Cisco Software-Defined Access

Cisco Secure Enterprise

Jason Gooley, CCIE® x2 (RS & SP) No. 38759
Roddie Hasan, CCIE® RS No. 7472
Srilatha Vemula, CCIE® SEC No. 33670

ciscopress.com

Cisco Software-Defined Access

Jason Gooley, CCIE No. 38759
Roddie Hasan, CCIE No. 7472
Srilatha Vemula, CCIE No. 33670

Cisco Press

Cisco Software-Defined Access

Table of Contents

Cover
Title Page
Copyright Page
About the Authors
About the Technical Reviewers
Dedications
Acknowledgments
Contents at a Glance
Contents
Introduction
Chapter 1 Todays Networks and the Drivers for Change
- Networks of Today
- Common Business and IT Trends
- Common Desired Benefits
- High-Level Design Considerations
- Cisco Digital Network Architecture
- Past Solutions to Todays Problems
  - Spanning-Tree and Layer 2Based Networks
- Introduction to Multidomain
  - Cloud Trends and Adoption
- Summary

Chapter 2 Introduction to Cisco Software-Defined Access

Table of Contents

Challenges with Todays Networks

Software-Defined Networking

Cisco Software-Defined Access

- Cisco Campus Fabric Architecture
- Campus Fabric Fundamentals
- Cisco SD-Access Roles

Network Access Control

- Why Network Access Control?

Introduction to Cisco Identity Services Engine

- Overview of Cisco Identity Services Engine
- Cisco ISE Features
- Secure Access
- Device Administration
- Guest Access
- Profiling
- Bring Your Own Device
- Compliance
- Integrations with pxGrid

Cisco ISE Design Considerations

- Cisco ISE Architecture
- Cisco ISE Deployment Options
- Standalone Deployment
- Distributed Deployment
- Dedicated Distributed Deployment

Segmentation with Cisco TrustSec

- Cisco TrustSec Functions
- Classification
- Propagation
- Enforcement

Table of Contents

Summary

Chapter 3 Introduction to Cisco DNA Center

Network Planning and Deployment Trends

History of Automation Tools

Cisco DNA Center Overview

Design and Visualization of the Network

Site Design and Layout

Network Settings

Wireless Deployments

Network Discovery and Inventory

Discovery Tool

Inventory

Device Configuration and Provisioning

Summary

Chapter 4 Cisco Software-Defined Access Fundamentals

Network Topologies

Cisco Software-Defined Access Underlay

Manual Underlay

Automated Underlay: LAN Automation

Wireless LAN Controllers and Access Points in Cisco Software-Defined Access

Shared Services

Transit Networks

IP-Based Transit

SD-Access Transit

Fabric Creation

Fabric Location

Fabric VNs

Table of Contents

- Fabric Device Roles
  - Control Plane
  - Fabric Borders
  - Border Automation
  - Border and Control Plane Collocation
  - Fabric Edge Nodes
  - Intermediate Nodes
  - External Connectivity
  - Fusion Router
- Host Onboarding
  - Authentication Templates
  - VN to IP Pool Mapping
  - SSID to IP Pool Mapping
  - Switchport Override
- Summary
- References in This Chapter

Chapter 5 Cisco Identity Services Engine with Cisco DNA Center

- Policy Management in Cisco DNA Center with Cisco ISE
  - Integration of Cisco DNA Center and ISE
  - Certificates in Cisco DNA Center
  - Certificates on Cisco Identity Services Engine
  - Cisco ISE and Cisco DNA Center Integration Process
- Group-Based Access Control
- Segmentation with Third-Party RADIUS Server
- Secure Host Onboarding in Enterprise Networks
  - Endpoint Host Modes in 802.1X
  - Single-Host Mode
  - Multi-Host Mode

Table of Contents

Multi-Domain Mode

Multi-Auth Mode

802.1X Phased Deployment

Why a Phased Approach?

