

Inver Hills Community College

ITC 2530: Enterprise Networking, Security, and Automation

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites:

ITC 2520 - Switching, Routing, and Wireless Essentials (CCNA 2) (Minimum grade: 2.0 GPA equivalent); OR

ITC 2510 - Introduction to Networks (CCNA1) (Minimum grade: 2.0 GPA equivalent) AND ITC 2515 - Introduction to Networks and Routing and Switching Essentials (CCNA 1/2) AND ITC 2516 - Intro to Networks and Switching, Routing, and Wireless Essentials (CCNA1/2)

Corequisites: None

MnTC Goals: None

Explores the design, management, configuration, and troubleshooting of enterprise computer networks. This includes the ability to configure a dynamic routing protocol, access control lists, and NAT, as well as an understanding of wide area networking, VPNs, quality of service, network security, virtualization, and automation technologies. Enterprise Networking, Security, and Automation is the final in a sequence of three courses focusing on preparation for the Cisco Certified Network Associate (CCNA) certification.

B. COURSE EFFECTIVE DATES: 08/26/2013 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. OSPFv2 Concepts & Configuration 14%
Network Security and ACL Concepts, ACL and NAT Implementation 29%
WAN, VPN, and QoS Concepts 21%
Network Design, Management, and Troubleshooting 22%
Network Virtualization and Automation 14%

D. LEARNING OUTCOMES (General)

1. The student will be able to:
 - Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
 - Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
 - Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
 - Explain how ACLs are used as part of a network security policy.
 - Implement IPv4 ACLs to filter traffic and secure administrative access.
 - Implement NAT services on the edge router to provide IPv4 address scalability.
2.
 - Explain how WAN access technologies can be used to satisfy business requirements.
 - Explain how VPNs and IPsec are used to secure site-to-site and remote access connectivity.
 - Explain how networking devices implement QoS.
 - Implement network management protocols to monitor the network.
 - Explain the characteristics of scalable network architectures.
 - Troubleshoot enterprise networks using the layered model, a systematic process, and appropriate tools.
 - Explain the purpose and characteristics of network virtualization.
3.
 - Explain how network automation is enabled through RESTful APIs and configuration management tools.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted