Florida Department of Education
Curriculum Framework

Program Title: **Network Systems Technology**
Career Cluster: **Information Technology**

AS	
CIP Number	1511100112
Program Type	College Credit
Standard Length	60 credit hours
CTSO	Phi Beta Lambda, BPA
SOC Codes (all applicable)	15-1122 – Information Security Analysts 15-1142 – Network and Computer Systems Administrators 15-1152 – Computer Network Support Specialists
CTE Program Resources	http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml

Purpose

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and careers such as cabling specialists, network control operators, data communications analysts, network technicians, computer security specialists, network specialists, network managers, network systems analysts, network systems technicians, network troubleshooters, WAN/LAN managers, or systems administrators in the Information Technology career cluster; provides technical skill proficiency, and includes competency-based applied learning that contributes to the academic knowledge, higher-order reasoning and problem-solving skills, work attitudes, general employability skills, technical skills, and occupation-specific skills, and knowledge of all aspects of the Information Technology career cluster.

The content includes but is not limited to planning, installing, configuring, monitoring, troubleshooting, and managing computer networks in a LAN/WAN environment. Students will be prepared to apply conceptual, theoretical and practical knowledge to the workplace utilizing technical skills learned during the program.

Additional Information relevant to this Career and Technical Education (CTE) program is provided at the end of this document.

Program Structure

This program is a planned sequence of instruction consisting of core standards and eight different tracts to permit students to specialize in network administration, network infrastructure, network virtualization, network security/cybersecurity, IP communications, digital forensics, advanced network infrastructure. Or Linux system administrator. Standards comprising each specialization area are completed in addition to the core standards. Due to the foundational nature of the core, it is recommended that students complete the core, or demonstrate a mastery of the student performance

standards contained in the core, before advancing to courses comprising a specialization tract. Standards in the core prepare students with requisite foundational knowledge and skills related to computer maintenance and support, networking fundamentals, operating systems, network security, technical communications, and project management. The total Associate in Science degree program consists of 60 credit hours.

In addition, students will complete the standards in one of the following specializations:

Standards

After successfully completing this program, the student will be able to perform the following:

01.0 Demonstrate proficiency in basic computer maintenance and support.
02.0 Demonstrate a fundamental understanding of computer networking.
03.0 Demonstrate an understanding of common operating system concepts and associated practices.
04.0 Demonstrate fundamental proficiency in network security essentials.
05.0 Demonstrate proficiency in technical communications and workplace protocols.
06.0 Demonstrate a basic understanding of project management concepts and processes.
07.0 Demonstrate workplace-readiness skills.

In addition, students will complete the standards in one of the following specializations:

Network Administration Specialization Standards

08.0 Demonstrate an understanding of the directory services infrastructure and installation.
09.0 Demonstrate an understanding of organizational units and related objects.
10.0 Demonstrate an understanding of group policy.
11.0 Demonstrate an understanding of implementing sites to manage Active Directory replication.
12.0 Demonstrate an understanding of maintaining Active Directory services availability.
13.0 Demonstrate how to install and deploy a server operating system.
14.0 Demonstrate how to provide infrastructure services
15.0 Demonstrate how to provide file and print services.
16.0 Demonstrate how to provide remote and wireless network access.
17.0 Demonstrate how to monitor and maintain network servers and services.
18.0 Demonstrate an understanding of securing data transmission and authentication.
19.0 Demonstrate an understanding of planning for business continuity and high availability.

Network Infrastructure Specialization Standards

08.0 Demonstrate understanding of routing concepts.
09.0 Demonstrate understanding of routing protocols.
10.0 Demonstrate router configuration skills.
11.0 Demonstrate an understanding of LAN design and concepts.
12.0 Demonstrate VLAN configuration skills.
13.0 Demonstrate an understanding of wide area networks (WAN).
14.0 Demonstrate WAN configuration skills.
15.0 Demonstrate an understanding of network security.
16.0 Demonstrate an understanding of remote access.

17.0 Demonstrate an understanding of IP addressing services.
18.0 Demonstrate an understanding of network maintenance, support and troubleshooting.

Network Security/Cybersecurity Specialization Standards

08.0 Demonstrate proficiency in securing network infrastructures and protecting data.
09.0 Demonstrate proficiency in performing security penetration testing.
10.0 Demonstrate proficiency in responding to security incidents.

Network Virtualization Specialization Standards

08.0 Demonstrate an understanding of virtualization concepts.
09.0 Install and configure the virtualization server platform.
10.0 Install, configure and manage virtualized clients.
11.0 Install, configure, and maintain a virtualized application.
12.0 Demonstrate proficiency in managing a virtualization infrastructure.
13.0 Demonstrate proficiency in securing a virtualization infrastructure.

Digital Forensics Specialization Standards

08.0 Demonstrate proficiency in basic and advanced security concepts.
09.0 Demonstrate proficiency in managing hardware involved in imaging and data collection activities.
10.0 Demonstrate proficiency in analyzing common file systems.
11.0 Demonstrate proficiency in performing computer forensics investigations.
12.0 Demonstrate proficiency in performing mobile device forensics.
13.0 Demonstrate proficiency in incident handling and response.
14.0 Identify key pieces of legislation and processes related to digital forensics.
15.0 Demonstrate an understanding of the tasks related to the casework process.

IP Communications Specialization Standards

08.0 Demonstrate an understanding of IP communication theory.
09.0 Demonstrate an understanding of digitizing voice traffic and voice compression standards.
10.0 Demonstrate an understanding of quality of service (QoS) requirements in a converged data and voice network.
11.0 Demonstrate an understanding of IP communications design.
12.0 Demonstrate an understanding of troubleshooting procedures for IP communications.
13.0 Demonstrate an understanding of utilizing advanced Voice over IP (VoIP) and data bundle solutions to provide a single network connection for phone services and high-speed Internet.
14.0 Demonstrate an understanding of using Statistical Analysis System (SAS) sessions to exchange data by using the TCP/IP communications access method.
15.0 Demonstrate how to configure VoIP fax applications for universal access servers.
16.0 Demonstrate an understanding of key concepts for Video over IP.

Advanced Network Infrastructure Specialization Standards

08.0 Demonstrate an understanding of routing concepts.
09.0 Demonstrate an understanding of routing protocols.
10.0 Demonstrate router configuration skills.
11.0 Demonstrate an understanding of LAN design and concepts.
12.0 Demonstrate VLAN configuration skills.
13.0 Demonstrate an understanding of network maintenance, support and troubleshooting.

Linux System Administrator Specialization Standards

08.0 Understand and use essential tools.
09.0 Operate running systems.
10.0 Configure local storage.
11.0 Create and configure file systems.
12.0 Deploy, configure, and maintain systems.
13.0 Manage users and groups.
14.0 Manage security.

