



Dear Candidate,

We would like to take this opportunity to thank you for inquiring about our training services here at Brand College. This package has been compiled to provide the information you will need to choose the training program that will be most beneficial for you.

In this package, you will find information on:

- Our organization and its philosophy
- Training programs we offer
- Details on the training program of your inquiry

Every journey begins with a first step. You have already taken this first step by expressing interest in pursuing an educational program. We would welcome the opportunity to be your partner on this journey and help you complete your journey successfully.

Brand College was founded in direct response to the overwhelming demand for qualified computer professionals in today's information age. Armed with extensive background in information technology consulting and training, we are committed to providing students with high quality education that is relevant for today's rapidly changing IT environment. Our team is comprised of certified engineers and trainers who, as a group, have accumulated more than fifty years of practical experience in the field of information technology. Our goal is to maximize each student's educational experience by ensuring that entry-level students are not overwhelmed while more experienced students remain challenged.

Brand College currently offers several certification programs including:

- **CompTIA A+** PC Hardware Technician
- **CompTIA Linux+** Linux Certified Professional
- **MCITP** Microsoft Certified IT Professional
- **CCNA** Cisco Certified Network Associate
- **CCNA Voice** Cisco Certified Network Associate Voice
- **CCNP** Cisco Certified Network Professional
- **CCSP** Cisco Certified Security Professional
- **CCVP** Cisco Certified Voice Professional
- **CNTE** Certified Network Technologies Expert
- **CDNS** Certified Desktop and Network Specialist
- **CLWS** Certified LAN and WAN Specialist
- **CMNS** Certified Multi-Platform Network Specialist
- **CCNE** Cisco Certified Network Expert

Once again, thank you for your inquiry and we look forward to hearing from you in the very near future. Should you have any questions, please do not hesitate to contact our Admissions department by e-mail at [info@brandcollege.us](mailto:info@brandcollege.us) or by phone at (818) 550-0770.

Sincerely,

Brand College

### **Certified Cisco Network Expert (CCNE)**

This program 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 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, and Cisco Certified Security Professional (CCSP).

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

#### **TERM 1**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
CCA100	CISCO I	6	96
<b>Total</b>		<b>6</b>	<b>96</b>

#### **TERM 2**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
CCA110	CISCO II	3	48
CCA120	CISCO III	3	48
<b>Total</b>		<b>6</b>	<b>96</b>

#### **TERM 3**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
CCA130	CISCO IV	3	48
CCA140	CISCO V	3	48
<b>Total</b>		<b>6</b>	<b>96</b>

**TERM 4**

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP100	Security I	3	48
CSP110	Security II	3	48
<b>Total</b>		<b>6</b>	<b>96</b>

**TERM 5**

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP120	Security III	3	48
CSP130	Security IV	3	48
<b>Total</b>		<b>6</b>	<b>96</b>

**TERM 6**

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP140	Security V	6	96
<b>Total</b>		<b>6</b>	<b>96</b>

**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.

## CCNE Program Details

### COURSE CCA100

Title: Cisco Certified Network Associate

Exam: 640-802

#### **Describe how a network works**

- Describe the purpose and functions of various network devices
- Select the components required to meet a network specification
- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- Describe common networked applications including web applications
- Describe the purpose and basic operation of the protocols in the OSI and TCP models
- Describe the impact of applications (Voice Over IP and Video Over IP) on a network
- Interpret network diagrams
- Determine the path between two hosts across a network
- Describe the components required for network and Internet communications
- Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach
- Differentiate between LAN/WAN operation and features

#### **Configure, verify and troubleshoot a switch with VLANs and interswitch communications**

- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- Explain the technology and media access control method for Ethernet networks
- Explain network segmentation and basic traffic management concepts
- Explain basic switching concepts and the operation of Cisco switches
- Perform and verify initial switch configuration tasks including remote access management
- Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands
- Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures
- Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q)
- Describe how VLANs create logically separate networks and the need for routing between them
- Configure, verify, and troubleshoot VLANs
- Configure, verify, and troubleshoot trunking on Cisco switches
- Configure, verify, and troubleshoot interVLAN routing
- Configure, verify, and troubleshoot VTP
- Configure, verify, and troubleshoot RSTP operation
- Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.
- Implement basic switch security (including: port security, trunk access, management vlan other than vlan1, etc.)

