



Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers

Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers

Simone Arena

Francisco Sedano Crippa, CCIE No. 14859

Nicolas Darchis, CCIE No. 25344

Sudha Katgeri, CCIE No. 45857

Cisco Press

Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers

Table of Contents

Cover

Title Page

Copyright Page

Acknowledgments

Contents at a Glance

Contents

Introduction

Chapter 1 Cisco C9800 Series

- Why Cisco C9800?

 - Intent-Based Networking (IBN)

 - Flexible Software

 - Flexible Hardware

- The Role of the Wireless Controller in a Cloud Era

- Managing the Cisco C9800

 - Traditional Management Tools

 - On Box Management

 - Cisco Prime Infrastructure

 - Cisco DNA Center

 - C9800 Prerequisites for Cisco DNA Center

 - CI/CD Tools

 - Licensing

- Cisco Next-Generation Wireless Stack

Table of Contents

Summary

References

Chapter 2 Hardware and Software Architecture of the C9800

General CAPWAP Split MAC Architecture

The Controller Control Plane Architecture Elasticity

IOS-XE Software Architecture

WNCd: The Heart of the Wireless Controller Control Plane

Other Wireless Processes

Wireless Client State Machine

One Dataplane to Rule Them All (or Three at the Maximum)

Hardware Overview

C9800-40 and C9800-80

C9800-L

C9800-CL

Summary

Chapter 3 C9800 Configuration Model

C9800 New Configuration Model

What Does My AireOS AP Group Migrate To?

What About FlexConnect?

Cisco C9800 Series Profile and Tag Considerations

Assigning Tags

Moving APs Between Wireless Controllers and Preserving Tags

Roaming Between Policy Tags

Designing with Site Tags in Mind (Local Mode APs)

Designing with Site Tags in Mind (FlexConnect Mode APs)

Summary

References

Chapter 4 C9800 Deployment and Installation

Table of Contents

C9800 Deployment Models

C9800 for Private Cloud

C9800 Physical Appliance

C9800 Virtual Appliance

Embedded Wireless Controller on Catalyst AP and Switch

C9800 for Public Cloud

Setting Up Your First Catalyst Wireless Network

C9800 Initial Setup

Access Point Join

Configuring WLAN and Connecting a Client

Summary

References

Chapter 5 Security

Network Security Fundamentals

Access Control Lists (ACLs)

Defining ACLs

Applying ACLs

Applying Wireless ACLs on the WLC

FlexConnect ACLs on the AP

The Case of Downloadable ACLs (DACLS)

URL Filters (a.k.a. DNS-Based ACLs)

Certificates and Trustpoints

A Case for Trustpoints

How to Add a Certificate on the Controller

AAA

RADIUS

RADIUS Attributes

RADIUS Sequence Example

RADIUS Change of Authorization (CoA)

Table of Contents

RADIUS Configuration and Load Balancing

Configuring RADIUS Servers

Configuring RADIUS Server Groups

RADIUS Server Fallback

RADIUS Load Balancing

RADIUS Accounting

AAA Methods

Local EAP

TACACS+

LDAP

Wireless Security Fundamentals

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

802.1X for WPA Enterprise

802.1X Components

EAP

EAP Methods

WPA3 Enterprise

Preshared Key for WPA Personal

WPA3 SAE

MPSK

Identity PSK (iPSK)

MAC Filtering

Enhanced Open

Securing the Air

WPA2 Personal

WPA3 SAE

WPA2 with iPSK

Enhanced Open

Table of Contents

- (Local) Web Authentication
- Central Web Authentication
- Web Authentication Best Practices
- HTTPS Redirection
- Captive Portal Bypass
- Web Authentication Takeaways
- Rogue Detection and WIPS

Securing Your Access Points

- AP Authorization
- AP 802.1X Authentication
- Securing the AP Join Process Using Locally Significant Certificates

Securing Your Wireless Controller

- Securing Administrator Access
- Using TACACS+
- Using RADIUS
- Guest Users
- The Lobby Ambassador Type of User
- NETCONF
- Granularity of WebUI Access
- Connect to the WebUI Using Certificates
- Securing Traffic

Encrypted Traffic Analytics

Cisco Umbrella

Cisco Secure Development Lifecycle (CSDL)

Summary

References

Chapter 6 Mobility and Client Roaming

802.11 Roaming

Table of Contents

- Full-Auth Roaming (or Slow Roam)
- Fast Secure Roaming
- PMKID Caching (Sticky Key Caching)
- OKC
- CCKM
- Fast Transition (802.11r)
- Roaming Optimizations
- 802.11k
- 802.11v BSS Transition

Types of Client Roaming

- Intra-Controller Roaming
- Intra-WNCd Roaming (Same Site Tag, Same Policy Profile)
- Inter-WNCd Roam (Different Site Tags, Same Policy Profile)
- Intra-WLC Roam (Same Site Tag, Different Policy Profile)
- Inter-Controller Roaming
- Layer 2 Roaming
- Layer 3 Roaming
- Static IP Client Mobility
- Auto-Anchor Mobility (Guest Tunnel)
- Configuring Secure Mobility Tunneling on a C9800

