



"Charting the Course ...

protechtraining.com

... to Your Success!"

MOC 10970 B Networking with Windows Server

Course Summary

Description

Get hands-on instruction and practice implementing networking with Windows Server 2012 and Windows Server 2012 R2 in this 5-day Microsoft Official Course. You will learn the skills you need to help reduce networking complexity while lowering costs, simplifying management tasks, and delivering services reliably and efficiently. You will learn how to automate and consolidate networking processes and resources, more easily connect private clouds with public cloud services, and more easily connect users to IT resources and services across physical boundaries. You will learn how to configure some of the key networking features such as IP Addressing, IPAM, DNS and DHCP, Remote Access technologies such as DirectAccess and VPNs. You will learn how to secure networks using Windows Firewall, IPSec and Network Access Protection, as well as becoming familiar with high performance technologies such as NIC Teaming, Receive Side Scaling, SMB Direct and SMB MultiChannel. You will learn how to integrate your network infrastructure with Hyper-V and leverage virtual high performance technologies such as SR-IOV, virtual Machine Queue, (VMQ), virtual Receive Side Scaling (vRSS) as well as provision multitenant networks using Hyper-V Network Virtualization and provisioning external access for those multitenant networks using the built in software gateway in Window Server 2012 R2. As part of the learning experience, you will perform hands-on exercises in a virtual lab environment.

Objectives

At the end of this course, students will be able to:

- Plan and implement an IPv4 network and configure and manage DHCP.
- Implement name resolution by using DNS.
- Implement IPv6 and integrate IPv6 and IPv4 networks.
- Implement and manage the IP Address Management feature in Windows Server 2012.
- Implement and manage remote access technologies in Windows Server 2012 such as DirectAccess, VPNs and Web Application Proxy
- Implement network security by using Windows Firewall with Advanced Security and IPsec in Windows Server 2012.
- Implement and manage Network Access Protection (NAP).
- Implement network services for branch offices.
- Implement network infrastructure for file and data services.
- Implement and manage networking in Hyper-V.
- Virtualize the physical network infrastructure in Windows Server 2012 and Windows Server 2012 R2 using Hyper-V Network Virtualization and the built in Gateway.

Topics

- Implementing IPv4 Services
- Implementing Name Resolution by Using DNS
- Implementing IPv6
- Implementing and Managing IPAM
- Implementing Remote Access
- Implementing Network Security
- Implementing Network Access Protection
- Implementing Networking for Branch Offices
- Implementing Networking Infrastructure for File and Data Services
- Implementing and Managing Networking in Hyper-V
- Virtualizing your Network Infrastructure

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically.

MOC 10970 B Networking with Windows Server

Course Summary (cont'd)

Audience

This course is intended for Information Technology (IT) professionals who have some networking knowledge and experience and are looking for a single course that will further develop that knowledge and skillset on core and advanced networking technologies in Windows Server 2012 and Windows Server 2012 R2. This would typically include:

- Network administrators who are looking to further develop skills with the latest networking technology in Windows Server 2012 and Window Server 2012 R2
- System or Infrastructure Administrators with general networking knowledge who are looking to build upon that core knowledge and cross train into advanced networking technologies on Windows Server 2012 and Windows Server 2012 R2
- IT Professionals who have taken the 10967A: *Fundamentals of a Windows Server Infrastructure* course or have knowledge equivalent to the technologies covered in that course and are looking to build upon that knowledge

Prerequisites

Before attending this course, in addition to their professional experience, students who attend this training must have the following technical knowledge:

- Experience working with Windows Server 2008 or Windows Server 2012
- Experience working in a Windows Sever infrastructure enterprise environment
- An understanding of core networking infrastructure components and technologies such as cabling, routers, hubs, switches
- Familiarity with networking topologies and architectures such as LANs, WANs, and wireless networking
- Some basic knowledge of the TCP/IP protocol stack, addressing, and name resolution
- Experience with and knowledge of Hyper-V and virtualization technologies
- Hands-on experience working with Windows Client operating systems such as Windows 7 or Windows 8

Pre-requisite knowledge can be obtained by taking course 10967A: *Fundamentals of a Windows Server Infrastructure* or having knowledge equivalent the technologies covered in that course.

