DNAIE (CISCO DIGITAL NETWORK ARCHITECTURE IMPLEMENTATION ESSENTIALS) 2.0

Objetivo

After completing this course, you should be able to: â¢ Identify the Cisco DNA solution by describing its vision, strategy, general concepts, and components; â¢ Implement network automation using Cisco APIC-EM and built-in applications such as Network Plug and Play, Easy QoS, IWAN, and Path Trace; â¢ Implement network virtualization using Cisco Enterprise NFV in enterprise branch networks; â¢ Implement network analytics using Cisco CMX Cloud; â¢ Implement network security using Cisco Stealthwatch, Cisco TrustSec, and Cisco Identity Services Engine (ISE).

PÃºblico Alvo

Experienced network engineers, especially those who work for enterprise organizations using Cisco Digital Network Solutions.

PrÃ©-Requisitos

We recommend but do not require the following skills and knowledge before attending this course: â¢ Foundational understanding of network design, routing, switching, QoS, and security; â¢ Understanding of Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), Dynamic Host Configuration Protocol (DHCP), DNS, Network Time Protocol (NTP), and Simple Network Management Protocol (SNMP); â¢ Understanding of TCP protocols such as HTTP, HTTPS, and Telnet; â¢ Understanding of routing concepts and the ability to configure routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF); â¢ Understanding of enterprise WAN and Dynamic Multipoint VPN (DMVPN); â¢ Understanding of firewall operation (especially transparent mode); â¢ Basic understanding of Cisco PrimeÂ® Infrastructure, KVM virtualization, and programming concepts; â¢ Basic understanding of SDN, northbound APIs, southbound APIs, and representational state transfer (REST) APIs; â¢ Understanding of WLAN parameters; â¢ Basic understanding of wireless controllers (WLCs) and access point capabilities in WLCs; â¢ Understanding of Power over Ethernet (PoE) in Cisco switches.

Carga HorÃ¡ria

40 horas (5 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
Course Outline
Course Goals & Objectives

Identifying the Cisco Digital Network Architecture Vision
Describe the Cisco Digital Network Architecture vision
Identify new network priorities and requirements
Describe the Cisco DNA strategy

Identifying Cisco Digital Network Architecture Solution Components
Describe the solution components of Cisco DNA
Cisco DNA Overview
Describe Cisco DNA
Describe the network virtualization component in Cisco DNA
Describe the network automation component in Cisco DNA
Describe the network analytics component in Cisco DNA
Describe the network cloud services component in Cisco DNA
Describe the custom network programmability component in Cisco DNA

Identifying the Role of Automation and Orchestration Controllers in Cisco DNA
Identify and describe the role of automation and orchestration controllers in Cisco DNA
Describe the role of the automation controller in Cisco DNA
Automation Controller Overview
Explain automation controllers in Cisco DNA and the role of Cisco ESA in Cisco Enterprise NFV

Implementing Automation in Enterprise Networks
Describe the essentials of Cisco APIC-EM for enterprise networks
Describe the need for automation in enterprise networks
Describe the Cisco APIC-EM controller
Describe the high-level Cisco APIC-EM controller architecture
Describe the system requirements and installation of Cisco APIC-EM
Practical Use: Navigate Cisco APIC-EM GUI: Network, Device, and Topology Discovery Using
Describe how Cisco APIC-EM builds the network information database and topology

Implementing the Cisco Network Plug and Play Solution
Implement day-zero automation in enterprise networks using Cisco APIC-EM (DNA controller)
Customer Challenge with Network and Device Deployment
Describe the challenges in enterprise networks in device onboarding and deployment
Describe the Cisco Network PnP solution and its components
Describe the discovery options for Cisco PnP
Describe the workflow for configuration/mage upload using PnP application on Cisco APIC-EM
Describe the provisioning of unclaimed devices using the Cisco APIC-EM PnP application
Describe bulk import and export using the Cisco APIC-EM PnP application
Practical Use: Implement the Cisco Network Plug and Play Solution Using Cisco APIC-EM
Describe the provisioning of new devices, using the PnP application on Cisco APIC-EM
Describe the mobile application in the Cisco PnP solution
Describe the secure connectivity that is used by the Cisco Network PnP application on Cisco

Implementing the Cisco EasyQoS Solution
Implement the Cisco EasyQoS solution
Describe the customer challenges with QoS deployment in enterprise networks

