Tom P. Haney Technical College
Enterprise Network and Server Support Technology (ENSST)
Program Type: Career Preparatory - Information Technology
Program Number: Y300500
Program Length: 750 hours

Class of '26-'27
Instructor: Mr. Jim Spring
sprinjg@bay.k12.fl.us
Mr. Reagan Oman
omanre@bay.k12.fl.us
(850) 767-5500 ext. 212-3218
Monday through Friday; 7am to 12pm

OCP B.3 – Interconnecting Cisco Networking Devices (CTS0094 - 600 Hours)

Cisco CCNA3: Enterprise Networking, Security, and Automation Essentials Ver. 7.0

COURSE DESCRIPTION

The courses in the CCNA Version 7.0 curriculum help students develop a comprehensive foundation for designing, securing, operating, and troubleshooting modern computer networks, on the scale from small business networks to enterprise networks, with an emphasis on hands-on learning and essential career skills like problem solving and collaboration.

The third course in the CCNAv7.02 curriculum describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access. ENSA also introduces software-defined networking, virtualization, and automation concepts that support the digitalization of networks. Students gain skills to configure and troubleshoot enterprise networks and learn to identify and protect against cybersecurity threats. They are introduced to network management tools and learn key concepts of software-defined networking, including controller-based architectures and how application programming interfaces (APIs) enable network automation.

GRADING SCALE	OCP A WEIGHTED GRADE CALCULATION
A = 90-100%	Canvas Lab Assignments and Skills Assessment = 35%
B = 80-89%	NetAcad Module Quizzes (Formative) = 10%
C = 70-79%	NetAcad CheckPoint and Final Exams (Summative) = 40%
F = 0-69%	Employability Skills = 15%

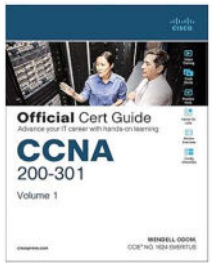
NOTE: Your weighted grade in each OCP must be greater than or equal to 80% to pass this course.

COURSE ORGANIZATION

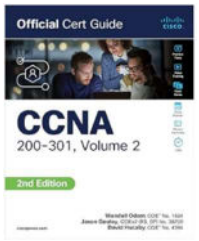
This instructor-led course utilizes online course materials via *haney.instructure.com* (Canvas) and Cisco's *NetAcad.com* meaning that most activities are completed online. This course is designed to prepare the student to take the Cisco Certified Network Associate (CCNA) certification exam. All email correspondence with students will take place via their student email account. Students need to check this email daily for information from the instructor and the college. Students will also need to log into Canvas daily to check for new announcements regarding any changes or information about instructional material and activities and to upload their completed lab assignments. After every couple of NetAcad course chapters, students will complete the CheckPoint Exam Assessments. These assessments have been set up in NetAcad in quiz format for easier grading. These assessments will have a time limit and allow for two submissions. Once a student has submitted their assessment, they will be able to view their grade and decide whether they would like to attempt the assessment a second time. Students will not be able to view the answers to the assessments until after the due date has passed for the assessment. The highest grade between the two attempts counts. Students will also complete hands-on labs to practice the skills learned in the lesson. Students will be assigned to a Cisco "pod" consisting of two Cisco switches, two Cisco routers and two computer workstations which are used to complete hands-on labs. Students will also use Cisco's Packet Tracer virtual environments to complete virtual lab assignments. The provided lab worksheets MUST be completed along with each lab and must be submitted via Canvas. A final exam *and* a final skills assessment will also be administered that covers all topics covered in class.

REQUIRED TEXTS:

No textbook is required for this class. Below is a list of recommended reference books that can help you in class and/or study for your certification exam.



CCNA 200-301 Official Cert Guide, Volume 1 by Wendell Odom



CCNA 200-301 Official Cert Guide, Volume 2 by Wendell Odom, et. al.

ATTENDANCE POLICY

Students are required to attend class Monday through Friday, 7 AM to 12 PM. Class will begin at 7 AM with morning announcements and chapter reviews. It is important to be on time each day. College policy requires that a student be present 90% of the enrollment period designated hours. For ENSST, an enrollment period is 375 hours (one semester), therefore a student is allowed to miss 37.5 hours per semester. If a student exceeds 37.5 hours absence in an enrollment period, the student will be withdrawn from the ENSST program. This policy is not negotiable. Withdrawal exceptions cannot and will not be made for any student exceeding their allowed 10% absences. Students will be responsible for any missed work or assignments. NOTE: Military veterans or dependents using VA assistance have a different attendance policy. Please refer to the Tom P. Haney Student Handbook for more information on Haney's attendance policy.

ACADEMIC INTEGRITY

Tom P. Haney Technical College is committed to providing an honest and fair learning environment and to preparing students for academic and career success. Students are expected to recognize and uphold standards of intellectual and academic integrity. Integrity means being honest, responsible, respectful, and ethical, and applies whether working independently or collaboratively, regardless of the level of supervision. Integrity and honesty are a part of professionalism and demonstrate employability skills. The College will not tolerate any dishonest practices, including plagiarism, in the academic environment.

ELECTRONIC DEVICE POLICY

- Cell phones are not allowed to be used in the classroom. Students will be able to store their cell phones in a cell phone locker in the back of the classroom. Students are allowed to use their cell phones outside of class when on breaks or at lunch. Please refer to Haney's Student Handbook for more information on our cell phone policy.
- Personal laptops and tablets are not allowed to be used in the classroom. If laptops are required in this course, the college will provide one per student. Students are not allowed to take their assigned laptops home for any reason and must be placed in the laptop cart at the end of the day.

