ENWLSI (IMPLEMENTING CISCO ENTERPRISE WIRELESS NETWORKS) 1.12

Objetivo

After taking this course, you should be able to: • Implement network settings to provide a secure wireless network infrastructure; • Troubleshoot security issues as they relate to the wireless network infrastructure; • Implement a secure wireless client and troubleshoot wireless client connectivity issues; • Implement and troubleshoot QoS in wireless networks; • Implement and troubleshoot advanced capabilities in wireless network services.

Público Alvo

Professionals interested in knowing and implementing solutions using the Cisco Wireless portfolio. This course also helps prepare student to take the Implementing Cisco Enterprise Wireless Networks (300-430 ENWLSI) exam, which is part of the new CCNP® Enterprise.

Pré-Requisitos

Before taking this course, you should have: • General knowledge of networks; • General knowledge of wireless networks; • Routing and switching knowledge. For reference only: the following Cisco courses can help you gain the knowledge you need to prepare for this course: • Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) • Understanding Cisco Wireless Foundations (WLFNDU)

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Course Introduction
Course Outline
Course Goals & Objectives

Module 1: Securing and Troubleshooting the Wireless Network Infrastructure

Part 1: Implement network settings to provide a secure wireless network infrastructure
Describe troubleshoot security issues as it relates to the wireless network infrastructure
Practice Uses: Lab Familiarization (Base Learning Lab)
• Verify the Network Configuration of Campus-C9800-CL
• List the Network Configuration of Remote-C9800-CL
• Identify the AP-Connected Switch Ports
• Enable the WLAN on Campus-C9800-CL

• Connect the Client Laptop to the Wireless Network
• Implement Secure Access to the WLCs and Access Points

Part 2: Configure WLCs and APs to require secure access to management interfaces
Configure the Network for Access Point 802.1X Authentication
Configure the access switch and the access points to use 802.1x port authentication
Practice Uses: Configure Secure Management Access for WLCs and APs
• Configure devices for secure management access.
• Configure the Cisco WLC for TACACS+
• Configure Cisco ISE for TACACS+
• Verify TACACS+ Access
• Configure and Verify SSH Access to Access Points

Part 3: Use Cisco DNA Center for Controller and AP Auto Install
Describe the auto-configuration process and procedures for access points and wireless LAN controllers using Cisco DNA Center
Configure and integrate devices to implement Cisco Prime Infrastructure into the wireless network.
Practice Uses: Add Network Devices and External Resources to Cisco Prime Infrastructure
• Configure Cisco WLC for SNMPv3
• Add Cisco WLCs to Cisco Prime Infrastructure with SNMPv3
• Add Cisco ISE to Cisco Prime Infrastructure
• Add Cisco CMX to Cisco Prime Infrastructure
Practice Uses: Customize Cisco Prime Infrastructure for Network Monitoring
• Customize Cisco Prime Infrastructure for network monitoring.
• Validate Connected Devices and Associate a Client
• Monitor Health and Performance Data with Dashboards and Alarms
• Use the 360° View
• Explore Scheduling and Managing Reports
Practice Uses: Configure 802.1X Port Access for the APs
• Configure secure port access for the APs.
• Configure Cisco ISE to Accept RADIUS Requests

Part 4:Define Network Troubleshooting Techniques
Monitor and troubleshoot wireless network Infrastructure issues.
Troubleshoot Access Point Join Issues
Practice Uses: Capture a Successful AP Authentication
• Capture a successful AP authentication.
• Capture a Successful Join from Cisco WLC
• Use Wireshark to Identify the Steps in a WLC-Join
Monitor the Wireless Network
Monitor the wireless network for rogue access points using the WLCs and Cisco Prime Infrastructure.

Module 2: Implementing and Troubleshooting Secure Client Connectivity

Part 5: Implement a secure wireless client and troubleshoot wireless client connectivity issues
Configure the Cisco WLC for Wireless Client 802.1X Authentication
Configure the Wireless Client for 802.1X Authentication
Configure various wireless client operating system supplicants for WPA2 enterprise association.