Describe the Cisco EasyQoS solution and its business value
Describe the Cisco QoS baseline, and briefly
Describe the QoS classification, marking, and shaping tools
Describe the Cisco EasyQoS workflow on Cisco APIC-EM
Describe the components of Cisco EasyQoS and their functions
Practical Use: Implement Cisco EasyQoS Using the Cisco APIC-EM GUI
Implement the Cisco EasyQoS application on the APIC-EM GUI
Describe the need for dynamic QoS, and explain the dynamic EasyQoS workflow

Implementing Cisco Intelligent WAN Solution
Describe the implementation of the Cisco IWAN solution using the application on Cisco
Need for the Cisco Intelligent WAN Application
Describe customer challenges related to WAN deployment
Describe how the Internet can be extension of enterprise WAN using Cisco IWAN
Describe briefly the Cisco IWAN solution
Describe the Cisco IWAN deployment models
Describe the Cisco IWAN design and technology using Cisco Validated Designs
Describe the Cisco IWAN application features and benefits
Practical Use: Perform Site Provisioning and Monitoring Using the Cisco IWAN Application
Perform hub site provisioning using Cisco IWAN on APIC-EM

Troubleshooting Using Path Trace Application
Describe the use of the Path Trace application on Cisco APIC-EM
Describe the need for Path Trace application for troubleshooting
Describe the Cisco APIC-EM Path Trace application workflow
Practical Use: Troubleshoot Using the Cisco APIC-EM Path Trace Application
Implement the traffic path analysis using the Path Trace application

Implementing Cisco Enterprise Network Functions Virtualization
Describe Cisco Enterprise NFV architecture and solution components
Identify its role in Cisco DNA architecture
Implement the Cisco Enterprise NFV solution
Describe the current enterprise network challenges, and discuss the Cisco Enterprise NFV approach as a solution
Explain where and how Cisco Enterprise NFV fits in the Cisco DNA architecture
Describe the building blocks of Cisco Enterprise NFV
Expand the description of building blocks of ENFV, includes description of each components - OAM, VNF, NFVIS and Hardware platforms.
Cisco 5400 Series ENCS Deep Dive
Explain Cisco ENCS hardware details, chassis options, internal networking, and server management
Describe day-zero services orchestration with the Cisco Enterprise NFV OAM system
Describe the virtualization layer and local management of NFVIS and life-cycle management of VNFs
Describe the OAM system Cisco ESA workflow
Practical Use: Perform Site Provisioning with NFVIS on Cisco UCS C220 Using OAM Servers
Students perform site provisioning with NFVIS and UCS-C using OAM servers (APIC-EM, ESA & PI)
Describe the Cisco Enterprise NFV deployment options
Describe Cisco ENCS single WAN IP deployment scenarios

Implementing Network Programmability in a DNA Architecture

Identify and use basic programmability features to facilitate information gathering and automation
Programmability Overview
Explain the benefits of network programmability as related to Cisco DNA architecture, focusing on the concepts of automation
Use of Network Automation
Network Automation Scenarios
Automation Tools
Describe some of the automation tools, focusing on Ansible
Explain the various components—including inventory, playbooks, plays, tasks, modules, and variables
Describe the primary attributes and requirements of next-generation programmatic interfaces
Describe the various programming interfaces and data models, including scripting programming,
model-based interfaces, and application hosting
Explain the YANG data model structure, including an explanation of how to create custom YANG models, and a discuss the various node types for data modeling
Define NETCONF, and provide a detailed explanation of the mechanisms for installing, manipulating, or deleting the configuration of network devices, including an overview of the NETCONF communications flow
Identify and define analytics, describe how network analytics enables new insights and outcomes in Cisco DNA networks, and describe network analytics as a Cisco DNA tenant
Define network analytics in the Cisco DNA network
New Insights and Outcomes with Network Analytics
Describe how analytics provides better insights in how the network is used, which results in making better business decisions
Describe the three priorities that Cisco DNA addresses in networks (insights and actions, automation and assurance, and security and compliance)

Cisco DNA Analytics Architecture
Describe various data sources, the instrumentation, telemetry, and Cisco DNA Analytics architecture today
Describe the sources of data in a Cisco DNA network
Describe the issues in data analytics collection in the network
Describe the types of data and protocols that make up telemetry in the network
Describe the Cisco DNA Analytics architecture as it is today, the different use cases, the typical
analytics solution, and the areas of major interest

DNA Analytics Proof Points
Describe how the network can operate as a sensor and an enforcer.
Provide analytics data about the health of the network devices, applications, and clients, and how analytics can be provided as a cloud service.
Describe how the network can be used as a sensor to detect potential security attacks across
hundreds of devices across the network, and monitor infected devices to uncover other malicious entities from the compromised devices.
Describe how the network can function as an enforcer for network policies.
Describe the scope of network health in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: Site
Describe how network health is viewed at the site level in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: Floor
Describe how network health is viewed at the floor level in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: APs on a Floor
Describe how network health is viewed at the AP level in a DNA network.

