CISCO CERTIFIED NETWORKING ASSOCIATE

UPGRADE YOUR KNOWLEDGE

Cisco Certified Network Associate Training

Course Overview

Cisco Certified Network Associate (CCNA) is a certification program for entry-level network engineers that helps maximize your investment in foundational networking knowledge and increase the value of your employer's network.

Duration & Module Coverage

Duration: 14 Days (35hrs)

Session Options	Module Coverage
Session Weekdays[4] : 2.5 hours per day 4 days per week **Session Weekends:** 2.5 hours per day	**Day 1 - Module 1** **Day 2 - Module 1 contd.** **Day 3 - Module 1 contd.** **Day 4 - Module 2** **Day 5 - Module 2 contd.** **Day 6 – Module 3** **Day 7 – Module 3 contd.** **Day 8 – Module 3 contd.** **Day 9- Module 4** **Day 10- Module 5** **Day 11- Module 5 contd.** **Day 12- Module 5 contd.** **Day 13- Module 6** **Day 14- Module 6 contd.**

Learning Goals

By the end of this course participants will be able to:

1. Understand concepts of networking.
2. Gain familiarity with LAN switching and routing technologies.
3. Understand infrastructure and network security, management and services.
4. Network programmability and automation concepts

Pre-Requisites

The pre-requisite for this course is basic computer knowledge.

Teaching Methodology

This is a very hands-on course where participants carry out practical exercises according to the lab guide provided. The concepts are taught through implementation of real-world use-cases. Our exercises have been carefully designed to replicate scenarios participants will face in real life work conditions.

Who Should Take This Course?

This course is designed for network specialists, network administrator and network support engineers with 1 to 3 years of experience.

Course Content

1. **Networking Fundamentals**
   - Describe network infrastructure component – router, switches, firewalls, access points, end-points and servers.
   - Network architectures – 2-tier, 3-tier, spine leaf, WAN and SOHO.
   - Compare physical interface and cabling types – copper, PoE and fiber- single-mode and multi-mode
   - Identify interface and cable issues – collision, errors, mismatch duplex and/or speed
   - Compare TCP to UDP
   - IPv4 addressing and types – public and private
   - Subnetting
   - IPv6 addressing and prefix
   - IPv6 address types – global unicast, link local, unique local, anycast and multicast
   - Verify IP parameters for Client OS [Windows, Linux and MAC]
   - Describe wireless principles – SSID, RF, Encryption and Non-overlapping Wi-Fi Channels.
   - Explain virtualization fundamentals – virtual machines
   - Describe switching concepts – Frame switching and flooding, MAC address table, learning and aging.
2. **Network Access**
   - Virtual LANs – access ports, default VLANs and connectivity
   - Inter-switch connectivity – trunk ports, 802.1q and Native VLAN
   - Layer-2 discovery protocols – CDP and LLDP
   - Etherchannel
   - Rapid Spanning Tree Protocol – root port, root bridge, port states and portfast
   - Cisco Wireless Architecture and AP modes
   - Physical Infrastructure Connections of WLAN components
   - AP and WLC management access connections – Telnet, SSH, HTTP, HTTPS, console and RADIUS
   - Wireless LAN Access – WLAN creation, security settings and QoS settings.
3. **IP Connectivity**
   - Forwarding decisions in a router – longest match, routing protocol and metric
   - Components of routing table – prefix, network mask, next-hop, protocol code, metric and administrative distance.
   - IPv4 and IPv6 static routing – default route, network route and floating static
   - OSPFv2 – neighbor formation – point-to-point and broadcast, router-ID
   - First Hop Redundancy Protocols
4. **IP Services**
   - Inside source NAT – static and pool
   - NTP in client and server pool
   - DHCP and DNS in a network
   - SNMP in network operations
   - QoS – classification, marking, queuing, congestion, policing and shaping
   - FTP and TFTP in a network
   - Remote access using SSH
5. **Security Fundamentals**
   - Security concepts – threats, vulnerabilities and exploits
   - Security program elements – user awareness, training and physical access control
   - Access control using local passwords

- Password policies elements – management, complexities and multi-factor authentication
- Remote access and site-to-site VPNs
- Access controls lists
- Layer-2 security – DHCP snooping, ARP inspection and port security
- Authorization, authentication and accounting concepts
- Wireless security protocols – WPA, WPA2 and WPA3

6. Automation and Programmability

- Impact of automation on network management
- Traditional networks versus controller based networks
- Northbound and Southbound APIs
- Separation of control plane and data plane
- Cisco DNA center device management
- REST based APIs – CRUD, HTTP verbs and data encoding
- Configuration management mechanisms – Puppet, Chef and Ansible
- Interpret JSON encoded data

Practical Learning Exercises

A lab guide will be provided to each student with requirement scenarios. Along with lab guide required VMs will be provided to set up individual labs for self practice.

There would be scenarios for implementing, verifying and troubleshooting all modules covered in the course.