COURSE SYLLABUS

MCSE

- Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Exam 70-293)
- Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure (Exam 70-294/297)

50 Cragwood Rd, Suite 350
South Plainfield, NJ 07080

Victoria Commons, 613 Hope Rd Building #5,
Eatontown, NJ 07724

130 Clinton Rd,
Fairfield, NJ 07004

Avtech Institute of Technology Course

Instructor:
Course Duration:
Date/Time:
Training Location:

Course: NEPE 107 (Exam 70-293)

Text / Lab Books:

MCSA/MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft ® Windows Server™ 2003 Network Infrastructure

Craig Zacker with Anthony Steven of Content Master

Microsoft Express

Course Description

In this course students will lean to Plan and maintain a Microsoft Windows Server 2003 network infrastructure. This course aids in the preparation for the Microsoft Exam 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure certification exam.

Learning Objectives

1.0 Planning a Network Topology

1.1. Define what a network infrastructure is and understand how to plan, implement and maintain a network infrastructure. Understand what the OSI reference model is and define the purpose of and select the data-link layer protocol. Practice choosing and Ethernet variant. Define the purpose of and select the network/transport layer protocols and understand how TCP/IP is used.

1.2. Determine the location of network resources for the following criteria: Workstations, peripherals, cables, connectivity devices and servers. Practice blueprinting a network infrastructure.

2.0 Planning TCP/IP Network Infrastructure

2.1. Determine the requirements of IP addressing using public and private addresses and by accessing the internet from a private network. Understand how to plan for IP addresses accordingly and practice using registered and unregistered IP address.

2.2. Understand and plan an IP routing solution by creating LANs, WANs using routers and switches. Design an internetwork by combining routing and switching.

2.3. Plan an IP address and subnet strategy by obtaining network addresses and

understand how IP address are classed and subnetted. Practice subnetting IP addresses. Assign an IP address by manually configuring TCP/IP clients and installing a DHCP server. Understand its allocation methods and plan a deployment scheme.

2.4. Become familiar with isolating TCP/IP problems and troubleshoot problems associated with client configuration and DHCP.

3.0 Planning Internet Connectivity

3.1. Plan an internet connectivity infrastructure by determining the requirements of internet connectivity as well as choosing a connection type. Understand the various WAN speeds that can be implemented.

3.2. Select routers and ISPs by choosing a router type and a suitable internet service provider. Practice configuring an NAT router.

3.3. Secure and regulate internet access by determining the requirements for internet security using NAT, proxy server and selecting a suitable internet access method. Practice configuring an NAT router.

3.4. Determine the scope of a problem with internet connectivity and diagnose client configuration problems such as NAT, proxy server and internet connection problems.

4.0 Planning a Name Resolution

4.1. Define what a name resolution is and determine the requirements used for name resolution. Understand what types of names need to be resolved using the DNS. Determine requirements of DNS also and become familiar with using NetBIOS and local host name resolutions. Practice specifying name resolution requirements.

4.2. Design a DNS namespace using an existing namespace and creating internet and internal domains. Design a DNS namespace by combining the internet and internal domains and create an internal root and host names.

4.3. Implement a DNS name resolution strategy and det4rmine how many DNS servers are being used. Understand DNS server types and functions used and create a zone. Implement a NetBIOS name resolution strategy and install a WINS server/ Determine DNS security threats and understand the techniques used for DNS security. Troubleshoot client configuration problems and DNS server problems.

5.0 Using Routing and Remote Access

5.1. Plan a routing and remote access strategy by choosing a WAN topology and selecting a WAN technology. Select an appropriate router and determine how static and dynamic routing is used. Understand how to route IP multicast traffic and install RIP.

5.2. Determine security requirements to secure remote access and control access using dial-in properties and plan authentication methods using remote access policies. Practice installing a routing and remote access server.

5.3. Troubleshooting TCP/IP routing by isolating router problems. Troubleshoot remote routing and remote access configuration as well as the routing table.

6.0 Maintaining Server Availability

6.1. Monitor network traffic using the performance console and analyze network traffic with the network monitor. Become familiar with using the network monitor. Monitor network server services and locate system bottlenecks. Practice establishing a performance baseline.

6.2. Understand the importance of a network backup and create a backup plan. Understand how to perform a backup restore using Volume Shadow Copy and practice using Windows Server 2003 backup.

7.0 Clustering Servers

7.1. Understand and design a clustering solution. Understand the use of network load balancing and plan a deployment for it. Monitor network load balancing and create a network load balancing cluster.

7.2. Design a server cluster deployment and plan a server cluster hardware configuration. Create an application deployment plan, a server cluster and a single node cluster. Configure failover policies.

8.0 Planning a Secure Baseline Installation

8.1. Understand a computer's role and create hardware specifications and selecting a suitable operating system. Plan a security framework using high-level security planning. Create a security design team and map out a security life cycle. Identify and evaluate security settings and modify default security settings.

