MCSE 2003 Security Certification Online – IT107
280 hours

To achieve MCSE 2003 Security Certification, you must pass five core exams and three security specialization exams. Plus, you'll earn the MCP (Microsoft Certified Professional) and MCSE (Microsoft Certified Systems Engineer) titles as you advance your way to MCSE 2003 Certification. On-line mentors are available 24 hours a day, 7 days a week, 365 days a year and a detailed report can always be generated showing student progress and percentages of accuracy. As course upgrades occur, the course will reflect the latest technologies.

Core Exams (Five Required)

1. Exam 70-270: MS Win XP Professional: Installing, Configuring, and Administering Microsoft Windows XP Professional
2. Exam 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment
3. Exam 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
4. Exam 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
5. Exam 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Security Specialization Exams (Three Required)

6. Exam 70-298: Designing Security for a Microsoft Windows Server 2003 Network
7. Exam 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network
8. Exam 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition

I. Exam 70-270: Installing, Configuring and Administering MS Win XP Professional

Installing Windows XP Professional

Overview/Description
To demonstrate how to install or upgrade to Windows XP Professional

Target Audience
Students preparing for the Microsoft Exam 70-270

Prerequisites
Working knowledge of Windows 95, Windows 98, Windows 2000 Professional, or Windows NT Workstation 4.0 from administrative, support, and architectural perspectives

Installing Windows XP Professional

- Prepare for an installation, discuss disk partitioning, choose a file system and explain the differences between a domain and workgroup installation
- Install Windows XP Professional from a CD
- Identify system requirements for installing Windows XP Professional
- Create Answer files and understand basic Answer file syntax
- Describe Uniqueness Database Files and Unique IDs
- Describe how to use an Answer file and a Uniqueness Database File during setup of Windows XP Professional
- Configure a reference computer, configure the sysprep.inf file, and use the sysprep.exe tool
- Discuss RIS and create a remote installation boot disk
- Identify the necessary steps when performing an upgrade
- Upgrade Windows 98, Windows 2000, and Windows NT Workstation 4.0 SP 6 to Windows XP Professional
- Upgrade from Windows 98 to Windows XP Professional
- Transfer user settings and user states
- Activate Windows XP Professional, prepare for automatic system recovery in the event of system errors, and troubleshoot common post-installation problems
- Troubleshoot a failed installation of Windows XP Professional

Managing Files, Folders, and Devices in Windows XP

Overview/Description
To show how to manage, control, and troubleshoot files and folders, network devices, and drivers in Windows XP Professional

Target Audience
Students preparing for the Microsoft Exam 70-270; Installing, configuring and administering Microsoft Windows XP Professional

Prerequisites
Working knowledge of Microsoft Windows 2000 Professional, Windows 98/95, or Windows NT Workstation 4 from administrative, support, and architectural perspectives

Managing Files, Folders, and Devices in Microsoft Windows XP

- Control access to files and folders in Windows XP Professional
- Create a shared folder and set permissions for it in Windows XP Professional
- Discuss cookie management and how to make web folders available for offline use in Windows XP Professional
- Explain offline files and configure caching options in Windows XP Professional
- To manage and control printers and print jobs in Windows XP Professional
- Configure printer permissions in Windows XP Professional
- Configure file systems in Windows XP Professional
- Install a fax printer, discuss fax options, and troubleshoot fax problems in Windows XP Professional
- Explain printer access

- Manage file compression and explain how to copy and move compressed files in Windows XP Professional
- Install CD-ROM and DVD devices and monitor and configure tape devices in Windows XP Professional
- Discuss basic disks, create a dynamic disk, and manage volumes and disks in Windows XP Professional
- Create a primary partition, convert a disk, and create a volume in Windows XP Professional
- Configure display support and video adapters in Windows XP Professional
- Monitor and configure devices in Windows XP Professional
- Discuss the use of infrared devices, wireless networking, USB devices, and handheld devices in Windows XP Professional
- Configure modems and an IrDA device in Windows XP
- Manage and troubleshoot drivers in Windows XP Professional
- Troubleshoot and update printer drivers in Windows XP Professional
- Configure and manage the Windows XP Professional advanced configuration power interface

System Reliability and the Desktop in Windows XP Professional

Overview/Description
To demonstrate how to monitor and improve system performance and how to configure desktop settings in Windows XP Professional

Target Audience
Students preparing for the Microsoft Exam 70-270; Installing, configuring and administering Microsoft Windows XP Professional

Prerequisites
Working knowledge of Windows 95, Windows 98, Windows 2000 Professional, or Windows NT Workstation 4.0 from administrative, support, and architectural perspectives

System Reliability and the Desktop in Windows XP Professional

- Determine system information and understand the four subcategories of the system information folder
- Use the task manager to monitor performance
- To discuss monitoring processes and process measures
- Discuss networking options in Task Manager and to monitor statistics for network connections
- Use maintenance tools to improve performance
- Configure processor scheduling and memory usage
- Monitor event logs, locate events, and configure the event log
- Archive an event log, clear all events in an event log, and limit the size of log files
- Manage applications by using Windows Installer packages
- Configure desktop settings
- Configure and manage accessibility services in Windows XP Professional
- Configure and manage accessibility services in Windows XP Professional
- Configure and manage user profiles
- Configure language support in Windows XP Professional
- Configure language support in Windows XP Professional
- Configure language support

