Protection (AMP), Cisco Threat grid, and Cisco Security Management Appliances.

This course will teach you when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

Audience

Individuals looking to use automation and programmability to design more efficient networks, increase scalability and protect against cyberattacks.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the overall architecture of the Cisco security solutions and how APIs help enable security.
- Knowing how to use Cisco Firepower APIs.
- Explaining how pxGrid APIs function and their benefits.
- Demonstrating what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes.
- Describing the features and benefits of using Cisco Stealthwatch Cloud APIs.
- Learning how to use the Cisco Umbrella Investigate API.
- Explaining the functionality provided by Cisco AMP and its APIs.
- Describing how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats.

Pre-Requisites

- Basic programming language concepts
- Basic understanding of virtualization
- Ability to use Linux and Command Line Interface (CLI) tools, such as Secure Shell (SSH) and bash
- CCNP level core networking knowledge
- CCNP level security networking knowledge

Recommended courses:

- DEVCOR - Developing Applications Using Cisco Platforms and APIs
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Introducing Cisco Security APIs

- Role of APIs in Cisco Security Solutions
- Cisco Firepower, Cisco ISE, Cisco pxGrid and Cisco Stealthwatch APIs
- Use Cases and Security Workflow

Consuming Cisco Advanced Malware Protection APIs

- Cisco AMP Overview
- Cisco AMP Endpoint API
- Cisco AMP Use Cases and Workflows

Using Cisco ISE

- Introducing Cisco Identity Services Engine
- Cisco ISE Use Cases
- Cisco ISE APIs

Using Cisco pxGrid APIs

- Cisco pxGrid Overview
- WebSockets and STOMP Messaging Protocol

Using Cisco Threat Grid APIs

- Cisco Threat Grid Overview
- Cisco Threat Grid API
- Cisco Threat Grid Use Cases and Workflows

Investigating Cisco Umbrella Security Data Programmatically

- Cisco Umbrella Investigate API Overview
- Cisco Umbrella Investigate API: Details

Exploring Cisco Umbrella Reporting and Enforcement APIs

- Cisco Umbrella Reporting and Enforcement APIs Overview
- Cisco Umbrella Reporting and Enforcement APIs: Deep Dive

Automating Security with Cisco Firepower APIs

- Review Basic Constructs of Firewall Policy Management
- Design Policies for Automation
- Cisco FMC APIs in Depth
- Cisco FTD Automation with Ansible
- Cisco FDM API In Depth

Operationalizing Cisco Stealthwatch and the API Capabilities

- Cisco Stealthwatch Overview
- Cisco Stealthwatch APIs: Details

Using Cisco Stealthwatch Cloud APIs

- Cisco Stealthwatch Cloud Overview
- Cisco Stealthwatch Cloud APIs Deep Dive

Describing Cisco Security Management Appliance APIs

- Cisco SMA APIs Overview
- Cisco SMA API

Labs

- Query Cisco AMP Endpoint APIs for Veerifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Query Security Data with the Cisco Umbrella Investigate API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuartion
- Automate Firewall policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct a Report Using Cisco Stealthwatch Cloud APIs
- Construct Reports Using Cisco SMA APIs

Exam Details

This course leads to the 300-735 - Automating and Programming Cisco Security Solutions (SAUTO) exam.

Successful completion will earn you the Cisco Certified DevNet Specialist - Security Automation and Programmability certification and satisfy the concentration exam requirements for the CCNP Security certification and the Cisco Certified DevNet Professional certification.

Implementing and Operating Cisco Security Core Technologies

Course Code	SCOR
Duration	5 days

Overview

The Implementing and Operating Cisco Security Core Technologies (SCOR) course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility and enforcements. You will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco ASA Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud threat detection features.

Please note that this course is a combination of Instructor-Led and Self-Paced Study; 5 days in the classroom and approximately 3 days of self-study.

Audience

Security individuals who need to be able to implement and operate core security technologies including network security, cloud security, content security, endpoint protection and detection, secure network access, visibility and enforcements.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing information security concepts and strategies within the network.
- Describing common TCP/IP, network application, and endpoint attacks.
- Describing how various network security technologies work together to guard against attacks.
- Implementing access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall.
- Describing and implementing basic email content security features and functions provided by Cisco Email Security Appliance.
- Describing and implementing web content security features and functions provided by Cisco Web Security Appliance.
- Describing Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console.
- Introducing VPNs and describing cryptography solutions and algorithms.
- Describing Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco FirePower NGFW.
- Describing and deploying Cisco secure remote access connectivity solutions and describing how to configure 802.1X and EAP authentication.
- Providing basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features.

- Examining various defenses on Cisco devices that protect the control and management plane.
- Configuring and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls.
- Describing Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions.
- Describing basics of cloud computing and common cloud attacks and how to secure cloud environment.

Pre-Requisites

- Familiarity with Ethernet and TCP/IP networking
- Working Knowledge of the Windows operating system
- Working Knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions

Course Contents

Describing Information Security Concepts (Self-Study)

- Information Security Overview
- Managing Risk
- Vulnerability Assessment
- Understanding CVSS

Describing Common TCP/IP Attacks (Self-Study)

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP Vulnerabilities
- TCP Vulnerabilities
- UDP Vulnerabilities
- Attack Surface and Attack Vectors
- Reconnaissance Attacks
- Access Attacks
- Man-In-The-Middle Attacks
- Denial of Service and Distributed Denial of Service Attacks
- Reflection and Amplification Attacks
- Spoofing Attacks
- DHCP Attacks

Describing Common Network Application Attacks (Self-Study)

- Password Attacks
- DNS-Based Attacks
- DNS Tunneling
- Web-Based Attacks
- HTTP 302 Cushioning
- Command Injections
- SQL Injections
- Cross-Site Scripting and Request Forgery
- Email-Based Attacks

Describing Common Endpoint Attacks (Self-Study)

- Buffer Overflow
- Malware
- Reconnaissance Attack
- Gaining Access and Control
- Gaining Access via Social Engineering
- Gaining Access via Web-Based Attacks
- Exploit Kits and Rootkits
- Privilege Escalation
- Post-Exploitation Phase
- Angler Exploit Kit

Describing Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Security Intelligence Overview
- Threat Information Standardization
- Network-Based Malware Protection Overview
- IPS Overview
- Next Generation Firewall Overview
- Email Content Security Overview
- Web Content Security Overview
- Threat Analytic Systems Overview
- DNS Security Overview
- Authentication, Authorization, and Accounting Overview
- Identity and Access Management Overview
- Virtual Private Network Technology Overview
- Network Security Device Form Factors Overview

Deploying Cisco ASA Firewall

- Cisco ASA Deployment Types
- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups
- Network Address Translation
- Cisco ASA Interface ACLs
- Cisco ASA Global ACLs
- Cisco ASA Advanced Access Policies
- Cisco ASA High Availability Overview

Deploying Cisco Firepower Next-Generation Firewall

- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects
- Cisco Firepower NGFW NAT
- Cisco Firepower NGFW Prefilter Policies
- Cisco Firepower NGFW Access Control Policies
- Cisco Firepower NGFW Security Intelligence
- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

Deploying Email Content Security

- Cisco Email Content Security Overview
- SMTP Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview
- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

Deploying Web Content Security

- Cisco WSA Overview
- Deployment Options
- Network Users Authentication
- HTTPS Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

Deploying Cisco Umbrella (Self-Study)

- Cisco Umbrella Architecture
- Deploying Cisco Umbrella
- Cisco Umbrella Roaming Client
- Managing Cisco Umbrella
- Cisco Umbrella Investigate Overview

Explaining VPN Technologies and Cryptography

- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services
- Keys in Cryptography
- Public Key Infrastructure

Introducing Cisco Secure Site-to-Site VPN Solutions

- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

Deploying Cisco IOS VTI-Based Point-to-Point

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec IKEv2 VPN Configuration

Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW

- Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
- Cisco ASA Point-to-Point VPN Configuration
- Cisco Firepower NGFW Point-to-Point VPN Configuration

Introducing Cisco Secure Remote Access VPN Solutions

- Remote Access VPN Components
- Remote Access VPN Technologies
- SSL Overview

Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Cisco ASA Remote Access VPN Configuration
- Cisco Firepower NGFW Remote Access VPN Configuration

Explaining Cisco Secure Network Access Solutions

- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution
- Cisco Identity Services Engine
- Cisco TrustSec

Describing 802.1X Authentication

- 802.1X and EAP
- EAP Methods
- Role of RADIUS in 802.1X Communications
- RADIUS Change of Authorization

Configuring 802.1X Authentication

- Cisco Catalyst Switch 802.1X Configuration
- Cisco WLC 802.1X Configuration
- Cisco ISE 802.1X Configuration
- Supplicant 802.1x Configuration
- Cisco Central Web Authentication

Describing Endpoint Security Technologies (Self-Study)

- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Application Whitelists and Blacklists
- Host-Based Malware Protection
- Sandboxing Overview
- File Integrity Checking

Deploying Cisco AMP for Endpoints (Self-study)

- Cisco AMP for Endpoints Architecture
- Cisco AMP for Endpoints Engines
- Retrospective Security with Cisco AMP
- Cisco AMP Device and File Trajectory
- Managing Cisco AMP for Endpoints

Introducing Network Infrastructure Protection (Self-Study)

- Identifying Network Device Planes
- Control Plane Security Controls
- Management Plane Security Controls
- Network Telemetry
- Layer 2 Data Plane Security Controls
- Layer 3 Data Plane Security Controls

Deploying Control Plane Security Controls (Self-Study)

- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Routing Protocol Security

Deploying Layer 2 Data Plane Security Controls (Self-Study)

- Overview of Layer 2 Data Plane Security Controls
- VLAN-Based Attacks Mitigation
- STP Attacks Mitigation
- Port Security
- Private VLANs
- DHCP Snooping
- ARP Inspection
- Storm Control
- MACsec Encryption

Deploying Layer 3 Data Plane Security Controls (Self-Study)

- Infrastructure Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard

Labs

- Configure Network Settings And NAT On Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, HAT, and RAT on Cisco ESA
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore CTA in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

Exam Details

This course leads to the 350-701 - Implementing and Operating Cisco Security Core Technologies (SCOR) exam.

