

CISCO QUAD CERTIFICATION TRAINING – CCENT, CCNA, CCDA, IINS

thinQtank[®] Learning is offering a unique seven day boot camp in which students can receive four certifications in one week. As with all of our Cisco Training Experiences – exams are delivered in the classroom.

thinQtank[®] Learning Exclusive

In our classroom, students receive gigabytes of take-home CBT and lab material with over four-hundred labs to keep practicing and refining the skills learned in the classroom. Additionally, our students receive:

- ✓ thinQtank[®] Accelerated Exam Study Guides for ICND1, ICND2, IINS and CCDA
- ✓ Exam Delivery in the classroom with a 95% success rate
- ✓ Custom and focused exam preparation software and materials
- ✓ Course specific thinQtank[®] Learning publications to promote a fun and exciting learning
- ✓ Membership to the thinQtank[®] Learning University Online
- ✓ Online access and comprehensive take-home training material for the CCDA Certification
- ✓ WE DO NOT “TEACH THE TEST” – Students will receive valuable hands-on experience
- ✓ Receive all of the reading material and exam study guides as soon as you register

Q. Are There Any Prerequisites?

A. If you are seriously considering this course, you should have basic computer skills, operating systems familiarity, and basic Internet knowledge.





Material Covered Days One Through Five

The Cisco Certified Entry Networking Technician (CCENT) certification validates the ability to install, operate and troubleshoot a small enterprise branch network, including basic network security. With a CCENT, a network professional demonstrates the skills required for entry-level network support positions - the starting point for many successful careers in networking. The curriculum covers networking fundamentals, WAN technologies, basic security and wireless concepts, routing and switching fundamentals, and configuring simple networks. CCENT is the first step toward achieving CCNA, which covers medium-size enterprise branch networks with more complex connections.

The Cisco Certified Network Associate (CCNA) Routing and Switching is a certification program for entry-level network engineers that helps maximize your investment in foundational networking knowledge and increase the value of your employer's network. CCNA Routing and Switching is for Network Specialists, Network Administrators, and Network Support Engineers with 1-3 years of experience. The CCNA Routing and Switching validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks.



Material Covered Day Six and Seven

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.





CCDA Training

Cisco Certified Design Associate (CCDA) is for network design engineers, technicians, and support engineers, who enable efficient network environments with an understanding of network design fundamentals. A CCDA certified network professional demonstrates the skills required to design basic campus, data center, security, voice, and wireless networks. To prepare for the CCDA exam, students will receive hours of E-learning material and specialized exam preparation material.



What You Should Expect to Learn

- Network fundamentals covering Local Area Networks and Wide Area Networks
- Establish Internet connectivity
- Manage network device security
- Expand small to medium-sized networks with WAN connectivity
- IPv6 basics
- Review how to configure and troubleshoot a switch and router in a network environment
- Expand the switched network from a small to medium network environment
- Issues with redundant switching
- Spanning Tree Protocol (STP)
- Concepts of VLANs and Trunking
- Routing between VLANs
- Implementing VLSM
- Configure, verify, and troubleshoot OSPF and EIGRP
- When to use access control lists (ACLs) and how to configure, verify, and troubleshoot them
- Configure NAT and PAT



- Configure IPv6 addressing and Routing Information Protocol Next Generation (RIPng)
- Configure PPP, CHAP, and PAP
- Frame Relay operation and troubleshooting
- Principles of network design and the guidelines for building a network design solution
- How the Enterprise Composite Network model simplifies the complexity of today's networks
- Design an Enterprise Campus in hierarchical modular fashion
- Borderless Networks and modular design
- Design Enterprise Campus and Enterprise Edge networks
- Select the appropriate Network Management Solution
- Design a network addressing plan
- Select optimal routing protocols for the network
- Design a modern data center using Cisco and industry best practices
- Evaluate security solutions for the network
- Design Voice over IP and IP Telephony
- Design a wireless solution using Lightweight Access Points and the Wireless LAN Controller
- All topics on the CCDA certification exam
- Test-taking tips and techniques
- Develop a comprehensive network security policy to counter threats
- Configure routers with Cisco IOS Software security features
- Configure IPv6 addressing, routing, and access control in Cisco network routers
- Bootstrap the Cisco Adaptive Security Appliance (ASA) Firewall
- Configure the Cisco ASA Firewall for remote access SSL VPN
- Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations
- Configure site-to-site VPNs using Cisco IOS features
- Configure IOS IPS on Cisco network routers
- Configure security features on IOS switches to mitigate various Layer 2 attacks



- How a network can be compromised using freely available tools
- Implement line passwords, and enable passwords and secrets
- Examine Authentication, Authorization, and Accounting (AAA) concepts
- Run a CCP security audit and analyze the results
- Configure packet filtering on the Perimeter Router
- Define a virtual tunnel interface Using GRE with IPSec

Q. Once I Successfully Complete This Course, What is Next?

A.

