NETWORKING 4
Course Code 5313
(COURSE NAME CHANGES TO "ADVANCED SERVER ADMINISTRATION" IN 2016-17)

COURSE DESCRIPTION: Advanced Server Administration provides students with classroom and laboratory experience in current and emerging networking technologies. Upon successful completion of the course sequence, students will be able to seek employment or further their education and training in the information technology field. Students will benefit most from the curriculum if they possess a strong background in reading, math, and problem solving skills. Instruction includes advanced system hardware, advanced software, advanced storage, advanced IT environments, advanced disaster recovery, advanced troubleshooting, and leadership skills. Particular emphasis is placed on critical thinking skills and problem-solving techniques found in math and communication programs.

Advanced Server Administration may articulate with postsecondary institutions for completion of some advanced level competencies. Advanced Server Administration is the final course in a four course sequence of study.

OBJECTIVE: Given the essential classroom and work-based learning experiences, the student will be able to perform the following advanced competencies.

COURSE CREDIT: 1 or 2 Carnegie units

PREREQUISITE(S): Server Administration (5312)

RECOMMENDED GRADE LEVEL: 10-12

A. SAFETY

1. Review school safety policies and procedures.
2. Review classroom safety rules and procedures.
3. Review safety procedures for using equipment in the classroom.
4. Identify major causes of work-related accidents in office environments.
5. Demonstrate safety skills in an office/work environment.

B. STUDENT ORGANIZATIONS

1. Identify the purpose and goals of a Career and Technology Student Organization (CTSO).
2. Explain how CTSOs are integral parts of specific clusters, majors, and/or courses.
3. Explain the benefits and responsibilities of being a member of a CTSO.
4. List leadership opportunities that are available to students through participation in CTSO conferences, competitions, community service, philanthropy, and other activities.
5. Explain how participation in CTSOs can promote lifelong benefits in other professional and civic organizations.

C. TECHNOLOGY KNOWLEDGE

1. Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation.
2. Identify proper netiquette when using e-mail, social media, and other technologies for communication purposes.
3. Identify potential abuse and unethical uses of laptops, tablets, computers, and/or networks.
4. Explain the consequences of social, illegal, and unethical uses of technology (e.g., piracy; illegal downloading; licensing infringement; inappropriate uses of software, hardware, and mobile devices in the work environment).
5. Discuss legal issues and the terms of use related to copyright laws, fair use laws, and ethics pertaining to downloading of images, photographs, documents, video, sounds, music, trademarks, and other elements for personal use.
6. Describe ethical and legal practices of safeguarding the confidentiality of business-related information.
7. Describe possible threats to a laptop, tablet, computer, and/or network and methods of avoiding attacks.

D. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS

1. Demonstrate punctuality.
2. Demonstrate self-representation.
3. Demonstrate work ethic.
4. Demonstrate respect.
5. Demonstrate time management.
6. Demonstrate integrity.
7. Demonstrate leadership.
8. Demonstrate teamwork and collaboration.
9. Demonstrate conflict resolution.
10. Demonstrate perseverance.
11. Demonstrate commitment.
12. Demonstrate a healthy view of competition.
13. Demonstrate a global perspective.
14. Demonstrate health and fitness.
15. Demonstrate self-direction.
16. Demonstrate lifelong learning.

E. PROFESSIONAL KNOWLEDGE

1. Demonstrate effective speaking and listening skills.
2. Demonstrate effective reading and writing skills.
3. Demonstrate mathematical reasoning.
4. Demonstrate job-specific mathematics skills.
5. Demonstrate critical-thinking and problem-solving skills.
6. Demonstrate creativity and resourcefulness.

7. Demonstrate an understanding of business ethics.
8. Demonstrate confidentiality.
9. Demonstrate an understanding of workplace structures, organizations, systems, and climates.
10. Demonstrate diversity awareness.
11. Demonstrate job acquisition and advancement skills.
12. Demonstrate task management skills.
13. Demonstrate customer-service skills.

F. 1.0 ADVANCED SYSTEM HARDWARE

1.1 Differentiate between system board types, features, components, and their purposes.

- Dip switches/jumpers
- Processor (single and multi)
- Bus types and bus speeds
- On board components
    - NICs
    - Video
    - Audio
    - USB
    - HID
    - Serial
    - Parallel
- Expansion slots
    - PCI
    - PCIe
    - PCIx
    - AGP
    - ISA
- BIOS
- Riser Card/backplane
- Storage connectors
    - SCSI
    - SATA
    - IDE
    - Floppy

1.2 Deploy different chassis types and the appropriate components.

- Cooling
    - Fans
    - Water cooled
    - Passive
    - Active
    - Shroud
    - Ducts
    - Redundant cooling

