



CCNAv7: Enterprise Networking, Security, and Automation

Companion Guide



Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Press

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Table of Contents

Cover

Title Page

Copyright Page

About the Contributing Authors

Contents at a Glance

Contents

Introduction

Chapter 1 Single-Area OSPFv2 Concepts

Objectives

Key Terms

Introduction (1.0)

OSPF Features and Characteristics (1.1)

Introduction to OSPF (1.1.1)

Components of OSPF (1.1.2)

Routing Protocol Messages

Data Structures

Algorithm

Link-State Operation (1.1.3)

1. Establish Neighbor Adjacencies
2. Exchange Link-State Advertisements
3. Build the Link-State Database
4. Execute the SPF Algorithm
5. Choose the Best Route

Table of Contents

Single-Area and Multiarea OSPF (1.1.4)

Multiarea OSPF (1.1.5)

OSPFv3 (1.1.6)

OSPF Packets (1.2)

Types of OSPF Packets (1.2.2)

Link-State Updates (1.2.3)

Hello Packet (1.2.4)

OSPF Operation (1.3)

OSPF Operational States (1.3.2)

Establish Neighbor Adjacencies (1.3.3)

1. Down State to Init State
2. The Init State
3. Two-Way State
4. Elect the DR and BDR

Synchronizing OSPF Databases (1.3.4)

1. Decide First Router
2. Exchange DBDs
3. Send an LSR

The Need for a DR (1.3.5)

LSA Flooding with a DR (1.3.6)

- Flooding LSAs
- LSAs and DR

Summary (1.4)

OSPF Features and Characteristics

OSPF Packets

OSPF Operation

Practice

Check Your Understanding

Chapter 2 Single-Area OSPFv2 Configuration

Objectives

Table of Contents

Key Terms

Introduction (2.0)

OSPF Router ID (2.1)

OSPF Reference Topology (2.1.1)

Router Configuration Mode for OSPF (2.1.2)

Router IDs (2.1.3)

Router ID Order of Precedence (2.1.4)

Configure a Loopback Interface as the Router ID (2.1.5)

Explicitly Configure a Router ID (2.1.6)

Modify a Router ID (2.1.7)

Point-to-Point OSPF Networks (2.2)

The network Command Syntax (2.2.1)

The Wildcard Mask (2.2.2)

Configure OSPF Using the network Command (2.2.4)

Configure OSPF Using the ip ospf Command (2.2.6)

Passive Interface (2.2.8)

Configure Passive Interfaces (2.2.9)

OSPF Point-to-Point Networks (2.2.11)

Loopbacks and Point-to-Point Networks (2.2.12)

Multiaccess OSPF Networks (2.3)

OSPF Network Types (2.3.1)

OSPF Designated Router (2.3.2)

OSPF Multiaccess Reference Topology (2.3.3)

Verify OSPF Router Roles (2.3.4)

R1 DROTHER

R2 BDR

R3 DR

Verify DR/BDR Adjacencies (2.3.5)

R1 Adjacencies

R2 Adjacencies

Table of Contents

R3 Adjacencies

Default DR/BDR Election Process (2.3.6)

DR Failure and Recovery (2.3.7)

R3 Fails

R3 Rejoins Network

R4 Joins Network

R2 Fails

The ip ospf priority Command (2.3.8)

Configure OSPF Priority (2.3.9)

Modify Single-Area OSPFv2 (2.4)

Cisco OSPF Cost Metric (2.4.1)

Adjust the Reference Bandwidth (2.4.2)

OSPF Accumulates Costs (2.4.3)

Manually Set OSPF Cost Value (2.4.4)

Test Failover to Backup Route (2.4.5)

Hello Packet Intervals (2.4.7)

Verify Hello and Dead Intervals (2.4.8)

Modify OSPFv2 Intervals (2.4.9)

Default Route Propagation (2.5)

Propagate a Default Static Route in OSPFv2 (2.5.1)

Verify the Propagated Default Route (2.5.2)

