Cisco Certified Network Associate

Course Duration:40 Hrs. **Course Code:200-301**

Course Overview

The CCNA (Cisco Certified Network Associate) course is an entry-level IT certification that validates fundamental networking knowledge and skills, covering topics like network fundamentals, IP connectivity, IP services, security, and automation.

What you'll learn?

Network Fundamentals:

Learn about network architectures, protocols, and basic networking concepts.

IP Addressing and Subnetting:

Understand how IP addresses are assigned and how to subnet networks.

Routing and Switching:

Learn about routers, switches, and how they work together to forward data packets.

Cisco Devices:

Gain practical experience with Cisco routers and switches, including configuration and troubleshooting.

Network Security:

Learn about basic security concepts, such as access control lists (ACLs) and firewalls.

Target Audience

Entry-Level Network Professionals:
The CCNA is a great starting point for those new to the networking field, providing the necessary knowledge and skills for entry-level roles.

Network Engineers:
Individuals seeking to specialize in network engineering can benefit from the CCNA's focus on core networking concepts and Cisco technologies.

Network Administrators:
The CCNA equips network administrators with the skills to manage and maintain basic network infrastructure, including Cisco devices.

Pre-Requisites

No Formal Requirements:
You don't need a specific degree, previous certification, or any other formal qualification to enroll in a CCNA course or take the exam.

Recommended Background:
While not mandatory, having some familiarity with networking concepts like IP addressing, basic networking terminology, and router/switch administration is beneficial.

Practical Experience:
Hands-on experience with networking technologies and tools can also be advantageous.

Course Content

Module 1: Network Fundamentals

A. Explain the role and function of network components.
B. Describe characteristics of network topology architectures
C. Compare physical interface and cabling types.
D. Identify interface and cable issues.
E. Compare TCP to UDP
F. Configure and verify IPv4 addressing and subnetting.
G. Describe the need for private IPv4 addressing.
H. Configure and verify IPv6 addressing and prefix.
I. Describe IPv6 address types.

Module 2: Network Access

A. Configure and verify VLANs (normal range) spanning multiple switches.
B. Configure and verify Interswitch connectivity.
C. Configure and verify Layer 2 discovery protocols.
D. Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
E. Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
F. Describe Cisco Wireless Architectures and AP modes.
G. Describe physical infrastructure connections of WLAN components.

Module 3: IP Connectivity

A. Interpret the components of routing table.
B. Determine how a router makes a forwarding decision by default.
C. Configure and verify IPv4 and IPv6 static routing.
D. Configure and verify single area OSPFv2.
E. Describe the purpose, functions, and concepts of first hop redundancy protocols.

Module 4: IP Services

A. Configure and verify inside source NAT using static and pools.
B. Configure and verify NTP operating in a client and server mode.
C. Explain the role of DHCP and DNS within the network.
D. Explain the function of SNMP in network operations.
E. Describe the use of syslog features including facilities and levels.
F. Configure and verify DHCP client and relay.
G. Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping.
H. Configure network devices for remote access using SSH.
I. Describe the capabilities and function of TFTP/FTP in the network.

Module 5: Security Fundamentals

A. Define key security concepts.
B. Describe security program elements.
C. Configure and verify device access control using local passwords.
D. Describe security password policies elements, such as management, complexity, and password alternatives.
E. Describe IPsec remote access and site-to-site VPNs.
F. Configure and verify access control lists.
G. Configure and verify Layer 2 security features.
H. Compare authentication, authorization, and accounting concepts.
I. Describe wireless security protocols (WPA, WPA2, and WPA3)
J. Configure and verify WLAN within the GUI using WPA2 PSK

Module 6: Automation and Programmability

A. Explain how automation impacts network management.
B. Compare traditional networks with controller-based networking.
C. Describe controller-based, software defined architecture.
D. Compare traditional campus device management with Cisco DNA Center enabled device management.
E. Describe characteristics of REST-based APIs
F. Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
G. Recognize components of JSON-encoded data

Exam Preference

Exam Code	200-301
Length Of Test	120 Minutes
Passing Score	85%
Types Of Questions	1. MCQ. 2. Drag-and-Drop. 3. Simulations (Hands-on-tasks)