

# MS 6421B Configuring and Troubleshooting a Windows Server 2008 Network Infrastructure

## Introduction

This five-day instructor-led course provides students with the knowledge and skills to configure and troubleshoot Windows Server 2008 and Windows Server 2008 R2 Sp1 Network Infrastructures. It will cover networking technologies most commonly used with Windows Server 2008 and Windows Server 2008 R2 Sp1 such as DNS, DHCP, IPv4 and IPv6 network addressing, Network Policy server and Network Access Protection and configuring secure network access. It also covers fault tolerant storage technologies, Network Storage and routing and remote access, monitoring and compliance updates as well as other relevant technologies

## Audience

This course will be of interest and benefit to attendees with different back grounds and career aspirations. It will be of interest to Network Administrators who currently are, or will be, working with Windows Server 2008 servers. It will also be of interest and benefit to Active Directory technology specialists who aspire to be Enterprise Administrators (Tier 4 day-to-day network operations) or experienced Server Administrators who aspire to be Enterprise Administrators.

## At Course Completion

After completing this course, students will be able to:

After completing this course, students will be able to:

- Plan and configure an IPv4 network infrastructure.
- Implement DHCP within their organization.
- Configure and troubleshoot DNS.
- Configure, transition to, and troubleshoot IPv6.
- Configure and troubleshoot Routing and Remote Access.
- Install, configure, and troubleshoot the Network Policy Server Role service.
- Implement Network Access Protection.
- Implement security features within Windows Server 2008 and Windows Server 2008 R2.
- Implement security features within Windows Server 2008 and Windows Server 2008 R2 that help to secure network communications.
- Configure and troubleshoot file and print services.
- Enable and configure services to optimize branch office data access.
- Control and monitor network storage.
- Recover data on Windows Server 2008 and Windows Server 2008 R2 servers.
- Monitor Windows Server 2008 and Windows Server R2 network infrastructure services.

## Prerequisites

Before attending this course, students must have:

- You must have an intermediate understanding of Windows Server operating systems such as Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2 Sp1 and Windows client operating systems such as Windows Vista or Windows 7. Client operating system knowledge equivalent to the below certifications would be of benefit.
- You should understand how TCP/IP functions and have a basic understanding of addressing, name resolution (Domain Name System [DNS]/Windows Internet Name Service [WINS]), connection methods (wired, wireless, virtual private network [VPN]).
- You should have an awareness of security best practices such as understanding file system permissions, authentication methods, workstation, and server hardening methods, and so forth.

Basic knowledge of Active Directory would also be of benefit.

## **Course Outline**

### **Module 1: Planning and Configuring IPv4**

This module explains how to deploy and configure networking services in your organization. This module explains how to implement an IPv4 addressing scheme, determine which name services to deploy, and troubleshoot network-related problems.

#### **Lessons**

- Implementing an IPv4 Network Infrastructure
- Overview of Name Resolution Services in an IPv4 Network Infrastructure
- Configuring and Troubleshooting IPv4

#### **Lab : Planning and Configuring IPv4**

- Selecting an IPv4 Addressing scheme for branch offices
- Implementing and Verifying IPv4 in the branch office

#### **After completing this module, students will be able to:**

- Plan an IPv4 addressing scheme.
- Determine which name services you must deploy.
- 
- Configure and troubleshoot an IPv4 network.

## **Module 2: Configuring and Troubleshooting DHCP**

This module introduces you to Dynamic Host Configuration Protocol (DHCP), which plays an important role in the Windows Server 2008 R2 infrastructure. It is the primary means of distributing important network configuration information to network clients, and it provides configuration information to other network-enabled services, including Windows Deployment Services (WDS) and Network Access Protection (NAP). To support and troubleshoot a Windows Server-based network infrastructure, it is important that you understand how to deploy, configure, and troubleshoot the DHCP Server Role.

### **Lessons**

- Overview of the DHCP Server Role
- Configuring DHCP Scopes
- Configuring DHCP Options
- Managing a DHCP Database
- Monitoring and Troubleshooting DHCP
- Configuring DHCP Security

### **Lab : Configuring and Troubleshooting the DHCP Server Role**

- Selecting a Suitable DHCP Configuration
- Implementing DHCP
- Reconfiguring DHCP in the Head Office
- Testing the Configuration
- Troubleshooting DHCP Issues

### **After completing this module, students will be able to:**

- Describe the function of the DHCP Server Role.
- Configure DHCP scopes.
- Configure DHCP options.
- Manage a DHCP database.