Verify Single-Area OSPFv2 (2.6)

Verify OSPF Neighbors (2.6.1)

Verify OSPF Protocol Settings (2.6.2)

Verify OSPF Process Information (2.6.3)

Verify OSPF Interface Settings (2.6.4)

Summary (2.7)

OSPF Router ID

Point-to-Point OSPF Networks

OSPF Network Types

Table of Contents

Modify Single-Area OSPFv2

Default Route Propagation

Verify Single-Area OSPFv2

Practice

Check Your Understanding

Chapter 3 Network Security Concepts

Objectives

Key Terms

Introduction

Ethical Hacking Statement (3.0.3)

Current State of Cybersecurity (3.1)

Current State of Affairs (3.1.1)

Vectors of Network Attacks (3.1.2)

Data Loss (3.1.3)

Threat Actors (3.2)

The Hacker (3.2.1)

Evolution of Hackers (3.2.2)

Cyber Criminals (3.2.3)

Hacktivists (3.2.4)

State-Sponsored Hackers (3.2.5)

Threat Actor Tools (3.3)

Introduction to Attack Tools (3.3.2)

Evolution of Security Tools (3.3.3)

Attack Types (3.3.4)

Malware (3.4)

Overview of Malware (3.4.1)

Viruses and Trojan Horses (3.4.2)

Other Types of Malware (3.4.3)

Table of Contents

Common Network Attacks (3.5)

Overview of Network Attacks (3.5.1)

Reconnaissance Attacks (3.5.3)

Access Attacks (3.5.5)

Trust Exploitation Example

Port Redirection Example

Man-in-the-Middle Attack Example

Buffer Overflow Attack

Social Engineering Attacks (3.5.6)

DoS and DDoS Attacks (3.5.9)

DoS Attack

DDoS Attack

IP Vulnerabilities and Threats (3.6)

IPv4 and IPv6 (3.6.2)

ICMP Attacks (3.6.3)

Amplification and Reflection Attacks (3.6.5)

Address Spoofing Attacks (3.6.6)

TCP and UDP Vulnerabilities (3.7)

TCP Segment Header (3.7.1)

TCP Services (3.7.2)

TCP Attacks (3.7.3)

TCP SYN Flood Attack

TCP Reset Attack

TCP Session Hijacking

UDP Segment Header and Operation (3.7.4)

UDP Attacks (3.7.5)

UDP Flood Attacks

IP Services

ARP Vulnerabilities (3.8.1)

ARP Cache Poisoning (3.8.2)

Table of Contents

ARP Request

ARP Reply

Spoofed Gratuitous ARP Replies

DNS Attacks (3.8.4)

DNS Open Resolver Attacks

DNS Stealth Attacks

DNS Domain Shadowing Attacks

DNS Tunneling (3.8.5)

DHCP (3.8.6)

DHCP Attacks (3.8.7)

1. Client Broadcasts DHCP Discovery Messages

2. DHCP Servers Respond with Offers

3. Client Accepts Rogue DHCP Request

4. Rogue DHCP Acknowledges the Request

Network Security Best Practices (3.9)

Confidentiality, Integrity, and Availability (3.9.1)

The Defense-in-Depth Approach (3.9.2)

Firewalls (3.9.3)

IPS (3.9.4)

Content Security Appliances (3.9.5)

Cisco Email Security Appliance (ESA)

Cisco Web Security Appliance (WSA)

Cryptography (3.10)

Securing Communications (3.10.2)

Data Integrity (3.10.3)

Hash Functions (3.10.4)

MD5 with 128-Bit Digest

SHA Hashing Algorithm

SHA-2

SHA-3

Origin Authentication (3.10.5)

Table of Contents

HMAC Hashing Algorithm

Creating the HMAC Value

Verifying the HMAC Value

Cisco Router HMAC Example

Data Confidentiality (3.10.6)

Symmetric Encryption (3.10.7)

Asymmetric Encryption (3.10.8)

Diffie-Hellman (3.10.9)