Networking Protocols and Services in Microsoft Windows XP

Overview/Description
To explain how to configure networking utilities and IIS and how to manage the remote assistance and remote desktop utilities in Windows XP Professional

Target Audience
Students preparing for the Microsoft Exam 70-270; Installing, configuring and administering Microsoft Windows XP Professional

Prerequisites
Working knowledge of Windows 95, Windows 98, Windows 2000 Professional, or Windows NT Workstation 4.0 from administrative, support, and architectural perspectives

Networking Protocols and Services in Microsoft Windows XP

- Discuss TCP/IP communication in Windows XP Professional
- Define subnets and IP address assignment
- Troubleshoot IP addressing in Windows XP Professional
- Enable DHCP on a Windows XP Professional computer and configure an alternative static address for the computer
- Describe how to use dial-up connections in Windows XP Professional
- Create a dial-up, remote access connection and a direct cable connection to a private network and configure an Internet connection to an ISP
- Describe how to set up Internet Connection Sharing in Windows XP Professional
- Connect through a VPN connection to a computer network using Windows XP Professional
- Install IIS in Windows XP professional
- Test and troubleshoot an IIS installation using Windows XP Professional
- Enable and configure the Internet Connection Firewall
- Enable ICF in Windows XP Professional
- Describe how to use the remote desktop in Windows XP Professional
- To use remote assistance in Windows XP Professional
- Configure and use remote assistance in Windows XP Professional
- Use remote assistance
- Configure and troubleshoot scheduled tasks in Windows XP Professional

Backup and Security Settings in Microsoft Windows XP

Overview/Description
To explain how to recover from a backup and how to configure security settings in Windows XP Professional

Target Audience
Students preparing for the Microsoft Exam 70-270; Installing, configuring and administering Microsoft Windows XP Professional

Prerequisites

Working knowledge of Windows 95, Windows 98, Windows 2000 Professional, or Windows NT Workstation 4.0 from administrative, support, and architectural perspectives

Backup and Security Settings in Microsoft Windows XP

- Perform Windows XP Professional backups
- Use the Backup utility to recover Windows XP Professional from a backup
- Use the Windows Backup utility to restore data and boot files to a Windows XP Professional installation
- Describe advanced boot options for troubleshooting startup problems in Windows XP Professional system restorations
- Set up an auditing policy and track events in the Event Viewer
- Explain Windows XP Professional account settings and policies
- Set up an account policy to enforce a password and an account lockout policy in Windows XP Professional
- Explain the use of local users and groups and how to configure their rights in Windows XP Professional
- Explain the encrypting file system
- Configure the encrypting file system
- Configure security options using the local security settings of Windows XP Professional
- Configure the elements of a local security policy in Windows XP Professional
- Use security templates and analyze system security in Windows XP Professional
- Apply a security configuration policy to a computer using a security template
- Configure Internet Explorer security settings in Windows XP Professional
- Configure Internet Explorer security settings in Windows XP Professional

II. Exam 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment

Basic Concepts

Overview/Description
To outline introductory and essential concepts for Windows Server 2003

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Basic Concepts

- Distinguish between the services and editions provided by Windows Server 2003
- Identify the main characteristics of Active Directory
- Create and configure consoles using the Microsoft Management Console (MMC
- Create a secure console using the Microsoft Management Console (MMC)

Managing Users, Groups and Computers

Overview/Description
To describe how to manage and troubleshoot computer accounts, user accounts, user profiles, and groups in Windows Server 2003

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Managing Users, Groups, and Computers

- Create and manage computer accounts in the Windows Server 2003 Active Directory
- Create suitable user accounts and manage them in the Windows Server 2003 Active Directory
- Create and manage local, roaming, and mandatory user profiles in a domain
- Create and manage computer accounts, user accounts, and roaming profiles in Active Directory
- Create and manage groups in Windows 2003
- Implement groups appropriately in Windows Server 2003
- Identify troubleshooting responses to typical user and computer account problems
- Present troubleshooting strategies for problems with user and computer accounts

Managing Resource Access

Overview/Description
To identify the primary considerations and processes for managing NTFS and shared folder permissions, and for accessing remote servers, including Terminal Services

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Managing Resource Access

- Manage NTFS file and folder permissions in Windows Server 2003
- Manage shared folder permissions in Windows Server 2003
- Administer permissions for NTFS files and folders and for shared folders in Windows Server 2003
- Recognize examples of appropriate troubleshooting responses to typical issues that arise with shared folder and NTFS permissions in Windows Server 2003
- Choose the appropriate remote administration tool to manage a server in a given scenario
- Install and configure Terminal Services in Windows Server 2003
- Manage Terminal Services by using the Manager tool and by identifying appropriate troubleshooting strategies for typical problems
- Configure and manage Terminal Services
- Propose solutions and troubleshooting strategies for issues with NTFS and shared folder permissions and Terminal Services

