CCNA 200-301 Instructor-Led Training

This course is the first step towards excellence in IT sector. This CCNA certification (CCNA v1.0) course will gives you the fundamental skills and knowledge for the fresher & IT people. The course will give you deep understanding of configuring network components such as switches, routers, and wireless LAN controllers, managing network devices, and identifying basic security threats.

The CCNA certification course also gives you a foundation in network programmability, automation, and software-defined networking (SDN).

About this training

- **Study Material:-** 24*7 Lab Access, Live lectures of Training, Streaming Recorded Videos, Online Lab Workbook, and Remote Virtual Lab access.
- **Duration:-** 32 hours

What you will learn?

- Fundamental knowledge of CCNA & it's detailed concepts
- Learning and Configuring the cisco devices Understanding the foundation of networking
- Configuring & gaining the knowledge of how to secure networks Monitoring and tracking new devices
- Understanding the automation & security
- Managing and maintaining the small to medium sized networks

Certification

CCNA 200-301

About Instructor

This training course is created by one of the most experienced and multi-vendor certified trainer, verified by UniNets. He has covered each topic with an in-depth explanation. He has delivered over 80+ retail trainings across the world. He has been working as a solution architect with one of the largest IT sector company.

Course Content

- **Network Fundamentals**
  - o Explain the role and function of network components
  - o Describe characteristics of network topology architectures
  - o Compare physical interface and cabling types
  - o Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
  - o Compare TCP to UDP
  - o Configure and verify IPv4 addressing and subnetting
  - o Configure and verify IPv6 addressing and prefix
  - o Compare IPv6 address types
  - o Verify IP parameters for Client OS (Windows, Mac OS, Linux)
  - o Describe wireless principles
  - o Explain virtualization fundamentals (virtual machines)
  - o Describe switching concepts

- **Network Access**
  - o Configure and verify VLANs (normal range) spanning multiple switches
  - o Configure and verify interswitch connectivity
  - o Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
  - o Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
  - o Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
  - o Compare Cisco Wireless Architectures and AP modes
  - o Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
  - o Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
  - o 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**
  - o Determine how a router makes a forwarding decision by default
  - o Configure and verify IPv4 and IPv6 static routing
  - o Configure and verify single area OSPFv2
  - o Describe the purpose of first hop redundancy protocol

- **IP Services**
  - o Security Fundamentals
  - o Automation and Programmability

- **Security Fundamentals**
  - o Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
  - o Describe security program elements (user awareness, training, and physical access control)
  - o Configure device access control using local passwords
  - o Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
  - o Describe remote access and site-to-site VPNs
  - o Configure and verify access control lists
  - o Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
  - o Differentiate authentication, authorization, and accounting concepts
  - o Describe wireless security protocols (WPA, WPA2, and WPA3)
  - o Configure WLAN using WPA2 PSK using the GUI

- **Automation and Programmability**
  - o Explain how automation impacts network management
  - o Compare traditional networks with controller-based networking
  - o Describe controller-based and software defined architectures (overlay, underlay, and fabric)
  - o Compare traditional campus device management with Cisco DNA Center enabled device management
  - o Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
  - o Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
  - o Interpret JSON encoded data

Note: ***Most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You
Visit us

https://www.uninets.com/