Summary (3.11)

Current State of Cybersecurity

Threat Actors

Threat Actor Tools

Malware

Common Network Attacks

IP Vulnerabilities and Threats

TCP and UDP Vulnerabilities

IP Services

Network Security Best Practices

Cryptography

Practice

Check Your Understanding

Chapter 4 ACL Concepts

Objectives

Key Terms

Introduction (4.0)

Purpose of ACLs (4.1)

What Is an ACL? (4.1.1)

Packet Filtering (4.1.2)

ACL Operation (4.1.3)

Table of Contents

Wildcard Masks in ACLs (4.2)

Wildcard Mask Overview (4.2.1)

Wildcard Mask Types (4.2.2)

Wildcard to Match a Host

Wildcard Mask to Match an IPv4 Subnet

Wildcard Mask to Match an IPv4 Address Range

Wildcard Mask Calculation (4.2.3)

Example 1

Example 2

Example 3

Example 4

Wildcard Mask Keywords (4.2.4)

Guidelines for ACL Creation (4.3)

Limited Number of ACLs per Interface (4.3.1)

ACL Best Practices (4.3.2)

Types of IPv4 ACLs (4.4)

Standard and Extended ACLs (4.4.1)

Numbered and Named ACLs (4.4.2)

Numbered ACLs

Named ACLs

Where to Place ACLs (4.4.3)

Standard ACL Placement Example (4.4.4)

Extended ACL Placement Example (4.4.5)

Summary (4.5)

Purpose of ACLs

Wildcard Masks

Guidelines for ACL Creation

Types of IPv4 ACLs

Practice

Check Your Understanding Questions

Table of Contents

Chapter 5 ACLs for IPv4 Configuration

Objectives

Key Term

Introduction (5.0)

Configure Standard IPv4 ACLs (5.1)

Create an ACL (5.1.1)

Numbered Standard IPv4 ACL Syntax (5.1.2)

Named Standard IPv4 ACL Syntax (5.1.3)

Apply a Standard IPv4 ACL (5.1.4)

Numbered Standard IPv4 ACL Example (5.1.5)

Named Standard IPv4 ACL Example (5.1.6)

Modify IPv4 ACLs (5.2)

Two Methods to Modify an ACL (5.2.1)

Text Editor Method (5.2.2)

Sequence Numbers Method (5.2.3)

Modify a Named ACL Example (5.2.4)

ACL Statistics (5.2.5)

Secure VTY Ports with a Standard IPv4 ACL (5.3)

The access-class Command (5.3.1)

Secure VTY Access Example (5.3.2)

Verify the VTY Port Is Secured (5.3.3)

Configure Extended IPv4 ACLs (5.4)

Extended ACLs (5.4.1)

Numbered Extended IPv4 ACL Syntax (5.4.2)

Protocols and Ports (5.4.3)

Protocol Options

Port Keyword Options

Protocols and Port Numbers Configuration Examples (5.4.4)

Apply a Numbered Extended IPv4 ACL (5.4.5)

Table of Contents

TCP Established Extended ACL (5.4.6)

Named Extended IPv4 ACL Syntax (5.4.7)

Named Extended IPv4 ACL Example (5.4.8)

Edit Extended ACLs (5.4.9)

Another Named Extended IPv4 ACL Example (5.4.10)

Verify Extended ACLs (5.4.11)

show ip interface

show access-lists

show running-config

Summary (5.5)

Configure Standard IPv4 ACLs

Modify IPv4 ACLs

Secure VTY Ports with a Standard IPv4 ACL

Configure Extended IPv4 ACLs

Practice

Check Your Understanding Questions

Chapter 6 NAT for IPv4

Objectives

Key Terms

Introduction (6.0)

NAT Characteristics (6.1)

IPv4 Private Address Space (6.1.1)

What Is NAT? (6.1.2)

How NAT Works (6.1.3)

NAT Terminology (6.1.4)

Inside Local

Inside Global

Outside Global

Outside Local

Types of NAT (6.2)