Managing Hardware, Disks and Logical Devices

Overview/Description
To describe the considerations and outline the processes for managing server hardware and disk performance

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Managing Hardware, Disks, and Logical Devices

- Manually or automatically install hardware on a Windows 2003 server
- Configure hardware by using the Device Manager, driver signing options, and hardware profiles
- Use the relevant tools for monitoring hardware in Windows Server 2003
- Manage hardware devices in Windows Server 2003
- Configure basic and dynamic disks
- Implement the appropriate RAID level in a given scenario
- Assess and repair a disk using CHKDSK and the defragmentation tool
- Configure a disk, implement an appropriate RAID level on it, and optimize the disk

Managing the Server Environment

Overview/Description
To outline the processes and considerations for monitoring and managing system performance, system services, software, file and printer resources, and IIS

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Managing the Server Environment

- Use the System Monitor to view relevant indicators of system performance
- Use appropriate log types in given scenario
- Use the appropriate services monitoring tool in a given scenario
- Use the relevant tools to monitor system services and performance
- Configure update services and software site licensing
- Perform basic printer administration tasks, including troubleshooting
- Manage file resources and disk quotas
- Manage resources and services
- Perform basic web-administration tasks in Internet Information Services (IIS)
- Determine appropriate security settings for given scenarios
- Administer Internet Information Services (IIS) tasks and implement appropriate security settings

Managing Disaster Recovery

Overview/Description
To discuss the processes and considerations for preventing, preparing for, and implementing recovery strategies for system failures

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals tasked with managing and maintaining Windows Server 2003; learners preparing for the MCSA and MCSE certification exams for Windows Server 2003

Prerequisites
Network+ certification or the equivalent knowledge and skills; A+ certification or the equivalent knowledge and skills; a good working knowledge of networking components, services, and applications, including remote access, computer hardware components, and device management

Managing Disaster Recovery

- Implement steps for preventing and preparing for system failure
- Schedule backups in Windows Server 2003
- Implement preparatory steps for a potential disk failure
- Recover from data loss and disk failure situations

- Identify the appropriate tools or processes for recovering from a hardware or system failure
- Implement an appropriate disaster recovery strategy
- Identify appropriate recovery solutions for system and disk failures

III. Exam 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Implementing, Managing and Maintaining TCP/IP

Overview/Description
To demonstrate how to implement, manage, and maintain TCP/IP

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining TCP/IP

- Compare IP addresses to determine whether computers are on the same network
- Calculate, at IP address level, how a subnet, supernet, or variable-length subnet mask (VLSM) may be implemented on a network
- Implement the most appropriate IP configuration for a computer in a given scenario
- Configure two computers with the most typically appropriate TCP/IP settings
- Use the appropriate utilities to troubleshoot TCP/IP configuration and network connections
- Use the appropriate commands to test TCP/IP configuration and connectivity
- Analyze TCP/IP configuration and connections in a given scenario

Implementing, Managing and Maintaining DHCP

Overview/Description
To demonstrate how to implement, manage, and maintain DHCP

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining DHCP

- Define the key terms and operations of the DHCP service
- Explain how to install the DHCP service
- Perform the tasks necessary to configure different elements of the DHCP service
- Configure various elements of the DHCP service in a given scenario
- Follow the appropriate steps to manage the DHCP database in a given scenario
- Implement a DHCP relay agent and verify its operation
- Enable a DHCP relay agent
- Troubleshoot DHCP, using Windows Server 2003 monitoring tools
- Use the appropriate monitoring tool to troubleshoot DHCP in a given scenario

Implementing, Managing and Maintaining Name Resolution
Overview/Description
To demonstrate how to implement, manage, and maintain name resolution

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining Name Resolution

- Identify the procedures used in Windows Server 2003 name resolution
- Follow the steps involved in deploying a DNS server
- To configure a DNS server
- Create the appropriate zone and resource record in a given scenario
- Perform the necessary tasks to configure DNS clients
- Configure DNS zones and advanced properties for DNS servers
- Configure zone transfers and advanced properties for a DNS server
- Use the DNS troubleshooting tool Nslookup in a given scenario
- Use DNS logs for troubleshooting a given scenario
- Decide on the appropriate DNS monitoring tools to use in a given scenario
- Use the DNS debug log to capture and view query data on a DNS server
- Take the appropriate DNS troubleshooting steps, using the appropriate DNS troubleshooting tools

Implementing, Managing and Maintaining Network Security and Software

Overview/Description
To demonstrate how to implement, manage, and maintain network security and Software Update Services (SUS)

