

CISCO

Revised 2/7/2012

/training/etc

The Art of Knowledge.

This Page Intentionally Left Blank

Table of Contents

Data Center

DCUFI v4.0 - Implementing Cisco Data Center Unified Fabric.....	1
DCNX1K v1.0 - Implementing the Cisco Nexus 1000V	2
ICN52K v3.0 - Implementing the Cisco Nexus 5000 and 2000.....	3
DCNID v2.0 - Data Center Network Infrastructure Design.....	4
DCUCD v4.0 - Designing Cisco Virtualized Data Centers.....	5
ICN7K v3.0 - Implementing the Cisco Nexus 7000.....	6
IEDIS V1.0 - Implementing Enterprise Data Center Infrastructure Security.....	7
DCUCI v4.0 - Data Center Unified Computing Implementation.....	8
UC-UCS v3.0- Installing Cisco UC on UCS.....	9

Enterprise (Switches & Routers)

ICND1 v1.1 - Interconnecting Cisco Network Devices 1.....	10
ICND2 v1.1 - Interconnecting Cisco Network Devices 2.....	11
CCNAX v1.1 - Interconnecting Cisco Networking Devices: Accelerated.....	12
IP6FD v3.0 - IPv6 Fundamentals, Design and Deployment.....	13
CCIE-RSW-N - CCIE Routing & Switching Written Boot Camp.....	14
IUWNE v1.0 - Implementing Cisco Unified Wireless Networking Essentials.....	15
ROUTE v1.0 - Implementing Cisco IP Routing.....	16
SWITCH v1.0 - Implementing Cisco Switched Networks	17
TSHOOT v1.0 - Troubleshooting and Maintaining Cisco IP Networks.....	18

IP Communications

CCMSA v6.0 - Cisco Communications Manager System Administration.....	19
UCA v8.5 - Unity Connection Administration.....	20
CIPT1 v8.0 - Implementing Cisco Unified Communications Manager Part 1	21
CIPT2 v8.0 - Implementing Cisco Unified Communications Manager, Part 2.....	22
CIPT2 v7.0/v6.0 - Implementing Cisco Unified Communications IP Telephony Part 2.....	23
CVOICE v8.0 - Implementing Cisco Voice Communications and QoS.....	24
TUC v1.0 - Troubleshooting Cisco Unified Communications Systems.....	25
CMA v8.5 - Communications Manager Administration.....	26
CAPPS v8.0 - Integrating Cisco Unified Communications Applications.....	27
TVOICE v8.0 - Troubleshooting Cisco Unified Communications.....	28

IP Contact Center (ICM, IPCC)

ICMBC v7.0 - Intelligent Contact Manager Boot Camp.....	29
IPCCE v1.0 - IP Contact Center Enterprise.....	30
UCCXD v4.0 - Deploying Cisco Unified Contact Center Express.....	31
CVPI v7.0 - Cisco Unified Customer Voice Portal Implementation.....	32

SANs (MDS)

ICSNS v4.2 - Implementing Cisco Storage Networking Solutions.....	33
---	----

Security

IPS v6.0 - Implementing Cisco Intrusion Prevention System.....	34
CANAC v2.1 - Implementing Cisco NAC Appliance.....	35
MARS v3.0 - Cisco Security Monitoring, Analysis and Response System.....	36
IINS v1.0 - Implementing Cisco IOS Network Security.....	37
FIREWALL v2.0 - Deploying Cisco ASA Firewall Features.....	38
SECURE v1.0 - Securing Networks with Cisco Routers and Switches.....	39
VPN 1.0 - Deploying Cisco ASA VPN Solutions.....	40

This Page Intentionally Left Blank

Course Description:

The DCUFI v4.0 - Implementing Cisco Data Center Unified Fabric is a five-day instructor-led course with lab exercises that are intended to prepare students for the certification exam. The course schedule consists of approximately 50 percent lecture and 50 percent lab exercises. The Delivery Lab for this course is accessed using a remote access procedure coupled with a GUI application that provides connectivity to all lab devices.

Who Should Attend:

The primary audience for this course are network engineers, systems engineers, consulting systems engineers, technical solutions architects, and Cisco integrators and Partners who sell, implement, and maintain Cisco Nexus products in the data center. The secondary audience for this course are network designers, network administrators, and network managers responsible for identifying and managing Cisco Nexus products in the data center.

Prerequisites:

The knowledge and skills that a learner must have before attending this course are a good understanding of networking protocols (recommended CCNA Certification), good understanding of the Fibre Channel protocol and the SAN environment (recommended attendance of a Fibre Channel protocol class or equivalent experience), and recommended attendance of the Implementing Cisco Storage Network Solutions (ICSNS) class or equivalent experience.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify the Cisco Nexus product family, specifically the Cisco Nexus 7000 Switch chassis and components, the Cisco Nexus 5000 Switch, and the Cisco Nexus 2000 Fabric Extender
- Install the Cisco Nexus products in a Cisco Data Center Business Advantage environment
- Identify how to plan and implement virtual device contexts into the solution, given a requirement
- Evaluate the security features available on the Cisco Nexus 7000 Switch to identify which features should be implemented into a solution
- Evaluate and configure the Connectivity Management Processor on the Cisco Nexus 7000 Switch and identify the management options available
- Evaluate the service-level and network-level high availability of the Cisco Nexus switches and how to use the Cisco IOS In-Service Software Upgrade feature
- Discuss the Fibre Channel protocol including Fibre Channel addressing, flow control, and zoning

Course Outline:**Module 1: Cisco Nexus Product Overview**

Identifying the Cisco Data Center Business Advantage Architecture
Identifying Cisco Nexus Products
Identifying the Cisco Unified Fabric Solution
Integrating Services

Module 2: Cisco Nexus Switch Feature Configuration

Configuring Virtual Device Contexts
Configuring Layer 2 Switching Features
Configuring Port Channels
Configuring Layer 3 Switching Features
Configuring IP Multicast
Lab 2-1: Configuring Layer 2 Switching
Lab 2-2: Configuring vPCs
Lab 2-3: Configuring Layer 3 Switching

Module 3: Cisco Nexus Switch Advanced Feature Configuration

Configuring Security Features
Understanding Overlay Transport Virtualization
Implementing Quality of Service
Lab 3-1: Configuring Security Features
Lab 3-2: Configuring OTV
Lab 3-3: Configuring QoS

Module 4: Cisco Nexus Series Switch Management

Using the Connectivity Management Processor
Configuring User Management
Understanding System Management
Lab 4-1: Configuring System Management
Lab 4-2: Implementing Cisco DCNM

Module 5: Redundancy on Cisco Nexus Switches

Understanding High Availability and Redundancy
Implementing Cisco FabricPath
Lab 5-1: Configuring Cisco FabricPath

Module 6: Fibre Channel over Ethernet

Understanding Fibre Channel Protocol
Understanding FCoE Protocol
Identifying Data Center Bridging Ethernet Enhancements

Module 7: Fibre Channel over Ethernet Configuration

Implementing FCoE
Configuring SAN Switching Features
Configuring NPV Mode
Using SAN Management Tools
Lab 7-1: Configuring FCoE
Lab 7-2: Configuring NPV

Module 8: Troubleshooting on Cisco Nexus Switches

Troubleshooting the Data Center Infrastructure
Troubleshooting Tools and Resources

Course Description:

This course is a 3-day ILT training program designed for systems and field engineers who install and implement the Cisco Nexus 1000V Switch. The course covers the key components and procedures you need to know to install, configure, manage, and troubleshoot the Cisco Nexus 1000V Switch.

Who Should Attend:

The primary students for this course are Network, systems, and consulting systems engineers, as well as server administrators. The secondary students for this course are Network designers, administrators, and managers.

Prerequisites:

Students must have a good understanding of networking protocols and of the VMware environment. It is recommended that students have attended the VMware vSphere: Install, Configure, Manage class or have equivalent knowledge. It is also recommended that students have CCNA Certification.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Position the VMware networking solution
- Position the Cisco Nexus 1000V Switch in the VMware infrastructure, install the Virtual Supervisor and Virtual Ethernet Modules, and establish an SVS connection to the vCenter Server
- Configure the key features of the Cisco Nexus 1000V Switch and understand how these features are used in the data center virtual infrastructure design
- Identify which management features should be implemented on the Cisco Nexus 1000V and how to configure the features selected
- Identify which tools can be used when troubleshooting the Cisco Nexus 1000V and how to troubleshoot key features

Course Outline:**VMware Networking Overview**

Reviewing the Virtual Infrastructure
Networking in the VMware Infrastructure
Configuring VMware Switching
Lab 1-1 Setting Up the Lab Environment

Cisco Nexus 1000V Series Switch Installation

Reviewing the Cisco Nexus 1000V Product
Reviewing the Cisco Nexus 1010 Virtual Services Appliance and Virtual Service Blades
Installing the Virtual Supervisor and Virtual Ethernet Modules
Lab 2-1 Install the Cisco Nexus 1000V VSM
Lab 2-2 Install the Cisco Nexus 1000V VEM

Cisco Nexus 1000V Feature Configuration

Configuring Port Profiles
Configuring Security Features
Configuring Quality of Service
Lab 3-1 Optimize the Cisco Nexus 1000V Implementation
Lab 3-2 Configuring Security Features
Lab 3-3 Configuring Quality of Service

Cisco Nexus 1000V Switch Management

Configuring Management Features
Configuring System Management Features
Lab 4-1 Configuring Management Features

Troubleshooting the Cisco Nexus 1000V Switch

Using Basic Troubleshooting Tools
Troubleshooting Modules
Troubleshooting Ports and Port Profiles
Lab 5-1 Configuring SPAN and ERSPAN
Lab 5-2 Troubleshooting the Cisco Nexus 1000V

Course Description:

The Implementing the Cisco 5000 Switch and 2000 Fabric Extender course is a two-day instructor-led course with lab exercises that are intended to prepare students to install, configure and support the Cisco Nexus 5000 Switch and 2000 Fabric Extender. The course schedule consists of approximately 50 percent lecture and 50 percent lab exercises. The lab for this course is accessed using a remote access procedure coupled with a GUI application that provides connectivity to all lab devices.

If ICN1K v1.0 is offered the same week as ICN52K v3.0, at the same location, you can attend both classes for \$3,995.00, giving you a \$1,795.00 discount off the regular pricing for the individual classes.

Who Should Attend:

The primary audience is those individuals involved in the technical handling of Cisco platforms and solutions, namely installing, configuring, operating, and troubleshooting Data Center equipment, specifically the Nexus 5000 Switch and Nexus 2000 Fabric Extender. In this course, the target audience will be referred to generically as technicians.

Prerequisites:

The recommended prerequisites for students attending the Implementing the Cisco 5000 and 2000 course are Interconnecting Cisco Networking Devices (ICND1) or equivalent, Interconnecting Cisco Networking Devices (ICND2) or equivalent, and Building Cisco Multilayer Switched Networks (BCMSN) or equivalent.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Deploy, configure and troubleshoot data center networks using the Cisco Nexus 5000 and 2000 products.
- Understand the enhancements associated with the Cisco NX-OS Software
- Understand product placement for the Cisco Nexus Platform Family
- Describe the migration of data center architectures, including unified I/O and unified fabric

Course Outline:**Module 1: Implementing the Cisco Nexus 5000 and 2000 in Data Center Networks**

Overview of the Cisco Nexus 5000 and Cisco Nexus 2000
Understanding Fibre Channel
Understanding Converged Network Adapters (CNA)
Implementing an FCoE Network Using Cisco Nexus 5000 Series Switches
Implementing QoS on the Nexus 5000 and 2000
Understanding Virtual Port Channels (VPC)
Integrating the Nexus 5000 into a SAN Environment (Issues, Evolving Standards, etc.)

Lab Exercises

Lab Exercise 1: Cisco Nexus 5000 Hardware Platform
Lab Exercise 2: Configuring the Cisco Nexus 2000 Fabric Extender
Lab Exercise 3: Using Fibre Channel HBAs
Lab Exercise 4: Configuring FCoE on the Nexus 5000 and FC on the Cisco 9124
Lab Exercise 5: Implementing CNAs and FCoE on the VMware server
Lab Exercise 6: Configuring VSANs and Zoning in the Nexus DC environment
Lab Exercise 7: Cisco Nexus Product Family Solution Example
Lab Exercise 8: Implementing QoS in the Nexus 5000, 2000 and VMware environment
Lab Exercise 9: Configuring N_Port Virtualization on the Cisco Nexus 5000

Course Description:

This 5-day course enables students to create a Data Center network design that optimizes availability, scalability, performance, and security, using the Nexus Products, Catalyst 6500, Catalyst 4948, Firewall Services Module, Intrusion Detection Services Module, and Network Analysis Module.

Who Should Attend:

This course is for Channel Partners/Resellers, Customers, and Employees.

Prerequisites:

Students should have taken Designing for Cisco Internetworks Solutions (DESGN) and Securing Cisco Network Devices (SND).

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Create a Data Center network designs that optimizes availability, scalability, and performance for that environment
- Create a core layer design that optimizes data flows
- Create an aggregation layer design that optimizes data flows
- Create an access layer design that optimizes data flows
- Optimize a data center design to achieve high availability
- Design a security implementation using Catalyst 6500 service modules
- Design a management infrastructure that provides centralized management services

Course Outline:**Module 1: Data Center Design Models**

Lesson 1: Data Center Business Objectives

Lesson 2: Data Center Networking Components: Cisco Platforms and Modules

Lesson 3: Data Center Environmental Requirements

Module 2: Cisco Nexus 7010 Switch

Lesson 1: Cisco Nexus 7010 Hardware Architecture

Lesson 2: Cisco Nexus 7010 Software Architecture

Lesson 3: Cisco Nexus 7010 Continual Availability

Lesson 4: Cisco Nexus 7010 Switch Network Management

Lesson 5: Cisco Nexus 7010 Security Overview

Lesson 6: Cisco Nexus 7010 QoS implementation

Lesson 7: Cisco Nexus 7010 Switch Positioning in the Data Center

Module 3: Cisco Nexus 5000 Series Switches

Lesson 1: Fibre Channel over Ethernet

Lesson 2: Cisco Nexus 5000 Series Switches Overview

Module 4: Data Center Design Models

Lesson 1: Data Center Design Overview

Lesson 2: Data Center Application Design

Module 5: Data Center Design Strategy

Lesson 1: Data Center Strategy

Module 6: Data Center Network Design

Lesson 1: Data Center Network Design

Course Description:

The Cisco Data Center Unified Computing Design (DCUCD) v4.0 course enables engineers to choose and design scalable, reliable, and intelligent data center unified computing and virtualization solutions. These solutions are based on the Cisco data center product portfolio with a Cisco Unified Computing System (UCS) as a centerpiece integrated with contemporary server virtualization solutions (such as VMware vSphere, Microsoft Hyper-V R2, and Citrix for Cisco Virtualization Experience Infrastructure [VXI]) and operating systems (such as Microsoft Windows and Linux).

The DCUCD v4.0 course is an update of the Data Center Unified Computing Design (DCUCD) v3.0 and describes the data center unified computing and virtualization solutions that are based on the Cisco data center product portfolio. The course explains how to evaluate existing data center computing solution, determine the requirements, and design Cisco data center unified computing and virtualization solutions.

Who Should Attend:

The primary students for this course are data center designers, data center administrators, and system engineers. The secondary students for this course are data-center designers and managers. The tertiary audience for this course are Program and project managers.

Prerequisites:

Students should have the skills taught in Designing for Cisco Internetwork Solutions (DESGN) course, Designing Cisco Data Center Unified Fabric (DCUFD) course, and Designing Cisco Storage Networking Solutions (DCSNS) course. Students should also have Linux or Windows system administration familiarity and should have taken Introduction to Virtualization (Virt101EL) precourse online training.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Evaluate the Cisco Unified Computing System solution design process in regards to the contemporary data center challenges, the Cisco Data Center Business Advantage architectural framework, and components
- Use the reconnaissance and analysis tools to assess computing solution performance characteristics and requirements
- Describe the hardware components of the Cisco Unified Computing System and select proper hardware for a given set of requirements
- Describe the basic server deployment model of the Cisco Unified Computing System
- Propose a Cisco Unified Computing System solution management design for a given environment
- Describe the advanced Cisco UCS server deployment model
- Calculate the ROI and TCO for the solution by using the Cisco UCS ROI tool
- Design a migration plan for an existing implementation to a Cisco Unified Computing System solution

Course Outline:**Cisco Unified Computing System Solution**

Analyzing Data Center Computing Solutions
Identifying a Cisco Unified Computing System Solution
Evaluating Server Deployment Options
Defining a Cisco Unified Computing System Solution Design

Assess Computing Solution Requirements

Analyzing Performance Characteristics
Employing Data Center Reconnaissance and Analysis Tools
Lab 2-1: Analyze the Existing Computing Solution

Design Cisco Unified Computing System Solution

Evaluating Cisco UCS C-Series Architecture
Sizing the Cisco UCS C-Series Solution
Evaluating Cisco UCS B-Series Architecture
Sizing the Cisco UCS B-Series Solution
Planning Physical Deployment
Examining the Cisco UCS Network and Storage
Designing the Cisco UCS Network and Storage
Lab 3-1: Size the Small Cisco UCS Solution
Lab 3-2: Size the Large Cisco UCS Solution
Lab 3-3: Plan the Physical Deployment

Design Server Deployment

Designing Cisco UCS Server Deployment Model

Design Cisco UCS Solution Management

Examining Cisco UCS Solution Management
Designing Cisco UCS Solution Management
Lab 5-1: Design the Cisco Unified Computing System Solution Management

Design Advanced Server Deployment

Evaluating Cisco UCS Deployment with Microsoft Hyper-V
Evaluating Cisco UCS Integration with VMware vSphere
Evaluating Cisco UCS and Cisco Nexus 1000V Integration with VMware vSphere
Lab 6-1: Design the Server Deployment for Microsoft Hyper-V
Lab 6-2: Design the Server Deployment for VMware vSphere
Lab 6-3: Design the Server Deployment for VMware vSphere with Cisco Nexus 1000V

Evaluate Cisco Unified Computing System Solutions

Evaluating Solution Design
Determining Solution ROI and TCO

Plan Migration to Cisco Unified Computing System Solution

Designing a Migration Plan

Course Description:

Implementing the Cisco 7000 (ICN7K v3.0) is a three-day instructor-led course with lab exercises that are intended to prepare students to install, configure and support the Cisco Nexus 7000 Switch. The course schedule consists of approximately 50 percent lecture and 50 percent lab exercises. The lab for this course is accessed using a remote access procedure coupled with a GUI application that provides connectivity to all lab devices.