Table of Contents

Static NAT (6.2.1)

Dynamic NAT (6.2.2)

Port Address Translation (6.2.3)

Next Available Port (6.2.4)

NAT and PAT Comparison (6.2.5)

NAT

PAT

Packets Without a Layer 4 Segment (6.2.6)

NAT Advantages and Disadvantages (6.3)

Advantages of NAT (6.3.1)

Disadvantages of NAT (6.3.2)

Static NAT (6.4)

Static NAT Scenario (6.4.1)

Configure Static NAT (6.4.2)

Analyze Static NAT (6.4.3)

Verify Static NAT (6.4.4)

Dynamic NAT (6.5)

Dynamic NAT Scenario (6.5.1)

Configure Dynamic NAT (6.5.2)

Analyze Dynamic NAT Inside to Outside (6.5.3)

Analyze Dynamic NAT Outside to Inside (6.5.4)

Verify Dynamic NAT (6.5.5)

PAT (6.6)

PAT Scenario (6.6.1)

Configure PAT to Use a Single IPv4 Address (6.6.2)

Configure PAT to Use an Address Pool (6.6.3)

Analyze PAT PC to Server (6.6.4)

Analyze PAT Server to PC (6.6.5)

Verify PAT (6.6.6)

NAT64 (6.7)

Table of Contents

NAT for IPv6? (6.7.1)

NAT64 (6.7.2)

Summary (6.8)

NAT Characteristics

Types of NAT

NAT Advantages and Disadvantages

Static NAT

Dynamic NAT

PAT

NAT64

Practice

Check Your Understanding Questions

Chapter 7 WAN Concepts

Objectives

Key Terms

Introduction (7.0)

Purpose of WANs (7.1)

LANs and WANs (7.1.1)

Private and Public WANs (7.1.2)

WAN Topologies (7.1.3)

Point-to-Point Topology

Hub-and-Spoke Topology

Dual-homed Topology

Fully Meshed Topology

Partially Meshed Topology

Carrier Connections (7.1.4)

Single-Carrier WAN Connection

Dual-Carrier WAN Connection

Evolving Networks (7.1.5)

Small Network

Table of Contents

Campus Network

Branch Network

Distributed Network

WAN Operations (7.2)

WAN Standards (7.2.1)

WANs in the OSI Model (7.2.2)

Layer 1 Protocols

Layer 2 Protocols

Common WAN Terminology (7.2.3)

WAN Devices (7.2.4)

Serial Communication (7.2.5)

Circuit-Switched Communication (7.2.6)

Packet-Switched Communications (7.2.7)

SDH, SONET, and DWDM (7.2.8)

Traditional WAN Connectivity (7.3)

Traditional WAN Connectivity Options (7.3.1)

Common WAN Terminology (7.3.2)

Circuit-Switched Options (7.3.3)

Public Service Telephone Network (PSTN)

Integrated Services Digital Network (ISDN)

Packet-Switched Options (7.3.4)

Frame Relay

Asynchronous Transfer Mode (ATM)

Modern WAN Connectivity (7.4)

Modern WANs (7.4.1)

Modern WAN Connectivity Options (7.4.2)

Dedicated Broadband

Packet-Switched

Internet-Based Broadband

Ethernet WAN (7.4.3)

MPLS (7.4.4)

Table of Contents

Internet-Based Connectivity (7.5)

Internet-Based Connectivity Options (7.5.1)

Wired Options

Wireless Options

DSL Technology (7.5.2)

DSL Connections (7.5.3)

DSL and PPP (7.5.4)

Host with PPPoE Client

Router PPPoE Client

Cable Technology (7.5.5)

Optical Fiber (7.5.6)

Wireless Internet-Based Broadband (7.5.7)

Municipal Wi-Fi

Cellular

Satellite Internet

WiMAX

VPN Technology (7.5.8)

ISP Connectivity Options (7.5.9)