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems

Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining Network Security

- Provide an overview of how security is implemented in a Windows Server 2003 environment
- Follow the steps to implement network security and review security settings
- Create a security baseline for a computer
- Install (SUS) and configure automatic updates on a client
- Configure Software Update Services (SUS) to manage server synchronization, update approval, backup, and restoration of (SUS) data
- Synchronize servers for software updates, manage updates, and back up the Software Update Services (SUS) configuration
- Use the appropriate tools to view Kerberos and verify its operation
- Sequence the steps involved in IPSec network traffic processing
- Use IPsec to secure an IP-based network
- Create an IPSec policy
- Follow the steps to obtain IPSec policy information
- Monitor IPSec

Implementing, Managing and Maintaining Remote Access

Overview/Description
To demonstrate how to implement, manage, and maintain remote access

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining Remote Access

- Follow the steps to configure dial-up and VPN remote-access clients
- Follow the steps to configure a remote access server and VPN
- Configure a dial-up VPN remote access client and a remote access server
- Create and modify remote access policies
- Follow the steps to configure a standard RADIUS service and a proxy RADIUS service
- Deploy a standard RADIUS service and remote access policies in a given scenario
- Use the appropriate tools to troubleshoot remote access in a given scenario

- Follow the appropriate sequence of steps to resolve a remote access problem in a given scenario

Implementing, Managing and Maintaining Routing

Overview/Description
To demonstrate how to implement, manage, and maintain routing

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Implementing, Managing, and Maintaining Routing

- Identify the routing technology supported by Windows Server 2003
- Implement static routing in a Windows Server 2003 environment in a given scenario
- To implement the appropriate dynamic routing protocol in a given scenario
- Enable and configure RIP version 2 on a router and interface
- Enable demand-dial routing and create a demand-dial interface
- To configure demand-dial interface properties
- To implement demand-dial filters and create a router-to-router VPN
- Follow the steps to configure network address translation (NAT) on a demand-dial interface and dedicated interface
- Configure network address translation (NAT) on a demand-dial interface in a given scenario
- Follow the steps to troubleshoot router-to-router VPN and NAT
- Resolve a NAT-related routing issue

Maintaining a Network Infrastructure

Overview/Description: To demonstrate how to maintain a network infrastructure

Target Audience
Managers, IT consultants, analysts, network administrators, and support professionals tasked with managing a Windows 2003 network infrastructure; students preparing for certification in Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) programs

Prerequisites
CompTIA A+ certification or equivalent knowledge and skills; Network+ certification or equivalent knowledge

and skills; a good working knowledge of TCP/IP, Internet technologies, internetworking, computer hardware components, and networking concepts

Windows Server 2003: Maintaining a Network Infrastructure

- Follow the steps to perform and review network captures and configure Network Monitor
- Use Network Monitor to filter and display data on network traffic
- Use the Performance console to monitor system performance and configure the monitoring of system performance
- Use the Performance console to add counters to System Monitor and create a performance alert
- Manage Windows Server 2003 server services
- Configure server services to resolve a service-dependency issue and specify what actions to take in the event of a service failure

IV. Exam 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Planning the Network Infrastructure

Overview/Description
To describe the decisions and considerations for planning a network and Internet connectivity strategy

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Planning the Network Infrastructure

- Determine the appropriate network protocol services in a given scenario
- Determine the logical components of a TCP/IP addressing scheme
- Determine the components of a subnet scheme
- Determine the components of an IP routing solution in a given scenario
- Identify appropriate troubleshooting strategies for common TCP/IP problems
- Create a TCP/IP connectivity plan
- Identify the appropriate Internet connection methods in a given scenario
- Recognize the considerations for implementing a NAT solution for a network
- Determine a suitable ISA server configuration in a given scenario
- Identify appropriate troubleshooting steps and causes for common Internet connection problems
- Plan the components of an Internet connectivity solution for a given network environment

Planning for Name Resolution

Overview/Description
To discuss the decisions and considerations that should go into planning a name resolution strategy for a

network infrastructure

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites: Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Planning for Name Resolution

- Determine a suitable DNS solution that integrates with other DNS systems
- Determine suitable DNS optimization, security, and troubleshooting methods in given scenarios
- Implement an appropriate DNS replication strategy for a given DNS implementation
- Determine an appropriate DNS solution in a given scenario
- Determine an appropriate WINS solution in a given scenario
- Identify appropriate optimizing, security, and troubleshooting strategies for WINS
- Implement the appropriate WINS replication strategy for a given WINS implementation
- Determine an appropriate WINS solution in a given scenario
- Determine an appropriate name resolution solution for a given scenario

Implementing Routing and Remote Access

Overview/Description: To determine an appropriate routing and remote access implementation strategy and a suitable security solution for it

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites: Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Implementing Routing and Remote Access

- Determine an appropriate routing strategy for a given scenario
- Determine a suitable remote access solution in a given scenario
- Recognize examples of the benefits of RADIUS and IAS
- Plan an appropriate RRAS strategy for a given scenario
- Determine a suitable security strategy for a remote access solution based on specific network infrastructure requirements
- Recognize the effects of how remote access policies are implemented
- Determine a suitable router security solution for a given scenario
- Recognize appropriate steps for troubleshooting routing and remote access
- Determine an appropriate security solution for a routing and remote access network configuration

