LITC
COMPUTER EDUCATION

Duration: 60 hours

CCNA Training – 200-301

(Cisco Certified Network Associate)

Master networking fundamentals and prepare for the official Cisco CCNA 200-301 certifications. Learn network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation programming with hands-on labs and real-world scenarios.

Prerequisites

- Basic understanding of computer networks
- Familiarity with IP addressing concepts
- Basic knowledge of operating systems
- Understanding of command-line interface

Reg. Office : Ground Floor p13, Metro Tower, near Mangal city, Vijay Nagar, Indore (M.P.)
8878855568, 9522220892, E-mail: info@litcinfore.com, litcindore@gmail.com

Duration: 60 hours

Course Syllabus (CCNA)

Module 1: Network Fundamentals (20%)

- Explain the role and function of network components
- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- 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
- Describe IPv6 address types (Unicast, Anycast, and Multicast)

Duration: 60 hours

Module 2: Network Access (20%)

- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify interswitch connectivity
- 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
- Compare Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components
- Describe AP and WLC management access connections
- Configure the components of a wireless LAN access for client connectivity

Module 3: IP Connectivity (25%)

- Interpret the components of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2
- Describe the purpose of first hop redundancy protocol
- Configure and verify HSRP (priority and preemption)
- Configure and verify EIGRP (Feasible Distance / Feasible Successors /Administrative distance)
- Configure and verify default routing
- Configure and verify network connectivity using ping, traceroute, and show commands

LITC
COMPUTER EDUCATION

Duration: 60 hours

Module 4: IP Services (10%)

- 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.

Duration: 60 hours

Module 5: Security Fundamentals (15%)

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives
- 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)

LITC
COMPUTER EDUCATION

Duration: 60 hours

Module 6: Automation and Programmability (10%)

- Explain how automation impacts network management.
- Compare traditional networks with controller-based networking.
- Describe controller-based and software defined architectures (overlay, underlay, and fabric).
- 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.
- Describe the capabilities of Cisco DNA Center.
- Configure and verify basic network programming concepts (Python scripts, EEM, and API calls).