Single-Homed

Dual-Homed

Multihomed

Dual-Multihomed

Broadband Solution Comparison (7.5.10)

Summary (7.6)

Purpose of WANs

WAN Operations

Traditional WAN Connectivity

Modern WAN Connectivity

Internet-Based Connectivity

Practice

Check Your Understanding Questions

Table of Contents

Chapter 8 VPN and IPsec Concepts

Objectives

Key Terms

Introduction (8.0)

VPN Technology (8.1)

Virtual Private Networks (8.1.1)

VPN Benefits (8.1.2)

Site-to-Site and Remote-Access VPNs (8.1.3)

Site-to-Site VPN

Remote-Access VPN

Enterprise and Service Provider VPNs (8.1.4)

Types of VPNs (8.2)

Remote-Access VPNs (8.2.1)

SSL VPNs (8.2.2)

Site-to-Site IPsec VPNs (8.2.3)

GRE over IPsec (8.2.4)

Dynamic Multipoint VPNs (8.2.5)

IPsec Virtual Tunnel Interface (8.2.6)

Service Provider MPLS VPNs (8.2.7)

IPsec (8.3)

IPsec Technologies (8.3.2)

IPsec Protocol Encapsulation (8.3.3)

Confidentiality (8.3.4)

Integrity (8.3.5)

Authentication (8.3.6)

Secure Key Exchange with Diffie-Hellman (8.3.7)

Summary (8.4)

VPN Technology

Types of VPNs

Table of Contents

IPsec

Practice

Check Your Understanding Questions

Chapter 9 QoS Concepts

Objectives

Key Terms

Introduction (9.0)

Network Transmission Quality (9.1)

Prioritizing Traffic (9.1.2)

Bandwidth, Congestion, Delay, and Jitter (9.1.3)

Packet Loss (9.1.4)

Traffic Characteristics (9.2)

Network Traffic Trends (9.2.2)

Voice (9.2.3)

Video (9.2.4)

Data (9.2.5)

Queuing Algorithms (9.3)

Queuing Overview (9.3.2)

First-In, First Out (9.3.3)

Weighted Fair Queuing (WFQ) (9.3.4)

Limitations of WFQ

Class-Based Weighted Fair Queuing (CBWFQ) (9.3.5)

Low Latency Queuing (LLQ) (9.3.6)

QoS Models (9.4)

Selecting an Appropriate QoS Policy Model (9.4.2)

Best Effort (9.4.3)

Integrated Services (9.4.4)

Differentiated Services (9.4.5)

Table of Contents

QoS Implementation Techniques (9.5)

Avoiding Packet Loss (9.5.2)

QoS Tools (9.5.3)

Classification and Marking (9.5.4)

Marking at Layer 2 (9.5.5)

Marking at Layer 3 (9.5.6)

Type of Service and Traffic Class Field (9.5.7)

DSCP Values (9.5.8)

Class Selector Bits (9.5.9)

Trust Boundaries (9.5.10)

Congestion Avoidance (9.5.11)

Shaping and Policing (9.5.12)

QoS Policy Guidelines (9.5.13)

Summary (9.6)

Network Transmission Quality

Traffic Characteristics

Queuing Algorithms

QoS Models

QoS Implementation Techniques

Practice

Check Your Understanding Questions

Chapter 10 Network Management

Objectives

Key Terms

Introduction (10.0)

Device Discovery with CDP (10.1)

CDP Overview (10.1.1)

Configure and Verify CDP (10.1.2)

Table of Contents

Discover Devices by Using CDP (10.1.3)

Device Discovery with LLDP (10.2)

LLDP Overview (10.2.1)

Configure and Verify LLDP (10.2.2)

Discover Devices by Using LLDP (10.2.3)

NTP (10.3)

Time and Calendar Services (10.3.1)

NTP Operation (10.3.2)

Stratum 0

Stratum 1

Stratum 2 and Lower

Configure and Verify NTP (10.3.3)

SNMP

Introduction to SNMP (10.4.1)

SNMP Operation (10.4.2)