C9800 to AireOS Inter-Release Controller Mobility (IRCM)

Summary

References

Chapter 7 RF Deployment and Guidelines

Radio Resources Management (RRM) Concepts and Components

- Antennas and Signal Propagation
- Countries and Domains

Challenging RF Environments

- Metal-Heavy Areas

Table of Contents

- High-Density Crowd Areas
- Shielded Doors and Sudden Turns
- Uneven Ceilings
- Atriums

Radio Resources Management (RRM)

- Data Collection
- RF Grouping
- RF Grouping Modes
- TPC
- TPC Overview
- TPC Minimum and Maximum
- Coverage Hole Detection

DCA

- Overlapping Basic Service Set (BSS)
- Cloud-Based RRM

RF Profiles

Spectrum Intelligence and CleanAir

- Configuring CleanAir
- Monitoring the Spectrum Live
- Interferer Location Tracking
- Monitoring the RF Space

Advanced RF Features

- Band Select
- Aggressive Client Load Balancing
- Off-Channel Scanning Defer

Airtime Fairness (ATF)

- Wi-Fi 6 Features
- OFDMA
- Multi User Multiple Input Multiple Output (MU-MIMO)

Table of Contents

Target Wake Time (TWT)

BSS Coloring

Channel Width

Dynamic Frequency Selection (DFS)

DFS Overview

DFS in the C9800

Flexible Radio Assignment (FRA)

Tri-radio

Wireless Intrusion Prevention System (WIPS) and Rogue Detection

Rogue AP Detection and Classification

Detecting a Rogue Access Point

Classifying Rogue Access Points

Understanding the Danger of a Rogue Access Point

Containing Rogue Access Points

Adaptive WIPS

Client Exclusion

Summary

References

Chapter 8 Multicast and Multicast Domain Name System (mDNS)

Wireless Multicast

Multicast Packet Flow in Wireless

Multicast in a Centralized Wireless Deployment

Multicast in Flex

Multicast in Fabric

How to Configure Multicast on the C9800

IGMP and MLD on the C9800

CAPWAP Multicast

Multicast over Unicast (MoU)

Multicast over Multicast (MoM)

Table of Contents

802.11 Multicast

Wireless Broadcast and Non-IP Multicast

Multicast in Client Roaming Scenarios

Media Stream Feature

Cell Planning

Components of VideoStream

How to Configure Media Stream

mDNS

mDNS Bridging

mDNS Gateway

How to Configure mDNS Gateway

mDNS Gateway on WLAN

mDNS Service Policy on Policy Profile

mDNS Service Policy

mDNS Service Policy on VLAN SVI

mDNS Service Policy via AAA Override

mDNS-the AP

mDNS Gateway in FlexConnect Deployment

mDNS Gateway with Guest Anchor

Summary

References

Chapter 9 Quality of Service (QoS)

Wi-Fi Quality of Service (QoS)

Wi-Fi (802.11) QoS Fundamentals

QoS Design

UP and DSCP Mapping

DSCP to UP Mapping

Wireless Call Admission Control (CAC)

Implementing Wireless QoS on the C9800

Table of Contents

QoS Policy Targets

Modular QoS CLI

Trust DSCP Model

Designing and Deploying Catalyst C9800 QoS

QoS Deployment Workflow

Auto QoS

QoS Profiles (a.k.a. Metal QoS Profiles)

Application Visibility and Control (AVC)

Deployment Verification and Restrictions

Fastlane+ (Plus)

Best Practices

Summary

References

Chapter 10 C9800 High Availability

SSO Redundancy

Prerequisites

Ports and Interfaces

Redundancy Management Interface (RMI)

Redundancy Port (RP)

Uplink Ports

Console Port

Out-of-Band Management/Service Port (SP)

RP+RMI Supported Topologies

Building an RP+RMI HA Pair

Configuration

Active-Standby Election Process

HA Sync

HA Formation in Action

SSO Switchover

Table of Contents

System and Network Error Handling

Monitoring HA

Monitoring an HA Pair via the CLI

Monitoring an HA Pair via the GUI

Monitoring an HA Pair via SNMP

Monitoring an HA Pair via Programmatic Interfaces

RP Only to RP+RMI HA Migration

HA Teardown

SSO Deployment: Impact on Features

Mobility (Mobility MAC)

Link Aggregation Group (LAG)

Multi-Chassis LAG

N+1 Redundancy

N+1 HA Configuration

Configuration on the AP Join Profile

CAPWAP Timers

Preserving AP-to-Tag Mapping across N+1 Failovers

Licensing with N+1

N+1 vs. SSO High Availability

HA in EWC-AP Deployment

HA in EWC-SW Deployment

Summary

References

Chapter 11 Cisco DNA Spaces Integration and IoT

Value-Added Wireless Services

Location Tracking

Accuracy

Location Update Frequency

Table of Contents

Presence

The Impact of Privacy MAC Addresses

Location Deployment Guidelines

Other Technologies

Analytics

Guest Services

Bluetooth and IoT

BLE

IoT

Bluetooth Location Tracking

Connected Mobile Experiences (CMX)

Cisco DNA Spaces

Deployment Modes

Direct Connection

Cisco DNA Spaces Connector

CMX Tethering

Specific Service Examples

OpenRoaming

What Problem Is OpenRoaming Trying to Solve?