- Hot swappable
- Ventilation

- Form Factor (tower, rack, blade)
  - Space utilization (U size, height, width, depth)
- Power
  - Connectors
  - Voltages
  - Phase
- Redundant power
- Shut off switches – chassis intrusion
- Power buttons
- Reset buttons
- Diagnostic LEDs
- Expansion bays

1.3 Differentiate between memory features/types and, given a scenario, select appropriate memory.

- Memory pairing
- ECC vs. non ECC
- Registered vs. non-registered
- RAID and hot spares
- Types
  - DDR
  - Fully buffered DIMM
  - DDR2
  - SDRAM
  - DDR3
- Memory compatibility
  - Speed
  - Size
  - Pins
  - CAS latency
  - Timing
  - Vendor specific memory
- On board vs. riser card

1.4 Explain the importance of a Hardware Compatibility List (HCL).

- Vendor standards for hardware
- Memory and processor compatibility
- Expansion cards compatibility
- Virtualization requirements

1.5 Differentiate between processor features/types and, given a scenario, select the appropriate processor.

- Multicore
- Multiprocessor

- Cache levels
- Stepping
- Speed
- VRMs
- Execute disable (XD) or not execute (NX)
- Hyper-Threading
- VT or AMD-V
- AMD vs. Intel (non-compatible CPUs)
- Processor architecture (RISC, CISC)
- Vendor slot types
- 64bit vs. 32 bit
- Heat dissipation (heat sinks, fans, liquid cooling)

1.6 Install appropriate expansion cards into a server while taking fault tolerance into consideration given a scenario.

- Manufacturer specific
  - o Fax cards
  - o PBX cards
  - o Camera cards
  - o VoIP
- HBAs
- NICs
- Video
- Audio
- Storage controller (SCSI, SATA, RAID)
  - o SCSI low voltage/high voltage (LVD/HVD)
  - o SCSI IDs
  - o Cables and connectors
  - o Active vs. passive termination
- Port expansion cards
  - o USB
  - o IEEE 1394
  - o Serial
  - o Parallel

1.7 Install, update, and configure appropriate firmware.

- Driver/hardware compatibility
- Implications of a failed firmware upgrade (redundant BIOS)
- Follow manufacturer instructions and documentation.

G. 2.0 ADVANCED SOFTWARE

2.1 Install, deploy, configure, and update NOS (Windows/*nix).

- Installation methods (optical media, USB, network share, PXE)
  - o Imaging – system cloning and deployment (Ghost, RIS/WDS, Altiris, virtualization templates)

- Bootloader
- File systems
  - FAT
  - FAT32
  - NTFS
  - VMFS
  - ZFS
  - EXT3
- Driver installation
  - Driver acquisition
  - Installation methods
  - Required media
- Configure NOS
  - Initial network
  - User
  - Device
  - Roles
  - OS environmental settings
  - Applications and tools
- Patch management

2.2 Explain NOS security software and its features.

- Software firewall
  - Port blocking
  - Application exception
  - ACL
- Malware protection software
  - Antivirus
  - Antispyware
- Basics of file level permissions vs. share permissions

2.3 Implement and administer NOS management features based on procedures and guidelines given a scenario.

- User management
  - Adding and removing users
  - Setting permissions
  - Group memberships
  - Policies
  - Logon scripts
- Resource management
  - ACLs
  - Quotas
  - Shadow volumes
  - Disk management
  - Performance monitoring
  - Baselining

- Monitoring (tools and agents)
    - SNMP (MIBs)
    - WBEM (WMI)

2.4 Explain different server roles, their purpose, and how they interact.

- File and print server
- Database server
- Web server
- Messaging server
- DHCP server
- Directory services server
- DNS server
- Application server
    - Update server and proxy server
    - Filtering server
    - Monitoring server
    - Dedicated
    - Distributed
    - Peer to peer
- Remote access server
- Virtualized services
- NTP server
- Explain the difference between a workstation, desktop, and a server.
- Server shut down and start up sequence (one server vs. multiple servers vs. attached components)

2.5 Summarize server virtualization concepts, features, and considerations.

- Resource utilization
- Configuration
- Interconnectivity
- Management server
- Reasons for virtualization
    - Cost benefits
    - Redundancy
    - Green initiative
    - Disaster recovery
    - Testing environment
    - Ease of deployment

2.6 Describe common elements of networking essentials.

- TCP/IP
    - Subnetting
    - DNS
    - DHCP
    - Classes
    - Gateways

- o Static vs. dynamic
- o IP stack
- o Ports
- o Teaming/Link Aggregation

□□Ethernet

- o Types
- o Speeds
- o Cables

□□VPN
□□VLAN
□□DMZ

H. 3.0 ADVANCED STORAGE

3.1 Describe RAID technologies and RAID's features and benefits.
□□Hot spare
□□Software vs. hardware
□□Cache read/write levels (data loss potential)
□□Performance benefits and tradeoffs

