Network Engineering/Cyber Security I & II

Program Description: The first year course teaches the basic techniques of computer safety and maintenance. Students learn to assemble/disassemble personal computers (PCs) and to recognize the essential components that comprise a PC, including memory types, bus architecture, CPUs, motherboards, storage devices, and the various Microsoft operating systems – including MS-DOS. The course follows CompTIA's A+ certification program emphasizing "hands on" training in upgrading, diagnosing, and repairing PCs.

The second year begins with students reviewing installation, maintenance, and troubleshooting techniques. The first semester follows CompTIA's Network + Certification requirements. The students are reintroduced to network hardware, cabling, architecture, and protocols. TCP/IP basics are emphasized together with network models and troubleshooting.

Level I: PC Hardware and Software

Unit 1: Introduction to the Personal Computer (PC)

Unit Objectives:

1. Demonstrate knowledge of various Informational Technology industry certifications.
2. Identify a computer system.
3. Identify the names, purposes, and characteristics of cases and power supplies, internal components, and ports and cables.
4. Define and identify input and output devices.
5. Identify system resources and know their particular purpose.
6. Identify the various expansion buses and give their use in the PC.
7. Define AGP, PCI, and PCIe and describe the impact each has had on PC video.
8. Identify the many personal computer acronyms.

Unit 2: Safe Lab Procedures and Tool Use

Unit Objectives:

1. Demonstrate knowledge of proper work conditions and procedures.
2. Define ESD and its impact on a personal computer.
3. Identify personal computer materials that are hazardous and how proper disposal procedures.
4. Understand what EMI is, its sources, and how it can impact a PC's storage abilities.
5. Understand power fluctuations and the devices that can minimize it.
6. Identify appropriate tools and software are used with personal computers components and their particular purpose.
7. Demonstrate an understanding of proper use of tools used in computer repair.
8. Define and demonstrate PC safety – protecting yourself and the personal computer.

Unit 3: Computer Assembly – Step-by-Step

Unit Objectives:

1. Demonstrate an understanding of how to open the various personal computer cases.
2. Demonstrate how to install a power supply, motherboard, and CPU.
3. Demonstrate how to install the various adapter cards, their usage, and proper configuration.
4. Identify various computer parts and be able to determine compatibility.
5. Identify and properly attach cables to the PC – both internally and externally.
6. Demonstrate proper method to assemble/disassemble a PC and have it in working order.

Unit 4: Basics of Preventive Maintenance and Troubleshooting (Section 5)

Unit Objectives:
1. Demonstrate an understanding of the purpose of preventive maintenance.
2. Demonstrate the proper – and improper – PC cleaning procedures.
3. To understand the basic PC troubleshooting procedure and the need therefore.
4. Understand why you document all changes to the personal computer.
5. Discuss the importance of replacing old PC parts with quality replacements.

Unit 5: Fundamental Operating Systems - DOS, Win 2000, Win XP, Ubuntu

Unit Objectives:
1. Define how an operating system works.
2. Describe the basic functions of an operating system.
3. Demonstrate how DOS 6.22 works.
4. Demonstrate an understanding of the different operating systems and to describe the advantages and disadvantages of each system.
5. Demonstrate knowledge of determining appropriate operating systems for various client environments.
6. To be able to install an operating system – Win 2000, Win XP, Ubuntu – and explain how each works.

Unit 6: Fundamental Networks

Unit Objectives:
1. Define a network.
2. Describe basic network concepts and technologies.
3. Identify network physical components and have a basic idea of how they work.
4. Describe the different topologies and architectures of the various networks.
5. Demonstrate an understanding of the different access methods and be able to give their advantages/ disadvantages.
6. Understand the basics of the OSI and TCP/IP models, their different data models, and their advantages.

Unit 7: Fundamental Laptops

Unit Objectives:
1. Demonstrate an understanding of the basic workings of a laptop computer.
2. Demonstrate an understanding of how laptops work.
3. Describe the advantages/disadvantages of laptop devices versus a desktop.
4. Demonstrate the common preventive maintenance techniques to maximize laptop efficiency.

Unit 8: Fundamental Mobile Devices

Unit Objectives:
1. Demonstrate an understanding of the basic workings of mobile devices
2. Demonstrate the common preventive maintenance techniques to maximize portable device efficiency.
3. Demonstrate knowledge of methods to configure the various portable devices.
4. Demonstrate the common preventive maintenance techniques to maximize portable device efficiency.
5. Demonstrate knowledge of methods to configure the various portable devices.

Unit 9: Fundamental Printers and Scanners

Unit Objectives:
1. Recognize the different types of printers and scanners.
2. Demonstrate how to configure/install the different printers and scanners.
3. Articulate the advantages/disadvantages of the various printers and scanners.
4. Demonstrate how a dot matrix, inkjet, and laser printer work and describe the advantages/disadvantages of each.
5. Demonstrate the basic routine preventive maintenance used for printers/scanners.