#### **Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network**

- Describe the operation and benefits of using private and public IP addressing
- Explain the operation and benefits of using DHCP and DNS
- Configure, verify and troubleshoot DHCP and DNS operation on a router.(including: CLI/SDM)
- Implement static and dynamic addressing services for hosts in a LAN environment
- Calculate and apply an addressing scheme including VLSM IP addressing design to a network
- Determine the appropriate classless 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 (including: protocols, dual stack, tunneling, etc).
- Describe IPv6 addresses
- Identify and correct common problems associated with IP addressing and host configurations

#### **Configure, verify, and troubleshoot basic router operation and routing on Cisco devices**

- Describe basic routing concepts (including: packet forwarding, router lookup process)
- Describe the operation of Cisco routers (including: router bootup process, POST, router components)
- Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
- Configure, verify, and troubleshoot RIPv2
- Access and utilize the router to set basic parameters.(including: CLI/SDM)
- Connect, configure, and verify operation status of a device interface
- Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities
- Perform and verify routing configuration tasks for a static or default route given specific routing requirements
- Manage IOS configuration files. (including: save, edit, upgrade, restore)
- Manage Cisco IOS.
- Compare and contrast methods of routing and routing protocols
- Configure, verify, and troubleshoot OSPF
- Configure, verify, and troubleshoot EIGRP
- Verify network connectivity (including: using ping, traceroute, and telnet or SSH)
- Troubleshoot routing issues
- Verify router hardware and software operation using SHOW & DEBUG commands.
- Implement basic router security

#### **Explain and select the appropriate administrative tasks required for a WLAN**

- Describe standards associated with wireless media (including: IEEE WI-FI Alliance, ITU/FCC)
- Identify and describe the purpose of the components in a small wireless network. (Including: SSID, BSS, ESS)
- Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
- Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)
- Identify common issues with implementing wireless networks. (Including: Interface, misconfiguration)

#### **Identify security threats to a network and describe general methods to mitigate those threats**

- Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats
- Explain general methods to mitigate common security threats to network devices, hosts, and applications
- Describe the functions of common security appliances and applications
- Describe security recommended practices including initial steps to secure network devices

#### **Implement, verify, and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network.**

- Describe the purpose and types of ACLs
- Configure and apply ACLs based on network filtering requirements.(including: CLI/SDM)
- Configure and apply an ACLs to limit telnet and SSH access to the router using (including: SDM/CLI)
- Verify and monitor ACLs in a network environment
- Troubleshoot ACL issues
- Explain the basic operation of NAT
- Configure NAT for given network requirements using (including: CLI/SDM)
- Troubleshoot NAT issues

#### **Implement and verify WAN links**

- Describe different methods for connecting to a WAN

- Configure and verify a basic WAN serial connection
- Configure and verify Frame Relay on Cisco routers
- Troubleshoot WAN implementation issues
- Describe VPN technology (including: importance, benefits, role, impact, components)
- Configure and verify a PPP connection between Cisco routers

### COURSE CCA110

Title: Building Scalable Cisco Internetworks (BSCI)

Exam: 642-901

- List the Key Information Routers Needs to Route Data
- Describe Classful & Classless Routing Protocols
- Describe Link-State Router Protocol Operation
- Compare Classful & Classless Routing Protocols
- Compare Distance Vector & Link State Routing Protocols
- Describe Concepts to Extending IP Addresses & the Use of VLSMs to Extend IP addresses
- Describe the Features & Operation of EIGRP
- Describe the Features & Operation of Single Area OSPF
- Describe the Hierarchical Structure of IS-IS Areas
- Describe the Features & Operation of BGP