3.2 Select the appropriate RAID level given a scenario.
□□0, 1, 3, 5, 6, 10, 50
□□Performance benefits and tradeoffs

3.3 Install and configure different internal storage technologies.
□□Hot swappable vs. non-hot swappable
□□SCSI, Ultra SCSI, Ultra320 (termination), LUNs
□□SAS, SATA
□□Tape
□□Optical

- o DVD
- o DVD-R
- o CD-ROM
- o CD-R
- o CD-RW
- o Blu-Ray

□□Flash
□□Floppy (USB)
□□Controller (firmware levels)
□□Hard drive (firmware, JBOD)

3.4 Summarize the purpose of external storage technologies.
□□Network attached storage
□□Storage area network
□□Tape library
□□WORM

- Optical jukebox
- Transport media
    - o iSCSI
    - o SATA
    - o SAS
    - o SCSI
    - o Fibre Channel

I. 4.0 ADVANCED IT ENVIRONMENT

4.1 Write, utilize, and maintain documentation, diagrams, and procedures.

- Following pre-installation plan when building or upgrading servers
- Labeling
- Diagramming server racks and environment topologies
- Hardware and software upgrade, installation, configuration, server role and repair logs
- Document server baseline (before and after service)
- Original hardware configuration, service tags, asset management, and warranty
- Vendor specific documentation
    - o Reference proper manuals
    - o Web sites
    - o Support channels (list of vendors)

4.2 Explain the purpose of the following industry best practices given a scenario.

- Follow vendor specific server best practices.
    - o Documentation
    - o Tools
    - o Web sites
- Explore ramifications before implementing change; determine organizational impact.
- Communicate with stakeholders before taking action and upon completion of action.
- Comply with all local laws/regulations and industry and corporate regulations.
- Explain purpose of Service Level Agreements (SLAs).
- Follow change control procedures.
- Follow proper equipment disposal procedures.

4.3 Determine an appropriate physical environment for the server location.

- Check for adequate and dedicated power, proper amperage, and voltage.
    - o UPS systems (check load, document service, periodic testing)
    - o UPS specifications (run time, max load, bypass procedures, server communication and shut down, proper monitoring)
- Server cooling considerations – HVAC
    - o Adequate cooling in room
    - o Adequate cooling in server rack
    - o Temperature and humidity monitors

4.4 Implement and configure different methods of server access.

- KVM (local and IP based)
- Direct connect
- Remote management
    - o Remote control
    - o Administration
    - o Software deployment
    - o Dedicated management port

4.5 Classify physical security measures for a server location given a scenario.

- Physical server security
    - o Locked doors
    - o Rack doors
    - o CCTV
    - o Mantraps
    - o Security personnel
- Access control devices (RFID, keypads, pinpads)
    - o Biometric devices (fingerprint scanner, retina)
- Security procedures
    - o Limited access
    - o Access logs
    - o Limited hours
- Defense in-depth – multiple layers of defense
- Reasons for physical security
    - o Theft
    - o Data loss
    - o Hacking
- Secure documentation related to servers
    - o Passwords
    - o System configurations
    - o Logs

J. 5.0 ADVANCED DISASTER RECOVERY

5.1 Compare and contrast backup and restoration methodologies, media types, and concepts.

- Methodologies (full, incremental, differential, selective)
    - o Snapshot
    - o Copy
    - o Bare metal
    - o Open file
    - o Databases
    - o Data vs. OS restore
    - o Rotation and retention (grandfather, father and son)
- Media types
    - o Tape
    - o Disk
    - o WORM

- Optical
- Flash

- Backup security and off-site storage
- Importance of testing the backup and restoration process

5.2 Given a scenario, compare and contrast the different types of replication methods.

- Disk to disk
- Server to server
  - Clustering
  - Active/active
  - Active/passive
- Site to site
- Site types
  - Cold site
  - Hot site
  - Warm site
  - Distance requirements

5.3 Explain data retention and destruction concepts.

- Awareness of potential legal requirements
- Awareness of potential company policy requirements
- Differentiating between archiving and backup

5.4 Carry out the following basic steps of a disaster recovery plan given a scenario.

- Disaster recovery testing process
- Following emergency procedures (people first)
- Using appropriate fire suppressants
- Following escalation procedures for emergencies
- Classification of systems (prioritization during recovery)

K. 6.0 ADVANCED TROUBLESHOOTING

6.1 Explain troubleshooting theory and methodologies.

- Identify the problem and determine the scope.
  - Question users/stakeholders and identify changes to the server/environment.
  - Collect additional documentation/logs.
  - Replicate the problem as appropriate, if possible.
  - Perform backups before making changes, if possible.
- Establish a theory of probable cause (question the obvious).
  - Determine whether or not there is a common element or symptom causing multiple problems.
- Test the theory to determine cause.
  - Once theory is confirmed, determine next steps to resolve problem.
  - Re-establish new theory or escalate if theory is not confirmed.
- Establish a plan of action to resolve the problem and notify impacted users.
- Implement the solution or escalate as appropriate.