Who Should Attend:

The primary audience is those individuals involved in the technical handling of Cisco platforms and solutions, namely installing, configuring, operating, and troubleshooting Data Center equipment, specifically the Nexus 7000 Switch.

Prerequisites:

Students attending the Implementing the Cisco Nexus 7000 course should have taken the following classes or have equivalent experience: Interconnecting Cisco Networking Devices (ICND1), Interconnecting Cisco Networking Devices (ICND2), and Building Cisco Multilayer Switched Networks (BCMSN).

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Deploy, configure and troubleshoot data center networks using the Cisco Nexus 7000 Switch.
- Describe the enhancements associated with the Cisco NX-OS Software over previous switch OSs
- Identify product placement within the Cisco Nexus Platform Family
- Describe the migration of data center architectures, including unified I/O and unified fabric

Course Outline:**Module 1: Using the Cisco Nexus 7000 in Data Center Networks**

Lesson 1: Understanding the Cisco Nexus 7000 Series Switches

Lesson 2: Overview of the Cisco Nexus 7000

Lesson 3: Introducing the Virtual Device Contexts in the Cisco Nexus 7000

Lesson 4: Managing the Cisco Nexus 7000

Lesson 5: Cisco Nexus 7000 and Cisco NX-OS Layer 2 Protocols and Features

Lesson 6: Cisco Nexus 7000 and Cisco NX-OS Layer 3 Protocols and Features

Lesson 7: Cisco Nexus 7000 and Cisco NX-OS Quality of Service

Lesson 8: Cisco Nexus 7000 and Cisco NX-OS Security

Lesson 9: Troubleshooting

Lesson 10: Additional Features Coming – Virtual Port Channels

Lab Exercise 1: Cisco Nexus 7000 Hardware Platform

Lab Exercise 2: Managing System Configuration

Lab Exercise 3: Creating VDCs

Lab Exercise 4: Layer 2 Switching

Lab Exercise 5: First-Hop Redundancy Protocols

Lab Exercise 6: Configuring Routing Protocols

Lab Exercise 7: Quality of Service

Lab Exercise 8: Cisco Nexus 7000 Security Features

Lab Exercise 9: Cisco Data Center Network Manager

Lab Exercise 10: Troubleshooting Using Ethalyzer and SPAN

Course Description:

Implementing Enterprise Datacenter Infrastructure Security (IEDIS) is a lab-intensive course that allows students to integrate and test Cisco® security products and security best practices that compose the Cisco Enterprise Data Center Architecture. Students will implement and integrate Layer 2 and Layer 3 network security best practices as well as the Cisco Nexus™ 7000 platform into the data center. Hands-on labs for the Cisco Nexus 7000 include initial network configuration with virtual switching, Layer 2 security, and control-plane policing (CoPP). The course also includes the integration of the Cisco ASA into the data center architecture as a redundant routed pair with additional labs on the implementation of the IPS functionality using the AIP-SSM-40 module. Once the infrastructure has been deployed and secured, the students will deploy Cisco Security Manager and Cisco Secure Monitoring Analysis and Response System (Cisco Security MARS) to manage network security devices.

Who Should Attend:

This course is targeted toward data center managers and administrators, network administrators, security professionals, and engineers interested in deploying and securing Cisco network data center solutions.

Prerequisites:

Students must have CCNA® level networking knowledge and experience configuring Cisco network routers and switches and an introductory level understanding of available Cisco security products. It is recommended that students have CCNP level networking knowledge and experience configuring Cisco network routers and switches

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify key components of the Data Center 3.0 solution
- Identify and describe network security threats for the enterprise data center
- Configure a Cisco Nexus 7000 platform for Layer 2 and Layer 3 network security
- Configure a Cisco Nexus 7000 platform for secure virtual switching
- Configure CoPP for the Cisco Nexus 7000 platform
- Deploy Layer 2 network security on the Cisco Catalyst 4900M switch
- Deploy Layer 3 network security for Cisco IOS® Software routers
- Configure the Cisco ASA to protect an enterprise data center
- Deploy the Cisco AIP-SSM module in the ASA to provide IPS services to the enterprise data center
- Configure the Cisco Security MARS management platform for network threat correlation
- Integrate Cisco Security Manager with the Cisco Security MARS platform for data center device configuration and management

Course Outline:

Introduction

Data Center Security Overview

Cisco Nexus Architecture Overview and Setup

CoPP for the Cisco Nexus 7000

Layer 2 Network Security

Layer 3 Network Security

Deploying the Cisco ASA in an Enterprise Data Center

Configuring IPS Services for the Data Center Using the Cisco ASA

Securing Data Center DNS Using the Cisco ASA and AIP-SSM

Managing Network Security Threats Using Cisco Security MARS

Integrating Cisco Security Manager into the Data Center

Lab 1: Remote Network Connectivity

Lab 2: Configuring the Cisco Nexus 7000 for Layer 2 and Layer 3 Connectivity

Lab 3: Deploying CoPP for the Cisco Nexus 7000

Lab 4: Configuring Layer 2 Network Security

Lab 5: Configuring Layer 3 Network Security

Lab 6: Configuring the Cisco ASA to Protect the Enterprise Data Center

Lab 7: Deploying IPS Services Using the Cisco ASA

Lab 8: Securing Data Center DNS Using the Cisco ASA and AIP-SSM

Lab 9: Managing Network Security Using the Cisco Security MARS

Lab 10: Integrating Cisco Security Manager into the Data Center

Course Description:

Data Center Unified Computing Implementation (DCUCI) is designed to serve the needs of engineers and technicians who implement Cisco Unified Computing System (UCS) B-Series Blade Servers and Cisco UCS C-Series Rack-Mount Servers.

Data Center Unified Computing Implementation (DCUCI) v4.0 updates and replaces Data Center Unified Computing Implementation (DCUCI) v3.0 and guides learners through rack installation and the provisioning of server hardware, operating systems or hypervisors, and applications. Significant content is devoted to management, maintenance, and troubleshooting. Data Center Unified Computing Implementation (DCUCI) v4.0 articulates Cisco data-center virtualization solutions and explains how to execute a virtualization solution that is based on a detailed implementation plan.

Who Should Attend:

The primary audience for this course are data-center technicians, data-center administrators, and system engineers. The secondary audience for this course are data-center designers and managers. The tertiary audience for this course program and project managers.

Prerequisites:

The following prerequisite skills and knowledge are recommended before attending this course: understanding of server system design and architecture, familiarity with Ethernet and TCP/IP networking, familiarity with SANs, familiarity with Fibre Channel Protocol (FCP), understanding of Cisco Enterprise Data Center Architecture, and familiarity with hypervisor technologies (VMware vSphere, Microsoft Hyper-V, Citrix Xen).

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Explain how Cisco Unified Computing System addresses key management challenges in data center server environments
- Describe the Cisco UCS B-Series and C-Series system architectures, hardware components, and field-installable options
- Explain how to connect to and manage Cisco Unified Computing System components
- Configure Cisco UCS B-Series blade servers with Cisco UCS Manager
- Configure Cisco UCS C-Series blade servers with Cisco IMC
- Explain the connectivity requirements for the Cisco UCS platform
- Configure server profiles to allocate physical resources
- Configure maintenance tasks
- Configure high availability at the LAN, SAN, and server NIC level
- Identify common deployment scenarios for Cisco Unified Computing System
- Troubleshoot common LAN and SAN connectivity issues

Course Outline:**Module 1: Review of Data Center Unified Computing Implementation E-Learning**

Brief Survey of Cisco Data Center Unified Computing Implementation E-Learning

Module 2: Installation of the Cisco UCS C-Series Rack-Mount Servers

Updating Firmware Components of the Cisco UCS C-Series Rack-Mount Servers

Module 3: Cisco IMC Configuration

Configuring Cisco IMC

Provisioning Server Hardware with Cisco IMC

Lab 3-1: Initial Cisco UCS C-Series Configuration

Module 4: Cisco UCS B-Series Hardware and Management

Describing Cisco UCS B-Series Hardware Components

Assembling B-Series Architecture and Features

Installing Cisco UCS B-Series Hardware

Module 5: Cisco UCS Connectivity Configuration and Management

Configuring Cisco UCS B-Series Physical Connectivity

Exploring the Cisco UCS B-Series User Interfaces

Configuring Compute Node LAN Connectivity

Configuring Compute Node SAN Connectivity

Lab 5-1: Configure LAN and SAN Physical Connections

Module 6: Server Resources Implementation

Creating Identity and Resource Pools

Creating Service Profiles

Creating Service Profile Templates and Cloning Service Profiles

Managing Service Profiles

Lab 6-1: Configure Identity and Resource Pools

Lab 6-2: Create Mobile Service Profiles from Updating Templates

Module 7: Virtual Server Networking

Evaluating the Cisco Nexus 1000V

Working with VMware Ethernet Networking

Characterizing Cisco Nexus 1000V Architecture

Installing and Configuring the Cisco Nexus 1000V Switch

Configuring Basic Cisco Nexus 1000V Networking

Configuring Cisco UCS Manager for VMware PTS

Lab 7-1: Create a Data-Center Cluster in VMware vCenter

Lab 7-2: Install a Cisco Nexus 1000V VSM

Lab 7-3: Configure Port Profiles

Module 8: Cisco Unified Computing System Management and Maintenance

Implementing Cisco Unified Computing System Startup and Shutdown Procedures

Configuring Role-Based Access Control

Backing Up and Restoring the Cisco UCS Manager Database

Managing High Availability

Monitoring System Events

Managing and Upgrading Cisco UCS B-Series Firmware

Lab 8-1: Configure RBAC

Lab 8-2: Back up and Import Cisco UCS Manager Configuration Data

Lab 8-3: Reporting in the Cisco Unified Computing System

Lab A-1: Initial Cisco UCS B-Series Configuration

Course Description:

This three day training event is intended for individuals who are responsible for migrating current UC environments onto UCSM-managed Cisco server based technologies (B-Series and C-Series) running VMware ESXi.

Unlike traditional server based installations, Cisco UCS servers can be configured through the UCS Manager (UCSM) using Service Profiles. This training will begin with a brief discussion of the changing Data Center server environment, where the Cisco UCS system fits into this environment, and LAN and storage (SAN) considerations.

An overview of the UCS products will be provided, with emphasis on the advantages the UCS Manager brings to server provisioning. Server provisioning, through the use of easy-to-configure Service Profiles, will also be covered in detail, along with supporting labs.

VMware ESXi is an integral part of this installation and so an overview of VMware will be included.

UC on UCS specific considerations will then be discussed, including minimum requirements, caveats, recommendations, etc.

Lectures will be complemented by hands-on labs:

Who Should Attend:

Individuals interested in, or responsible for, the installation or migration of Cisco's Unified Communications (UC) Manager (a.k.a. CallManager) on a Unified Computing System (UCS) B-Series blade server platform running VMware®.

Prerequisites:

All students are expected to be trained and experienced on Cisco's Unified Communications products.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Install Cisco UC on UCS.

Course Outline:**Overview of Today's Data Center and UCS**

Data Center Computing Challenges
Understanding Server Evolution
Introduction to UCS

UCS Architecture

UCS Hardware Overview
Chassis, B-Series Servers (Blades) and Fabric Interconnects
C-Series Servers

UCS Connectivity and Access

Hardware Connectivity
High Availability Considerations
UCS Interfaces (GUI and CLI)

The UCS Manager

Managing the UCS System using UCSM

Compute Node Connectivity

LAN Connectivity
SAN Connectivity

Service Profiles

Creating Resource Pools
Creating Service Profiles
Using Service Profiles

Customizing the Server - The Service Profile

BIOS and Boot Options
Network Options
Storage Options
Optional Options

Virtualization in the Data Center

Introduction to Virtualization
VMware Overview
Configuring VMware and VMware Networking

Adding Unified Communications to the UCS Environment - Planning and Design

Implementation Considerations
Feature Impact
Minimum Requirements
LAN Planning

SAN Planning

Deployment Considerations

Using the B-Series Servers
Migration Considerations
QoS Considerations
Provisioning and Configuration Considerations

Installing UC on UCS

Building the Service Profile
Preparing the Infrastructure for the Installation
Installing VMware – ESXi
Installing the UC Code
Verifying the Installation

Lab Outline

UCS Manager Overview
Creating Resource Pools
Creating a Service Profile
Installing and Booting an OS from the Hard Drive
Creating the Service Profile for the UC Installation
Installing the UC Subscriber
Validating Publisher / Subscriber Connectivity

Course Description:

ICND1 v1.1 focuses on providing the skills and knowledge necessary to implement and support a small switched and routed network. For the purpose of this course, a small network is defined as 1-20 hosts connected to a single switch with the switch running a single VLAN. The switch is also connected to a router that is providing a routed link (RIP & default) to a simulated Internet and corporate office.

ICND1 v1.0 works from the bottom up providing knowledge and skills as they are needed. The course starts with an introduction to networking. It then introduces host-to-host communications using TCP/IP. Next Layer 2 devices (switches, etc.) are introduced into the network. Next Layer 3 devices (routers) are introduced into the network. The introduction of Layer 3 devices leads to the use of WANs and routing to connect the site to the Internet and corporate sites. Finally, device management skills (CDP, TFTP, etc.) are introduced.

Who Should Attend:

The primary audience for this course includes Network Administrators, Network Engineers, Network Managers, and Systems Engineers.

Prerequisites:

Students should have basic computer literacy, basic Windows navigation skills, basic Internet usage skills, and basic e-mail usage skills.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe how networks function, identifying major components, function of network components and the Open System Interconnection (OSI) reference model.
- Using the host-to-host packet delivery process, describe issues related to increasing traffic on an Ethernet LAN and identify switched LAN technology solutions to Ethernet networking issues.
- Describe the reasons for extending the reach of a LAN and the methods that can be used with a focus on RF wireless access.
- Describe the reasons for connecting networks with routers and how routed networks transmit data through networks using TCP/IP.
- Describe the function of Wide Area Networks (WANs), the major devices of WANs, and configure PPP encapsulation, static and dynamic routing, PAT and RIP routing.
- Use the command-line interface to discover neighbors on the network and managing the router's startup and configuration.

Course Outline:**Course Introduction****Module 1: Building a Simple Network**

Exploring the Functions of Networking
 Securing the Network
 Understanding the Host-to-Host Communication Model
 Understanding TCP/IP's Internet Layer
 Understanding TCP/IP's Transport Layer
 Exploring the Packet Delivery Process
 Understanding Ethernet
 Connecting to an Ethernet LAN
 Lab 1-1: Using Windows Applications as Network Tools
 Lab 1-2: Observing the TCP Three-Way Handshake
 Lab 1-3: Observing Extended PC Network Information

Module 2: Ethernet Local Area Networks (LAN's)

Understanding the Challenges of Shared LANs
 Solving Network Challenges with Switched LAN Technology
 Exploring the Packet Delivery Process
 Operating Cisco IOS Software
 Starting a Switch
 Understanding Switch Security
 Maximizing the Benefits of Switching
 Troubleshooting Switch Issues
 Lab 2-1: Connecting to Remote Lab Equipment
 Lab 2-2: Switch Startup and Initial Configuration
 Lab 2-3: Enhancing Security of Switch Configuration
 Lab 2-4: Operating and Configuring a Cisco IOS Device

Module 3: Wireless Local Area Networks (WLAN's)

Exploring Wireless Networking
 Understanding WLAN Security
 Implementing a WLAN

Module 4: Local Area Network Connections

Exploring the Functions of Routing
 Understanding Binary Basics
 Constructing a Network Addressing Scheme
 Starting a Router
 Configuring a Router
 Exploring the Packet Delivery Process
 Understanding Router Security

Using Cisco Router and Security Device Manager
 Using a Router as a DHCP Server
 Accessing Remote Devices
 Lab 4-1: Converting Decimal to Binary and Binary to Decimal
 Lab 4-2: Classifying Network Addressing
 Lab 4-3: Computing Usable Sub-networks and Hosts
 Lab 4-4: Calculating Subnet Masks
 Lab 4-5: Initial Router Startup
 Lab 4-6: Initial Router Configuration
 Lab 4-7: Enhancing Security of Initial Router Configuration
 Lab 4-8: Using SDM to Configure DHCP Server Function
 Lab 4-9: Managing Remote Access Sessions

Module 5: Wide Area Networks (WANs)

Understanding WAN Technologies
 Enabling the Internet Connection
 Enabling Static Routing
 Configuring Serial Encapsulation
 Enabling Routing Information Protocol (RIP)
 Lab 5-1: Connecting to the Internet
 Lab 5-2: Connecting to the Main Office
 Lab 5-3: Enable Dynamic Routing to Main Office

Module 6: Network Environment Management

Managing Cisco Devices
 Lab 6-1: Using CDP
 Lab 6-2: Managing Router Startup Options
 Lab 6-3: Managing Cisco Devices
 Lab 6-4: Confirming the Re-Configuration of the Branch Network

Course Description:

Interconnecting Cisco Networking Devices Part 2 (ICND2) v1.1 is an instructor-led course presented by Cisco training partners to their end-user customers. This five-day course focuses on using Cisco Catalyst switches and Cisco routers connected in LANs and WANs typically found at medium-sized network sites.

Who Should Attend:

The primary audience for this course include Network Administrators, Network Engineers, Network Managers, and Systems Engineers. The secondary audience for this course includes Network Designers and Project Managers.