This is the core exam for the Cisco CCNP Security certification, in order to gain the CCNP Security certification you will also need to pass one of the concentration exams.

Securing Email with Cisco Email Security Appliance

Course Code SESA
Duration 4 days

Overview

Learn how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise and ransomware. Help streamline email security policy management. This hands-on course provides you with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

Audience

Individuals responsible for the deployment, administration and troubleshooting of a Cisco Email Security Appliance.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing and administering the Cisco Email Security Appliance (ESA).
- Controlling sender and recipient domains.
- Controling spam with Talos SenderBase and anti-spam.
- Using anti-virus and outbreak filters & using mail policies and content filters
- Using message filters to enforce email policies.
- Preventing data loss and Performing LDAP queries.
- Authenticating Simple Mail Transfer Protocol (SMTP) sessions.
- Authenticating email and Encrypting email
- Using system quarantines and delivery methods.
- Performing centralized management using clusters.
- Testing and troubleshooting.

Pre-Requisites

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- Experience with IP routing

Recommended qualifications (1 of the following):

- Cisco certification (Cisco CCNA® certification or higher)
- Relevant industry certification, such as (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC), and ISACA
- Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A+, Network+, Server+)

Recommended courses:

- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Describing the Cisco Email Security Appliance

- Cisco Email Security Appliance Overview
- Technology Use Case
- Cisco Email Security Appliance Data Sheet
- SMTP Overview
- Email Pipeline Overview
- Installation Scenarios
- Initial Cisco Email Security Appliance Configuration
- Centralizing Services on a Cisco Content Security Management Appliance (SMA)
- Release Notes for AsyncOS 11.x

Administering the Cisco Email Security Appliance

- Distributing Administrative Tasks
- System Administration
- Managing and Monitoring Using the Command Line Interface (CLI)
- Other Tasks in the GUI
- Advanced Network Configuration
- Using Email Security Monitor
- Tracking Messages
- Logging

Controlling Sender and Recipient Domains

- Public and Private Listeners
- Configuring the Gateway to Receive Email
- Host Access Table Overview
- Recipient Access Table Overview
- Configuring Routing and Delivery Features

Controlling Spam with Talos SenderBase and Anti-Spam

- SenderBase Overview
- Anti-Spam
- Managing Graymail
- Protecting Against Malicious or Undesirable URLs
- File Reputation Filtering and File Analysis
- Bounce Verification

Using Anti-Virus and Outbreak Filters

- Anti-Virus Scanning Overview
- Sophos Anti-Virus Filtering
- McAfee Anti-Virus Filtering
- Configuring the Appliance to Scan for Viruses
- Outbreak Filters
- How the Outbreak Filters Feature Works
- Managing Outbreak Filters

Using Mail Policies

- Email Security Manager Overview
- Mail Policies Overview
- Handling Incoming and Outgoing Messages Differently
- Matching Users to a Mail Policy
- Message Splintering
- Configuring Mail Policies

Using Content Filters

- Content Filters Overview
- Content Filter Conditions
- Content Filter Actions
- Filter Messages Based on Content
- Text Resources Overview
- Using and Testing the Content Dictionaries Filter Rules
- Understanding Text Resources
- Text Resource Management
- Using Text Resources

Using Message Filters to Enforce Email Policies

- Message Filters Overview
- Components of a Message Filter
- Message Filter Processing
- Message Filter Rules
- Message Filter Actions
- Attachment Scanning
- Examples of Attachment Scanning Message Filters
- Using the CLI to Manage Message Filters
- Message Filter Examples
- Configuring Scan Behavior

Preventing Data Loss

- Overview of the Data Loss Prevention (DLP) Scanning Process
- Setting Up Data Loss Prevention
- Policies for Data Loss Prevention
- Message Actions
- Updating the DLP Engine and Content Matching Classifiers

Using LDAP

- Overview of LDAP
- Working with LDAP
- Using LDAP Queries
- Authenticating End-Users of the Spam Quarantine
- Configuring External LDAP Authentication for Users
- Testing Servers and Queries
- Using LDAP for Directory Harvest Attack Prevention
- Spam Quarantine Alias Consolidation Queries
- Validating Recipients Using an SMTP Server

SMTP Session Authentication

- Configuring AsyncOS for SMTP Authentication
- Authenticating SMTP Sessions Using Client Certificates
- Checking the Validity of a Client Certificate
- Authenticating User Using LDAP Directory
- Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
- Establishing a TLS Connection from the Appliance
- Updating a List of Revoked Certificates

Email Authentication

- Email Authentication Overview
- Configuring DomainKeys and DomainKeys Identified MailDKIM) Signing
- Verifying Incoming Messages Using DKIM
- Overview of Sender Policy FrameworkSPF) and SIDF Verification
- Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- Forged Email Detection

Email Encryption

- Overview of Cisco Email Encryption
- Encrypting Messages
- Determining Which Messages to Encrypt
- Inserting Encryption Headers into Messages
- Encrypting Communication with Other Message Transfer Agents (MTAs)
- Working with Certificates
- Managing Lists of Certificate Authorities
- Enabling TLS on a Listener's Host Access Table (HAT)
- Enabling TLS and Certificate Verification on Delivery
- Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services

Using System Quarantines and Delivery Methods

- Describing Quarantines
- Spam Quarantine
- Setting Up the Centralized Spam Quarantine
- Using Safelists and Blocklists to Control Email Delivery Based on Sender
- Configuring Spam Management Features for End Users
- Managing Messages in the Spam Quarantine
- Policy, Virus, and Outbreak Quarantines
- Managing Policy, Virus, and Outbreak Quarantines
- Working with Messages in Policy, Virus, or Outbreak Quarantines
- Delivery Methods

Centralized Management Using Clusters

- Overview of Centralized Management Using Clusters
- Cluster Organization
- Creating and Joining a Cluster
- Managing Clusters
- Cluster Communication
- Loading a Configuration in Clustered Appliances
- Best Practices

Testing and Troubleshooting

- Debugging Mail Flow Using Test Messages: Trace
- Using the Listener to Test the Appliance
- Troubleshooting the Network
- Troubleshooting the Listener
- Troubleshooting Email Delivery
- Troubleshooting Performance
- Web Interface Appearance and Rendering Issues
- Responding to Alerts
- Troubleshooting Hardware Issues
- Working with Technical Support

References

- Model Specifications for Large Enterprises
- Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
- Cisco Email Security Appliance Model Specifications for Virtual Appliances
- Packages and Licenses

Labs

- Verify and Test Cisco ESA Configuration
- Perform Basic Administration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Content and Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- DomainKeys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting

Exam Details

This course leads to the 300-720 - Securing Email with Cisco Email Security Appliance exam.

This is one of the concentration exams for the new CCNP Security Certification, to obtain the CCNP Security Certification you will also need to take the 300-701 SCOR exam. Passing the 300-720 exam will also earn you the Cisco Certified Specialist - Email Content Security Certification.

skilltec training

Moving forward in knowledge and training

Implementing and Configuring Cisco Identity Services Engine Bootcamp

Course Code	SISE
Duration	5 days

Overview

The Implementing and Configuring Cisco Identity Services Engine course shows you how to deploy and use Cisco Identity Services Engine (ISE) v2.4, an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless and VPN connections. This hands-on course provides you with the knowledge and skills required to implement and use Cisco ISE, including policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration. Through expert instruction and hands-on practice, you will learn how to use Cisco ISE to gain visibility into what is happening in your network, streamline security policy management and contribute to operational efficiency.

Delegates will be expected to work in groups and share lab equipment; if you are attending virtually you may also be required to work in virtual breakout rooms. Extended hours may also be required to cover all of the content included in this class.

Audience

Individuals involved in the deployment and maintenance of the Cisco ISE platform.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture. Describing the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages.
- Describing concepts and configuring components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services.
- Describing how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization.
- Describing third-party network access devices (NADs), Cisco TrustSec®, and Easy Connect.
- Describing and configuring web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios.
- Describing and configuring Cisco ISE profiling services, and understanding how to monitor these services to enhance your situational awareness about network-connected endpoints. Describing best practices for deploying this profiler service in your specific environment.
- Describing BYOD challenges, solutions, processes, and portals. Configuring a BYOD solution, and describing the relationship between BYOD processes and their related configuration components. Describing and configuring various certificates related to a BYOD solution.

- Describing the value of the My Devices portal and how to configure this portal.
- Describing endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE.
- Describing and configuring TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understanding the role of TACACS+ within the authentication, authentication, and accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols.
- Migrating TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool.

Pre-Requisites

- Foundational level understanding of Security Concepts
- Understand the concepts of 802.1X.
- Familiarity with Cisco AnyConnect Secure Mobility Client.
- Familiarity with Microsoft Windows and Active Directory.