SNMP Agent Traps (10.4.3)

SNMP Versions (10.4.4)

Community Strings (10.4.6)

MIB Object ID (10.4.7)

SNMP Polling Scenario (10.4.8)

SNMP Object Navigator (10.4.9)

Syslog (10.5)

Introduction to Syslog (10.5.1)

Syslog Operation (10.5.2)

Syslog Message Format (10.5.3)

Syslog Facilities (10.5.4)

Configure Syslog Timestamp (10.5.5)

Router and Switch File Maintenance (10.6)

Router File Systems (10.6.1)

Table of Contents

The Flash File System

The NVRAM File System

Switch File Systems (10.6.2)

Use a Text File to Back Up a Configuration (10.6.3)

Use a Text File to Restore a Configuration (10.6.4)

Use TFTP to Back Up and Restore a Configuration (10.6.5)

USB Ports on a Cisco Router (10.6.6)

Use USB to Back Up and Restore a Configuration (10.6.7)

Restore Configurations with a USB Flash Drive

Password Recovery Procedures (10.6.8)

Password Recovery Example (10.6.9)

Step 1. Enter the ROMMON mode

Step 2. Change the configuration register

Step 3. Copy the startup-config to the running-config

Step 4. Change the password

Step 5. Save the running-config as the new startup-config

Step 6. Reload the device

IOS Image Management

TFTP Servers as a Backup Location (10.7.2)

Backup IOS Image to TFTP Server Example (10.7.3)

Step 1. Ping the TFTP server

Step 2. Verify image size in flash

Step 3. Copy the image to the TFTP server

Copy an IOS Image to a Device Example (10.7.4)

Step 1. Ping the TFTP server

Step 2. Verify the amount of free flash

Step 3. Copy the new IOS image to flash

The boot system Command (10.7.5)

Summary (10.8)

Device Discovery with CDP

Device Discovery with LLDP

Table of Contents

NTP

SNMP

Syslog

Router and Switch File Maintenance

IOS Image Management

Practice

Check Your Understanding Questions

Chapter 11 Network Design

Objectives

Key Terms

Introduction (11.0)

Hierarchical Networks (11.1)

The Need to Scale the Network (11.1.2)

Borderless Switched Networks (11.1.3)

Hierarchy in the Borderless Switched Network (11.1.4)

Three-Tier Model

Two-Tier Model

Access, Distribution, and Core Layer Functions (11.1.5)

Access Layer

Distribution Layer

Core Layer

Three-Tier and Two-Tier Examples (11.1.6)

Three-Tier Example

Two-Tier Example

Role of Switched Networks (11.1.7)

Scalable Networks (11.2)

Design for Scalability (11.2.1)

Redundant Links

Multiple Links

Scalable Routing Protocol

Table of Contents

Wireless Connectivity

Plan for Redundancy (11.2.2)

Reduce Failure Domain Size (11.2.3)

Edge Router

AP1

S1

S2

S3

Limiting the Size of Failure Domains

Switch Block Deployment

Increase Bandwidth (11.2.4)

Expand the Access Layer (11.2.5)

Tune Routing Protocols (11.2.6)

Switch Hardware (11.3)

Switch Platforms (11.3.1)

Campus LAN Switches

Cloud-Managed Switches

Data Center Switches

Service Provider Switches

Virtual Networking

Switch Form Factors (11.3.2)

Fixed Configuration Switches

Modular Configuration Switches

Stackable Configuration Switches

Thickness

Port Density (11.3.3)

Forwarding Rates (11.3.4)

Power over Ethernet (11.3.5)

Switch

IP Phone

WAP

Cisco Catalyst 2960-C

Table of Contents

Multilayer Switching (11.3.6)

Business Considerations for Switch Selection (11.3.7)

Router Hardware (11.4)

Router Requirements (11.4.1)

Cisco Routers (11.4.2)

Branch Routers

Network Edge Routers

Service Provider Routers

Industrial

Router Form Factors (11.4.3)

