

CCNA (200-301) + Cisco Security

The CCNA Implementing and Administering Cisco Solutions is meant for engineers looking to get a foothold in networking. This forms the base of the Cisco training pyramid and offers different specializations for network engineers. This course gives you a strong fundamental knowledge for all IT careers. With a combination of theory and hands-on labs, you will come to learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network devices such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a Basic in network programmability, automation, and software-defined networking.

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 (200-301)

- Network Fundamentals
- Network Access
 - LAN Switching Technologies
- WAN Technologies
- IP Addressing IPv4 and IPv6
- Easy Subnetting
- IP Connectivity
 - Describe the Routing Concepts
 - Routing Technologies
- Describe IP Services
- Security Fundamentals
- NAT Technologies
- Troubleshooting

☞ CISCO Security

- Common Security threats and attacks
- Cisco IOS Firewall Technologies
- Implementing Security on Cisco Routers
- Implementing Security on Cisco Switches
- Securing Administrative Access Using AAA and RADIUS
- Configuration on User Privileges
- VPN Technologies
- Secure Network Management and Reporting



CCNA
(200-301)



Cisco
Security

We are not an Affiliated Institution. Trademarks are properties of the respective vendors.

CCNA (200-301)

Course Curriculum

Network Fundamentals

- Compare & contrast OSI & TCP/IP models
- Compare & contrast TCP & UDP protocols
- Impact of infrastructure components in a network
 - ▶ Firewalls, Access points, Wireless controllers
- Effects of cloud resources on network architecture
 - ▶ Traffic path to internal and external cloud services
 - ▶ Virtual services
 - ▶ Basic virtual network infrastructure
- Compare & contrast collapsed core and three-tier architecture
- Compare & contrast network topologies
 - ▶ Star, Mesh, Hybrid
- Select the appropriate cabling type (Straight & Cross)
- Apply troubleshooting methodologies to resolve problems
 - ▶ Perform and document fault isolation
 - ▶ Resolve or escalate
 - ▶ Verify & monitor resolution
- Configure, verify & troubleshoot IPv4 addressing & subnetting
- Compare & contrast IPv4 address types
 - ▶ Unicast, Broadcast, Multicast
- Describe the need for private IPv4 addressing
- Identify IPv6 addressing to use in LAN / WAN environment
- Configure, verify & troubleshoot IPv6 addressing
- Configure & verify IPv6 Stateless Address Auto Configuration
- Compare & contrast IPv6 address types
- Global unicast, Unique local, Link local, Multicast, Modified EUI 64, Autoconfiguration, Anycast

LAN Switching Technologies

- Describe & verify switching concepts
 - ▶ MAC learning & aging, Frame switching, Frame flooding, MAC address table
- Interpret Ethernet frame format
- Troubleshoot interface & cable issues (collisions, errors, duplex, speed)
- Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches
 - ▶ Access ports (data & voice), Default VLAN
- Configure, verify, and troubleshoot interswitch connectivity
 - ▶ Trunk ports, Add & remove VLANs on a trunk
 - ▶ DTP, VTP (v1&v2), and 802.1Q Native VLAN
- Configure, verify, & troubleshoot STP protocols
 - ▶ STP mode (PVST+ and RPVST+), STP root bridge selection
- Configure, verify & troubleshoot STP related optional features
 - ▶ PortFast, BPDU guard
- Configure & verify Layer 2 protocols
 - ▶ Cisco Discovery Protocol, LLDP
- Configure, verify, & troubleshoot (Layer 2/Layer 3) EtherChannel
 - ▶ Static, PAGP, LACP
- Describe the benefits of switch stacking & chassis aggregation

Routing Technologies

- Describe the routing concepts
 - ▶ Packet handling along the path through a network
 - ▶ Forwarding decision based on route lookup
 - ▶ Frame rewrite
- Interpret the components of a routing table
 - ▶ Prefix, Network mask, Next hop, Routing protocol code

- ▶ Administrative distance, Metric
- ▶ Gateway of last resort & Admin distance
- Configure, verify, & troubleshoot inter-VLAN routing
 - ▶ Router on a stick & SVI
- Compare & contrast static routing & dynamic routing
- Compare & contrast distance vector and link state routing protocols
- Compare & contrast interior and exterior routing protocols
- Configure, verify & troubleshoot IPv4 and IPv6 static routing
 - ▶ Default route, Network route, Host route, Floating static
- Configure, verify & troubleshoot single area & multi-area OSPFv2 for IPv4 & IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)
- Configure, verify & troubleshoot EIGRP for IPv4 & IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)
- Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)
- Troubleshoot basic Layer 3 end-to-end connectivity issues

WAN Technologies

- Configure & verify PPP and MLPPP on WAN interfaces using local authentication
- Configure, verify, & troubleshoot PPPoE client-side interfaces using local authentication
- Configure, verify, & troubleshoot GRE tunnel connectivity
- Describe WAN topology options
 - ▶ Point-to-point, Hub and spoke, Full mesh, Single vs dual-homed
- Describe WAN access connectivity options
 - ▶ MPLS, Metro Ethernet, Broadband PPPoE, Internet VPN (DMVPN), site-to-site VPN, client VPN
- Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)
- Describe basic QoS concepts
 - ▶ Marking, Device trust, Prioritization, (Voice, Video & Data)
 - ▶ Shaping, Policing, Congestion management

Infrastructure Services

- Describe DNS lookup operation
- Troubleshoot client connectivity issues involving DNS
- Configure and verify DHCP on a router (excluding static reservations)
 - ▶ Server, Relay, Client, TFTP, DNS, & gateway options
- Troubleshoot client- and router-based DHCP connectivity issues
- Configure, verify, and troubleshoot basic HSRP
 - ▶ Priority, Pre-emption, Version
- Describe common access layer threat mitigation techniques
 - ▶ Using CDP or LLDP for device discovery
 - ▶ Licensing, Logging, Time zone & Loopback
- Configure and verify initial device configuration
- Perform device maintenance
- Introduction to Controllers (Cisco DNA Center and WLC)
- 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
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure WLAN using WPA2 PSK using the GUI