Prerequisites:

The knowledge and skills that a learner must have before attending this course include basic computer literacy, basic Microsoft Windows navigation skills, basic Internet usage skills, basic email usage skills, skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1), and the ability to install, configure, and troubleshoot a small network.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Review how to configure and troubleshoot a small network
- Expand the switched network from a small LAN to a medium-sized LAN with multiple switches, supporting VLANs, Trunking, and Spanning Tree
- Describe routing concepts as they apply to a medium-sized network and discuss considerations when implementing routing on the network
- Configure, verify, and troubleshoot OSPF
- Configure, verify, and troubleshoot EIGRP
- Determine how to apply ACLs based on network requirements, and to configure, verify, and troubleshoot ACLs on a medium-sized network
- Describe when to use NAT or PAT on a medium-sized network, and configure NAT or PAT on routers
- Identify and implement the appropriate WAN technology based on network requirements

Course Outline:**Course Introduction****Module 1: Small Network Implementation**

Introducing the Review Lab
Lab 1-1: Implementing a Small Network (Review Lab)

Module 2: Medium-Sized Switched Network Construction

Implementing VLANs and Trunks
Optimizing Spanning Tree Performance
Routing Between VLANs
Securing the Expanded Network
Trouble shooting Switched Networks
Lab 2-1: Configuring Expanded Switched Networks
Lab 2-2: Troubleshooting Switched Networks

Module 3: Medium-Sized Routed Network Construction

Reviewing Routing Operations
Implementing VLSM

Module 4: Single Area OSPF Implementation

Implementing OSPF
Troubleshooting OSPF
Lab 4-1: Implementing OSPF
Lab 4-2: Troubleshooting OSPF

Module 5: EIGRP Implementation

Implementing EIGRP
Troubleshooting EIGRP
Lab 5-1: Implementing EIGRP
Lab 5-2: Troubleshooting EIGRP

Module 6: Access Control Lists

Introducing ACL Operation
Configuring and Troubleshooting ACLs
Lab 6-1: Implementing and Troubleshooting ACLs

Module 7: Address Space Management

Scaling the Network with NAT and PAT
Transitioning to IPv6
Lab 7-1: Configuring NAT and PAT
Lab 7-2: Implementing IPv6

Module 8: LAN Extension into a WAN

Introducing VPN Solutions
Establishing a Point-to-Point WAN Connection with PPP
Establishing a WAN Connection with Frame Relay
Troubleshooting Frame Relay WANs
Lab 8-1: Establishing a Frame Relay WAN
Lab 8-2: Troubleshooting Frame Relay WANs

Course Description:

Interconnecting Cisco Networking Devices: Accelerated (CCNAX) v1.0 is an extended hours instructor-led boot camp that provides students with the knowledge and skills necessary to install, operate, and troubleshoot a small to medium-sized network, including connecting to a WAN and implementing network security.

This course is the equivalent of Interconnecting Cisco Network Devices Part 1 v1.0 and Interconnecting Cisco Network Devices Part 2 v1.0 together.

The ideal candidate would be someone who has worked in a data network environment (PC support/helpdesk or network operations/monitoring), and has had hands-on experience, though no formal training, with Cisco IOS devices. This boot camp will serve to review and expand on what the candidate already knows and add to it, the detailed configuration and implementation of Cisco IOS devices.

Prospective CCNAX v1.0 students should prepare themselves for course days consisting of at least 10 hours and as long as 12 hours. Homework will be assigned and reviewed daily.

Those new to networking and to Cisco IOS should consider taking the ICND1 and ICND2 classes instead of CCNAX v1.0.

Who Should Attend:

The primary audience for this course includes Network Administrators, Network Engineers, Network Managers, and Systems Engineers. The secondary audience for this course includes Network Designers and Project Managers.

Prerequisites:

Students should have basic computer literacy, basic Microsoft Windows navigation skills, and basic Internet usage skills.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe how networks function, identifying major components, function of network components, and the OSI reference model
- Describe issues related to increasing traffic on an Ethernet LAN and expand the switched network from a small LAN to a medium-sized LAN with multiple switches supporting VLANs, trunking, and spanning tree
- Describe the reasons for extending the reach of a LAN and the methods that can be used, with a focus on RF wireless access
- Describe the reasons for connecting networks and connecting multiple IP subnets with routers
- Configure and verify a Cisco router for WAN connections with HDLC and PPP encapsulation, PAT, static routing, and describe the components that make up a VPN solution
- Use the command-line interface to discover neighbors on the network and manage the router startup and configuration
- Describe routing concepts as they apply to a medium-sized network, discuss dynamic routing with distance vector and link-state routing protocols, and configure RIP
- Configure, verify, and troubleshoot single-area OSPF
- Configure, verify, and troubleshoot EIGRP

Course Outline:

Module 1: Building a Simple Network

Exploring the Functions of Networking
Securing the Network
Understanding the Host-to-Host Communications Model
Understanding the TCP/IP Internet Layer
Understanding the TCP/IP Transport Layer
Exploring the Packet Delivery Process
Understanding Ethernet
Connecting to an Ethernet LAN

Module 2: Switching

Understanding the Challenges of Shared LANs
Solving Network Challenges with Switched LAN Technology
Exploring the Packet Delivery Process
Operating Cisco IOS Software
Starting a Switch
Securing the Switch
Maximizing the Benefits of Switching
Implementing VLANs and Trunks
Improving Performance with Spanning Tree
Routing Between VLANs
Troubleshooting Switched Networks

Module 3: Wireless LANs

Exploring Wireless Networking
Understanding WLAN Security
Implementing a WLAN

Module 4: LAN Connections

Understanding Binary Basics

Constructing a Network Addressing Scheme
Exploring the Packet Delivery Process
Starting a Cisco Router
Configuring a Cisco Router
Understanding Cisco Router Security
Using Cisco SDM
Using a Cisco Router as a DHCP Server

Module 5: WAN Connections

Understanding WAN Technologies
Enabling the Internet Connection
Introducing VPN Solutions
Configuring Serial Encapsulation
Enabling Static Routing

Module 6: Network Environment Management

Accessing Remote Devices
Discovering Neighbors on the Network
Managing Cisco Router Startup and Configuration
Managing Cisco Devices

Module 7: Medium-Sized Routed Network Construction

Exploring the Functions of Routing
Enabling RIP
Implementing VLSM

Module 8: Single-Area OSPF Implementation

Implementing OSPF
Troubleshooting OSPF

Module 9: EIGRP Implementation

Implementing EIGRP
Troubleshooting EIGRP

Module 10: Access Control Lists

Introducing ACL Operation
Configuring and Troubleshooting ACLs

Module 11: Address Space Management

Scaling the Network with NAT and PAT
Transitioning to IPv6

Module 12: LAN Extension into a WAN with Frame Relay

Establishing a WAN Connection with Frame Relay
Troubleshooting Frame Relay WANs

Course Description:

The IPv6 Fundamentals, Design, and Deployment (IP6FD) v3.0 course is an instructor-led course that is presented by Cisco Learning Partners to their end-user customers. This five-day course aims at providing network engineers and technicians that are working in the enterprise sector with the knowledge and skills that are needed to study and configure Cisco IOS Software IPv6 features. The course also provides an overview of IPv6 technologies, covers IPv6 design and implementation, describes IPv6 operations, addressing, routing, services, transition, and deployment of IPv6 in enterprise as well as in service provider networks, and includes case studies useful for deployment scenarios.

Who Should Attend:

This course is for channel partners / resellers and customers.

Prerequisites:

Students must be ICND1 or ICND2 certified, have an understanding of networking and routing (on Cisco CCNP® level, but no formal certification is required), and have working knowledge of the Microsoft Windows operating system.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the factors that led to the development of IPv6 and possible uses of this new IP structure
- Describe the structure of the IPv6 address format, how IPv6 interacts with data link layer technologies, and how IPv6 is supported in Cisco IOS Software
- Implement IPv6 services and applications
- Understand the updates to IPv4 routing protocols needed to support IPv6 topologies
- Understand multicast concepts and IPv6 multicast specifics
- Evaluate the scenario and desired outcome and identify the best transition mechanism for the situation
- Describe security issues, how security for IPv6 is different than for IPv4, and emerging practices for IPv6-enabled networks
- Describe the standards bodies that define IPv6 address allocation, in addition to one of the leading IPv6 deployment issues—multihoming
- Describe the deployment strategies that service providers might consider when deploying IPv6

Course Outline:**Introduction to IPv6**

Explaining the Rationale for IPv6
Evaluating IPv6 Features and Benefits
Understanding Market Drivers

IPv6 Operations

Understanding the IPv6 Addressing Architecture
Describing the IPv6 Header Format
Enabling IPv6 on Hosts
Enabling IPv6 on Cisco Routers
Using ICMPv6 and Neighbor Discovery
Troubleshooting IPv6
Lab 2-1: Enabling IPv6 on Hosts
Lab 2-2: Using Neighbor Discovery

IPv6 Services

IPv6 Mobility
Describing DNS in an IPv6 Environment
Understanding DHCPv6 Operations
Understanding QoS Support in an IPv6 Environment
Using Cisco IOS Software Features
Lab 3-1: Using Prefix Delegation

IPv6-Enabled Routing Protocols

Routing with RIPv6
Examining OSPFv3
Examining Integrated IS-IS
Examining EIGRP for IPv6
Understanding MP-BGP
Configuring IPv6 Policy-Based Routing
Configuring FHRP for IPv6
Configuring Route Redistribution
Lab 4-1: Routing with OSPFv3
Lab 4-2: Routing with IS-IS
Lab 4-3: Routing with EIGRP
Lab 4-4: Routing with BGP and MP-BGP

IPv6 Multicast Services

Implementing Multicast in an IPv6 Network
Using IPv6 MLD
Lab 5-1: Multicasting

IPv6 Transition Mechanisms

Implementing Dual-Stack
Describing IPv6 Tunneling Mechanisms
Lab 6-1: Implementing Tunnels for IPv6

IPv6 Security

Configuring IPv6 ACLs
Using IPsec, IKE, and VPNs
Discussing Security Issues in an IPv6 Transition Environment
Understanding IPv6 Security Practices
Configuring Cisco IOS Firewall for IPv6
Lab 7-1: Configuring Advanced ACLs
Lab 7-2: Implementing IPsec and IKE
Lab 7-3: Configuring Cisco IOS Firewall

Deploying IPv6

Examining IPv6 Address Allocation
Understanding the IPv6 Multihoming Issue
Identifying IPv6 Enterprise Deployment Strategies

IPv6 and Service Providers

Identifying IPv6 Service Provider Deployment
Understanding Support for IPv6 in MPLS
Understanding 6VPE
Understanding IPv6 Broadband Access Services
Lab 9-1: Configuring 6PE and 6VPE

IPv6 Case Studies

Planning and Implementing IPv6 in Enterprise Networks
Planning and Implementing IPv6 in Service Provider Networks
Planning and Implementing IPv6 in Branch Networks

Course Description:

CCIE R&S Written Bootcamp is a 4 day Boot Camp with the class hours being: Monday through Thursday 9:00 AM through 7:00 PM. The course includes a combination of lectures and quizzes that will prepare you for the written exam. The class is designed to provide the students with the best possible techniques to pass the CCIE R&S written exam.

Who Should Attend:

The class is designed for students who will be taking the CCIE R&S written exam.

Prerequisites:

There are no prerequisites.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- be prepared for the CCIE R&S written exam.

Course Outline:

802.1d, 802.1w, 802.1s, loop guard, Root guard, BPDUs, Storm control, RSTP, MSTP, Unicast flooding, STP, trunking, VLANs, VTP, Ethernet (Speed, Duplexing, Ethernet, Fast Ethernet and Gigabit Ethernet)

IP Addressing, Subnetting the easy way, VLSM, NAT, PAT, SNAT, HSRP, VRRP, GLBP

IP services: NTP, DHCP, WCCP and DRP

Network Management: SNMP, RMON, and Syslog

OSPF: LSAs, Adjacency, Network types, Single area, Multi-area, STUB, Totally Stubby, NSSA, Totally NSSA, injecting default routes and filtering

EIGRP: Best path, Operation, unequal cost load balancing, Summarization, SIA, Stub, injecting default routes and Filtering

Policy Routing: Concepts, Basic configuration and advanced configurations

BGP: IBGP and EBGP peering, Next-hop, Attributes and advanced topics

QOS: NBAR, CBWFQ, MDRR, LLQ, Policing and CAR, Classification and marking, RED and CBWRED, DE-lists (Legacy and MQC), FRTS and CB-Shaping

Frame-relay: LMI, Hub and Spoke and Full mesh

Multicasting: IGMP (V1, V2 and V3), CGMP, Group addresses and layer 2 to layer 3 translation, Source versus shared trees, PIM-DM and PIM-SM, Auto-RP, BSR, and MSDO/Anycast

Security: Standard and Extended ACLs, VACL, MAC access-lists, ARP access-lists, Time based ACL, Dynamic and Reflexive ACLs, CBAC, IP Source Guard and uRPF

MPLS: LSR, LSP, RD, Label Format, Imposition, Disposition and Distribution

IPv6: Addressing and types, ND, Tunneling techniques (IPv6 over IPv4, IPv6 over IPv6, 6to4 and ISATAP), RIPng, EIGRPv3 and OSPFv3

Course Description:

This course is instructor-led training and includes instructor assisted, hands-on labs. The Implementing Cisco Unified Wireless Networking Essentials training class is designed to help you prepare for the CCNA Wireless certification, an associate level certification in the wireless field. The goal of the IUWNE is to provide you with information to prepare you to help design, install, configure, monitor and conduct basic troubleshooting tasks of a Cisco WLAN in small and medium-sized business and enterprise installations. The IUWNE training class reinforces the instruction by providing you with hands-on labs that range from creating an ad-hoc network and analyzing the communication, configuring a controller, configure and migrate standalone access points (APs), install and configure a Mobility Express Wireless Controller and AP, experiment with connections and roaming, configure Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) authentication with Wi-Fi Protected Access (WPA), configure the controller and the AP from the Cisco Wireless Control System (WCS) interface, add a map to the WCS, enhance it with the Map editor tool and locate the AP on the map, backup the controller configuration, as well as troubleshooting issues introduced by the instructor.

Who Should Attend:

The Implementing Cisco Unified Wireless Network Essentials course is targeted to Network Engineers, Network Administrators, Network Managers, System Engineers, WLAN designers, Project Managers, and any individual wishing to attain the CCNP-Wireless level.

Prerequisites:

Students should have their Cisco Certified Networking Associate certification- CCNA.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the fundamentals of wireless technologies
- Install and configure a WLAN controller, in the main Cisco Unified Wireless Networks line or Mobility Express
- Install the ADU and configure wireless clients
- Configure wireless security
- Manage the network with WCS
- Use the controller and WCS tools to troubleshoot a wireless network

Course Outline:**Module 0 -- Course Introduction****Module 1 – Wireless Fundamentals**

Lab 1-1: Familiarization with Antennae And Ranges
Lab 1-2: EIRP Calculation and Antenna Choice
Lab 1-3: Creating and Ad-hoc (IBSS) Network and Analyzing the Communication

Module 2 – Basic Cisco WLAN Installation

Lab 2-1: Configure A Controller
Lab 2-2: Configuring And Migrating Standalone Access Points
Lab 2-3: Installing And Configuring A Mobility Express Wireless Controller And Access Point

Module 3 – Wireless Clients

Lab 3-1: Installing And Using The ADU
Lab 3-2: Experimenting with Connections And Roaming

Module 4 – WLAN Security

Lab 4-1: 802.1Q and Web Authentication
Lab 4-2: Configure EAP-FAST Authentication

Module 5 – WCS Administration

Lab 5-1: Configuring Controllers And Access Points From The WCS
Lab 5-2: Working With Maps
Lab 5-3: Monitor The Network And Containing Devices

Module 6 – WLAN Maintenance and Troubleshooting

Lab 6-1: Backup The Controller Configuration
Lab 6-2: Troubleshooting
Lab 6-3: Troubleshooting With Wireshark And Converting and Access Point to Autonomous Mode (Optional)

Course Description:

Implementing Cisco IP Routing (ROUTE) v1.0 is an instructor-led training course presented by Cisco training partners to their end customers. This five-day course is designed to help students prepare for Cisco CCNP® certification. The ROUTE course is a component of the CCNP curriculum.

The ROUTE course is designed to provide professionals of medium to large network sites with information on the use of advanced routing in implementing scalability for Cisco routers that are connected to LANs and WANs. The goal is to train professionals to dramatically increase the number of routers and sites using these techniques instead of redesigning the network when additional sites or wiring configurations are added. The ROUTE training reinforces the instruction by providing students with hands-on labs to ensure they thoroughly understand how to implement advanced routing within their networks.

Who Should Attend:

The primary audience for this course is network professionals who want to correctly implement routing-based solutions given a network design using Cisco IOS services and features, where implementation of routing includes planning, configuration, and verification.

