529 Hahn Ave. Suite 101 ♦ Glendale CA 91203-1052 ♦ Tel 818.550.0770 ♦ Fax 818.550.8293 ♦ www.brandcollege.edu

Cisco Certified Network Expert (CCNE)

Program Summary

This instructor-led program with a combination of lecture and hands-on laboratory exercises covers networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized.

This program is also designed to build advanced or journeyman knowledge of both LAN and WAN infrastructure implementations in a Cisco environment. This set of courses builds on the concepts introduced in the CCNA program. Students will be exposed to more in-depth concepts relating to routing implementation and design; TCP/IP design strategies; switching concepts; WAN optimization and performance issues; as well as, basic troubleshooting/support techniques and approaches. Some of the many protocols that will be studied include: TCP/IP, RIP, EIGRP, OSPF, IS-IS, BGP. Other topics include: VLAN implementation and management; spanning-tree protocol; multicast management; remote access implementation; Cisco security features including AAA; subnet concepts, design considerations, and implementation; VLSM; CIDR and more.

In addition, this program covers advanced topics and concepts related to securing Cisco networks. This course covers a wide array of security topics including: Cisco IOS firewall implementation; PIX firewall technology and features; VPN concepts and implementation; IPSec; implementation and design of intrusion detection systems; Cisco's SAFE implementation; AAA; protocol monitoring and management and much more. The goal of this course is to give the student the tools and knowledge necessary to secure and manage complex network infrastructures – protecting data and productivity, as well as, reducing costs.

This program provides the skills and knowledge necessary to pass the Cisco certifications including Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP Route & Switch), and Cisco Certified Security Professional (CCNP Security).

- Certification program
- 576 Contact Hours, 36 Credit Hours, 72 Weeks

TERM 1

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE100	Expert I	6	96
	Total	**6**	**96**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE110	Expert II	3	48
CCE120	Expert III	3	48
	Total	**6**	**96**

TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE130	Expert IV	6	96
	Total	**6**	**96**

TERM 4

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE140	Expert V	3	48
CCE150	Expert VI	3	48
	Total	**6**	**96**

TERM 5

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP160	Expert VII	3	48
CCE170	Expert VIII	3	48
	Total	**6**	**96**

TERM 6

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE180	Expert IX	6	96
	Total	**6**	**96**

Prerequisites
Candidates wishing to enter this course should have completed either a Microsoft or Linux+ networking program or have commensurate experience with PC networking and TCP/IP.

Type of Document Received Upon Graduation
Upon successful completion of all program requirements, each student will be awarded a Certificate of Completion.

Certification Tests
All certification exams are scored on a pass/fail basis. Depending on the specific exam, a correct response to 75% - 80% of the questions will be required to achieve a passing score. Students are encouraged to take exams immediately following completion of the corresponding course.

Career Development
Students who successfully complete this program will be prepared for midlevel to advanced professional opportunities in the IT field with emphasis on installation, configuration and maintenance of Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Sr. Network Design Engineer, Sr. Network Security Engineer, Sr. Network Design Specialist, Sr. Network Systems Manager, Network Support or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 15-1143 Computer Network Architects
- 25-1021 Computer Science Teacher, Postsecondary
- 11-3021 Computer & Information System Manager

CCNE Program Details

COURSE CCE100

Title: Cisco Certified Network Associate
Exam: 200-120

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises covers basic networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized. This is an advanced course providing the skills and knowledge necessary to pass the Cisco certification exam (one exam) necessary to become a Cisco Certified Network Associate (CCNA).

Course Objectives

This course will cover the following subjects:

Operation of IP Data Networks

- Recognize the purpose and functions of various network devices such as Routers, Switches, Bridges and Hubs
- Select the components required to meet a given network specification
- Identify common applications and their impact on the network
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models
- Predict the data flow between two hosts across a network
- Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN

LAN Switching Technologies

- Determine the technology and media access control method for Ethernet networks
- Identify basic switching concepts and the operation of Cisco switches
- Configure and verify initial switch configuration including remote access management
- Verify network status and switch operation using basic utilities
- Describe how VLANs create logically separate networks and the need for routing between them
- Configure and verify VLANs
- Configure and verify trunking on Cisco switches
- Identify enhanced switching technologies
- Configure and verify PVSTP operation

IP Addressing

- Describe the operation and necessity of using private and public IP addresses for IPv4 addressing
- Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
- Identify the appropriate IPv4 addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment
- Describe the technological requirements for running IPv6 in conjunction with IPv4
- Describe IPv6 addresses

