



## MASTER COURSE OUTLINE

Prepared By: Arthur Wanner/Tom Willingham

Date: March 2020

## COURSE TITLE

Cisco Networking: Enterprise Networking, Security, and Automation

## GENERAL COURSE INFORMATION

Dept.: CS

Course Num: 173

(Formerly: CS 156)

CIP Code: 11.0901

Intent Code: 21

Program Code: 527

Credits: 6

Total Contact Hrs Per Qtr.: 88

Lecture Hrs: 44

Lab Hrs: 44

Other Hrs:

Distribution Designation: General Elective (GE)

## COURSE DESCRIPTION (as it will appear in the catalog)

This course helps students develop workforce readiness skills and build a foundation for success in networking-related careers and degree programs. Students learn, apply, and practice CCNA knowledge and skills through a series of in-depth hands-on experiences and simulated activities including comprehensive networking concepts and skills, from network applications to the protocols and services provided to those applications. Upon completion of CS 171, CS172, and CS 173, learners will be prepared to take the Cisco CCNA Unified certification exam.

## PREREQUISITES

CS 172

## TEXTBOOK GUIDELINES

Textbook and materials to be determined by CS Faculty

## COURSE LEARNING OUTCOMES

*Upon successful completion of the course, students should be able to demonstrate the following knowledge or skills:*

1. Explain how single-area OSPF operates in both point-to-point and broadcast multi-access networks.
2. Implement single-area OSPFv2 in both point-to-point and broadcast multi-access networks.
3. Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
4. Explain how ACLs are used as part of a network security policy.
5. Implement IPv4 ACLs to filter traffic and secure administrative access.
6. Configure NAT services on the edge router to provide IPv4 address scalability.
7. Explain how WAN access technologies can be used to satisfy business requirements.
8. Explain how VPNs and IPsec secure site-to-site and remote access connectivity.
9. Explain how networking devices implement QoS.
10. Implement protocols to manage the network.
11. Explain the characteristics of scalable network architectures.
12. Troubleshoot enterprise networks.
13. Explain the purpose and characteristics of network virtualization.
14. Explain how network automation is enabled through RESTful APIs and configuration management tools

## INSTITUTIONAL OUTCOMES

- IO1 **Communication:** Students will be able to communicate clearly and effectively within a workplace context
- IO2 **Quantitative Reasoning:** Analyze and solve computational problems using a modern program language
- IO3 **Human Relations/Workplace Skills:** Students will be able to demonstrate teamwork, ethics, appropriate safety awareness and/or workplace specific skills

### **COURSE CONTENT OUTLINE**

1. Single-Area OSPFv2 Concepts
2. Single-Area OSPFv2 Configuration
3. WAN Concepts
4. Network Security Concepts
5. ACL Concepts
6. ACLs for IPv4 Configuration
7. NAT for IPv4
8. VPN and IPsec Concepts
9. QoS Concepts
10. Network Management
11. Network Design
12. Network Troubleshooting
13. Network Virtualization
14. Network Automation

### **DEPARTMENTAL GUIDELINES** *(optional)*

This is the third course in the newly revised Cisco Networking Academy CCNAv7 Routing and Switching curricula. Students will be prepared to take the Cisco CCNA® certification exam after completing CS 171, CS 172 and CS 173.

---

**DIVISION CHAIR APPROVAL**

---

**DATE**