Prerequisites:

Students must have the knowledge and skill level equal to Cisco CCNA® certification. They must also have knowledge of and experience with the implementation and verification of enterprise routing and switching technologies as offered by the Interconnecting Cisco Networking Devices Part 1 (ICND1) and Interconnecting Cisco Networking Devices Part 2 (ICND2) courses or equivalent skills and knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Plan and document the configuration and verification of routing protocols and their optimization in enterprise networks.
- Identify the technologies, components, and metrics of EIGRP used to implement and verify EIGRP routing in diverse, large-scale internetworks based on requirements.
- Identify, analyze, and match OSPF multiarea routing functions and benefits for routing efficiencies in network operations in order to implement and verify OSPF routing in a complex enterprise network
- Implement and verify a redistribution solution in a multi-protocol network that uses Cisco IOS features to control path selection and provides a loop-free topology according to a given network design and requirements
- Evaluate common network performance issues and identify the tools needed to provide Layer 3 path control that uses Cisco IOS features to control the path
- Implement and verify a Layer 3 solution using BGP to connect an enterprise network to a service provider

Course Outline:**Module 1: Planning Routing Services to Requirements**

Lesson 1: Assessing Complex Enterprise Network Requirements
Lesson 2: Common Maintenance Processes and Procedures
Lab 1-1: Assess Skills for Implementing Complex Networks
Lesson 3: Lab 1-1 Debrief

Module 2: Implementing an EIGRP based Solution

Lesson 1: Planning Routing Implementations with EIGRP
Lesson 2: Implementing and Verifying Basic EIGRP for the Enterprise LAN Architecture
Lab 2-1: Configure and Verify EIGRP Operations
Lesson 3: Lab 2-1 Debrief
Lesson 4: Configuring and Verifying EIGRP for the Enterprise WAN Architecture
Lab 2-2: Configure and Verify EIGRP Circuit Emulation, and Frame Relay Operations
Lesson 5: Lab 2-2 Debrief
Lesson 6: Implementing and Verifying EIGRP Authentication
Lab 2-3: Configure and Verify EIGRP Authentication
Lesson 7: Lab 2-3 Debrief
Lesson 8: Advanced EIGRP Features in an Enterprise Network
Lab 2-4: Implement and Verify EIGRP Operations
Lesson 9: Lab 2-4 Debrief

Module 3: Implementing a Scalable Multiarea Network OSPF Based Solution

Lesson 1: Planning Routing Implementations with OSPF as Scalable Routing Protocol
Lesson 2: How OSPF Packet Processes Work
Lesson 3: Improving Routing Performance in a Complex Enterprise Network
Lesson 4: Configuring and Verifying OSPF Routing
Lab 3-1: Configure and Verify OSPF to Improve Routing Performance
Lesson 5: Lab 3-1 Debrief
Lab 3-2: Implement and Verify OSPF Multiarea Routing
Lesson 6: Lab 3-2 Debrief
Lesson 7: Configuring and Verifying OSPF Route Summarization
Lab 3-3: Configure and Verify OSPF Route Summarization for Interarea and External Routes
Lesson 8: Lab 3-3 Debrief
Lesson 9: Configuring and Verifying OSPF Special Area Types
Lab 3-4: Configure and Verify OSPF Special Area Types
Lesson 10: Lab 3-4 Debrief
Lesson 11: Configuring and Verifying OSPF Authentication
Lab 3-5: Configure and Verify OSPF Authentication

Lesson 12: Lab 3-5 Debrief

Module 4: Implement an IPv4-based Redistribution Solution

Lesson 1: Assessing Network Routing Performance and Security Issues
Lesson 2: Operating a Network Using Multiple IP Routing Protocols
Lesson 3: Configuring and Verifying Route Redistribution
Lab 4-1: Configure Route Redistribution Between Multiple IP Routing Protocols
Lesson 4: Lab 4-1 Debrief

Module 5: Implementing Path Control

Lesson 1: Assessing Path Control Network Performance Issues
Lab 5-1: Configure and Verify Path Control between Multiple IP Routing Protocols
Lesson 2: Lab 5-1 Debrief
Lesson 3: References to additional Path Control in E-Learning

Module 6: Connection of an Enterprise Network to an ISP Network

Lesson 1: Planning the Enterprise-to-ISP Connection
Lesson 2: Considering the Advantages of Using BGP
Lesson 3: Comparing the Functions and Uses of EBGP and IBGP
Lesson 4: Configuring and Verifying Basic BGP Operations
Lab 6-1: Configure BGP Operations
Lesson 5: Lab 6-1 Debrief
Lesson 6: Using the BGP Attributes and Path Selection Process
Lab 6-2: Manipulate EBGP Path Selections
Lesson 7: Lab 6-2 Debrief
Lesson 8: E-Learning Training on IPv6 and Routing for Branch Offices and Remote Workers

Course Description:

Implementing Cisco Switched Networks (SWITCH) v1.0 is a five-day instructor-led training course, designed to help students prepare to plan, configure, and verify the implementation of complex enterprise switching solutions for campus environments using the Cisco Enterprise Campus Architecture. These skills are validated in the Cisco CCNP® Routing and Switching certification, a professional-level certification specializing in the routing and switching field. This course is a component of the Cisco CCNP Routing and Switching curriculum. This course is designed to give students a firm understanding of how to manage switches in an enterprise campus environment. This training class reinforces the instruction by providing students with hands-on labs.

Who Should Attend:

The primary audience for this course are network professionals who will need to correctly implement switch-based solutions given a network design using Cisco IOS services and features. The typical job roles for this type of professional are network engineers, network operations center (NOC) technical support personnel, or help desk technicians.

Prerequisites:

Students must have knowledge and experience equivalent to having attended the Interconnecting Cisco Networking Devices Part 1 (ICND1) and Interconnecting Cisco Networking Devices Part 2 (ICND2) courses.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Analyze campus network designs
- Implement VLANs in a network campus
- Implement spanning tree
- Implement inter-VLAN routing in a campus network
- Implement a highly available network
- Implement high-availability technologies and techniques using multilayer switches in a campus environment
- Implement security features in a switched network
- Integrate WLANs into a campus network
- Accommodate voice and video in campus networks

Course Outline:**Module 1: Analyzing Campus Network Designs**

Lesson 1: Enterprise Campus Architecture
Lesson 2: Cisco Lifecycle Services and Network Implementation
Lab 1-1: New Hire Test
Lesson 3: Lab 1-1 Debrief

Module 2: Implementing VLANs in Campus Networks

Lesson 1: Applying Best Practices for VLAN Topologies
Lesson 2: Configuring Private VLANs
Lesson 3: Configuring Link Aggregation with EtherChannel
Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel
Lesson 4: Lab 2-1 Debrief
Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues
Lesson 5: Lab 2-2 Debrief
Lab 2-3: Configure Private VLANs
Lesson 6: Lab 2-3 Debrief

Module 3: Implementing Spanning Tree

Lesson 1: Spanning Tree Protocol Enhancements
Lesson 2: Describing STP Stability Mechanisms
Lab 3-1: Implement Multiple Spanning Tree
Lesson 3: Lab 3-1 Debrief
Lab 3-2: Implement PVSRT+
Lesson 4: Lab 3-2 Debrief
Lab 3-3: Troubleshoot Spanning Tree Issues
Lesson 5: Lab 3-2 Debrief

Module 4: Implementing Inter-VLAN Routing

Lesson 1: Describing Routing Between VLANs
Lesson 2: Deploying Multilayer Switching with Cisco Express Forwarding
Lab 4-1: Implement Inter-VLAN Routing
Lesson 3: Lab 4-1 Debrief
Lab 4-2: Troubleshoot Inter-VLAN Routing
Lesson 4: Lab 4-2 Debrief

Module 5: Implementing a Highly Available Network

Lesson 1: Understanding High Availability
Lesson 2: Implementing High Availability
Lesson 3: Implementing Network Monitoring
Lab 5-1: Implement High Availability in a Network Design
Lesson 4: Lab 5-1 Debrief

Module 6: Implementing Layer 3 High Availability

Lesson 1: Configuring Layer 3 Redundancy with HSRP
Lesson 2: Configuring Layer 3 Redundancy with VRRP and GLBP
Lab 6-1: Implement and Tune HSRP
Lesson 3: Lab 6-1 Debrief
Lab 6-2: Implement VRRP

Lesson 4: Lab 6-2 Debrief

Module 7: Minimizing Service Loss and Data Theft in a Campus Network

Lesson 1: Understanding Switch Security Issues
Lesson 2: Protecting Against VLAN Attacks
Lesson 3: Protecting Against Spoofing Attacks
Lesson 4: Securing Network Services
Lab 7-1: Secure Network Switches to Mitigate Security Attacks
Lesson 5: Lab 7-1 Debrief

Module 8: Accommodating Voice and Video in Campus Networks

Lesson 1: Planning for Support of Voice in a Campus Network
Lesson 2: Integrating and Verifying VoIP in a Campus Infrastructure
Lesson 3: Working with Specialists to Accommodate Voice and Video on Campus Switches
Lab 8-1: Plan Implementation and Verification of VoIP in a Campus Network
Lesson 4: Lab 8-1 Debrief

Module 9: Integrating Wireless LANs into a Campus Network

Lesson 1: Comparing WLANs with Campus Networks
Lesson 2: Assessing the Impact of WLANs on Campus Networks
Lesson 3: Preparing the Campus Infrastructure for WLANs
Lab 9-1: Integrate Wireless in the Campus
Lesson 4: Lab 9-1 Debrief

Course Description:

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) v1.0 is an instructor-led training course that is presented by Cisco training partners to customers who use Cisco products. This five-day course is designed to help network professionals improve the skills and knowledge that they need to maintain their network and to diagnose and resolve network problems quickly and effectively. It also assists the network professional in preparing for Cisco CCNP® certification. This course is a component of the CCNP curriculum.

The course is designed to teach professionals who work in complex network environments the skills that they need to maintain their networks and to diagnose and resolve network problems quickly and effectively. The course will provide information about troubleshooting and maintaining particular technologies, as well as procedural and organizational aspects of the troubleshooting and maintenance process. A large part of the training will consist of practicing these skills and reinforcing the concepts by putting them to use in a controlled environment. At the end of the course, the students will have increased their skill level and developed a set of best practices that are based on their own experience and the experiences of other students and that they can take back to their organizations.

Who Should Attend:

The primary audience for this course are network professionals who want to increase their skill level at maintaining and troubleshooting complex Cisco IP networks. The typical job roles for this type of professional are network engineer, network operations center (NOC) technical support personnel, or help desk technicians.

Prerequisites:

Students must have Cisco CCNA® certification. In addition to CCNA certification, it is recommended that the student have practical experience in installing, operating, and maintaining Cisco routers and switches in an enterprise environment. Students should also have knowledge of and experience with the implementation and verification of enterprise routing and switching technologies as offered by the Implementing Cisco Switched Networks (SWITCH) and Implementing Cisco IP Routing (ROUTE) courses or have equivalent skills and knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Plan and document the most commonly performed maintenance functions in complex enterprise networks
- Develop a troubleshooting process to identify and resolve problems in complex enterprise networks
- Select tools that best support specific troubleshooting and maintenance processes in large, complex enterprise networks
- Practice maintenance procedures and fault resolution in switching-based environments
- Practice maintenance procedures and fault resolution in routing-based environments
- Practice maintenance procedures and fault resolution in a secure infrastructure
- Troubleshoot and maintain integrated, complex enterprise networks

Course Outline:**Module 1: Planning Maintenance for Complex Networks**

Lesson 1: Applying Maintenance Methodologies
Lesson 2: Common Maintenance Processes and Procedures
Lesson 3: Network Maintenance Tools, Applications, and Resources
Lab 1-1: Lab Access

Module 2: Planning Troubleshooting Processes for Complex Enterprise Networks

Lab 2-1: Introduction to Troubleshooting
Lesson 1: Lab 2-1 Debrief
Lesson 2: Applying Troubleshooting Methodologies
Lesson 3: Planning and Implementing Troubleshooting Procedures
Lesson 4: Integrating Troubleshooting into the Network Maintenance Process

Module 3: Maintenance and Troubleshooting Tools and Applications

Lesson 1: Assembling a Basic Diagnostic Toolkit Using Cisco IOS Software
Lesson 2: Using Specialized Maintenance and Troubleshooting Tools
Lab 3-1: Maintenance and Troubleshooting Tools
Lesson 3: Lab 3-1 Debrief

Module 4: Maintaining and Troubleshooting Campus Switching-Based Solutions

Lesson 1: Troubleshooting VLANs
Lesson 2: Troubleshooting Spanning Tree
Lab 4-1: Layer 2 Connectivity and Spanning Tree
Lesson 3: Lab 4-1 Debrief
Lesson 4: Troubleshooting Switched Virtual Interfaces and Inter VLAN Routing
Lesson 5: Troubleshooting FHRPs
Lab 4-2: Layer 3 Switching and First-Hop Redundancy
Lesson 6: Lab 4-2 Debrief
Lesson 7: Troubleshooting Performance Problems on Switches
Lesson 8: References to Additional Campus Switching Technologies in E-Learning

Module 5: Maintaining and Troubleshooting Routing-Based Solutions

Lesson 1: Troubleshooting Network Layer Connectivity
Lesson 2: Troubleshooting EIGRP
Lab 5-1: Layer 3 Connectivity and EIGRP
Lesson 3: Lab 5-1 Debrief
Lesson 4: Troubleshooting OSPF
Lesson 5: Troubleshooting Route Redistribution
Lab 5-2: OSPF and Route Redistribution
Lesson 6: Lab 5-2 Debrief
Lesson 7: Troubleshooting BGP
Lab 5-3: Border Gateway Protocol
Lesson 8: Lab 5-3 Debrief
Lesson 9: Troubleshooting Performance Problems on Routers
Lab 5-4: Router Performance
Lesson 10: Lab 5-4 Debrief
Lesson 11: References to Additional Troubleshooting on NAT and DHCP in E-Learning

Module 6: Maintaining and Troubleshooting Network Security Solutions

Lesson 1: Troubleshooting Security Features
Lab 6-1: Introduction to Network Security
Lesson 2: Lab 6-1 Debrief
Lesson 3: Security Features Review
Lab 6-2: Cisco IOS Security Features
Lesson 4: Lab 6-2 Debrief
Lesson 5: References to Additional Security Troubleshooting in E-Learning

Module 7: Maintaining and Troubleshooting Integrated, Complex Enterprise Networks

Lesson 1: Troubleshooting Complex Environments
Lab 7-1: Troubleshooting Complex Environments
Lesson 2: Lab 7-1 Debrief

Course Description:

Cisco Communications Manager System Administration v6.0 (CCMSAv6.0) course focuses on the basic administration of the Cisco Communications Manager product and the devices that register to the Cisco Communications Manager. The course is 40% hands-on laboratory exercises that challenge the student to configure IP Phones, voice gateways, media resources such as Music on Hold, conference and transcoders as well as Call Admission Control.

Who Should Attend:

The target audience for this course combination would be first and second level customer support personnel. The course will teach basic function and programming for Cisco Communications Manager 6.0. This course is equally beneficial to personnel with either data or voice backgrounds.

Prerequisites:

The knowledge and skills a learner must have before attending this course include basic networking and telephony knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify and describe the UC architecture, hardware, and software.
- Access the online administration guide to perform Moves, Adds, and Changes to IP phones, voice gateways, and Call Admission Control components of a Unified Communications solution.
- Access the online administration guide to configure Music on Hold, conference resources, media termination points, and transcoders then allocate these resources to devices as needed.
- Provide level one support to IP Phone users.

Course Outline:

Cisco Unified Communications Manager

Communications Manager Functions
Operating System, Database and Supporting Applications
Cluster Definition
Intra-cluster Communication
Clustering Options
Cisco Communications Manager Components
Deployment Models
Backing up the Communications Manager
Lab 1-1: Performing General Administration
Lab 1-2: Configuring Cisco Unified Communications Manager 6.0 Basic Settings

System Configuration

Access to Communications Manager Administration
MLA - Multi Level Administration
System Parameter
Auto-registration
Cisco IP Phones
IP Phone Models
Phone Button Templates
Softkey Templates
Registration Process
Basic Phone and Directory Number Configuration
Lab 2-1: Configuring Cisco Unified Communications Manager to Support Cisco IP Phones

Route Plan Basics

External Call Routing
Route Pattern Wildcards
Digit Analysis
Route Plan Configuration
Lab 3-1: Configuring Basic Dial Plan Elements

Advanced Route Plan

Route Filters
Discard Digits Instructions
Transformation Masks
Translation Patterns
Transformation Patterns
Route Plan Report
Lab 4-1: Configuring Complex Dial Plan Elements

Telephony Class of Service

Partitions
Calling Search Spaces
Problems Addressed
Time of Day Routing
Lab 5-1: Implementing Calling Privileges and Restrictions

Call Admission Control (CAC) and Survivable Remote Site Telephony (SRST)

Why Call Admission Control?
Distributed Call Processing CAC - Gatekeeper
Centralized Call Processing CAC - Locations

Survivable Remote Site Telephony (SRST)
Automated Alternate Routing (AAR)

Media Resources

Media Resource Overview
Conferencing Resources
Media Termination Points
Music On Hold Resources
Annunciator Resources
Media Resource Management
Lab 7-1: Configuring Media Resources

Communications Manager Features

Call Park
Call Pickup
Callback
Barge and Privacy
Hunt List
Cisco IP Phone Services
Mobile Connect and Mobile Voice Access
Lab 8-1: Configuring User Features
Lab 8-2: Configuring Hunt Groups and Call Coverage

LDAP Users

Adding a User
User Logon and Device Selection
Call Forward
Speed Dials
Cisco IP Phone Services Subscription
Personal Address Book
Message Waiting Lamp Policy
Personal Device Locale
User Options Web Pages Locale
Lab 9-1: Create/Associate Users

Adding Individual Phone Profiles

Phone Configuration Screens
Directory Number Configuration Screens

Bulk Administration Tool (BAT)

Installation and Features
Templates
Creating .csv Files
Adding and Updating
Lab 10-1: Using the Cisco Unified Communications Manager Bulk Administration Tool

Course Description:

Unity Connection Administration (UCA) v8.5 describes Cisco Unity Connection administration features, options, and configuration settings as they apply to the administrator. The course presents Cisco Unity Connection with the focused goal of providing the administrators with the necessary skills to perform their day-to-day job functions using the Cisco Unity Connection version 8.5 system. Students that require skills beyond administration where engineering, integration, and networking skills are required should consider the Implementing Cisco Unity Connection (IUC) course.

This course provides an understanding of latest Cisco Unity Connection version 8.5 features such as Unified Messaging concepts and implementation, including Single Inbox, Text to Speech, and calendars.

Who Should Attend:

The primary audiences for this course are Administrators, IT support personnel, and Helpdesk support staff. The secondary audiences for this course are Network Engineering Staff Personnel.