9.0 Hardening Servers

9.1. Create a baseline for member services and set audit policies, event log policies and configure services and security options. Practice creating a group policy object. Create role=specific server configurations by securing domain controllers, infrastructure servers, file and print servers and application servers. Practice modifying the GPO for the main controllers and container's GPO. Deploy role-specific GPO's by combining policies and deploying multiple GPO's.

10.0 Deploying Security Configurations

10.1. Deploy security configurations by creating a testing environment, a pilot deployment as well as a pilot deployment plan. Understand security templates, using the templates console and the supplied security templates.

10.2. Deploy the security templates and use group policies, security configuration and the analysis tool to assist in security configuration.

11.0 Creating and Managing Digital Certificates

11.1. Define and understand the use of the public key infrastructure as well as the functions associated with it. Define the requirements of a certificate. Design a public key infrastructure by creating a CA infrastructure and configuring the certificate. Practice installing a Windows Server 2003 Certification Authority.

11.2. Understand how to manually request, enroll and renew a certificate as well as how to revoke a certificate when required.

12.0 Securing Network Communications Using IPSec

12.1. Define the purpose of packet filtering and specify criteria. Understand how Windows Server 2003 uses packet filtering and create packet filters in routing and remote access services.

12.2. Plan an IPSec implementation by evaluating threats. Understand IPSec protocols including the transport and tunnel modem. Deploy IPSec Components and understand how to work with and create IPSec policies.

12.3. Troubleshoot policy mismatches and examine IPSec traffic using Resultant Set of Policy feature.

13.0 Designing a Security Infrastructure

13.1. Understand software update practices using Windows Update feature and practice how to update a network and become familiar with using Microsoft Baseline Security Analyzer.

13.2. Determine how to secure a wireless network and understand wireless networking standards. Control wireless access using group policies and authenticate users by encrypting traffic.

13.3. Provide secure Network Administration by configuring remote assistance and remote desktop.

Course: NEPE 109 (Exam 70-294 & Exam 70-297)  **Active Directory**

Text / Lab Books:

MCSA/MCSE Self-Paced Training Kit (Exam 70-294): Planning, Implementing and Maintaining a Microsoft ® Windows Server™ 2003 Active Directory Infrastructure

Jill Spealman, Kurt Hudson, and Melissa Craft with Anthony Steven of Content Master

Microsoft Press

Course Description

In this course students will lean to Planning, Implementing and Maintaining a Microsoft ® Windows Server™ 2003 Active Directory Infrastructure. This course aids in the preparation for the Microsoft Exam 70-294 & 70-297: Design and Maintaining a Microsoft Windows Server 2003 Active Directory certification exam.

Learning Objectives

1.0 Introduction to Active Directory and Network Infrastructure

1.1. Define the purpose of Active Directory is and understand its logical active directory structure, its trust relationships and how the active directory database is partitioned. Understand the basic physical network structure of the active directory.

1.2. Define the purpose of name resolution services, DNS and how Active Directory uses DNS. Define how these are used to resolve host names to IP addresses. Define the use of TCP/IP, its architecture and the use of IP addressing and routing including how it is assigned using DHCP.

1.3. Understand what remote access provides and recognize the connection methods used. Define the protocols used by routing and remote access as well as its security features.

2.0 Analyzing an Existing Infrastructure

2.1. Identify the main geographical company models and differentiate between these models and the state of connection between the locations. Understand the geographical considerations that are controlled by companies and offices. Analyze the current administration model and the existing network topology within a network environment. Analyze performance requirements.

2.2. Analyze an existing directory structure such as Windows 2000 and NT 4.0 infrastructure. Gather information by creating diagrams showing the existing domain and their trust relationships.

3.0 Planning an Active Directory Structure

3.1. Use single and multiple domains deploy simple structures and implement different security policies. Use multiple domain trees to support multiple DNS namespaces. Use multiple forests to support multiple distinct companies. .

3.2. Define a name strategy using Active Directory naming and LDAP. Identify what needs to be considered when implementing and creating a naming scheme. Choose a domain name and support registered DNS names.

4.0 Design an Active Directory Structure

4.1. Define the purpose of Organizational Unit Structures. Design and create an OU structure to delegate administrative control, limit object visibility, and control group

policy. Administer inheritance in your designs to facilitate the flow of permissions throughout the structure.

4.2. Identify the different types of accounts used when planning an account strategy. Plan computer, user and group accounts. Understand the purpose of a group policy and plan a GPO structure as well as the deployment of a GPO. Design a group policy implementation.

5.0 Design a Site Plan

5.1. Design a site topology and understand why it is used. Create a site for each LAN, location and domain controller. Plan domain controller placement, operations master servers, global catalog servers and domain controller capacity. Design a migration path and consider the easiest and most cost effective method of upgrading.

6.0 Design a DNS Structure

6.1. Analyze and identify the current DNS infrastructure. Understand the purpose of DNS and how it functions. Design a DNS namespace and identify the considerations to be taken to design the Active Directory structure. Secure the DNS components to reduce the risk of threats. Design a DNS namespace for forests and domain.

6.2. Design DNS implementation taking zone storage into consideration. Design a DNS service placement and design a DNS infrastructure.