Florida Department of Education
Student Performance Standards

Program Title: Network Systems Technology
CIP Number: 1511100112
Program Length: 60 credit hours
SOC Code(s): 15-1122, 15-1142, 15-1152

Refer to Rule 6A-14.030 (4) F.A.C., for the minimum amount of general education coursework required in the Associate of Science (AS) degree. At the completion of this program, the student will be able to:	
01.0	Demonstrate proficiency in basic computer maintenance and support. The student will be able to:
01.01	Describe the main computer components and their functions.
01.02	Describe the operation of computer systems, including input and output systems, file systems, device management, program loading and execution and data storage.
01.03	Describe and identify the safe and ethical use of computers.
01.04	Describe and identify proficiency in connecting to and safely using the Internet.
01.05	Describe emerging computer technologies and discuss their potential impact.
01.06	Implement proper procedures for handling and safeguarding equipment.
01.07	Describe procedures for proper disposal of computer components.
01.08	Install, configure, maintain and secure computer systems and peripherals following institutional protocol.
01.09	Configure and update firmware and ROM-BIOS.
01.10	Implement work order procedures.
01.11	Design and implement systems redundancy and data backups.
01.12	Describe effective troubleshooting strategies and techniques to resolve basic hardware, software, and network problems.
01.13	List the steps in problem solving.
01.14	Recognize and resolve basic computer configuration problems.
01.15	Examine and identify the parts of the Windows Registry.
02.0	Demonstrate a fundamental understanding of computer networking. The student will be able to:

02.01	Explain the use of binary numbers and perform related binary and hexadecimal arithmetic.
02.02	Describe current network environments.
02.03	Describe network communications and architecture.
02.04	Identify network components, media, connectors, applications and protocols.
02.05	Compare and contrast the OSI and TCP/IP reference models and their layers.
02.06	Identify and describe current relevant IEEE network standards.
02.07	Create an IP addressing scheme using Variable Length Subnet Masks (VLSM) and Classless Inter-Domain Routing (CIDR).
02.08	Identify and discuss issues related to networked environments, such as security, access control, fair use, privacy and redundancy.
02.09	Identify and discuss issues related to naming conventions for user IDs, email, passwords, and network hosts and devices.
02.10	Identify standard network topologies and describe the advantages and disadvantages of each topology.
02.11	Describe the major functions of LAN protocols.
02.12	Explain the functions of wireless components, standards, hardware, software, and infrastructure design.
02.13	Configure and manage the TCP/IP protocol stack.
02.14	Describe how TCP and UDP Port addresses, IP addresses, and MAC addresses function, and how they are used to deliver data across the network.
02.15	Identify emerging technologies and discuss related technical issues.
02.16	Design a local area network (LAN), including the specification of architecture, hardware and software.
02.17	Identify the advantages and use of virtual local area networks (VLANs).
02.18	Identify and explain wide area network (WAN) concepts.
02.19	Plan, configure and test a small network and establish baselines.
02.20	Describe the major functions of network server software components.
02.21	Install applications on a server and configure clients for network access.
03.0	Demonstrate an understanding of common operating system concepts and associated practices. The student will be able to:

03.01	Describe the components and functions of major operating systems.
03.02	Compare and contrast major functions and features of current network operating systems (including directory services).
03.03	Install, configure and update client and server operating systems.
03.04	Describe the purpose and uses of computer virtualization.
03.05	Manage device drivers and software for peripheral devices.
03.06	Manage the network and firewall settings of a client.
03.07	Use an operating system for activities such as data and file management.
03.08	Identify current systems utilities and describe their functions.
03.09	Use system software to perform routine maintenance tasks such as backup and hard drive defragmentation.
03.10	Create, use, maintain, backup and restore system configuration files.
03.11	Describe procedures for uninstalling operating system software.
03.12	Install and configure client software for connecting to LANs, WANs, and the Internet.
03.13	Demonstrate knowledge of basic troubleshooting methodology.
04.0	Demonstrate fundamental proficiency in network security essentials. The student will be able to:
04.01	Describe common security threats to, and vulnerabilities of, computer systems and the corresponding best practices for mitigation.
04.02	Define and describe malicious software and techniques to protect systems from its effects.
04.03	Describe Denial of Service attacks and means to defend against them.
04.04	Identify the risks and techniques of data loss and its prevention.
04.05	Describe the principles and techniques of securing data storage and transmission.
04.06	Identify current encryption and authentication standards.
04.07	Describe security policies, including compliance and operational security.
04.08	Configure access control, identity management and security logging.
04.09	Describe client and network system security software and related updates.

04.10	Describe the functions and characteristics of firewalls.
04.11	Perform a ping sweep to identify network hosts.
04.12	Perform a port scan to probe network hosts for open TCP and UDP ports.
04.13	Describe the purpose and operation of network protocol analyzers.
04.14	Utilize a network protocol analyzer to capture and analyze network traffic for security issues.
05.0	Demonstrate proficiency in technical communications and workplace protocols. The student will be able to:
05.01	Identify issues in the communication of technical information to a non-technical audience.
05.02	Create, utilize, and maintain system documentation.
05.03	Utilize online resources to locate and evaluate technical information and documentation.
05.04	Identify and discuss issues contained within professional codes of conduct.
05.05	Prepare and deliver a technical presentation.
05.06	Create and interpret technical and business communications.
05.07	Demonstrate the basic principles of teamwork and the techniques for being a productive and effective contributing member of a team.
05.08	Identify and describe acceptable strategies for resolving conflicts in the workplace.
05.09	Deliver and follow oral and written technical instructions.
05.10	Describe the roles of the network specialist in a business enterprise.
05.11	Document problems and solutions in service reports and maintain proper documentation.
05.12	Perform research on technical issues using Internet and database resources.
06.0	Demonstrate a basic understanding of project management concepts and processes. The student will be able to:
06.01	Examine the organization, planning, and controlling of projects.
06.02	Define Project Integration Management.
06.03	Describe project phases, process groups, and the full project life cycle.
06.04	Choose appropriate actions in situations that require effective time management. Understand the basic tools and techniques to plan, organize, and manage a project.

	06.05 Describe a project life cycle from initiation to planning through execution, acceptance, support, quality, budgeting, and closure.
	06.06 Explain the factors contributing to risk management planning.
	06.07 Explain the project environment including: cultural, social, international, political and physical.
	06.08 Describe the principles of identifying, developing, and managing resources.
	06.09 Plan and monitor a project budget and schedule using project management tools.
	06.10 Explain the technical and human aspects of project control, especially change control.
	06.11 Describe the basic tools and techniques of managing project quality and risk.
	06.12 Explain the contextual relationship between the project and the organization that hosts the project.
	06.13 Demonstrate an understanding of the importance of working in teams, managing team members, and interacting with stakeholders.
	06.14 Explain the importance of ethical considerations in every aspect of a project's operation.
07.0	Demonstrate workplace-readiness skills. The student will be able to:
	07.01 Explain the value of proper communication in the classroom and workplace environment.
	07.02 Participate in group discussions as a member and as a leader.
	07.03 Explain the importance of self-motivation and responsibility in completing assigned tasks.
	07.04 Choose appropriate actions in situations requiring effective time management.
	07.05 Apply principles and techniques for being a productive, contributing member of a team.
	07.06 Discuss the ethical aspects of intellectual property rights and licensing issues.
	07.07 Identify and discuss issues contained within professional codes of conduct.
	07.08 Describe appropriate communication skills, courtesy, manners, and dress in the workplace.

Network Administration Specialization Standards	
08.0	Demonstrate an understanding of the directory services infrastructure and installation. The student will be able to:
08.01	Describe the architecture of Active Directory.
08.02	Discuss how Active Directory works.
08.03	Describe the Active Directory design, plan, and implementation processes.
08.04	Create a forest and domain structure.
08.05	Configure the Domain Name Service (DNS) in an Active Directory environment.
08.06	Raise the functional level of a forest and a domain.
08.07	Create trust relationships between domains.
08.08	Create, manage, and delegate administrative control for organizational units.
09.0	Demonstrate an understanding of organizational units and related objects. The student will be able to:
09.01	Discuss user, group, and computer accounts.
09.02	Create and manage multiple accounts.
09.03	Implement user principal name suffixes.
09.04	Move objects in Active Directory.
09.05	Plan an account strategy.
09.06	Plan an Active Directory audit strategy.
10.0	Demonstrate an understanding of group policy. The student will be able to:
10.01	Create and configure group policy objects (GPOs).
10.02	Configure group policy refresh rates and group policy settings.
10.03	Manage GPOs.
10.04	Verify and troubleshoot group policy.
10.05	Delegate administrative control of group policy.

