COURSES

COMPUTER NETWORKING TECHNOLOGY COURSES

CNT 43 - Professional Communications

3 units

This course applies the principles of ethical and effective communication to the creation of letters, memos, emails, and written and oral reports for a variety of business situations. The course emphasizes critical thinking and analysis, planning, organizing, composing, and revising business documents to create and deliver professional-level oral presentations in-person and virtually. Additional focus will be placed on developing interpersonal skills, team participation skills, and technical report writing skills. Students who have completed or are enrolled in CIS 43 or CS 43 may not receive credit. 54 hours lecture.

Recommended Course Preparation: ENG 1A with a minimum grade of C or ENG 1AEX with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 51 - CompTIA's A+ Certification Computer Technician

4 units

This course provides an introduction to the computer hardware and software skills needed to help meet the industry demand for entry-level PC Technicians. This course covers PC hardware, software, security, networking, laptops, printers, operational procedures, operating systems, security, troubleshooting, and mobile devices. The students will study the topics needed to become certified PC technicians. Preparation for the CompTIA A + certification, which verifies knowledge equivalent to that of an entry-level ICT (Information and Communications Technology) technician with about 12 months of hands-on experience. The responsibilities of an ICT professional will be introduced. Students who have completed or are enrolled in APIS 51 may not receive credit. 54 hours lecture, 54 hours laboratory. Transfer: CSU; C-ID# ITIS 110.

Recommended Course Preparation: CIS 50 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 52 - Networking Fundamentals

3 units

This course provides an introduction to computer networking fundamentals skills needed to meet the industry demand for entry-level Network Technicians. Topics include: Ethernet network fundamentals, Local Area Networks (LANs), and Wide Area Networks (WAN) technologies, the Open Systems Interconnection (OSI) model, wiring implementations, network adapters and connectivity devices, IPv4/IPv6 addressing, Voice over IP (VoIP), and wireless standards. Tools to help prevent cyber attacks with IDS (Intrusion Detection Systems), authentication, and encryption are demonstrated. Student labs include: configuration of a SOHO (Small Office/Home Office), a firewall, a virtual private network (VPN), a switch, and a router and documenting a networking using professional drawing software. The responsibilities of an ICT (Information and Communications Technology) professional will be introduced. This course prepares students for the CompTIA Network+ Certification Exam. This professional certification verifies the student has the knowledge equivalent to that of an ICT technician with about 12 months of hands-on experience. Students who have completed or are enrolled in CIS 66 or APIS 52 may not receive credit. 54 hours lecture, 18 hours laboratory. Transfer: CSU; C-ID# ITIS 150.

Recommended Course Preparation: CIS 50 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 55 - MCSA I Windows Server Installation, Storage, and Compute

3 units

This course prepares students for the Microsoft's Examination: Installation, Storage and Compute with Windows Server, which is the first of three exams a student must pass to obtain a MCSA (Microsoft Certified Solutions Associate) Certification. By passing this exam, one become a Microsoft Certified Professional (MCP) and gains access to MCP benefits. The MCSA Windows Server certification qualifies its holder for a position as a network or computer systems administrator or as a computer network specialist. The topics include installation, storage, and compute features and functionality available in the current Windows Server, Nano Server, images for deployment, storage solutions, data deduplication, high availability, disaster recovery, storage spaces direct, and failover clustering solutions. Also covered: Hyper-V and containers.. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 155.

Recommended Course Preparation: CNT 52 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 56 - MCSA II Networking with Windows Server

3 units

This course prepares students for the Microsoft's Examination: Networking with Windows Server, which is the second of three exams a student must pass to obtain a MCSA (Microsoft Certified Solutions Associate) Certification. By passing this exam, one become a Microsoft Certified Professional (MCP) and gains access to MCP benefits. Through many hands-on labs, students will install and configure DNS, DHCP, IPAM, VPN and RADIUS. Also covered: managing DFS and branch cache solutions, and implementing Software Defined Networking (SDN) solutions such as Hyper-V Network Virtualization (HNV) and Network Controller, Implement Network Connectivity and Remote Access Solutions, Implement Core and Distributed Network Solutions. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CNT 55 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 57 - MCSA III Identity with Windows Server

3 units

This course prepares students for the Microsoft's Examination: Identity with Windows Server, which is the second of three exams a student must pass to obtain a MCSA (Microsoft Certified Solutions Associate) Certification. By passing this exam, one become a Microsoft Certified Professional (MCP) and gains access to MCP benefits. In this course, students manage identities, install, configure, manage, and maintain Active Directory Domain Services (AD DS) as well as implement Group Policy Objects (GPOs). Students also install and manage Active Directory Certificate Services (AD CS), Active Directory Federations Services (AD FS), Active Directory Rights Management Services (AD RMS), and Web Application proxy. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CNT 56 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 68 - Digital Forensics Fundamentals

3 units

A practical course in Digital Forensics; the detection, and investigation of incidents involving computers, networks, the Internet, and digital information. Case oriented, following the objectives for the CFE Computer Forensics Examiner certification exam and the International Association of Computer Investigative Specialists (IACIS), the class includes understanding and practice in basic computer forensics, methods of investigation, analysis of storage media, logs, and tracking persons and data, using court-approved

evidence collection tools. Also covered, computer forensics as a profession, the computer investigation process, and technical writing. Students who have completed or are enrolled in APIS 55 may not receive credit. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 165.

Recommended Course Preparation: CIS 66 with a minimum grade of C or CNT 52 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 69 - Network Security; CompTIA Security + Certification

3 units

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability. This course provides an introduction to the concepts and practices of secure network design and management using desktop and network operating systems, router and switch operating systems, hardware and software Firewall and VPN technology for wired and wireless systems. The program includes authentication methods and devices, protocol analysis and IP network troubleshooting, strategies for identifying and countering vulnerabilities, network media and topologies in a secure network, intrusion detection and forensic incident response. CompTIA Security+ meets the ISO 17024 standard and is approved by U.S. Department of Defense. Security+ is also compliant with government regulations under the Federal Information Security Management Act (FISMA). Students who have completed or are enrolled in APIS 53 may not receive credit. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 160.

Recommended Course Preparation: CNT 51 with a minimum grade of C. CNT 52 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 7285 - Cloud Infrastructure: CompTIA Cloud+ Certification

3 units

IT professionals need to understand the concepts and principles required to build cloud infrastructure. This course covers the objectives of the CompTIA Cloud+ and Dell/EMC Cloud Infrastructure and Services (CIS) certification exams. Topics include: Cloud Computing Concepts; Models; Disk Storage Systems; Storage Networking; Network Infrastructure; Virtualization Components; Virtualization and the Cloud; Network Management; Performance Tuning; Systems Management; Security in the Cloud and Best Practices; Business Continuity and Disaster Recovery; Testing; Automation; and Changes. The EMC cloud computing reference model includes five fundamental layers (physical, virtual, control, orchestration, and service) and three cross-layer functions (business continuity, security, and service management). Technologies, components, processes, and mechanisms for each layer and cross-layer function will be covered. The course follows the U.S. National Institute of Standards and Technology as a guide for all definitions of cloud computing. Upon completing this course, participants will have the knowledge to make informed decisions on technologies, processes, and mechanisms required to build cloud infrastructure. CompTIA certification is normally valid for three years. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CNT 8001 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 7401 - Red Hat Linux Administration I

3 units

This course provides hands-on training covering basic installation, management, configuration, documentation and hardware topics for the Linux/UNIX operating system on workstations in a network environment. The course includes comprehensive coverage of topics related to Linux distributions, installation, administration, X-Windows, and networking. This course prepares students for the CompTIA Linux+ Certification Exam. Students who have completed or are enrolled in CS 41 or APIS 54 may not receive credit. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CIS 50 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 7402 - Red Hat Linux Administration II

3 units

This course focuses on the key tasks needed to become a full time Linux Administrator and to validate those skills via the Red Hat Certified System Administrator exam. This course goes deeper into Enterprise Linux administration including filesystems and partitioning, logical volumes, SELinux, fire-walling, BASH script development and troubleshooting. Students who have completed or are enrolled in CS 3 may not receive credit. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CNT 7401 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 7501 - Ethical Hacking

3 units

This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network. These methodologies are presented within the context of properly securing the network. The course will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to an virtual environment. Students will receive a hands-on practical approach in penetration testing measures and ethical hacking. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 164.

