

Module 7 – Network Access and Security

In Module 7 students will learn several strategies for controlling network access and enhancing network security. These will include: controlling network location profiles, configuring a RADIUS client, server and proxy, configuring a DHCP server as an enforcement point, enforcing network authentication using Kerberos and NTLM, configuring a firewall, and configuring IPsec to protect IP packets during transmission.

Section 7.1: Network Location Profiles

Summary

This section provides a summary of using network location profiles to identify network connection types. Details include:

- Network profile types:
 - Domain
 - Public
 - Private
- Configuring profile settings manually
- Enforcing profile settings



Students will learn how to:

- Change the location type on a client computer.
- Configure Network List Manager Policies to control client network connections profiles.

Configuring Server 2008 Network Infrastructure Objectives

- 104. Configure Windows Firewall with Advanced Security.
 - Configure firewall by using Group Policy
 - Network location profiles

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo	Time
<input type="checkbox"/>  7.1.1 Network Location Profiles	1:31
<input type="checkbox"/>  7.1.2 Configuring Network List Manager Policies	<u>6:00</u>
<i>Total</i>	7:31

Total Time: About 10 minutes

Section 7.2: RADIUS

Summary

This section discusses using Remote Authentication Dial-In User Service (RADIUS) to consolidate network policies for multiple servers to authenticate remote access clients. Details include:

- Components of a RADIUS solution:
 - Remote access clients
 - RADIUS client
 - RADIUS server
 - RADIUS proxy
 - Remote RADIUS server group
 - Network policies
 - Connection request policies
 - RADIUS Accounting
 - NPS templates
 - User account databases
 - RADIUS messages
- Configuring the components to configure a RADIUS solution:
 - RADIUS server
 - RADIUS client
 - Remote access client
 - RADIUS proxy
 - RADIUS accounting
- Best practices for configuring NPS for RADIUS

Students will learn how to:

- Configure a remote access server as a RADIUS client.
- Configure a RADIUS server.
- Configure a RADIUS proxy by configuring Remote RADIUS Server groups and Connection Request policies.




Configuring Server 2008 Network Infrastructure Objectives

- 301. Configure remote access.
- 304. Configure Network Policy Server (NPS)
 - RADIUS accounting
 - Connection Request policies
 - RADIUS proxy
 - NPS templates

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

CIST2413 Microsoft Network Infrastructure

Video/Demo

	Time
<input type="checkbox"/>  7.2.1 RADIUS	3:57
<input type="checkbox"/>  7.2.2 Installing the NPS Role	2:08
<input type="checkbox"/>  7.2.3 Configuring RADIUS	<u>6:25</u>
<i>Total</i>	<u>12:30</u>

Lab/Activity

- Configure a RADIUS Server
- Configure a RADIUS Client
- Configure a RADIUS Proxy

Number of Exam Questions: 9 questions

Total Time: About 40 minutes

Section 7.3: Network Access Protection (NAP)

Summary

This section examines how NAP can be used to regulate network access or communication based on a computer's compliance with health requirement policies.

Details include:

- Features of NAP
 - Health state validation
 - Health policy compliance
 - Limited access network
- Components that comprise the NAP system:
 - NAP Client
 - NAP Server
 - Enforcement Server (ES)
 - Remediation Server
- Configuring NAP requires:
 - Configuring the NAP server
 - Configuring the client computer
 - Configuring the following enforcement points:
 - DHCP
 - VPN
 - 802.1x
 - Remote Desktop Gateway
 - IPsec

Students will learn how to:

- Configure a DHCP server as an enforcement point.
- Configure SHV settings, remediation server groups, health policies, and network policies for NAP.





CIST2413 Microsoft Network Infrastructure

- Enable NAP enforcement on a client computer.

Configuring Server 2008 Network Infrastructure Objectives

- 302. Configure Network Access Protection (NAP).
 - DHCP enforcement
 - VPN enforcement
 - Configure NAP health policies
 - IPsec enforcement
 - Multi-configuration System Health Validator (SHV)

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo	Time
<input type="checkbox"/>  7.3.1 Network Access Protection (NAP)	4:53
<input type="checkbox"/>  7.3.3 Configuring DHCP Enforcement	15:56
<input type="checkbox"/>  7.3.4 Configuring VPN Enforcement	13:03
<input type="checkbox"/>  7.3.5 NAP Enforcement Configuration	<u>8:16</u>
<i>Total</i>	<i>42:08</i>

Number of Exam Questions: 17 questions

Total Time: About 65 minutes

Section 7.4: Network Authentication

Summary

In this section students will learn network authentication mechanisms for logging on to the server or domain. Details include:



- Kerberos authentication and authorization
- NTLM authentication and authorization
- Conditions of when to use different authentication methods:
 - Kerberos
 - NTLM v2
 - NTLM or LM
- Best practices regarding configuring domain authentication
- Kerberos policy settings:
 - Enforce user logon restrictions
 - Maximum lifetime for service ticket
 - Maximum lifetime for user ticket
 - Maximum lifetime for user ticket renewal
 - Maximum tolerance for computer clock synchronization

Students will learn how to:

CIST2413 Microsoft Network Infrastructure

- Configure Group Policy to enforce the use of NTLMv2 for authentication.

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo	Time
<input type="checkbox"/>  7.4.1 LAN Authentication	1:49
<input type="checkbox"/>  7.4.2 Configuring LAN Authentication	<u>2:41</u>
<i>Total</i>	4:30

Lab/Activity

- Enforce NTLM v2

Number of Exam Questions: 1 question

Total Time: About 15 minutes

Section 7.5: Firewall

Summary

This section discusses the specifics of managing a firewall. Details include:

- Tools you can use to manage the firewall:
 - Windows Firewall (in Control Panel)
 - Windows Firewall with Advanced Security
- Features of Windows Firewall with Advanced Security:
 - Profiles
 - Firewall rules
 - Connection security rules
 - Monitoring
 - Policies
- Use Window Firewall with Advanced Security to create the following types of inbound and outbound rules:
 - Program rule
 - Port rule
 - Predefined rule
 - Custom rule
- Types of connection security rules:
 - Isolation
 - Authentication exemption
 - Server-to-server
 - Tunnel
 - Custom
- Action options that apply to the traffic which meet the rule's conditions:
 - Allow the connection
 - Block the connection

CIST2413 Microsoft Network Infrastructure

- Allow the connection if it is secure
- Options that can be configured for network profiles:
 - Firewall state
 - Inbound connections
 - Outbound connections
- Tips for managing firewall settings
- Port numbers for common services




Students will learn how to:

- Use the Basic Firewall to allow traffic based on port, protocol, or application.
- Use the Windows Firewall with Advanced Security to manage custom firewall rules.
- Use Group Policy to enforce firewall rules.

Configuring Server 2008 Network Infrastructure Objectives

- 104. Configure Windows Firewall with Advanced Security.
 - Inbound and outbound rules
 - Custom rules
 - Authorized users
 - Authorized computers
 - Configure firewall by using Group Policy
 - Network location policies
 - Isolation policy
 - Connection security rules

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo	Time
<input type="checkbox"/>  7.5.1 Windows Firewall	4:04
<input type="checkbox"/>  7.5.3 Configuring Windows Firewall with Advanced Security	14:07
<input type="checkbox"/>  7.5.4 Configuring Firewall GPO Settings	<u>2:39</u>
<i>Total</i>	<u>20:50</u>

Number of Exam Questions: 11 questions

Total Time: About 40 minutes

Section 7.6: IPsec

Summary

This section provides the details of how Internet Protocol Security (IPsec) protects IP packets during transmission. Details include:

- IPsec protocols:

CIST2413 Microsoft Network Infrastructure

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)
- Authenticated IP (AuthIP)
- Phases to establish the IPsec connection:
 - Phase 1 (Main Mode)
 - Phase 2 (Quick Mode)
- Protocols supported for configuring IPsec:
 - Integrity:
 - SHA1
 - MD5
 - Encryption:
 - AES-256
 - AES-192
 - AES-128
 - 3DES (Triple-DES)
 - DES
 - Key exchange:
 - Elliptic Curve Diffie-Hellman P-384
 - Elliptic Curve Diffie-Hellman P-256
 - Diffie-Hellman Group 14
 - Diffie-Hellman Group 2
 - Diffie-Hellman Group 1
- Authentication:
 - Kerberos
 - NTLMv2
 - Computer certificates, including health certificates
 - Preshared key
- Configuring IPsec through Windows Firewall with Advanced Security console

Students will learn how to:

- Configure connection security rules by determining the rule type, requirements, authentication method, and profile(s) to which the rule applies.
- Monitor connection security rules and security associations.

Configuring Server 2008 Network Infrastructure Objectives

- 104. Configure IPsec.
 - IPsec group policy



Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo

Time

- | | |
|--|------|
| <input type="checkbox"/>  7.6.1 IPsec | 6:14 |
| <input type="checkbox"/>  7.6.3 IPsec Connection Security Rules | 3:13 |

CIST2413 Microsoft Network Infrastructure

<input type="checkbox"/>  7.6.4 Configuring IPsec	7:17
<input type="checkbox"/>  7.6.6 IPsec Improvements	<u>3:16</u>
<i>Total</i>	<u>20:00</u>

Number of Exam Questions: 10 questions

Total Time: About 40 minutes

Section 7.7: DirectAccess

Summary

This section discusses using DirectAccess as an automatic connectivity solution. Details include:

- A comparison of a VPN solution to a DirectAccess solution
- The support that DirectAccess provides
- DirectAccess connection methods:
 - Full enterprise network access (end-to-edge)
 - Selected server access (modified end-to-edge)
 - End-to-end
- The process that the DirectAccess client uses to connect to intranet resources
- DirectAccess requirements for the:
 - Infrastructure
 - Server
 - Client
- Configuration details for DirectAccess components:
 - Server
 - Client side

Configuring Server 2008 Network Infrastructure Objectives

- 303. Configure DirectAccess.
 - IPv6
 - IPsec
 - Server requirements
 - Client requirements

Log into LabSim and complete the tasks listed under Resources for each of the items listed below. As you complete them Checkoff the boxes:

Video/Demo	Time
<input type="checkbox"/>  7.7.1 DirectAccess	9:00

Number of Exam Questions:13 questions

Time: About 30 minutes