Duration

Five days

MOC 10970 B Networking with Windows Server

Course Outline

I. Implementing IPv4 Services

Windows networks rely heavily on the IPv4 protocol for the transmission of network data. As a network administrator, you must understand the functionality of IPv4. This module explains how to plan and troubleshoot IPv4-based networks to ensure a properly functioning network environment.

- A. Planning IPv4 Addressing
- B. Managing and Troubleshooting IPv4 Connectivity
- C. Deploying DHCP
- D. Managing and Troubleshooting DHCP

Lab : Implementing IPv4 Services

- Planning IPv4 Address Assignments
- Planning the DHCP Server Implementation
- Implementing the DHCP Configuration
- Validate the DHCP Deployment

II. Implementing Name Resolution by Using DNS

The DNS is the foundation name service in Windows Server 2012. It provides name resolution, and enables DNS clients to locate network services, such as Active Directory Domain Services (AD DS) domain controllers, global catalog servers, and messaging servers. If you configure your DNS infrastructure poorly, or if DNS is not working correctly, these important network services will be inaccessible to your network servers and clients. This module explains how to deploy, configure, manage, and troubleshoot DNS.

- A. Implementing DNS Servers
- B. Configuring Zones in DNS
- C. Configuring DNS Integration with AD DS
- D. Configuring Advanced DNS Settings

Lab : Planning and Implementing Name Resolution by Using DNS

- Planning DNS Name Resolution
- Implementing DNS Servers and Zones
- Integrating DNS with AD DS
- Validating the DNS Implementation

III. Implementing IPv6

IPv6 is a technology that helps the Internet support a growing user base and an increasingly large number of IP-enabled devices. IPv4 has been the underlying Internet protocol for almost 30 years. Its robustness,

scalability, and limited feature set is now challenged by the growing need for new IP addresses. This is largely because of the rapid growth of new network-aware devices. This module explains how to implement coexistence between IPv4 and IPv6 networks and transition from an IPv4 network to an IPv6 network.

- A. Overview of IPv6 Addressing
- B. Implementing IPv6 and IPv4 Coexistence
- C. Transitioning from IPv4 to IPv6

Lab : Configuring and Evaluating IPv6 Transition Technologies

- Reviewing the Default IPv6 Configuration
- Configuring Network Integration by Using ISATAP
- Configuring Native IPv6 Connectivity
- Configuring 6to4 Connectivity

IV. Implementing and Managing IPAM

This module explains how to implement and manage the IP Address Management feature in Windows Server 2012.

- A. IPAM Overview
- B. Deploying IPAM
- C. Managing IP Address Spaces with IPAM

Lab : Implementing IPAM

- Installing the IPAM Server Role
- Configuring IPAM Clients
- Managing IP Address Spaces

V. Implementing Remote Access

Remote access technologies in Windows Server 2012 enable users to securely connect to data and resources in corporate networks. In Windows Server 2012, four component technologies (Remote Access, DirectAccess, Routing, and Web Application Proxy) are integrated into a single, unified server role called Windows Server 2012 Remote Access. This module explains how to implement remote access technologies in Windows Server 2012. It also describes the different implementation scenarios for small or medium-sized organizations and enterprise organizations.

- A. Remote Access Overview
- B. Implementing DirectAccess by Using the Getting Started Wizard

MOC 10970 B Networking with Windows Server

Course Outline (cont'd)

- C. Implementing and Managing an Advanced DirectAccess Infrastructure
- D. Implementing VPN
- E. Planning a Complex Remote Access Infrastructure
- F. Implementing Web Application Proxy

Lab : Implementing DirectAccess by Using the Getting Started Wizard

- Verifying Readiness for a DirectAccess Deployment
- Running the Getting Started Wizard
- Validating the DirectAccess Deployment

Lab : Deploying an Advanced DirectAccess Solution

- Preparing the Environment for DirectAccess
- Implementing the Advanced DirectAccess Infrastructure
- Validating the DirectAccess Deployment

Lab : Implementing VPN

- Implementing VPN
- Validating the VPN Deployment

Lab : Implementing Web Application Proxy

- Implementing Web Application Proxy
- Validating the Web Application Proxy Deployment

VI. Implementing Network Security

When you connect your server computers to a network, you might expose them to additional security threats. You must formulate a strategy to protect your servers from these threats. User policies, antivirus software, encrypted network traffic, and other protective measures can work together to help shield your servers from security threats. This module explores some of the technologies in Windows Server 2012 that you can use to help to mitigate these network security threats.

