Implementing and Administering Cisco Solutions (200-301 CCNA) v2.0

Exam Description: Implementing and Administering Cisco Solutions (200-301 CCNA) v2.0 is a 120-minute exam that validates your expertise of IP routing, switching and network access, network services and security, network infrastructure and connectivity, AI, and network operations and management. As part of the exam, you may be required to evaluate output and recommendations from agentic AI and digital network assistants to support network operations and troubleshooting activities. Passing this exam earns you the CCNA certification.

The following topics serve as a general guide for the exam. Please note that additional related topics may be included in any given exam version. These guidelines are subject to change at any time without notice to ensure they remain accurate and relevant.

25% 1.0 Network Infrastructure and Connectivity

- 1.1 Diagnose interface and cable (copper and fiber) issues such as collisions, errors, mismatched duplex, speed, distance, interface, signal levels, pin out, and cable types
- 1.2 Describe the role and function of hypervisors, virtual machines, and containers
- 1.3 Troubleshoot IPv4 address configuration, assignment, and subnetting (public and private)
- 1.4 Troubleshoot IPv6 address configuration, assignment, and prefix sizing (unicast and modified EUI 64)
- 1.5 Describe wireless principles
  - 1.5.a Band and channel selection
  - 1.5.b RF characteristics
  - 1.5.c Security protocols
  - 1.5.d Cause of interference
- 1.6 Troubleshoot wired and wireless client connectivity (IP configuration, network reachability, and wireless security parameters on Windows, MacOS, and Linux)
- 1.7 Troubleshoot DHCPv4 client, server, and relay on IOS devices

25% 2.0 Switching and Network Access

- 2.1 Configure network infrastructure connectivity (switch-to-switch and switch-to-router)
  - 2.1.a Layer 2/Layer 3 physical interfaces
  - 2.1.b Layer 2 802.1Q trunk interfaces
  - 2.1.c Layer 2/Layer 3 LACP port-channel/EtherChannel
  - 2.1.d Switch virtual interface (SVI)
- 2.2 Configure Layer 2 switch port attributes for edge-host connectivity (VLAN, PoE, port channel, and LACP)
  - 2.2.a Desktop, printer, and IOT appliances
  - 2.2.b Wireless access points (standalone and controller based)
  - 2.2.c Voice over IP phone
  - 2.2.d Virtualized hosts
  - 2.2.e Network appliances
- 2.3 Validate the accuracy of network documentation using CDP and LLDP

- 2.4 Troubleshoot basic Layer 2/Layer 3 connectivity and device operations using show commands (including show logs), ping, extended ping, trace route, and packet capture output
- 2.5 Configure operations of the Rapid Per VLAN Spanning Tree Protocol (Rapid PVST+)
  - 2.5.a Root port, root bridge (primary/secondary), and other port names
  - 2.5.b Port states and roles
  - 2.5.c PortFast
  - 2.5.d Root guard, loop guard, and BPDU guard

20% 3.0 IP Routing

- 3.1 Interpret a routing table to identify the next hop for a packet (routing protocol, prefix/mask, administrative distance, metric, and default route)
- 3.2 Troubleshoot IPv4 and IPv6 static routing
  - 3.2.a Default route
  - 3.2.b Network route
  - 3.2.c Host route
  - 3.2.d Floating static
- 3.3 Configure single area OSPFv2 for IPv4 and OSPFv3 for IPv6
  - 3.3.a Neighbor adjacencies (excluding authentication)
  - 3.3.b Point-to-point
  - 3.3.c Broadcast (DR/BDR selection)
  - 3.3.d Router ID
- 3.4 Interpret the operational status of First Hop Redundancy Protocols (HSRP and VRRP)

20% 4.0 Network Services and Security

- 4.1 Configure network devices with local usernames and as an AAA client (TACACS+ and RADIUS) for management
- 4.2 Manage device configuration and software files using secure file transfer operations with SFTP/SCP
- 4.3 Configure NAT/PAT on IOS XE routers
- 4.4 Diagnose issues with DNS records (A, AAAA, CNAME, MX, NS, and PTR) to support host, web application, and mail server access by name
- 4.5 Describe IPsec remote access and site-to-site VPNs (protocols and transport modes)
- 4.6 Configure IPv4 access control lists (standard, extended, numbered, and named ACLs)
- 4.7 Configure Layer 2 security features
  - 4.7.a DHCP snooping
  - 4.7.b Dynamic ARP inspection
  - 4.7.c Storm control
  - 4.7.d RA guard
  - 4.7.e Port security

10% 5.0 AI, and Network Operations and Management

- 5.1 Describe the role of agentic AI in network operations
- 5.2 Select a prompt to send to a generative AI system to support network operations considering prompt components such as data classification, output format, persona, and instructions
- 5.3 Describe network management approaches (device-based, cloud-based, controller-based, automation-based, and infrastructure as code)

5.4 Describe the function of SNMP in network operations
5.5 Use configuration management mechanisms such as Ansible to execute commands
5.6 Interpret syslog message content, severity levels, and facilities