INFOSECTRAIN

CISCO CERTIFIED NETWORK ASSOCIATE

CCNA

200-301 CERTIFICATION TRAINING

www.infosectrain.com

INFOSECTRAIN

CCNA COURSE HIGHLIGHTS

40 Hrs of
Instructor-Led Training

Blended learning
delivery model

Certified and
highly skilled trainers

Get certified
at an affordable price

Access to the
recorded sessions

CCNA Course Description

Overview

The CISCO Certified Network Associate (CCNA) certification serves as a stepping stone for professionals willing to make a career in networking or IT technology. CCNA certification training course from InfosecTrain provides a comprehensive introduction to the fundamental concepts and principles of computer networking. It covers the TCP/IP networking model's history and structure. Participants will gain an understanding of the application, transport, network, data link, and physical layers of TCP/IP. The course also explores topics such as IP addressing, routing, and error recovery. The OSI and TCP/IP models will also be compared. By the end of the course, participants will have a solid foundation in networking fundamentals and be able to apply their knowledge to real-world scenarios.

Why CCNA Certification Training Course with InfosecTrain

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our CCNA Certification Training course will equip you with fundamental concepts and principles of computer networking.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS and recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.
- **Expert Career Guidance:** Free Career Guidance and support from industry experts.

www.infosectrain.com

INFOSECTRAIN

Target Audience

- Network Administrators
- Network Support Engineer
- System Administrators
- Network Security Specialists
- Network Security Operators
- Anyone willing to make a career in Network Security

Pre-Requisites

While there are no mandatory prerequisites for the CCNA examination, it is recommended to possess a foundational understanding of the following concepts:

- IP Addressing
- Networking Fundamentals

Exam Information

Exam Name	Cisco Certified Network Associate (CCNA)
Exam Code	200-301
Exam Duration	120 Minutes
Number of Questions	120
Passing Score	849 (on a scale of 1000)
Exam Languages	English, Japanese

INFOSECTRAIN

Course Objectives

- **Domain 1:** Network Fundamentals (20%)
- **Domain 2:** Network Access (20%)
- **Domain 3:** IP Connectivity (25%)
- **Domain 4:** IP Services (10%)
- **Domain 5:** Security Fundamentals (15%)
- **Domain 6:** Automation and Programmability (10%)

www.infosectrain.com

INFOSECTRAIN

COURSE CONTENT

Introduction to Networking

Chapter 1: Introduction to TCP/IP Networking

- TCP/IP Networking Model
- History Leading to TCP/IP
- Overview of the TCP/IP Networking Model
- TCP/IP Application Layer
- HTTP Overview
- HTTP Protocol Mechanisms
- TCP/IP Transport Layer
- TCP Error Recovery Basics
- Same-Layer and Adjacent-Layer Interactions
- TCP/IP Network Layer
- Internet Protocol and the Postal Service
- Internet Protocol Addressing Basics
- IP Routing Basics
- TCP/IP Data-Link and Physical Layers
- Data Encapsulation Terminology
- Names of TCP/IP Messages
- OSI Networking Model and Terminology
- Comparing OSI and TCP/IP Layer Names and Numbers
- OSI Data Encapsulation Terminology

Chapter 2: Fundamentals of Ethernet LANs

- An Overview of LANs
- SOHO LANs
- Enterprise LANs
- The Variety of Ethernet Physical Layer Standards
- Consistent Behavior over All Links Using the Ethernet Data-Link Layer
- Building Physical Ethernet LANs with UTP
- Transmitting Data Using Twisted Pairs
- Breaking Down a UTP Ethernet Link
- UTP Cabling Pinouts for 10BASE-T and 100BASE-T
- Straight-Through Cable Pinout
- Choosing the Right Cable Pinouts
- UTP Cabling Pinouts for 1000BASE-T
- Building Physical Ethernet LANs with Fiber
- Fiber Cabling Transmission Concepts
- Using Fiber with Ethernet
- Sending Data in Ethernet Networks
- Ethernet Data-Link Protocols
- Ethernet Addressing
- Identifying Network Layer Protocols with the Ethernet Type Field
- Error Detection with FCS
- Sending Ethernet Frames with Switches and Hubs
- Sending in Modern Ethernet LANs Using Full Duplex
- Using Half Duplex with LAN Hubs

Chapter 3: Fundamentals of WANs and IP Routing

- Wide-Area Networks
- Leased-Line WANs
- Physical Details of Leased Lines
- HDLC Data-Link Details of Leased Lines
- How Routers Use a WAN Data Link
- Ethernet as a WAN Technology
- Ethernet WANs That Create a Layer 2 Service
- How Routers Route IP Packets Using Ethernet Emulation
- IP Routing
- Network Layer Routing (Forwarding) Logic
- Host Forwarding Logic: Send the Packet to the Default Router
- R1 and R2's Logic: Routing Data Across the Network
- R3's Logic: Delivering Data to the End Destination
- How Network Layer Routing Uses LANs and WAN
- How IP Addressing Helps IP Routing
- Rules for Groups of IP Addresses (Networks and Subnets)
- The IP Header
- How IP Routing Protocols Help IP Routing
- Other Network Layer Features
- Using Names and the Domain Name System
- The Address Resolution Protocol
- ICMP Echo and the ping Command