Planning for Network Availability

Overview/Description
To discuss the decisions and considerations for maintaining server availability and performance

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Planning for Network Availability

- Identify the causes of availability issues and recognize the tools that can be used to determine the cause of these issues
- Determine a suitable backup and recovery strategy in a given scenario
- Recognize appropriate methods for planning server clustering
- Determine an appropriate clustering implementation in a given scenario, and recognize security and recovery considerations
- Recognize the main considerations for using network load balancing
- Plan an appropriate clustering solution for a given scenario

Planning Server Roles and Server Security

Overview/Description
To outline the processes and considerations for planning server roles and server security

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Planning Server Roles and Server Security

- Determine an appropriate placement of operations master roles in a given network scenario
- Recognize planning considerations for using remote administration and remote assistance with Terminal Services
- Plan specific server roles in a given scenario
- Recognize the basic considerations for determining security for a network infrastructure
- Recognize considerations and processes for implementing security for specific server roles
- Create and use security templates and import them into Group Policy
- Recognize default security policy settings

- Recognize steps for implementing server security in a given scenario

Planning a Security Infrastructure

Overview/Description
To outline the processes and considerations for the planning the public key infrastructure and securing network data

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of networking concepts

Planning a Security Infrastructure

- Plan an appropriate IPSec implementation in a given scenario
- Recognize deployment considerations for IPSec and the relevant troubleshooting tools
- Recognize steps to maintain security for wireless networks
- Determine an appropriate IPSec and wireless network security implementation in a given scenario
- Determine an appropriate CA implementation in a given scenario
- Recognize considerations for managing certificates
- Recognize the considerations for planning and deploying smart card authentication using certificates
- Plan the security for a network infrastructure based on the use of certificates
- Recognize the tools necessary for implementing a change management strategy

V. Exam 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Planning and Implementing an Active Directory Infrastructure

Overview/Description
To identify the role and features of Windows Server 2003 Active Directory and the factors and requirements for planning and implementing an Active Directory infrastructure

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Planning and Implementing an Active Directory Infrastructure

- Identify the role and features of Active Directory as a directory service in Windows Server 2003
- Distinguish between the features of Active Directory and their role in the logical and physical network structure
- Choose the appropriate Active Directory administration tool in a given scenario
- Recognize the steps involved in creating an Active Directory structure
- Verify and troubleshoot an Active Directory installation in a given scenario
- Set an Active Directory forest or domain functional level in a given scenario
- Install and configure an Active Directory forest and domain structure
- Suggest the best practices involved in installing and administering an Active Directory infrastructure
- Suggest a suitable strategy for backing up Active Directory
- Suggest a suitable restore operation in a given scenario
- Carry out a backup and restore operation on Active Directory in an enterprise environment

Planning Active Directory Services

Overview/Description
To distinguish between global catalog servers and operations master roles and identify how they are enabled, administered, and placed in Active Directory infrastructure

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Planning Active Directory Services

- Customize a global catalog server in a given scenario
- Select an appropriate placement strategy for global catalog servers and domain controllers in a given scenario
- Determine the need for universal group caching in a given scenario
- Carry out global catalog services administration in an enterprise scenario
- Determine the placement of operations master roles in a given scenario
- Choose a suitable strategy for managing operations master roles in a given scenario
- Manage operations master roles in an enterprise Active Directory structure
- Suggest the best practices involved in assigning and managing operations master roles in an Active Directory infrastructure

Active Directory Sites, Replication and Trusts

Overview/Description
To distinguish between Active Directory sites, replication, and trusts, and identify how they are implemented and administered

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Active Directory Sites, Replication, and Trusts

- Create a site environment in a given scenario
- Configure a site topology in a given scenario
- Create and configure sites in an Active Directory infrastructure
- Associate replication topologies with their corresponding networking environments
- Choose the appropriate Windows tool for monitoring replication in a given scenario
- Troubleshoot replication in a given scenario
- Manage Active Directory replication for an enterprise
- Establish suitable trust relationships in a given scenario
- Select a suitable strategy for managing trusts in a given scenario
- Establish and manage a trust relationship
- Suggest the most appropriate ways to establish and manage trusts in an Active Directory infrastructure

Implementing Active Directory Users and Groups

Overview/Description
To identify how to plan and implement Active Directory OU, user, and group strategies

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Implementing Active Directory Users and Groups

- Determine a suitable OU structure in a given scenario
- Implement an OU structure in a given scenario
- Select a suitable procedure for administering OUs in a given scenario

- Create and administer an OU structure for an enterprise
- Implement a user account strategy in a given scenario
- Determine a security group strategy in a given scenario
- Suggest a user authentication strategy in a given scenario
- Configure user and group settings in an enterprise scenario

Planning and Implementing Group Policy

Overview/Description: To identify how to plan and implement group policy

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Planning and Implementing Group Policy

- Determine a group policy planning strategy in a given scenario
- Carry out Group Policy management and planning in a given scenario using the appropriate Group Policy tools
- Suggest a suitable configuration for Group Policy settings in a user and computer environment
- Create an RSoP query and configure Group Policy settings in an enterprise environment
- Suggest a strategy for implementing Group Policy objects in a given scenario
- Suggest a strategy for managing files and folders using Group Policy
- Create and configure Group Policy objects in an enterprise environment

