

# Windows Server 2003 Planning Network Infrastructure

5 Sessions –

15 Hours of Interactive On Line Training

The Windows Server 2003 Planning Network Infrastructure course from ExamForce prepares you with the knowledge and skills needed to plan and maintain a Windows Server 2003 network. Expert instructor Michael Storm demonstrates critical skills like how to plan for server and network security, routing and remote access, and server availability. At the conclusion of the course, you will understand the skills required to plan a Windows Server 2003 network, and be prepared to pass MCP exam 70-293.

## Benefits

- ExamForce certification courses meet or exceed exam objectives.
- You will build on current abilities and be prepared to pass the MCP exam 70-293.
- Increase your career opportunities and earning potential.

## Session 1

### Section A: Introduction

- Connectivity
- RRAS
- Availability
- Security
- Components

### Section B: TCP/IP Networking

- Network Planning
- IP Addressing
- IP Address Classes
- Subnet Mask
- Addressing Scheme

### Section C: Network Availability

- Subnetting Requirements
- Network Planning
- Availability
- Redundancy

### Section D: Network Performance

- Affecting Factors
- Physical Subnets
- Logical Subnets
- Ethernet Usage - 10 Mbps
- Ethernet Usage - 100/1000 Mbps

### Section E: Planning for Growth

- Requirements
- Traffic Flow
- How to Plan

### Section F: DHCP Planning

- Config Methodologies
- DHCP Features
- Integration Benefits
- LAN
- Routed Networks
- Planning
- Non-Microsoft Clients

### Section G: Troubleshooting TCP/IP Addressing

- DHCP Performance
- Lease Duration
- DHCP Security
- DHCP Issues
- Troubleshooting Tools
- Traffic Monitoring

## Session 2

### Section A: Internet Connectivity

- Additional Features
- Design Options
- Design Requirements
- Active Directory
- Perimeter Design

### Section D: Enhancing ISA Server

- Enhance Availability
- Clustering Type
- Caching Method
- Organize Hierarchy
- Distribute IP Traffic

### Section E: Clustering Technologies

- NLBS
- CLB
- Server Clusters
- X Node Clustering
- Clustering Components
- Failover/Failback
- Cluster Management

### Section F: Planning RRAS

- Planning Decisions
- Isolation
- Integration
- Protocol Support
- Routing Solution
- Solution Integration

## Session 3

### Section A: RRAS Advanced Features

- RRAS Filtering
- Wireless Standards
- Wireless Enhancements
- 802.1x Authentication
- Wireless Security
- Enhancing Performance

### Section B: IP Troubleshooting

- Local Clients
- Reachability Issues
- NAT Issues
- Routing Issues
- Strategy for Routing
- Outside-In
- Inside-Out
- Divide-by-Half

### Section C: Secure Remote Access

- IPSec
- Connect with IPSec
- IPSec Mode

### Section E: Planning IPSec Policy

- IPSec Policy
- Requirements
- Components
- Identify Needs
- IPSec Phases
- Negotiation Policies
- Policy Filters

### Section F: Planning IPSec Deployment

- Authentication Types
- Digital Certificates
- Certificate Use
- Deployment Options
- GPO Deployment
- Processing Order
- Effective Policy

## Session 4

### Section A: IPSec Troubleshooting

- IPSec Monitor
- IP Security Management
- Users & Computers
- RSoP
- Event Viewer
- Troubleshooting Process

### Section B: DNS

- Design Process
- DNS Features
- AD Integrated Zone
- Traditional Zone
- Choosing Zone Type
- Connecting to Internet

### Section C: Integrating DNS

- Options
- Namespace
- First DNS Server
- Secure DNS
- Secure Zone Replication
- DNS Availability
- DNS Performance
- DNS Troubleshooting

### Section D: Planning WINS

- WINS Solution
- Routed Network
- Client Considerations
- Multiple Servers
- Secure WINS
- WINS Availability
- WINS Performance

- Connectivity Solutions
- Connection Components
- Using NAT
- Secure Perimeter

#### Section B: Network Address Translation

- Define Translation
- NAT Solution
- NAT Server Options
- IP Filters
- Address Pools/Ports
- VPN Tunnels
- Availability/Performance

#### Section C: Internet Security & Acceleration

- Planning Decisions
- Filtering Features
- Security Features

- Verify & Analyze
- Deploy & Update

### Session 5

#### Section A: Perimeter Security

- Router Security
- External Attacks
- DoS/Port Scanning
- Firewalls
- DMZ Subnets
- Three-Prong Approach
- Midground Screen

#### Section B: Securing Public Servers

- Vulnerabilities
- Public Server Roles
- HTTP/FTP Server
- DNS Server
- Messenger Server
- Application Server
- VPN Server
- Terminal Server

#### Section C: Authentication/Encryption

- Transmission Options
- VPN Connection
- Design Decisions

#### Section D: Certificates

- PKI
- Reliability
- Requirements
- CA Distribution
- Issuing CAs
- Commercial CAs
- Private CAs

#### Section E: CA Design

- Guidelines
- Planning CA Hierarchy
- User Accounts
- Mapping

#### Section F: Planning for Administration

- Planning Aspects
- Remote Administration
- Terminal Services
- Monitoring Performance
- Monitoring Services
- Backup/Recovery
- Media Handling
- Data/System Protection

- VPN Tunnels
- Tunneling Protocol
- VPN Compulsory Tunnel
- VPN Voluntary Tunnel
- Tunneling Comparisons

#### Section D: RAS Authentication

- Planning Decisions
- Authentication Methods
- Kerberos
- Certificate-based
- Smart Cards
- NTLM/Clear-text
- Digest/SSL/RADIUS
- RAS Policy

#### Section E: Security Design Process

- Server Roles
- Security Categories
- Identify Risks
- Identify Threats
- Business Requirements
- System Requirements

#### Section F: Security Baseline

- Baseline Strategy
- Baseline Server Roles
- Physical Security
- Passwords
- Hardware
- Security Templates