INFOSECTRAIN

Implementing Ethernet LANs

Chapter 4: Using the Command-Line Interface

- Accessing the Cisco Catalyst Switch CLI
- Cisco Catalyst Switches
- Accessing the Cisco IOS CLI
- Cabling the Console Connection
- Accessing the CLI with Telnet and SSH
- User and Enable (Privileged) Modes
- Password Security for CLI Access from the Console
- CLI Help Features
- The debug and show Commands
- Configuring Cisco IOS Software
- Configuration Submodels and Contexts
- Storing Switch Configuration Files
- Copying and Erasing Configuration Files

Chapter 5: Analysing Ethernet LAN Switching

- LAN Switching Concepts
- Overview of Switching Logic
- Forwarding Known Unicast Frames
- Learning MAC Addresses
- Flooding Unknown Unicast and Broadcast Frames
- Avoiding Loops Using Spanning Tree Protocol
- LAN Switching Summary
- Verifying and Analyzing Ethernet Switching
- Demonstrating MAC Learning

- Switch Interfaces
- Finding Entries in the MAC Address Table
- Managing the MAC Address Table (Aging, Clearing)
- MAC Address Tables with Multiple Switches

Chapter 6: Configuring Basic Switch Management

- Securing the Switch CLI
- Securing User Mode and Privileged Mode with Simple Passwords
- Securing User Mode Access with Local Usernames and Passwords
- Securing User Mode Access with External Authentication Servers
- Securing Remote Access with Secure Shell
- Enabling IPv4 for Remote Access
- Host and Switch IP Settings
- Configuring IPv4 on a Switch
- Configuring a Switch to Learn Its IP Address with DHCP
- Verifying IPv4 on a Switch
- Miscellaneous Settings Useful in the Lab
- History Buffer Commands
- The logging synchronous, exec-timeout, and no ip domain-lookup Commands

Chapter 7: Configuring and Verifying Switch Interfaces

- Configuring Switch Interfaces
- Configuring Speed, Duplex, and Description
- Configuring Multiple Interfaces with the interface range Command
- Administratively Controlling Interface State with shutdown
- Removing Configuration with the no Command
- Auto-negotiation
- Auto-negotiation Under Working Conditions
- Auto-negotiation Results When Only One Node Uses Autonegotiation
- Auto-negotiation and LAN Hubs
- Analyzing Switch Interface Status and Statistics
- Interface Status Codes and Reasons for Nonworking States
- Interface Speed and Duplex Issues
- Common Layer 1 Problem on Working Interfaces

INFOSECTRAIN

Implementing VLANs and STP

Chapter 8: Implementing Ethernet Virtual LANs

- Virtual LAN Concepts
- Creating Multiswitch VLANs Using Trunking
- VLAN Tagging Concepts
- The 802.1Q and ISL VLAN Trunking Protocols
- Forwarding Data Between VLANs
- The Need for Routing Between VLANs
- Routing Packets Between VLANs with a Router
- VLAN and VLAN Trunking Configuration and Verification
- Creating VLANs and Assigning Access VLANs to an Interface
- VLAN Configuration Example 1: Full VLAN Configuration
- VLAN Configuration Example 2: Shorter VLAN Configuration
- VLAN Trunking Protocol
- VLAN Trunking Configuration
- Implementing Interfaces Connected to Phones
- Data and Voice VLAN Concepts
- Data and Voice VLAN Configuration and Verification
- Summary: IP Telephony Ports on Switches
- Troubleshooting VLANs and VLAN Trunks
- Access VLANs Undefined or Disabled
- Mismatched Trunking Operational State
- The Supported VLAN List on Trunks
- Mismatched Native VLAN on a Trunk

Chapter 9: Spanning Tree Protocol Concepts

- STP and RSTP Basics
- The Need for Spanning Tree
- What Spanning Tree Does
- How Spanning Tree Works
- The STP Bridge ID and Hello BPDU
- Electing the Root Switch
- Choosing Each Switch's Root Port
- Choosing the Designated Port on Each LAN Segment
- Configuring to Influence the STP Topology
- Details Specific to STP (and Not RSTP)
- STP Activity When the Network Remains Stable
- STP Timers That Manage STP Convergence
- Changing Interface States with STP
- Rapid STP Concepts
- Comparing STP and RSTP
- RSTP and the Alternate (Root) Port Role
- RSTP States and Processes
- RSTP and the Backup (Designated) Port Role
- RSTP Port Types
- Optional STP Features
- EtherChannel
- PortFast
- BPDU Guard

Chapter 10: RSTP and EtherChannel Configuration

- Understanding RSTP Through Configuration
- The Need for Multiple Spanning Trees
- STP Modes and Standards
- The Bridge ID and System ID Extension
- How Switches Use the Priority and System ID Extension
- RSTP Methods to Support Multiple Spanning Trees
- Other RSTP Configuration Options
- Configuring Layer 2 EtherChannel
- Configuring a Manual Layer 2 EtherChannel
- Configuring Dynamic EtherChannels
- Physical Interface Configuration and EtherChannels
- EtherChannel Load Distribution
- Configuration Options for EtherChannel Load Distribution
- The Effects of the EtherChannel Load Distribution Algorithm