Unit 10: Fundamental Security

Unit Objectives:
1. Demonstrate an understanding of the importance of network security.
2. Identify the basic security threats and how to procedures to deal with them effectively.
3. Understand how best to combat security issues and identify the tools (software and hardware) used.

Unit 11: The IT Professional

Unit Objectives:
1. Identify the importance of communication skills and customer relations.
2. Identify methods in gaining information from the client in order to troubleshoot.
3. Demonstrate a knowledge and understanding of the ethics and legal aspects of working in the computer field.

**Unit 12: Advanced Troubleshooting **

Unit Objectives:
1. Advanced troubleshooting of Operating Systems
2. Advanced troubleshooting of Networks
3. Advanced troubleshooting of Laptops
4. Advanced troubleshooting of Printers
5. Advanced Security

Level I: Introduction to Networking

Unit 1: Exploring the Network

Unit Concepts:
1. Globally Connected
2. LANs, WANs, and the Internet
3. The Network as Platform
4. The Changing Network Environment

Unit 2: Configuring a Network Operating System

Unit Concepts:
1. IOS Bootcamp (Cisco IOS Commands)

2. Getting Basic (Basic network device configurations)
3. Addressing Schemes (IP Addressing)

Unit 3: Network Protocols and Communications

Unit Concepts:
1. Rules of Communication
2. Network Protocols and Standards
3. Moving Data in the Network

Unit 4: Network Access

Unit Concepts:
1. Physical Layer Protocols
2. Network Media (Making Network Cables)
3. Data Link Layer Protocols
4. Media Access Control

Unit 5: Ethernet

Unit Concepts:
1. Ethernet Protocol
2. Address Resolution Protocol
3. LAN Switches

Unit 6: Network Layer

Unit Concepts:
1. Network Layer Protocols
2. Routing
3. Routers
4. Configuring a Cisco Router

Unit 7: IP Addressing

Unit Concepts:
1. IPv4 Network Addresses
2. IPv6 Network Addresses
3. Connectivity Verification

Unit 8: Subnetting IP Networks

Unit Concepts:
1. Subnetting IPv4 Network
2. Addressing Schemes
3. Design Considerations for IPv6

Unit 9: Transport Layer

Unit Concepts:
1. Transport Layer Protocols
2. TCP and UDP

Unit 10: Application Layer

Unit Concepts:
1. Application Layer Protocols
2. Well-Known Application Layer Protocols and Services

Unit 11: It's A Network

Unit Concepts:
1. Network Design
2. Network Security
3. Basic Network Performance

.

Level II: Routing and Switching Essentials

Unit 1: Introduction to Switched Networks

Unit Concepts:
1. LAN Design
2. The Switched Environment

Unit 2: Basic Switching Concepts and Configuration

Unit Concepts:
1. Basic Switch Configuration
2. Switch Security: Management and Implementation

Unit 3: VLANs

Unit Concepts:
1. VLAN Segmentation
2. VLAN Implementation
3. VLAN Security and Design

Unit 4: Routing Concepts

Unit Concepts:
1. Initial Configuration of a Router
2. Routing Decisions
3. Router Operation

Unit 5: Inter-VLAN Routing

Unit Concepts:
1. Inter-VLAN Routing Configuration
2. Troubleshoot Inter-VLAN Routing
3. Layer 3 Switching

Unit 6: Static Routing

Unit Concepts:
1. Static Routing Implementation
2. Configure Static and Default Routes
3. Review of CIDR and VLSM
4. Configure Summary and Floating Static Routes
5. Troubleshoot Static and Default Route Issues

Unit 7: Routing Dynamically

Unit Concepts:
1. Dynamic Routing Protocols
2. Distance Vector Routing Protocols
3. RIP and RIPng Routing
4. Link-State Dynamic Routing
5. The Routing Table

Unit 8: Single-Area OSPF

Unit Concepts:
1. Characteristics of OSPF
2. Configuring Single-Area OSPFv2
3. Configuring Single-Area OSPFv3

Unit 9: Access Control Lists

Unit Concepts:
1. IP ACL Operating
2. Standard IPv4 ACLs
3. Extended IPv4 ACLs
4. Troubleshoot ACLs
5. IPv6 ACLs

Unit 10: DHCP

Unit Concepts:
1. Dynamic Host Configuration Protocol v4
2. Dynamic Host Configuration Protocol v6

Unit 11: Network Address Translation for IPv4

Unit Concepts:
1. NAT Operation
2. Configuring NAT
3. Troubleshooting NAT

Level II: Scaling Networks (Advanced Networking)

Unit 1: Introduction to Scaling Networks

Unit Concepts:
1. Implementing a Network Design
2. Selecting Network Devices

Unit 2: LAN Redundancy

Unit Concepts:
1. Spanning Tree Concepts
2. Varieties of Spanning Tree Protocol
3. Spanning Tree Configuration
4. First-Hop Redundancy