- Monitor and troubleshoot the DHCP Server Role.
- Configure security the DHCP Server Role.

### **Module 3: Configuring and Troubleshooting DNS**

This module introduces you to Domain Name System (DNS), which is the foundation name service in Windows Server 2008 R2. It is vital that you understand how to deploy, configure, manage, and troubleshoot this critical service.

#### **Lessons**

- Installing the DNS Server Role
- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS

#### **Lab : Configuring and Troubleshooting DNS**

- Selecting a DNS Configuration
- Deploying and Configuring DNS
- Troubleshooting DNS

#### **After completing this module, students will be able to:**

- Install the DNS server role.
- Configure the DNS server role.
- Create and configure DNS zones.
- Configure zone transfers.
- Manage and troubleshoot DNS.

#### **Module 4: Configuring and Troubleshooting IPv6 TCP/IP**

This module introduces you to IPv6, a technology that will help ensure that the Internet can support a growing user base and the increasingly large number of IP-enabled devices. The current Internet Protocol Version 4 (IPv4) has served as the underlying Internet protocol for almost thirty years. Its robustness, scalability, and limited feature set is now challenged by the growing need for new IP addresses, due in large part to the rapid growth of new network-aware devices.

#### **Lessons**

- Overview of IPv6
- IPv6 Addressing
- Coexistence with IPv6
- IPv6 Transition Technologies
- Transitioning from IPv4 to IPv6

#### **Lab : Configuring an ISATAP Router**

- Configuring a New IPv6 Network and Client
- Configuring an ISATAP Router to Enable Communication Between an IPv4 Network and an IPv6 Network

#### **Lab : Converting the Network to Native IPv6**

- Transitioning to a Native IPv6 Network

#### **After completing this module, students will be able to:**

- Describe the features and benefits of IPv6.
- Implement IPv6 addressing.
- Implement an IPv6 coexistence strategy.

- Describe and select a suitable IPv6 transition solution.
- Transition from IPv4 to IPv6.
- Troubleshoot an IPv6-based network.

### **Module 5: Configuring and Troubleshooting Routing and Remote Access**

To support your organization's distributed workforce, you must become familiar with technologies that enable remote users to connect to your organization's network infrastructure. These technologies include virtual private networks (VPNs) and DirectAccess. It is important that you understand how to configure and secure your remote access clients by using network policies. This module explores these remote access technologies.

#### **Lessons**

- Configuring Network Access
- Configuring VPN Access
- Overview of Network Policies
- Overview of the Connection Manager Administration Kit
- Troubleshooting Routing and Remote Access
- Configuring DirectAccess

#### **Lab : Configuring and Managing Network Access**

- Configuring Routing and Remote Access as a VPN Remote Access Solution
- Configuring a Custom Network Policy
- Create and distribute a CMAK Profile

#### **Lab : Configuring and Managing DirectAccess**

- Configure the AD DS Domain Controller and DNS
- Configure the PKI Environment

- Configure the DirectAccess Clients and Test Intranet Access
- Configure the DirectAccess Server
- Verify DirectAccess Functionality

**After completing this module, students will be able to:**

- Configure network access.
- Create and configure a VPN solution.
- Describe the role of network policies.
- Use the Connection Manager Administration Kit to create and configure client connection profiles.
- Troubleshoot routing and remote access.
- Implement DirectAccess.

**Module 6: Installing, Configuring, and Troubleshooting the Network Policy Server Role Service**

NPS provides support for the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured as a RADIUS server or proxy. Additionally, NPS provides functionality that is essential for the implementation of Network Access Protection (NAP). This module explains how to install, configure, and troubleshoot NPS.

**Lessons**

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server

**Lab : Configuring and Managing Network Policy Server**

- Installing and Configuring the Network Policy Server Role Service

- Configuring a RADIUS Client
- Configuring Certificate Auto-Enrollment
- Configuring and Testing the VPN

**After completing this module, students will be able to:**

- Install and configure NPS.
- Configure RADIUS clients and servers.
- Describe NPS authentication methods.
- Monitor and troubleshoot NPS.

