CCNA Exam v1.0 (200-301)

Exam Description: CCNA Exam v1.0 (CCNA 200-301) is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. The course, Implementing and Administering Cisco Solutions (CCNA), helps candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.
20% 1.0 Network Fundamentals
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 the need for 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

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 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
2.6 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 AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced 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 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

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 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

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, 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 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 Recognize components of JSON-encoded data

Switch Configurations (Syntax Only)

```
enable
configure terminal
! 2.2 Trunk Ports
interface <interface>
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan <vlan-id>
 switchport trunk allowed vlan <vlans>
 switchport nonegotiate
```

```
! 2.3 Layer 2 Discovery
cdp enable
lldp run
! 2.4 EtherChannel LACP
interface range <interfaces>
 channel-group <id> mode active
interface port-channel <id>
 switchport mode trunk
! 5.7 Layer 2 Security
ip dhcp snooping
ip dhcp snooping vlan <vlans>
ip arp inspection vlan <vlans>
interface <interface>
 switchport port-security maximum <num>
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 ip dhcp snooping trust
 ip arp inspection trust
end
write memory
```

Switch Configuration

```
Switch(config)# ho S1
S1(config)# ena sec class
S1(config)# ser pass
S1(config)# banner motd #Banner goes here#
```

```
S1(config)# line con 0
S1(config-line)# pass cisco
S1(config-line)# login
S1(config-line)# exec-timeout 10
S1(config-line)# line vty 0 15
S1(config-line)# pass cisco
S1(config-line)# login
S1(config-line)# exec-timeout 10
```

```
S1(config-line)# int vlan 1
S1(config-if)# ip add 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# description Description goes here

enable
configure terminal
! 2.2.a/b/c Trunk Ports, 802.1Q, Native VLAN
vlan 99
interface gi0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,99
! 2.3 Layer 2 Discovery (CDP/LLDP)
cdp enable
lldp run
! 2.4 EtherChannel (LACP Layer 2)
interface range gi0/1 - 2
 channel-group 1 mode active
interface port-channel 1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,99
! 2.7/2.8 WLAN Connections (AP to access/trunk, WLC LAG, mgmt access)
! AP to access port example
interface fa0/10
 switchport mode access
 switchport access vlan 20
 description AP-Data
! Trunk to WLC
interface gi0/3
 switchport mode trunk
 switchport trunk allowed vlan 10,20
! WLC LAG (EtherChannel to WLC)
interface range gi0/47 - 48
 channel-group 10 mode active
interface port-channel 10
 switchport mode trunk
 description WLC-LAG
```

```
! 5.7 Layer 2 Security
ip dhcp snooping
ip dhcp snooping vlan 10,20
ip arp inspection vlan 10,20
interface range fa0/1 - 12
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
! Trust for uplink
interface gi0/1
 ip dhcp snooping trust
 ip arp inspection trust
end
write memory
```

```
S1# cop r s
```

Router Configurations (Syntax Only)

```
enable
configure terminal
! 3.3 Static Routes
ip route <network> <mask> <next-hop> [AD]
ipv6 route <prefix/prefix-length> <next-hop>
! 3.4 OSPFv2
router ospf <process-id>
```

```
 router-id <ip>
 network <net> <wildcard> area <area-id>
interface <interface>
 ip ospf network point-to-point
! 4.1 NAT
ip nat inside source static <local-ip> <global-ip>
ip nat inside source list <acl> pool <name> overload
access-list <num> permit <src> <wc>
ip nat pool <name> <start> <end> prefix-length <len>
interface <int>
 ip nat inside
 ip nat outside
! 4.2 NTP
ntp server <ip> [prefer]
! 5.3 Local Passwords & 5.6 ACLs
username <name> privilege <level> secret <pass>
line console 0
 login local
line vty 0 4
 login local
 transport input ssh
access-list <num> {permit|deny} <protocol> <src> <src-wc> <dst> <dst-wc>
interface <int>
 ip access-group <acl> in
end
write memory
```

Router Configuration

```
Router(config)# ho R1
R1(config)# ena sec class
R1(config)# ser pass
R1(config)# no ip dom lo
R1(config)# banner motd #Banner goes here#
R1(config)# login block-for 120 attempts 3 within 60
```

```
R1(config)# security pass min 8

R1(config)# line con 0
R1(config-line)# pass cisco
R1(config-line)# login
R1(config-line)# exec-timeout 10
R1(config-line)# line vty 0 15
R1(config-line)# pass cisco
R1(config-line)# login
R1(config-line)# exec-timeout 10

R1(config-if)# int g0/0
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# description Description goes here

R1# cop r s
Enabling SSH
R1(config)# ip domain-name CCNA-labs.com
R1(config)# cry key gen rsa general-keys mod 1024
R1(config)# username Bob secret cisco
R1(config)# line vty 0 15
R1(config-line)# login local
R1(config-line)# transport input ssh

enable
configure terminal
! 3.3 IPv4/IPv6 Static Routing
ip route 0.0.0.0 0.0.0.0 203.0.113.1          ! Default
ip route 192.168.2.0 255.255.255.0 192.168.1.2 ! Network
ip route 10.1.1.1 255.255.255.255 192.168.1.2  10 ! Host, floating (higher AD)
ipv6 route ::/0 2001:db8::1
! 3.4 OSPFv2 Single Area
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area 0          ! Broadcast (DR/BDR)
router ospf 1
area # stub no-summary
 interface serial0/0/0
  ip ospf network point-to-point              ! Point-to-point
```

```
! 4.1 Inside Source NAT (Static & Pools)
ip nat inside source static 192.168.1.10 203.0.113.10
ip nat inside source list 1 pool NATPOOL overload
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool NATPOOL 203.0.113.20 203.0.113.30 prefix-length 24
interface gi0/0
 ip nat inside
interface gi0/1
 ip nat outside
! 4.2 NTP Client/Server
ntp server  pool.ntp.org prefer
ntp server 192.168.2.1                    ! Local server
! 5.3 Device Access Control (Local Passwords)
username admin privilege 15 secret cisco123
line console 0
 login local
line vty 0 4
 login local
 transport input ssh
! 5.6 Access Control Lists
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 permit ip any any
interface gi0/1
 ip access-group 101 in
end
write memory
```