Recommended courses:

- 8021X-CPLL - Introduction to 802.1X Operations for Cisco Security Professionals - CPLL
- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Introducing Cisco ISE Architecture and Deployment

- Using Cisco ISE as a Network Access Policy Engine
- Cisco ISE Use Cases
- Describing Cisco ISE Fucntions
- Cisco ISE Deployment Models
- Context Visibility

Cisco ISE Policy Enforcement

- Using 802.1X for Wired and Wireless Access
- Using MAC Authentication Bypass for Wired and Wireless Access
- Introducing Identity Management
- Configuring Certificate Services
- Introducing Cisco ISE Policy
- Implementing Third-Party Network Access Device Support
- Introducing Cisco TrustSec
- TrustSec Configuration
- Easy Connect

Web Authentication and Guest Services

- Introducing Web Access with Cisco ISE
- Introducing Guest Access Components
- Configuring Guest Access Services
- Configure Sponsor and Guest Portals

Cisco ISE Profiler

- Introducing Cisco ISE Profiler
- Profiling Deployment and Best Practices

Cisco ISE BYOD

- Introducing the Cisco ISE BYOD Process
- Describing BYOD Flow
- Configuring the My Devices Portal
- Configuring Certificates in BYOD Scenarios

Cisco ISE Endpoint Compliance Services

- Introducing Endpoint Compliance Services
- Configuring Client Posture Services and Provisioning

Working with Network Access Devices

- Cisco ISE TACACS+ Device Administration
- Configure TACACS+ Device Administration Guidelines and Best Practices
- Migrating from Cisco ACS to Cisco ISE

Labs

- Access the SISE Lab and Install ISE 2.4
- Configure Initial Cisco ISE Setup, Gui Familiarization and System Certificate Usage
- Integrate Cisco ISE with Active Directory
- Configure Cisco ISE Policy
- Configure Access Policy for Easy Connect
- Configure Guest Access
- Configure Guest Access Operations
- Create Guest Reports
- Configure Profiling
- Customize the Cisco ISE Profiling Configuration
- Create Cisco ISE Profiling Reports
- Configure BYOD
- Blacklisting a Device
- Configure Cisco ISE Compliance Services
- Configure Client Provisioning
- Configure Posture Policies
- Test and Monitor Compliance Based Access
- Test Compliance Policy
- Configure Cisco ISE for Basic Device Administration
- Configure TACACS+ Command Authorization

Exam Details

This course leads to the 300-715 - Implementing and Configuring Cisco Identity Services Engine (SISA) exam.

Successful completion will earn you the CIsco Certified Specialist - Security Identity Management certification and satisfy the concentration requirement for the CCNP Security certification.

skilltec training
Moving forward in knowledge and training

Securing Networks with Cisco Firepower Next-Generation IPS

Course Code	SSFIPS
Duration	5 days

Overview

The Securing Networks with Cisco Firepower Next-Generation IPS course shows you how to deploy and use Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). This hands-on course gives you the knowledge and skills required to use the platform features and includes firewall security concepts, platform architecture and key features; in-depth event analysis including detection of network-based malware and file type, NGIPS tuning and configuration including application control, security intelligence, firewall, and network-based malware and file controls; Snort® rules language; file and malware inspection, security intelligence, and network analysis policy configuration designed to detect traffic patterns; configuration and deployment of correlation policies to take action based on events detected; troubleshooting; system and user administration tasks, and more.

Audience

Technical professionals who need to know how to deploy and manage a Cisco FirePower NGIPS in their network environment.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the components of Cisco Firepower Threat Defense and the managed device registration process.
- Detailing Next-Generation Firewalls (NGFW) traffic control and configuring the Cisco Firepower system for network discovery.
- Implementing access control policies and describing access control policy advanced features.
- Configuring security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection.
- Implementing and managing intrusion and network analysis policies for NGIPS inspection.
- Describing and demonstrating the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center.
- Integrating the Cisco Firepower Management Center with an external logging destination.
- Describing and demonstrating the external alerting options available to Cisco Firepower Management Center and configuring a correlation policy.
- Describing key Cisco Firepower Management Center software update and user account management features.
- Identifying commonly misconfigured settings within the Cisco Firepower Management Center and using basic commands to troubleshoot a Cisco Firepower Threat Defense device.

Pre-Requisites

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS
- CCNA Security (ICND1 and IINS) recommended.

Recommended courses:

- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

- **Cisco Firepower** Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- **File Control and** Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Network Analysis Policies
- Detailed Analysis Techniques
- Cisco Firepower Platform Integration
- Alerting and Correlation Policies
- System Administration
- Cisco Firepower **Troubleshooting**

Labs

- **Initial** Device Setup
- Device Management
- Configuring Network Discovery
- Implementing and Access Control Policy
- Implementing Security Intelligence
- File Control and Advanced Malware Protection
- Implementing NGIPS
- Customizing a Network Analysis Policy
- Detailed Analysis
- Configuring Cisco Firepower Platform Integration with Splunk
- Configuring Alerting and Event Correlation
- System Administration
- Cisco **Firepower Troubleshooting**

Exam Details

This course is currently not aligned to an exam.

skilltec training

Moving forward in knowledge and training

Securing Networks with Cisco Firepower Next-Generation Firewall

Course Code	SSNGFW
Duration	5 days

Overview

The Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 course shows you how to deploy and use Cisco Firepower® Threat Defense system. This hands-on course gives you knowledge and skills to use and configure Cisco® Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS). You can take these courses in any order.

Audience

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS and NGFW in their network environments.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system and identifying deployment scenarios.
- Performing initial Firepower Threat Defense device configuration and setup tasks.
- Describing how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense.
- Describing how to implement NAT by using Cisco Firepower Threat Defense.
- Performing an initial network discovery, using Cisco Firepower to identify hosts, applications and services.
- Describing the behavior, usage and implementation procedure for access control policies.
- Describing the concepts and procedures for implementing security Intelligence features.
- Describing Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware Protection.
- Implementing and managing intrusion policies.
- Describing the components and configuration of site-to-site VPN.
- Describing and configuring a remote-access SSL VPN that uses Cisco AnyConnect.
- Describing SSL decryption capabilities and usage.

Pre-Requisites

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, vpn and IPS concepts

Recommended courses:

- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Cisco Firepower Threat Defense Overview

- Examining Firewall and IPS Technology
- Firepower Threat Defense Features and Components
- Examining Firepower Platforms
- Examining Firepower Threat Defense Licensing
- Cisco Firepower Implementation Use Cases

Cisco Firepower NGFW Device Configuration

- Firepower Threat Defense Device Registration
- FXOS and Firepower Device Manager
- Initial Device Setup
- Managing NGFW Devices
- Examining Firepower Management Center Policies
- Examining Objects
- Examining System Configuration and Health Monitoring
- Device Management
- Examining Firepower High Availability
- Configuring High Availability
- Cisco ASA to Firepower Migration
- Migrating from Cisco ASA to Firepower Threat Defense

Cisco Firepower NGFW Traffic Control

- Firepower Threat Defense Packet Processing
- Implementing QoS
- Bypassing Traffic

Cisco Firepower NGFW Address Translation

- NAT Basics
- Implementing NAT
- NAT Rule Examples
- Implementing NAT

Cisco Firepower Discovery

- Examining Network Discovery
- Configuring Network Discovery

Implementing Access Control Policies

- Examining Access Control Policies
- Examining Access Control Policy Rules and Default Action
- Implementing Further Inspection
- Examining Connection Events
- Access Control Policy Advanced Settings
- Access Control Policy Considerations
- Implementing an Access Control Policy

Security Intelligence

- Examining Security Intelligence
- Examining Security Intelligence Objects
- Security Intelligence Deployment and Logging
- Implementing Security Intelligence

File Control and Advanced Malware Protection

- Examining Malware and File Policy
- Examining Advanced Malware Protection

Next-Generation Intrusion Prevention Systems

- Examining Intrusion Prevention and Snort Rules
- Examining Variables and Variable Sets
- Examining Intrusion Policies

Site-to-Site VPN

- Examining IPsec
- Site-to-Site VPN Configuration
- Site-to-Site VPN Troubleshooting
- Implementing Site-to-Site VPN

Remote-Access VPN

- Examining Remote-Access VPN
- Examining Public-Key Cryptography and Certificates
- Examining Certificate Enrollment
- Remote-Access VPN Configuration
- Implementing Remote-Access VPN

SSL Decryption

- Examining SSL Decryption
- Configuring SSL Policies
- SSL Decryption Best Practices and Monitoring

Detailed Analysis Techniques

- Examining Event Analysis
- Examining Event Types
- Examining Contextual Data
- Examining Analysis Tools
- Threat Analysis

System Administration

- Managing Updates
- Examining User Account Management Features
- Configuring User Accounts
- System Administration

Cisco Firepower Troubleshooting

- Examining Common Misconfigurations
- Examining Troubleshooting Commands
- Firepower Troubleshooting

Labs

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

Exam Details

This course leads to the 300-710 - Securing Networks with Cisco Firepower (SNCF) exam.

Please note you should also attend the Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS) in preparation for this exam.

Implementing Secure Solutions with Virtual Private Networks

Course Code	SVPN
Duration	5 days

Overview

The Implementing Secure Solutions with Virtual Private Networks (SVPN) course teaches you how to implement, configure, monitor, and support enterprise Virtual Private Network (VPN) solutions. Through a combination of lessons and hands-on experiences you will acquire the knowledge and skills to deploy and troubleshoot traditional Internet Protocol Security (IPsec), Dynamic Multipoint Virtual Private Network (DMVPN), FlexVPN, and remote access VPN to create secure and encrypted data, remote accessibility, and increased privacy.

Audience

Network engineers responsible for selecting, designing and deploying secure solutions using VPNs.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Introducing site-to-site VPN options available on Cisco router and firewalls.
- Introducing remote access VPN options available on Cisco router and firewalls.
- Reviewing site-to-site and remote access VPN design options.
- Reviewing troubleshooting processes for various VPN options available on Cisco router and firewalls.

