Program Description

This career curriculum prepares students for entry-level positions in cybersecurity. Intended for those already employed in computing or who have a computing background, the certificate prepares the student to install, operate, and troubleshoot medium-sized router and switched networks including implementation and verification of connections to remote sites in a WAN. It includes basic introduction to wireless networking concepts and hands-on performance-based skills. The certificate instructs the student in basic and intermediate cybersecurity skills, such as how to develop a security infrastructure, recognize vulnerabilities to networks, and mitigate security threats. This cybersecurity curriculum emphasizes core security technologies and the installation, troubleshooting, and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices. It provides the foundation for students to sit for the following industry-recognized certifications: Network+, Security+, CCNA (Cisco Certified Network Associate), and the Cisco CCNA Security certification.

Program Outcomes

Upon completion of this program a student will be able to:

- Describe common network devices; the OSI model; common network protocols; features of LANs and WANs; types of network topologies; bandwidth.
- Describe characteristics of Ethernet networks; client/server networks; function of network devices; router serial ports; characteristics of WAN technologies.
- Describe basics of Ethernet technologies; framing process; MAC; CSMA/CD; types of duplex; 10/100/1000/10000BPS Ethernet technologies.
- Describe commands used to name a router, how administrators set passwords on a router, the use of the show commands, the command and steps required to configure a serial interface, the command and steps required to configure an Ethernet interface, how an administrator executes changes to a router, how an administrator saves changes to a router, the command and steps required to configure an interface description, the command and steps required to configure a log-in banner, the command and steps required to configure host tables, the purpose of backup documentation, and the steps for password recovery on a router.
- Describe the basic principles of routing, the difference between routed and routing protocols, what interior and exterior protocols are used for in routing, the difference between static versus dynamic routes, how static routes are configured, how default routes are configured, some methods for troubleshooting static route configurations, why dynamic routing protocols are necessary, distance vector routing, link-state routing, and how different routing protocols are used in context.
- Describe classless interdomain routing (CIDR); calculate subnets with variable-length subnet masking (VLSM); describe route aggregation with VLSM and Routing Information Protocol version 2 (RIPv2); configure, verify and troubleshoot RIPv2, EIGRP, and OSPF.
- Describe microsegmentation, how a switch learns addresses, and switch forwarding; describe switches and collision domains and switches and broadcast domains; configure LAN switches; verify LAN switch configuration; and manage LAN switches.
- Describe the goals of redundant topologies; define Spanning Tree Protocol (STP); describe the stages of spanning-tree port states and election of designated ports; describe the stages of selecting a root bridge; describe Path cost; set STP timers; explain how STP helps convergence; and describe Rapid Spanning Tree Protocol (RSTP).
- Explain what VLANs are; cite reasons to create VLANs and describe the benefits of VLANs; name and describe the methods of VLAN implementation; create, verify, and delete
VLAN configurations; describe basic VLAN troubleshooting methods.

• Explain the differences between LANs and WANs; identify the devices used in a WAN; list WAN standards; describe WAN encapsulation; classify the various WAN link options; differentiate between packet-switched and circuit-switched WAN technologies; describe the steps in WAN design.

• Identify and describe the basic components that define Point-to-Point Protocol (PPP) communication; define and describe the use of link control protocol (LCP) and Network Control Protocol (NCP) frames in PPP; describe the process for configuring and verifying PPP; describe and explain PPP authentication; define and describe the use of password authentication; define and describe the use of Challenge Handshake Authentication Protocol (CHAP).

• Describe Frame Relay services, standards, and components; describe Local Management Interface (LMI) features; describe the use of Frame Relay subinterfaces; configure, verify, and troubleshoot basic Frame Relay.

• Describe industry security terminology and acronyms, basic security vulnerabilities, and design and manage a security policy.

• Design and implement trust and identity technology at layer 2 and 3 of the OSI Model.

• Configure, monitor, and maintain advanced router firewall installation.

• Implement Secure Network Design.
Program Requirements
A suggested course sequence for full-time students follows. All students should review this advising guide and consult an advisor.

Program Requirements
  NWIT 151 - Introduction to Networking 3 semester hours
  NWIT 252 - Cisco Networking 2 3 semester hours
  NWIT 253 - Cisco Networking 3 3 semester hours
  NWIT 254 - Cisco Networking 4 3 semester hours
  NWIT 261 - CCNA SECURITY 4 semester hours

Total Credit Hours: 16