



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 Network Technologies Expert (CNTE)**

This is our most comprehensive and diverse program combining the coursework of multiple disciplines. This program begins with a PC hardware and software course, provides in-depth coursework on the Microsoft operation systems, offers an introduction to the Linux operating system, and guides the student through multiple levels of network infrastructure study for both Cisco and Microsoft environments. The goal of this program is to offer the student a single program to build the knowledge, skills, and certifications necessary to become a well-respected and well-trained professional poised to become a success in today's information technology environment.

- Certification program
- 1152 Contact Hours, 72 Credit Hours, 72 Weeks

#### **TERM 1**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
IPC100	PC I	6	96
MCS100	Windows I	3	48
MCS110	Windows II	3	48
<b>Total</b>		<b>12</b>	<b>192</b>

#### **TERM 2**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
MCS120	Windows III	3	48
MCS130	Windows IV	3	48
MCS140	Windows V	6	96
<b>Total</b>		<b>12</b>	<b>192</b>

#### **TERM 3**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
MCS150	Windows VI	3	48
MCS160	Windows VII	3	48
MCS170	Windows VIII	3	48
MCS180	Windows VIII	3	48
<b>Total</b>		<b>12</b>	<b>192</b>

#### **TERM 4**

<b>Course No.</b>	<b>Course Name</b>	<b>Quarter Credit Hours</b>	<b>Clock Hours</b>
CCA100	Cisco I	6	96
CCA110	Cisco II	3	48
CCA120	Cisco III	3	48
<b>Total</b>		<b>12</b>	<b>192</b>

**TERM 5**

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCA130	Cisco IV	3	48
CCA140	Cisco V	3	48
CSP100	Security I	3	48
CSP110	Security II	3	48
<b>Total</b>		<b>12</b>	<b>192</b>

**TERM 6**

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP120	Security III	3	48
CSP130	Security IV	3	48
CSP140	Security V	6	96
<b>Total</b>		<b>12</b>	<b>192</b>

**Type of Document Received Upon Graduation**

Upon successfully completing all requirements of the programs offered at Brand College, the student will be awarded a Certificate of Completion.

**Certification Tests**

Performance on a certification test is based on a pass or fail. You must receive between 75% and 80%, depending on the test, to pass. It is encouraged to take each test as soon as you complete the corresponding course.

## CNTE Program Details

### COURSE IPC100

Title: PC Hardware and Operating System

Exam: A+ Essentials Exam 220-601 and A+ Elective Exam (220-602 or 220-603 or 220-604)

- Personal Computer Components
- System Unit Components
- Storage Devices
- Personal Computer Connection Methods
- Personal Computer Operating Systems
- Windows User Interface Components
- Windows File System Management
- Windows System Management Tools
- Tools of the Trade
- Electronic Safety
- Environmental Safety and Materials Handling
- Perform Preventive Maintenance
- Diagnostics and Troubleshooting
- Professionalism and Communication
- Install and Configure Display Devices
- Install and Configure Input Devices
- Install and Configure Adapter Cards
- Install and Configure Multimedia Devices
- Install and Configure Storage Devices
- Install and Configure Power Supplies
- Install and Configure Memory
- Install and Configure CPUs
- Install and Configure System Boards
- Troubleshoot Display Devices
- Maintain and Troubleshoot Input Devices
- Troubleshoot Adapter Cards, Multimedia Devices, Storage Devices, Power Supplies, Memory, CPUs, and System Boards
- Install, Upgrade, and Optimize Microsoft Windows
- Add Devices to Windows
- Operating System Utilities
- Maintain and Troubleshoot Microsoft Windows
- Recover Microsoft Windows
- Network Concepts and Communications
- Network Connectivity
- Internet Technologies
- Create Network Connections
- Install and Configure Web Browser
- Maintain and Troubleshoot Network Connections
- Laptop and Portable Computing Device Components
- Install and Configure Laptops and Portable Computing Devices
- Maintain and Troubleshoot Laptops and Portable Computing Devices
- Printer and Scanner Technologies
- Printer and Scanner Components
- Printer and Scanner Processes
- Install and Configure Printers and Scanners
- Maintain and Troubleshoot Printers and Scanners