- WIFUND - Implementing Cisco Wireless Networking Fundamentals v1.0
- IINS 2.0 - Implementing Cisco IOS Network Security
- ROUTE - Implementing Cisco IP Routing v1.0
- SWITCH - Implementing Cisco IP Switched Networks v1.0
- CCNP Training Camp
- CCNP Security Training Camp





Course Outline

- Building a Simple Network
 - Exploring the Functions of Networking
 - Host-to-Host Communications Model
 - Introducing LANs
 - Operating Cisco IOS Software
 - Starting a Switch
 - Ethernet and Switch Operation
 - Troubleshooting Common Switch Media Issues
- Establishing Internet Connectivity
 - TCP/IP Internet Layer
 - IP Addressing and Subnets
 - TCP/IP Transport Layer
 - Exploring the Functions of Routing
 - Configuring a Cisco Router
 - Exploring the Packet Delivery Process
 - Enabling Static Routing
 - Managing Traffic Using ACLs
 - Enabling Internet Connectivity
- Managing Network Device Security
 - Securing Administrative Access
 - Implementing Device Hardening
 - Implementing Traffic Filtering with ACLs
- Building a Medium-Sized Network
 - Implementing VLANs and Trunks



- Routing Between VLANs
- Using a Cisco Network Device as a DHCP Server
- WAN Technologies
- Dynamic Routing Protocols
- Implementing OSPF
- Introducing IPv6
 - Basic IPv6
 - Configuring IPv6 Routing
- Small Network Implementation
- Medium-Sized Switched Network Construction
 - VLANs and Trunks
 - Spanning Tree Performance Optimization
 - Routing Between VLANs
 - Securing the Expanded Network
 - Troubleshooting Switched Networks
- Medium-Sized Routed Network Construction
 - Routing Operations
 - Implementing VLSM
- Single-Area Open Shortest Path First (OSPF)
 - Implementing OSPF
 - Troubleshooting OSPF
- Enhanced Interior Gateway Routing Protocol (EIGRP)
 - Implementing EIGRP
 - Troubleshooting EIGRP
- Access Control Lists (ACLs)
 - ACL Operation



- Configuring and Troubleshooting ACLs
- Address Space Management
 - Scaling the Network with NAT and PAT
 - Transitioning to IPv6
- LAN Extension into a WAN
 - VPN Solutions
 - Establishing a Point-to-Point WAN Connection with PPP
 - Establishing a WAN Connection with Frame Relay
 - Troubleshooting Frame Relay WANs
- Applying a Methodology to Network Design
 - SONA
 - Identifying Design Requirements
 - Characterizing the Existing Network
 - Using the Top-Down Approach
 - Implementing the Design Methodology
- Structuring and Modularizing the Network
 - Designing the Network Hierarchy
 - Modular Approach to Network Design
 - Infrastructure Services
 - Network Management Protocols and Features
- Campus and Data Center Design Considerations
 - Campus Design Methodology
 - Designing the Campus Infrastructure Module
 - Enterprise Data Center Considerations
- Remote Connectivity Design
 - Enterprise Edge WAN Design Methodology



- Selecting Wide Area Network (WAN) Technology
- Designing the Enterprise Branch
- IP Addressing Design and Routing Protocols Selection
 - Designing IP Addressing
 - IPv6
 - Enterprise Routing Protocols
- Security Solutions for the Network
 - Defining Network Security
 - Cisco Self-Defending Network
 - Selecting Network Security Solutions
- Voice Networking Design
 - Traditional Voice Architectures and Features
 - Integrating Voice Architectures
 - Voice Technology Requirements
- Wireless Network Considerations
 - Cisco Unified Wireless Network
 - Wireless Network Controller Technologies
 - Designing Wireless Networks with Controllers
- Networking Security Fundamentals
 - Networking Security Concepts
 - Security Policies Using a Lifecycle Approach
 - Building a Security Strategy for Borderless Networks
- Protecting the Network Infrastructure
 - Cisco Network Foundation Protection
 - Protecting the Network Infrastructure Using Cisco Configuration Professional
 - Securing the Management Plane on Cisco IOS Devices



- Configuring AAA on Cisco IOS Devices Using Cisco Secure ACS
- Securing the Data Plane on Cisco Catalyst Switches
- Securing the Data Plane in IPv6 Environments
- Threat Control and Containment
 - Planning a Threat Control Strategy
 - Implementing Access Control Lists for Threat Mitigation
 - Firewall Fundamentals
 - Implementing Cisco IOS Zone-Based Policy Firewalls
 - Configuring Basic Firewall Policies on Cisco ASA
 - IPS Fundamentals
 - Implementing Cisco IOS IPS
- Secure Connectivity
 - Fundamentals of VPN Technologies
 - Public Key Infrastructure
 - IPSec Fundamentals
 - Implementing Site-to-Site VPNs on Cisco IOS Routers
 - Implementing SSL VPNs Using Cisco ASA



Exam Information

- 100-101 – Interconnecting Cisco Networking Devices Part 1 (ICND1) v2.0
- 200-101 – Interconnecting Cisco Networking Devices Part 2 (ICND2) v2.0
- 200-310 – Designing for Cisco Internetwork Solutions (DESGN) v3.0
- 210-260 – Implementing Cisco Network Security (IINS)

