CS 82.2C Course Outline as of Fall 2025

CATALOG INFORMATION

Dept and Nbr: CS 82.2C Title: ENT NET SEC
Full Title: Enterprise Networking, Security, and Automation
Last Reviewed: 2/22/2021

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	4.00	Lecture Scheduled	4.00	17.5	Lecture Scheduled	70.00
Minimum	4.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	4.00		Contact Total	70.00
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 140.00 Total Student Learning Hours: 210.00

Title 5 Category:	AA Degree Applicable
Grading:	Grade or P/NP
Repeatability:	00 - Two Repeats if Grade was D, F, NC, or NP
Also Listed As:	
Formerly:	CS 82.22C

Catalog Description:
This third and final course in the Cisco Certified Network Associate (CCNA) series 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.

Prerequisites/Corequisites:
Course Completion of CS 82.2B (or CS 82.22B)

Recommended Preparation:

Limits on Enrollment:

Schedule of Classes Information:
Description: This third and final course in the Cisco Certified Network Associate (CCNA) series 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. (Grade or P/NP)
Prerequisites/Corequisites: Course Completion of CS 82.2B (or CS 82.22B)
Recommended:
Limits on Enrollment:
Transfer Credit: CSU;
Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	**Area**			Effective:	Inactive:
CSU GE:	**Transfer Area**			Effective:	Inactive:
IGETC:	**Transfer Area**			Effective:	Inactive:
CSU Transfer:	Transferable	Effective:	Fall 2021	Inactive:	
UC Transfer:		Effective:		Inactive:	

CID:

Certificate/Major Applicable:
Both Certificate and Major Applicable

COURSE CONTENT

Student Learning Outcomes:
At the conclusion of this course, the student should be able to:
1. Configure, troubleshoot, and secure enterprise network devices
2. Differentiate application programming interfaces (APIs) and the configuration management tools that make network automation possible.

Objectives:
At the conclusion of this course, the student should be able to:

1. Configure single-area Open Shortest Path First (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 Access Control Lists (ACLs) to filter traffic and secure administrative access.
4. Configure Network Address Translation (NAT) services on the edge router to provide IPv4 address scalability.
5. Explain techniques to provide address scalability and secure remote access (such as Virtual Private Network (VPN) and Internet Protocol Security (IPSec)) for Wide Area Networks (WANs).
6. Explain how to optimize, monitor, and troubleshoot scalable network architectures.
7. Explain how networking devices implement Quality of Service (QoS).
8. Implement protocols to manage the network.

9. Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.

Topics and Scope:

I. Single-Area OSPFv2 Concepts
II. Single-Area OSPFv2 Configuration
III. Network Security Concepts
IV. ACL Concepts and Configuration
V. NAT for IPv4
VI. WAN Concepts
VII. Virtual Private Network (VPN) and Internet Protocol Security (IPSec) Concepts
VIII. QoS Concepts
IX. Network Management
X. Network Design
XI. Network Troubleshooting
XII. Network Virtualization
XIII. Network Automation

Assignment:

Reading assignments include:
1. Online research of security devices and deployment practices
2. Approximately 50 pages weekly from the textbook

Homework problems include:
1. Weekly online discussion thread participation
2. Hands-on exercises and class performances to demonstrate proficiency with topics
3. Online quizzes
4. Creation of security design diagrams and layouts

Other assignments include:
1. Quizzes (9 - 11) and skill demonstration exam
2. Classroom scenario-based exercises

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Weekly written online discussions	Writing 5 - 10%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Homework problems, Creation of network, operating system and security design diagrams and layouts	Problem solving 15 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

Skill demonstration exam	Skill Demonstrations 20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

Quizzes and skill demonstration exam	Exams 20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Attendance and participation in scenario based exercises	Other Category 5 - 20%

Representative Textbooks and Materials:
Enterprise Networking, Security, and Automation Companion Guide (CCNAv7). Cisco Networking Academy. Cisco Press. 2020
Enterprise Networking, Security, and Automation Course Booklet (CCNAv7). Cisco Networking Academy. Cisco Press. 2020