OpenRoaming Architecture

OpenRoaming Configuration

Captive Portal

Advantages of a Portal on Cisco DNA Spaces

Proximity

BLE Gateway on Cisco DNA Spaces

Summary

References

Chapter 12 Network Programmability

Table of Contents

What Is Network Programmability?

Why Is Network Programmability Needed?

Is Network Programmability a New Concept?

Orchestration of the Entire Network

Configuration Repeatability

Idempotency

Imperative vs. Declarative Models

Infrastructure as Code (IaC)

Network Programmability in the C9800

Data Models

YANG Data Models

Encoding Formats

- XML

- JSON

- Protobuf

Protocols

- NETCONF

- NETCONF Capabilities

- NETCONF Layers

- RESTCONF

- HTTP Methods

- HTTP Return Codes

- gNMI/gRPC

Tools to Examine YANG Models

- pyang

- Using pyang in a Docker Container

- YANG Suite

How to Examine Data Using NETCONF and YANG Suite

Table of Contents

How to Examine Data Using RESTCONF and POSTMAN

- Enabling RESTCONF

- RESTCONF URIs

- Root

- Resource

- Data Model

- Searching Data

- Updating the Configuration

Python and Network Programmability

- Assigning Tags to APs Based on Serial Number

- Program Structure

Summary

References

Chapter 13 Model-Driven Telemetry

What Is Model-Driven Telemetry?

How to Enable Model-Driven Telemetry

- NETCONF

- RESTCONF

- gNMI

Operational Data and KPIs

Polling vs. Subscribing

Telemetry Streams

- Yang-notif-native Stream

- Yang-push Stream

How to Identify Subtrees in YANG Models

Dial-out vs. Dial-in

- Dial-out

- Dial-in

Table of Contents

Creating Dial-in Subscriptions

Tools

YANG Suite

TIG (Telegraf, Influx, Grafana)

Creating a Dashboard

Summary

References

Chapter 14 Cisco DNA Center/Assurance Integration

Introduction

Cisco DNA Center Assurance Architecture

Managing the C9800 with Cisco DNA Center

Client 360

AP 360

Network Services Analytics

Device Analytics

Apple Analytics

Samsung Analytics

Intel Analytics

Intelligent Capture

Cisco Active Sensor

Sensor Provisioning and Onboarding

Test Suites

Troubleshooting the Assurance Application

Summary

References

Chapter 15 Backing Up, Restoring, and Upgrading Your C9800

Saving and Restoring the Configuration for Disaster Recovery

Saving the Configuration Changes

Table of Contents

- Backing Up the Configuration and Restoring It
- Backing Up Everything for Restoring on Another Controller
- The Advantage of Backing Up Using the WebUI
- The Case of Configuration Encryption
- Backing Up Using Cisco Prime Infrastructure
- Backing Up Using Cisco DNA Center

Running IOS-XE in Install or Bundle Mode

- Bundle Mode
- Install Mode

Upgrading (and Downgrading) the Controller Safely

- Standard Upgrade
- AP Predownload
- Efficient Upgrade
- Rolling AP Upgrade (for N+1)
- In-Service Software Upgrade (ISSU)

Summary

References

Chapter 16 Troubleshooting

Control Plane Tracing

- Syslog
- Binary Tracing
- Always-On Tracing
- Per-Process Debugging
- Radioactive Tracing

Embedded Packet Capture (EPC)

Packet Tracer

Troubleshooting Dashboard

- Core Dump and System Report

Table of Contents

Debug Bundle

Ping and Trace Route

Other On-the-Box Tools on the C9800 GUI

AireOS Config Translator

Command-Line Interface

File Manager

Walk-Me Integrated with the C9800 GUI

Configuration Validator

Offline Tools for the C9800

Wireless Configuration Convertor

Wireless Config Analyzer

Wireless Debug Analyzer

Log Advisor

Health and KPI Monitoring

Dashboard

Hardware Monitoring

Smart Licensing

Direct Connect

On-Premises SSM or CSLU

Airgap

AP Health Monitoring

Client Health Monitoring

CPU Monitoring

Memory Monitoring

Data Plane Monitoring

Summary

References

Appendix A: Setting Up a Development Environment

Index

Table of Contents