Pre-Requisites

- Familiarity with the various Cisco router and firewall command modes
- Experience navigating and managing Cisco routers and firewalls
- Clear understanding of the benefits of site-to-site and Remote Access VPN options

Recommended courses:

- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Introducing VPN Technology Fundamentals

- Role of VPNs in Network Security
- VPNs and Cryptography

Implementing Site-to-Site VPN Solutions

- Site-to-Site VPN Solutions Overview
- Cisco IOS VPN Point-to-Point Solutions
- Cisco ASA VPN Point-to-Point Solutions
- Cisco IOS VTI Point-to-Point Solutions
- Cisco DMVPN Solutions

Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions

- Overview of the Cisco FlexVPN Solution
- Point-to-Point Flex VPN
- Hub-and-Spoke FlexVPN
- Spoke-to-Spoke FlexVPN

Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions

- Overview of Cisco GET VPN Solution
- Configure GET VPN

Implementing Cisco AnyConnect VPNs

- Remote Access Overview
- Design Remote Access Solutions
- Basic Cisco AnyConnect VPN on Cisco ASA
- Advanced Cisco AnyConnect TLS VPN on Cisco ASA
- Advanced AAA in Cisco AnyConnect VPNs
- Cisco AnyConnect IKEv2 VPNs

Implementing Clientless VPNs

- Remote Access Overview
- Design Remote Access Solutions
- Clientless TLS VPN Overview
- Basic Cisco AnyConnect TLS VPN on Cisco ASA
- Application Access in Cisco ASA Clientless VPN
- Advanced AAA in Clientless VPN

Labs

- Explore IPsec Technologies
- Implement and Verify Cisco IOS Point-to-Point VPN
- Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Troubleshoot DMVPN
- Implement and Verify FlexVPN with Smart Defaults
- Implement and Verify Point-to-Point FlexVPN
- Implement and Verify Hub and Spoke FlexVPN
- Implement and Verify Spoke-to-Spoke FlexVPN
- Troubleshoot Cisco IOS FlexVPN
- Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on AnyConnect VPN
- Implement and Verify Clientless VPN on ASA

Exam Details

This course leads to the 300-730 - Implementing Secure Solutions with Virtual Private Networks (SVPN) exam.

Successful completion will earn you the Cisco® Certified Specialist - Network Security VPN Implementation certification and satisfy the concentration exam requirement for the CCNP Security certification.

Securing the Web with Cisco Web Security Appliance

Course Code	SWSA
Duration	2 days

Overview

Learn how to implement, use, and maintain a Cisco® Web Security Appliance (WSA), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, you'll learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more.

This course is worth 16 Credits in the Continuing Education Program.

Audience

Individuals involved in the deployment, installation and administration of a Cisco Web Security Appliance.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing Cisco WSA.
- Deploying proxy services.
- Utilizing authentication.
- Describing decryption policies to control HTTPS traffic.
- Understanding differentiated traffic access policies and identification profiles.
- Enforcing acceptable use control settings.
- Defending against malware.
- Describing data security and data loss prevention.
- Performing administration and troubleshooting.

Pre-Requisites

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

Recommended qualifications (1 of the following):

- Cisco certification (CCENT or higher) - ICND1 Recommended
- Relevant industry certification (ISC)2, (CompTIA) Security+, EC-Council, GIAC, ISACA
- Cisco Net Academy letter of completion (CCNA 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Recommended courses:

- G013 - CompTIA Security+
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Describing Cisco WSA

- Technology Use Case
- Cisco WSA Solution
- Cisco WSA Features
- Cisco WSA Architecture
- Proxy Service
- Integrated Layer 4 Traffic Monitor
- Data Loss Prevention
- Cisco Cognitive Intelligence
- Management Tools
- Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
- Cisco Content Security Management Appliance (SMA)

Deploying Proxy Services

- Explicit Forward Mode vs. Transparent Mode
- Transparent Mode Traffic Redirection
- Web Cache Control Protocol
- Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
- Proxy Bypass
- Proxy Caching
- Proxy Auto-Config (PAC) Files
- FTP Proxy
- Socket Secure (SOCKS) Proxy
- Proxy Access Log and HTTP Headers
- Customizing Error Notifications with End User Notification (EUN) Pages

Utilizing Authentication

- Authentication Protocols
- Authentication Realms
- Tracking User Credentials
- Explicit (Forward) and Transparent Proxy Mode
- Bypassing Authentication with Problematic Agents
- Reporting and Authentication
- Re-Authentication
- FTP Proxy Authentication
- Troubleshooting Joining Domains and Test Authentication
- Integration with Cisco Identity Services Engine (ISE)

Creating Decryption Policies to Control HTTPS Traffic

- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
- Certificate Overview
- Overview of HTTPS Decryption Policies
- Activating HTTPS Proxy Function
- Access Control List (ACL) Tags for HTTPS Inspection
- Access Log Examples

Understanding Differentiated Traffic Access Policies and Identification Profiles

- Overview of Access Policies
- Access Policy Groups
- Overview of Identification Profiles
- Identification Profiles and Authentication
- Access Policy and Identification Profiles Processing Order
- Other Policy Types
- Access Log Examples
- ACL Decision Tags and Policy Groups
- Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications

Defending Against Malware

- Web Reputation Filters
- Anti-Malware Scanning
- Scanning Outbound Traffic
- Anti-Malware and Reputation in Policies
- File Reputation Filtering and File Analysis
- Cisco Advanced Malware Protection
- File Reputation and Analysis Features
- Integration with Cisco Cognitive Intelligence

Enforcing Acceptable Use Control Settings

- Controlling Web Usage
- URL Filtering
- URL Category Solutions
- Dynamic Content Analysis Engine
- Web Application Visibility and Control
- Enforcing Media Bandwidth Limits
- Software as a Service (SaaS) Access Control
- Filtering Adult Content

Data Security and Data Loss Prevention

- Data Security
- Cisco Data Security Solution
- Data Security Policy Definitions
- Data Security Logs

Performing Administration and Troubleshooting

- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports
- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface

Labs

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication
- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Validate an Intermediate Certificate
- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

Exam Details

There is no exam currently aligned to this course.

skilltec training

Moving forward in knowledge and training

Implementing DevOps Solutions and Practices Using Cisco Platforms

Course Code	C-DEVOPS
Duration	5 days

Overview

The Implementing DevOps Solutions and Practices Using Cisco Platforms course teaches you how to automate application deployment, enable automated configuration, enhance management and improve scalability of cloud microservices and infrastructure processes on Cisco® platforms. Learn to integrate Docker and Kubernetes to create advanced capabilities and flexibility in application deployment.

Audience

Network and software engineers interested in automation and programmability.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the DevOps philosophy and practices, and how they apply to real-life challenges.
- Explaining container-based architectures and available tooling provided by Docker.
- Describing application packaging into containers and start building secure container images.
- Utilizing container networking and deploying a three-tier network application.
- Explaining the concepts of configuration item (CI) pipelines and what tooling is available.
- Implementing a basic pipeline with Gitlab CI that builds and deploys applications.
- Implementing automated build testing and validation.
- Describing DevOps principles applied to infrastructure.
- Implementing on-demand test environments and explaining how to integrate them with an existing pipeline.
- Implementing tooling for metric and log collection, analysis, and alerting.
- Describing the benefits of application health monitoring, telemetry, and chaos engineering in the context of improving the stability and reliability of the ecosystem.
- Describing how to implement secure DevOps workflows by safely handling sensitive data and validating applications.
- Explaining design and operational concepts related to using a mix of public and private cloud deployments.
- Describing modern application design and microservices architectures.
- Describing the building blocks of Kubernetes and how to use its APIs to deploy an application.
- Explaining advanced Kubernetes deployment patterns and implementing an automated pipeline.
- Explaining how monitoring, logging, and visibility concepts apply to Kubernetes.

Pre-Requisites

- Basic programming language concepts and familiarity with Python
- Basic understanding of compute virtualization
- Ability to use Linux, text-driven interfaces, and CLI tools, such as Secure Shell (SSH), bash, grep, ip, vim/nano, curl, ping, traceroute, and telnet
- Foundational understanding of Linux-based OS architecture and system utilities
- CCNA® level core networking knowledge
- Foundational understanding of DevOps concepts
- Awareness and familiarity with continuous integration, continuous deployment, and continuous delivery CI/CD) concepts
- Hands-on experience with Git

Course Contents

Introducing the DevOps Model

- DevOps Philosophy
- DevOps Practices

Introducing Containers

- Container-Based Architectures
- Linux Containers
- Docker Overview
- Docker Commands

Packaging an Application Using Docker

- Dockerfiles
- Golden Images
- Safe Processing Practices

Deploying a Multitier Application

- Linux Networking
- Docker Networking
- Docker Compose

Introducing CI/CD

- Continuous Integration
- CI Tools
- DevOps Pipelines

Building the DevOps Flow

- GitLab Overview
- GitLab CI Overview
- Continuous Delivery with GitLab

Validating the Application Build Process

- Automated Testing in the CI Flow

Building an Improved Deployment Flow

- Post deployment Validation
- Release Deployment Strategies

Extending DevOps Practices to the Entire Infrastructure

- Introduction to NetDevOps
- Infrastructure as Code

Implementing On-Demand Test Environments at the Infrastructure Level

- Configuration Management Tools
- Terraform Overview
- Ansible Overview
- Ansible Inventory File
- Use the Cisco IOS Core Configuration Module
- Jinja2 and Ansible Templates
- Basic Jinja2 with YAML
- Configuration Templating with Ansible

