HDTC Training Center

Provide

Technical proposal of the Training program

CISCO CCNA CERTIFICATION

Course Overview:

CCNA (200-301): Implementing and Administering Cisco Solutions is a comprehensive entry-level Cisco course that is designed to wholly equip IT personnel and technology enthusiasts (specifically, those looking to start a career in IT) with knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, automation, and programmability.

Program Objectives:

By the end of this program, participants will be able to:

- Understand networking fundamentals.
- Design and configure networks.
- Ensure network security.
- Troubleshoot and maintain networks.
- Master routing and switching.
- Learn about wireless and cloud networking.
- Manage IP addressing and subnets.
- Monitor network performance.

Program Outlines:

Network Fundamentals

- 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
- Compare IPv6 address types
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
- Explain virtualization fundamentals (virtual machines)
- Describe switching concepts

Network Access

- 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 and identify basic operations

- 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

IP Connectivity

- Interpret the components of the 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

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 behaviour (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

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 policy 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

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)
- 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

Target Audience:

- Entry-level IT personnel
- Network Engineer
- Network Analyst
- Network Support Engineer

Training methods:

- Technology-Based Learning.
- Simulation in Training.
- On-the-job guidance.
- Trainer-Led Training.
- Work Teams and Roles.
- Films and Videos.
- Case Studies and Workshops.