IP Routing Technologies

- Describe basic routing concepts
- Configure and verify utilizing the CLI to set basic router configuration

- Configure and verify operation status of a device interface
- Verify router configuration and network connectivity using
- Configure and verify routing configuration for a static or default route given specific routing requirements
- Differentiate methods of routing and routing protocols
- Configure and verify OSPF
- Configure and verify interVLAN routing (Router on a stick)
- Configure SVI interfaces
- Manage Cisco IOS Files
- Configure and verify EIGRP (single AS)

IP Services
- Configure and verify DHCP (IOS Router)
- Describe the types, features, and applications of ACLs
- Configure and verify ACLs in a network environment
- Identify the basic operation of NAT
- Configure and verify NAT for given network requirements
- Configure and verify NTP as a client
- Recognize High availability (FHRP)
- Configure and verify syslog
- Describe SNMP v2 and v3

Network Device Security
- Configure and verify network device security features
- Configure and verify switch port security
- Configure and verify ACLs to filter network traffic
- Configure and verify an ACLs to limit telnet and SSH access to the router

Troubleshooting
- Troubleshoot and correct common problems associated with IP addressing and host configurations
- Troubleshoot and resolve VLAN problems
- Troubleshoot and resolve trunking problems on Cisco switches
- Troubleshoot and resolve ACL issues
- Troubleshoot and resolve Layer 1 problems
- Identify and correct common network problems
- Troubleshoot and resolve spanning tree operation issues
- Troubleshoot and resolve routing issues
- Troubleshoot and resolve OSPF problems
- Troubleshoot and resolve EIGRP problems
- Troubleshoot and resolve interVLAN routing problems
- Troubleshoot and resolve WAN implementation issues
- Monitor NetFlow statistics
- Troubleshoot EtherChannel problems

WAN Technologies
- Identify different WAN Technologies
- Configure and verify a basic WAN serial connection
- Configure and verify a PPP connection between Cisco routers
- Configure and verify frame relay on Cisco routers
- Implement and troubleshoot PPPoE

COURSE CCE110

Title: Implementing Cisco IP Routing (ROUT)
Exam: 300-101

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to use advanced IP addressing and routing in implementing scalability for Cisco ISR routers connected to LANs and WANs. The exam covers topics on Advanced IP Addressing, Routing Principles, Multicast Routing, IPv6, Manipulating Routing Updates, Configuring basic BGP, Configuring EIGRP, OSPF, and IS-IS.

Course Objectives

This course will cover the following subjects:

- Identify Cisco Express Forwarding Concepts
- Explain General Network Challenges
- Describe IP Operations
- Explain TCP Operations
- Describe UDP Operations
- Recognize Proposed Changes to the Network
- Configure and Verify PPP
- Explain Frame Relay
- Identify, Configure, and Verify IPv4 addressing and subnetting
- Identify IPv6 Addressing and Subnetting
- Configure and Verify Static Routing
- Configure and Verify Default Routing
- Evaluate Routing Protocol Types
- Configure and Verify GRE
- Describe DMVPN
- Describe Easy Virtual Networking
- Describe IOS AAA Using Local Database
- Describe Device Security Using IOS AAA with TACACS+ and RADIUS
- Configure and Verify Device Access Control
- Configure and Verify Router Security Features
- Configure and Verify Device Management
- Configure and Verify SNMP
- Configure and Verify Logging
- Configure and Verify Network Time Protocol
- Configure and Verify IPv4 and IPv6 DHCP
- Configure and Verify IPv4 Network Address Translation
- Describe IPv6 NAT
- Describe SLA Architecture
- Configure and Verify IP SLA
- Configure and Verify Tracking Objects
- Configure and Verify Cisco NetFlow

COURSE CCE120

Title: Implementing Cisco Switched Network (SWITCH)
Exam: 300-115

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to implement scalable multilayer switched networks. The exam includes topics on Campus Networks, describing and implementing advanced Spanning Tree concepts, VLANs and Inter-VLAN routing, High Availability, Wireless Client Access, Access Layer Voice concepts, and minimizing service Loss and Data Theft in a Campus Network.

Course Objectives

This course will cover the following subjects:

- Configure and Verify Switch Administration
- Configure and Verify Layer 2 Protocols
- Configure and Verify VLANs
- Configure and Verify Trunking
- Configure and Verify EtherChannels
- Configure and Verify Spanning Tree
- Configure and Verify Other LAN Switching Technologies
- Describe Chassis Virtualization and Aggregation Technologies
- Configure and Verify Switch Security Features
- Describe Device Security Using Cisco IOS AA with TACACS+ and RADIUS
- Configure and Verify First-Hop Redundancy Protocols

COURSE CCE130

Title: Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)
Exam: 300-135

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to secure and expand the reach of an enterprise network to (1) plan and perform regular maintenance on complex enterprise routed and switched networks and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting.