INFOSECTRAIN

IPv4 Addressing

Chapter 11: Perspectives on IPv4 Subnetting

- Introduction to Subnetting
- Subnetting Defined Through a Simple Example
- Operational View Versus Design View of Subnetting
- Analyze Subnetting and Addressing Needs
- Rules About Which Hosts Are in Which Subnet
- Determining the Number of Subnets
- Determining the Number of Hosts per Subnet
- One Size Subnet Fits All—Or Not
- Defining the Size of a Subnet
- One Size Subnet Fits All
- Multiple Subnet Sizes (Variable-Length Subnet Masks)
- One Mask for All Subnets, or More Than One
- Make Design Choices
- Choose a Classful Network
- Public IP Networks
- Growth Exhausts the Public IP Address Space
- Private IP Networks
- Choosing an IP Network During the Design Phase
- Choose the Mask
- Classful IP Networks Before Subnetting
- Borrowing Host Bits to Create Subnet Bits
- Choosing Enough Subnet and Host Bits
- Example Design: 172.16.0.0, 200 Subnets, 200 Hosts
- Masks and Mask Formats
- Build a List of All Subnets
- Plan the Implementation
- Assigning Subnets to Different Locations
- Choose Static and Dynamic Ranges per Subnet

Chapter 12: Analysing Classful IPv4 Networks

- Classful Network Concepts
- IPv4 Network Classes and Related Facts
- The Number and Size of Class A, B, and C Networks
- Address Formats
- Default Masks
- Number of Hosts per Network
- Deriving the Network ID and Related Numbers
- Unusual Network IDs and Network Broadcast Addresses
- Practice with Classful Networks
- Practice Deriving Key Facts Based on an IP Address
- Practice Remembering the Details of Address Classes

Chapter 13: Analyzing Subnet Masks

- Subnet Mask Conversion
- Three Mask Formats
- Converting Between Binary and Prefix Masks
- Converting Between Binary and DDN Masks
- Converting Between Prefix and DDN Masks
- Practice Converting Subnet Masks
- Identifying Subnet Design Choices Using Masks
- Masks Divide the Subnet's Addresses into Two Parts
- Masks and Class Divide Addresses into Three Parts
- Classless and Classful Addressing
- Calculations Based on the IPv4 Address Format
- Practice Analyzing Subnet Masks

Chapter 14: Analyzing Existing Subnets

- Defining a Subnet
- An Example with Network 172.16.0.0 and Four Subnets
- Subnet ID Concepts
- Subnet Broadcast Address
- Range of Usable Addresses
- Analyzing Existing Subnets: Binary
- Finding the Subnet ID: Binary
- Finding the Subnet Broadcast Address: Binary
- Binary Practice Problems
- Shortcut for the Binary Process
- Brief Note About Boolean Math
- Finding the Range of Addresses
- Analyzing Existing Subnets: Decimal
- Analysis with Easy Masks
- Predictability in the Interesting Octet
- Finding the Subnet ID: Difficult Masks
- Resident Subnet Example 1
- Resident Subnet Example 2
- Resident Subnet Practice Problems
- Finding the Subnet Broadcast Address: Difficult Masks
- Subnet Broadcast Example 1
- Subnet Broadcast Example 2
- Subnet Broadcast Address Practice Problems
- Practice Analyzing Existing Subnets
- A Choice: Memorize or Calculate

INFOSECTRAIN

IPv4 Routing

Chapter 15: Operating Cisco Routers

- Installing Cisco Routers
- Installing Enterprise Routers
- Cisco Integrated Services Routers
- Physical Installation
- Installing SOHO Routers
- Enabling IPv4 Support on Cisco Router Interfaces
- Accessing the Router CLI
- Router Interfaces
- Interface Status Codes
- Router Interface IP Addresses
- Bandwidth and Clock Rate on Serial Interfaces
- Router Auxiliary Port

Chapter 16: Configuring IPv4 Addresses and Static Routes

- IP Routing
- IPv4 Routing Process Reference
- An Example of IP Routing
- Host Forwards the IP Packet to the Default Router (Gateway)
- Routing Step 1: Decide Whether to Process the Incoming Frame
- Routing Step 2: De-encapsulation of the IP Packet
- Routing Step 3: Choosing Where to Forward the Packet
- Routing Step 4: Encapsulating the Packet in a New Frame
- Routing Step 5: Transmitting the Frame
- Configuring IP Addresses and Connected Routes
- Connected Routes and the ip address Command
- The ARP Table on a Cisco Router
- Configuring Static Routes
- Static Network Routes
- Static Host Routes
- Floating Static Routes
- Static Default Routes
- Troubleshooting Static Routes
- Troubleshooting Incorrect Static Routes That Appear in the IP Routing Table
- The Static Route Does Not Appear in the IP Routing Table
- The Correct Static Route Appears but Works Poorly
- IP Forwarding with the Longest Prefix Match
- Using show ip route to Find the Best Route
- Using show ip route address to Find the Best Route
- Interpreting the IP Routing Table

Chapter 17: IP Routing in the LAN

- VLAN Routing with Router 802.1Q Trunks
- Configuring ROAS
- Verifying ROAS
- Troubleshooting ROAS
- VLAN Routing with Layer 3 Switch SVIs
- Configuring Routing Using Switch SVIs
- Verifying Routing with SVIs
- Troubleshooting Routing with SVIs
- VLAN Routing with Layer 3 Switch Routed Ports
- Implementing Routed Interfaces on Switches
- Implementing Layer 3 EtherChannels
- Troubleshooting Layer 3 EtherChannels

Chapter 18: Troubleshooting IPv4 Routing

- Problem Isolation Using the Ping Command
- Ping Command Basics
- Strategies and Results When Testing with the Ping Command
- Testing Longer Routes from Near the Source of the Problem
- Using Extended Ping to Test the Reverse Route
- Testing LAN Neighbors with Standard Ping
- Testing LAN Neighbors with Extended Ping
- Testing WAN Neighbors with Standard Ping
- Using Ping with Names and with IP Addresses
- Problem Isolation Using the Traceroute Command
- Traceroute Basics
- How the Traceroute Command Works
- Standard and Extended Traceroute
- Telnet and SSH
- Common Reasons to Use the IOS Telnet and SSH Client
- IOS Telnet and SSH Examples

OSPF

Chapter 19: Understanding OSPF Concepts

- Comparing Dynamic Routing Protocol Features
- Routing Protocol Functions
- Interior and Exterior Routing Protocols
- Comparing IGPs
- IGP Routing Protocol Algorithms
- Metrics
- Other IGP Comparisons
- Administrative Distance
- OSPF Concepts and Operation
- OSPF Overview
- Topology Information and LSAs
- Applying Dijkstra SPF Math to Find the Best Routes
- Becoming OSPF Neighbors
- The Basics of OSPF Neighbors
- Meeting Neighbors and Learning Their Router ID
- Exchanging the LSDB Between Neighbors
- Fully Exchanging LSAs with Neighbors
- Maintaining Neighbors and the LSDB
- Using Designated Routers on Ethernet Links
- Calculating the Best Routes with SPF
- OSPF Areas and LSAs
- OSPF Areas
- How Areas Reduce SPF Calculation Time
- (OSPFv2) Link-State Advertisements
- Router LSAs Build Most of the Intra-Area Topology
- Network LSAs Complete the Intra-Area Topology

Chapter 20: Implementing OSPF

- Implementing Single-Area OSPFv2
- OSPF Single-Area Configuration
- Wildcard Matching with the network Command
- Verifying OSPF Operation
- Verifying OSPF Configuration
- Configuring the OSPF Router ID
- Implementing Multiarea OSPF
- Using OSPFv2 Interface Subcommands
- OSPF Interface Configuration Example
- Verifying OSPF Interface Configuration
- Additional OSPFv2 Features
- OSPF Passive Interfaces
- OSPF Default Routes
- OSPF Metrics (Cost)
- Setting the Cost Directly
- Setting the Cost Based on Interface and Reference Bandwidth
- OSPF Load Balancing

INFOSECTRAIN

Chapter 21: OSPF Network Types and Neighbors

- OSPF Network Types
- The OSPF Broadcast Network Type
- Verifying Operations with Network Type Broadcast
- Configuring to Influence the DR/BDR Election
- The OSPF Point-to-Point Network Type
- OSPF Neighbor Relationships
- OSPF Neighbor Requirements
- Issues That Prevent Neighbor Adjacencies
- Finding Area Mismatches
- Finding Duplicate OSPF Router IDs
- Finding OSPF Hello and Dead Timer Mismatches
- Shutting Down the OSPF Process
- Issues That Allow Adjacencies but Prevent IP Routes
- Mismatched MTU Settings
- Mismatched OSPF Network Types

INFOSECTRAIN

IP Version 6

Chapter 22: Fundamentals of IP Version 6

- Introduction to IPv6
- The Historical Reasons for IPv6
- The IPv6 Protocols
- IPv6 Routing
- IPv6 Routing Protocols
- IPv6 Addressing Formats and Conventions
- Representing Full (Unabbreviated) IPv6 Addresses
- Abbreviating and Expanding IPv6 Addresses
- Abbreviating IPv6 Addresses
- Expanding Abbreviated IPv6 Addresses
- Representing the Prefix Length of an Address
- Calculating the IPv6 Prefix (Subnet ID)
- Finding the IPv6 Prefix
- Working with More Difficult IPv6 Prefix Lengths

Chapter 23: IPv6 Addressing and Subnetting

- Global Unicast Addressing Concepts
- Public and Private IPv6 Addresses
- The IPv6 Global Routing Prefix
- Address Ranges for Global Unicast Addresses
- IPv6 Subnetting Using Global Unicast Addresses
- Deciding Where IPv6 Subnets Are Needed
- The Mechanics of Subnetting IPv6 Global Unicast Addresses