Prerequisites:

Students should have a basic understanding of fundamental terms and concepts of computer networking, including LANs, WANs, and IP switching and routing. They should also have a basic knowledge of traditional PSTN operations and technologies, including PBX and voice-mail administration tasks and also have a basic understanding of Cisco Unified Communications Manager.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Explain the function of Cisco Unity Connection and the various interfaces that are used to access the system
- Describe the components that are required for user call processing by Cisco Unity Connection
- Implement the various features and options that are available to users in Cisco Unity Connection
- Explore the version 8.5 features and function of Unified Messaging, including Single Inbox, Text to Speech and calendars.
- Use the various applications, tools, and reports that are available in Cisco Unity Connection

Course Outline:**Module 1: Introduction to Cisco Unity Connection**

An Overview of Cisco Unity Connection
Navigating Cisco Unity Connection
Understanding Call Handlers, Users, and Call Flow
Lab 1-1: Verifying Connectivity and Call Flow
Lab 1-2: Verifying and Configuring Call Handlers
Lab 1-3: Working with Users and Extensions in Voice Mail

Module 2: Configuring Users and Contacts

Explaining Users and Contacts
Managing Multiple Users
Lab 2-1: Preparing to Configure Users and Contacts
Lab 2-2: Managing Users and Contacts
Lab 2-3: Managing Multiple Users

Module 3: Implementing Features

Implementing the Dial Plan
Understanding User Features
Accessing Voice Messaging and User Features
Managing Distribution Lists
Lab 3-1: Implementing the Dial Plan
Lab 3-2: Understanding User Features
Lab 3-3: Implementing Messaging and User Features

Module 4: Using Cisco Unity Connection Applications, Tools and Reports

Designing an Audiotext Application
Using Cisco Unity Connection Tools and Reports
Using the Disaster Recovery System
Lab 4-1: Implementing an Audiotext Application
Lab 4-2: Using Cisco Unity Connection Tools and Reports

Course Description:

Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) v8.0 prepares you for implementing a Cisco Unified Communications Manager solution at a single-site environment. This course focuses primarily on Cisco Unified Communications Manager Version 8.0, which is the call routing and signaling component for the Cisco Unified Communications solution.

You will perform post-installation tasks, configure Cisco Unified Communications Manager, implement Media Gateway Control Protocol (MGCP) and H.323 gateways, and build dial plans to place on-net and off-net phone calls. You will also implement media resources, Cisco IP Phone Services, Cisco Unified Communications Manager native presence, and Cisco Unified Mobility.

Who Should Attend:

The primary audiences for this course are network administrators, network engineers, and CCNP Voice candidates. The secondary audience for this course are systems engineers.

Prerequisites:

The knowledge and skills that a learner must have before attending this course include working knowledge of fundamental terms and concepts of computer networking, including LANs, WANs, and IP switching and routing. Students must also have the ability to configure and operate Cisco routers and switches and to enable VLANs and DHCP, know the basics of digital interfaces, PSTN, and VoIP, have fundamental knowledge of converged voice and data networks, and have the ability to configure Cisco IOS gateways with traditional and VoIP call legs.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe Cisco Unified Communications Manager, including its functions, architecture, deployment and redundancy options, and how to install or upgrade
- Perform Cisco Unified Communications Manager initial configuration and user management
- Configure Cisco Unified Communications Manager to support on-cluster calling
- Implement PSTN access in Cisco Unified Communications Manager and to build a dial plan in a single-site Cisco Unified Communications Manager deployment
- Implement Cisco Unified Communications Manager media resources
- Implement Cisco Unified Communications Manager features and applications

Course Outline:**Module 1: Introduction to Cisco Unified Communications Manager**

Understanding Cisco Unified Communications Manager Architecture
Understanding Cisco Unified Communications Manager Deployment and Redundancy Options

Module 2: Administering Cisco Unified Communications Manager

Managing Services and Initial Configuration of Cisco Unified Communications Manager
Managing User Accounts in Cisco Unified Communications Manager
Lab 2-1: Configuring Cisco Unified Communications Manager Initial Settings
Lab 2-2: Managing User Accounts in Cisco Unified Communications Manager

Module 3: Single-Site On-Net Calling

Understanding Endpoints in Cisco Unified Communications Manager
Implementing IP Phones
Lab 3-1: Implementing IP Phones

Module 4: Single-Site Off-Net Calling

Implementing PSTN Gateways in Cisco Unified Communications Manager
Configuring Cisco Unified Communications Manager Call-Routing Components
Using Partitions and CSSs to Implement Calling Privileges for On-Net Calls
Implementing Cisco Unified Communications Manager Digit Manipulation
Implementing Gateway Selection and PSTN Access Features
Implementing Call Coverage in Cisco Unified Communications Manager
Lab 4-1: Implementing PSTN Gateways
Lab 4-2: Configuring Cisco Unified Communications Manager Call-Routing Components
Lab 4-3: Implementing Digit Manipulation
Lab 4-4: Implementing Calling Privileges in Cisco Unified Communications Manager
Lab 4-5: Implementing Call Coverage in Cisco Unified Communications Manager

Module 5: Media Resources

Implementing Media Resources in Cisco Unified Communications Manager
Lab 5-1: Implementing Media Resources

Module 6: Feature and Application Implementation

Configuring Cisco IP Phone Services
Configuring Cisco Unified Communications Manager Native Presence
Configuring Cisco Unified Mobility
Lab 6-1: Configuring Cisco Unified Communications Manager Native Presence
Lab 6-2: Configuring Cisco Unified Mobility

Course Description:

Implementing Cisco Unified Communications Manager, Part 2 (CIPT2) v8.0 prepares you for implementing Cisco Unified Communications solution in a multisite environment. It covers globalized call routing, Cisco Service Advertisement Framework (SAF) and Call Control Discovery (CCD), tail-end hop-off (TEHO), Cisco Unified Survivable Remote Site Telephony (SRST), and mobility features such as Device Mobility and Cisco Extension Mobility.

You will apply a dial plan for a multisite environment including TEHO, configure survivability for remote sites during WAN failure, and implement solutions to reduce bandwidth requirements in the IP WAN. You will also enable Call Admission Control (CAC), including Session Initiation Protocol (SIP) Preconditions and automated alternate routing (AAR).

Who Should Attend:

The primary audiences for this course are network administrators and network engineers, as well as CCNP Voice candidates. The secondary audiences for this course are systems engineers.

Prerequisites:

Students should have working knowledge of converged voice and data networks, working knowledge of the MGCP, SIP, and H.323 protocols and their implementation on Cisco IOS gateways, the ability to configure and operate Cisco routers and switches, and the ability to configure and operate Cisco Unified Communications Manager in a single-site environment.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe multisite deployment issues and solutions, and describe and configure required dial plan elements
- Implement call-processing resiliency in remote sites by using Cisco Unified SRST, MGCP fallback, and Cisco Unified Communications Manager Express in Cisco Unified SRST mode
- Implement bandwidth management and CAC to prevent oversubscription of the IP WAN
- Implement Device Mobility and Cisco Extension Mobility
- Describe and implement CCD deployments

Course Outline:**Module 1: Multisite Deployment Implementation**

Identifying Issues in a Multisite Deployment
Identifying Multisite Deployment Solutions
Implementing Multisite Connections
Implementing a Dial Plan for International Multisite Deployments
Lab 1-1: Implementing Basic Multisite Connections
Lab 1-2: Implementing a Dial Plan for International Multisite Deployments

Module 2: Centralized Call-Processing Redundancy Implementation

Examining Remote Site Redundancy Options
Implementing SRST and MGCP Fallback
Implementing Cisco Unified Communications Manager Express in SRST Mode
Lab 2-1: Implementing SRST and MGCP Fallback
Lab 2-2: Implementing Cisco Unified Communications Manager Express in SRST Mode

Module 3: Bandwidth Management and CAC Implementation

Managing Bandwidth
Implementing CAC
Lab 3-1: Implementing Bandwidth Management
Lab 3-2: Implementing CAC

Module 4: Implementation of Features and Applications for Multisite Deployments

Implementing Device Mobility
Implementing Cisco Extension Mobility
Lab 4-1: Implementing Device Mobility
Lab 4-2: Implementing Cisco Extension Mobility

Module 5: Call Control Discovery

Implementing SAF and CCD
Lab 5-1: Implementing Cisco SAF and CCD

Course Description:

Implementing Cisco Unified Communications IP Telephony Part 2 (CIPT2) v7.0/v6.0 prepares you for implementing and configuring, a Cisco Unified Communications Manager solution in a multisite environment. This course focuses on Cisco Unified CallManager, the call routing and signaling component for the Cisco Unified Communications solution. It also includes H.323 and Media Gateway Control Protocol (MGCP) gateway implementation, the use of a Cisco Unified Border Element, and configuration of Survivable Remote Site Telephony (SRST), different mobility features and voice security.

This course includes lab activities in which you will apply a dial plan for a multisite environment, configure survivability for remote sites during WAN failure and implement solutions to reduce bandwidth requirements in the IP WAN. You will also enable call admission control (CAC) and automated alternate routing (AAR), a feature that allows rerouting of calls over the public switched telephone network (PSTN) in case of no available bandwidth. There are labs for implementing Cisco Unified Communications Manager Device Mobility, Cisco Unified Communications Manager Extension Mobility, Cisco Unified Mobility, and voice security.

Who Should Attend:

This course is primarily for Network designers, Network administrators, Network engineers, Network managers, and Systems engineers.

Prerequisites:

The knowledge and skills that a learner must have before attending this course are as follows: * Working knowledge of converged voice and data networks, * Working knowledge of MGCP, session initiation protocol (SIP), and H.323, as well as their implementation on Cisco IOS gateways, * Ability to configure and operate Cisco routers and switches, and * Ability to configure and operate Cisco Unified Communications Manager in a single-site environment.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the issues in multisite deployments and their solutions, and describe and configure required dial plan elements.
- Implement call-processing resiliency in remote sites using SRST, MGCP fallback, and Cisco Unified Communications Manager Express.
- Implement CAC to prevent oversubscription of the IP WAN.
- Implement Cisco IOS Tcl and VoiceXML applications, along with mobility features such as Cisco Unified Communications Manager Device Mobility, Cisco Unified Communications Manager Extension Mobility, and Cisco Unified Mobility, so that users are reachable via their office phone numbers, regardless of their physical location and the various devices they may use.
- Secure a Cisco Unified Communications IP telephony deployment.

Course Outline:**Course Introduction**

Overview
Course Goal and Objectives
Course Flow
Additional References
Your Training Curriculum

Module 1: Multisite Deployments

Identifying Issues in a Multisite Deployment
Identifying Solutions for a Multisite Deployment
Implementing Multisite Connections
Implementing a Dial Plan for Multisite Deployments
Lab 1-1: Implementing Basic Multisite Connections
Lab 1-2: Implementing Multisite Dial Plans

Module 2: Centralized Call-Processing Redundancy

Examining Remote Site Redundancy Options
Implementing SRST and MGCP Fallback
Implementing CiscUnified Communications Manager Express in SRST Mode
Lab 2-1: Implementing CiscUnified SRST and MGCP Fallback
Lab 2-2: Implementing CiscUnified Communications Manager Express as SRST Fallback

Module 3: Bandwidth Management and Call Admission Control

Implementing Bandwidth Management
Implementing Call Admission Control
Lab 3-1: Implementing Bandwidth Management
Lab 3-2: Implementing CAC

Module 4: Features and Applications for Multisite Deployments

Implementing Call Applications on CiscIOS Gateways
Implementing Device Mobility
Implementing Extension Mobility
Implementing CiscUnified Mobility
Lab 4-1: Enabling the Device Mobility Feature
Lab 4-2: Implementing CiscUnified Communications Manager Extension Mobility
Lab 4-3: Implementing CiscUnified Mobility

Module 5: IP Telephony Security

Understanding Cryptographic Fundamentals and PKI
Understanding Native CiscUnified Communications Manager Security Features and CiscUnified Communications Manager PKI
Implementing Security in CiscUnified Communications Manager
Lab 5-1: Implementing Security in CiscUnified Communications Manager

Course Description:

Implementing Cisco Voice Communications and QoS (CVOICE) v8.0 teaches learners about voice gateways, characteristics of VoIP call legs, dial plans and their implementation, basic implementation of IP phones in Cisco Unified Communications Manager Express environment, and essential information about gatekeepers and Cisco Unified Border Element. The course provides the learners with voice-related quality of service (QoS) mechanisms that are required in Cisco Unified Communications networks.

Who Should Attend:

This course is for network administrators, network engineers, and CCNP Voice candidates. Systems engineers will also benefit from taking this course.

Prerequisites:

The knowledge and skills that a learner must have before attending this course includes working knowledge of fundamental terms and concepts of computer networking, including LANs, WANs, and IP switching and routing, the ability to configure and operate Cisco IOS routers in an IP environment at the Cisco CCNA® Routing and Switching level, and basic knowledge of traditional voice, converged voice, and data networks at the Cisco CCNA Voice level.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Explain what a voice gateway is, how it works, and describe its usage, components, and features
- Describe the characteristics and configuration elements of VoIP call legs
- Describe how to implement IP phones using Cisco Unified Communications Manager Express
- Describe the components of a dial plan, and explain how to implement a dial plan on a Cisco Unified voice gateway
- Explain what gatekeepers and Cisco Unified Border Elements are, how they work, and what features they support
- Describe why QoS is needed, what functions it performs, and how it can be implemented in a Cisco Unified Communications network

Course Outline:**Module 1: Introduction to Voice Gateways**

Understanding Cisco Unified Communications Networks and the Role of Gateways
Examining Gateway Call Routing and Call Legs
Configuring Gateway Voice Ports
Understanding DSP Functionality, Codecs, and Codec Complexity
Lab 1-1: Configuring Voice Ports
Lab 1-2: Configuring DSPs

Module 2: VoIP Call Legs

Examining VoIP Call Legs and VoIP Media Transmission
Explaining H.323 Signaling Protocol
Explaining SIP Signaling Protocol
Explaining MGCP Signaling Protocol
Describing Requirements for VoIP Call Legs
Configuring VoIP Call Legs
Lab 2-1: Configuring VoIP Call Legs

Module 3: Cisco Unified Communications Manager Express Endpoints Implementation

Introducing Cisco Unified Communications Manager Express
Examining Cisco Unified Communications Manager Express Endpoint Requirements
Configuring Cisco Unified Communications Manager Express Endpoints
Lab 3-1: Configuring Cisco Unified Communications Manager Express to Support Endpoints

Module 4: Dial Plan Implementation

Introducing Call Routing
Understanding Dial Plans
Describing Digit Manipulation
Configuring Path Selection
Configuring Calling Privileges
Lab 4-1: Implementing Digit Manipulation
Lab 4-2: Implementing Path Selection
Lab 4-3: Implementing Calling Privileges

Module 5: Gatekeeper and Cisco Unified Border Element Implementation

Understanding Gatekeepers
Examining Cisco Unified Border Element
Lab 5-1: Implementing Gatekeepers
Lab 5-2: Implementing Cisco Unified Border Element

Module 6: Quality of Service

Introducing QoS
Understanding QoS Mechanisms and Models
Explaining Classification, Marking, and Link Efficiency Mechanisms
Managing Congestion and Rate Limiting
Understanding Cisco AutoQoS
Lab 6-1: Implementing QoS Using Cisco AutoQoS and Manual Configuration

Course Description:

Troubleshooting Cisco Unified Communications Systems (TUC) v1.0 equips network professionals with the knowledge and skills required to troubleshoot Unified Communications systems & solutions in Enterprise, Mid-Market, and Commercial deployments. TUC teaches troubleshooting methodology, triage, resources, tools and fixes at the integrated system or solution level, and for components such as Cisco Unified Call Manager, Cisco Unity, videoconferencing, and infrastructure. This is a troubleshooting course and the learners should spend 60-70 percent of their time in the lab.

Who Should Attend:

This course is for Network administrators, Network engineers, System engineers, and Network managers.

Prerequisites:

The knowledge and skills that a learner must have before attending this course are as follows: * Sound fundamental networking knowledge (CCNA), * Voice fundamentals: Cisco Voice over IP (CVOICE), * Call Agent (Cisco Unified CallManager) skills and knowledge: Cisco IP Telephony Part 1 and Part 2 (CIPT1 and CIPT2), * Voice Infrastructure: Implementing Gateways and Gatekeepers (GWGK), and * an understanding of factors that affect voice and video quality: Implementing Cisco Quality of Service (QoS).

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Use a systematic methodology to troubleshoot Cisco Unified Communication systems by using knowledge of tools and reports that help isolate Cisco Unified Communication system problems.
- Isolate the specific problem, propose a solution, and, where appropriate, implement the solution when given a trouble call that has been categorized as a Cisco Unified CallManager-related issue.
- Diagnose a call setup issue and resolve the issues.
- Troubleshoot the quality of both voice and video streams.
- Isolate the specific problem, propose a solution, and, where appropriate, implement the solution when given a trouble call that has been isolated to a Cisco Unified Communications system component application.

Course Outline:**Course Introduction**

Overview
Course Goal and Objectives
Course Flow
Additional References
Your Training Curriculum

Module 1: A Methodology and Tools for Troubleshooting Cisco Unified Communications Systems

Introducing Cisco Unified Communications Systems Troubleshooting
Understanding Troubleshooting Methodology in Cisco Unified Communications Systems
Gathering Information for Troubleshooting
Lab 1-1: Lab Discovery and Phone Configuration
Lab 1-2 Using TUC Tools

Module 2: Troubleshoot Cisco Unified CallManager-Related Issues

Troubleshooting Common Endpoint Registration Issues
Troubleshooting Cisco Unified CallManager Availability Issues
Troubleshooting Cisco Unified CallManager Security Issues
Troubleshooting Database Replication Issues
Troubleshooting LDAP Replication Issues
Troubleshooting Common Gateway Registration Issues
Lab 2-1: Trouble Ticket 1
Lab 2-2: Trouble Ticket 2
Lab 2-3: Trouble Ticket 3
Lab 2-4: Trouble Ticket 4
Case Study 2-5: Troubleshoot LDAP Synchronization Issues for Cisco Unified CallManager Release 4.1(3)
Lab 2-6: Trouble Ticket 6
Case Study 2-7: Troubleshoot Database Replication Issues for Cisco Unified CallManager Release 4.x
Lab 2-8: Trouble Ticket 8

Module 3: Troubleshoot Call Setup Issues

Introducing Call Setup Issues and Causes
Troubleshooting On-Premises Single-Site Calling Issues
Troubleshooting Offsite Call Issues
Troubleshooting Intercluster Dial Plan Issues
Troubleshooting Gatekeepers in a Cisco Unified Communications System
Lab 3-1: Trouble Ticket 1
Lab 3-2: Trouble Ticket 2
Lab 3-3: Trouble Ticket 3
Lab 3-4: Trouble Ticket 4
Lab 3-5: Trouble Ticket 5

Lab 3-6: Trouble Ticket 6
Lab 3-7: Trouble Ticket 7
Lab 3-8: Trouble Ticket 8
Lab 3-9: Trouble Ticket 9
Lab 3-10: Trouble Ticket 10

Module 4: Troubleshoot Voice and Video Quality Issues

Defining Common Voice and Video Quality Issues
Troubleshooting VoIP Quality Problems
Troubleshooting Echo
Troubleshooting Quality Problems of Cisco Unified Video Advantage
Lab 4-1: Trouble Ticket 1
Lab 4-2: Trouble Ticket 2
Lab 4-3: Trouble Ticket 3
Lab 4-4: Trouble Ticket 4

Module 5: Application Integration and Media Resource Issues

Troubleshooting Common Cisco Unity Integration Issues
Troubleshooting CTI Issues
Troubleshooting Media Resources
Lab 5-1: Trouble Ticket 1
Lab 5-2: Trouble Ticket 2
Lab 5-3: Trouble Ticket 3
Lab 5-4: Trouble Ticket 4
Lab 5-5: Trouble Ticket 5
Lab 5-6: Trouble Ticket 6

Course Description:

Communications Manager Administration (CMA) v8.5 provides system administrators and networking professionals with an understanding of the Cisco Unified Communications Manager System. This course teaches the concepts of IP telephony based in system administration, including its function, features, and configuration. This is an entry-level course that begins with the basic concepts of IP telephony and very quickly moves the learner forward into an understanding of system concepts: clustering, creation of phones and users, route plans, digit manipulation, media resources, phone features and services, which are all important to supporting IP telephony in the enterprise network. The course focuses on Cisco Unified Communications Manager version 8.5.