Monitoring in NetDevOps

- Introduction to Monitoring, Metrics and Logs
- Introduction to Elasticsearch, Beats and Kibana
- Introduction to Prometheus and Instrumenting Python Code for Observability

Engineering for Visibility and Stability

- Application Health and Performance
- AppDynamics Overview
- Chaos Engineering Principles

Securing DevOps Workflows

- DevSecOps Overview
- Application Security in the CI/CD Pipeline
- Infrastructure Security in the CI/CD Pipeline

Exploring Multicloud Strategies

- Application Deployment to Multiple Environments
- Public Cloud Terminology Primer
- Tracking and Projecting Public Cloud Costs
- High Availability and Disaster Recovery Design Considerations
- IaC for Repeatable Public Cloud Consumption
- Cloud Services Strategy Comparison

Examining Application and Deployment Architectures

- The Twelve-Factor Application
- Microservices Architectures

Describing Kubernetes

- Kubernetes Concepts: Nodes, Pods and Clusters
- Kubernetes Concepts: Storage
- Kubernetes Concepts: Networking
- Kubernetes Concepts: Security
- Kubernetes API Overview

Integrating Multiple Data Center Deployments with Kubernetes

- Kubernetes Deployment Patterns
- Kubernetes Failure Scenarios
- Kubernetes Load-Balancing Techniques
- Kubernetes Namespaces
- Kubernetes Deployment via CI/CD Pipelines

Monitoring and Logging in Kubernetes

- Kubernete Resource Metrics Pipeline
- Kubernetes Full Metrics Pipeline and Logging

Labs

- Interact with GitLab Continuous Integration
- Explore Docker Command-Line Tools
- Package and Run a WebApp Container
- Build and Deploy Multiple Containers to Create a Three-Tier Application
- Explore Docker Networking
- Build and Deploy an Application Using Docker Compose
- Implement a Pipeline in Gitlab CI
- Automate the Deployment of an Application
- Validate the Application Build Process
- Validate the Deployment and Fix the Infrastructure
- Build a YAMl IaC Specification for the Test Enviroment
- Manage On-Demand Test Environments with Terraform
- Build Ansible Playbooks to Manage Infrastructure
- Integrate the Testing Enviroment in the CI/CD Pipeline
- Implement Pre-Deployment Health Checks
- Set Up Logging for the Application Servers and Visualize with Kibana
- Create System Dashboard Focused on Metrics
- Use Alerts Through Kibana
- Instrument Application Monitoring
- Use Alerts and Thresholds to Notify Webhook Listener and Webex Teams Room
- Secure Infrastructure in the CI/CD Pipeline
- Explore Kubernetes Setup and Deploy an Application
- Explore and Modify a Kubernetes CI/CD Pipeline
- Kubernetes Monitoring and Metrics - ELK

Exam Details

This course leads to the 300-910 - Implementing DevOps Solutions and Practices using Cisco Platforms exam.

Successful completion will earn you the Cisco Certified DevNet Specialist - DevOps certification, and satisfies the concentration exam requirement for the Cisco Certified DevNet Professional certification.

Implementing Automation for Cisco Collaboration Solutions

Course Code	CLAUI
Duration	3 days

Overview

The Implementing Automation for Cisco Collaboration Solutions (CLAUI) course teaches you how to implement Cisco® Collaboration automated, programmable solutions for voice, video, collaboration, and conferencing on-premises or in the cloud. Through a combination of lessons and hands-on labs, you will combine tools and processes to tackle communication challenges using key platforms including Cisco Unified Communications Manager, Cisco IP Phone Services, Cisco Unity® Connection, Cisco Finesse®, Cisco Collaboration Endpoints, Cisco Webex Teams™, and Cisco Webex® Meetings.

Learn how to use application programming interfaces (APIs) interfaces such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP), parsing data in Extensible Markup Language (XML) and JavaScript Object Notation (JSON) formats, and leverage frameworks such as Python.

Audience

Network and software engineers interested in Cisco Collaboration and Webex automation.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Examining API and automation capabilities and concepts for Cisco Unified Communication Manager.
- Examining API and automation capabilities and concepts for Cisco Unity Connection.
- Examining API and automation capabilities and concepts for Cisco Finesse.
- Examining Experience API (xAPI) and automation capabilities and concepts for Cisco Collaboration endpoints.
- Examining API and automation capabilities and concepts for Cisco Webex Teams.
- Examining API and automation capabilities and concepts for Cisco Webex Meetings.

Pre-Requisites

- Basic knowledge of Simple Object Access Protocol (SOAP) and REST APIs
- Basic programming and scripting skills in Python
- Intermediate knowledge in managing and configuring three or more of the following Cisco Collaboration offerings: Cisco Unified Communications Manager; Cisco IP Phones; Cisco Finesse; Cisco Webex Devices (Collaboration and Video Endpoints); Cisco Webex Teams.; Cisco Webex Meetings.

Recommended courses:

- CLCOR - Implementing and Operating Cisco Collaboration Core Technologies

Course Contents

Automating Cisco Unified Communications Manager

- Cisco Unified Communications Manager: AXL API Overview
- Built-In AXL API Calls
- SQL API Calls
- Computer Telephony Integration
- CDRs and Performance APIs
- Phone Services APIs

Automating Cisco Unity Connection

- Cisco Unity Connection

Automating Cisco Finesse

- Cisco Finesse APIs
- Cisco Finesse Gadgets

Examining Cisco Collaboration Endpoint Automation

- Cisco xAPI Overview
- In-Room Control Editor Introduction
- Macro Introduction

Examining Cisco Cloud Collaboration Automation

- Cisco Webex Administration API Overview
- Cisco Webex Teams Bots Overview
- Widgets Overview
- Cisco Webex Teams SDK

Examining Cisco Conferencing Automation

- Cisco Webex Meetings API
- Cisco Meeting Server API

Labs

- Configure the Initial Collaboration Lab Environment
- Verify Phone Details
- Configure Phone Line Label
- Configure User Pin
- Configure System Forward No Answer Timer
- Configure Route Plan Report
- Deploy Basic SQL Query
- Deploy Advanced SQL Query
- Configure and Alternate Extension in Cisco Unity Connection
- Configure Voicemail Pin
- Verify Agent Settings
- Deploy Gadget
- Configure Cisco Webex Meetings User
- Configure and Record Cisco Webex Meeting
- Verify System Status
- Configure Host Access on Cisco Meeting Server Spaces

Exam Details

This course leads to the 300-835 - Automating and Programming Cisco Collaboration Solutions (CLAUTO) exam.

Successful completion will earn you the Cisco Certified DevNet Specialist - Collaboration Automation and Programmability certification and satisfy the concentration exam requirements for the Cisco CCNP Collaboration Certification and the Cisco Certified DevNET Professional certification.

Developing Applications and Automating Workflows using Cisco Platforms

Course Code	DEVASC
Duration	5 days

Overview

The Developing Applications and Automating Workflows Using Cisco Core Platforms course helps you prepare for the Cisco® DevNet Associate certification and for associate-level network automation engineer roles. You will learn how to implement basic network applications using Cisco platforms as a base, and how to implement automation workflows across network, security, collaboration, and computing infrastructure. The course gives you hands-on experience solving real world problems using Cisco Application Programming Interfaces (APIs) and modern development tools.

This course helps you prepare for the DevNet Associate (DEVASC) exam. By passing this exam, you earn the Cisco Certified DevNet Associate certification.

Please note this course is a combination of Instructor-Led and Self-Paced Study; 5 days in the classroom and approximately 3 days of self-study. The self-study content will be provided as part of the digital courseware that you receive at the beginning of the course and should be part of your preparation for the exam.

Audience

This course is designed for anyone who performs or seeks to perform a developer role and has one or more years of hands-on experience developing and maintaining applications that are built on top of Cisco platforms.

The course is appropriate for software developers, application developers, and network engineers who want to expand their skill base and validate their skills in programmability, software, and automation. Students preparing for Cisco Certified DevNet Associate certification.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the importance of APIs and use of version control tools in modern software development.
- Describing common processes and practices used in software development.
- Describing options for organizing and constructing modular software.
- Describing HTTP concepts and how they apply to network-based APIs.
- Applying Representational State Transfer (REST) concepts to integration with HTTP-based APIs.
- Describing Cisco platforms and their capabilities.
- Describing programmability features of different Cisco platforms.
- Describing basic networking concepts and interpret simple network topology.
- Describing interaction of applications with the network and tools used for troubleshooting issues.
- Applying concepts of model-driven programmability to automate common tasks with Python scripts.
- Identifying common application deployment models and components in the development pipeline.
- Describing common security concerns and types of tests, and utilize containerization for local development.
- Utilizing tools to automate infrastructure through scripting and model-driven programmability.