- Make one change at a time and test/confirm whether or not the change has resolved the problem.
- Reverse the change, if appropriate, and implement new change if the problem is not resolved.

- Verify full system functionality and, if applicable, implement preventative measures.
- Perform a root cause analysis.
- Document findings, actions, and outcomes throughout the process.

6.2 Effectively troubleshoot hardware problems, selecting the appropriate tools and methods, given a scenario.

- Common problems
  - Failed POST
  - Overheating
  - Memory failure
  - Onboard component failure
  - Processor failure
  - Incorrect boot sequence
  - Expansion card failure
  - Operating system not found
  - Drive failure
  - Power supply failure
  - I/O failure
- Causes of common problems
  - Third party components or incompatible components
  - Incompatible or incorrect BIOS
  - Cooling failure
  - Mismatched components
  - Backplane failure
- Environmental issues
  - Dust
  - Humidity
  - Temperature
  - Power surge/failure
- Hardware tools
  - Power supply tester (multimeter)
  - System board tester
  - Compressed air
  - ESD equipment

6.3 Troubleshoot software problems effectively, selecting the appropriate tools and methods, given a scenario.

- Common problems
  - User unable to logon
  - User cannot access resources
  - Memory leak
  - BSOD/stop

- o OS boot failure
- o Driver issues
- o Runaway process
- o Cannot mount drive
- o Cannot write to system log
- o Slow OS performance
- o Patch update failure
- o Service failure
- o Hangs; no shut down
- o Users cannot print

- Cause of common problems
  - o Malware
  - o Unauthorized software
  - o Software firewall
  - o User Account Control (UAC/SUDO)
  - o Improper permissions
  - o Corrupted files
  - o Lack of hard drive space
  - o Lack of system resources
  - o Virtual memory (misconfigured, corrupt)
  - o Fragmentation
  - o Encryption
  - o Print server drivers/services
  - o Print spooler
- Software tools
  - o System logs
  - o Monitoring tools (resource monitor, performance monitor)
  - o Defragmentation tools

6.4 Diagnose network problems effectively, selecting the appropriate tools and methods, given a scenario.

- Common problems
  - o Internet connectivity failure
  - o Email failure
  - o Resource unavailable
  - o DHCP server mis-configured
  - o Non-functional or unreachable
  - o Destination host unreachable
  - o Unknown host
  - o Default gateway mis-configured
  - o Failure of service provider
  - o Can reach by IP; not by host name
- Causes of common problems
  - o Improper IP configuration
  - o VLAN configuration
  - o Port security

- o Improper subnetting
- o Component failure
- o Incorrect OS route tables
- o Bad cables
- o Firewall (mis-configuration, hardware failure, software failure)
- o Mis-configured NIC, routing/switch issues
- o DNS and/or DHCP failure
- o Mis-configured hosts file

□□Networking tools

- o ping
- o tracert/traceroute
- o ipconfig/ifconfig
- o nslookup
- o net use/mount
- o route
- o nbtstat
- o netstat

6.5 Troubleshoot storage problems effectively, selecting the appropriate tools and methods, given a scenario.

□□Common problems

- o Slow file access
- o OS not found
- o Data not available
- o Unsuccessful backup
- o Error lights
- o Unable to mount the device
- o Drive not available
- o Cannot access logical drive
- o Data corruption
- o Slow I/O performance
- o Restore failure
- o Cache failure
- o Multiple drive failure

□□Causes of common problems

- o Media failure
- o Drive failure
- o Controller failure
- o HBA failure
- o Loose connectors
- o Cable problems
- o Mis-configuration
- o Improper termination
- o Corrupt boot sector
- o Corrupt file system table
- o Array rebuild

- Improper disk partition
- Bad sectors
- Cache battery failure
- Cache turned off
- Insufficient space
- Improper RAID configuration
- Mis-matched drives
- Backplane failure

- Storage tools
  - Partitioning tools
  - Disk management
  - RAID array management
  - Array management
  - System logs
  - Net use/mount command
  - Monitoring tools