The course is geared to individuals that will be using and managing the system and performing administration for level 1 and beginning level 2 support. Level 1 support is geared toward supporting phone users and making moves, adds, and changes to the desktop phone environment. Level 2 support is oriented to supporting changes in the organization, such as opening new office locations or relocating departments. The course does not cover issues of initial deployment, new cluster deployment or international deployments. Also, the course does not cover issues with the underlying network that involve routers, switches, or Cisco IOS software configuration.

This course includes various lab exercises to apply what was learned in each preceding lesson. Labs begin with a newly installed publisher. The only element that is preconfigured is two MGCP gateways, for the headquarters (HQ) and branch (BR), and an intercluster trunk pointing to the neighbor's pod. Therefore, the student will become familiar with all the various concepts through configuration of the elements in the lab environment.

Who Should Attend:

The primary audience for this course are phone network administrators, data system administrators, and entry-level network engineers. The secondary audience for this course includes those looking to gain a technical overview of Cisco Unified Communications Manager and those who need a preparatory course before taking CIPT1 and CIPT2.

Prerequisites:

Students must have basic knowledge of the Windows desktop environment. They should also have basic knowledge of IP and networking or voice networks, but it is not required.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the Cisco Unified Communications Manager network, service, and features
- Understand the importance of and configuration of redundancy and high availability in the enterprise network
- Explore the basic server configuration and administration
- Describe user configuration and web interface
- Explain the user configuration and functions and features in credential policies
- Understand the configuration and features of the Disaster Recovery System to configure backups and perform a restore
- Explain basic phone configuration options and the use of the Bulk Administration Tool (BAT)
- Understand the purpose and function of Class of Control and the various configuration elements required for the traditional and line/device approach
- Explain the route plan and on-net/off-net calling
- Understand the various dial plan configuration elements, including translation patterns, route filters and various digit manipulation elements

Course Outline:**Module 1: Introduction to IP Telephony**

Exploring IP Telephony
Describing Deployment Models

Module 2: Defining the Basic Configuration

Logging In to Cisco Unified Communications Manager
Basic Server Configuration
Describing User Administration
Configuring DRS Backup and Restore Procedures
Lab 2-1: Performing General Administration
Lab 2-2: Configuring Basic Settings
Lab 2-3: Backing Up and Restoring the Publisher

Module 3: User Administration

Understanding User Configuration
Using the User Web Pages
Lab 3-1: Creating and Associating Users

Module 4: Preparing for Phone Registration

Configuring System Parameters
Supporting Cisco IP Phones
Exploring Phone Registration and Cisco IP Phones
Using the Bulk Administration Tool (BAT)

Lab 4-1: Configuring the System to Support Cisco IP Phones
Lab 4-2: Using the Cisco Unified Communications Manager BAT

Module 5: Configuring a Basic Route Plan

Dial Plan Connectivity
Creating a Route Plan
Lab 5-1: Configuring Basic Dial Plan Elements

Module 6: Understanding Route Filters and Digit Manipulation

Configuring Translation Patterns and Route Filters
Understanding Digit Manipulation
Understanding Multisite Features
Lab 6-1: Configuring Complex Dial Plan Elements

Module 7: Class of Control

Defining Class of Control
Using Class of Control Features
Lab 7-1: Implementing Calling Privileges and Restrictions

Module 8: Understanding Media Resources

Defining Media Resources
Exploring Media Resource Management

Lab 8-1: Configuring Media Resources

Module 9: Describing CUCM Features

Understanding Basic Features
Exploring Hunt Groups
Describing Phone Services
Lab 9-1: Configuring User Features
Lab 9-2: Configuring Hunt Groups and Call Coverage
Lab 9-3: Configuring IP Phone Services

Course Description:

Integrating Cisco Unified Communications Applications (CAPPS) v8.0 teaches learners the integration options of Cisco Unified Presence, Cisco Unity Express, and Cisco Unity Connection. It describes voice messaging deployment scenarios, Cisco Unified Presence features, and troubleshooting mechanisms as well as Cisco Unified Presence and Cisco Unified Personal Communicator integration options with Cisco Unified Communications Manager.

Who Should Attend:

The primary students for this course are Network administrators and network engineers and CCNP Voice candidates. The secondary students for this course are Systems engineers.

Prerequisites:

Students should have working knowledge of converged voice and data networks, basic knowledge of Cisco IOS gateways, and working knowledge of Cisco Unified Communications Manager and Cisco Unity Connection.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe voice-mail integration options and requirements
- Implement Cisco Unity Connection in a Cisco Unified Communications Manager deployment
- Describe how to implement Cisco Unity Express in a Cisco Unified Communications Manager Express deployment
- Implement voice-mail networking using VPIM
- Implement Cisco Unified Presence and Cisco Unified Personal Communicator

Course Outline:**Module 1: Introduction to Voice Mail**

Voice-Mail Integration Overview
General Requirements for Voice-Mail Integration

Module 2: Cisco Unity Connection in a Cisco Unified Communications Manager Environment

Integrating with Cisco Unified Communications Manager
Configuring the Cisco Unity Connection System
Using Cisco Unity Connection Partitions and Search Spaces
Implementing Cisco Unity Connection Call Management
Configuring Cisco Unity Connection Users
Monitoring and Troubleshooting Cisco Unity Connection
Lab 2-1: Integrating Cisco Unity Connection with Cisco Unified Communications Manager
Lab 2-2: Configuring Cisco Unity Connection System Settings
Lab 2-3: Implementing Cisco Unity Connection Partitions and Search Spaces
Lab 2-4: Implementing Cisco Unity Connection Call Management
Lab 2-5: Configuring Cisco Unity Connection Users
Lab 2-6: Troubleshooting Cisco Unity Connection (Optional)

Module 3: Cisco Unity Express Implementation in Cisco Unified Communications Manager Express Environment

Understanding Cisco Unity Express
Integrating Cisco Unity Express with Cisco Unified Communications Manager Express
Configuring the Cisco Unity Express System
Configuring Cisco Unity Express Users
Understanding Cisco Unity Express AutoAttendant
Troubleshooting Cisco Unity Express
Lab 3-1: Integrating Cisco Unity Express with Cisco Unified Communications Manager Express
Lab 3-2: Configuring Cisco Unity Express System Settings
Lab 3-3: Configuring Cisco Unity Express Users
Lab 3-4: Implementing Cisco Unity Express AutoAttendant
Lab 3-5: Troubleshooting Cisco Unity Express (Optional)

Module 4: Voice Profile for Internet Mail Implementation

Understanding VPIM
Implementing VPIM in Cisco Unity Connection
Implementing VPIM in Cisco Unity Express
Lab 4-1: Implementing VPIM in Cisco Unity Connection and Cisco Unity Express

Module 5: Cisco Unified Presence Implementation

Understanding Cisco Unified Presence
Understanding Cisco Unified Presence Components and Communication Flows
Integrating Cisco Unified Presence
Configuring Cisco Unified Presence Features and Implementing Cisco Unified Personal Communicator
Verifying and Troubleshooting Tools for Cisco Unified Presence Components
Lab 5-1: Integrating Cisco Unified Presence with Cisco Unified Communications Manager
Lab 5-2: Configuring Cisco Unified Presence Features and Implementing Cisco Unified Personal Communicator
Lab 5-3: Troubleshooting and Verifying Cisco Unified Presence Components (Optional)

Course Description:

Troubleshooting Cisco Unified Communications (TVOICE) v8.0 prepares network professionals with the knowledge and skills that are required to troubleshoot Cisco Unified Communications systems and solutions in enterprise, midmarket, and commercial deployments in single-site and multisite environments. The course teaches troubleshooting methodology, triage, resources, tools, and fixes at the integrated system or solution level for Cisco Unified Communications Manager.

Who Should Attend:

The primary students for this course are Network administrators and network engineers and CCNP Voice candidates. The secondary students for this course are Systems engineers.

Prerequisites:

Students need to have working knowledge of converged voice and data networks, working knowledge of the MGCP, SIP, and H.323 and their implementation on Cisco IOS gateways, working knowledge of Cisco Unified Communications Manager, Cisco Unified Communications features and applications, and Cisco IOS voice gateways in single-site and multisite environments.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe a systematic methodology to troubleshoot Cisco Unified Communications solutions
- Isolate and troubleshoot reported issues that relate to Cisco Unified Communications Manager
- Diagnose a call setup issue and resolve the issues as you discover or reveal them, given a trouble call for which the source of the problem is unknown
- Solve the common issues of an SAF-enabled network and CCD
- Troubleshoot issues that are related to Cisco Unified Communications Manager features and applications
- Troubleshoot voice quality issues and issues that are related to media resources

Course Outline:**Module 1: Introduction to Troubleshooting Cisco Unified Communications Solutions**

Identifying Cisco Unified Communications Deployments
Using Troubleshooting Methodology
Using Troubleshooting and Monitoring Tools

Troubleshooting Issues with Conferences
Troubleshooting Transcoder Issues
Troubleshooting Issues with RSVP Agents
Troubleshooting Voice Quality Issues

Module 2: Cisco Unified Communications Manager Troubleshooting

Troubleshooting Common Gateway and Endpoint Registration Issues
Troubleshooting Cisco Unified Communications Manager Availability Issues
Troubleshooting Database Replication Issues
Troubleshooting LDAP Integration Issues
Lab 2-1: Integrating Cisco Unity Connection with Cisco Unified Communications Manager
Lab 2-2: Configuring Cisco Unity Connection System Settings
Lab 2-3: Implementing Cisco Unity Connection Partitions and Search Spaces
Lab 2-4: Implementing Cisco Unity Connection Call Management
Lab 2-5: Configuring Cisco Unity Connection Users
Lab 2-6: Troubleshooting Cisco Unity Connection (Optional)

Module 3: Troubleshooting Call Setup Issues

Examining Call Setup Issues and Causes
Troubleshooting On-Premises Single-Site Calling Issues
Troubleshooting On-Net Multisite Calling Issues
Troubleshooting Off-Net Calling Issues
Lab 3-1: Integrating Cisco Unity Express with Cisco Unified Communications Manager Express
Lab 3-2: Configuring Cisco Unity Express System Settings
Lab 3-3: Configuring Cisco Unity Express Users
Lab 3-4: Implementing Cisco Unity Express AutoAttendant
Lab 3-5: Troubleshooting Cisco Unity Express (Optional)

Module 4: SAF and CCD Issues

Troubleshooting SAF
Troubleshooting CCD
Lab 4-1: Implementing VPIM in Cisco Unity Connection and Cisco Unity Express

Module 5: Troubleshooting Cisco Unified Communications Manager Features and Application Issues

Troubleshooting Device Mobility Issues
Troubleshooting Cisco Extension Mobility Issues
Troubleshooting Cisco Unified Mobility Issues
Troubleshooting Cisco Unified Communications Manager Native Presence Issues
Lab 5-1: Integrating Cisco Unified Presence with Cisco Unified Communications Manager
Lab 5-2: Configuring Cisco Unified Presence Features and Implementing Cisco Unified Personal Communicator
Lab 5-3: Troubleshooting and Verifying Cisco Unified Presence Components (Optional)

Module 6: Voice Quality and Media Resources Issues

Troubleshooting MOH Issues
Troubleshooting MTP Issues

Course Description:

The Intelligent Contact Manager Boot Camp v7.0 (ICMBC) is an accelerated class combining the complete Cisco classes for Cisco Intelligent Contact Management Product Training Part 1(ICMPT1), and Cisco Intelligent Contact Management Product Training Part 2(ICMPT2). The classes are condensed by having longer days (8:00 AM to 6:00 PM) and reducing the overlap. This allows those students who attend only to be away from their work for one week instead of the two weeks for the normal ICMPT1, and ICMPT2, classes.

The two and a half day ICMPT1 portion covers an overview of the ICM, configuration, basic scripting, WebView reporting, as well as Pre-Routing, Post-Routing, and Translation Routing.

The two and a half day ICMPT2 portion provides the knowledge and experience necessary to install, set-up, support and troubleshoot the Cisco ICM system. Students will install and configure Cisco ICM software as it was used in ICMPT1. A pre-configured IPCC Express will be used for the second Contact Center and will be connected by the student installing an IPCC Express Gateway PG. Installation will also include a WebView Server, a Historical Data Server (HDS), and the optional products for Application Gateway and Database Routing. The Cisco Support Tools v2.0 is introduced and will be installed in class. Through the use of Support Tools Dashboard utility, and various monitoring and testing utilities, (the process Log files, command line reference) students will be able to identify, analyze, and diagnose various system alarms and events.

Who Should Attend:

This course is intense and fast paced and is intended for personnel who will implement, configure and support the Cisco ICM/IPCC Product.

System Engineers, Channel Partner/Resellers, Cisco Employees, Customers, Deployment Engineers, and other personnel wanting to meet the pre-requisite of completing the ICMPT1 course prior to attending the IP Contact Center Enterprise (IPCCE) v1.0 class will want to attend.

Prerequisites:

Students should have strong knowledge of MS Windows Server 2003 and TCP/IP networking and familiarity with your call center operations (ACD, Network, and any IVR implementations).

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Configure a generic ICM system using the Configure ICM utility (ICMPT1).
- Create several call routing and administrative scripts using the Script Editor utility.
- Generate real time and historical ICM reports using standard templates from the Webview utility.
- Describe ICM system components, their functions, and processes that run on the System Components.
- Install the needed third party software for proper WebView operation.
- Install the ICM System Software in a duplexed Enterprise environment.
- Use the Cisco Support Tools Dashboard utility and ICM tools for basic System Administration and Troubleshooting.
- Identify solution models and their issues.
- Build an ICM Enterprise (ICMPT2) solution.
- Install, configure, test, and maintain ICM components for the single-site environment.
- Formulate and implement ICM call flows and routing scripts.
- Troubleshoot the ICM solution set.

Course Outline:**ICMPT1 v7.0****Module 1: Call Routing Concepts**

Call Routing Options
ICM Components
ICM Call Routing

Module 2: Boston Contact Center

Configure Boston Contact Center
Script Editor

Module 3: Basic Administration

Additional Boston Configuration
Advanced Script Editor
Administration Labs

Module 4: Extended Functions

External Database Lookup
Call Variables
Multiple Skill Groups

Module 5: Administrative Scripts

Administrative Scripts

Module 6: Translation Routing

Translation Routing

Module 7: Virtual Contact Center

Adding A Contact Center

Enterprise Services and Skill Groups

Module 8: WebView

WebView

ICMPT2 v7.0**Module 1: ICM Topology**

ICM Deployment Models

Module 2: Processes

Functional Description
Fault Tolerance

Module 3: Classroom Lab Setup

Before you begin

Module 4: Central Controller

Domain Manager
Router
Logger

Module 5: Admin Workstation and Historical Data Server

Admin Workstation

Module 6: Device Management Protocol Devices

Network Interface Controller (NIC)

Peripheral Gateway (PG)

Module 7: Routing Options

External SQL Database
Application Gateway

Module 8: IPCC Express Gateway PG

IPCC Express Gateway PG
Module 9: Administration Tools
WebView Server
Support Tools

Course Description:

The new release Cisco IP Contact Center Enterprise v1.0 is based on updated Call Manager, IP IVR and ICM software. All labs have been rewritten and tested. New call flows have been created and are used as the basis to help students understand how to configure IP Contact Center and understand how it operates. The new course also includes coverage of CAD, the Cisco Agent Desktop, and expanded reporting.

Who Should Attend:

This course is intended for personnel who will implement, configure and support the Cisco IPCC Product and have already attended training on the ICM Product.

Prerequisites:

Students should have attended and completed ICMPT (ICM Product Training) and Call Manager courses and it is recommended that they have attended and completed CRSD.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Accurately explain the IPCC solution concept.
- Identify solution models and their issues.
- Build a "clean order" for an IPCC solution.
- Design an IPCC solution using all applicable components.
- Install, configure, test, and maintain IPCC components for the single-site environment.
- Formulate and implement IPCC call flows and routing.
- Use Cisco's standard IPCC deployment tools.
- Troubleshoot the IPCC solution set.