Unit 3: Link Aggregation

Unit Concepts:
1. Link Aggregation Concepts
2. Link Aggregation Configuration

Unit 4: Wireless LANs

Unit Concepts:
1. Wireless LAN Concepts
2. Wireless LAN Operation
3. Wireless LAN Security
4. Wireless LAN Configuration

Unit 5: Adjust and Troubleshoot Single-Area OSPF

Unit Concepts:
1. Advanced Single-Area OSPF Configurations
2. Troubleshooting Single-Area OSPF Implementations

Unit 6: Multi-Area OSPF

Unit Concepts:
1. Multi-Area OSPF Operation
2. Configuring Multi-Area OSPF

Unit 7: EIGRP

Unit Concepts:
1. Characteristics of EIGRP
2. Configuring EIGRP for IPv4
3. Operation of EIGRP
4. Configuring EIGRP for IPv6

Unit 8: EIGRP Advanced Configurations and Troubleshooting

Unit Concepts:
1. Advanced EIGRP Configurations
2. Troubleshoot EIGRP

Unit 9: IOS Images and Licensing

Unit Concepts:
1. Managing IOS System Files
2. IOS Licensing

Level II: Connecting Networks (Advanced Networking)

Unit 1: Hierarchical Network Design

Unit Concepts:
1. Hierarchical Network Design Overview
2. Cisco Enterprise Architecture
3. Evolving Network Architectures

Unit 2: Connecting to the WAN

Unit Concepts:
1. WAN Technologies Overview
2. Selecting a WAN Technology

Unit 3: Point-to-Point Connections

Unit Concepts:
1. Serial Point-to-Point Overview
2. PPP Operation
3. Configure PPP
4. Troubleshoot WAN Connectivity

Unit 4: Frame Relay

Unit Concepts:
1. Introduction to Frame Relay
2. Configure Frame Relay
3. Troubleshoot Connectivity

Unit 5: Network Address Translation for IPv4

Unit Concepts:
1. NAT Operation
2. Configuring NAT
3. Troubleshoot NAT

Unit 6: Broadband Solutions

Unit Concepts:
1. Teleworking
2. Comparing Broadband Solutions
3. Configuring xDSL Connectivity

Unit 7: Securing Site-to-Site Connectivity

Unit Concepts:
1. VPNs
2. Site-to-Site GRE Tunnels
3. Introducing IPsec
4. Remote Access

Unit 8: Monitoring the Network

Unit Concepts:
1. Syslog
2. SNMP
3. Netflow

Unit 9: Troubleshooting the Network

Unit Concepts:
1. Troubleshooting with a Systematic Approach
2. Network Troubleshooting

Level II: Security + (Cyber Security)

Unit 1: Cyber Ethics

Unit Concepts:
1. Define terms related to Ethics
2. Ethical Behavior
3. Ethics and Cybersecurity
4. Ethics Applications

Unit 2: Network Security

Unit Objectives:
1. Implement security configuration parameters on network devices
2. Use secure network administration principles
3. Explain network design elements and components
4. Implement common protocols and services
5. Troubleshoot security issues related to wireless networking

Unit 3: Compliance and Operational Security

Unit Objectives:

1. Explain the importance of risk related concepts
2. Implement appropriate risk mitigation strategies
3. Implement basic forensic procedures
4. Summarize common incident response procedures
5. Explain the importance of security related awareness and training
6. Compare and contrast physical security and environmental controls
7. Summarize risk management best practices
8. Select the appropriate control to meet the goals of security

Unit 4: Threats and Vulnerabilities

Unit Objectives:
1. Explain types of Malware
2. Summarize various types of attacks
3. Summarize social engineering attacks and the associated effectiveness of each attack
4. Explain types of wireless attacks
5. Explain types of application attacks
6. Analyze a scenario and select appropriate type of mitigation and deterrent techniques
7. Use appropriate tools and techniques to discover security threats and vulnerabilities
8. Explain the proper use of penetration testing versus vulnerability scanning

Unit 5: Application, Data, and Host Security

Unit Objectives:
1. Explain the importance of application security controls and techniques
2. Summarize mobile security concepts and technologies
3. Select the appropriate solution to establish host security
4. Implement the appropriate controls to ensure data security
5. Compare and contrast alternative methods to mitigate security risks in static environments

Unit 6: Access Control and Identity Management

Unit Objectives:
1. Compare and contrast the function and purpose of authentication services
2. Select the appropriate authentication, authorization, or access control
3. Install and configure security controls when performing account management, based on best practices

Unit 7: Cryptography

Unit Objectives:
1. Utilize general cryptography concepts
2. Use appropriate cryptographic methods
3. Use appropriate PKI, certificate management and associated components

Articulated Credit
6 College Credits for College of Southern Maryland

Certifications Available:
A+, CCENT, CCNA, Network+