- Security Fundamentals
- Security Protection Measures
- Data and Physical Security
- Wireless Security
- Social Engineering
- Install and Configure Security Measures
- Maintain and Troubleshoot Security Measures

## COURSE MCS100

Title: Planning and Administering Windows Server 2008 Servers

Exam: Microsoft Exam 70-646

### **Course Description**

This instructor-led course provides students with the knowledge and skills to plan, manage, and maintain Windows Server 2008 servers. This course is intended for Windows Server 2008 Technology Specialists, in Network Infrastructure and Active Directory, who are interested in learning professional level Server Administrator skills to plan, manage, and maintain Windows Server 2008 servers.

### **Course Objectives**

This course will cover the following subjects:

- Plan a Windows Server 2008 deployment
- Plan and implement server commissioning and decommissioning for Windows Server 2008
- Plan the installation of server roles for Windows Server 2008
- Create a configuration change plan for Windows Server 2008
- Plan and implement Windows Server 2008 security
- Manage application versioning in Windows Server 2008
- Plan for a high-availability Windows Server 2008 deployment
- Plan a server update maintenance schedule for Windows Server 2008
- Maintain a Distributed File System (DFS) in Windows Server 2008
- Define server backup requirements and policies for Windows Server Backup
- Plan and implement a Windows Server 2008 restore
- Plan Windows Server 2008 monitoring
- Troubleshoot hardware issues
- Troubleshoot software issues
- Troubleshoot network issues

## COURSE MCS110

Title: Configuring and Troubleshooting a Windows Server 2008 Network Infrastructure

Exam: Microsoft Exam 70-642

### **Course Description**

This instructor-led course provides students with the knowledge and skills to configure and troubleshoot a Windows Server 2008 network infrastructure. Students will learn to implement and configure secure network access and implement fault tolerant storage technologies. Students will gain an understanding of the network technologies most commonly used with Windows Server 2008 and IP-enabled networks. Students will also learn how to secure servers and maintain update compliance.

### **Course Objectives**

This course will cover the following subjects:

#### *Configuring IP Addressing and Services (24 percent)*

- Configure IPv4 and IPv6 addressing. May include but is not limited to: configure IP options, subnetting, supernetting, alternative configuration
- Configure Dynamic Host Configuration Protocol (DHCP). May include but is not limited to: DHCP options, creating new options, PXE boot, default user profiles, DHCP relay agents, exclusions, authorize server in Active Directory, scopes, server core, and Windows Server Hyper-V
- Configure routing. May include but is not limited to: static routing, persistent routing, Routing Internet Protocol (RIP), Open Shortest Path First (OSPF)
- Configure IPsec. May include but is not limited to: create IPsec policy, IPsec Authentication Header (AH), IPsec Encapsulating Security Payload (ESP)

#### *Configuring Name Resolution (27 percent)*

- Configure a Domain Name System (DNS) server. May include but is not limited to: conditional forwarding, external forwarders, root hints, cache-only, server core, WINS and DNS integration, Windows Server virtualization
- Configure DNS zones. May include but is not limited to: DNS Refresh no-refresh, intervals, DNS listserv address (NSLOOKUP), primary/secondary zones, Active Directory integration, Dynamic Domain Name System (DDNS), GlobalNames, SOA refresh
- Configure DNS records. May include but is not limited to: record types, host, pointer, MX, SRV, NS, dynamic updates, Time to Live (TTL)
- Configure DNS replication. May include but is not limited to: DNS secondary zones, DNS stub zones, DNS scavenging interval, replication scope
- Configure name resolution for client computers. May include but is not limited to: DNS and WINS integration, configuring HOSTS file, LMHOSTS, node type, Link-Local Multicast Name Resolution (LLMNR), broadcasting, resolver cache, DNS Server list, Suffix Search order, manage client settings by using group policy

