

CCNA Cisco Certified Network Associate

On February 24, 2020, Cisco released this new consolidated CCNA exam, the Cisco Certified Network Associate (200-301 CCNA).

SecureNinja's instructor-led 5-day Cisco Certified Network Associate CCNA hands-on training and certification boot camp in Washington, DC and San Diego, CA covers the exam objectives for exam 200-301. Packed with updated topics that have been added to the latest version of the CCNA certification exam released on February 2020.

Course Details

Through a combination of lecture, hands-on labs, and self-study, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

Who Would Benefit

This training bootcamp is designed for students who have a basic understanding of IT concepts; especially in relation to computer networking infrastructure. This course is excellent preparation for students who wish not only to be CCNA certified but who desire to move on towards the higher certifications of CCNP, CCVP, CCSP, Security+, MCP, MCSE, MCTS, or MCITP. Job Roles include help desk technicians, pre & post-sales network engineers who install and support office networks, entry-level network engineers, network administrators, and network support technicians.

The job roles are best suited to the material in this course are:

- Entry-level network engineer
- Network Administrator
- Network support technician
- Help desk technician

CCNA Course Objectives

- Identify the components of a computer network and describe their basic characteristics
- Understand the model of host-to-host communication
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software

- Describe LANs and the role of switches within LANs
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Install a switch and perform the initial configuration
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- Describe the TCP/IP Transport layer and Application layer
- Explore functions of routing
- Implement basic configuration on a Cisco router
- Explain host-to-host communications across switches and routers
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity
- Describe the operation, benefits, and limitations of static routing
- Describe, implement, and verify Virtual Local Area Networks (VLANs) and trunks
- Describe the application and configuration of inter-VLAN routing
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF)
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols
- Describe basic WAN and VPN concepts
- Describe the operation of Access Control Lists (ACLs) and their applications in the network
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure Network Address Translation (NAT) on Cisco routers
- Describe basic Quality of Service (QoS) concepts
- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs)
- Describe network and device architectures and introduce virtualization
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN)
- Configure basic IOS system monitoring tools
- Describe the management of Cisco devices
- Describe the current security threat landscape
- Describe threat defense technologies
- Implement a basic security configuration of the device management plane
- Implement basic steps to harden network devices

CCNA (200-301) Exam Details

CCNA Exam v1.0 (CCNA 200-301) is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. The exam covers 6 different domains and each domain is weighted differently.

- Network Fundamentals 20%
- Network Access 20%
- IP Connectivity 25%
- IP Services 10%
- Security Fundamentals 15%
- Automation and programmability 10%

Prerequisites

There are no formal prerequisites for the CCNA certification, but you should have an understanding of the following exam topics: One or more years of experience implementing and administering Cisco solutions, basic computer literacy, basic PC operating system navigation skills, internet usage skills and IP address knowledge. Network+ is recommended prior to taking this course/exam.

Career Track & Roles

- Network Administrator
- Systems Administrator
- Systems Engineer
- Systems Architect
- Network Security Specialist
- Information Security Specialist