Practice Uses: Implement AAA Services for Central Mode WLANs
• Configure the network settings with Cisco ISE to implement AAA services for central (local) mode WLANs
• Configure Campus-C9800-CL for 802.1X Access
• Configure Cisco ISE for RADIUS Integration with the Cisco WLCs
• Configure a Basic Access Policy for Employees
• Verify Employees Can Log In and Reach Correct VLAN

Part 6: Configure a Wireless LAN for FlexConnect
Practice Uses: Implement AAA Services for FlexConnect Mode WLANs
• Configure the network settings with Cisco ISE to implement AAA services for FlexConnect mode
• Configure the Ethernet Port to Allow All VLANs
• Configure WLAN for FlexConnect Local Switching with 802.1x Authentication
• Configure a Flex Location and Modify the Necessary Policies
• Configure the Access Point Switch Port for Trunking
• Configure a Policy Set to Provide Access to the Configured VLAN on the WLAN
• Verify the Configuration with Client PC

Part 7: Implement Guest Services in the Wireless Network
Implement guest services in the wireless network to allow network access to guest users and devices
Configure the WLC to use Cisco ISE to provide centralized web authentication.
Implement AAA Override
Configure the network settings to implement AAA based wireless security.
Configure Cisco ISE to provide a centralized Web portal for guest networks.
Practice Uses: Configure Guest Services in the Wireless Network
• Configure guest services in the wireless network.
• Configure AAA Authentication and Authorization Method List
• Configure Hotspot Guest WLAN on Cisco WLC
• Create a Redirect ACL for Guest Flow
• Configure an Authorization Profile
• Configure a Policy Set to Access the Configured VLAN
• Verify the Configuration with Client PC

Part 8: Implement BYOD
Implement BYOD in the wireless network.
Practice Uses: Configure BYOD in the Wireless Network
Configure the BYOD settings in the wireless network.
• Configure the Ethernet Port and Add the VLANs
• Configure BYOD Guest and Cisco ISE WLANs on the Cisco WLC
• Modify the Native Supplicant Profile
• Edit the NSP_Onboard Authorization Profile
• Edit the Default Policy Set
• Edit the Default Self-Registered Guest Portal
• Update the Windows File to Activate BYOD on a Personal Device
• Verify the Configuration with Client PC

Part 9: Implement Location-Aware Guest Services
Implement location aware guest services in the wireless network.
Troubleshoot Client Connectivity

Identify and resolve client connectivity issues.
Describe Issues That Affect Client Performance
Identify client performance issues resulting from RF conditions in the wireless environment.
Practice Uses: Capture Successful Client Authentications
• Capture successful client authentications.
• Prepare the Cisco WLC and Cisco ISE to Capture Data
• Use the Radioactive Trace Feature to Capture a Client Authentication
• Use Debugs to Observe a Successful Client Authentication
• Use Cisco ISE to View a Successful Authentication
Practice Uses: Configure Cisco CMX Facebook Wi-Fi
• Configure the wireless network for Cisco CMX Facebook Wi-Fi.
• Configure ACLs for Facebook Wi-Fi
• Configure a Default Facebook Page to Host on Cisco CMX
• Configure WLAN for Web Passthrough Authentication
• Create a Facebook Page for Your Organization
• Cisco CMX Facebook Wi-Fi Reporting

Part 10: Monitor Wireless Clients
Utilize Cisco Prime Infrastructure and Cisco DNA Center to monitor the wireless client in the network.