	10.06 Plan a group policy strategy for the enterprise.
	10.07 Configure, deploy and maintain applications using group policy.
	10.08 Monitor and maintain security policies.
	10.09 Prepare and implement group policy strategy and backup/recovery of group policy objects.
11.0	Demonstrate an understanding of implementing sites to manage Active Directory replication. The student will be able to:
	11.01 Discuss directory services replication.
	11.02 Design and document site topology.
	11.03 Manage site topology.
	11.04 Troubleshoot replication failures.
	11.05 Plan, create and configure a site.
	11.06 Implement the global catalog in Active Directory.
	11.07 Plan and determine the placement and type of domain controllers in Active Directory.
	11.08 Identify the various Operations Master Roles and Global Catalog.
	11.09 Plan the placement of Operations Masters and Global Catalog.
	11.10 Transfer and seize Operations Master Roles.
12.0	Demonstrate an understanding of maintaining Active Directory services availability. The student will be able to:
	12.01 Create an Active Directory implementation plan for a business enterprise.
	12.02 Implement the Active Directory infrastructure for a business enterprise.
	12.03 Describe the maintenance of the Active Directory.
	12.04 Move and defragment an Active Directory database.
	12.05 Backup and restore an Active Directory.
	12.06 Monitor an Active Directory.

13.0	Demonstrate how to install and deploy a server operating system. The student will be able to:
13.01	Identify server operating system (OS) versions, editions, features and capabilities.
13.02	Assess server installation readiness by inventorying hardware.
13.03	Describe the methods, options and requirements for a Windows server installation and upgrade.
13.04	Perform an attended and an unattended OS installation.
13.05	Configure basic network settings.
13.06	Configure storage.
13.07	Configure operating systems licensing.
13.08	Describe, identify and choose server roles and role services.
13.09	Perform a system review and troubleshoot installation issues.
13.10	Discuss the system installation.
13.11	Automate server deployments using unattended installation tools and Windows.
13.12	Implement deployment services.
14.0	Demonstrate how to provide infrastructure services. The student will be able to:
14.01	Describe the purpose and function of Dynamic Host Configuration Protocol (DHCP).
14.02	Install, configure, and authorize the DHCP server role.
14.03	Manage, backup and restore the DHCP Database.
14.04	Configure the DHCP Relay Agent.
14.05	Describe the DNS name resolution process.
14.06	Configure DNS zones, records and replication.
14.07	Integrate DNS servers with Active Directory.
14.08	Configure name resolution for client computers.

15.0	Demonstrate how to provide file and print services. The student will be able to:
15.01	Design a file sharing strategy.
15.02	Install the file and print server roles and services.
15.03	Manage file sharing security, encryption, redundancy, and offline access.
15.04	Manage disk quotas, file screening and shadow copy services.
15.05	Backup and restore files.
15.06	Configure Distributed File System (DFS) roots, targets and replication.
15.07	Identify and install print drivers.
15.08	Manage printer security, priorities, schedules and pools.
15.09	Publish printers and file shares to Active Directory.
15.10	Monitor and troubleshoot print and file services.
16.0	Demonstrate how to provide remote and wireless network access. The student will be able to:
16.01	Compare and contrast remote access protocols, wireless standards and network authentication methods.
16.02	Configure static and dynamic routing, Network Address Translation (NAT).
16.03	Configure remote access services, protocols and policies, conditions and settings.
16.04	Configure Remote Access Dial-In User Service (RADIUS).
17.0	Demonstrate how to monitor and maintain network servers and services. The student will be able to:
17.01	Monitor and compare network and server performance data to establish and document baselines, isolate problems and optimize performance, adaptability, and scalability.
17.02	Optimize traffic flow conditions on network connections based on analysis of traffic types, characteristics and user needs.
17.03	Monitor event logs for information, errors and warnings.
17.04	Maintain system documentation and service histories.
17.05	Configure server and client settings to implement patch management strategy.
17.06	Develop strategies for remote server management using command-line and GUI tools.

18.0	Demonstrate an understanding of securing data transmission and authentication. The student will be able to:
	18.01 Explain the social, ethical and technical issues regarding data integrity and confidentiality.
	18.02 Secure network traffic using IPSec.
	18.03 Configure network authentication.
	18.04 Install, configure and manage certificate services.
	18.05 Describe and deploy a network access protection strategy.
	18.06 Configure firewall settings.
	18.07 Identify ports and protocols and create filters for incoming and outgoing traffic.
19.0	Demonstrate an understanding of planning for business continuity and high availability. The student will be able to:
	19.01 Discuss virtualization architectures.
	19.02 Estimate data storage requirements.
	19.03 Select a storage technology.
	19.04 Plan for storage fault tolerance.
	19.05 Develop strategies to ensure application and service availability.
	19.06 Plan for backup and recovery of data, servers, and directory services.

Network Infrastructure Specialization Standards	
08.0	Demonstrate an understanding of routing concepts. The student will be able to:
08.01	Describe the purpose, architecture, and operations of a router.
08.02	Identify the hardware and software components of routers.
08.03	Explain the purpose and nature of routing tables.
08.04	Describe administrative distance and routing metrics such as hop counts and cost.
08.05	Describe how a router determines a path and switches packets.
08.06	Differentiate between static and dynamic routing.
08.07	Explain the differences between class-full and classless routing.
08.08	Describe the use and operation of VLSM and CIDR.
08.09	Describe how a network converges.
09.0	Demonstrate an understanding of routing protocols. The student will be able to:
09.01	Describe the characteristics of distance vector routing protocols.
09.02	Describe the characteristics of link state routing protocols.
09.03	Describe the differences between distance vector and link state routing protocols and determine the best routing protocol to use in a given situation.
09.04	Describe the features and operation of current internal and external routing protocols.
10.0	Demonstrate router configuration skills. The student will be able to:
10.01	Configure and verify router interfaces.
10.02	Perform basic router configuration using the Command Line Interface (CLI) to inspect the operations of the router.
10.03	Design and implement a classless IP addressing scheme for a network.
10.04	Configure a router for RIP version 2 operation.
10.05	Use advanced configuration commands with routers.
10.06	Configure a router for OSPF routing in a network.

	10.07 Fine-tune OSPF settings on a router, including the configuration of reference bandwidth, redistribution of static and default routes, and modification of OSPF intervals, in order to optimize network performance.
	10.08 Verify and troubleshoot router operations in an OSPF network.
	10.09 Configure and modify metric on a router to improve network performance.
	10.10 Configure summarization and default route settings on a router to optimize network performance.
	10.11 Verify and troubleshoot router operations in complex network environment.
11.0	Demonstrate an understanding of LAN design and concepts. The student will be able to:
	11.01 Identify the layers and functions of switched network architecture.
	11.02 Describe the principles and benefits of a hierarchical network design.
	11.03 Explain the technology and media access control method for Ethernet networks.
	11.04 Describe the issues associated with Layer 2.
	11.05 Describe the operation of a LAN switch.
	11.06 Describe the benefits of Virtual Local Area Networks (VLAN).
	11.07 Identify and describe the different VLAN encapsulation protocols and their operation.
	11.08 Describe the purpose and operation of VLAN Trunking Protocol (VTP) in the management of a switched network domain.
	11.09 Describe the purpose and operation of Spanning Tree Protocol (STP), and its variants.
	11.10 Describe the use of Inter-VLAN routing to connect different Networks in a switch-based network topology.
	11.11 Analyze business requirements and design a LAN structure to meet those requirements.
	11.12 Discuss quality-of-service considerations and switching prioritization.
12.0	Demonstrate VLAN configuration skills. The student will be able to:
	12.01 Perform and verify initial LAN switch configuration tasks including remote access management, switch port modes, and trunks.
	12.02 Configure, verify, and troubleshoot VLANs on a LAN switch.
	12.03 Implement a VLAN Domain by configuring LAN switches for VTP network operation.
	12.04 Configure a router to provide Inter-VLAN routing using multiple physical interfaces, and on a single physical interface with sub-interfaces.