Configuring and Troubleshooting Group Policy

Overview/Description
To identify the tasks and strategies involved in configuring and troubleshooting group policy

Target Audience
Systems administrators, systems engineers, systems analysts, IT consultants, and support professionals with responsibility for planning, implementing, and maintaining Microsoft Windows Server 2003 Active Directory; learners preparing for MCSE certification exams

Prerequisites
Experience in implementing and administrating Windows network operating systems with directory services, and a proficient working knowledge of networking concepts

Configuring and Troubleshooting Group Policy

- Suggest a suitable strategy to distribute software using Group Policy
- Configure user and computer security settings in a given scenario

- Configure an appropriate software update in a given scenario using Group Policy
- Configure user and computer security settings using security templates in a given scenario
- Carry out software distribution for an enterprise, using Group Policy
- Suggest a strategy for troubleshooting Group Policy in a given scenario
- Troubleshoot Group Policy in an enterprise environment
- Suggest best practices for managing Group Policy in an enterprise Active Directory environment

VI. Exam 70-298: Designing Security for a Microsoft Windows Server 2003 Network

Security Basics

Overview/Description
To outline the processes and considerations for performing a security analysis and securing the network management process

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

Security Basics

- Distinguish between types of threats using the STRIDE model
- Recognize the steps involved in security risk management
- Recognize the criteria for establishing good security policies and procedures
- Identify steps to take to secure the network management process
- Recognize the recommended components of an audit policy
- Assess the weaknesses in an existing network management security scenario

Logical Network Security

Overview/Description
To outline the decisions and considerations for designing a public key infrastructure and an authentication strategy

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

Logical Network Security

- Design an appropriate CA infrastructure in a given scenario
- Recognize methods for securing CA servers and managing certificates
- Design an appropriate CA infrastructure and management strategy for a given scenario
- Recognize and distinguish between basic authentication best practices
- Recognize appropriate steps for managing interoperability with other authentication protocols
- Determine an appropriate trust configuration in a given scenario
- Determine an appropriate authentication strategy in a given scenario

Securing Clients

Overview/Description
To outline the processes and considerations for securing client machines and securing remote access

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

Securing Clients

- Recognize relevant steps for addressing threats to client machines
- Determine a suitable security update process in a given scenario
- Design an appropriate strategy for securing client machines in a given scenario
- Recognize steps to secure the IAS server against specific threats
- Determine an appropriate remote access policy for a given scenario
- Determine an appropriate strategy to secure remote authentication in a given scenario

Physical Network Security

Overview/Description: To outline the decisions and considerations for securing VPNs and wireless networks, and for using IPSec to increase security

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites

Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

Physical Network Security

- Determine a suitable use of IPSec in a given scenario
- Determine an appropriate IPSec policy in a given scenario
- Determine an appropriate IPSec implementation in a given scenario
- Determine the appropriate VPN protocol in a given scenario
- Determine a suitable VPN connection in a given scenario
- Design an appropriate VPN solution in a given scenario
- Recognize the recommended components of a security solution for private and public wireless LANs
- Determine an appropriate 802.1x authentication strategy for a given wireless network
- Determine an appropriate security design for a wireless network

Securing Data and Server Roles

Overview/Description
To outline the processes and considerations for securing data and securing server roles

Target Audience
Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

Securing Data and Server Roles

- Determine an appropriate permission structure in a given scenario
- Determine a suitable Active Directory access control strategy in a given scenario
- Recognize best practices for designing an EFS recovery plan and for securing general backup and restores
- Design an appropriate strategy for securing data and securing access to it in a given scenario
- Determine an appropriate baseline template in a given scenario
- Recognize security threats and describe recommended practices for securing specific server roles
- Determine an appropriate baseline security solution for a given scenario

IIS Security and Firewalls

Overview/Description
To outline the processes and considerations for securing an IIS implementation, including the use of firewalls

Target Audience

Systems engineers, systems analysts, IT consultants, and support professionals tasked with planning and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) program

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services, and a proficient working knowledge of security concepts

IIS Security and Firewalls

- List guidelines for hardening IIS servers and securing data on them
- Determine the appropriate IIS authentication method in a given scenario
- List guidelines for IIS encryption and monitoring
- Design a strategy to secure a given IIS implementation
- Determine a suitable firewall configuration for a given scenario
- Plan an appropriate firewall configuration in a given scenario
- Design a security strategy for a given scenario using firewalls and IIS

VII. Exam 70-299: Implementing and Administering Security in a MS Win Server 2003 Network

Managing System Security in Windows Server 2003

Overview/Description: To outline the process and considerations for securing the software infrastructure and for using security templates

Target Audience
Systems engineers, systems administrators, systems analysts, IT consultants, and support professionals tasked with implementing and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) or Microsoft Certified Systems Administrator(MCSA) programs