Pre-Requisites

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Hands-on experience with a programming language (specifically Python)

Recommended courses:

- PRNE-CPLL - Programming for Network Engineers - CPLL

Course Contents

Practicing Modern Software Development
Rise of APIs in Software Design
API Data Formats
Serialization and Deserialization of Data
Collaborative Software Development
Version Control with GIT
Branching with GIT

Describing Software Development Process (Self-Study)
Software Development Methodologies
Test-Driven Development
TDD Example
Code Review

Designing Software (Self-study)
Modular Software Design
Modular Design Benefits
Architecture and Design Patterns
MVC Architecture Pattern
Observer Design Pattern

Introducing Network-Based APIs
HTTP Protocol Overview
HTTP Protocol Applied to Web-Based APIs
HTTP Content Negotiation
RPC-Style APIs
REST-Style APIs
Postman for REST API Consumption
Advanced Postman Topics
Consuming notification Events Using Webhooks

Consuming REST-Based APIs
Common API Constraints
API Authentication Mechanisms
Using HTTP Authentication
Leveraging HTTPS for Security
Handling Secrets for API Consumption

Introducing Cisco Platforms and APIs (Self-study)
Cisco Network Management Platforms
Cisco Compute Management Platforms
Cisco Compute Management APIs
Cisco Collaboration Platforms
Cisco Collaboration APIs
Cisco Security Platforms
Cisco Security APIs
Cisco Network Management Platforms in Cloud

Employing Programmability on Cisco Platforms
Automating Cisco Network Operations
Cisco IOS XE Device-Level APIs
Cisco NX-OS Device-Level APIs
Cisco Controller APIs
Automating Cisco Webex Teams Operations
DevNet Developer Resources

Describing IP Networks (Self-Study)
Basic Networking Concepts
MAC Addresses and VLANs
Network Routes and Routing
Transport Layer and Packet Delivery
Network Device Planes

Relating Network and Applications
Standard IP Network Services
Network Address Translation
Common Protocols
Application Connectivity Issues
Tools for Troublshooting Connectivity Issues
Explaining the Impact of Network Constraints on Applications

Employing Model-Driven Programmability
Model-Driven Programmability Stack
Network Automation and NETCONF
Exploring YANG Models
Utilizing Data Models with RESTCONF Protocol
Using Python Scripts and Cisco SDKs
Model Driven Programmability in a Cisco Environment

Deploying Applications
Application Deployment Types
Application Deployment Models
Edge Computing Overview
DevOps Practices and Principles
Components of a CI-CD Pipeline
Essential Bash Commands for Development and Operations

Automating Infrastructure
SDN and Intent-Based Networking
Infrastructure as Code
System Management with Ansible
Infrastructure Automation with Ansible Playbooks
CI/CD Pipelines for Infrastructure Automation

Testing and Securing Applications
Software Test Types
Verifying Code Behaviour with Unit Tests
Dockerfile Composition
Using Docker in a Local Developer Environment
Application Security
Securing and Scaling Application Ingress Traffic
Network Simulation and Test Tools

Labs
Parse API Data Formats with Python
Use Git for Version Control
Identify Software Architecture and Design Patterns on a Diagram
Implement Singleton Pattern and Abstraction-Based Method
Inspect HTTP Protocol Messages
Use Postman
Troubleshoot an HTTP Error Response
Utilize APIs with Python
Use the Cisco Controller APIs
Use the Cisco Webex Teams™ Collaboration API
Interpret a Basic Network Topology Diagram
Identify the Cause of Application Connectivity Issues
Perform Basic Network Configuration Protocol (NETCONF) Operations
Use Cisco Software Development Kit (SDK) and Python for Automation Scripting
Utilize Bash Commands for Local Development
Construct Infrastructure Automation Workflow
Construct a Python Unit Test
Interpret a Dockerfile
Utilize Docker Commands to Manage Local Developer Environment
Exploit Insufficient Parameter Sanitization

Exam Details

This course leads to the 200-901 - DevNet Associate Exam.

Developing Applications Using Cisco Platforms and APIs

Course Code	DEVCOR
Duration	5 days

Overview

The Developing Applications Using Cisco Core Platforms and APIs (DEVCOR) course helps you prepare for the Cisco DevNet Professional certification and for professional-level network automation engineer roles. You will learn how to implement network applications using Cisco® platforms as a base, from initial software design to diverse system integration, as well as testing and deployment automation. The course gives you hands-on experience solving real world problems using Cisco Application Programming Interfaces (APIs) and modern development tools.

To fully benefit from this course, you should have three to five years of experience designing and implementing applications that are built on top of Cisco platforms.

Please note this course is a combination of Instructor-Led and Self-Paced Study; 5 days in the classroom and approximately 3 days of self-study. The self-study content will be provided as part of the digital courseware that you receive at the beginning of the course and should be part of your preparation for the exam.

Audience

This course is designed for anyone who performs or seeks to perform a developer role and has one or more years of hands-on experience developing and maintaining applications that are built on top of Cisco platforms, as well as network engineers looking to expand their knowledge to include software and automation.

This course covers specialized material about designing, developing, and debugging applications using Cisco APIs and platforms, and managing and deploying applications on Cisco infrastructure.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the architectural traits and patterns that improve application maintainability.
- Describing the architectural traits and patterns that improve application serviceability.
- Identifying steps to design and build a ChatOps application.
- Implementing robust Representational State Transfer (REST) API integrations with network error handling, pagination, and error flow control.
- Describing the necessary steps for securing user and system data in applications.
- Describing the necessary steps for securing applications.
- Identifying common tasks in automated application release process.
- Describing best practices for application deployment.
- Describing methodologies for designing distributed systems.
- Describing the concepts of infrastructure configuration management and device automation.
- Utilizing Yet Another Next Generation (YANG) data models to describe network configurations and telemetry.
- Comparing various relational and nonrelational database types and how to select the appropriate type based on requirements.

Pre-Requisites

- Knowledge of program design and coding with focus on Python
- Familiarity with Ethernet, TCP/IP, and Internet-related networking
- Understand the utilization of APIs
- Understanding of software development and design methodologies
- Hands-on experience with a programming language (specifically Python)

Recommended courses:

- DEVASC - Developing Applications and Automating Workflows using Cisco Platforms

Course Contents

Designing for Maintainability (Self-study)

- Functional and Non-Functional Requirements
- Non-Functional Requirements and Application Quality
- Maintainability Through Design
- Maintainability Through Implementation
- Modularity in Application Design
- Dependency Injection

Designing for Serviceability (Self-study)

- Observability in Application Design
- Scalability in Application Design
- High Availability and Resiliency
- Latency and Rate Limiting
- Architectural Patterns
- Sequence Diagrams

Implementing ChatOps Application

- Introducing ChatOps
- ChatOps with Cisco Webex Teams
- API Sequence Diagramming
- ChatOps Application Design
- Managing SSIDs and Retrieving Location Data Using Cisco Meraki API

Describing Advanced REST API Integration

- Consuming Paginated REST API Endpoints
- REST API Network Error Strategies
- REST API Error Control Flow
- Optimizing API Usage

Securing Application Data (Self-study)

- Data Storage and Protecting Data Privacy
- Storing Application Secrets
- Public Key Infrastructure
- Configuring Public Key Certificates for Applications
- Applying End-to-End Encryption for APIs

Securing Web and Mobile Applications (Self-study)

- OWASP Top 10
- Injection Attacks and Data Validation
- Cross-Site Scripting and Request Forgery
- OAuth Authorization Framework
- OAuth 2.0 Three-Legged Authorization Flow

Automating Application-Release

- Release Packaging and Dependency Management
- Advanced Version Control with Git
- Branching Strategies
- Continuous Testing and Static Code Analysis in CI Pipeline
- Identifying CI/CD Pipeline Failures

Deploying Applications

- 12-Factor App Methodology
- Containerizing Applications Using Docker
- Kubernetes Introduction
- Integrating Applications into Exisiting CI/CD Environment
- Hosting Applications on Network Devices

Understanding Distributed Systems

- Distributed Application Concepts
- Custom Dashboard Example
- Event-Driven Architecture Concepts
- Microservice Architecture Concepts
- Effective Distributed Application Logging Strategies
- Using Distributed Logging to Diagnose Problems
- Application Monitoring with Cisco AppDynamics
- Limitations of Distributed Systems and CAP Theorem
- Overcoming Challenges in Distributed Systems

Orchestrating Network and Infrastructure

- Configuring Servers Using Cisco UCS APIs
- Infrastructure as Code with Terraform
- Differentiating Configuration Management Solutions
- Configuring Network Parameters Using Puppet
- Configuring Network Parameters Using Ansible
- Defining Network Automation Source of Truth
- Creating and Deleting Objects Using Firepower Threat Defense API

Modeling Data with YANG

- YANG Overview
- XPath Query Language
- YANG Language Syntax
- Data Model Modularity
- Network Configuration Using RESTCONF
- Model-Driven Telemetry
- Streaming Telemetry with gNMI

Using Relational and Non-Relational Databases (Self-study)

- Evaluating Database Types to Meet Application Needs
- Relational Database Concepts
- Key-Value Database Concepts
- Document-Based Database Concepts
- Graph-Based Database Concepts
- Columnar-Based Database Concepts
- Time-Series Database Concepts

Labs

- Construct Sequence Diagram
- Construct Web Sequence Diagram
- Use Cisco Webex Teams™ API to Enable ChatOps
- Integrate Cisco Meraki™ API to List Service Set Identifiers (SSIDs) and Retrieve Location Data
- Use Paginated REST API Endpoint
- Utilize REST API Error Control Flow Techniques
- Evaluate Application for Common Open Web Application Security Project (OWASP) Vulnerabilities
- Resolve Merge Conflicts with Git
- Diagnose Continuous Integration and Continuous Delivery (CI/CD) Pipeline Failures
- Containerize Application Using Docker
- Integrate Application into Existing CI/CD Environment
- Diagnose Problems Using Application Logs
- Configure Network Parameters Using Ansible and Puppet
- Synchronize Firepower Device Configuration
- Utilize RESTCONF for Network Configuration
- Query Relational Database
- Query Document Store
- Query Time Series Database
- Query Graph Database

Exam Details

This course leads to the 350-901 - DEVCOR Exam.