Cisco Prime Infrastructure 3.1—Network Health: AP Details
Describe how detailed network health is viewed at the AP level.
Cisco Prime Infrastructure 3.1—Network Health: Services
Describe how network health of services such as IP voice are viewed in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: Site View
Describe the types of data that Prime Assurance provides at the site level in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: Device View
Describe the types of data that Prime Assurance provides at the device level in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: AP View
Describe the types of data that Prime Assurance provides at the client view level in a DNA network.
Cisco Prime Infrastructure 3.1—Network Health: Client View
Describe the types of data that Prime Assurance provides at the client view level in a DNA network.
Describe the benefits of moving analytics to the cloud.
Describe the benefits Cisco Connected Analytics for network deployment.
Describe how Cisco Connected Analytics for network deployment is Software as a Service (SAAS) that increase consistency and reduce disruptions in network operations.
Describe how Cisco CMX Cloud provides additional customer insights and points of engagement.
Describe how CMX on premise differs from the Cisco CMX Cloud in presence analytics, and presence analytics can provide additional insight to how your network is used by your customers.
Describe how presence analytics can be used to understand mobile device patterns in your network.

Cisco Network Data Platform Architecture
Describe the Cisco DNA Analytics architecture today and the migration to the network data platform analytics engine.
Explain how data visualization, comparison, remediation, strategic policy analysis, and strategic policy suggestions enhance network operations. Describe the evolution of the Cisco DNA Analytics architecture.
Describe the DNA Analytics architecture in networks today and the challenges that are posed by multiple collectors using multiple data formats and protocols
Describe how Cisco NDP functions and reduces the complexity in the collection and analysis of network data
Describe how network visualization assists in identifying network trends from multiple data streams
Describe how comparing current network data to the same day and time a week, month, or a year ago provides a view of network performance
Describe how Cisco NDP sends requests to Cisco APIC-EM to remediate identified network issues
Describe how the assurance and remedy application can analyze configured performance versus the actual performance
Cisco DNA Analytics Architecture—Assurance and Remedy Application: Strategic Policy Recommendations
Describe the differences between the current analytics collection process and a network using Cisco NDP for analytics collection

Cisco CMX On Premises
Describe how Cisco Connected Mobile Experiences (CMX) provides new insights and ways to innovate through the network
Describe how Cisco CMX can provide insights into network use that can be used for business relevant decisions.
Describe the different levels of accuracy that locations can provide, and describe where and by which devices data for locations is measured. Describe the best-practice guidelines for location-based services.
Describe the accuracy of location with FastLocate, and how location is calculated with FastLocate.
Describe how Cisco Hyperlocation improves location accuracy, and explain the elements that Hyperlocation uses

for location calculation and how Hyperlocation can be used in a Wi-Fi network.
Describe the Hyperlocation module and its capabilities. Describe the performance of location-based services in best practices, nonstandard, and box retail and manufacturing environments.
Describe how Cisco CMX uses Detect, Connect, and Engage to transform the network into a customer experience engine
Describe the types of analytics information that can be displayed through Cisco CMX
Different Levels of Accuracy
Describe where the data for locations is measured, and which devices are used to measure the location
Describe the best-practice guidelines for location-based services
Describe the accuracy of location with FastLocate and how it can be implemented in a Wi-Fi network
Describe how location is calculated with FastLocate
Describe how Cisco Hyperlocation improves location accuracy
Describe the Cisco Hyperlocation module and its capabilities
Describe the performance of location-based services in the best-practice, nonstandard, and box retail and manufacturing environments

