

CCNA :(Routing&Switching)

Duration: 100 Hrs

CCNA Course description:

Introduces the architecture, structure, functions, components, and models of the Internet and computer networks. The principles of IP addressing and fundamentals of Ethernet concepts, media, and operations are introduced to provide a foundation for the curriculum

Key Features:

1. The CCNA certification is accepted all around the world.
2. Professionals armed with the coveted CCNA certificate are entitled to get higher paying jobs when compared to their non-certified counterparts.
3. Nowadays, more CCNA jobs are available globally, and to get one easily, possessing the CCNA certificate is a smart choice.
4. CCNA certification processes are enhancing the knowledge base of networking experts – and in many more ways than one!
5. Are you working in an IT firm at present? A CCNA certification would surely increase your chances of getting a promotion.

What are the course objectives?

This course is designed to impart detailed knowledge of Computer Networks, various protocols used in Communication, Managing and configuring Cisco Switches and Routers and various WAN technologies.

CCNA Course Benefits:

- Around the world, 93% of employers are of the notion that Cisco certified employees add more value to their business, and are more knowledgeable than their non-Cisco certified job aspirants.
- It is exclusively required by Cisco partners that they employ people with CCNA certification. Due to this reason, Cisco certification is observed as a prerequisite by the employers of many businesses.
- Clearly, all these reasons state that once you acquire the CCNA certification, you are “in-demand” within the IT industry – instantly!

CCNA Placement Training:

Best CCNA Course & Placements Training on Routers & Switches. Lab Facilities. Lowest Fees. Experienced Faculties. 100% Placement Training

CCNA Course Syllabus:

20% 1.0 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

- Describe characteristics of network topology architectures
 - 2 tier
 - 3 tier
 - Spine-leaf
 - WAN
 - Small office/home office (SOHO)
 - On-premise and cloud

- 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 prefix

 - Compare IPv6 address types
 - Global unicast
 - Unique local
 - Link local
 - Any cast
 - Multicast
 - Modified EUI 64

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

 - Describe wireless principles
 - No overlapping Wi-Fi channels
 - SSID
 - RF
 - Encryption

- Explain virtualization fundamentals (virtual machines)

 - Describe switching concepts
 - MAC learning and aging
 - Frame switching
 - Frame flooding

MAC address table

20% 2.0 Network Access

Configure and verify VLANs (normal range) spanning multiple switches

Access ports (data and voice)

Default VLAN

Connectivity

Configure and verify inter-switch connectivity

Trunk ports

2.2.b 802.1Q

2.2.c Native VLAN

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

Configure and verify (Layer 2/Layer 3) EtherChannel (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)

2.5.c PortFast benefits

2.6 Compare 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 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

25% 3.0 IP Connectivity

3.1 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

Configure and verify single area OSPFv2

Neighbor adjacencies

Point-to-point

Broadcast (DR/BDR selection)

Router ID

3.5 Describe the purpose of first hop redundancy protocol

10% 4.0 IP Services

4.1 Configure and verify inside source NAT using static address 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 device access control using local passwords

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

5.5 Describe remote access and site-to-site VPNs

5.6 Configure and verify access control lists

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

5.8 Differentiate authentication, authorization, and accounting concepts

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

5.10 Configure WLAN using WPA2 PSK using the GUI

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 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

Who should do CCNA and Certification Courses?

Final year Students B.E & Diploma I.T, C.S, E.C.E, E.E.E

Final year Students BSC C.S, I.T – Job Seeker students

Those with computer-related positions, such as **computer support specialists** and **network system administrators**, can benefit from obtaining the Cisco Certified Network Associate (CCNA) credential.

Exam & certification:

Option1: CCNA Composite 200-125 CCNA Routing & Switching.

Last date to test: February 23, 2020

Option2: ICND1 100-125 Interconnecting Cisco Networking Devices, Part 1

ICND2 200-105 Interconnecting Cisco Networking Devices Part 2

Last date to test: February 23, 2020