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services such as messaging, database, file and print, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management, and a basic working knowledge of security

Managing System Security in Windows Server 2003

- Identify a suitable use of the MBSA tool in a given scenario
- Distinguish between and configure authentication methods
- Determine an appropriate SUS configuration in a given scenario
- Plan and implement software restriction policies
- Implement appropriate patch management and software restriction configurations
- Define a security template

- Recognize recommended practices for securing specific server roles
- Deploy and troubleshoot security templates
- Configure auditing and manage logs
- Manage security templates and auditing

Securing Access to Resources in Windows Server 2003

Overview/Description
To outline the decisons and processes for securing networks using authentication and authorization

Target Audience
Systems engineers, systems administrators, systems analysts, IT consultants, and support professionals tasked with implementing and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) or Microsoft Certified Systems Administrator(MCSA) programs

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services such as messaging, database, file and print, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management, and a basic working knowledge of security

Securing Access to Resources in Windows Server 2003

- Configure a secure authentication implementation in a given scenario
- Determine an appropriate group type in a given scenario
- Determine a suitable nesting solution in a given scenario
- Configure an appropriate trust relationship in a given scenario
- Configure appropriate permissions in a given scenario
- Determine a suitable authorization and permission structure for a given scenario

Securing Wireless and Remote Communications in Windows Server 2003

Overview/Description
To outline the considerations and procedures for securing wireless and remote communications

Target Audience: Systems engineers, systems administrators, systems analysts, IT consultants, and support professionals tasked with implementing and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) or Microsoft Certified Systems Administrator(MCSA) programs

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services such as messaging, database, file and print, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management, and a basic working knowledge of security

Securing Wireless and Remote Communications in Windows Server 2003

- Identify an appropriate 802.1x authentication method in a given scenario

- Configure security for wireless access connections
- Determine and configure appropriate security settings for a wireless network implementation
- Enable and configure remote access on the server
- Configure an appropriate remote access implementation for clients
- Configure an appropriate remote access security solution

Managing IPSEC in Windows Server 2003

Overview/Description
To outline the decisions, considerations, and procedures for implementing an IPSec solution

Target Audience
Systems engineers, systems administrators, systems analysts, IT consultants, and support professionals tasked with implementing and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) or Microsoft Certified Systems Administrator(MCSA) programs

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services such as messaging, database, file and print, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management, and a basic working knowledge of security

Managing IPSec in Windows Server 2003

- Determine an appropriate IPSec configuration in a given scenario
- Identify the steps required to implement a specific IPSec configuration
- Recognize the steps to implement IPSec packet filtering in a given scenario
- Determine the appropriate IPSec policy component in a given scenario
- Use MMC snap-in tools to configure an IPSec policy
- Recognize tools and steps for managing and troubleshooting IPSec
- Identify tools and steps to manage the use of IPSec

Managing Certificates in Windows Server 2003

Overview/Description
To outline the considerations and procedures for using certificates to secure a network

Target Audience
Systems engineers, systems administrators, systems analysts, IT consultants, and support professionals tasked with implementing and maintaining a Windows Server 2003 network infrastructure; learners preparing for certification in the Microsoft Certified Systems Engineer (MCSE) or Microsoft Certified Systems Administrator(MCSA) programs

Prerequisites
Experience in implementing and administrating Windows network operating systems with network services such as messaging, database, file and print, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management, and a basic working knowledge of security

Managing Certificates in Windows Server 2003

- Install a certificate authority hierarchy
- Recognize the steps and options for configuring a CA
- Manage certificate revocation and CA backup
- Install, configure, and administer a CA
- Distinguish between the processes for obtaining public and private server certificates
- Enable SSL security and use it to secure communication channels
- Enable and use SSL to secure communications

VIII. Exam 70-227: Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000

Installation of ISA Server 2000

Overview/Description
To demonstrate how to install ISA Server on a computer running Microsoft Windows 2000 Server and configure web proxy, firewall, and SecureNAT clients

Target Audience
IT Professionals including web administrators, network administrators, and security administrators but not network architects

Prerequisites
The Group Policy module in the Microsoft Windows 2000 learning path; the Microsoft Windows 2000 - Implementing a Network Infrastructure learning path, or equivalent skills

Installation of ISA Server 2000

- Identify ISA Server 2000 editions, describe the benefits of ISA Server, and list the ISA server modes
- Describe how ISA servers cache web content, and identify the types of caching that ISA Server supports
- Describe the function of firewalls
- Explain common roles of ISA Server 2000 in different deployment scenarios
- List hardware and software requirements for ISA Server 2000
- Specify the initial cache size and configure the LAT for an ISA server
- Install ISA Server in Integrated mode
- Upgrade servers from Microsoft Proxy 2.0 to Microsoft ISA Server 2000
- Install the ISA Server administration tools on another computer
- Identify the clients that ISA Server 2000 supports
- Configure web proxy and SecureNAT clients
- Install and configure firewall clients
- Install and configure ISA Server 2000 clients
- Troubleshoot ISA Server 2000 installation and client installation
- Describe the management tools available in ISA Server 2000 and maintain the LAT and LDT
- Back up and restore ISA Server configuration and describe managing the services associated with ISA Server
- Use the ISA Management snap-in to add a new range of IP addresses to a LAT and back up and restore an ISA Server