Successful completion will satisfy the core exam requirement toward Cisco Certified DevNet Professional, and you earn the Cisco Certified DevNet Specialist – Core certification.

skilltec training
Moving forward in knowledge and training

Developing Solutions Using Cisco IoT and Edge Platforms

Course Code	DEVIOT
Duration	5 days

Overview

The Developing Solutions Using Cisco IoT and Edge Platforms course prepares you to develop Internet of Things (IoT) applications for Cisco® IoT edge compute and network architectures. Through a combination of lessons and hands-on experience, you will learn to implement and deploy Cisco IOx applications using Cisco Field Network Director and Cisco Kinetic.

This course covers designing, deploying, and troubleshooting edge applications, and understanding the use of management tools, so you can control your industrial network and connected devices at scale.

Audience

Network and software engineers who are interested in learning about automation and programmability.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Explaining the fundamentals of Cisco IoT and listing common devices involved.
- Listing the common protocols, standards, and data flows of IoT.
- Explaining the Cisco IoT, common needs, and the corresponding solutions.
- Explaining how programmability can be used to automate and make operations, deployment, and support of Cisco IoT more effective.
- Describing common Cisco IoT applications and how they apply to Cisco IoT use cases.
- Explaining the functions and use cases for Cisco security applications and Cisco IoT.

Pre-Requisites

- General software development or coding skills
- Basic functional and object-oriented programming skills
- Basic understanding of where applications live and how they are deployed in real-world scenarios
- Basic understand of how networking works
- Basic Linux OS skills: installing code language dependencies, installing code libraries, and general scripting
- Understanding of how to store code using git or another version-control system (VCS)

Recommended courses:

- DEVASC - Developing Applications and Automating Workflows using Cisco Platforms
- DEVCOR - Developing Applications Using Cisco Platforms and APIs

Course Contents

Defining Cisco IoT

- Describe Cisco IoT and the motivations behind it, as well common standards and protocols used in IoT and Cisco IoT

IoT Networking and Other Devices

- List common devices used with Cisco IoT

Examining IoT Protocols

- List the common protocols used with IoT

Examining IoT Standards

- Describe Cisco IoT common standards and protocols used in Cisco IoT

Recognizing Cisco IoT Needs and Solutions

- Describe the fundamentals of Cisco IoT operations

Using Programmability with Cisco IoT

- Explain how programmability can be used to automate and make operations, deployment, and support of Cisco IoT more effective

Describing Cisco IoT Applications

- Describe common Cisco IoT applications and how they apply to Cisco IoT use cases

Defining Cisco Security Applications

- Describe Cisco security applications that form a foundation for Cisco IOT security design considerations

Labs

- Use an MQTT Consumer to Subscribe to Sensor Data
- Use Cisco IOx Applications to Receive and Process Sensor Data
- Troubleshoot a Sensor Connection
- Use and Interpret Freeboard Data
- Use and Interpret Grafana Data
- Use and Interpret Kibana Data
- Cisco IOx Familiarity Lab
- Develop and Deploy a Cisco IOx Application
- Troubleshoot Cisco IOx
- Navigate Cisco Field Network Director
- Explore Cisco Field Network Director API

Exam Details

This course leads to the 300-915 - Developing Solutions Using Cisco IoT and Edge Platforms (DEVIOT) exam.

skilltec training
Moving forward in knowledge and training

Understanding Cisco Cybersecurity Operations Fundamentals

Course Code	CBROPS
Duration	5 days

Overview

The Understanding Cybersecurity Operations Fundamentals (CBROPS) course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification.

Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx. 1 day of self-study. The self-study content will be provided as part of the digital courseware that you will receive at the beginning of the course and should be part of your preparation for the exam.

Audience

This course is designed for an associate-level cybersecurity analyst who is working in security operation centers.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviours.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure the effectiveness of the SOC.
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.

- Describe a typical incident response plan and the functions of a typical CSIRT.
- Explain the use of VERIS to document security incidents in a standard format.
- Describe the Windows operating system features and functionality.
- Describe the Linux operating system features and functionality

Pre-Requisites

Attendees should meet the following prerequisites:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions

Course Contents

- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behaviour
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Describing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics

Labs

- Configure the Initial Collaboration Lab Environment
- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System

Exam Details

This course leads to the 200-201 - CBROPS Understanding Cisco Cybersecurity Operations Fundamentals exam.

Implementing Cisco NX-OS Switches and Fabrics in the Data Center

Course Code	DCNX
Duration	5 Days

Overview

The Implementing Cisco NX-OS Switches and Fabrics in the Data Center (DCNX) course gives you a detailed understanding of the Cisco® Nexus switch platform and teaches you how to install, configure, and manage Cisco Nexus® switch platforms in a scalable, highly available environment. Through a combination of lectures and hands-on labs, you will learn how to describe various aspects of the Cisco Nexus product families and platforms, including implementation, management, security, programmability and storage. Additionally, you will learn how to configure device aliases and zoning, Fibre Channel over Ethernet (FCoE), and N-Port Identifier Virtualization (NPIV), and N-Port Virtualization (NPV) modes.

Audience

Engineers using the Cisco Nexus Series Switch Platforms.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describe the platforms that make the Cisco Nexus 9000, 7000, 3000, and 2000 product families
- Describe Cisco Nexus platform implementations
- Explain Cisco Nexus platform management
- Describe Port Channels and Virtual Port Channels
- Configure First Hop Redundancy protocols
- Configure security features of Cisco Nexus devices
- Describe the Cisco Nexus devices routing and forwarding
- Describe Virtual Extensible LAN (VXLAN)
- Describe Quality of Service (QoS) on Cisco Nexus Devices
- Explain system management and monitoring processes
- Describe Cisco NX-OS programmability
- Describe Cisco Nexus storage services
- Configure device aliases and zoning
- Configure FCoE
- Configure NPIV and NPV modes

Pre-Requisites

- Be familiar with Cisco data center technologies
- Understand networking protocols, routing, and switching

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions
- DCFNDU - Understanding Cisco Data Center Foundations

Course Contents

Describing Cisco Nexus Series Switches

- Describe Cisco Nexus 9000 Series Switches
- Describe Cisco Nexus 7000 Series Switches
- Describe Cisco Nexus 3000 Series Switches
- Describe Cisco Nexus 2000 Series Fabric Extenders

Describing Cisco Nexus Platforms Implementation

- Describe Cisco Nexus in the Data Center Architecture
- Describe Cisco NX-OS Software
- Describe the Licensing Model

Describing Cisco Nexus Platforms Management

- Describe Cisco Nexus CLI and GUI Management Interfaces
- Describe Cisco NX-OS Setup Utility
- Describe Virtual Device Context on Cisco Nexus 7000 Series
- Describe PowerOn Auto Provisioning
- Describe Cisco NX-OS User Management
- Describe Cisco NX-OS AAA Services

Describing Port Channels and Virtual Port Channels

- Describe Port Channel Operation
- Describe vPC Concepts and Benefits
- Describe vPC Architecture
- Describe vPC Control and Data Plane

Configuring First Hop Redundancy Protocols

- Describe HSRP
- Describe VRRP

Configuring Cisco Nexus Security Features

- Configure Access Control Lists
- Configure Port Security
- Configure DHCP Snooping
- Configure Dynamic ARP Inspection
- Configure IP Source Guard
- Configure Unicast RPF
- Configure Keychain Management
- Configure Control Plane Policing
- Configure MACsec

Describing Cisco NX-OS Routing and Forwarding

- Describe Routing in Cisco NX-OS
- Describe Multicast Routing in Cisco NX-OS
- Describe Unicast and Multicast RIB and FIB in NX-OS
- Describe Layer 3 Best Practices for vPC

Describing Virtual Extensible LAN

- Describe VXLAN Benefits over VLAN
- Describe VXLAN Overlay
- Describe VXLAN MP-BGP EVPN Control Plane
- Describe VXLAN Data Plane

Describing QoS on Cisco Nexus Devices

- Describe QoS on Cisco Nexus Devices
- Configure QoS on Cisco Nexus Devices
- Describe Monitoring of QoS Statistics

Configuring System Management and Monitoring

- Configure System Management
- Configure System Monitoring and Troubleshooting Tools

Describing Cisco NX-OS Programmability

- Describe On-Box Programmability on Cisco NX-OS
- Describe Ansible for Cisco NX-OS

Describing Cisco Nexus Storage Services

- Describe IP Storage on Cisco Nexus Switches
- Describe Fibre Channel
- Describe Fibre Channel Flow Control
- Describe Fibre Channel Domain Initialization
- Describe Fibre Channel Addressing

Configuring Fibre Channel Over Ethernet

- Describe Fibre Channel over Ethernet
- Describe FCoE Requirements
- Describe Data Center Bridging
- Describe FCoE Addressing Scheme
- Describe FCoE Initialization Protocol
- Describe FCoE Port Types

Describing Device Aliases and Zoning

- Describe Distributed Device Alias Services
- Describe Zoning
- Describe Zone Merging
- Describe Recovering from Zone Merge Failures
- Describe Enhanced Zoning

Configuring NPIV and NPV Modes

- Describe N-Port ID Virtualization
- Describe Fibre Channel NPV Mode
- Describe FCoE NPV Mode

Labs

- Test Cisco Nexus Platforms
- Configure User Management
- Configure vPC
- Configure First Hop Redundancy Protocol (FHRP) Protocols
- Configure Cisco Nexus Security Features
- Configure Open Shortest Path First (OSPF)
- Configure VXLAN
- Configure QoS
- Configure System Management
- Configure Cisco NX-OS On-Box Programmability
- Configure Containers on Cisco NX-OS
- Configure Cisco NX-OS Using Ansible
- Configure Basic Fibre Channel Features
- Configure FCoE
- Configure Fibre Channel Device Aliases and Zoning
- Configure NPV

Exam Details

There is no exam relating directly to this course.