Module 3: Implementing and Troubleshooting QoS in Wireless Networks

Part 11: Implement QoS in the Wireless Network
Configure the Cisco WLC to Support Voice Traffic
Practice Uses: Configure QoS in the Wireless Network for Voice and Video Services
• Configure WLAN for Voice Only
• Configure the AAA Policy for Enterprise

Part 12: Optimize Wireless Utilization on the Cisco WLC
Implement Cisco AVC in the Wireless Network
Practice Uses: Configure Cisco AVC in the Wireless Network
Configure the AVC profiles in the wireless network.
• Configure Application Visibility on the WLAN
• Verify Cisco AVC Configuration with Client PC
• Configure AVC Profile to Block Access to YouTube
Practice Uses: Configure mDNS in the Wireless Network
Configure mDNS in the wireless network.
• Validate VLC Streaming Video Player and Sample Video
• Configure the Wireless Client PC for Access
• Use VLC to Start a Video Stream
• Configure Client PC to Receive the Streamed Video
• Improve the Multicast Stream Quality with VideoStream for Multicast
• Validation Steps

Part 13: Implement Multicast Services
Implement mDNS Service
Implement Cisco Media Stream
Troubleshoot QoS Issues in the Wireless Network

Identify and resolve QoS issues for wireless clients.
Troubleshoot mDNS Issues
Troubleshoot Media Stream Issues
Practice Uses: Capture Successful QoS Traffic Marking in the Wireless Network
Capture successful QoS traffic marking in the wireless network.
• Configure Cisco AVC to Mark ICMP Traffic as Scavenger Class
• Configure AP on Remote-C9800-CL in Sniffer Mode
• Capture and Decode Traffic

Module 4: Implementing and Troubleshooting Advanced Wireless Network Services

Part 14: Implement Base Location Services on Cisco Prime Infrastructure
Implement location tracking on Cisco Prime Infrastructure using Cisco CMX Detect and
Implement Hyperlocation in the Wireless Network
Implement Detect and Locate Services on Cisco CMX
Implement Analytics on Cisco CMX
Implement Presence Services on Cisco CMX
Monitor and Locate Rogue Devices with Cisco Prime Infrastructure and Cisco CMX
Practice Uses: Configure Detect and Locate Services on Cisco CMX
Configure Detect and Locate Services on the Cisco CMX.
• Validate Connected Devices and Associate a Client
• Monitor the Wireless Client on the Cisco WLC
• Monitor Wireless Rogue Devices on the Cisco WLC
• Add AP to Map in Cisco Prime Infrastructure
• Monitor Wireless Clients on Cisco Prime Infrastructure
• Monitor Rogue Devices and Security Threats on Cisco Prime Infrastructure
• Monitor Wireless Security Threats on Cisco Prime Infrastructure
• Add Maps and Controllers to Cisco CMX
• View Devices in Cisco CMX

Part 15: Monitor and Detect Wireless Clients with Cisco CMX and Cisco DNA Center
Monitor and detect wireless clients with Cisco CMX and Cisco DNA Center.
Run Analytics on Wireless Clients
Troubleshoot Location Accuracy with Cisco Hyperlocation
Monitor and Manage RF Interferers on the Cisco WLC
Monitor and Manage RF Interferers on Cisco Prime Infrastructure and Cisco CMX

Lab Outline
Lab 1: Lab & WLC 9800 Familiarization (Base Learning Lab)
Lab 2: Configure Secure Management Access for WLCs and APs
Lab 3: Add Network Devices and External Resources to Cisco Prime Infrastructure
Lab 4: Customize Cisco Prime Infrastructure for Network Monitoring
Lab 5: Configure 802.1X Port Access for the APs
Lab 6: Capture a Successful AP Authentication
Lab 7: Implement AAA Services for Central Mode WLANs
Lab 8: Implement AAA Services for FlexConnect Mode WLANs
Lab 9: Configure Guest Services in the Wireless Network
Lab 10: Configure BYOD in the Wireless Network

Lab 11: Capture Successful Client Authentications
Lab 12: Configure Cisco CMX Facebook Wi-Fi
Lab 13: Configure QoS in the Wireless Network for Voice and Video Services
Lab 14: Configure Cisco AVC in the Wireless Network
Lab 15: Configure mDNS in the Wireless Network
Lab 16: Capture Successful QoS Traffic Marking in the Wireless Network
Lab 17: Configure Detect and Locate Services on Cisco CMX