	12.05 Configure and troubleshoot STP and its variants on a switched network environment.
	12.06 Configure and verify the bridge to optimize STP.
	12.07 Establish and configure port priorities.
	12.08 Troubleshoot and resolve issues with STP operations.
	12.09 Manage router and switch OS software.
13.0	Demonstrate an understanding of wide area networks (WAN). The student will be able to:
	13.01 Describe WAN and MAN topologies.
	13.02 Differentiate between WAN and LAN topologies.
	13.03 Identify and describe WAN protocols.
	13.04 Describe the impact of applications (Voice Over IP, Video Over IP) on a network.
	13.05 Identify major network issues associated with the Internet, intranets and extranets.
	13.06 Explain the differences between the use of leased lines, packet-switched, and circuit-switched technologies.
	13.07 Describe typical WAN links and discuss bandwidth considerations.
	13.08 Identify and manage licensing.
14.0	Demonstrate WAN configuration skills. The student will be able to:
	14.01 Configure and verify Point-to-Point WAN connection.
	14.02 Configure and verify a packet switched WAN connection.
	14.03 Configure and verify a basic WAN serial connection and a PPP connection between routers.
	14.04 Configure and verify a PPP connection between routers.
	14.05 Troubleshoot WAN implementation issue.
	14.06 Implement LAN/WAN connections, including virtual private networks (VPN), and tunneling.

15.0	Demonstrate an understanding of network security. The student will be able to:
15.01	Implement basic switch security measures such as port security, trunk access, and management VLANs.
15.02	Identify current network security threats and explaining how to implement a comprehensive security policy to mitigate common threats to network devices, hosts, and applications.
15.03	Describe the functions of common security appliances and applications.
15.04	Implement recommended security practices to secure network devices.
15.05	Discuss the functions of authentication servers.
15.06	Describe the function and use of Access Control Lists (ACLs).
15.07	Verify, monitor, and troubleshoot ACLs in a network environment.
16.0	Demonstrate an understanding of remote access. The student will be able to:
16.01	Compare and contrast remote access protocols, wireless standards and network authentication methods.
16.02	Configure static and dynamic routing and Network Address Translation (NAT).
16.03	Configure remote access services, protocols and policies, conditions and settings.
16.04	Describe Remote Access Dial-In User Service (RADIUS).
16.05	Monitor and troubleshoot remote access.
17.0	Demonstrate an understanding of IP addressing services. The student will be able to:
17.01	Describe the purpose and operation of DHCP and DNS in a networked environment.
17.02	Configure, verify, and troubleshoot DHCP and DNS operation on a router.
17.03	Describe the operation and use of NAT and Port Address Translation (PAT) to provide Internet access to Private IP Address networks.
17.04	Configure, verify, and troubleshoot NAT on a router, including static translation, use of IP Address pools, and sharing a public IP address on a router interface.
17.05	Describe the purpose and operation of IPv6.
17.06	Configure, verify, and troubleshoot IPv6 routing in a network.

18.0	Demonstrate an understanding of network maintenance, support and troubleshooting. The student will be able to:
18.01	Identify, interpret and maintain network documentation, procedures and practices.
18.02	Describe effective troubleshooting strategies and techniques to resolve basic hardware, software, and network problems.
18.03	Follow standard operating procedures for troubleshooting hardware and software.
18.04	Manage, maintain and backup router and switch system and configuration files.
18.05	Recognize and resolve hardware and software configuration problems.
18.06	Identify and resolve common network problems at Layers 1, 2, 3, and 7 using a layered model approach. Describe the use and features of diagnostic test equipment.
18.07	Determine type of programs and procedures required to: baseline network performance, identify intrusion and unacceptable system use, identify performance issues, predict system failures, and optimize network availability.
18.08	Use network monitoring and management tools effectively to integrate and manage network resources.
18.09	Explain SNMP and its use in monitoring a network.
18.10	Configure network devices to send SNMP traps or alerts to network management systems.
18.11	Establish and document a network baseline.
18.12	Compare and analyze initial performance measurements with the availability of critical network devices and connections to determine the difference between abnormal behavior and proper network performance as the network grows or traffic patterns change.
18.13	Describe optimization of traffic flow conditions on network connections based on analysis of traffic types, characteristics and user needs.

Network Security/Cybersecurity Specialization Standards	
08.0	Demonstrate proficiency in securing network infrastructures and protecting data. The student will be able to:
08.01	Explain the major categories of computer crimes and attacks.
08.02	Identify vulnerabilities inherent in network devices, protocols and services.
08.03	Develop institutional security policies and practices in compliance with relevant governmental standards and regulations.
08.04	Implement protective measures in securing critical information assets.
08.05	Deploy various network security related equipment including, firewalls, intrusion prevention systems, and proxies.
08.06	Secure critical network services such as Directory Services, Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and File Transfer Protocol (FTP).
08.07	Secure desktop client operating systems against viruses, malware and other malicious attacks.
08.08	Detect malicious and abnormal activities through logs, intrusion detection systems and other utilities and appliances.
09.0	Demonstrate proficiency in performing security penetration testing. The student will be able to:
09.01	Identify organizational compliance with regulatory and legislative Information Assurance (IA) requirements.
09.02	Identify physical and logical weaknesses in computers and networks as well as physical weaknesses and weaknesses in policies, procedures and practices relating to the network and the organization.
09.03	Test the network perimeter defense mechanisms to ensure boundaries.
09.04	Simulate methods that intruders use to gain unauthorized access to an organization's networked systems and attempted to compromise them.
09.05	Deploy proprietary and/or open source tools to test known technical vulnerabilities in networked systems.
09.06	Determine which vulnerabilities are exploitable and the degree of information exposure or network control that the organization could expect an attacker to achieve after successfully exploiting vulnerability.
09.07	Recommend procedures to mitigate against discovered vulnerabilities and security gaps.
09.08	Prepare penetration testing deliverables including reports, documentations.
09.09	Describe the ethics of a licensed Penetration Tester.
10.0	Demonstrate proficiency in responding to security incidents. The student will be able to:
10.01	Explain contingency planning and its components.
10.02	Collect data from logs and other resources to aid in detecting security incidents.
10.03	Assemble an incident response plan.
10.04	Recover from incidents by restoring services and processes.
10.05	Manage evidentiary data in an electronic environment.