#### *Configuring Network Access (22 percent)*

- Configure remote access. May include but is not limited to: dial-up, Remote Access Policy, Network Address Translation (NAT), Internet Connection Sharing (ICS), VPN, Routing and Remote Access Services (RRAS), inbound/outbound filters, configure Remote Authentication Dial-In User Service (RADIUS) server, configure RADIUS proxy, remote access protocols, Connection Manager
- Configure Network Access Protection (NAP). May include but is not limited to: network layer protection, DHCP enforcement, VPN enforcement, configure NAP health policies, IPsec enforcement, 802.1x enforcement, flexible host isolation
- Configure network authentication. May include but is not limited to: LAN authentication by using NTLMv2 and Kerberos, WLAN authentication by using 802.1x, RAS authentication by using MS-CHAP, MS-CHAP v2, and EAP

- Configure wireless access. May include but is not limited to: Set Service Identifier (SSID), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), ad hoc versus infrastructure mode, group policy for wireless
- Configure firewall settings. May include but is not limited to: incoming and outgoing traffic filtering, Active Directory account integration, identify ports and protocols, Microsoft Windows Firewall versus Windows Firewall with Advanced Security, configure firewall by using group policy, isolation policy

*Configuring File and Print Services (13 percent)*

- Configure a file server. May include but is not limited to: file share publishing, Offline Files, share permissions, NTFS permissions, encrypting file system (EFS)
- Configure Distributed File System (DFS). May include but is not limited to: DFS namespace, DFS configuration and application, creating and configuring targets, DFS replication
- Configure shadow copy services. May include but is not limited to: recover previous versions, set schedule, set storage locations
- Configure backup and restore. May include but is not limited to: backup types, backup schedules, managing remotely, restoring data
- Manage disk quotas. May include but is not limited to: quota by volume or quota by user, quota entries, quota templates
- Configure and monitor print services. May include but is not limited to: printer share, publish printers to Active Directory, printer permissions, deploy printer connections, install printer drivers, export and import print queues and printer settings, add counters to Reliability and Performance Monitor to monitor print servers, print pooling, print priority

*Monitoring and Managing a Network Infrastructure (14 percent)*

- Configure Windows Server Update Services (WSUS) server settings. May include but is not limited to: update type selection, client settings, Group Policy object (GPO), client targeting, software updates, test and approval, disconnected networks
- Capture performance data. May include but is not limited to: Data Collector Sets, Performance Monitor, Reliability Monitor, monitoring System Stability Index
- Monitor event logs. May include but is not limited to: custom views, application and services logs, subscriptions, DNS log
- Gather network data. May include but is not limited to: Simple Network Management Protocol (SNMP), Baseline Security Analyzer, Network Monitor

## COURSE MCS120

Title: Configuring and Troubleshooting Windows Server 2008 Active Directory Domain Services & Configuring and Troubleshooting Identity and Access Solutions with Windows Server 2008 Active Directory

Exam: Microsoft Exam 70-640

### **Course Description**

This instructor-led course provides to teach Active Directory Technology Specialists with the knowledge and skills to configure Active Directory Domain Services in a distributed environment, implement Group Policies, perform backup and restore, and monitor and troubleshoot Active Directory related issues. This course also provides the knowledge and skills that IT Professionals need to configure identity and access solutions with Windows Server 2008 Active Directory.

### **Course Objectives**

This course will cover the following subjects:

#### *Configuring Domain Name System (DNS) for Active Directory (16 percent)*

- Configure zones. May include but is not limited to: Dynamic DNS (DDNS), Non-dynamic DNS (NDDNS), and Secure Dynamic DNS (SDDNS), Time to Live (TTL), GlobalNames, Primary, Secondary, Active Directory Integrated, Stub, SOA, zone scavenging, forward lookup, reverse lookup
- Configure DNS server settings. May include but is not limited to: forwarding, root hints, configure zone delegation, round robin, disable recursion, debug logging, server scavenging
- Configure zone transfers and replication. May include but is not limited to: configure replication scope (forestDNSzone, domainDNSzone), incremental zone transfers, DNS Notify, secure zone transfers, configure name servers, application directory partitions