Context-Aware Service Architecture
Describe the hardware and software platforms that are associated with Cisco Connected Mobile Experiences (CMX) version 10.2.2, and the context-aware service hardware and data flows.
Explain how to place Aps on the map in Cisco Prime Infrastructure as well as the importance of accurate information.
Describe the default positioning of APs on a ceiling, and the Hyperlocation AIR-ANT-LOC.
Discuss context-aware service software requirements
Describe the different hardware platforms in context-aware services and the data flows between them
Describe the placement of APs on maps in Cisco Prime Infrastructure and the importance of accurate information
Describe the default placement of APs on a ceiling
Describe the Cisco Hyperlocation AIR-ANT-LOC module for APs

Cisco CMX Connect
Describe the Cisco CMX Connect scalability and product specifications, and the use of CMX Connect in a network.
Describe Cisco CMX Connect and discuss the guest and administrative experiences
Cisco CMX Connect: Scalability and Product Specifications
Describe the product specifications for Cisco MSE
Use Case: Guest Registration Experience
Describe how Cisco CMX Connect can be used for guest registration

Cisco CMX Analytics
Compare the presence and location and where they are typically used
Describe update rates for locations using fast locate and probe-based location
Describe presence update rates for passers-by and ignored devices, and visitors, and explain indoor/outdoor site with presence
Describe the best practice prerequisites for multi-floor Location-Based Services, and the recommendations for location based services.
Describe how presences works in detail, and also explain how presence works with associated and unassociated client
Describe the Cisco CMX Analytics offerings for presence and location for indoors and outdoors with basic and good RF

Describe the location update rates for FastLocate and probe-based location
Describe the presence update rates for passers-by, ignored devices, and visitors
Describe the different types of analytics data that can be displayed for presence in an indoor and outdoor environment
Best Practice: Prerequisite Multifloor Location-Based Services
Describe the best-practice prerequisites for deploying location-based services in a multifloor
environment
Describe the recommendations for deploying location-based services
Describe how presence works in detail, specifically the changes in RSSI when a passer-by is detected and becomes a visitor and when a visitor leaves the venue
Describe how presence works with an unassociated client, specifically how the unassociated client is detected when it enters the venue and how it becomes a visitor and changes sites
Describe how the associated client moved from an AP in one site to an AP in another site and
maintains being associated with the network

Cisco CMX API
Describe the types of information that you could extract from the network data
Describe the type of data that can be provided and analyzed when using the Cisco CMX API
Describe where the Cisco CMX API gathers network data and how the gathered data can be used to improve the user experience

Cisco CMX Configuration
Describe the initial switch and WLC configuration for Cisco CMX
Describe how to add and export maps in Cisco Prime Infrastructure
Explain how to configure Cisco CMX using the System Settings menu
Describe the Detect and Locate function
Describe customized reports and adding widgets to customized reports.
Practical Use: Configure Switch and WLC for Cisco CMX
Verify the current state of PoE on the switch ports that support the APs that contain the Hyperlocation modules; configure the switch to support more power if needed; verify that the AP has joined the WLC; configure the APs to support Hyperlocation and NTP; and verify that the configuration is correct in the WLC.
Practical Use: Add Maps to Cisco Prime Infrastructure
Use Google Earth to locate and measure RCDN5 in the Cisco Richardson campus
Practical Use: Continue to Add Maps to Cisco Prime Infrastructure
Import maps into Cisco Prime Infrastructure and place the APs on the map
Practical Use: Add the AP Placement and Orientation
Continue with the previous lab regarding adding maps to Cisco Prime Infrastructure by adding the AP placement and orientation to the existing map
Practical Use: Use the System Settings Menu to Configure Cisco CMX
Configure Cisco CMX using the System Setup menu; this process will include importing maps and controllers from Cisco Prime Infrastructure and adding and verifying email services.
Practical Use: Add Outline of Walls to Cisco CMX Floor Plan Maps
Configure the outline walls to the floor maps in Cisco CMX.
Practical Use: Use Detect and Locate
Verify that the APs shown in Cisco CMX are the same as shown in the WLC,and verify the information on each AP in the floor map.
Practical Use: Continue to Customize Detect and Locate in Cisco CMX
Configure Cisco CMX to provide different views of clients on the floor map, and verify information on associated

and unassociated clients from the floor map.
Practical Use: Work with Analytics in Cisco CMX
Configure an Auto-Generate report in Cisco CMX
Practical Use: Work with Customized Reports in the Analytics Service
Create a customized report in the Cisco CMX Analytics service
Practical Use: Continue to Add Widgets to a Customized Report
Configure Cisco CMX customized reports to display up to six widgets.