Course Outline:**Volume 1****Introduction****Overview**

Lesson 1: IPCC Pre Routing Call Flow
Lesson 2: IPCC Post Route from CallManager Call Flow
Lesson 3 and LAB Module 3: Configure CallManager for IPCC
Lesson 4: CRS Script Editor
Lesson 5 and LAB Module 5: Create a CRS Script
Lesson 6 and LAB Module 6: Configure IPIVR for IPCC
Lesson 7 and LAB Module 7: ICM Configuration
Lesson 8 and LAB Module 8: ICM Component Installation
Lesson 9 and LAB Module 9: CTIOS and CTIOS Desktop
Lesson 10 and LAB Module 10: Translation Route Wizard
Lesson 11 and LAB Module 11: ICM Script and Call Tracer

Volume 2

Lesson 1 and LAB Module 1: System IPCC Installation
Lesson 2 and LAB Module 2: Deployment Wizard
Lesson 3 and LAB Module 3: Post Installation Configuration
Lesson 4: Cisco Agent Desktop (CAD)
Lesson 5 and LAB Module 5: Cisco Desktop Applications Installation
Lesson 6 and LAB Module 6: System IPCC Script
Lesson 7 and LAB Module 7: CAD Workflow
Lesson 8: Cisco Outbound Option
Lesson 9 and LAB Module 9: Cisco Outbound Option Installation
Lesson 10 and Lab Module 10: Parent/Child

Course Description:

This course, Deploying Cisco Unified Contact Center Express (UCCXD) v4.0, provides the student with hands-on experience and knowledge of tasks typically performed during contact center deployment. This includes the deployment of Cisco Unified Contact Center Express (CCX) v8.0 and Cisco Unified IP Interactive Voice Response (IVR) as contact center solutions. Tasks include planning, installation and configuration, scripting, and troubleshooting.

Who Should Attend:

This course is for Cisco Unified Communications system channel partners and resellers, system engineers, and customers deploying and maintaining Cisco Unified Contact Center Express products.

Prerequisites:

Students should have experience with internetworking fundamentals, basic IP telephony concepts, Cisco Unified Communications Manager, Cisco IP Phones and Cisco IP Communicator, Contact Center Operations, Microsoft Windows Server 2000, 2003, XP, and MS SQL Server.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Design and plan a Cisco Unified CCX v8.0 and a Cisco Unified IP IVR implementation
- Install or discuss all Cisco Unified CCX v8.0 components, servers, and clients
- Configure all Cisco Unified CCX v8.0 components
- Build work flow applications to exploit Cisco Unified IP IVR features and capabilities
- Build contact center work flows to exploit Cisco Unified Contact Center Express v8.0 features and capabilities
- Deploy and use Cisco Agent and Supervisor Desktop software
- Deploy the Cisco Desktop Work Flow Administrator and set contact center options
- Use real-time and historical reporting
- Deploy the Outbound Preview Dialer
- Deploy Agent Email
- Deploy Automatic Speech Recognition and text-to-speech applications
- Discuss maintenance activities

Course Outline:**Module 1: Cisco Unified Contact Center Express v8.0 Product Overview**

Cisco Unified Contact Center Express v8.0 Product Packages
Cisco Unified Contact Center Express v8.0 Architecture
Cisco Unified Contact Center Express v8.0 Design and Order Tools

Student Pod Configuration
Teardown and Restoration

Module 2: Installing and Configuring Cisco Unified Contact Center Express v8.0

Installing Cisco Unified Contact Center Express v8.0
Cisco Unified Contact Center Express v8.0 Management
Call Process and Basic Cisco Unified Contact Center Express v8.0 Configuration

Module 3: Cisco Unified Contact Center Express v8.0 Scripting

Cisco Unified Contact Center Express v8.0 Script Editor
Creating a Basic IVR Script
Prompting and Collecting Information
Accessing an External Database
Loops, Counters, and Decision Making
Confirming Caller Input

Module 4: Cisco Unified Contact Center Express v8.0 ACD Operations

Cisco Unified Contact Center Express v8.0
Cisco Unified Contact Center Express v8.0 Scripting Fundamentals
Cisco Desktop Work Flow Administrator Fundamentals
Advanced Cisco Unified Contact Center Express v8.0 Scripting Topics
Cisco Unified Contact Center Express v8.0 Reporting

Module 5: Cisco Unified Contact Center Express v8.0 Premium Functions

Remote Monitoring
Outbound Preview Dialer
Agent Email
Automatic Speech Recognition and Text-to-Speech

Module 6: Cisco Unified Contact Center Express v8.0 Maintenance Tools

Real-Time Monitoring Tool
Cisco Unified Analysis Manager
Disaster Recovery System

Lab Outline

Overview
Lab Topology
Hardware and Software Requirements
Admin Server Installation and Configuration
Cisco Unified Communications Manager Server Installation and Configuration
ASR/TTS Server Setup
Cisco Unified Contact Center Express v8.0 Server Installation and Configuration

Course Description:

Cisco Unified Voice Portal Implementation (CVPI) 7.0 is a hands-on, instructor-led course that covers the tasks necessary for the operation, administration, maintenance and provisioning (Ops Console) of Unified CVP as it is installed in a comprehensive Intelligent Contact manager Enterprise (ICME) environment. Lab exercises address the configuration of all CVP 7.0 product components as well as external components including gateways, gatekeepers, Unified Communications Manager (formerly known as CallManager), ICM and CVP studio so as to properly interface with CVP. The course addresses CVP serviceability issues such as troubleshooting, redundancy, failover and remote monitoring. The purpose of the course is to enable a student to achieve working-level competency on CVP 7.0.

Who Should Attend:

This course is for individuals with telephony or data networking background who are familiar with the network infrastructure and IP communications components on which Cisco Unified CVP will be implemented.

Prerequisites:

Students must have taken the following classes or have equivalent experience: Interconnecting Cisco Network Devices (ICND1 and 2), Cisco IP Telephony Part I (CIPT1), Implementing Cisco Voice Gateways and Gatekeepers (GWGK), and Cisco Intelligent Contact manager Product Training (ICMPT 1, ICMPT 2). Students must also have experience with the following: Telephony experience – IP and Legacy, Contact Center experience, basic networking knowledge, Cisco IOS CLI familiarity, working knowledge of Cisco Unified Communications Manager, Gateway and Gatekeeper for H.323 Networks, and Microsoft Windows 2003 Server.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Explain the components, functions and call flow of a CVP solution when deployed in either a standalone or comprehensive model
- Group, summarize and complete the steps necessary to configure a functional Unified CVP comprehensive deployment model with Unified ICME
- Demonstrate use of 6 Unified ICME MicroApps available to support caller interaction with Unified CVP
- Demonstrate setup and configuration of Unified CVP components to support Automatic Speech Recognition (ASR) and Text To Speech (TTS)
- Configure Unified CVP Comprehensive solution to support subsequent transfer and queuing
- Associate VoiceXML as a technology and the benefits it provides to Unified CVP
- Install and configure the CVP VoiceXML Solution for Unified CVP
- Define and discuss security and reporting as it relates to a Unified CVP Solution

Course Outline:

Module 1: Cisco Unified CVP Technical Overview

Cisco Unified CVP Overview
 Components, Capabilities and Licensing
 Deployment Models and Call Flow
 Management and Reporting
 Labs 1-1 through 1-3: Familiarization with Cisco Unified CVP

Troubleshooting
 Lab 6-1: Troubleshooting Cisco Unified CVP

Module 2: Cisco Unified CVP Comprehensive

Cisco Unified CVP Comprehensive Overview
 Cisco Unified CVP Software Installation and Configuration
 Cisco IOS Voice Browser Configuration for Cisco Unified CVP
 Cisco Unified ICM Enterprise Configuration for Cisco Unified CVP
 Cisco Unified Communications Manager Configuration for Cisco Unified CVP
 Labs 2-1 and 2-2: Cisco Unified CVP Comprehensive Part 1
 Labs 2-3 and 2-4: Cisco Unified CVP Comprehensive Part 2

Module 3: Cisco Unified ICM Enterprise Scripting to Support Cisco Unified CVP

Scripting Overview
 Cisco Unified ICM Enterprise Scripting Micro-Applications
 Advanced Speech
 Advanced Cisco Unified ICM Enterprise Scripting Micro-Applications
 Subsequent Transfers and Queuing Calls
 Labs 3-1 through 3-4: Cisco Unified ICM Enterprise Scripting for Cisco Unified CVP

Module 4: Cisco Unified CVP VXML Solution

VoiceXML Overview
 VoiceXML Installation and Configuration
 Lab 4-1 through 4-3: VoiceXML Solution for Cisco Unified CVP

Module 5: Events, Log Files, and Reporting

Cisco Unified CVP Reporting
 Events and Log Files
 Lab 5-1: Reporting Database and Backup

Module 6: Failover, Diagnostics, and Troubleshooting

Failover and High Availability

Course Description:

Implementing Cisco Storage Networking Solutions (ICSNS) v4.2 is a five-day lecture and lab course using NX-OS v5.0.4, that provides learners with fundamental skills in implementing and troubleshooting Cisco storage networks.

Course topics include installing and bringing up the switch, configuring virtual SANs (VSANs), domains, interfaces, and zones, implementing port channels, configuring management security, and basic troubleshooting. Students will also learn how to configure highly available Fibre Channel over IP (FCIP) tunnels and tune the performance of your FCIP links.

Who Should Attend:

This course is for field and systems engineers.

Prerequisites:

Students must have a basic understanding of data storage hardware components and protocols, including SCSI and Fibre Channel and a basic understanding of network protocols, including Ethernet and IP. CCNA certification is recommended.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify the components, services, and features of the MDS 9000 platform that can be used to improve the availability, scalability, performance, and manageability of the SAN
- Describe how to safely install the switch hardware and perform the initial software configuration process
- Explain how to implement the logical topology that is specified by a SAN design, so that connectivity between end devices can be verified and traffic management features applied
- Describe how to use FCIP to implement appropriate solutions for SAN extension
- Use Cisco MDS 9000 Series Switch diagnostic tools to diagnose SAN problems and common configuration errors

Course Outline:**Module 1: Cisco MDS 9000 Platform**

Introducing the MDS 9000 Platform
System Architecture
Using Intelligent Fabric Services
Implementing Integrated Management

Module 2: System Installation and Initial Configuration

Installing Switch Hardware
Performing the Initial Switch Configuration
Installing and Licensing Cisco NX-OS Software
Configuring the Call Home Feature
Lab 2-1: Quick Start Switch Configuration
Lab 2-2: Upgrading Switch Software
Lab 2-3: Configuring Call Home

Module 3: Building Virtual SANs

Configuring VSANs
Managing Domains
Using Distributed Device Aliases
Configuring Interfaces
Configuring PortChannels
Configuring Fabric Services
Improving Management Security
Implementing Zones
Lab 3-1: Creating VSANs
Lab 3-2: Configuring Interfaces
Lab 3-3: Configuring PortChannels
Lab 3-4: Using Advanced Cisco Fabric Services
Lab 3-5: Configuring Zones

Module 4: Implementing FCIP

FCIP Protocol Overview
Configuring FCIP
Configuring FCIP High Availability
Implementing IVR for SAN Extension
Tuning FCIP Performance
Lab 4-1: Implementing an FCIP Tunnel
Lab 4-2: Configuring FCIP High Availability
Lab 4-3: Implementing IVR for SAN Extension
Lab 4-4: Tuning FCIP Performance

Module 5: Troubleshooting Tools and Scenarios

Using Diagnostic Tools and Methodologies
Capturing and Analyzing SAN Traffic
Troubleshooting SAN Configuration
Lab 5-1: Using SPAN and the Cisco Port Analyzer Adapter
Lab 5-2: Challenge Lab

Course Description:

Implementing Cisco Intrusion Prevention Systems (IPS) v6.0 provides the knowledge and skills needed to design, install, configure, and maintain a Cisco IPS sensor for small, medium, and enterprise networks. The course also describes the procedures for managing intrusion prevention system (IPS) alarms.

Who Should Attend:

The primary audience for this course are network designers and network security administrators.

Prerequisites:

Students must have familiarity with networking and security terms and concepts, including completion of the Securing Cisco Network Devices (SND) course. Students must also have strong user-level experience with Microsoft Windows operating systems.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Explain how the Cisco IPS protects network devices from attacks
- Install and configure the basic settings on a Cisco IPS 4200 Series Sensor
- Use the Cisco IDM to configure built-in signatures to meet the requirements of a given security policy
- Configure some of the more advanced features of the Cisco IPS product line
- Initialize and install into your environment the rest of the Cisco IPS family of products
- Use the CLI and the Cisco IDM to obtain system information, and configure the Cisco IPS sensor to allow an SNMP NMS to monitor the Cisco IPS sensor

Course Outline:**Course Introduction**

Overview
Course Goal and Objectives
Course Flow
Additional References
Your Training Curriculum

Module 1: Intrusion Prevention Overview

Explaining Intrusion Prevention
Examining Cisco IPS Products
Examining Cisco IPS Sensor Software Solutions
Examining Evasive Techniques

Module 2: Installation of a Cisco IPS 4200 Series Sensor

Installing a Cisco IPS Sensor Using the CLI
Using the Cisco IDM
Configuring Basic Sensor Settings
Lab 2-1: Install and Configure a Cisco IPS Sensor from the CLI
Lab 2-2: Use the Cisco IDM to Perform a Basic Sensor Configuration

Module 3: Cisco IPS Signatures

Configuring Cisco IPS Signatures and Alerts
Examining the Signature Engines
Customizing Signatures
Lab 3-1: Working with Signatures and Alerts
Lab 3-2: Customizing Signatures

Module 4: Advanced Cisco IPS Configuration

Performing Advanced Tuning of Cisco IPS Sensors
Monitoring and Managing Alarms
Configuring a Virtual Sensor
Configuring Advanced Features
Configuring Blocking
Lab 4-1: Tune a Cisco IPS Sensor Using the Cisco IDM
Lab 4-2: Monitor and Manage Alarms
Lab 4-3: Configure a Virtual Sensor (Optional)
Lab 4-4: Configure Anomaly Detection and POSFP

Module 5: Additional Cisco IPS Devices

Installing the Cisco Catalyst 6500 Series IDSM-2
Initializing the Cisco ASA AIP-SSM

Module 6: Cisco IPS Sensor Maintenance

Maintaining Cisco IPS Sensors
Managing Cisco IPS Sensors
Lab 6-1: Maintain Sensors and Verify System Configuration

Course Description:

The Cisco NAC Appliance is an easily deployed software NAC solution that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access your network. The Implementing Cisco NAC Appliance (CANAC) v2.1 course provides learners with the skills and knowledge needed to implement the Cisco NAC Appliance solution.

Who Should Attend:

This course is for those who need to learn how to implement the Cisco NAC Appliance solution.

Prerequisites:

Students should have the following: * Certification as a CCSP or the equivalent knowledge, * Basic knowledge of the Microsoft Windows operating system, * Familiarity with networking and security terminology and concepts, * Fundamental knowledge of implementing network security or CCSP or Cisco Security CSQ, * BCMSN or working knowledge of VLANs, * SNRS or working knowledge of digital certificates, and * BCSI or working knowledge of HSRP.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Given client network security requirements, explain how a Cisco NAC Appliance deployment scenario will meet or exceed network security requirements
- Configure the common elements of a Cisco NAC Appliance solution
- Configure the Cisco NAC Appliance in-band and out-of-band implementation options
- Implement a highly available Cisco NAC Appliance solution to mitigate network threats and facilitate network access for those users that meet corporate security requirements
- Maintain a highly available Cisco NAC Appliance deployment in medium and enterprise network environments

Course Outline:**Module 1: Cisco NAC Endpoint Security Solutions**

Introducing Cisco Self-Defending Networks

Introducing Cisco NAC Appliance

Introducing In-Band and Out-of-Band Deployment Options

Lab 1-1: Preparing the Cisco NAM to Support Web-Based Administration Console Configuration

Module 2: Cisco NAC Appliance Common Elements Configuration

Configuring User Roles

Configuring External Authentication

Configuring DHCP on the Cisco NAS

Lab 2-1: Configuring User Roles

Module 3: Cisco NAC Appliance Implementation

Implementing Cisco NAC Appliance In-Band Deployment

Implementing the Microsoft Windows SSO Feature on the Cisco NAC Appliance

Implementing the Cisco VPN SSO Feature on the Cisco NAC Appliance

Implementing Cisco NAC Appliance Out-of-Band Deployment

Managing Switches

Lab 3-1: Adding an In-Band Virtual Gateway Cisco NAS to the Cisco NAM

Lab 3-2: Configuring the Microsoft Windows Active Directory SSO Feature on the Cisco NAC Appliance

Lab 3-3: Configuring the Cisco VPN SSO Feature on the Cisco NAC Appliance

Lab 3-4: Adding an Out-of-Band Virtual Gateway Cisco NAS to an HA Cisco NAC Appliance Deployment

Lab 3-5: Configuring SNMP, Switch, and Port Profiles for an Out-of-Band Cisco NAC Appliance Deployment

Module 4: Cisco NAC Appliance Implementation Options

Implementing Cisco NAC Appliance on a Network

Implementing Network Scanning

Configuring the Cisco NAM to Implement the Cisco NAA on User Devices

Configuring Cisco NAM High Availability

Configuring Cisco NAS High Availability

Lab 4-1: Configuring Cisco NAA

Lab 4-2: Configuring a High Availability In-Band VPN Cisco NAC Appliance Solution

Module 5: Cisco NAC Appliance Monitoring and Administration

Monitoring a Cisco NAC Appliance Deployment

Administering the Cisco NAM

Course Description:

The Cisco Security Monitoring Analysis and Response System (CS-MARS) is part of the Cisco Security Management Suite which provides security monitoring for network security devices and host application made by Cisco or non-Cisco providers. In addition to event correlation and data reduction features found in SIM products, CS-MARS also provides topology awareness and automatic mitigation features. In knowing the topology of a network, CS-MARS can determine where the attack is originating and apply the appropriate remediation. CS-MARS is a key component in the Cisco Self Defending Network strategy. CS-MARS exchanges information with CS-Manager to provide a unified security management solution. For example, an administrator can view IPS signatures or the Firewall block / permit syslog messages received from sensors or firewalls. CS-MARS will communicate with CS-Manager and display the IPS signature table or firewall rule table. From there the IPS signature or firewall rule can be modified as necessary. Together CS-MARS and CS-Manager provide a unified management solution for monitoring and provisioning.

Who Should Attend:

This course is for engineers who support sales of Cisco security product solutions, Cisco channel partners who sell, implement, and maintain secure networks, and Cisco customers who implement and maintain secure networks.