#### *Configuring the Active Directory infrastructure (25 percent)*

- Configure a forest or a domain. May include but is not limited to: remove a domain, perform an unattended installation, Active Directory Migration Tool (ADMT) v3 (pruning and grafting), raise forest and domain functional levels, interoperability with previous versions of Active Directory, alternate user principal name (UPN) suffix, forestprep, domainprep
- Configure trusts. May include but is not limited to: forest trust, selective authentication versus forest-wide authentication, transitive trust, external trust, shortcut trust, SID filtering
- Configure sites. May include but is not limited to: create Active Directory subnets, configure site links, configure site link costing, configure sites infrastructure
- Configure Active Directory replication. May include but is not limited to: Distributed File System, one-way replication, bridgehead server, replication scheduling, configure replication protocols, force intersite replication
- Configure the global catalog. May include but is not limited to: Universal Group Membership Caching (UGMC), partial attribute set, promote to global catalog
- Configure operations masters. May include but is not limited to: seize and transfer, backup operations master, operations master placement, Schema Master, extending the schema, time service

#### *Configuring additional Active Directory server roles (9 percent)*

- Configure Active Directory Lightweight Directory Service (AD LDS). May include but is not limited to: migration to AD LDS, configure data within AD LDS, configure an authentication server, server core, Windows Server 2008 Hyper-V
- Configure Active Directory Rights Management Service (AD RMS). May include but is not limited to: certificate request and installation, self-enrollments, delegation, Active Directory Metadirectory Services (AD MDS), Windows Server virtualization
- Configure the read-only domain controller (RODC). May include but is not limited to: unidirectional replication, Administrator role separation, read-only DNS, BitLocker, credential caching, password replication, syskey, Windows Server virtualization

- Configure Active Directory Federation Services (AD FS). May include but is not limited to: install AD FS server role, exchange certificate with AD FS agents, configure trust policies, configure user and group claim mapping, Windows Server virtualization

#### *Creating and maintaining Active Directory objects (24 percent)*

- Automate creation of Active Directory accounts. May include but is not limited to: bulk import, configure the UPN, create computer, user, and group accounts (scripts, import, migration), template accounts, contacts, distribution lists
- Maintain Active Directory accounts. May include but is not limited to: configure group membership, account resets, delegation, AGDLP/AGGUDLP, deny domain local group, local versus domain, Protected Admin, disabling accounts versus deleting accounts, deprovisioning, contacts, creating organizational units (OUs), delegation of control
- Create and apply Group Policy objects (GPOs). May include but is not limited to: enforce, OU hierarchy, block inheritance, and enabling user objects, Group Policy processing priority, WMI, Group Policy filtering, Group Policy loopback
- Configure GPO templates. May include but is not limited to: user rights, ADMX Central Store, administrative templates, security templates, restricted groups, security options, starter GPOs, shell access policies
- Configure GPO templates. May include but is not limited to: user rights, ADMX Central Store, administrative templates, security templates, restricted groups, security options, starter GPOs, shell access policies
- Configure software deployment GPOs. May include but is not limited to: publishing to users, assigning software to users, assigning to computers, software removal
- Configure account policies. May include but is not limited to: domain password policy, account lockout policy, fine-grain password policies
- Configure audit policy by using GPOs. May include but is not limited to: audit logon events, audit account logon events, audit policy change, audit access privilege use, audit directory service access, audit object access

#### *Maintaining the Active Directory environment (13 percent)*

- Configure backup and recovery. May include but is not limited to: using Windows Server Backup, backup files and system state data to media, backup and restore by using removable media, perform an authoritative or non-authoritative Active Directory restore, linked value replication, Directory Services Recovery Mode (DSRM) (reset admin password), back up and restore GPOs
- Perform offline maintenance. May include but is not limited to: offline defragmentation and compaction, Restartable Active Directory, Active Directory database storage allocation
- Monitor Active Directory. May include but is not limited to: Network Monitor, Task Manager, Event Viewer, ReplMon, RepAdmin, Windows System Resource Manager, Reliability and Performance Monitor, Server Performance Advisor, RSOP