Cisco CMX Cloud
Describe the three components of analytics, Detect, Connect, and Engage, and how these
components can be used to enhance the user experience and optimize operations Introducing Cisco CMX Cloud
Describe how CMX Cloud can provide visitor access through social media logins
Describe how the analytics data that CMX Cloud can provide can be used to make actionable
business decisions. Also, describe how the analytic data can be viewed on the Presence Analytics screen.
Describe traffic flow from the Wi-Fi network to the CMX Cloud, and how Detect, Connect, and Engage functions provide actionable business data
Describe how the cloud proxy server operates with AireOS 8.2 and older versions of software
Describe the operational difference that using AireOS 8.3 and newer provides to collecting data with CMX Cloud
Practical Use: Log in to the CMX Portal
In this lab, you will learn how to use your user credentials to log in to the CMX Cloud portal to do the initial setup of your CMX Cloud portal.
Practical Use: Configure an ACL in the WLC for Use with CMX Cloud
In this lab, you will configure an ACL to provide bidirectional access for the two IP addresses that are associated with Cisco CMX Cloud.
Practical Use: Configure the WLAN and Security in the WLC to Support CMX Cloud
In this lab, you will configure a WLAN and apply security to the WLAN in order for clients to join the network.
Practical Use: Create a Presence Site in CMX Cloud
In this lab, you will create a site and add AP(s) to the site so you can gather presence data from the site.
Practical Use: Create the Initial Portal in Connect and Engage
In this lab, you will perform the initial portal creation in the Connect & Engage component of CMX Cloud. This will create the template that you will customize in upcoming labs.
Practical Use: Add and Delete an Element and Add a Background Image to the Portal Template
In this lab, you will learn the elements of a template and how to add, delete and customize the
elements of a portal template.
Practical Use: Customize Text and Registration Elements in the Portal Template
In this lab, you will learn how to customize the text element and customize the registration element in the portal template.
Practical Use: Explore the Background Image, Themes, and Languages in the Portal Template
In this lab, you will learn to explore the options available in the Image, Themes, and Language
elements in the portal template.
Practical Use: Connect a Client to the Wi-Fi Network
In this lab, you will connect your client PC to the CMXaaS Wi-Fi network and observe how a visitor is onboarded to the network.
Practical Use: Work with Presence Analytics and Connect and Engage
In this lab, you will use the Presence Analytics option to view the data that is collected by CMX Cloud from the Test network.
Practical Use: Use the Manage Function in CMX Cloud
In this lab, you will use the Manage capability to verify Authorized Users, verify your Account

Information and Purchased Licenses, Enable or Disable Meraki Presence Integration, View Notifications, verify and review CMX Proxy information, and CMX Enable WLC information.
Practical Use: Integrate Meraki with CMX Cloud
In this lab, you will integrate CMX Cloud into an existing Meraki Wireless network to gather analytics data. You will set up a new site and integrate a Meraki network into the CMX Cloud to gather presence data.
Practical Use: Configure Northbound Notifications
In this lab, you will integrate CMX Cloud into an existing Meraki Wireless network to gather analytics data. You will set up a new site and integrate a Meraki network into the CMX Cloud to gather presence data.

Pervasive Security
Describe the Cisco security model that works across the attack continuum
New IT Landscape
Threat Landscape
Addressing the Full Attack Continuum
Building Security into the Network
Describe how to use Stealthwatch, ISE, and TrustSec to implement security into the network
Unbalanced Protection
Pervasive Protection Strategy
Architect for Defense in Depth
Risk Management Approach
Enabling the New Security Model
Covering the Full Attack Continuum

Introduction to NetFlow
Describe NetFlow, including the different versions and operational benefits
Increasing Importance of Network Awareness
Creating a Flow in the NetFlow Cache
Accessing Data Produced by NetFlow
Format of Export Data
Implementing NetFlow
NetFlow Applications
Describe how to configure NetFlow on Cisco devices.
Configuring a Customized Flow Record
Configuring Exporters
Creating a Customized Flow Monitor
Apply the Monitor to Each Layer 3-Enabled Interface
Verify the Configuration

Introduction to Cisco Stealthwatch
Describe each of the Cisco (Lancope) Stealthwatch system components
Stealthwatch Components
Cisco Stealthwatch Management Center
Describe the Stealthwatch Management Center web GUI and Java-based client
Describe the use of the host groups in the SMC
Describe how to verify the flow records using the SMC