Phase I: Monitor Mode (Visibility Mode)

Phase II: Low-Impact Mode

Phase II: Closed Mode

Host Onboarding with Cisco DNA Center

No Authentication Template

Open Authentication Template

Closed Authentication

Easy Connect

Security in Cisco Software-Defined Access Network

Macro-Segmentation in Cisco SD-Access

Micro-Segmentation in Cisco SD-Access

Policy Set Overview in Cisco ISE

Segmentation Policy Construction in Cisco SD-Access

Corporate Network Access Use Case

Guest Access Use Case

Segmentation Outside the Fabric

Summary

References in This Chapter

Chapter 6 Cisco Software-Defined Access Operation and Troubleshooting

Cisco SD-Access Under the Covers

Fabric Encapsulation

LISP

VXLAN

Table of Contents

MTU Considerations

Host Operation and Packet Flow in Cisco SD-Access

DHCP in Cisco SD-Access

Wired Host Onboarding and Registration

Wired Host Operation

Intra-Subnet Traffic in the Fabric

Inter-Subnet Traffic in the Fabric

Traffic to Destinations Outside of the Fabric

Wireless Host Operation

Initial Onboarding and Registration

Cisco SD-Access Troubleshooting

Fabric Edge

Fabric Control Plane

Authentication/Policy Troubleshooting

Authentication

Policy

Scalable Group Tags

Summary

References in This Chapter

Chapter 7 Advanced Cisco Software-Defined Access Topics

Cisco Software-Defined Access Extension to IoT

Types of Extended Nodes

Extended Nodes

Policy Extended Nodes

Configuration of Extended Nodes

Onboarding the Extended Node

Packet Walk of Extended Cisco SD-Access Use Cases

Use Case: Hosts in Fabric Communicating with Hosts Connected Outside the Fabric

Table of Contents

Use Case: Traffic from a Client Connected to a Policy Extended Node

Use Case: Traffic to a Client Connected to a Policy Extended Node

Use Case: Traffic Flow Within a Policy Extended Node

Multicast in Cisco SD-Access

Multicast Overview

IP Multicast Delivery Modes

Multicast Flows in Cisco SD-Access

Scenario 1: Multicast in PIM ASM with Head-End Replication (Fabric RP)

Scenario 2: Multicast in PIM SSM with Head-End Replication

Scenario 3: Cisco SD-Access Fabric Native Multicast

Cisco SD-Access Multicast Configuration in Cisco DNA Center

Layer 2 Flooding in Cisco SD-Access

Layer 2 Flooding Operation

Layer 2 Border in Cisco SD-Access

Layer 2 Intersite

Layer 2 Intersite Design and Traffic Flow

Fabric in a Box in Cisco SD-Access

Cisco SD-Access for Distributed Campus Deployments

Types of Transit

IP Transit

Fabric Multisite or Multidomain with IP Transit

Cisco SD-Access Transit

Cisco SD-WAN Transit

Policy Deployment Models in Cisco SD-Access Distributed Deployment

Cisco SD-Access Design Considerations

Latency Considerations

Cisco SD-Access Design Approach

Very Small Site

Small Site

Table of Contents

- Medium Site
- Large Site
- Single-Site Design Versus Multisite Design
- Cisco SD-Access Component Considerations
- Underlay Network
- Underlay Network Design Considerations
- Overlay Network
- Overlay Fabric Design Considerations
- Fabric Control Plane Node Design Considerations
- Fabric Border Node Design Considerations
- Infrastructure Services Design Considerations
- Fabric Wireless Integration Design Considerations
- Wireless Over-the-Top Centralized Wireless Option Design Considerations
- Mixed SD-Access Wireless and Centralized Wireless Option Design Considerations
- Wireless Guest Deployment Considerations
- Security Policy Design Considerations

Cisco SD-Access Policy Extension to Cisco ACI

Summary

References in This Chapter

Chapter 8 Advanced Cisco DNA Center

Cisco DNA Center Architecture and Connectivity

- Hardware and Scale
- Network Connectivity
- High Availability and Clustering with Cisco DNA Center

Software Image Management

- Image Repository
- Golden Image
- Upgrading Devices

Table of Contents

Cisco DNA Center Templates

Template Creation

Template Assignment and Network Profiles

Deploying Templates

Plug and Play

Onboarding Templates

PnP Agent

Claiming a Device

Cisco DNA Center Tools

Topology

Command Runner

Security Advisories

Summary

References in This Chapter

Chapter 9 Cisco DNA Assurance

Assurance Benefits

Challenges of Traditional Implementations

Cisco DNA Analytics

Cisco DNA Assurance Architecture

Cisco DNA Assurance Data Collection Points

Streaming Telemetry

Network Time Travel

Health Dashboards

Overall Health Dashboard

Network Health Dashboard

Cisco SD-Access Fabric Network Health

Client Health Dashboard

Application Health Dashboard

Cisco DNA Assurance Tools

Table of Contents

Intelligent Capture

Anomaly Capture

Path Trace

Sensor Tests

Cisco AI Network Analytics

Summary

References in This Chapter

Glossary

A

B

C

D

E

F-K

L

M

N-O

P

Q

R

S

T

U

V

W-X

Index

Pearson