#### *Configuring Active Directory Certificate Services (13 percent)*

- Install Active Directory Certificate Services. May include but is not limited to: standalone versus enterprise, CA hierarchies—root versus subordinate, certificate requests, certificate practice statement
- Configure CA server settings. May include but is not limited to: key archival, certificate database backup and restore, assigning administration roles
- Manage certificate templates. May include but is not limited to: certificate template types, securing template permissions, managing different certificate template versions, key recovery agent
- Manage enrollments. May include but is not limited to: network device enrollment service (NDES), autoenrollment, Web enrollment, smart card enrollment, creating enrollment agents
- Manage certificate revocations. May include but is not limited to: configure Online Responders, Certificate Revocation List (CRL), CRL Distribution Point (CDP), Authority Information Access (AIA)

## COURSE MCS130

Title: Installing & Configuring the Windows Vista Operating Systems & Configuring Windows Vista Mobile Computing and Applications

Exam: Microsoft Exam 70-620

### **Course Description**

This instructor-led course provides students with the knowledge and skills to install and configure Windows Vista desktops. It will focus on four main areas: installing, securing, networking, and browsing. By the end of the course, the student will have installed and configured a Windows Vista desktop that is secure, on the network, and ready for browsing. This course also provides students with the knowledge and skills to successfully configure mobile computers and applications that run Windows Vista. It will also provide them with the knowledge and skills necessary to ensure successful configuration of the IT Pro tools and productivity applications that ship with Windows Vista. Students will focus on six main areas: maintenance and optimization tools, media applications, productivity applications, notebook computers, mobile devices, and Tablet PCs.

### **Course Objectives**

This course will cover the following subjects:

#### *Installing and upgrading Windows Vista*

- Identify hardware requirements
- Perform a clean installation
- Upgrade to Windows Vista from previous versions of Windows
- Upgrade from one edition of Windows Vista to another edition
- Troubleshoot Windows Vista installation issues
- Install and configure Windows Vista drivers

#### *Configuring and troubleshooting Post-installation system settings*

- Troubleshoot post-installation configuration issues
- Configure and troubleshoot Windows Aero
- Configure and troubleshoot parental controls
- Configure Microsoft Internet Explorer

#### *Configuring Windows security features*

- Configure and troubleshoot User Account Control
- Configure Windows Defender
- Configure Dynamic Security for Microsoft Internet Explorer 7
- Configure security settings in Windows Firewall

#### *Configuring network connectivity*

- Configuring networking by using the Network and Sharing Center
- Troubleshoot connectivity issues
- Configure remote access

#### *Configuring applications included with Windows Vista*

- Configure and troubleshoot media applications
- Configure Windows Mail
- Configure Windows Meeting Space
- Configure Windows Calendar
- Configure Windows Fax and Scan
- Configure Windows Sidebar

*Maintaining and optimizing systems that run Windows Vista*

- Troubleshoot performance issues
- Troubleshoot reliability issues by using built-in diagnostic tools
- Configure Windows Update
- Configure data protection

*Configuring and troubleshooting mobile computing*

- Configure mobile display settings
- Configure mobile devices
- Configure Tablet PC software
- Configure power options

## COURSE MCS140

Title: Designing a Windows Server 2008 Network Infrastructure & Designing a Windows Server 2008 Active Directory Infrastructure and Services & Designing a Windows Server 2008 Application Infrastructure

Exam: Microsoft Exam 70-647

### **Course Description**

This instructor-led course will provide students with an understanding of how to design a Windows Server 2008 Network Infrastructure that meets business and technical requirements for network services. At the end of this course, students will learn how to design an Active Directory Infrastructure in Windows Server 2008. Students will also learn how to design Active Directory forests, domain infrastructure, sites and replication, administrative structures, group policies, and Public Key Infrastructures. In addition students will also learn how to design for security, high availability, disaster recovery, and migrations. Students will learn how to design application infrastructure solutions based on Windows Server 2008 to meet varying business and technical requirements.