- Listing the IPv6 Subnet Identifier
- List All IPv6 Subnets
- Assign Subnets to the Internetwork Topology
- Assigning Addresses to Hosts in a Subnet
- Unique Local Unicast Addresses
- Subnetting with Unique Local IPv6 Addresses
- The Need for Globally Unique Local Addresses

Chapter 24: Implementing IPv6 Addressing Routers

- Implementing Unicast IPv6 Addresses on Routers
- Static Unicast Address Configuration
- Configuring the Full 128-Bit Address
- Enabling IPv6 Routing
- Verifying the IPv6 Address Configuration
- Generating a Unique Interface ID Using Modified EUI-64
- Dynamic Unicast Address Configuration
- Special Addresses Used by Routers
- Link-Local Addresses
- Link-Local Address Concepts
- Creating Link-Local Addresses on Routers
- Routing IPv6 with Only Link-Local Addresses on an Interface
- IPv6 Multicast Addresses
- Reserved Multicast Addresses
- Multicast Address Scopes
- Solicited-Node Multicast Addresses
- Miscellaneous IPv6 Addresses
- Anycast Addresses
- IPv6 Addressing Configuration Summary

Chapter 25: Implementing IPv6 Routing

- Connected and Local IPv6 Routes
- Rules for Connected and Local Routes
- Example of Connected IPv6 Routes
- Examples of Local IPv6 Routes
- Static IPv6 Routes
- Static Routes Using the Outgoing Interface
- Static Routes Using Next-Hop IPv6 Address
- Example Static Route with a Global Unicast Next-Hop Address
- Example Static Route with a Link-Local Next-Hop Address
- Static Routes over Ethernet Links
- Static Default Routes
- Static IPv6 Host Routes
- Floating Static IPv6 Routes
- Troubleshooting Static IPv6 Routes
- Troubleshooting Incorrect Static Routes That Appear in the IPv6 Routing Table
- The Static Route Does Not Appear in the IPv6 Routing Table
- The Neighbor Discovery Protocol
- Discovering Neighbor Link Addresses with NDP NS and NA
- Discovering Routers with NDP RS and RA
- Using SLAAC with NDP RS and RA
- Discovering Duplicate Addresses Using NDP NS and NA
- NDP Summary

INFOSECTRAIN

Wireless LANs

Chapter 26: Fundamentals of Wireless Networks

- Comparing Wired and Wireless Networks
- Wireless LAN Topologies
- Basic Service Set
- Distribution System
- Extended Service Set
- Independent Basic Service Set
- Other Wireless Topologies
- Repeater
- Workgroup Bridge
- Outdoor Bridge
- Mesh Network
- RF Overview
- Wireless Bands and Channels
- APs and Wireless Standards

Chapter 27: Analysing Cisco Wireless Architectures

- Autonomous AP Architecture
- Cloud-based AP Architecture
- Split-MAC Architectures
- Comparing Wireless LAN Controller Deployments
- Cisco AP Modes

Chapter 28: Securing Wireless Networks

- Anatomy of a Secure Connection
- Authentication
- Message Privacy
- Message Integrity
- Wireless Client Authentication Methods
- Open Authentication
- WEP
- 802.1x/EAP
- LEAP
- EAP-FAST
- PEAP
- EAP-TLS
- Wireless Privacy and Integrity Methods
- TKIP
- CCMP
- GCMP
- WPA, WPA2, and WPA3

Chapter 29: Building a Wireless LAN

- Connecting a Cisco AP
- Accessing a Cisco WLC
- Connecting a Cisco WLC
- Using WLC Ports
- Using WLC Interfaces
- Configuring a WLAN
- Step 1. Configure a RADIUS Server
- Step 2. Create a Dynamic Interface
- Step 3. Create a New WLAN
- Configuring WLAN Security
- Configuring WLAN QoS
- Configuring Advanced WLAN Settings
- Finalizing WLAN Configuration

IP Access Control Lists

Chapter 30: Introduction to TCP/IP Transport and Applications

- TCP/IP Layer 4 Protocols: TCP and UDP
- Transmission Control Protocol
- Multiplexing Using TCP Port Numbers
- Popular TCP/IP Applications
- Connection Establishment and Termination
- Error Recovery and Reliability
- Flow Control Using Windowing
- User Datagram Protocol
- TCP/IP Applications
- Uniform Resource Identifiers
- Finding the Web Server Using DNS
- Transferring Files with HTTP
- How the Receiving Host Identifies the Correct Receiving Application

Chapter 31: Basic IPv4 Access Control Lists

- IPv4 Access Control List Basics
- ACL Location and Direction
- Matching Packets
- Taking Action When a Match Occurs
- Types of IP ACLs
- Standard Numbered IPv4 ACLs
- List Logic with IP ACLs
- Matching Logic and Command Syntax
- Matching the Exact IP Address
- Matching a Subset of the Address with Wildcards
- Binary Wildcard Masks
- Finding the Right Wildcard Mask to Match a Subnet
- Matching Any/All Addresses
- Implementing Standard IP ACLs
- Standard Numbered ACL Example 1
- Standard Numbered ACL Example 2
- Troubleshooting and Verification Tip
- Practice Applying Standard IP ACLs
- Practice Building access-list Commands
- Reverse Engineering from ACL to Address Range