7.0 Designing a WINS Structure

7.1. Define the purpose of WINS and understand what it does and identify the use of its components, databases including the database files and size. Design a WINS infrastructure by creating a conceptual design. Design a NetBIOS name resolution strategy. Create a replication strategy and understand how to delete and tombstone records. Determine the best method of securing a WINS replication strategy.

8.0 Designing a Network and Routing Infrastructure

8.1. Understand how IP addressing is used to configure all client workstations, printers, servers etc. with unique IP addresses. Create an IP addressing scheme. Determine subnets to be created and number of available host addresses needed for each subnet.

8.2. Design a perimeter network and understand how to protect a private network. Understand the use of DHCP and how it is used to secure an infrastructure. Create a DHCP strategy by designing a DHCP addressing scheme and enabling it to support various DHCP clients.

9.0 Design Internet Connectivity

9.1. Identify and design redundancy into a connectivity design. Verify that redundancy is required. Identify hardware components that affect the infrastructure. Identify, calculate

and obtain bandwidth requirements needed for a VPN.

9.2. Understand the use of Network Address Translation (NAT) and the limitations associated with it. Design a NAT strategy by creating a conceptual design and securing a NAT solution.

10.0 Designing a Remote Access Strategy

10.1. Identify the components of Dial-Up Remote Access through a physical connection and the differences between Network Access Client and Server. Understand the various methods of authenticating remote access and virtual private networking. Create a conceptual design for a wireless network.

10.2. Plan and design the capacity of a remote access infrastructure. Use an internet authentication service server to aid in the design of a security infrastructure for remote access users.

Prerequisite

Familiarity with PC & Windows OS

Contact Hours

_____ Contact Hours (Lecture ___ Hours / Lab ____ Hours)

Semester Credit Hours

_____ semester credit hours

Teaching Strategies

A variety of teaching strategies may be utilized in this course, including but not limited to, lecture, discussion, written classroom exercises, written lab exercises, performance based lab exercises, demonstrations, quizzes and examinations. Some quizzes may be entirely or contain lab based components. A mid-course and end course examination will be given.

Method of Evaluating Students

Grade Distribution

Class Attendance	10
Mid Term	30
Finals	50
Special Projects Makeup projects	10
Total	**100%**

Grading Policy

At the end of each course, each student is assigned a final grade as follows:

Point Range	Interpretation	Grade	Quality Points
90 – 100	Excellent	A	4.0
80 – 89	Very Good	B	3.0 – 3.9
70 – 79	Average	C	2.0 – 2.9
60 – 69	Poor	D	1.0 – 1.9
Below 60	Failure	F	0
N/A	Withdrawal	W	0
N/A	Pass	P	0
N/A	Incomplete	I	0

A student earning a grade of D or above is considered to have passed the course and is eligible to pursue further studies. A student receiving a grade of F has failed the course. A failed course must be repeated and passed to meet Avtech Institute's graduation requirements, in addition to an overall program GPA of 2.0.

Requirements for Successful Completion of the Course

At a minimum, students must achieve the following:

- A passing grade of **D** or above
- Completion of all required examinations
- Submission of all required lab exercises and projects and;
- Adherence to the school attendance policy.

Equipment Needed

Industry standard desktop computer for lab exercises.

Equipment Breakdown Lab room

Videos and Projector

Library Assignments

To be determined by the instructor.

Portfolio Assignment

Student program outcome portfolios are required to demonstrate student competencies. In conjunction with your course structure, please select a project/paper that best demonstrates what you have learned in this course and add it to your program portfolio.

Course Policies

Disruptive Behavior

Disruptive behavior is an activity that interferes with learning and teaching. Inappropriate talking during class, surfing inappropriate website, tardiness, cheating, alcohol or drug use, use of cell phone, playing lout music during class, etc. all disrupt the learning process.

Copyright Infringement

Specific exemptions to copyright infringement are made for student use in the context of learning activities. Graphic design students often download images from the Internet, or scan images from publications. As long as this work is for educational purpose, and subject to faculty permission, this is not a problem.

Plagiarism

Faculty cannot tolerate the ***misrepresentation of work as the student's own***. This often involves the use by one student or another student's design, whether voluntarily or involuntarily. In the event that plagiarism is evident and documented, all students involved in the conscious decision to misrepresent work must receive an F as the grade for the project. A second occurrence may result in suspension for the rest of the quarter, and return to the school only after a review by the Academic Standards Committee.

Attendance

Attendance and Lateness

In education and the workplace, regular attendance is necessary if individuals are to excel. There is a direct correlation between attendance and academic success. Attendance is mandatory. All students must arrive on time and prepared to learn at each class session. At the faculty member's discretion, students may be marked absent if they arrive more than 15 minutes late to any class. More that five absences in a class that meets twice per week or more that two absences in a class that meets once per week may result in a failure.

Make-Up Work

Late Projects and Homework

All projects and homework must be handed in on time. Homework should be emailed to your instructor if you are going to miss a class. Work that is submitted one week late will result in the loss of one full grade; and work that is submitted two weeks late will result in the loss of two full grades; more than two weeks late you will receive a failing grade on the project.