Network Virtualization Specialization Standards	
08.0	Demonstrate an understanding of virtualization concepts. The student will be able to:
08.01	Describe the purpose, uses and software features of computer virtualization.
08.02	Identify and describe virtualization products, applications and services.
08.03	Identify compatibility issues among hardware and software products.
08.04	Identify the elements necessary for a Virtual Desktop Infrastructure.
08.05	Explain the benefits and considerations for virtual storage, including local host disk, iSCSI SAN, Fibre Channel SAN, and NFS SAN.
08.06	Explain storage architectures, including storage subsystems, DAS, SAN, NAS, and CAS.
08.07	Describe backup, recovery, disaster recovery, business continuity, and replication concepts.
08.08	Describe the policies and profile management which restrict and allow features.
08.09	Identify and modify desktop catalogs, groups, and a master virtual machine.
09.0	Install and configure the virtualization server platform. The student will be able to:
09.01	Install and configure the virtualization platform.
09.02	Install and configure the virtualization environment to create a new farm or join an existing farm.
09.03	Automate virtual machine and cluster deployment.
09.04	Monitor and maintain license usage requirements and trends.
09.05	Manage virtualization networking and storage.
09.06	Manage user sessions from the administrative console.
09.07	Configure network connectivity and storage for the virtualization software.
10.0	Install, configure and manage virtualized clients. The student will be able to:
10.01	Identify requirements for virtual machines according to task.
10.02	Configure the virtual environment and the virtual machine properties.
10.03	Install, configure and manage a virtual machine desktop client and a virtualized server.

	10.04 Manually deploy and migrate virtual machines.
	10.05 Configure and assign users to pooled virtual desktops and dedicated virtual desktops.
	10.06 Convert physical machines to virtual machines.
	10.07 Configure desktop resources for access by users.
	10.08 Configure and monitor back up virtual machine data to shared storage.
	10.09 Migrate, convert, and monitor virtual machines.
	10.10 Create and update shared disks.
11.0	Install, configure, and maintain a virtualized application. The student will be able to:
	11.01 Install and configure a virtualized application.
	11.02 Configure virtualization applications to use a proxy.
	11.03 Configure virtualized application resources for access by users.
	11.04 Install and use profiling software on a virtualized application for streaming, and linking dependent profiles to allow interaction between streamed applications.
	11.05 Monitor virtualization applications and implementing policies.
	11.06 Migrate, convert, and monitor virtual appliances.
	11.07 Test policies to verify the achievement of the desired effect.
	11.08 Configure and deliver a plug-in package, and verifying that self-service applications can be added from a client device.
	11.09 Install and configure provisioning services.
	11.10 Optimize a provisioning services server.
	11.11 Describe end user optimization techniques.
12.0	Demonstrate proficiency in managing a virtualization infrastructure. The student will be able to:
	12.01 Manage user access to virtualized applications and machines in the virtualization infrastructure.
	12.02 Manage the infrastructure to provide high availability and data access.
	12.03 Describe administration of the virtualization environment.

12.04	Describe tools that can be used to monitor virtualization application servers and sessions.
12.05	Manage and maintain network infrastructure and storage resources.
12.06	Create and apply worker groups.
12.07	Configure and optimize load management.
12.08	Configure a resource pool for optimal performance.
12.09	Troubleshoot infrastructure problems and virtual environment issues.
12.10	Resolve application compatibility issues.
13.0	Demonstrate proficiency in securing a virtualization infrastructure. The student will be able to:
13.01	Describe the securing and maintenance of a virtualization solution.
13.02	Restrict and protect administrator access to the virtualization solution.
13.03	Ensure that the hypervisor is properly secured.
13.04	Create a plan for the security for a virtualization solution before installing, configuring and deploying it.
13.05	Secure elements of a virtualization solution and maintain their security.

Digital Forensics Specialization Standards	
08.0	Demonstrate proficiency in basic and advanced security concepts. The student will be able to:
08.01	Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.
08.02	Describe the basic categories of vulnerabilities associated with cybersecurity (i.e., hardware, software, network, human, physical, organizational).
08.03	Describe the role of digital certificates and their role in IT security.
08.04	Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
08.05	Describe the use of firewalls and other means of intrusion prevention.
08.06	Describe security design principles and their role in limiting points of vulnerability.
08.07	Discuss authentication methods and strategies.
08.08	Describe the processes involved in hardening a computer system or network.
08.09	Compare and contrast the forms, limitations, and vulnerabilities associated with centralized and decentralized key management schemas, including the PKI web of trust model.
08.10	Evaluate an existing security posture and identify gaps and vulnerabilities in security.
08.11	Describe the types of penetration tests (i.e., human, physical, wireless, data networks, telecommunications), the goals of each type, the metrics tested, and the value of their results.
08.12	Compare and contrast the processes of black box versus white box penetration testing, including their characteristics, limitations, and appropriateness.
08.13	Describe common testing methodologies and standards used in penetration testing.
08.14	Demonstrate proficiency in basic forensic concepts.
08.15	Describe the range of testing/evaluation and associated tools used to monitor mitigation control effectiveness.
08.16	Create a risk management framework.
08.17	Describe the purpose and scope of an Information Systems Contingency Plan (ISCP).
08.18	Identify the five main components of a contingency plan (i.e., Supporting Information, Activation and Notification, Recovery, Reconstitution, and Appendices).
08.19	Describe the purpose and scope of an IT security disaster recovery plan.
08.20	Describe the purpose and scope of an IT security business continuity plan.
08.21	Describe the four phases of forensic analysis and discuss the activities performed in each phase.

	08.22 Describe the forensic and evidentiary considerations when determining containment.
	08.23 Describe the types and sources of data collected for forensic analysis.
	08.24 Explain the various forms of data and associated collection/retrieval tools for the application transport, IP, and link layers.
	08.25 Describe the essential elements of forensic analysis.
09.0	Demonstrate proficiency in managing hardware involved in imaging and data collection activities. The student will be able to:
	09.01 Discuss the different types of Motherboard Connections.
	09.02 Explain the components that comprise a Motherboard and their functions.
	09.03 Describe the different types of permanent storage.
	09.04 Compare and contrast the different host interface standards.
	09.05 Describe how Solid State storage processes differ from traditional storage.
	09.06 Discuss the different types of removable media and their impacts on data collection.
	09.07 Explain the concepts of RAID including the different Levels and their impacts on the imaging and collection process.
	09.08 Compare and contrast the read/write process of both permanent and temporary storage devices.
	09.09 Compare the standard boot process to the Forensic/controlled boot process.
10.0	Demonstrate proficiency in analyzing common file systems. The student will be able to:
	10.01 Define the Master Boot Record (MBR) and discuss its purpose and any important items that it may contain.
	10.02 Explain the purpose of the Boot Parameter Block (BPB) and its components.
	10.03 Discuss the different File Systems available in an OS environment. Identify the strengths and weaknesses of each system.
	10.04 Explain the process of file creation and deletion in an OS environment including the concept of file artifacts.
	10.05 Discuss the formatting process in an OS environment.
	10.06 Explain pertinent OS system files related to data storage and their functions.
	10.07 Discuss how Windows handles the concept of Date and Time in relation to file management and how it differs from UNIX-like operating systems.
	10.08 Define the different file systems that can be used with removable media.