Chapter 32: Advanced IPv4 Access Control Lists

- Extended Numbered IP Access Control Lists
- Matching the Protocol, Source IP, and Destination IP
- Matching TCP and UDP Port Numbers
- Extended IP ACL Configuration
- Extended IP Access Lists: Example 1
- Extended IP Access Lists: Example 2
- Practice Building access-list Commands
- Named ACLs and ACL Editing
- Named IP Access Lists
- Editing ACLs Using Sequence Numbers
- Numbered ACL Configuration Versus Named ACL Configuration
- ACL Implementation Considerations
- Additional Reading on ACLs

INFOSECTRAIN

Security Services

Chapter 33: Security Architectures

- Security Terminology
- Common Security Threats
- Attacks That Spoof Addresses
- Denial-of-Service Attacks
- Reflection and Amplification Attacks
- Man-in-the-Middle Attacks
- Address Spoofing Attack Summary
- Reconnaissance Attacks
- Buffer Overflow Attacks
- Malware
- Human Vulnerabilities
- Password Vulnerabilities
- Password Alternatives
- Controlling and Monitoring User Access
- Developing a Security Program to Educate Users

Chapter 34: Securing Network Devices

- Securing IOS Passwords
- Encrypting Older IOS Passwords with service password-encryption
- Encoding the Enable Passwords with Hashes
- Interactions Between Enable Password and Enable Secret
- Making the Enable Secret Truly Secret with a Hash
- Improved Hashes for Cisco's Enable Secret
- Encoding the Passwords for Local Usernames

- Controlling Password Attacks with ACLs
- Firewalls and Intrusion Prevention Systems
- Traditional Firewalls
- Security Zones
- Intrusion Prevention Systems (IPS)
- Cisco Next-Generation Firewalls
- Cisco Next-Generation IPS

35: Implementing Switch Port Security

- Port Security Concepts and Configuration
- Configuring Port Security
- Verifying Port Security
- Port Security MAC Addresses
- Port Security Violation Modes
- Port Security Shutdown Mode
- Port Security Protect and Restrict Modes

Chapter 36: Implementing DHCP

- Dynamic Host Configuration Protocol
- DHCP Concepts
- Supporting DHCP for Remote Subnets with DHCP Relay
- Information Stored at the DHCP Server
- Configuring DHCP Features on Routers and Switches
- Configuring DHCP Relay
- Configuring a Switch as DHCP Client
- Configuring a Router as DHCP Client
- Identifying Host IPv4 Settings

- Host Settings for IPv4
- Host IP Settings on Windows
- Host IP Settings on macOS
- Host IP Settings on Linux

Chapter 37: DHCP Snooping and ARP Inspection

- DHCP Snooping Concepts
- A Sample Attack: A Spurious DHCP Server
- DHCP Snooping Logic
- Filtering DISCOVER Messages Based on MAC Address
- Filtering Messages that Release IP Addresses
- DHCP Snooping Configuration
- Configuring DHCP Snooping on a Layer 2 Switch
- Limiting DHCP Message Rates
- DHCP Snooping Configuration Summary
- Dynamic ARP Inspection
- DAI Concepts
- Review of Normal IP ARP
- Gratuitous ARP as an Attack Vector
- Dynamic ARP Inspection Logic
- Dynamic ARP Inspection Configuration
- Configuring ARP Inspection on a Layer 2 Switch
- Limiting DAI Message Rates
- Configuring Optional DAI Message Checks
- IP ARP Inspection Configuration Summary

INFOSECTRAIN

IP Services

Chapter 38: Device Management Protocols

- System Message Logging (Syslog)
- Sending Messages in Real Time to Current Users
- Storing Log Messages for Later Review
- Log Message Format
- Log Message Severity Levels
- Configuring and Verifying System Logging
- The debug Command and Log Messages
- Network Time Protocol (NTP)
- Setting the Time and Timezone
- Basic NTP Configuration
- NTP Reference Clock and Stratum
- Redundant NTP Configuration
- NTP Using a Loopback Interface for Better Availability
- Analyzing Topology Using CDP and LLDP
- Examining Information Learned by CDP
- Configuring and Verifying CDP
- Examining Information Learned by LLDP
- Configuring and Verifying LLDP

Chapter 39: Network Address Translation

- Perspectives on IPv4 Address Scalability
- CIDR
- Private Addressing
- Network Address Translation Concepts
- Static NAT
- Dynamic NAT
- Overloading NAT with Port Address Translation
- NAT Configuration and Troubleshooting
- Static NAT Configuration
- Dynamic NAT Configuration
- Dynamic NAT Verification
- NAT Overload (PAT) Configuration
- NAT Troubleshooting

Chapter 40: Quality of Service (QoS)