### **Course Objectives**

This course will cover the following subjects:

#### *Planning network and application services (23 percent)*

- Plan for name resolution and IP addressing. May include but is not limited to: internal and external naming strategy, naming resolution support for legacy clients, naming resolution for directory services, IP addressing scheme, TCP/IP version coexistence
- Design for network access. May include but is not limited to: network access policies, remote access strategy, perimeter networks, server and domain isolation
- Plan for application delivery. May include but is not limited to: application virtualization, presentation virtualization, locally installed software, Web-based applications
- Plan for Terminal Services. May include but is not limited to: Terminal Services licensing, Terminal Services infrastructure

#### *Designing core identity and access management components (25 percent)*

- Design Active Directory forests and domains. May include but is not limited to: forest structure, forest and domain functional levels, intra-organizational authorization and authentication, schema modifications
- Design the Active Directory physical topology. May include but is not limited to: placement of servers, site and replication topology, printer location policies
- Design the Active Directory administrative model. May include but is not limited to: delegation, group strategy, compliance auditing, group administration, organizational structure
- Design the enterprise-level group policy strategy. May include but is not limited to: group policy hierarchy and scope filtering, control device installation, authentication and authorization

#### *Designing support identity and access management components (29 percent)*

- Plan for domain or forest migration, upgrade, and restructuring. May include but is not limited to: cross-forest authentication, backward compatibility, object migration, migration planning, implementation planning, environment preparation
- Design the branch office deployment. May include but is not limited to: authentication strategy, server security
- Design and implement public key infrastructure. May include but is not limited to: certificate services, PKI operations and maintenance, certificate life cycle management
- Plan for interoperability. May include but is not limited to: inter-organizational authorization and authentication, application authentication interoperability, cross-platform interoperability

#### *Designing for business continuity and data availability (23 percent)*

- Plan for business continuity. May include but is not limited to: service availability, directory service recovery

- Design for software updates and compliance management. May include but is not limited to: patch management and patch management compliance, Microsoft Update and Windows Update, security baselines, system health models
- Design the operating system virtualization strategy. May include but is not limited to: server consolidation, application compatibility, virtualization management, placement of servers
- Design for data management and data access. May include but is not limited to: data security, data accessibility and redundancy, data collaboration

## COURSE MCS150

Title: Deploying Windows Server 2008 & Configuring & Troubleshooting IIS In Windows Server 2008 & Configuring & Troubleshooting Windows Server 2008 Terminal Services

Exam: Microsoft Exam 70-643

### **Course Description**

This instructor-led course provides students with an understanding of migrating and deploying Windows Server 2008 including installation, configuration, and upgrading. Special emphasis is given to upgrading common server configurations and using the Microsoft Deployment Toolkit. In this course, the students will learn to install, configure, maintain, and troubleshoot an Internet Information Services (IIS) 7.0 Web Server in Windows Server 2008. In addition this course provides students with the knowledge and skills to configure, manage, monitor, and troubleshoot a Terminal Services (TS) environment. The course focuses on configuring of TS core functionality, licensing, Gateway, and Web Access.

### **Course Objectives**

This course will cover the following subjects:

#### *Deploying Servers (24 percent)*

- Deploy images by using Windows Deployment Services. May include but is not limited to: Install from media (IFM), configure Windows Deployment Services, capture Windows Deployment Services images, deploy Windows Deployment Services images, server core
- Configure Microsoft Windows activation. May include but is not limited to: install a KMS server, create a DNS SRV record, replicate volume license data
- Configure Windows Server Hyper-V and virtual machines. May include but is not limited to: virtual networking, virtualization hardware requirements, Virtual Hard Disks, migrate from physical to virtual, VM additions, backup, optimization, server core
- Configure high availability. May include but is not limited to: failover clustering, Network Load Balancing, hardware redundancy
- Configure storage. May include but is not limited to: RAID types, Virtual Disk Specification (VDS) API, Network Attached Storage, iSCSI and Fiber Channel storage area networks, mount points

