

CCNA Bootcamp: Implementing and Administering Cisco Solutions (CCNA) v1.0

Duration: 5 Day(s)

Course Overview:

The Implementing and Administering Cisco Solutions (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. 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. This course covers configuring network components such as switches, routers and wireless LAN controllers; managing network devices; and identifying basic security threats. It also gives you a foundation in network programmability, automation and software-defined networking. Finally, this course will also help you prepare to take the 200-301 Cisco® Certified Network Associate (CCNA®) exam and by passing this exam, you will earn a CCNA certification.

Who Should Attend?

This course is extremely fast-paced and only for those with significant experience already. It is designed for anyone seeking CCNA certification. It also provides foundational knowledge for all Support Technicians involved in the basic installation, operation and verification of Cisco networks.

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

- Entry-level Network Engineer
- Network Administrator
- Network Support Technician
- Help Desk Technician

Course Objectives:

This course will help you:

- Learn the knowledge and skills to install, configure and operate a small to medium-sized networks
- Gain a foundation in the essentials of networking, security and automation
- Prepare for the 200-301 CCNA exam, which earns CCNA certification

What to expect from the exam?

- The 200-301 CCNA exam certifies your knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals and automation & programmability
- After you pass 200-301 CCNA, you will earn CCNA certification

After taking this course, you should be able to:

- 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

Outline

20% 1.0 Network Fundamentals

- 1.1 Explain the role and function of network components
 - 1.1.a Routers
 - 1.1.b L2 and L3 switches
 - 1.1.c Next-generation firewalls and IPS
 - 1.1.d Access points
 - 1.1.e Controllers (Cisco DNA Center and WLC)
 - 1.1.f Endpoints
 - 1.1.g Servers
- 1.2 Describe characteristics of network topology architectures
 - 1.2.a 2 tier
 - 1.2.b 3 tier
 - 1.2.c Spine-leaf
 - 1.2.d WAN
 - 1.2.e Small office/home office (SOHO)
 - 1.2.f On-premises and cloud
- 1.3 Compare physical interface and cabling types
 - 1.3.a Single-mode fiber, multimode fiber, copper
 - 1.3.b Connections (Ethernet shared media and point-to-point)
 - 1.3.c Concepts of PoE
- 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- 1.5 Compare TCP to UDP
- 1.6 Configure and verify IPv4 addressing and subnetting

- 1.7 Describe the need for private IPv4 addressing
- 1.8 Configure and verify IPv6 addressing and prefix
- 1.9 Compare IPv6 address types
 - 1.9.a Global unicast
 - 1.9.b Unique local
 - 1.9.c Link local
 - 1.9.d Anycast
 - 1.9.e Multicast
 - 1.9.f Modified EUI 64
- 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- 1.11 Describe wireless principles
 - 1.11.a Non-overlapping Wi-Fi channels
 - 1.11.b SSID
 - 1.11.c RF
 - 1.11.d Encryption
- 1.12 Explain virtualization fundamentals (virtual machines)
- 1.13 Describe switching concepts
 - 1.13.a MAC learning and aging
 - 1.13.b Frame switching
 - 1.13.c Frame flooding
 - 1.13.d MAC address table

20%

2.0 Network Access

- 2.1 Configure and verify VLANs (normal range) spanning multiple switches
 - 2.1.a Access ports (data and voice)
 - 2.1.b Default VLAN
 - 2.1.c Connectivity
- 2.2 Configure and verify interswitch connectivity
 - 2.2.a Trunk ports
 - 2.2.b 802.1Q
 - 2.2.c Native VLAN
- 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
 - 2.5.a Root port, root bridge (primary/secondary) and other port names
 - 2.5.b Port states (forwarding/blocking)
 - 2.5.c PortFast benefits

- 2.6 Compare Cisco Wireless Architectures and AP modes
- 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
- 2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

25% **3.0 IP Connectivity**

- 3.1 Interpret the components of routing table
 - 3.1.a Routing protocol code
 - 3.1.b Prefix
 - 3.1.c Network mask
 - 3.1.d Next hop
 - 3.1.e Administrative distance
 - 3.1.f Metric
 - 3.1.g Gateway of last resort
- 3.2 Determine how a router makes a forwarding decision by default
 - 3.2.a Longest match
 - 3.2.b Administrative distance
 - 3.2.c Routing protocol metric
- 3.3 Configure and verify IPv4 and IPv6 static routing
 - 3.3.a Default route
 - 3.3.b Network route
 - 3.3.c Host route
 - 3.3.d Floating static
- 3.4 Configure and verify single area OSPFv2
 - 3.4.a Neighbor adjacencies
 - 3.4.b Point-to-point
 - 3.4.c Broadcast (DR/BDR selection)
 - 3.4.d Router ID
- 3.5 Describe the purpose of first hop redundancy protocol

10% 4.0 IP Services

- 4.1 Configure and verify inside source NAT using static and pools
- 4.2 Configure and verify NTP operating in a client and server mode
- 4.3 Explain the role of DHCP and DNS within the network
- 4.4 Explain the function of SNMP in network operations
- 4.5 Describe the use of syslog features including facilities and levels
- 4.6 Configure and verify DHCP client and relay
- 4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing and shaping
- 4.8 Configure network devices for remote access using SSH
- 4.9 Describe the capabilities and function of TFTP/FTP in the network

15% 5.0 Security Fundamentals

- 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- 5.2 Describe security program elements (user awareness, training, and physical access control)
- 5.3 Configure device access control using local passwords
- 5.4 Describe security password policies elements, such as management, complexity and password alternatives (multifactor authentication, certificates and biometrics)
- 5.5 Describe remote access and site-to site VPNs
- 5.6 Configure and verify access control lists
- 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection and port security)
- 5.8 Differentiate authentication, authorization and accounting concepts
- 5.9 Describe wireless security protocols (WPA, WPA2 and WPA3)
- 5.10 Configure WLAN using WPA2 PSK using the GUI

10% 6.0 Automation and Programmability

- 6.1 Explain how automation impacts network management
- 6.2 Compare traditional networks with controller-based networking
- 6.3 Describe controller-based and software defined architectures (overlay, underlay and fabric)
 - 6.3.a Separation of control plane and data plane
 - 6.3.b North-bound and south-bound APIs
- 6.4 Compare traditional campus device management with Cisco DNA Center enabled device management
- 6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
- 6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
- 6.7 Interpret JSON encoded data