Cisco 900 Series

ASR 9000 and 1000 Series

5500 Series

Cisco 800

Fixed Configuration or Modular

Summary (11.5)

Hierarchical Networks

Scalable Networks

Switch Hardware

Router Hardware

Practice

Check Your Understanding Questions

Chapter 12 Network Troubleshooting

Objectives

Key Terms

Introduction (12.0)

Network Documentation (12.1)

Documentation Overview (12.1.1)

Table of Contents

Network Topology Diagrams (12.1.2)

- Physical Topology

- Logical IPv4 Topology

- Logical IPv6 Topology

Network Device Documentation (12.1.3)

- Router Device Documentation

- LAN Switch Device Documentation

- End-System Documentation Files

Establish a Network Baseline (12.1.4)

Step 1 Determine What Types of Data to Collect (12.1.5)

Step 2 Identify Devices and Ports of Interest (12.1.6)

Step 3 Determine the Baseline Duration (12.1.7)

Data Measurement (12.1.8)

Troubleshooting Process (12.2)

General Troubleshooting Procedures (12.2.1)

Seven-Step Troubleshooting Process (12.2.2)

- Define the Problem

- Gather Information

- Analyze Information

- Eliminate Possible Causes

- Propose Hypothesis

- Test Hypothesis

- Solve the Problem

Question End Users (12.2.3)

Gather Information (12.2.4)

Troubleshooting with Layered Models (12.2.5)

Structured Troubleshooting Methods (12.2.6)

- Bottom-Up

- Top-Down

- Divide-and-Conquer

- Follow-the-Path

- Substitution

Table of Contents

Comparison

Educated Guess

Guidelines for Selecting a Troubleshooting Method (12.2.7)

Troubleshooting Tools (12.3)

Software Troubleshooting Tools (12.3.1)

Network Management System Tools

Knowledge Bases

Baselining Tools

Protocol Analyzers (12.3.2)

Hardware Troubleshooting Tools (12.3.3)

Digital Multimeters

Cable Testers

Cable Analyzers

Portable Network Analyzers

Cisco Prime NAM

Syslog Server as a Troubleshooting Tool (12.3.4)

Symptoms and Causes of Network Problems (12.4)

Physical Layer Troubleshooting (12.4.1)

Data Link Layer Troubleshooting (12.4.2)

Network Layer Troubleshooting (12.4.3)

Transport Layer Troubleshooting ACLs (12.4.4)

Transport Layer Troubleshooting NAT for IPv4 (12.4.5)

Application Layer Troubleshooting (12.4.6)

Troubleshooting IP Connectivity (12.5)

Components of Troubleshooting End-to-End Connectivity (12.5.1)

End-to-End Connectivity Problem Initiates Troubleshooting (12.5.2)

IPv4 ping

IPv4 traceroute

IPv6 ping and traceroute

Table of Contents

Step 1 Verify the Physical Layer (12.5.3)

- Input Queue Drops

- Output Queue Drops

- Input Errors

- Output Errors

Step 2 Check for Duplex Mismatches (12.5.4)

- Troubleshooting Example

Step 3 Verify Addressing on the Local Network (12.5.5)

- Windows IPv4 ARP Table

- Windows IPv6 Neighbor Table

- IOS IPv6 Neighbor Table

- Switch MAC Address Table

- Troubleshoot VLAN Assignment Example (12.5.6)

- Check the ARP Table

- Check the Switch MAC Table

- Correct the VLAN Assignment

Step 4 Verify Default Gateway (12.5.7)

- Troubleshooting IPv4 Default Gateway Example

- R1 Routing Table

- PC1 Routing Table

- Troubleshoot IPv6 Default Gateway Example (12.5.8)

- R1 Routing Table

- PC1 Addressing

- Check R1 Interface Settings

- Correct R1 IPv6 Routing

- Verify PC1 Has an IPv6 Default Gateway

Step 5 Verify Correct Path (12.5.9)

- Troubleshooting Example

Step 6 Verify the Transport Layer (12.5.10)

- Troubleshooting Example

Step 7 Verify ACLs (12.5.11)

- Troubleshooting Example

- show ip access-lists

Table of Contents

show ip interfaces

Correct the Issue

Step 8 Verify DNS (12.5.12)

Summary (12.6)

Network Documentation

Troubleshooting Process

Troubleshooting Tools

Symptoms and Causes of Network Problems

Troubleshooting IP Connectivity

Practice

Check Your Understanding Questions

Chapter 13 Network Virtualization

Objectives

Key Terms

Introduction (13.0)

Cloud Computing (13.1)

Cloud Overview (13.1.2)

Cloud Services (13.1.3)

Cloud Models (13.1.4)

Cloud Computing Versus Data Center (13.1.5)

Virtualization (13.2)

Cloud Computing and Virtualization (13.2.1)

Dedicated Servers (13.2.2)

Server Virtualization (13.2.3)

Advantages of Virtualization (13.2.4)

Abstraction Layers (13.2.5)

Type 2 Hypervisors (13.2.6)

Virtual Network Infrastructure (13.3)

Table of Contents

Type 1 Hypervisors (13.3.1)

Installing a VM on a Hypervisor (13.3.2)

The Complexity of Network Virtualization (13.3.3)

Software-Defined Networking (13.4)

Control Plane and Data Plane (13.4.2)

Layer 3 Switch and CEF

SDN and Central Controller

Management Plane

Network Virtualization Technologies (13.4.3)

Traditional and SDN Architectures (13.4.4)

Controllers (13.5)

SDN Controller and Operations (13.5.1)

Core Components of ACI (13.5.3)

Spine-Leaf Topology (13.5.4)

SDN Types (13.5.5)

Device-Based SDN

Controller-Based SDN

Policy-Based SDN

APIC-EM Features (13.5.6)

APIC-EM Path Trace (13.5.7)

Summary (13.6)

Cloud Computing

Virtualization

Virtual Network Infrastructure

Software-Defined Networking

Controllers

Practice

Check Your Understanding Questions

Chapter 14 Network Automation

Table of Contents

Objectives

Key Terms

Introduction (14.0)

Automation Overview (14.1)

 The Increase in Automation (14.1.2)

 Thinking Devices (14.1.3)

Data Formats (14.2)

 The Data Formats Concept (14.2.2)

 Data Format Rules (14.2.3)

 Compare Data Formats (14.2.4)

 JSON Data Format (14.2.5)

 JSON Syntax Rules (14.2.6)

 YAML Data Format (14.2.7)

 XML Data Format (14.2.8)

APIs (14.3)

 The API Concept (14.3.2)

 An API Example (14.3.3)

 Open, Internal, and Partner APIs (14.3.4)

 Types of Web Service APIs (14.3.5)

REST (14.4)

 REST and RESTful API (14.4.2)

 RESTful Implementation (14.4.3)

 URI, URN, and URL (14.4.4)

 Anatomy of a RESTful Request (14.4.5)

 RESTful API Applications (14.4.6)

 Developer Website

 Postman

 Python

 Network Operating Systems

Configuration Management Tools (14.5)

Table of Contents

Traditional Network Configuration (14.5.2)

Network Automation (14.5.3)

Configuration Management Tools (14.5.4)

Compare Ansible, Chef, Puppet, and SaltStack (14.5.5)

IBN and Cisco DNA Center (14.6)

Intent-Based Networking Overview (14.6.2)

Network Infrastructure as Fabric (14.6.3)

Cisco Digital Network Architecture (DNA) (14.6.4)

Cisco DNA Center (14.6.5)

Summary (14.7)

Automation Overview

Data Formats

APIs

REST

Configuration and Management

IBN and Cisco DNA Center

Practice

Check Your Understanding Questions

Appendix A Answers to the Check Your Understanding Questions

Glossary

A

B

C

D

E

F

G

H

Table of Contents

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z

Index