Course Objectives

This course will cover the following subjects:

- Use Cisco IOS Troubleshooting Tools
- Apply Troubleshooting methodologies
- Troubleshoot Switch Administration
- Troubleshoot Layer 2 Protocols
- Troubleshoot VLANs
- Troubleshoot Trunking
- Troubleshoot EtherChannels
- Troubleshoot Spanning Tree
- Troubleshoot other LAN Switching Technologies
- Troubleshoot Chassis Virtualization and Aggregation Technologies
- Troubleshoot IPv4 Addressing and Subnetting
- Troubleshoot IPv6 Addressing and Subnetting
- Troubleshoot Static Routing
- Troubleshoot Default Routing
- Troubleshoot Administrative Distance
- Troubleshoot GRE
- Troubleshoot IOS AAA using Local Database
- Troubleshoot Device Access Control
- Troubleshoot Router Security Features
- Troubleshoot Device Management
- Troubleshoot SNMP
- Troubleshoot Logging
- Troubleshoot Network Time Protocol
- Troubleshoot IPv4 and IPv6 DHCP
- Troubleshoot IPv4 Network Address Translation
- Troubleshoot SLA Architecture
- Troubleshoot Tracking Objects

COURSE CCE140

Title: Implementing Cisco Network Security (IINS)
Exam: 210-260

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the CCNA Security certification. This exam tests a candidate's knowledge of securing Cisco routers and switches and their associated networks. It leads to validated skills for installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices and develops competency in the technologies that Cisco uses in its security infrastructure.

Course Objectives

This course will cover the following subjects:

- Common Security Principals
- Common Security Treats
- Cryptography Concepts
- Describe Network Topologies
- Secure Management
- AAA Concepts
- 802.1X Authentication
- BYOD
- VPN Concepts
- Remote Access VPN
- Site to Site VPN
- Security on Cisco Routers
- Securing Routing Protocols
- Securing the Control Plane
- Common Layer to Attacks
- Mitigation Procedures
- VLAN security
- Describe Operational Strengths and weaknesses of the Different Firewall Technologies
- Compare Stateful vs. Stateless Firewalls
- Implement NAT on Cisco ASA 9.x
- Implement Zone-Based Firewall
- Firewall Features on the Cisco Adaptive Security Appliance 9.x
- Describe IPS Deployment Considerations
- Describe IPS Technologies
- Describe Mitigation Technology for Email-Based Treats
- Describe Mitigation Technology for Web-Based Treats
- Describe Mitigation Technology for Endpoint Treats

COURSE CCE150

Title: Implementing Cisco Secure Access Solutions (SISAS)
Exam: 300-208

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is one of the exams associated with the CCNP Security certification. This course will cover the components and architecture of secure access, by utilizing 802.1X and Cisco TrustSec. It includes knowledge of Cisco Identity Services Engine (ISE) architecture, solution, and components as an overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD) using posture and profiling services of ISE. Candidates can prepare for this exam by taking the Implementing Cisco Secure Access Solutions (SISAS) course.

Course Objectives

This course will cover the following subjects:

- Implement Device Administration
- Describe Identity Management
- Implement Wired/Wireless 802.1X
- Implement MAB
- Implement network authorization enforcement
- Implement Central Web Authentication
- Implement Profiling
- Implement Guest Services
- Implement Posture Services
- Implement BYOD Access
- Describe TrustSec Architecture
- Troubleshoot Identity Management Solutions
- Design Highly Secure Wireless Solution with ISE
- Device Administration
- Identity Management
- Profiling
- Guest Services
- Posturing Services
- BYOD Access

COURSE CCE160

Title: Implementing Cisco Edge Network Security Solutions (SENSS)
Exam: 300-206

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is one of the exams associated with the CCNP Security. The Implementing Cisco Edge Network Security Course includes the knowledge of a network security engineer to configure and implement security on Cisco network perimeter edge devices such as a Cisco switch, Cisco router, and Cisco ASA firewall. This course focuses on the technologies used to strengthen security of a network perimeter such as Network Address Translation (NAT), ASA policy and application inspect, and a zone-based firewall on Cisco routers.

