Cisco Certified Network Associate (CCNA)

Cisco Certified Network Associate Security (CCNA Security) - Implementing Cisco IOS Network Security (IINS). This course provides you with the fundamentals of network security technologies. You will be trained for the Cisco Security exam 210-160. You will learn how to develop a network security infrastructure, recognize threats and discover vulnerabilities in networks. Practical exposure will be given on both Cisco firewalls and Cisco devices with secure IOS. The training will be provided by Senior Network/WAN/Security Engineers with several years of field experience.

The CCNA course is taught by world class instructors in state of the art classrooms with labs equipped with cutting edge infrastructure, including high end routers, switches and servers. The course is taught in hands on manner so that students can get an actual feel of the nitty gritty of networking.

Course Outline

- **CCNA Routing and Switching**
  - Basics of IP networking
  - Lan Switching
  - IP Addressing IPv4 and IPv6
  - Routing Protocols
  - WAN Technologies
  - Troubleshooting
- **CCNA Security**
  - Common Security threats and attacks
  - Security on Cisco Routers
  - Cisco Firewall Technologies
  - Cisco IPS
  - VPN Technologies
  - Secure Network Management and Reporting
- **CCNA Voice:**
  - Cisco Unified Communications Manager Express
  - Cisco IP Phone Concepts, Rigistration and EPhone-DNS
  - VoIP
  - PSTN and digital network convergence
  - Cisco unified communications
  - Enabling Telephony Features with CUCM

CCNA Security

Course Curriculum

Implementing Security on Cisco Routers

- Securing the Router for Administrative Access
  - Basic Router configuration
  - Control Administrative Access to Routers
  - Configuring Cisco Router using Cisco Configuration Professional (CCP)
  - SSH configuration
  - Configure Administrative Roles
    - Privilege
    - Role based CLI (VIEWS)
  - Configure IOS Resilience and Management Reporting
  - Configure Automated Security Features
- Understanding, implementing, and verifying AAA (authentication, authorization, and accounting), including the details of TACACS+ and RADIUS
- Securing Administrative Access Using AAA and RADIUS
  - Configure Local Authentication
  - Configure Local Authentication Using AAA
  - Configure Centralized Authentication Using AAA and RADIUS
  - Password Recovery on Cisco Routers

Implementing Security on Cisco Switches

- Understanding and implementing protection against Layer 2 attacks, including CAM table overflow attacks, and VLAN hopping
  - Providing Layer 2 Security by implementing VLANs
  - Secure Trunks and Access Ports
  - BPDU Guard, Port Security
  - Configure SPAN and Monitor Traffic

Cisco IOS firewall

- Default Routing
- Implement Network Address Translation (NAT) and Port Address Translation (PAT)
- Implementing Access Control List in IPv4 & IPv6
- Standard, extended, and named access control lists used for packet filtering and for the classification of traffic

Cisco IOS VPN

- Understanding VPN
- Types of VPN - Site to Site, Remote Access, SSL
- Configure a Site-to-Site VPN IPsec VPN using CCP