Prerequisites:

Students must be Cisco CCSP certified or have equivalent knowledge. They must also have passed the Securing Cisco IOS Networks (SECUR) exam (642-501), the Securing Networks with Cisco Routers and Switches (SNRS) exam (642-502), or both and have at least six months of practical experience configuring Cisco routers and security products. In addition, students must be familiar with implementing network security policies and networking components and concepts.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Use CS-MARS to monitor security and host application devices.
- Know CS-MARS architecture and how CS-MARS process events.
- Know how to use archive and restore features.
- Use CS-MARS to run / create / customize reports
- Use CS-MARS to investigate an incident and mitigate the security threats.
- Use CS-MARS to do customer parser for unknown devices in CS-MARS.
- Use CS-MARS to create / customize rules that detects dark net through best practices example.
- Know how to tune signature / log level on device side and CS-MARS side.

Course Outline:

Introducing Cisco Security Monitoring, Analysis, and Response System

Effective Security Monitoring and Management
Cisco Self-Defending Network and the Role of Cisco Security MARS
Cisco Security MARS
Cisco Security MARS Terminology
Cisco Security MARS Technologies
Cisco Security MARS User Interface
Cisco Security MARS Product Portfolio
Pre-Lab Activity: Accessing the Remote Lab

Understanding the System Architecture

Cisco Security MARS Software Components
Cisco Security MARS Process Flow Details

Configuring a Cisco Security MARS Appliance

Initial Cisco Configuration Overview
Scenario: Configuration Tasks
Deployment Planning Guidelines
Lab 3: Accessing the Cisco Security MARS Appliance

Adding Reporting and Mitigation Devices

Overview of Reporting and Mitigation Devices
Scenario: Adding a Cisco Reporting Device and Enabling NetFlow
Data-Enabling Features of Cisco Security MARS
Integrating Cisco Security MARS with Third-Party Applications
Lab 4-1: Adding Reporting Devices and Enabling NetFlow
Lab 4-2: Configuring the Syslog Forwarding Feature

Viewing the Summary Page

Summary Page Overview
Dashboard
Network Status
My Reports
Scenario: Getting Information from the Summary Page
Lab 5: Generating Summary Reports

Managing Rules

Rules Overview
Working with System and User Inspection Rules
Working with Drop Rules
Rule Groups Overview
Lab 6-1: Configuring Cisco Security MARS Event Types
Lab 6-2: Configuring an Inspection Rule

Understanding Queries and Reports

Query Page
Scenario: Configuring a Query
Reports Page
Scenario: Configuring a System Report
Lab 7: Performing a Query and Creating a Custom Report

Investigating and Mitigating Incidents

Incidents Overview
Incidents
Scenario: Role of Cisco Security MARS in Your Network
False Positives
Case Management
Scenario: Configuring a Case to Track an Incident
Configuring Notifications
Case Study: Preventing the W32 Blaster Worm
Lab 8: Performing Incident Investigation and Mitigation

Working with User-Defined Log Parser Templates

Overview of User-Defined Log Parser Templates
Scenario: Configuring a Customer Parser
Lab 9: Configuring the Custom Parser

Integrating with Cisco Security Manager

Overview of Cisco Security Manager Policy Table Lookup
Scenario: Invoking Cisco Security Manager Policy Table Lookup from Cisco Security MARS

Managing and Administering the System

Lab 10: Performing Cisco Security Manager Policy Lookup

Management Overview
Overview of System Maintenance Tasks
IPS Signature Dynamic Update Settings
Upgrading the Cisco Security MARS Appliance Software
Migrating Data from Cisco Security MARS 4.3.x to 5.3.x
Lab 11-1: Reviewing the CLI and Upgrading the Device Version
Lab 11-2: Configuring IPS Auto Signature Download
Lab 11-3: Configuring AAA RADIUS Authentication and Working with the Account Locking and Session Timeout Menu
Lab 11-4: Retrieving Raw Messages

Troubleshooting and Optimizing Cisco Security MARS

Hardware Installation Issues
Device Configuration Issues
Global Controller-to-Local Controller Communications
Sizing Cisco Security MARS Deployment
Tuning Cisco Security MARS
Securing Cisco Security MARS

Using the Cisco Security MARS Global Controller

Cisco Security MARS Global Controller Overview
Configuring the Cisco Security MARS Global Controller
Summary Tab
Incidents Tab
Queries and Reports
Rules Tab
Management Tab
System Maintenance Tab

Course Review: Cisco Security MARS at Work

Cisco Security MARS At Work
Lab Outline

Course Description:

Implementing Cisco IOS Network Security (IINS) v1.0 is a five-day instructor-led course focused on the necessity of a comprehensive security policy and how it affects the posture of the network. Learners will be able to perform basic tasks to secure a small branch type office network using Cisco IOS security features available through web-based GUIs (Cisco Router and Security Device Manager [SDM]) and the command-line interface (CLI) on the Cisco routers and switches. Implementing Cisco IOS Network Security (IINS) v1.0, in conjunction with its prerequisite, Interconnecting Cisco Networking Devices, Part 1 (ICND1) v1.0, will form the recommended training component for this new associate level certification, CCNA Security. IINS v1.0 provides students with the knowledge and skills necessary to achieve competency in Cisco security solutions.

Who Should Attend:

This course is for employees, channel partners/resellers, and customers.

Prerequisites:

Students must have the skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1). Completion of ICND2 or CCNAX is recommended.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Develop a comprehensive network security policy to counter threats against information security.
- Configure routers on the network perimeter with Cisco IOS Software security features.
- Configure a Cisco IOS zone-based firewall to perform basic security operations on a network.
- Configure site-to-site VPNs using Cisco IOS features.
- Configure IPS on Cisco network routers.
- Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic.

Course Outline:**Module 1: Introduction to Network Security Principles**

Network Security Fundamentals
Attack Methodologies
Operations Security
Cisco Self-Defending Networks
Lab 1-1: Embedding a Secret Message Using Steganography
Lab 1-2: Scanning a Computer System Using Testing Tools
Lab 1-3: Scanning a Network Using Testing Tools

Voice Security
Layer 2 Attacks
Lab 6-1: Using Cisco Catalyst Switch Security Features

Module 2: Perimeter Security

Administrative Access to Cisco Routers
Cisco SDM
AAA on a Cisco Router Using the Local Database and on Secure ACS
Secure Management/Reporting
Locking Down the Router
Lab 2-1: Securing Administration Access to Cisco Routers
Lab 2-2: Configuring AAA on Cisco Routers to Use the Local Database
Lab 2-3: Configuring AAA on Cisco Routers to Use Cisco Secure ACS
Lab 2-4: Implementing Secure Management and Reporting
Lab 2-5: Using Cisco SDM One-Step Lockdown and Security Audit

Module 3: Network Security Using Cisco IOS Firewalls

Firewall Technologies
Static Packet Filters Using ACLs
Cisco IOS Zone-Based Policy Firewall
Lab 3-1: Creating Static Packet Filters Using ACLs
Lab 3-2: Configuring a Cisco IOS Zone-Based Policy Firewall

Module 4: Site-to-Site VPNs

Cryptographic Services
Symmetric Encryption
Examining Cryptographic Hashes and Digital Signatures
Asymmetric Encryption and PKI
IPsec Fundamentals
Site-to-Site IPsec VPN
IPsec on a Site-to-Site VPN Using Cisco SDM
Lab 4-1: Configuring a Site-to-Site IPsec VPN

Module 5: Network Security Using Cisco IOS IPS

IPS Technologies
Cisco IOS IPS Using Cisco SDM
Lab 5-1: Configuring Cisco IOS IPS

Module 6: LAN, SAN, Voice, and Endpoint Security Overview

Endpoint Security
SAN Security

Course Description:

The Deploying Cisco ASA Firewall Solutions (FIREWALL) v2.0 course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP® Security) certification. It is a five-day instructor-led course that is aimed at providing network security engineers with the knowledge and skills that are needed to implement and maintain perimeter solutions that are based on Cisco ASA v8.4(1) security appliances. At the end of the course, students will be able to reduce risk to their IT infrastructure and applications using Cisco ASA v8.4(1) security appliance features, and provide detailed operations support for the Cisco ASA v8.4(1) security appliance.

Who Should Attend:

The primary students for this course are Network Security Engineers (NSEs).

Prerequisites:

Students must have Cisco Certified Network Associate (CCNA) certification, Cisco Certified Network Associate Security (CCNA Security) certification, and working knowledge of the Microsoft Windows operating system.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Evaluate the basic firewall technology, features, hardware models, and licensing options of the Cisco ASA security appliance
- Implement and troubleshoot basic Cisco ASA security appliance connectivity and device management plane features
- Configure and verify Cisco ASA security appliance network integration
- Configure and verify Cisco ASA security appliance policy
- Configure and verify high availability and virtualization on Cisco ASA security appliances

Course Outline:**Cisco ASA Adaptive Security Appliance Essentials**

Evaluating Cisco ASA Adaptive Security Appliance Technologies
Identifying Cisco ASA Adaptive Security Appliance Families
Identifying Cisco ASA Adaptive Security Appliance Licensing Options

Basic Connectivity and Device Management

Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
Configuring Cisco ASA Adaptive Security Appliance Device Management Features
Lab 2-1: Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
Lab 2-2: Configuring the Cisco ASA Adaptive Security Appliance for Secure Network Integration
Lab 2-3: Configuring Management Features

Network Integration

Configuring Cisco ASA Adaptive Security Appliance NAT Features
Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features
Configuring Cisco ASA Adaptive Security Appliance Routing Features
Configuring the Cisco ASA Adaptive Security Appliance Transparent Firewall
Lab 3-1: Configuring NAT
Lab 3-2: Configuring Basic Cisco Access Control Features
Lab 3-3: Configuring Transparent Firewall (Optional)

Cisco ASA Adaptive Security Appliance Policy Control

Defining the Cisco ASA Adaptive Security Appliance MPF
Configuring Cisco ASA Adaptive Security Appliance Connection Policy and QoS Settings
Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections
Configuring Cisco ASA Adaptive Security Appliance User-Based Policies
Lab 4-1: Configuring MPF, Basic Stateful Inspections, and QoS
Lab 4-2: Configuring MPF Advanced Application Inspections
Lab 4-3: Configuring Cut-Through Proxy

Cisco ASA Adaptive Security Appliance High Availability and Virtualization

Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features
Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability
Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance
Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability
Lab 5-1: Configuring Active/Standby High Availability
Lab 5-2: Configuring Active/Active High Availability

Course Description:

The Securing Networks with Cisco Routers and Switches (SECURE) 1.0 course is an instructor-led course presented by Cisco training partners to their end-user customers. This five-day course aims at providing network security engineers with the knowledge and skills needed to secure Cisco IOS Software router- and switch-based networks, and provide security services based on Cisco IOS Software. Successful graduates will be able to secure the network environment using existing Cisco IOS Software features, and install and configure components of Cisco IOS Software. Components include the Zone-Based Policy Firewall, Cisco IOS Intrusion Prevention System (IPS), user-based firewall, and secure tunnels using IP Security (IPsec) virtual private network (VPN) technology including public key infrastructure (PKI). Components also include virtual tunnel interface/dynamic virtual tunnel interface (VTI/DVTI), Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint Virtual Private Network (DMVPN), Secure Sockets Layer (SSL) VPN, and advanced switch security features. The course focuses on the implementation and troubleshooting aspects of the lifecycle services approach, adding some elements of the design phase as well.

Who Should Attend:

The primary students for this course are Network Security Engineers (NSEs).

Prerequisites:

Students must have Cisco Certified Network Associate (CCNA) certification, Cisco Certified Network Associate Security (CCNA Security) certification, and working knowledge of the Microsoft Windows operating system.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Implement and maintain Cisco IOS Software infrastructure protection controls in a Cisco router- and switch-based network infrastructure
- Implement and maintain Cisco IOS Software threat control and containment technologies in a Cisco router-based perimeter infrastructure
- Implement and maintain Cisco IOS Software VPN technologies in a Cisco router-based WAN
- Implement and maintain Cisco IOS Software remote access VPN technologies in a Cisco router-based remote access solution

Course Outline:**Module 1: Deploying Cisco IOS Software Network Foundation Protection**

Deploying Network Foundation Protection Controls
Deploying Advanced Switched Data Plane Security Controls
Implementing Cisco Identity-Based Network Services
Deploying Basic 802.1X Features
Deploying Advanced Routed Data Plane Security Controls
Deploying Advanced Control Plane Security Controls
Deploying Advanced Management Plane Security Controls
Lab 1-1: Configuring Advanced Switched Data Plane Security Controls
Lab 1-2: Configuring Advanced Infrastructure Security Controls

Module 2: Deploying Cisco IOS Software Threat Control and Containment

Deploying Cisco IOS Software Network Address Translation
Deploying Basic Zone-Based Policy Firewalls
Deploying Advanced Zone-Based Policy Firewalls
Deploying Cisco IOS Software IPS
Lab 2-1: Configuring Basic Zone-Based Policy Firewall Features
Lab 2-2: Configuring Advanced Zone-Based Policy Firewall Features
Lab 2-3: Configuring Cisco IOS Software IPS

Module 3: Deploying Cisco IOS Software Site-to-Site Transmission Security

Site-to-Site VPN Architectures and Technologies
Deploying VTI-Based Site-to-Site IPsec VPNs
Deploying Scalable Authentication in Site-to-Site IPsec VPNs
Deploying DMVPNs
Deploying High Availability in Tunnel-Based IPsec VPNs
Deploying GET VPN
Lab 3-1: Configuring a PKI-Enabled Site-to-Site IPsec VPN
Lab 3-2: Configuring Cisco IOS Software DMVPN Spokes
Lab 3-3: Configuring GET VPN Group Members

Module 4: Deploying Secure Remote Access with Cisco IOS Software

Remote Access VPN Architectures and Technologies
Deploying Remote Access Solutions Using SSL VPN
Deploying Remote Access Solutions Using Cisco Easy VPN
Lab 4-1: Configuring a Cisco IOS Software SSL VPN Gateway
Lab 4-2: Configuring Cisco Easy VPN

Course Description:

The Deploying Cisco ASA VPN Solutions (VPN) 1.0 course is an instructor-led course that is presented by Cisco Learning Partners to their end-user customers. This five-day course aims at choosing, configuring, and troubleshooting the majority of Cisco ASA adaptive security appliance remote access and site-to-site VPN features to reduce risk to IT infrastructure and its applications.

Who Should Attend:

The primary students for this course are Network security engineers.

Prerequisites:

The knowledge and skills that a learner must have before attending this course include Cisco CCNA® certification, Cisco CCNA Security certification, familiarity with networking and security terms and concepts, and working knowledge of the Microsoft Windows operating system.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Evaluate the Cisco ASA adaptive security appliance VPN subsystem
- Deploy Cisco ASA adaptive security appliance IPsec VPN solutions
- Deploy Cisco ASA adaptive security appliance Cisco AnyConnect remote access VPN solutions
- Deploy Cisco ASA adaptive security appliance clientless remote access VPN solutions
- Deploy advanced Cisco ASA adaptive security appliance VPN solutions

Course Outline:**Module 1: Evaluation of the Cisco ASA Adaptive Security Appliance VPN Subsystem**

Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture
Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture
Applying Common Cisco ASA Adaptive Security Appliance Remote Access VPN Configuration Concepts

Module 2: Deployment of Cisco ASA Adaptive Security Appliance IPsec VPN Solutions

Deploying Basic Site-to-Site IPsec VPNs
Deploying Certificate Authentication in Site-to-Site IPsec VPNs
Deploying the Cisco VPN Client
Deploying Basic Cisco Easy VPN Solutions
Deploying Advanced Authentication in Cisco Easy VPN Solutions
Deploying the Cisco ASA 5505 Adaptive Security Appliance as Cisco Easy VPN Remote
Lab 2-1: Deploying a Basic Cisco ASA Adaptive Security Appliance IPsec Site-to-Site VPN
Lab 2-2: Deploying a Certificate-Based Cisco ASA Adaptive Security Appliance IPsec Site-to-Site VPN
Lab 2-3: Deploying Basic Cisco Easy VPN
Lab 2-4: Deploying Advanced Cisco Easy VPN Server with Certificate-Based Authentication
Lab 2-5: Deploying the Cisco ASA 5505 Adaptive Security Appliance as a Cisco Easy VPN Remote

Module 3: Deployment of Cisco ASA Adaptive Security Appliance Cisco AnyConnect Remote Access VPN Solutions

Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution
Deploying Advanced Cisco AnyConnect VPN Client
Deploying Advanced Authentication in Cisco AnyConnect Full Tunnel SSL VPNs
Lab 3-1: Configuring a Basic Cisco AnyConnect Full Tunnel SSL VPN Using Local Password Authentication
Lab 3-2: Deploying the Cisco AnyConnect Client with Centralized Management
Lab 3-3: Configuring a Basic Cisco AnyConnect Full Tunnel SSL VPN Using the Local CA

Module 4: Deployment of Cisco ASA Adaptive Security Appliance Clientless Remote Access VPN Solutions

Deploying a Basic Clientless VPN Solution
Deploying Advanced Application Access for Clientless SSL VPN
Deploying Advanced Authentication and SSO in a Clientless SSL VPN
Customizing the Clientless SSL VPN User Interface and Portal
Lab 4-1: Configuring Basic Clientless VPN Access on the Cisco ASA Adaptive Security Appliance
Lab 4-2: Configuring Advanced Application Access in Clientless SSL VPNs
Lab 4-3: Customizing the SSL VPN Portal on the Cisco ASA Adaptive Security Appliance

Module 5: Deployment of Advanced Cisco ASA Adaptive Security Appliance VPN Solutions

Deploying VPN Authorization, Access Control, and Accounting
Deploying Cisco Secure Desktop in SSL VPNs
Deploying Dynamic Access Policies
Deploying High Availability and High Performance in SSL and IPsec VPNs
Lab 5-1: Deploying SSL VPN Access Policies and Authorization Parameters
Lab 5-2: Deploying Cisco Secure Desktop and DAP in SSL VPNs
Lab 5-3: Configuring a Load-Balancing SSL VPN Cluster