**Module 7: Implementing Network Access Protection**

In this module, you will learn about Network Access Protection (NAP). NAP enables you to create customized health-requirement policies to validate computer health before allowing access or communication. NAP also automatically updates compliant computers to ensure on-going compliance and can limit the access of noncompliant computers to a restricted network until they become compliant.

**Lessons**

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP

**Lab : Implementing NAP into a VPN Remote Access Solution**

- Configuring NAP Components
- Configuring Client Settings to Support NAP

**After completing this module, students will be able to:**

- Describe how NAP can help protect your network.
- Describe the various NAP enforcement processes.
- Configure NAP.
- Monitor and troubleshoot NAP.

### **Module 8: Increasing Security for Windows Servers**

Security is an essential consideration for networking with Windows Server 2008. In this module, you will learn how to implement various methods to increase security. Windows Firewall with Advanced Security is one of the features in Windows Server 2008 that is used to increase security. You can also use Windows Server Update Services to ensure that approved security updates are applied to servers in a timely way.

#### **Lessons**

- Windows Security Overview
- Configuring Windows Firewall with Advanced Security
- Deploying Updates with Windows Server Update Services

#### **Lab : Increasing Security for Windows Servers**

- Deploying a Windows Firewall Rule
- Implementing WSUS

#### **After completing this module, students will be able to:**

- Describe a process for increasing the security of Windows Server 2008.
- Configure Windows Firewall with Advanced Security.
- Describe Windows Server Update Services and how to use it.

## **Module 9: Increasing Security for Network Communication**

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over IP networks through cryptographic security services. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft IPsec implementation is based on standards that the Internet Engineering Task Force (IETF) IPsec working group developed. In this module, you will learn how to implement, configure, and troubleshoot IPsec.

### **Lessons**

- Overview of IPsec
- Configuring Connection Security Rules
- Configuring NAP with IPsec Enforcement
- Monitoring and Troubleshooting IPsec

### **Lab : Increasing Security for Network Communication**

- Selecting a Network Security Configuration
- Configuring IPsec to Authenticate Computers
- Testing IPsec Authentication

### **After completing this module, students will be able to:**

- Describe when and how to use IPsec.
- Configure Connection Security rules.
- Configure IPsec with NAP Enforcement.
- Describe how to monitor and troubleshoot IPsec.

## **Module 10: Configuring and Troubleshooting Network File and Print Services**

File and print services are some of the most commonly implemented network services for end users. Unlike infrastructure services like DNS, file and print services are highly visible to the end users. In this module, you will learn how to configure and troubleshoot file and print services to provide high quality service to end users. In addition, you will see how both EFS and BitLocker can be used to increase the security of files that are located in file shares.

## Lessons

- Configuring and Troubleshooting File Shares
- Encrypting Network Files with EFS
- Encrypting Partitions with BitLocker
- Configuring and Troubleshooting Network Printing

## Lab : Configuring and Troubleshooting Network File and Print Services

- Creating and Configuring a File Share
- Encrypting and Recovering Files
- Creating and Configuring a Printer Pool

## After completing this module, students will be able to:

- Describe how to manage file share security.
- Explain how to encrypt network files with EFS.
- Describe how to encrypt partitions with BitLocker.
- Discuss how to configure and troubleshoot network printing.

## Module 11: Optimizing Data Access for Branch Offices

Many organizations maintain a large number of file resources that need to be organized and made highly available to users. These file resources are often stored on servers and provided to users who are distributed geographically in widespread locations. In this module, you will learn how to provide efficient access to network resources with minimal traffic over a WAN link.

## Lessons

- Branch Office Data Access

- DFS Overview
- Overview of DFS Namespaces
- Configuring DFS Replication
- Configuring BranchCache

**Lab : Implementing DFS**

- Installing the DFS Role Service
- Configuring the Required Namespace
- Configuring DFS Replication

**Lab : Implementing BranchCache**

- Performing Initial Configuration Tasks for BranchCache
- Configuring BranchCache Clients
- &

**Upcoming Classes**

Jul 16, 2012 - Jul 20, 2012  
Sep 10, 2012 - Sep 14, 2012  
Oct 15, 2012 - Oct 19, 2012