Recommended Course Preparation: CNT 52 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 7701 - IT Virtualization, Data Centers, VMware Certification

3 units

With VMware, students learn about virtualization, SDNs (Software Defined Networks), data center management, and remote operation of IT infrastructures in the Cloud. Increasingly, businesses are moving their IT services to data centers, and skilled VMware professionals are and will be in high demand for the foreseeable future. vSphere - the major VMware platform - includes features for configuration, backup, cloning, resizing, securing, and moving virtual machines. Upon completion of this course, students will have covered the topics required for taking the examination for the VMware Certified Professional (VCP). This hands-on training course will have students install, configure, and manage different VMware virtualization products. VMware certification is normally valid for two years. 45 hours lecture, 27 hours laboratory. Transfer: CSU.

Recommended Course Preparation: CNT 8001 with a minimum grade of C. CNT 51 with a minimum grade of C. CNT 52 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 8001 - Cisco CCNA1/3 Introduction to Networks (ITN)

3 units

This is course 1 of 3 of the Cisco CCNA Routing and Switching Certification Objectives. The concepts covered in this course include advances in modern

network technologies; Protocols and Models: how network protocols enable devices to access local and remote network resources; Physical Layer: how physical layer protocols, services, and network media support communications across networks; Data Link Layer: how media access control in the data link layer supports communication across networks; Ethernet Switching: how Ethernet operates in a switched network; Network Layer: how routers use network layer protocols and services to enable end-to-end connectivity; Address Resolution: Protocol (ARP) and Neighbor Discovery (ND) enable communication on a local area network; Transport Layer & Application Layer: Explain the operation of layers protocols in providing support to end-user applications. The hands-on labs include implementation of initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices; Basic Switch and Device Configuration; Calculation of numbers between decimal and binary systems; IPv4 Addressing: IPv4 subnetting scheme to segment a network; Implementing an IPv6 addressing scheme; ICMP and various tools to test network connectivity; Network Security Fundamentals: Configure switches and routers with device hardening features to enhance security; Build a Small Network: Implement a network design for a small network to include a router, a switch, and end devices. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 150.

Recommended Course Preparation: CIS 50 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 8002 - Cisco CCNA2/3 Switching, Routing, and Wireless Essentials (SRWE)

3 units

This is course 2 of 3 of the Cisco CCNA Routing and Switching Certification Objectives. The concepts covered in this course include Switching: how Layer 2 switches forward data; how STP enables redundancy in a Layer 2 network; the operation of dynamic address allocation in IPv6 networks by using SLAAC and DHCPv6; how FHRPs provide default gateway services in a redundant network; how vulnerabilities compromise LAN security; how Wireless LANs enable network connectivity; how routers use information in packets to make forwarding decisions; and troubleshooting static and default route configurations. The hands-on labs include Basic Configuration of devices by using security best practices; Implementing VLANs and trunking in a switched network; Troubleshooting inter-VLAN routing on Layer 3 devices; Troubleshooting EtherChannel on switched links; Implementing DHCPv4 to operate across multiple LANs; Configuring switch security to mitigate LAN attacks; Implementing a WLAN using a wireless router and WLC; configuring and troubleshooting IPv4 and IPv6 floating static routes. Students who have completed or are enrolled in APIS 56 may not receive credit. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 151.

Recommended Course Preparation: CNT 8001 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP

CNT 8003 - Cisco CCNA3/3 Enterprise Networking, Security, and Automation v7.0 (ENSA)

3 units

This is course 3 of 3 of the Cisco CCNA Routing and Switching Certification Objectives. The concepts covered in this course include the operation of single-area OSPFv2 in both point-to-point and broadcast multi-access networks; vulnerabilities, threats, and exploits and how they can be mitigated to enhance network security; ACLs operation as part of a network security policy; WAN access technologies used to satisfy business requirements; VPNs and IPsec and their use to secure site-to-site and remote access connectivity; networking devices implementing QoS; Network Design and characteristics of scalable network architectures; network automation enabled through RESTful APIs and configuration management tools; purpose and characteristics of network virtualization. The hands-on labs include the implementation of single-area OSPFv2 in both point-to-point and broadcast multi-access networks; IPv4 ACLs to filter traffic and secure administrative access; NAT services on the edge router to provide IPv4 address scalability; network management protocols to monitor the network; and Troubleshooting LANs and enterprise networks. 45 hours lecture, 27 hours laboratory. Transfer: CSU; C-ID# ITIS 150.

Recommended Course Preparation: CNT 8002 with a minimum grade of C.

- Credit - Degree Applicable
- Grading Option: Letter or P/NP