Course Objectives

This course will cover the following subjects:

- Implement Firewall
- Implement Layer 2 Security
- Configure Device Hardening Per Best Practices
- Implement SSHv2, HTTPS, and SNMPv3 Access on the Network Devices
- Implement RBAC on the ASA/IOS using CLI and ASDM
- Describe Cisco Prime Infrastructure
- Describe Cisco Security Manager
- Implement Device Mangers
- Configure NetFlow Exporter on Cisco Routers, Switches, and ASA
- Implement SNMPv3
- Implement Logging on Cisco Routers, Swtiches, and ASA Using Cisco Best Practices
- Implement NTP with Authentication on Cisco Routers, Switches, and ASA
- Describe CDP, DNS, SCP, SFTP, and DHCP
- Analyze Packet Tracer on the Fire Using CLI/ASDM
- Configure and Analyze Packet Capture Using CLI/ASDM
- Analyze Syslog Events Generated From ASA
- Design a Firewall Solution
- Layer 2 Security Solutions
- Describe Security Operations Management Architectures
- Describe Data Center Security Components and Considerations
- Describe Common IPv6 Security Considerations

COURSE CCE170

Title: Implementing Cisco Secure Mobility Solutions (SIMOS)
Exam: 300-209

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the Implementing Cisco Secure Mobility Solutions (SIMOS) tests a network security engineer on the variety of Virtual Private Network (VPN) solutions that Cisco has available on the Cisco ASA firewall and Cisco IOS software platforms. This course provides the knowledge necessary to properly implement highly secure remote communications through VPN technology, such as remote access SSL VPN and site-to-site VPN (DMVPN, FlexVPN). Candidates can prepare for this exam by taking the Implementing Cisco Secure Mobility Solutions (SIMOS) course.

Course Objectives

This course will cover the following subjects:

- Site-to-Site VPNs on Routers and Firewalls
- Describe GETVPN
- Implement IPsec
- Implement DMVPN
- Implement FlexVPN
- Implement Remote Access VPNs
- Implement AnyConnect IKEv2 VPNs on ASA and Routers
- Implement AnyConnect SSLVPN on ASA and Routers
- Implement Clientless SSLVPN on ASA and Routers
- Implement FLEX VPN on Routers
- Troubleshoot VPN Using ASDM & CLI
- Troubleshoot IPsec
- Troubleshoot DMVPN
- Troubleshoot FlexVPN
- Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and Routers
- Troubleshoot Clientless SSLVPN on ASA and Routers
- Design Site-to-Site VPN Solutions
- Identify Functional Components of GETVPN, FlexVPN, DMVPN, and IPsec
- VPN Technology Consideration Based on Functional Requirements
- High Availability Consideration
- Identify VPN Technology Based on Configuration Output
- Design Remote Access VPN Solution
- Clientless SSL Browser and Client Considerations / Requirements
- Identify Split Tunneling Requirements
- Describe Encryption, Hashing, and Next generation Encryption (NGE)
- Describe PKI Components Protection Methods
- Compare and Contrast SSL, DTLS, and TLS

COURSE CCE180

Title: Implementing Cisco Threat Control Solutions (SITCS)
Exam: 300-207

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the Cisco Certified Network Professional Security certification. The Implementing Cisco Threat Control Solutions (SITCS) provides a network security engineer on advanced firewall architecture and configuration with the Cisco next-generation firewall, utilizing access and identity policies. This Course covers integration of Intrusion Prevention System (IPS) and context-aware firewall components, as well as Web (Cloud) and Email Security solutions. Candidates can prepare for this exam by taking the Implementing Cisco Threat Control Solutions (SITCS) course.

Course Objectives

This course will cover the following subjects:

- Cisco ASA 5500-X NGFW Security Services
- Describe Features and Functionality
- Implement Web Usage Control
- Implement AVS
- Cisco Cloud Web Security
- Implement IOS and ASA Connectors
- Implement AnyConnect Web Security Module
- Implement Anti-Malware
- Cisco WSA
- Implement Data Security
- Describe Decryption Policies
- Describe Traffic Redirection and Capture Methods
- Cisco ESA
- Implement email Encryption
- Implement Anti-Spam Policies
- Implement Virus Outbreak Filter
- Network IPS
- Implement Traffic Redirection and Capture Methods
- Implement Network IPS Deployment Modes
- Describe Signatures Enginees
- Configure Device Hardening Per Best practices
- Content Security
- Configure IME and IP Logging for IPS
- Content Security
- Monitor Cisco Security IntelliShield
- Design IPS Solution
- Design Web Security Solution
- Design Email Security Solution
- Design Application Security Solution