	10.09 Explain the concepts of Open and Closed sessions.
11.0	Demonstrate proficiency in performing computer forensics investigations. The student will be able to:
	11.01 Create security incident handling and response policies.
	11.02 Recover deleted, encrypted, or damaged file information as evidence for civil or criminal cases.
	11.03 Deploy proprietary and/or open source tools to identify an intruder's footprints.
	11.04 Coordinate incident response activities in cooperation with law enforcement agencies.
	11.05 Prepare proper documentations of chain of custody, accounting for where each evidence item originated from, where it is going, and what entity has possession of the evidence.
	11.06 Preserve forensic integrity of evidence so they can be admissible in court.
	11.07 Describe moral and ethical standards in conducting digital forensics investigations.
12.0	Demonstrate proficiency in performing mobile device forensics. The student will be able to:
	12.01 Preserve, acquire, and examine data stored on mobile devices.
	12.02 Perform forensic acquisition and examination of SIM cards.
	12.03 Apply forensic principles and tools to mobile and IoT devices.
	12.04 Demonstrate proficiency in using open-source and proprietary mobile device forensics tools.
	12.05 Compare forensic acquisition tools and validate the completeness and accuracy of results.
	12.06 Describe forensic acquisition and examination of GPS navigation devices.
	12.07 Utilize the results from mobile device forensics for internal investigations or in civic/criminal litigation.
13.0	Demonstrate proficiency in incident handling and response. The student will be able to:
	13.01 Design an incident response plan including: assessment, communication, containment, evaluation, recovery, and documentation.
	13.02 Describe information-hiding techniques.
	13.03 Describe the steps required to collect, seize, and protect evidence.
	13.04 Recover data from various storage devices after physical and/or logical damage.
	13.05 Search and report on memory in real time with live and system forensics.

	13.06 Investigate network traffic using log files, time analysis, sniffers, and other traffic analysis tools.
	13.07 Explain the legal considerations to investigating emails as prescribed in the Electronic Communications Privacy Act.
	13.08 Identify email tracing techniques in forensic investigations.
14.0	Identify key pieces of legislation and processes related to digital forensics. The student will be able to:
	14.01 Describe the importance of creating an accurate representation of the facts.
	14.02 Explain the components of the Discovery Process.
	14.03 Discuss the 4th Amendment and its impact on the digital forensics investigative process.
	14.04 Identify laws and court cases related to computer forensics and their impacts on the investigation process.
	14.05 Identify and explain the basic Federal Rules of Evidence.
	14.06 Compare and contrast the different qualifications required to be a licensed computer forensics professional from state to state.
	14.07 Define the concept of a subpoena and explain the process of how one is obtained.
	14.08 Explain the steps required to acquire a search warrant.
	14.09 Discuss the concept of consent and the ways that it can be granted.
	14.10 Compare the legal process for civil and criminal cases.
	14.11 Define the concept of expert testimony and the process involved in being classified as an expert.
	14.12 Discuss appropriate courtroom behavior.
15.0	Demonstrate an understanding of the tasks related to the casework process. The student will be able to:
	15.01 Explain the steps involved in maintaining the integrity of digital evidence.
	15.02 Discuss the process of creating a forensics image.
	15.03 Define hashing and explain its uses in ensuring image authenticity.
	15.04 Describe sector slack space and its potential impact on evidence gathering.
	15.05 Describe the importance of documenting the examination process.
	15.06 Explain control/security access logs for images and their importance in maintaining evidence.

15.07	Describe the steps involved in preparing evidence and documents for trial.
15.08	Explain the procedures involved in creating a digital forensics investigation report including examples of report formats.
15.09	Discuss the importance of the Summation and Analysis sections of the digital investigation report.

IP Communications Specialization Standards	
08.0	Demonstrate an understanding of IP communication theory. The student will be able to:
	08.01 Describe the supported multivendor hardware platforms for VoIP technology, their limits, and their boundaries.
	08.02 Describe how Voice Gateways function in an IP Telephony (IPT) solution.
	08.03 Identify and describe the Local Area Network (LAN) switching products useable in an IPT solution.
09.0	Demonstrate an understanding of digitizing voice traffic and voice compression standards. The student will be able to:
	09.01 Identify the steps required for analog to digital conversion in a VoIP network.
	09.02 Identify the signaling steps required to complete a Public Switched Telephone Network (PSTN) call.
	09.03 Define the function of Private Branch eXchanges (PBX) or key systems.
	09.04 Configure Foreign eXchange Subscriber (FXS) and Foreign eXchange Office (FXO) interfaces on a Voice Gateway.
10.0	Demonstrate an understanding of Quality of Service (QoS) requirements in a converged data and voice network. The student will be able to:
	10.01 Identify the steps required to minimize jitter, packet loss and serialization delay in a VoIP network.
	10.02 Explain the function of IP precedence and different Class of Service (CoS) types.
	10.03 Identify and list the types of traffic coming into the interface and defining their relative priority.
	10.04 Configure a priority or custom queuing list.
11.0	Demonstrate an understanding of IP communications design. The student will be able to:
	11.01 Identify the most appropriate gateway in IP communication design.
	11.02 Identify and describe dial plan architecture in IP communication design.
	11.03 Identify the correct route patterns, filters, and use of wild cards in VoIP design scenarios.
	11.04 List available classes of services in IP communication design and their constraints.
	11.05 Describe how to use digit manipulation in VoIP design.
	11.06 Identify the appropriate QoS tools needed for the proper operation of voice traffic on a network.

12.0	Demonstrate an understanding of troubleshooting procedures for IP communications. The student will be able to:
	12.01 Identify the appropriate method for providing redundancy in VoIP design.
	12.02 Describe the tools used in troubleshooting IP communication networks.
	12.03 Identify and describe the different call flows and series of events through the call traces and debug outputs when troubleshooting.
	12.04 List the alarms used in IP communication troubleshooting.
13.0	Demonstrate an understanding of utilizing advanced Voice over IP (VoIP) and data bundle solutions to provide a single network connection for phone services and high-speed Internet. The student will be able to:
	13.01 Identify the required bandwidth speeds needed for uninterrupted service and fast uploads and downloads.
	13.02 Describe the impact of voice samples, codecs, and packet size on bandwidth.
	13.03 Describe on demand use of voice/data and voice prioritization, delivered over a private/secure line.
	13.04 Describe features for a VoIP and data bundle.
	13.05 Describe VoIP and data bundle used to dynamically alternate between voice and Internet as call volume needs dictate.
14.0	Demonstrate an understanding of using Statistical Analysis System (SAS) sessions to exchange data by using the TCP/IP communications access method. The student will be able to:
	14.01 Identify that a SAS/SHARE server ID has been added to the TCP/IP SERVICES file.
	14.02 Describe how to invoke SAS sessions utilizing TCP/IP communications access method.
	14.03 Describe syntax used to identify port numbers, defined in the client TCP/IP SERVICES file.
15.0	Demonstrate how to configure VoIP fax applications for universal access servers. The student will be able to:
	15.01 Describe fax applications that enable universal access servers to send and receive faxes across packet-based networks using modems.
	15.02 Describe universal inbox applications for fax and email and how faxes and emails can go to the same mailbox using direct inward dialing.
	15.03 Describe how to broadcast a fax to multiple recipients simultaneously.
16.0	Demonstrate an understanding of key concepts for Video over IP. The student will be able to:
	16.01 Describe video over IP systems using existing standards to reduce the data to a bitstream and then an IP network to carry the encapsulated data in a stream of IP packets.
	16.02 Describe the quality of service requirements which must be fulfilled for use in broadcast carrying video over IP networks.
	16.03 Describe bandwidth requirements, the maximum allowable packet loss rate, and approaches to achieve acceptable bandwidth such

	as quantity of service, network admission control, bandwidth reservation, traffic shaping, and traffic prioritization techniques.
16.04	Describe latency variation and its effect on making synchronization more complex by making the recovery of the underlying timing of the video signal far more difficult.