Introduction to Cisco ISE
Cisco ISE Overview

Describe the main functions of Cisco ISE
Cisco TrustSec Architecture
How TrustSec Works
Describe TrustSec and summarize the key points about the operation of TrustSec SGA
Describe SGTs and SGACLs, including a closer look at 802.1ae MacSec security and context-based access-control concepts

Integrating Security Tools
Cisco Stealthwatch and ISE Integration
Describe the purpose and integration of ISE and Stealthwatch by using the pxGrid platform
Describe how to use SGT in Stealthwatch
Describe the Cisco ISE integration configuration on Stealthwatch
Describe the quarantine function using ISE ANC, including enabling ANC in ISE and Stealthwatch
Describe the flow of events when ANC is activated via the Stealthwatch console, along with the procedure on how to verify the success of the quarantine action within ISE

Implementing Cisco Software-Defined Access in the Campus Network
Role of Software-Defined Access in Cisco DNA
Describe the role of the Cisco SD-Access solution in Cisco DNA
Need for Cisco SD-Access
Cisco SD-Access Fabric Overview
Describe the SD-Access fabric domain including overlay and underlay networks in the campus fabric
Describe the Cisco SD-Access fabric nodes: control plane node, edge node, and border node
Describe the terms and terminology used in SD-access fabric solution.
Describe the SD-access control plane based on LISP.
Describe the SD-Access fabric data plane that is based on VXLAN
Describe the SD-Access policy plane based on Cisco TrustSec
Understand the need for the fabric border in the SD-Access solution
Understand how wireless devices integrate with the overall Cisco SD-Access solution, and the parts that work together to create the solution
Describe the high-level architecture of DNA center components: APIC-EM, ISE, and NDP
Understand the purpose of the policy application, and how it relates to other applications in
Cisco DNA Center Policy Application
Cisco DNA Center Provisioning Application
Cisco DNA Center Assurance
DNA Center applications and specific uses case for Cisco SD-Access.
Cisco SD-Access Platform Support
Describe the platform hardware support for SD-Access

Lab outline
Lab 1: Introducing Cisco APIC-EM GUI – Network, Device, and Topology Discovery Using APIC-EM
Lab 2: Implementing Cisco Network Plug and Play Solution Using Cisco APIC-EM
Lab 3: Implementing EasyQoS Using Cisco APIC-EM GUI
Lab 4: Site Provisioning and Monitoring Using Cisco IWAN Application
Lab 5: Troubleshooting Using Cisco APIC-EM Path Trace Applications
Lab 6: Site Provisioning with NFVIS on Cisco UCS® C220 M3 Server Using OAM Servers
Lab 7: Initial Switch and WLC Configuration for Cisco CMX
Lab 8: Adding Maps to Cisco Prime Infrastructure

Lab 9: Continuing to Add Maps to Cisco Prime Infrastructure
Lab 10: AP Placement and Orientation
Lab 11: Exporting Maps from Cisco Prime Infrastructure
Lab 12: Performing the Initial Configuration of CMX
Lab 13: Using the System Settings Menu to Configure Cisco CMX
Lab 14: Adding Outline Wall to CMX Floor Plan Maps
Lab 15: Using Detect and Connect
Lab 16: Continuing to Customize Detect and Locate in CMX
Lab 17: Working with Analytics in Cisco CMX
Lab 18: Working with Customized Reports in the Analytics Service
Lab 19: Continuing to Add Widgets to a Customized Report in CMX
Lab 20: Logging in to the CMX Portal
Lab 21: Configuring an ACL in the WLC for Use with CMX Cloud
Lab 22: Configuring the WLAN and Security in the WLC to Support CMX Cloud
Lab 23: Creating a Presence Site in CMX Cloud
Lab 24: Initial Portal Creation in Connect and Engage
Lab 25: Adding and Deleting an Element and Adding a Background Image to the Portal Template
Lab 26: Customizing Text and Registration Elements in the Portal Template
Lab 27: Exploring the Background Image, Themes, and Languages in the Portal Template
Lab 28: Connecting a Client to the Wi-Fi Network
Lab 29: Working with Presence Analytics and Connect and Engage
Lab 30: Using the Manage Function in CMX Cloud
Lab 31: Meraki® Integration with CMX Cloud
Lab 32: Configuring Northbound Notifications