Access Policies, Caching, and VPNs

Overview/Description
To describe the components of access policies, configure caching on ISA Server, and explain the use of VPNs

Target Audience
IT Professionals including web administrators, network administrators, and security administrators but not network architects

Prerequisites
The Group Policy module in the Microsoft Windows 2000 learning path; the Microsoft Windows 2000 - Implementing a Network Infrastructure learning path, or equivalent skills

Access Policies, Caching, and VPNs in Microsoft ISA Server 2000

- Describe the components of an access policy, how to plan an access policy strategy, and the method that ISA Server uses to process outgoing client requests
- Describe policy elements
- Describe the policy elements available to ISA Server
- Create the most important types of ISA Server 2000 policy elements
- Plan appropriate access policies and create protocol rules and site and content rules
- Create protocol rules
- Explain and configure bandwidth rules
- Create a bandwidth rule
- Describe authentication methods available in ISA Server 2000 and configure authentication for outgoing web requests
- Configure authentication in ISA Server 2000
- Explain which type of client authentication to implement in specific scenarios
- Describe the ISA Server 2000 caching functions that improve cache performance
- Identify policies for configuring HTTP caching
- Configure FTP caching and caching for specific objects
- Adjust the cache size and the associated .cdat file for an ISA server
- Configure HTTP and FTP caching, active caching, advanced cache settings, and scheduled content downloads
- Describe the use of an ISA VPN server
- Configure an ISA VPN Server to accept client connections and to configure local and remote ISA VPN servers
- Configure PPTP connections for ISA Server 2000 client computers
- Configure a VPN connection between networks

Configuring a Firewall and Access to Internal Resources

Overview/Description: To describe securing the ISA server and explain publishing

Target Audience: IT Professionals including web administrators, network administrators, and security administrators but not network architects

Prerequisites
The Group Policy module in the Microsoft Windows 2000 learning path; the Microsoft Windows 2000 - Implementing a Network Infrastructure learning path, or equivalent skills

Firewalls and Access to Internal Resources with Microsoft ISA Server 2000

- Describe best security practices and identify the security levels available for an ISA server
- Secure an ISA server by running the ISA Server Security Configuration Wizard
- Explain the functionality of a perimeter network firewall configuration on a network
- Describe packet filtering and IP routing
- Configure packet filtering and IP routing in ISA Server 2000
- Create IP packet filters
- Describe and configure the application filters that are available in ISA Server 2000
- Configure an SMTP application filter
- Describe publishing servers and publishing server configurations using ISA Server 2000
- Create web publishing rules, configure listeners, and redirect requests

- Describe how to publish secure web sites
- Publish a web server
- Describe the steps for publishing a server and to use the message screener
- Publish an NNTP server and a mail server
- Explain how to add and configure an H.323 gatekeeper
- Add and configure an H.323 gatekeeper
- Configure gatekeeper destinations

Monitoring, Reporting, and ISA Server Enterprise Edition

Overview/Description
To describe the use of ISA Server in an enterprise and develop a strategy for monitoring ISA Server activity

Target Audience: IT Professionals including web administrators, network administrators, and security administrators but not network architects

Prerequisites
The Group Policy module in the Microsoft Windows 2000 learning path; the Microsoft Windows 2000 - Implementing a Network Infrastructure learning path, or equivalent skills

Monitoring, Reporting, and ISA Server Enterprise Edition

- Plan a monitoring and reporting strategy and describe the types of attacks that ISA Server can detect
- Describe how to configure intrusion detection and alerts
- Configure IP intrusion detection and create an alert
- Configure logging on ISA servers
- Create, view, and save reports in ISA Server 2000
- Create, open, and print a server activity report using ISA Server 2000
- Explain how to monitor ISA Server 2000 and H.323 gatekeeper sessions
- Monitor ISA server activity in real time
- Discover, diagnose, and correct problems with ISA Server servers
- Choose a logging format based on report information
- Describe the benefits of ISA Server 2000 Enterprise Edition and to plan the placement of Enterprise Edition ISA servers
- Initialize ISA Server 2000 Enterprise Edition
- Create and delete arrays, install the first ISA server in an array, promote a standalone server, and back up and restore enterprise configurations
- Perform ISA Server 2000 enterprise initialization and promote a standalone server
- Place ISA Server 2000 servers in a Windows 2000 domain structure
- Configure enterprise and array policies
- Configure routing for firewall and SecureNAT clients
- Explain when to implement routing of web requests in an enterprise environment
- Describe the procedures for configuring ISA Server 2000 clients and servers for automatic discovery
- Create an enterprise policy and configure an ISA server and domain name system (DNS) to enable automatic discovery
- Describe the process that CARP uses to resolve client requests and to describe network load balancing
- Explain how to configure CARP
- Explain how to extend the functionality of ISA Server 2000