Advanced Network Infrastructure Specialization Standards	
08.0	Demonstrate an understanding of routing concepts. The student will be able to:
08.01	Describe the purpose, architecture, and operations of a router.
08.02	Identify the hardware and software components of routers.
08.03	Explain the purpose and nature of routing tables.
08.04	Describe administrative distance and routing metrics such as hop counts and cost.
08.05	Describe how a router determines a path and switches packets.
08.06	Differentiate between static and dynamic routing.
08.07	Explain the differences between class-full and classless routing.
08.08	Describe the use and operation of Variable Length Subnet Masks (VLSM) and Classless Inter-Domain Routing (CIDR).
08.09	Describe how a network converges.
09.0	Demonstrate an understanding of routing protocols. The student will be able to:
09.01	Describe the characteristics of distance vector routing protocols.
09.02	Describe the characteristics of link state routing protocols.
09.03	Describe the differences between distance vector and link state routing protocols, and determine the best routing protocol to use in a given situation.
09.04	Describe the features and operation of current internal and external routing protocols.
09.05	Determine network resources needed for implementing various routing protocols.
10.0	Demonstrate router configuration skills. The student will be able to:
10.01	Configure and verify router interfaces.
10.02	Perform basic router configuration and using the Command Line Interface (CLI) to inspect the operations of the router.
10.03	Design and implement a classless IP addressing scheme for a network.
10.04	Use advanced configuration commands with routers.

10.05	Configure OSPF, EIGRP, BGP, eBGP, RIPv2, and RIPng routing in a network.
10.06	Fine-tune OSPF settings on a router, including the configuration of reference bandwidth, redistribution of static and default routes, and modification of OSPF intervals, in order to optimize network performance.
10.07	Verify and troubleshoot router operations in an OSPF network.
10.08	Configure and modify metric on a router to improve network performance.
10.09	Configure summarization and default route settings on a router to optimize network performance.
10.10	Verify and troubleshoot router operations in complex network environment.
10.11	Create an EIGRP implementation plan.
10.12	Create an EIGRP verification plan.
10.13	Verify an EIGRP solution was implemented properly using show and debug commands.
10.14	Document and verify results for an EIGRP implementation.
11.0	Demonstrate an understanding of LAN design and concepts. The student will be able to:
11.01	Identify the layers and functions of switched network architecture.
11.02	Describe the principles and benefits of a hierarchical network design.
11.03	Explain the technology and media access control method for Ethernet networks.
11.04	Describe the issues associated with Layer 2.
11.05	Describe the operation of a LAN switch.
11.06	Describe the benefits of Virtual Local Area Networks (VLAN).
11.07	Identify and describe the different VLAN encapsulation protocols and their operation.
11.08	Describe the purpose and operation of VLAN Trunking Protocol (VTP) in the management of a switched network domain.
11.09	Describe the purpose and operation of Spanning Tree Protocol (STP), and its variants.
11.10	Describe the use of Inter-VLAN routing to connect different Networks in a switch-based network topology.
11.11	Analyze business requirements and design a LAN structure to meet those requirements.
11.12	Discuss quality-of-service considerations and switching prioritization.

11.13	Describe a VoIP support solution.
11.14	Describe a video support solution.
11.15	Configure port security features.
11.16	Configure general security features.
12.0	Demonstrate VLAN configuration skills. The student will be able to:
12.01	Perform and verify initial LAN switch configuration tasks including remote access management, switch port modes, and trunks.
12.02	Configure, verify, and troubleshoot VLANs on a LAN switch.
12.03	Implement a VLAN Domain by configuring LAN switches for VTP network operation.
12.04	Configure a Router to provide Inter-VLAN routing using multiple physical interfaces, and on a single physical interface with sub-interfaces.
12.05	Configure and troubleshoot Spanning Tree Protocol and its variants on a switched network environment.
12.06	Configure and verify the bridge to optimize STP.
12.07	Establish and configure port priorities.
12.08	Troubleshoot and resolve issues with STP operations.
12.09	Create a Layer 3 path control implementation plan based upon the results of the redistribution analysis.
12.10	Create a Layer 3 path control verification plan.
12.11	Configure Layer 3 path control.
12.12	Verify that a Layer 3 path control was implemented.
12.13	Document results of a Layer 3 path control implementation and verification plan.
12.14	Describe basic VPN technologies.
12.15	Describe branch access technologies.
12.16	Configure private VLANs.
12.17	Configure VACL and PACL.
12.18	Configure switch-to-switch connectivity for the VLAN based solution.

12.19	Configure loop prevention for the VLAN based solution.
12.20	Configure Access Ports for the VLAN based solution.
12.21	Determine network resources needed for implementing a VLAN based solution on a network.
12.22	Create a VLAN based implementation plan.
12.23	Create a VLAN based verification plan.
12.24	Verify the VLAN based solution was implemented properly using show and debug commands.
12.25	Document the verification after implementing a VLAN solution.
13.0	Demonstrate an understanding of network maintenance, support and troubleshooting. The student will be able to:
13.01	Identify, interpret and maintain network documentation, procedures and practices.
13.02	Describe effective troubleshooting strategies and techniques to resolve basic hardware, software, and network problems.
13.03	Describe standard operating procedures for troubleshooting hardware and software.
13.04	Identify procedures to manage, maintain and backup router and switch system and configuration files.
13.05	Recognize and resolve hardware and software configuration problems.
13.06	Identify and resolve common network problems at layers 1, 2, 3, and 7 using a layered model approach. Describe the use and features of diagnostic test equipment.
13.07	Determine type of programs and procedures required to: baseline network performance, identify intrusion and unacceptable system use, identify performance issues, predict system failures, and optimize network availability.
13.08	Use network monitoring and management tools effectively to integrate and manage network resources.
13.09	Explain RMON and SNMP and their use in monitoring a network.
13.10	Configure network devices to send SNMP traps or alerts to network management systems.
13.11	Establish and document a network baseline.
13.12	Compare and analyze initial performance measurements with the availability of critical network devices and connections to determine the difference between abnormal behavior and proper network performance as the network grows or traffic patterns change.
13.13	Optimize traffic flow conditions on network connections based on analysis of traffic types, characteristics and user needs.
13.14	Determine network resources needed for implementing a switch based Layer 3 solution.
13.15	Create an implementation plan for the switch based Layer 3 solution.

13.16	Create a verification plan for the switch based Layer 3 solution.
13.17	Configure routing interfaces.
13.18	Configure Layer 3 security.
13.19	Verify the switch based Layer 3 solution was implemented properly using show and debug commands.
13.20	Document the verification results after implementing a switch based Layer 3 solution.
13.21	Develop a plan to monitor and manage a network.
13.22	Perform network monitoring using IOS tools.
13.23	Perform routine IOS device maintenance.
13.24	Isolate sub-optimal internetwork operation at the correctly defined OSI Model layer.
13.25	Troubleshoot EIGRP.
13.26	Troubleshoot OSPF.
13.27	Troubleshoot eBGP.
13.28	Troubleshoot routing redistribution solution.
13.29	Troubleshoot a DHCP client and server solution.
13.30	Troubleshoot NAT.
13.31	Troubleshoot first hop redundancy protocols.
13.32	Troubleshoot IPv6 routing.
13.33	Troubleshoot IPv6 and IPv4 interoperability.
13.34	Troubleshoot switch-to-switch connectivity for the VLAN based solution.
13.35	Troubleshoot loop prevention for the VLAN based solution.
13.36	Troubleshoot access ports for the VLAN based solution.
13.37	Troubleshoot private VLANS.
13.38	Troubleshoot port security.