- Introduction to QoS
- QoS: Managing Bandwidth, Delay, Jitter, and Loss
- Types of Traffic
- Data Applications
- Voice and Video Applications
- QoS, as mentioned in The Book
- QoS on Switches and Routers
- Classification and Marking
- Classification Basics
- Matching (Classification) Basics
- Classification of Routers with ACLs and NBAR
- Marking IP DSCP and Ethernet CoS

- Marking the IP Header
- Marking the Ethernet 802.1Q Header
- Other Marking Fields
- Defining Trust Boundaries
- DiffServ Suggested Marking Values
- Expedited Forwarding (EF)
- Assured Forwarding (AF)
- Class Selector (CS)
- Guidelines for DSCP Marking Values
- Queuing
- Round-Robin Scheduling (Prioritization)
- Low Latency Queuing
- A Prioritization Strategy for Data, Voice, and Video
- Shaping and Policing
- Policing
- Where to Use Policing
- Shaping
- Setting a Good Shaping Time Interval for Voice and Video
- Congestion Avoidance
- TCP Windowing Basics

Chapter 41: Miscellaneous IP Services

- First Hop Redundancy Protocol
- The Need for Redundancy in Networks
- The Need for a First Hop Redundancy Protocol
- The Three Solutions for First-Hop Redundancy
- HSRP Concepts
- HSRP Failover
- HSRP Load Balancing
- Simple Network Management Protocol
- SNMP Variable Reading and Writing: SNMP Get and Set
- SNMP Notifications: Traps and Informs
- The Management Information Base
- Securing SNMP FTP and TFTP
- Managing Cisco IOS Images with
- FTP/TFTP
- The IOS File System
- Upgrading IOS Images
- Copying a New iOS Image to a Local iOS File System Using TFTP
- Verifying IOS Code Integrity with MD5
- Copying Images with FTP
- The FTP and TFTP Protocols
- FTP Protocol Basics
- FTP Active and Passive Modes
- FTP over TLS (FTP Secure)
- TFTP Protocol Basics

INFOSECTRAIN

Network Architecture

Chapter 42: LAN Architecture

- Analyzing Campus LAN Topologies
- Two-Tier Campus Design (Collapsed Core)
- The Two-Tier Campus Design
- Topology Terminology Seen Within a Two-Tier Design
- Three-Tier Campus Design (Core)
- Topology Design Terminology
- Small Office/Home Office
- Power over Ethernet (PoE)
- PoE Basics
- PoE Operation
- PoE and LAN Design

Chapter 43: WAN Architecture

- Metro Ethernet
- Metro Ethernet Physical Design and Topology
- Ethernet WAN Services and Topologies
- Ethernet Line Service (Point-to-Point)
- Ethernet LAN Service (Full Mesh)
- Ethernet Tree Service (Hub and Spoke)
- Layer 3 Design Using Metro Ethernet
- Layer 3 Design with E-Line Service
- Layer 3 Design with E-LAN Service
- Multiprotocol Label Switching (MPLS)
- MPLS VPN Physical Design and Topology

- MPLS and Quality of Service
- Layer 3 with MPLS VPN
- Internet VPNs
- Internet Access
- Digital Subscriber Line
- Cable Internet
- Wireless WAN (3G, 4G, LTE, 5G)
- Fiber (Ethernet) Internet Access
- Internet VPN Fundamentals
- Site-to-Site VPNs with IPsec
- Remote Access VPNs with TLS
- VPN Comparisons

Chapter 44: Cloud Architecture

- Server Virtualization
- Cisco Server Hardware
- Server Virtualization Basics
- Networking with Virtual Switches on a
- Virtualized Host
- The Physical Data Center Network
- Workflow with a Virtualized Data Center
- Cloud Computing Services
- Private Cloud (On-Premise)
- Public Cloud
- Cloud and the “Software as a Service” Model
- Infrastructure as a Service
- Software as a Service

- (Development) Platform as a Service
- WAN Traffic Paths to Reach Cloud Services
- Enterprise WAN Connections to Public Cloud
- Accessing Public Cloud Services Using the Internet
- Pros and Cons of Connecting to Public Cloud with Internet
- Private WAN and Internet VPN Access to Public Cloud
- Pros and Cons of Connecting to the Cloud with Private WANs
- Intercloud Exchanges
- Summarizing the Pros and Cons of Public Cloud WAN Options
- A Scenario: Branch Offices and the Public Cloud
- Migrating Traffic Flows When Migrating to Email SaaS
- Branch Of ices with Internet and Private WAN

Network Automation

Chapter 45: Introduction to Controller-Based Networking

- SDN and Controller-Based Networks
- The Data, Control, and Management Planes
- The Data Plane
- The Control Plane
- The Management Plane
- Cisco Switch Data Plane Internals
- Controllers and Software-Defined Architecture
- Controllers and Centralized Control
- The Southbound Interface
- The Northbound Interface

