



CCNA



CCNA

About Course

CCNA (Cisco Certified Network Associate) is an information technology (IT) certification from Cisco Systems. CCNA certification is an associate-level wCisco Career certification.

CCNA

CURRICULUM

① Network Fundamentals

Explain the role and function of network components

Routers

L2 and L3 switches

Next-generation firewalls and IPS

Access points

Controllers (Cisco DNA Center and WLC)

Endpoints

Servers

② Describe characteristics of network topology architectures

2 tier

3 tier

Spine-leaf

WAN

Small office/home office (SOHO)

On-premises and cloud

3 Compare physical interface and cabling types

Single-mode fiber, multimode fiber, copper
Connections (Ethernet shared media and point-to-point)
Concepts of PoE

Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

Compare TCP to UDP

Configure and verify IPv4 addressing and subnetting

Describe the need for private IPv4 addressing

Configure and verify IPv6 addressing and pref

Compare IPv6 address types 1.9.a Global unicast

Unique local

Link local

Anycast

Multicast

Modified EUI 64

4 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

Describe wireless principles

Nonoverlapping Wi-Fi channels
SSID
RF
Encryption

5 Explain virtualization fundamentals
(virtual machines)

6 Describe switching concepts

MAC learning and aging
Frame switching
Frame flooding
MAC address table

7 2.0 Network Access

Configure and verify VLANs (normal range)
spanning multiple
switches Access ports (data and voice)
Default VLAN
Connectivity

8 Configure and verify interswitch
connectivity

Trunk ports
802.1Q
Native VLAN

**Configure and verify Layer 2 discovery protocols
(Cisco Discovery Protocol and LLDP)**

**Configure and verify (Layer 2/Layer 3) Ether
Channel (LACP)**

**Describe the need for and basic operations
of Rapid PVST+Spanning Tree Protocol and
identify basic operations**

**Root port, root bridge (primary/secondary),
and other port names**

Port states (forwarding/blocking)

PortFast benefits

Compare Cisco Wireless Architectures and AP modes

**Describe physical infrastructure connections of WLAN
components (AP, WLC, access/trunk ports, and LAG)**

**Describe AP and WLC management access connections
(Telnet, SSH, HTTP, HTTPS, console, and
TACACS+/RADIUS)**

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 3.0 IP Connectivity

Interpret the components of 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

Longest match

Administrative distance

Routing protocol metric

Configure and verify IPv4 and IPv6 static routing

Default route

Network route

Host route

Floating static

9

Configure and verify single area OSPFv2 3.4.a Neighbor adjacencies

Point-to-point

Broadcast (DR/BDR selection)

Router ID

10

Describe the purpose of first hop redundancy protocol

11

4.0 IP Services

Configure and verify inside source NAT using static and pools

Configure and verify NTP operating in a 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 levels

Configure and verify DHCP client and relay

Explain the forwarding per-hop behavior (PHB) for QoS such as

classification, marking, queuing, congestion, policing, shaping

Configure network devices for remote access using SSH

Describe the capabilities and function of TFTP/FTP in the network

12

5.0 Security Fundamentals

Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

Describe security program elements (user awareness, training, and physical access control)

Configure device access control using local passwords

Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

Describe remote access and site-to-site VPNs

Configure and verify access control lists

Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

Differentiate authentication, authorization, and accounting concepts

Describe wireless security protocols (WPA, WPA2, and WPA3)

Configure WLAN using WPA2 PSK using the GUI

6.0 Automation and Programmability

Explain how automation impacts network management
Compare traditional networks with controller-based networking

Describe controller-based and software defined architectures (overlay, underlay, and fabric)

Separation of control plane and data plane

North-bound and south-bound APIs

Compare traditional campus device management with Cisco DNA Center enabled device management

Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

Recognize the capabilities of configuration management mechanisms


Puppet, Chef, and Ansible Interpret JSON encoded data



 www.softcrayons.com

 info@softcrayons.com

 (+91) 854 501 2345

 693, Sector 14-A, Vasundhara, Ghaziabad (U.P.), 201012

   @softcrayons