IT C203: ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION (CISCO CCNA 3)

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070810 - Computer Networking
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Formerly: CST C203D. This is the third course in the Cisco Certified Network Associate (CCNA) curriculum series. It describes the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation. Students learn how to configure, troubleshoot, and secure enterprise network devices and understand how application programming interfaces (API) and configuration management tools enable network automation. Hands-on preparation for the CCNA exam is emphasized. ADVISORY: IT C202. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Explain concepts and terminology related to enterprise networks, security, and automaton.
2. Given a scenario configure a secure enterprise network.

Course Objectives

- 1. Configure single-area OSPFv2 in both point-to-point and multiaccess networks.
- 2. Explain how to mitigate threats and enhance network security using access control lists and security best practices.
- 3. Implement standard IPv4 ACLs to filter traffic and secure administrative access.
- 4. Configure NAT services on the edge router to provide IPv4 address scalability.
- 5. Explain techniques to provide address scalability and secure remote access for WANs.
- 6. Explain how to optimize, monitor, and troubleshoot scalable network architectures.
- 7. Explain how networking devices implement QoS.
- 8. Implement protocols to manage the network.
- 9. Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.

Lecture Content

Single-Area OSPFv2 Concepts Single-Area OSPFv2 Configuration Network Security Concepts ACL Concepts ACLs for IPv4 Configuration NAT for IPv4 WAN Concepts VPN and IPsec Concepts QoS Concepts Network Management Network Design Network Troubleshooting Network Virtualization Network Automation

Lab Content

Students will use enterprise switches and routers to design, build and test a secure network. Configure single-area OSPFv2 in both point-to-point and multiaccess networks. Implement standard IPv4 ACLs to filter traffic and secure administrative access. Configure NAT services on the edge router. Implement protocols to manage the network.

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion board student interactions, Internet problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

A. Read materials about computer networking from the Academy Curriculum.B. Read articles about the Cisco CLI (Command Line Interface)

Writing Assignments

A. Complete questions related to hands-on labs.

Out-of-class Assignments

A. Complete assigned labs using Packet Tracer.B. Compete assigned labs using Wireshark.

Demonstration of Critical Thinking

Given sets of operational data, the student will be able to critically analyze the data and make recommendations on how to improve the operations based on those findings.

Required Writing, Problem Solving, Skills Demonstration

Given a scenario, students will be able to troubleshoot a specific problem, write a detailed outline of the tasks that need to be accomplished to rectify the problem, complete the tasks as outlined, and test to determine if the problem has been solved.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years

of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Other Resources

1. Curriculum and labs are provided at cisco.netacad.com 2. Coastline Library 3. OER - Open Educational Resources.