### COURSE CCA120

Title: Building Cisco Multilayer Switched Networks (BCMSN)

Exam: 642-812

- Describe the Enterprise Composite Model used for designing networks and explain how it addresses enterprise network needs for performance, scalability and availability
- Describe the physical, data-link and network layer technologies used in a switched network, and identify when to use each
- Explain the role of switches in the various modules of the Enterprise Composite Model (Campus Infrastructure, Server Farm, Enterprise Edge, Network Management)
- Explain the function of the Switching Database Manager [specifically Content Addressable Memory (CAM) and Ternary Content Addressable Memory (TCAM)] within a Catalyst switch
- Describe the features and operation of VLANs on a switched network
- Describe the features of the VLAN trunking protocols including 802.1Q, ISL (emphasis on 802.1Q) and dynamic trunking protocol
- Describe the features and operation of 802.1Q Tunneling (802.1QinQ) within a service provider network
- Describe the operation and purpose of managed VLAN services
- Describe how VTP versions 1 and 2 operate including domains, modes, advertisements, and pruning
- Explain the function of the Switching Database Manager [specifically Content Addressable Memory (CAM) and Ternary Content Addressable Memory (TCAM)] within a Catalyst switch

### COURSE CCA130

Title: Implementing Secure Converged Wide Area Networks (ISCW)

Exam: 642-825

- Describe how different WAN technologies can be used to provide remote access to a network, including asynchronous dial-in, Frame Relay, ISDN, cable modem, and DSL
- Describe traffic control methods used to manage traffic flow on WAN links

- Explain the operation of remote network access control methods
- Identify PPP components, and explain the use of PPP as an access and encapsulation method
- Configure asynchronous modems and router interfaces to provide network access
- Configure frame relay operation and traffic control on WAN links
- Design a Cisco remote access solution using asynchronous dial-up technology
- Design a Cisco frame relay infrastructure to provide access between remote network components
- Plan traffic shaping to meet required quality of service on access links
- Troubleshoot non-functional remote access systems

### COURSE CCA140

Title: Optimizing Converged Cisco Networks (ONT)

Exam: 642-845

- Establish an optimal system baseline
- Diagram and document system topology
- Document end system configuration
- Verify connectivity at all layers
- Select an optimal troubleshooting approach
- Plan a network documentation system
- Plan a baseline monitoring scheme
- Plan an approach to troubleshooting that minimizes system downtime
- Use Cisco IOS commands and applications to identify system problems at all layers
- Isolate system problems to one or more specific layers
- Resolve sub-optimal system performance problems at layers 2 through 7
- Resolve local connectivity problems at layer 1
- Restore optimal baseline service
- Work with external providers to resolve service provision problems
- Work with system users to resolve network related end-use problems

### COURSE CSP100

Title: Implementing Cisco IOS Network Security

Exam: 640-553

- Describe and list mitigation methods for common network attacks
- Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
- Describe the Cisco Self Defending Network architecture
- Secure Cisco routers using the SDM Security Audit feature
- Use the One-Step Lockdown feature in SDM to secure a Cisco router
- Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
- Secure administrative access to Cisco routers by configuring multiple privilege levels
- Secure administrative access to Cisco routers by configuring role based CLI
- Secure the Cisco IOS image and configuration file
- Explain the functions and importance of AAA
- Describe the features of TACACS+ and RADIUS AAA protocols
- Configure AAA authentication
- Configure AAA authorization
- Configure AAA accounting
- Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets

- Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI
- Configure IP ACLs to prevent IP address spoofing using CLI
- Discuss the caveats to be considered when building ACLs
- Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
- Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server
- Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features
- Describe the operational strengths and weaknesses of the different firewall technologies
- Explain stateful firewall operations and the function of the state table
- Implement Zone Based Firewall using SDM
- Define network based vs. host based intrusion detection and prevention
- Explain IPS technologies, attack responses, and monitoring options
- Enable and verify Cisco IOS IPS operations using SDM
- Explain the different methods used in cryptography
- Explain IKE protocol functionality and phases
- Describe the building blocks of IPSec and the security functions it provides
- Configure and verify an IPSec site-to-site VPN with pre-shared key authentication using SDM

## COURSE CSP110

Title: Securing Networks with Cisco Routers & Switches (SNRS)

Exam: 642-503

- Utilize Cisco IOS commands to mitigate Layer 2 attacks
- Implement Cisco Identity-Based Networking Services on Cisco Catalyst Switches
- Implement Identity Management using ACS as the Authentication Server
- Identify and describe the advanced capabilities of the IOS firewall feature set
- Configure IOS Firewall to dynamically mitigate identified threats to the network
- Verify and troubleshoot IOS Firewall configuration and operation.
- Configure authentication proxy to apply security policies on a per-user basis
- Verify and troubleshoot authentication proxy configuration and operation
- Configure IOS zone-based Firewalls
- Troubleshoot Zone-based Firewalls
- Configure APPFW application Firewalls
- Configure Granular Protocol Inspection
- Identify and describe the advanced capabilities of the IOS-IPS feature
- Configure the IPS features to identify threats and dynamically block them from entering the network
- Verify and troubleshoot IPS operation
- Describe IPSec features and functionality
- Configure secure connectivity for site-to-site IPSec VPN using pre-shared keys
- Describe GRE features and functionality
- Configure secure connectivity for site-to-site VPN using certificate authorities
- Describe DMVPN features and functionality
- Configure secure connectivity for site-to-site VPN using DMVPN
- Verify and troubleshoot secure site-to-site connectivity operations
- Implement Clientless IOS SSL VPN
- Verify Clientless IOS SSL VPNs
- Configure Easy VPN server with pre-shared keys
- Configure administrative access to the CSACS server
- Configure CSACS system settings
- Configure AAA clients on the CSACS
- Configure users, groups and access rights

- Configure shared profile components in CSACS
- Configure network access profiles in CSACS
- Configure NADS to enable AAA to use a Radius Server
- Verify and troubleshoot AAA operation
- Describe NFP features and functionality
- Secure the management plane using Cisco IOS security features
- Secure the data plane using Cisco IOS security features
- Secure the control plane using Cisco IOS security features

## COURSE CSP120

Title: Securing Networks with ASA Foundation

Exam: 642-524

- Explain the functions of the three types of firewalls used to secure today's computer networks.
- Describe the technology and features of Cisco security appliances.
- Given diagrams of networks protected by Cisco Adaptive Security Appliances (ASAs) and Cisco PIX Security Appliances, explain how each appliance protects network devices from attacks and why each is an appropriate choice for the example network.
- Prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM), and launch and navigate ASDM.
- Use ASDM and the CLI to perform essential security appliance configuration.
- Use ASDM to configure dynamic and static address translations in the security appliance.
- Use ASDM to configure switching and routing on the security appliance.
- Use ASDM to configure access control lists, filter malicious active codes, and filter URLs to meet the requirements of the security policy.
- Use the packet tracer for troubleshooting.
- Use ASDM to configure object groups that meet the requirements of the security policy.
- Use ASDM to configure AAA as needed to meet the requirements of the security policy.
- Use ASDM to configure a modular policy that supports the security policy.
- Use ASDM to configure protocol inspection to meet the requirements of the security policy.
- Use ASDM and the CLI to configure threat detection to meet the requirements of the security policy.
- Use ASDM to configure the security appliance to support a site-to-site VPN that meets the requirements of the security policy.
- Use ASDM to configure the security appliance to provide secure connectivity using remote access VPNs.
- Configure the security appliance to run in transparent firewall mode as needed to meet the requirements of the security policy.
- Enable, configure, and manage multiple contexts as needed to meet the requirements of the security policy.
- Select and configure the type of failover that best suits the network topology.
- Monitor and manage an installed security appliance.

