Document Generated: 04/02/2026

Learning Style: Virtual Classroom

Technology: Cisco

Difficulty: Beginner

Course Duration: 5 Days

Next Course Date: May 18, 2026

Implementing and Administering Cisco Solutions (CCNA) v2.1)

The Cisco Certified Network Associate (CCNA) is one of the most recognized entry-level certifications in IT networking, validating your ability to install, configure, operate, and troubleshoot small to medium-sized networks. This CCNA instructor-

led course equips students with essential network administration training, helping them master the fundamentals of IPv4 and IPv6 addressing, routing and switching, wireless networking, and basic security protocols.

Through this CCNA virtual training, you'll participate in live Cisco networking online classes that combine guided lectures, Cisco IOS hands-on lab training, and real-world case studies. Each session is led by certified Cisco instructors who provide step-by-step guidance in configuring routers, switches, and network devices while building your understanding of troubleshooting and network operations. By the end of this Cisco 200-301 live training, you'll be prepared to take the exam with confidence and apply your skills to real-world networking environments.

The CCNA certification is widely respected in the IT industry and often serves as the first step toward advanced Cisco certifications and specialized roles. In the United States, network professionals with a CCNA certification typically earn between $75,000 and $92,000 per year, with experienced engineers and administrators earning $100,000 or more as they advance into senior or cloud networking roles.

Course Objectives:

After taking this course, you should be able to:

- Identify the components of a computer network and explain their basic characteristics
- Describe the features and functions of the Cisco IOS Software
- Explain IPv4 and IPv6 addressing scheme
- Implement basic configurations on a Cisco router
- Identify and resolve common switching and routing networking issues
- Describe network and device architectures and explain virtualization
- Describe the smart network management solutions like Cisco DNA Center, SD-Access and SD-WAN
- Outline threat defense technologies
- And many, many more aspects of a basic IPv4 and IPv6 network

Audience:

- Entry-level network engineer
- Network administrator

- Network support technician
- Help desk technician

Prerequisites:

Before taking this course, you should have:

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Basic IP address knowledge

Course Outline:

- Section 1: Exploring the Functions of Networking
- Section 2: Introducing the Host-To-Host Communications Model
- Section 3: Operating Cisco IOS Software
- Section 4: Introducing LANs
- Section 5: Exploring the TCP/IP Link Layer
- Section 6: Starting a Switch
- Section 7: Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets
- Section 8: Explaining the TCP/IP Transport Layer and Application Layer
- Section 9: Exploring the Functions of Routing
- Section 10: Configuring a Cisco Router
- Section 11: Exploring the Packet Delivery Process
- Section 12: Troubleshooting a Simple Network
- Section 13: Introducing Basic IPv6
- Section 14: Configuring Static Routing
- Section 15: Implementing VLANs and Trunks
- Section 16: Routing Between VLANs
- Section 17: Introducing OSPF
- Section 18: Building Redundant Switched Topologies
- Section 19: Improving Redundant Switched Topologies with EtherChannel
- Section 20: Exploring Layer 3 Redundancy
- Section 21: Introducing WAN Technologies
- Section 22: Explaining Basics of ACL
- Section 23: Enabling Internet Connectivity
- Section 24: Introducing QoS
- Section 25: Explaining Wireless Fundamentals
- Section 26: Introducing Architectures and Virtualization
- Section 27: Explaining the Evolution of Intelligent Networks
- Section 28: Introducing System Monitoring
- Section 29: Managing Cisco Devices

- Section 30: Examining the Security Threat Landscape
- Section 31: Implementing Threat Defense Technologies
- Section 32: Securing Administrative Access
- Section 33: Implementing Device Hardening

Labs Outline:

Discovery 1: Get Started with Cisco CLI
Discovery 2: Observe How a Switch Operates
Discovery 3: Perform Basic Switch Configuration
Discovery 4: Inspect TCP/IP Applications
Discovery 5: Configure an Interface on a Cisco Router
Discovery 6: Configure and Verify Layer 2 Discovery Protocols
Discovery 7: Configure Default Gateway
Discovery 8: Explore Packet Forwarding
Discovery 9: Troubleshoot Switch Media and Port Issues
Discovery 10: Troubleshoot Port Duplex Issues
Discovery 11: Configure Basic IPv6 Connectivity
Discovery 12: Configure and Verify IPv4 Static Routes
Discovery 13: Configure IPv6 Static Routes
Discovery 14: Configure VLAN and Trunk
Discovery 15: Configure a Router on a Stick
Discovery 16: Configure and Verify Single-Area OSPF
Discovery 17: Configure and Verify EtherChannel
Discovery 18: Configure and Verify IPv4 ACLs
Discovery 19: Configure a Provider-Assigned IPv4 Address
Discovery 20: Configure Static NAT
Discovery 21: Configure Dynamic NAT and PAT
Discovery 22: Log into the WLC
Discovery 23: Monitor the WLC
Discovery 24: Configure a Dynamic (VLAN) Interface
Discovery 25: Configure a DHCP Scope
Discovery 26: Configure a WLAN
Discovery 27: Define a RADIUS Server
Discovery 28: Explore Management Options
Discovery 29: Explore the Cisco DNA Center
Discovery 30: Configure and Verify NTP
Discovery 31: Create the Cisco IOS Image Backup
Discovery 32: Upgrade Cisco IOS Image
Discovery 33: Configure WLAN Using WPA2 PSK Using the GUI
Discovery 34: Secure Console and Remote Access
Discovery 35: Enable and Limit Remote Access Connectivity
Discovery 36: Configure and Verify Port Security
FASTLab 1: Implement the Initial Switch Configuration
FASTLab 2: Implement an Initial Router Configuration
FASTLab 3: Implement IPv4 Static Routing
FASTLab 4: Implement IPv6 Static Routing
FASTLab 5: Troubleshoot VLANs and Trunk
FASTLab 6: Implement Multiple VLANs and Basic Routing Between the VLANs

FASTLab 7: Improve Redundant Switched Topologies with EtherChannel
FASTLab 8: Implement Numbered and Named IPv4 ACLs
FASTLab 9: Implement PAT
FASTLab 10: Configure System Message Logging
FASTLab 11: Secure Device Administrative Access
FASTLab 12: Implement Device Hardening

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges