Corinata Solutions
PRIVATE LIMITED

CCNA — Course Syllabus

CCNA Certification

EXAM CODE	VERSION	STATUS	DURATION
200-301	v1.1	Current	120 minutes

Overview

CCNA validates a candidate's knowledge and skills across network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. It is the foundational certification for a networking career and the standard entry point into the Cisco certification path.

Associated with: CCNA Certification

Exam Domains

20% 1.0 Network Fundamentals

- Explain the role and function of network components
  - Routers
  - Layer 2 and Layer 3 switches
  - Next-generation firewalls and IPS
  - Access points
  - Controllers
  - Endpoints
  - Servers
  - PoE
- Describe characteristics of network topology architectures
  - Two-tier, three-tier, spine-leaf
  - WAN
  - Small office/home office (SOHO)
  - On-premises and cloud
- Compare physical interface and cabling types (single-mode/multimode fiber, copper)
- Identify interface and cable issues (collisions, errors, mismatched duplex/speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- Describe IPv6 address types
  - Unicast (global, unique local, link local)
  - Anycast

- Multicast
- Modified EUI 64

- Verify IP parameters for client OS (Windows, MacOS, Linux)
- Describe wireless principles (channels, SSID, RF, encryption)
- Explain virtualization fundamentals (server virtualization, containers, VRFs)
- Describe switching concepts (MAC learning/aging, frame switching/flooding, MAC address table)

20% 2.0 Network Access

- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify interswitch connectivity (trunk ports, 802.1Q, native VLAN)
- Configure and verify Layer 2 discovery protocols (CDP and LLDP)
- Configure and verify Layer 2/Layer 3 EtherChannel (LACP)
- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
  - Root port, root bridge (primary/secondary), and other port names
  - Port states and roles
  - PortFast
  - Root guard, loop guard, BPDU filter, and BPDU guard
- Describe Cisco wireless architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity

25% 3.0 IP Connectivity

- Interpret the components of a routing table
  - Routing protocol code, prefix, network mask, next hop
  - Administrative distance, metric, gateway of last resort
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing (default, network, host, floating static)
- Configure and verify single area OSPFv2 (neighbor adjacencies, point-to-point, broadcast DR/BDR, router ID)
- Describe the purpose, functions, and concepts of first hop redundancy protocols

10% 4.0 IP Services

- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features, including facilities and severity levels
- Configure and verify DHCP client and relay
- Explain the forwarding per-hop behavior (PHB) for QoS
- Configure network devices for remote access using SSH

- Describe the capabilities and functions of TFTP/FTP in the network

15% 5.0 Security Fundamentals

- Define key security concepts (threats, vulnerabilities, exploits, mitigation techniques)
- Describe security program elements (user awareness, training, physical access control)
- Configure and verify device access control using local passwords
- Describe security password policy elements (management, complexity, MFA, certificates, biometrics)
- Describe IPsec remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK

10% 6.0 Automation and Programmability

- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture
  - Separation of control plane and data plane
  - Northbound and southbound APIs
- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, data encoding)
- Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform
- Recognize components of JSON-encoded data