CCNA Exam Topics

Now Available: CCNA 1.1 Exam

Now Available: CCNA 1.1 Exam

The 200-301 CCNA 1.1 exam is now available. New topics on the exam include Generative AI, Cloud Network Management, and Machine Learning. These updates account for less than 10% of the total exam content. To see the latest minor updates to CCNA v1.1, review the exam topics. To take the exam, register now through Pearson VUE.

Now Available

- - 1.1 Explain the role and function of network components
    - 1.1.a Routers
    - 1.1.b Layer 2 and Layer 3 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
    - 1.1.h PoE
  - 1.2 Describe characteristics of network topology architectures
    - 1.2.a Two-tier
    - 1.2.b Three-tier
    - 1.2.c Spine-leaf
    - 1.2.d WAN
    - 1.2.e Small office/home office (SOHO)
    - 1.2.f On-premise 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)
  - 1.4 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 private IPv4 addressing
  - 1.8 Configure and verify IPv6 addressing and prefix
  - 1.9 Describe IPv6 address types
    - 1.9.a Unicast (global, unique local, and link local)
    - 1.9.b Anycast
    - 1.9.c Multicast
    - 1.9.d Modified EUI 64
  - 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
  - 1.11 Describe wireless principles
    - 1.11.a Nonoverlapping Wi-Fi channels
    - 1.11.b SSID
    - 1.11.c RF
    - 1.11.d Encryption
  - 1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)
  - 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

-
  - 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 InterVLAN 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 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
    - 2.5.a Root port, root bridge (primary/secondary), and other port names
    - 2.5.b Port states (forwarding/blocking)
    - 2.5.c PortFast
    - 2.5.d Root guard, loop guard, BPDU filter, and BPDU guard
  - 2.6 Describe 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 network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
  - 2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
-
  - 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 prefix 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, functions, and concepts of first hop redundancy protocols
-
  - 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 functions of TFTP/FTP in the network
- - 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 and verify 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 IPsec remote access and site-to-site VPNs
  - 5.6 Configure and verify access control lists
  - 5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
  - 5.8 Compare authentication, authorization, and accounting concepts
  - 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
  - 5.10 Configure and verify WLAN within the GUI using WPA2 PSK
- - 6.1 Explain how automation impacts network management
  - 6.2 Compare traditional networks with controller-based networking
  - 6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)
    - 6.3.a Separation of control plane and data plane
    - 6.3.b Northbound and Southbound APIs
  - 6.4 Explain AI (generative and predictive) and machine learning in network operations
  - 6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
  - 6.6 Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
  - 6.7 Recognize components of JSON-encoded data
-
-
-
-
-
-
-

-
-