#### *Configuring Terminal Services (32 percent)*

- Configure Windows Server 2008 Terminal Services RemoteApp (TS RemoteApp). May include but is not limited to: Configuring Terminal Services Web Access, configuring Terminal Services Remote Desktop Web Connection
- Configure Terminal Services Gateway. May include but is not limited to: certificate configuration, Terminal Services Gateway Manager (TS Gateway Manager), specifying resources that users can access through TS Gateway by using Terminal Services resource authorization policy (TS RAP) and Terminal Services connection authorization policy (TS CAP), Terminal Services group policy
- Configure Terminal Services load balancing. May include but is not limited to: Terminal Services Session Broker redirection modes, DNS registration, setting through group policy
- Configure and monitor Terminal Services resources. May include but is not limited to: allocate resources by using Windows Server Resource Manager, configure application logging
- Configure Terminal Services licensing. May include but is not limited to: deploy licensing server, connectivity between terminal servers and Terminal Services licensing server, recovering Terminal Services licensing server, managing Terminal Services client access licenses (TS CALs)
- Configure Terminal Services client connections. May include but is not limited to: connecting local devices and resources to a session, Terminal Services profiles, Terminal Services home folders, Remote Desktop Connection (RDC), single sign-on, Remote Desktop Snap-In, MSTSC.exe
- Configure Terminal Services server options. May include but is not limited to: logoff, disconnect, reset, remote control, monitor, Remote Desktop Protocol (RDP) permissions, connection limits, session time limits, managing by using GPOs, viewing processes, session permissions, display data prioritization

#### *Configuring a Web Services Infrastructure (30 percent)*

- Configure Web applications. May include but is not limited to: directory-dependent, publishing, URL-specified configuration, Microsoft .NET components, for example, .NET and .aspx, configure application pools
- Manage Web sites. May include but is not limited to: migrate sites and Web applications, publish IIS Web sites, configure virtual directories
- Configure a File Transfer Protocol (FTP) server. May include but is not limited to: configure for extranet users, configure permissions
- Configure Simple Mail Transfer Protocol (SMTP). May include but is not limited to: setting up smart hosts, configuring size limitations, setting up security and authentication to the delivering server, creating proper service accounts, authentication, SMTP relay
- Manage Internet Information Services (IIS). May include but is not limited to: Web site content backup and restore, IIS configuration backup, monitor IIS, configure logging, delegation of administrative rights
- Configure SSL security. May include but is not limited to: configure certificates, requesting SSL certificate, renewing SSL certificate, exporting and importing certificates
- Configure Web site authentication and permissions. May include but is not limited to: configure site permissions and authentication, configure application permissions, client certificate mappings

#### *Configuring Network Application Services (14 percent)*

- Configure Windows Media server. May include but is not limited to: on-demand replication, configure time-sensitive content, caching and proxy
- Configure Digital Rights Management (DRM). May include but is not limited to: encryption, sharing business rules, configuring license delivery, configuring policy templates
- Configure Microsoft Windows SharePoint Services server options. May include but is not limited to: site permissions, backup, antivirus, configuring Windows SharePoint Services service accounts
- Configure Windows SharePoint Services e-mail integration. May include but is not limited to: configuring a document library to receive e-mail, configuring incoming versus outgoing e-mail

## COURSE MCS160

Title: Introduction to Installing and Managing Microsoft Exchange Server 2007 & Monitoring and Troubleshooting Microsoft Exchange Server

Exam: Microsoft Exam 70-236

### **Course Description**

In this instructor-led course, students who are new to Microsoft Exchange Server will learn how to configure and manage a messaging environment in accordance with technical requirements. Students will learn how to install Microsoft Exchange Server 2007 and manage routing, client access, and the backup and restore of databases. They will also learn how to manage addressing and recipient objects such as mailboxes, distribution groups, and contacts. This course also teaches students how to monitor and troubleshoot an Exchange Server 2007 messaging system. Students will learn how to correlate client and server issues and resolve those issues. They will also learn how to monitor systems and create reports from the monitoring data.