13.39 Troubleshoot general switch security.
13.40 Troubleshoot VACLs and PACLs.
13.41 Troubleshoot switch virtual interfaces (SVIs).
13.42 Troubleshoot switch supervisor redundancy.
13.43 Troubleshoot switch support of advanced services (i.e., Wireless, VoIP, Video).
13.44 Troubleshoot a VoIP support solution.
13.45 Troubleshoot a video support solution.
13.46 Troubleshoot Layer 3 security.
13.47 Troubleshoot issues related to ACLs used to secure access to Cisco routers.
13.48 Troubleshoot configuration issues related to accessing the AAA server for authentication purposes.
13.49 Troubleshoot security issues related to IOS services (i.e., finger, NTP, HTTP, FTP, RCP).

Linux System Administrator Specialization Standards	
08.0	Understand and use essential tools. The student will be able to:
08.01	Access a shell prompt and issue commands with correct syntax.
08.02	Use input-output redirection (>, >>, |, 2>). Demonstrate the use of standard-in, standard-out, standard-error, and pipe.
08.03	Demonstrate the use of grep and regular expressions to analyze text.
08.04	Access remote systems using ssh.
08.05	Log in and switch users in multiuser targets.
08.06	Archive, compress, unpack, and uncompress files using a variety of tools.
08.07	Create and edit text files.
08.08	Create, delete, copy, and move files and directories.
08.09	Create hard and soft links.
08.10	List, set, and change standard ugo/rwx permissions.
08.11	Locate, read, and use system documentation including man, info, and files in /usr/share/doc.
09.0	Operate running systems. The student will be able to:
09.01	Boot, reboot, and shut down a system normally.
09.02	Boot systems into different targets manually.
09.03	Interrupt the boot process in order to gain access to a system.
09.04	Identify CPU/memory intensive processes, adjust process priority with renice, and kill processes.
09.05	Locate and interpret system log files and journals.
09.06	Perform various logging related activities such as configuring logging, log rotation and log reporting.
09.07	Access a virtual machine's console.
09.08	Explain the meaning and use of common metrics such as utilization values for CPU, memory, disk space, disk I/O, and network bandwidth.
09.09	Start and stop virtual machines.

	09.10 Start, stop, and check the status of network services.
	09.11 Securely transfer files between systems.
10.0	Configure local storage. The student will be able to:
	10.01 List, create, delete partitions on MBR and GPT disks.
	10.02 Create and remove physical volumes, assign physical volumes to volume groups, and create and delete logical volumes.
	10.03 Configure systems to mount file systems at boot by Universally Unique ID (UUID) or label.
	10.04 Create, use and remove snapshots of logical volumes.
	10.05 Add new partitions and logical volumes, and swap to a system non-destructively.
11.0	Create and configure file systems. The student will be able to:
	11.01 Create, mount, unmount, and using various file systems.
	11.02 Mount and unmount CIFS and NFS network file systems.
	11.03 Extend existing logical volumes.
	11.04 Discuss set UID and GID.
	11.05 Create and manage Access Control Lists (ACLs).
	11.06 Diagnose and correct file permission problems.
12.0	Deploy, configure, and maintain systems. The student will be able to:
	12.01 Configure networking and hostname resolution statically or dynamically.
	12.02 Schedule tasks using at and cron.
	12.03 Start and stop services and configure services to start automatically at boot.
	12.04 Configure systems to boot into a specific target automatically.
	12.05 Perform an unattended system install.
	12.06 Configure a physical machine to host virtual guests.
	12.07 Install Linux systems as virtual guests.

	12.08 Configure systems to launch virtual machines at boot.
	12.09 Configure network services to start automatically at boot.
	12.10 Configure a system to use time services.
	12.11 Install and update software packages from a remote repository or a local file system.
	12.12 Update the kernel package appropriately to ensure a bootable system.
	12.13 Modify the system bootloader.
13.0	Manage users and groups. The student will be able to:
	13.01 Create, delete, and modify local and global user accounts.
	13.02 Change passwords and adjust password aging for local and global user accounts.
	13.03 Create, delete, and modify local and global groups and group memberships.
	13.04 Configure a system to use an existing authentication service for user and group information.
14.0	Manage security. The student will be able to:
	14.01 Describe security basic concepts and mechanisms, including encryption, password safety, message digests and system security requirements.
	14.02 Demonstrate proper security techniques and monitoring.
	14.03 Configure firewall settings using firewall-config, firewall-cmd, or iptables.
	14.04 Configure key-based authentication for SSH.
	14.05 Set enforcing and permissive modes for SELinux.
	14.06 List and identify SELinux file and process context.
	14.07 Restore default file contexts.
	14.08 Use boolean settings to modify system SELinux settings.
	14.09 Diagnose and address routine SELinux policy violations.

Additional Information

Laboratory Activities

Laboratory investigations that include scientific inquiry, research, measurement, problem solving, emerging technologies, tools and equipment, as well as, experimental, quality, and safety procedures are an integral part of this career and technical program/course. Laboratory investigations benefit all students by developing an understanding of the complexity and ambiguity of empirical work, as well as the skills required to manage, operate, calibrate and troubleshoot equipment/tools used to make observations. Students understand measurement error; and have the skills to aggregate, interpret, and present the resulting data. Equipment and supplies should be provided to enhance hands-on experiences for students.

Career and Technical Student Organization (CTSO)

Phi Beta Lambda and Business Professionals of America (BPA) are the intercurricular career and technical student organizations providing leadership training and reinforcing specific career and technical skills. Career and Technical Student Organizations provide activities for students as an integral part of the instruction offered.

Accommodations

Federal and state legislation requires the provision of accommodations for students with disabilities to meet individual needs and ensure equal access. Postsecondary students with disabilities must self-identify, present documentation, request accommodations if needed, and develop a plan with their counselor and/or instructors. Accommodations received in postsecondary education may differ from those received in secondary education. Accommodations change the way the student is instructed. Students with disabilities may need accommodations in such areas as instructional methods and materials, assignments and assessments, time demands and schedules, learning environment, assistive technology and special communication systems. Documentation of the accommodations requested and provided should be maintained in a confidential file.

Certificate Programs

A College Credit Certificate consists of a program of instruction of less than sixty (60) credits of college-level courses, which is part of an AS or AAS degree program and prepares students for entry into employment (Rule 6A-14.030, F.A.C.). This AS degree program includes the following College Credit Certificates:

Network Server Administration (0511100112) – Primary/Secondary: 24/18 hours
Network Enterprise Administration (0511100113) – Primary/Secondary: 29/26 hours
Network Infrastructure (0511100114) – Primary/Secondary: 21/16 hours
Advanced Network Infrastructure (0511100115) – Primary/Secondary: 36/28 hours
Network Virtualization (0511100116) – Primary: 24/18 hours
Advanced Network Virtualization (0511100117) – Primary/Secondary: 34/27 hours
Network Security (0511100118) – Primary/Secondary: 30/20 hours
Digital Forensics (0511100119) – Primary/Secondary: 32/24 hours
IP Communications (0511100120) – Primary/Secondary: 32/21 hours
Network Support Technician (0511100121) – Primary/Secondary: 21/16 hours

Linux System Administrator (0511100122) – Primary/Secondary: 24/21 hours

Standards for the above certificate programs are contained in separate curriculum frameworks.

Additional Resources

For additional information regarding articulation agreements, Bright Futures Scholarships, Fine Arts/Practical Arts Credit and Equivalent Mathematics and Equally Rigorous Science Courses please refer to:
http://www.fldoe.org/academics/career-adult-edu/career-tech-edu/program-resources.stml