The Peninsula's Community College

Course Content Summary
ITN 109 – Internet and Network Foundations (3 Credits)

TNCC Cybersecurity Program web page: http://tncc.edu/programs/cyber-security

Course Description:

This course provides a basic comprehension of Internet and network technologies including IT job roles, connection methods, TCP/IP functionality and DNS. The content explores web server technologies with security and project management concepts. Topics include network creation, physical and logical topologies including media properties, server types, IP addressing and network security. Lecture 3 hours per week.

Statement of Purpose:

This course introduces the student to the basics of computer network operations and communications protocols. Students will learn how to install and configure basic networking technologies consistent with the job roles of network support technicians and entry-level network engineers. This course includes content that is directly related to the CompTIA Network+ industry certification and, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites / Corequisites:

ITE 120.

Required Text:

CompTIA Network+ Deluxe Study Guide for Exam N10-006 Third Edition.
Author: Lammle, Todd.
Publisher: Wiley Publishing, Inc.

COURSE OBJECTIVES

1.0 Explain the components, protocols, and services typically found on a network and how they are used in to create differing network topologies based on a given application. Demonstrate the ability to create a network topology based on given specifications.

2.0 Explain the use of network monitoring and performance tools in wired and wireless networks and demonstrate the ability to maintain an operating network and it constituent components.

3.0 Explain network risks, threats, and vulnerabilities and how they relate to network hardening techniques. Explain the network access control models and demonstrate the ability to install and configure network firewalls.

4.0 Explain network troubleshooting methodologies and given a scenario, demonstrate the ability to troubleshoot various network problems in wired and wireless topologies.

5.0 Explain basic network theory, protocols, models, and best practices. Demonstrate the installation and configuration of equipment in a given scenario using best practices.

STUDENT LEARNING OUTCOMES

1.0 Network Architecture

1.1 Explain the functions and applications of various network devices. **(NC4) (IT1) (IT2)**
1.2 Compare and contrast the use of networking services and applications. **(IT2)**
1.3 Install and configure common networking services/applications.
1.4 Explain the characteristics and benefits of various WAN technologies. **(NC3, NC7)**
1.5 Install and properly terminate various cable types and connectors using appropriate tools. **(NC2)**
1.6 Differentiate between common network topologies. **(NC7)**
1.7 Differentiate between network infrastructure implementations. **(NC3)**
1.8 Given a scenario, implement and configure the appropriate addressing schema.
1.9 Explain the basics of routing concepts and protocols. **(NC4)**
1.10 Identify the basics elements of unified communication technologies.
1.11 Compare and contrast technologies that support cloud and virtualization.
1.12 Given a set of requirements, implement a basic Local Area Network. **(NC3, NC7)**

2.0 Network operations

2.1 Given a scenario, use appropriate monitoring tools. **(NC5)**
2.2 Given a scenario, analyze metrics and reports from monitoring and tracking performance tools. **(NC5) (BD4)**
2.3 Given a scenario, use appropriate resources to support configuration management.
2.4 Explain the importance of implementing network segmentation.
2.5 Given a scenario, install and apply patches and updates.
2.6 Given a scenario, configure a switch using proper features. **(NC4) (SA5)**
2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.
2.8 Given a scenario, install and configure a router to simulate a WAN connection. **(NC4) (SA5)**

3.0 Network Security

3.1 Compare and contrast risk related concepts. **(NC8)**
3.2 Compare and contrast common network vulnerabilities and threats. **(NC8)**
3.3 Given a scenario, implement network hardening techniques. **(NC8)**
3.4 Compare and contrast physical security controls. **(NC8)**
3.5 Given a scenario, install and configure a basic firewall. **(NC4) (NC8) (SA5)**
3.6 Explain the purpose of various network access control models. **(NC8)**
3.7 Summarize basic forensic concepts. **(NC8)**

4.0 Troubleshooting

4.1 Given a scenario, implement the following network troubleshooting methodology.
4.2 Given a scenario, analyze and interpret the output of troubleshooting tools.
4.3 Given a scenario, troubleshoot and resolve common wireless issues.
4.4 Given a scenario, troubleshoot and resolve common copper cable issues.
4.5 Given a scenario, troubleshoot and resolve common fiber cable issues.
4.6 Given a scenario, troubleshoot and resolve common network issues.
4.7 Given a scenario, troubleshoot and resolve common security issues. **(NC8)**
4.8 Given a scenario, troubleshoot and resolve common WAN issues.

5.0 Industry Standards, Practices, and Network Theory

5.1 Analyze a scenario and determine the corresponding OSI layer. **(NC1) (NC6)**
5.2 Explain the basics of network theory and concepts.
5.3 Given a scenario, deploy the appropriate wireless standard. **(NC7)**
5.4 Given a scenario, deploy the appropriate wired connectivity standard.
5.5 Given a scenario, implement the appropriate policies or procedures.
5.6 Summarize safety practices.
5.7 Given a scenario, install and configure equipment in the appropriate location using best practices.
5.8 Explain the basics of change management procedures.
5.9 Compare and contrast operating ports and protocols. **(NC6)**
5.10 Given a scenario, configure and apply the appropriate ports and protocols. **(NC6)**

CAE2Y Knowledge Unit Domain Index

Course Content KU Indicator	CAE2Y KU Full Domain Name
BD	**Basic Data Analysis**
BS	**Basic Scripting**
CD	**Cyber Defense**
CT	**Cyber Threats**
FS	**Fundamental Security Design Principles**
IA	**Information Assurance Fundamentals**
IC	**Introduction to Cryptography**
IT	**Information Technology System Components**
NC	**Networking Concepts**
PL	**Policy legal Ethics and Compliance**
SA	**Systems Administration**

NOTE: the number following the KU Indicator represents the KU Domain topic as shown in the 2014 KU mapping matrix (Excel file).