### **Course Objectives**

This course will cover the following subjects:

#### *Installing and Configuring Microsoft Exchange Servers*

- Prepare the infrastructure for Exchange installation
- Prepare the servers for Exchange installation
- Install Exchange
- Configure Exchange server roles

#### *Configuring Recipients and Public Folders*

- Configure recipients
- Configure mail-enabled groups
- Configure resource mailboxes
- Configure public folders
- Move mailboxes
- Implement bulk management of mail-enabled objects

#### *Configuring the Exchange Infrastructure*

- Configure connectors
- Configure the antivirus and anti-spam system
- Configure transport rules and message compliance
- Configure policies
- Configure public folders
- Configure client connectivity

#### *Monitoring and Reporting*

- Monitor mail queues
- Monitor system performance
- Perform message tracking
- Monitor client connectivity
- Create server reports
- Create usage reports

#### *Configuring Disaster Recovery*

- Configure backups
- Recover messaging data
- Recover server roles
- Configure high availability

## COURSE MCS170

Title: Deploying Messaging Solutions with Microsoft Exchange Server 2007

Exam: Microsoft Exam 70-238

### **Course Description**

This instructor-led course teaches students how to design a high availability messaging solution using Microsoft Exchange Server 2007. Students will create a high availability design to meet service level agreement requirements and learn strategies for gaining approval for the design. They will learn how to identify risks and create mitigation plans to maintain the business continuity of the messaging system. Students will also learn how to design a backup strategy, disaster recovery procedures, and test plans for those procedures.

### **Course Objectives**

This course will cover the following subjects:

#### *Planning Microsoft Exchange Server 2007 Upgrades and Migrations*

- Plan the Exchange Server 2007 upgrade implementation
- Plan the Exchange Server 2007 migration implementation
- Plan interoperability with Exchange in separate organizations
- Plan coexistence with Exchange 2000 Server and Exchange Server 2003 in a single organization
- Plan interoperability with third-party messaging systems

#### *Planning for High Availability Implementation*

- Plan a backup solution implementation
- Plan a recovery solution implementation
- Plan the service's high availability implementation
- Plan a data redundancy implementation

#### *Planning the Exchange Topology Deployment*

- Plan the storage group deployment
- Plan the server role deployment
- Plan the deployment of required Exchange services
- Plan the deployment of optional Exchange services

#### *Planning Messaging Security and Compliance Implementation*

- Plan the antivirus and anti-spam implementation
- Plan the network layer security implementation
- Plan the transport rules implementation
- Plan the messaging compliance implementation

#### *Planning for Messaging Environment Maintenance*

- Plan for Exchange infrastructure improvements
- Plan for configuration changes
- Plan for change management
- Plan for patch and service pack implementation
- Plan for monitoring and reporting

## COURSE MCS180

Title: Designing a Messaging Infrastructure using Microsoft Exchange Server & Designing a High Availability Messaging Solution using Microsoft Exchange Server 2007

Exam: Microsoft Exam 70-237

### **Course Description**

This instructor-led course provides students with the knowledge and skills to design a messaging infrastructure. Students will learn to assess an existing infrastructure and determine technical and business requirements for both new Microsoft Exchange Server 2007 deployments and migrations. Students will create a design that addresses security, architecture, scalability, coexistence, and client access needs. They also will learn strategies for gaining approval for designs from stakeholders.

### **Course Objectives**

This course will cover the following subjects:

#### *Designing and planning messaging services*

- Evaluate and recommend Active Directory configuration
- Evaluate and plan server deployment based on best practices, budget, and other business factors
- Evaluate network topology and provide technical recommendations
- Design and plan for new Exchange features
- Design organization configuration to meet routing requirements

#### *Designing and planning server high availability*

- Define a high availability solution based on client types and client loads
- Plan policies to handle unsolicited e-mail and virus outbreaks
- Evaluate role availability requirements and design solutions
- Design a disaster recovery, backup, and restore solution
- Evaluate existing business requirements to define supporting infrastructure
- Design and recommend a strategy for dependent services that impact high availability

#### *Designing and planning coexistence and migration*

- Design and plan for migration of legacy Exchange features
- Design a migration strategy
- Plan for coexistence (management tools for 2003 and 2007)

#### *Defining policies and security procedures*

- Design a solution to address regulatory and legal requirements
- Design procedures for message content filtering
- Design secure messaging

## 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