Engineering Cisco Meraki Solutions 1

Course Code	ECMS1
Duration	1 day

Overview

The Engineering Cisco Meraki Solutions Part 1 (ECMS1) course is an introductory course that equips you with the knowledge and skills to confidently operate Cisco Meraki solutions as a unified management system of an entire network from a centralized dashboard.
Through a full day of instruction including live demos and guided lab practice, you will learn how to implement core configurations for a full stack solution in the Meraki Dashboard and leverage essential Meraki Dashboard tools to enforce device security policies, deploy software and apps, and perform remote, live troubleshooting on managed devices.

This is the first of two courses that prepare you to take the **Cisco Meraki Solutions Specialist** certification exam.
Those who have already attended CMNO do not need to attend this training, as the content is the same.

Audience

Meraki operators interested in introductory-level technical training or in preparing for the Cisco Meraki Solutions Specialist certification.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describe cloud architecture, administration, and licensing
- Understand hardware and features of all product families
- Implement best practices for troubleshooting and when to contact support

Pre-Requisites

- CCNA Certified or have an equivalent level of technical expertise.

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions

Course Contents

Cloud and Dashboard

- Cisco Merkai Devices and the Cloud.
- Licensing

Products and Administration

- MV Security Cameras
- MI Web-based application analytics

Operating and Troubleshooting

- Dashboard sync and real-time tools
- Application Program Interfaces

Lab

- Configuring the dashboard
- Advanced Features
- Troubleshooting in the Dashboard

Exam Details

This course leads to the Cisco Meraki Solutions Specialist Exam.

skilltec training

Moving forward in knowledge and training

Engineering Cisco Meraki Solutions 2

Course Code	ECMS2
Duration	3 days

Overview

Engineering Cisco Meraki Solutions Part 2 (ECMS2) elevates your knowledge of Cisco® Meraki™ technology suite. In this advanced technical training course, you'll learn how to plan for network deployments and integrations using the Cisco Meraki platform. Through practical hands-on instruction and experiences, you will learn how to operate Meraki networks and troubleshoot complex network incidents using the Meraki Dashboard and analytics. You will also learn how to design Meraki architectures for redundancy, high-density, and scalability by implementing comprehensive Meraki product features to meet design objectives. This course is the second of two courses that prepares you for Cisco Meraki certification.

This course is the second of two courses that prepares you for Cisco Meraki certification.

Audience

This course is ideal for those who regularly deploy or manage Meraki networks and want to deepen their technical expertise and understanding of the full Meraki product suite and features. his may include professionals with job titles or in roles such as: Consulting Systems Engineer: Deployment Engineer; Network Administrator; Network Manager; Network Engineer; Site Reliability Engineer; Systems Engineer; Technical Solutions Architect; Wireless Design Engineer; Wireless Engineer.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Plan new Cisco Meraki architectures and expand existing deployments
- Design the network for scalable management and high availability
- Describe how to automate and scale Meraki deployments with dashboard tools
- Use dynamic routing protocols to expand networks and improve WAN performance
- Describe proper QoS, policy and performance-based routing configurations across a Cisco Meraki network and WAN optimization through traffic shaping
- Describe Virtual Private Network (VPN) and Wide Area Network (WAN) topologies and how to integrate them
- Secure, expand, and shape the network
- Implement switched network concepts and practices, and configure guests' networks
- Implement wireless configurations concepts and practices
- Describe endpoint management concepts and practices using Cisco Meraki Systems Manager
- Describe physical security concepts and practices
- Gain network insight by monitoring applications
- Describe how to prepare monitoring, logging, and alerting services
- Set up reporting and auditing capabilities in the Cisco Meraki dashboard
- Monitor and troubleshoot issues using Cisco Meraki tools

Pre-Requisites

- Completed ECMS1 or CMNO, or possess equivalent Meraki knowledge and experience
- Be CCNA-certified or have an equivalent level of technical expertise
- Be employed by Cisco Systems, a Meraki partner, or a Meraki customer

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions
- ECMS1 - Engineering Cisco Meraki Solutions 1

Course Contents

Planning New Meraki Architectures and Expanding Existing Deployments

- Cisco Meraki Solution Sizing
- Explore Various Dashboard User Interface Features Demo
- Licensing
- Reference

Designing for Scalable Management and High Availability

- Role-Based Access
- Tag Design and Structure
- Cisco Meraki MX Security Appliance High-Availability
- Cisco Meraki MS Switch High Availability
- High-Density Wireless Design

Automation and Scaling Meraki Deployments

- RBAC with SAML
- Configure SAML and Create SAML Roles Demo
- Network Cloning
- Clone a Network and Synchronize a Configuration Demo
- Configuration Templates
- Explore Configuration Templates Demo
- Network Provisioning with APIs
- Use Google Sheets and Script Editor with the Cisco Meraki Dashboard API Demo

Designing Routing on the Cisco Meraki Platform

- Routing Across Cisco Meraki Networks
- Explore Layer 3 Routing Including Creating, Editing and Moving SVIs Demo
- Dynamic Routing with OSPF
- BGP for Scalable WAN Routing and Redundancy

Describing QoS and Traffic Shaping Design

- Wireless and Wired QoS Design
- Prepare the Network for Voice
- Traffic shaping and Prioritizing on the Cisco Meraki MX Platform

Building VPN and WAN Topologies

- Cisco Meraki MX VPN Operation Modes
- VPN Design and Topologies
- Auto VPN
- Design a Scalable VPN Topology
- Explore the Cisco Merkai MX Sizing Guide Demo
- Integrate Cisco Meraki vMX into an Auto VPN Architecture
- SD-WAN Fundamentals
- SD-WAN Design
- Explore Cisco Meraki vMX and SD-WAN Configurations in the Dashboard Demo

Securing, Expanding and Shaping the Network

- Cisco Meraki Security Overview
- Default Behaviour and Rule-Processing Order
- Advanced Security Services
- Content Filtering
- Cisco Umbrella Integration

Describing Switched Network Concepts and Practices

- Access Policies Using Cisco Meraki Authentication
- Cloning of Switch Settings
- Switch Templates and Profiles
- Explore Switch Profiles Demo
- LAN and WLAN Guest Access Best Practices

Implementing Wireless Configuration Practices and Concepts

- Cisco Meraki Dashboard Maps and Floor Plans
- RF Profiles
- Wireless Encryption and Authentication
- SSID Modes for Client IP Addressing
- Bluetooth Low Energy
- BLE Scanning and Bluetooth Clients Demo
- Wireless Threats

Describing Endpoint Management Concepts and Practices

- Cisco Meraki Systems Manager Platform Overview
- Cisco Meraki Systems Manager Overview Demo
- Device Deployment Methodologies
- Deployment of Applications and Containerization Profiles
- Security Policies and Devices Out of Compliance Demo
- Pairing Network Group Policies with Systems Manager Demo
- Agentless Onboarding with Trusted Access

Describing Physical Security Concepts and Practices

- Cisco Meraki MV Architecture
- Flexible Camera Deployments with Wireless
- Cisco Meraki MV Product Portfolio, Features and Functionalities
- Motion Search, Motion Recap, Motion Heat Maps and Person Detection Demo
- Business Intelligence

Gaining Network Insight by Monitoring Applications

- Cisco Meraki Insight Overview
- Cisco Meraki Insight Scaling and Licensing
- Cisco Meraki Insight Overview: A Closer Look at Tracked Applications and WAN Health Demo

Preparing Monitoring, Logging and Alerting Services

- Logging Capabilities
- Examine Event, Change and Video Access Logs Demo
- Monitoring Tools and Services
- Examine Monitoring Tools and Features Demo
- Supported Alerts
- Cisco Meraki Dashboard API

Setting up Reporting and Auditing Capabilities in the Cisco Meraki Dashboard

- Cisco Meraki Reports
- Manage Firmware Through the Dashboard
- PCI Auditing

Gaining Visibility and Resolving Issues using Cisco Meraki Tools

- Troubleshooting Methods
- Logging Capabilities
- Cisco Meraki Security Center Overview Demo
- Wireless Troubleshooting
- Explore Wireless Troubleshooting Tools Demo
- Troubleshoot Cisco Merkai Cloud Application Performance
- Explore VPN Status, Firewall and Static Port Forwarding Information Demo
- Troubleshoot Cisco Meraki Auto VPN
- Local Status Page

Labs

- Configure Tags, Link Aggregation, Port Mirroring, and High-Density SSIDs
- Establishing Auto VPN
- Configuring Virtual Interfaces and Routing on Cisco Meraki MS Switches
- Configuring Routes and Redistribution
- Configuring Quality of Service
- Configuring Traffic Shaping
- Configuring Load Balancing
- Defining Firewall Rules
- Enabling Advanced Malware Protection, Intrusion Detection, and Intrusion Prevention
- Enabling Content Filtering
- Configure and Apply Access Policies
- Configure Wireless Guest Access
- Configure Service Set Identifiers (SSIDs)
- Implementing RF Profiles
- Implement Air Marshal
- Create Cisco Meraki Systems Manager (SM) Configuration Profiles
- Define Security Policies
- Enforce End-to-End Security
- Set-up Motion Alerts
- Deploy Wireless Cameras
- Manage Video Retention
- Enable Alerts
- Add Monitoring and Reporting
- Generate and Analyze Summary Reports
- Manage Firmware
- Generate a Peripheral Component Interconnect (PCI) Compliance Report
- Troubleshoot an Offline Device
- Troubleshoot Content Filtering
- Troubleshooting Remote Site Connectivity

Exam Details

This course leads to the 500-220 - ECMS - Cisco Meraki Solutions Specialist.