- A. Managing Windows Firewall with Advanced Security
- B. Configuring IPsec and Connection Security Rules
- C. Implementing Isolation Zones

Lab : Implementing Network Security

- Planning the Windows Firewall and Isolation Solution

- Implementing the Proposed Windows Firewall and Isolation Solution
- Validating the Network Security Settings

VII. Implementing Network Access Protection

You can use Network Access Protection (NAP) to create customized health-requirement policies to validate the health of a computer before allowing it to access or communicate with a network. Additionally, NAP automatically updates compliant computers to ensure their ongoing compliance and limits the access of noncompliant computers to the restricted network until they become compliant. This module explains how to configure, monitor, and troubleshoot NAP.

- A. Implementing NPS
- B. Network Access Protection Overview
- C. Configuring NAP
- D. Configuring IPsec Enforcement for NAP
- E. Monitoring and Troubleshooting NAP

Lab : Implementing NAP with VPN Enforcement

- Configuring NAP with VPN Enforcement
- Testing the Deployment

Lab : Implementing IPsec Enforcement for NAP?

- Configuring IPsec Enforcement for Internal Computers
- Configuring IPsec Enforcement for DirectAccess
- Validating the Deployment

VIII. Implementing Networking for Branch Offices

Branch offices can provide challenges for network administrators. When organizations have centralized infrastructure, such as database servers in a data center or file servers in the head office, access from branch offices is often limited because of the decreased network bandwidth of wide area network (WAN) connections.

This module explains the different ways that you can use Windows Server 2012 to overcome the limitations of branch office scenarios.

- A. Networking Features and Considerations for Branch Offices
- B. Implementing DFS for Branch Offices
- C. Implementing BranchCache for Branch Offices

MOC 10970 B Networking with Windows Server

Course Outline (cont'd)

Lab: Implementing Networking for Branch Offices

- Implementing DFS
- Implementing BranchCache
- Validating the Deployment

IX. Implementing Networking Infrastructure for File and Data Services

Windows Server 2012 provides a large set of features that you can use for network file access. You can use shared folders for different remote storage usage scenarios. You can use the Internet SCSI (iSCSI) capability in Windows Server 2012 to connect to remote iSCSI storage or configure Windows Server 2012 as an iSCSI storage host. This module explains the key network file and data services available in Windows Server 2012. It also explains how to implement the network file and data services to address the network and remote storage needs of your organization.

- A. Implementing Network File Services in Windows Server 2012
- B. Implementing iSCSI
- C. Implementing High Performance Networking Features

Lab: Implementing File and Data Networking Infrastructure

- Configuring iSCSI Storage Connectivity
- Testing iSCSI High Availability

X. Implementing and Managing Networking in Hyper-V

Most companies are deploying almost all servers as virtual machines running on a physical host. Virtual machines are isolated even when they are running on the same Hyper-V host, and they communicate only over the network. Hyper-V in Windows Server 2012 and Windows Server 2012 R2 includes a completely redesigned and extensible virtual switch,

which enables basic network packet forwarding, and also more advanced features such as support for network virtualization. As a Windows server administrator, it is important that you know how to configure the networking environment for the virtual machines and hosts. This module describes the networking components available in Hyper-V and describes how to configure these components.

- A. Creating and Using Hyper-V Virtual Switches
- B. Configuring Advanced Hyper-V Networking Features

Lab: Creating and Configuring Virtual Machine Networks

- Creating and Using Hyper-V Virtual Switches
- Configuring and Using the Advanced Features of a Virtual Switch

XI. Virtualizing your Network Infrastructure

This module explains the concepts and technologies related to virtualizing a physical network infrastructure in Windows Server 2012 and Windows Server 2012 R2. It also explains how to implement some core components of these technologies such as Hyper-V Network Virtualization and the built in software gateway in Windows Server 2012 R2.

- A. Implementing Hyper-V Network Virtualization
- B. Managing Your Virtualized Network Infrastructure

Lab: Creating and Configuring Virtual Machine Networks

- Configuring Hyper-V Network Virtualization
- Creating VPN Gateway for two Isolated Networks
- Provide Internet Access for two Isolated Networks by Using Gateway