- Software Defined Architecture Summary
- Examples of Network Programmability and SDN
- OpenDaylight and OpenFlow
- The OpenDaylight Controller
- The Cisco Open SDN Controller (OSC)
- Cisco Application Centric Infrastructure (ACI)
- ACI Physical Design: Spine and Leaf
- ACI Operating Model with Intent-Based Networking
- Cisco APIC Enterprise Domain
- APIC-EM Basics
- APIC-EM Replacement
- Summary of the SDN Examples
- Comparing Traditional Versus Controller-Based Networks
- How Automation Impacts Network Management
- Comparing Traditional Networks with Controller-Based Networks

Chapter 46: Cisco Software-Defined Access (SDA)

- SDA Fabric, Underlay, and Overlay
- The SDA Underlay
- Using Existing Gear for the SDA Underlay
- Using New Gear for the SDA Underlay
- The SDA Overlay
- VXLAN Tunnels in the Overlay (Data Plane)
- LISP for Overlay Discovery and Location (Control Plane)
- DNA Center and SDA Operation
- Cisco DNA Center
- Cisco DNA Center and Scalable Groups
- Issues with Traditional IP-Based Security

- SDA Security Based on User Groups
- DNA Center as a Network Management Platform
- DNA Center Similarities to Traditional Management
- DNA Center Differences with Traditional Management

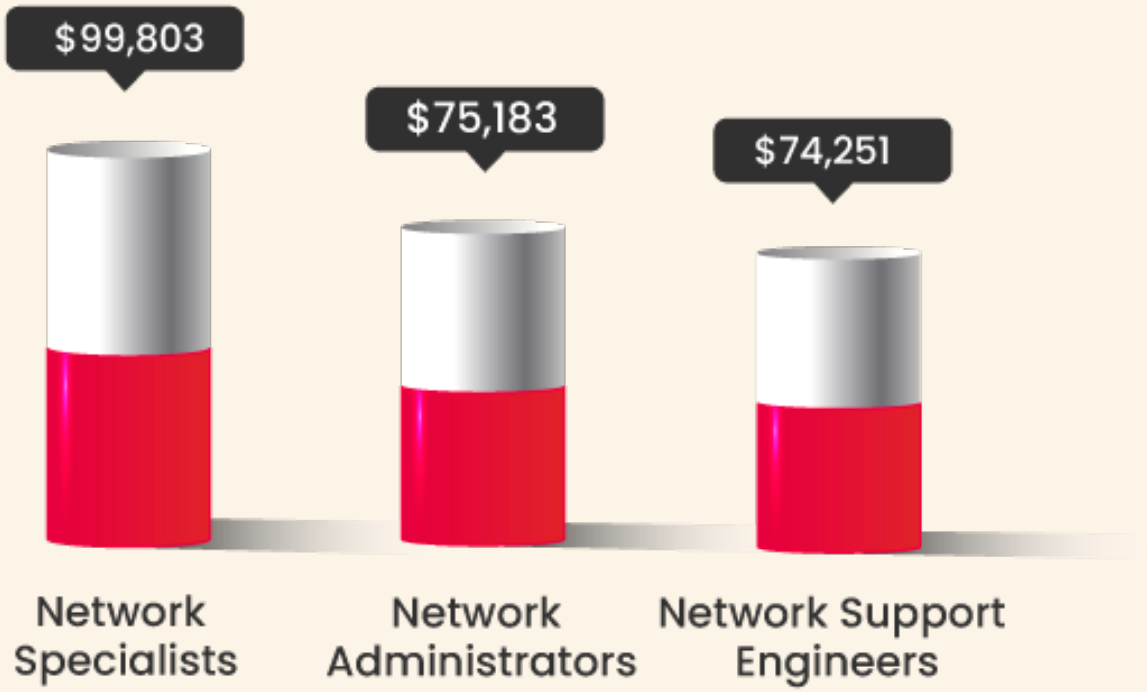
Chapter 47: Understanding REST and JSON

- REST-Based APIs
- REST-Based (RESTful) APIs
- Client/Server Architecture
- Stateless Operation
- Cacheable (or not)
- Background: Data and Variables
- Simple Variables
- List and Dictionary Variables
- REST APIs and HTTP
- Software CRUD Actions and HTTP Verbs
- Using URIs with HTTP to Specify the Resource
- Example of REST API Call to DNA Center
- Data Serialization and JSON
- The Need for a Data Model with APIs
- Data Serialization Languages
- JSON
- XML
- YAML
- Summary of Data Serialization
- Interpreting JSON
- Interpreting JSON Key: Value Pairs
- Interpreting JSON Objects and Arrays
- Minified and Beautified JSON

Chapter 48: Understanding Ansible, Puppet, and Chef

- Device Configuration Challenges and Solutions
- Configuration Drift
- Centralized Configuration Files and Version Control
- Configuration Monitoring and Enforcement
- Configuration Provisioning
- Configuration Templates and Variables
- Files That Control Configuration Automation
- Ansible, Puppet, and Chef Basics
- Ansible
- Puppet
- Chef
- Summary of Configuration Management Tool

CCNA Course Benefits



Hiring Companies

HCL intel vodafone

Source: Indeed, Glassdoor

www.infosectrain.com I sales@infosectrain.com