## COURSE CSP130

Title: Implementing Cisco Intrusion Prevention System

Exam: 642-533

- List sensor requirements for inline operations
- Explain the difference between inline and promiscuous mode sensor operations
- Explain how Cisco IPS protects network devices from attacks (Describe signatures, alerts, and actions)
- Explain the evasive techniques used by hackers and how Cisco IPS defeats those techniques

- Describe the considerations necessary for selection, placement, and deployment of a network intrusion prevention system
- Explain the Cisco IPS signature features
- Explain AIP-SSM functionalities
- Use the CLI to initialize the sensor
- Configure user accounts and explain the different user roles
- Configure management access to the sensor appliance
- Explain how allowed hosts are used and how they are configured
- Describe sensor interfaces, interface pairs, VLAN-pairs, and VLAN-groups
- Use the Cisco IDM to configure sensor interfaces (enable, create pairs, assign to virtual sensors)
- Describe and configure software bypass
- Describe sensor communications with external management and monitoring systems
- Launch, navigate, and use the Cisco IDM to manage and monitor the sensor
- Describe the various CLI configuration modes and sub modes and navigate between them
- List the tasks for installing and configuring the IDSM-2 and AIP-SSM
- Plan the mitigation of specific network vulnerabilities and exploits
- Describe sensor tuning
- Explain IP fragment and TCP stream reassembly options
- Explain how IP logging should be used and how it is configured
- Explain the use of Event Variables
- Describe signature engines and their functionality
- Determine which response actions need to be configured for a given scenario
- Describe the purpose of the Meta Event Generator
- Explain Target Value Ratings and how they are used
- Determine the need for Event Action Rules in a given scenario
- Explain event Risk Ratings and how they are used
- Use the IDM to tune the sensor to work optimally in the network
- Use the IDM to tune signatures to provide maximum protection for a network
- Given a scenario, use the IDM to create custom signature to meet the requirements
- Configure response actions for a signature
- Configure the sensor to take response actions based on a risk rating
- Use the Cisco IDM to create a Meta signature and disable alert production for the component signatures
- Configure Event Action Filters
- Configure Target Value Ratings
- Configure general settings for Event Action Rules
- Configure Event Variables
- Use the sensor application policy enforcement feature
- Configure passive OS fingerprinting (POSFP)
- Explain the External Product Interface, its benefits, and specifications
- Configure a virtual sensor
- Configure anomaly detection
- Use IDM/CLI to monitor advanced features such as POSFP and AD
- Move software images/upgrades and configuration files via HTTP, HTTPS, SCP, and FTP
- Apply the appropriate system image to the sensor
- Perform sensor password recovery
- Explain sensor licensing and how to install a license
- Describe service pack and signature update file names and how to install them

## COURSE CSP140

Title: Implementing Cisco security Monitoring, Analysis, and Respond System

Exam: 642-544

- Identify the components, features and functions of the Cisco Security MARS product
- Describe the process of installing the Cisco Security MARS appliance
- Add Cisco reporting devices into the Cisco Security MARS appliance
- Add non-Cisco reporting devices into the Cisco Security MARS appliance
- Investigate events that the Cisco Security MARS appliance collects from configured security devices
- Configure the Cisco Security MARS appliance to send alerts
- Create and view a long-duration query on the Cisco Security MARS appliance
- Configure rules to detect interesting patterns of network activity and other anomalous network behavior
- Use the management features in the Cisco Security MARS appliance to assign event, addressing, service, and user information
- Configure the Cisco Security MARS appliance hardware maintenance activities
- Utilize the Global Controller to manage multiple Cisco Security MARS appliances