

Course Description:

CIS-016H - Microsoft® Windows® 2000 Network Environment: Exam 70-218 **Units: 3**

This course provides a foundation for students who want to learn how to administer and manage Microsoft® Windows® 2000 on enterprise networks, including the skills required to manage and support a networked system. Administration of Microsoft® Windows® 2000 Network Environment is emphasized. Students have at least six months of experience administering and supporting Windows 2000 server and client operating systems that use Active Directory™ directory services in the above environment, or proficiency in CIS 16D & CIS 16E. This course prepares students for MCSA exam 70-218 that measures the student's ability to administer, support, and troubleshoot information systems that incorporate Microsoft Windows 2000.

Lecture Hours: 2.5 Lab Hours: 1.5 Repeatable: No Grading: L

Prerequisite: CIS 016D WITH C OR BETTER

Corequisite: CIS 200

CAN: None

Advisory Level: Read: 2 Write: 2 Math:

Transfer Status: CSU Degree Applicable: AA/AS

CSU GE: None District GE: None IGETC: None

Learning Outcomes:

1. Publish resources in Active Directory. Types of resources include printers and shared folders
 - a. Perform a search in Active Directory Users and Computers
 - b. Configure a printer object
2. Manage data storage. Considerations include file systems, permissions, and quotas
 - a. Implement NTFS and FAT file systems
 - b. Enable and configure quotas
 - c. Implement and configure Encrypting File System (EFS)
 - d. Configure volumes and basic and dynamic disks
 - e. Configure file and folder permissions
 - f. Manage a domain-based distributed file system (DFS)
 - g. Manage file and folder compression
3. Create shared resources and configure access rights. Shared resources include printers, shared folders, and Web folders
 - a. Share folders and enable Web sharing
 - b. Configure shared folder permissions
 - c. Create and manage shared printers
 - d. Configure shared printer permissions
4. Configure and troubleshoot Internet Information Services (IIS)
 - a. Configure virtual directories and virtual servers
 - b. Troubleshoot Internet browsing from client computers
 - c. Troubleshoot intranet browsing from client computers
 - d. Configure authentication and SSL for Web sites
 - e. Configure FTP services
 - f. Configure access permissions for intranet Web servers
5. Monitor and manage network security. Actions include auditing and detecting security breaches
 - a. Configure user-account lockout settings
 - b. Configure user-account password length, history, age, and complexity
 - c. Configure Group Policy to run logon scripts
 - d. Link Group Policy objects
 - e. Enable and configure auditing
 - f. Monitor security by using the system security log file
6. Troubleshoot routing and connectivity problems using various diagnostic utilities and tools include the **tracert** command, the **ping** command, and the **ipconfig** command
 - a. Configure and troubleshoot TCP/IP on servers and client computers. Considerations include subnet masks, default gateways, network IDs, and broadcast addresses
 - b. Configure, administer, and troubleshoot DHCP on servers and client computers
 - c. Configure, administer, and troubleshoot DNS
 - d. Troubleshoot name resolution on client computers. Considerations include WINS, DNS, NetBIOS, the Hosts file, and the Lmhosts file

7. Install and configure server and client computer hardware
 - a. Verify hardware compatibility by using the qualifier tools
 - b. Configure driver signing options
 - c. Verify digital signatures on existing driver files
 - d. Configure operating system support for legacy hardware devices
8. Troubleshoot starting servers and client computers. Tools and methodologies include Safe Mode, Recovery Console, and parallel installations
 - a. Interpret the startup log file
 - b. Repair an operating system by using various startup options and Recovery Console
 - c. Recover data from a hard disk in the event that the operating system will not start
 - d. Restore an operating system and data from a backup
9. Utilize various troubleshooting skills in different scenarios
 - a. Troubleshoot User and Group objects in Active Directory
 - b. Troubleshoot Active Directory replication problems
 - c. Troubleshoot end-user Group Policy
 - d. Troubleshoot remote access and virtual private network (VPN) connections
 - e. Troubleshoot a remote access policy
 - f. Troubleshoot Terminal Services for remote access
 - g. Troubleshoot Network Address Translation (NAT) and Internet Connection Sharing