FOOD AND DRINK POLICY

Food is not allowed in the classroom. Snacks and lunches are to be eaten in the Bldg 3 atrium or outside while on breaks. Water is allowed in class provided you use a container with a secured top such as water bottles, Tervis or Stanley tumblers. Fast food cups and aluminum cans are not considered secure containers. If you doubt your drink container is allowed, then ask your instructor.

STUDENTS WITH DISABILITIES STATEMENT

If you have a disability that may affect your academic performance and are seeking accommodations, it is your responsibility to inform the Student Services (Bldg 1). You may contact Ms. Sandy Johnson at (850) 767-5500 ext. 767-5527 if you have any questions concerning

accommodations and services. You may visit the Disability Services webpage or the Disability Services section of the Student Handbook to learn more about accommodations and special services. It is important to request accommodations early enough to give the Counseling Services office adequate time to consider your request and recommend reasonable accommodations. Students are encouraged to initiate the request process as soon as possible at the beginning of a semester or class. Accommodations are not retroactive and only become active after all required documents are submitted. Instructors will provide necessary accommodations based solely on the recommendations of the Disability Services office.

COURSE MODULES AND OBJECTIVES

Listed below are the current set of modules and their associated competencies outlined for this course. Each module is an integrated unit of learning that consists of content, activities and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency.

Module 1 – Single-Area OSPFv2 Concepts	Describe basic OSPF features and characteristics. Describe the OSPF packet types used in single-area OSPF. Explain how single-area OSPF operates.
Module 2 – Single-Area OSPFv2 Configuration	Configure an OSPFv2 router ID. Configure single-area OSPFv2 in a point-to-point network. Configure the OSPF interface priority to influence the DR/BDR election in a multiaccess network. Implement modifications to change the operation of single-area OSPFv2. Configure OSPF to propagate a default route. Verify a single-area OSPFv2 implementation.
CheckPoint Exam: OSPF Concepts and Configuration	
Module 3 – Network Security Concepts	Describe the current state of cybersecurity and vectors of data loss. Describe the threat actors who exploit networks. Describe tools used by threat actors to exploit networks. Describe malware types. Describe common network attacks. Explain how IP vulnerabilities are exploited by threat actors.

	Explain how TCP and UDP vulnerabilities are exploited by threat actors. Explain how IP services are exploited by threat actors. Describe best practices for protecting a network. Describe common cryptographic processes used to protect data in transit.
Module 4 – ACL Concepts	Explain how ACLs filter traffic. Explain how ACLs use wildcard masks. Explain how to create ACLs. Compare standard and extended IPv4 ACLs.
Module 5 – ACLs for IPv4 Configuration	Configure standard IPv4 ACLs to filter traffic to meet networking requirements. Use sequence numbers to edit existing standard IPv4 ACLs. Configure a standard ACL to secure vty access. Configure extended IPv4 ACLs to filter traffic according to networking requirements.
CheckPoint Exam: Network Security	
Module 6 – NAT for IPv4	Explain the purpose and function of NAT. Explain the operation of different types of NAT. Describe the advantages and disadvantages of NAT. Configure static NAT using the CLI. Configure dynamic NAT using the CLI. Configure PAT using the CLI. Describe NAT for IPv6.
Module 7 – WAN Concepts	Explain the purpose of a WAN. Explain how WANs operate. Compare traditional WAN connectivity options. Compare modern WAN connectivity options. Compare internet-based WAN connectivity options.

Module 8 – VPN and IPsec Concepts	Describe benefits of VPN technology. Describe different types of VPNs Explain how the IPsec framework is used to secure network traffic.
CheckPoint Exam: WAN Concepts	
Module 9 – QOS Concepts	Explain how network transmission characteristics impact quality. Describe minimum network requirements for voice, video, and data traffic. Describe the queuing algorithms used by networking devices. Describe the different QoS models. Explain how QoS uses mechanisms to ensure transmission quality.
Module 10 – Network Management	Use CDP to map a network topology. Use LLDP to map a network topology. Implement NTP between an NTP client and NTP server. Explain SNMP operation. Explain syslog operation. Use commands to back up and restore an IOS configuration file. Perform an upgrade of an IOS system image.
Module 11 – Network Design	Explain how data, voice, and video are converged in a switched network. Explain considerations for designing a scalable network. Explain how switch hardware features support network requirements. Describe the types of routers available for small to-medium-sized business networks.
Module 12 – Network Troubleshooting	Explain how network documentation is developed and used to troubleshoot network issues. Compare troubleshooting methods that use a systematic, layered approach. Describe different networking troubleshooting tools. Determine the symptoms and causes of network problems using a layered model. Troubleshoot a network using the layered model.

CheckPoint Exam: Optimize, Monitor, and Troubleshoot Networks	
Module 13 – Network Virtualization	Explain the importance of cloud computing. Explain the importance of virtualization. Describe the virtualization of network devices and services. Describe software-defined networking. Describe controllers used in network programming.
Module 14 – Network Automation	Describe automation. Compare JSON, YAML, and XML data formats. Explain how APIs enable computer to computer communications. Explain how REST enables computer to computer communications. Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack Explain how Cisco DNA center enables intent-based networking.
CheckPoint Exam: Emerging Network Technologies	
CCNA: Enterprise Networking, Security, and Automation Practice Final Exam	
CCNA: Enterprise Networking, Security, and Automation Final Exam	
CCNA: Enterprise Networking, Security, and Automation Practice Final Skills Assessment	
CCNA: Enterprise Networking, Security, and Automation Final Skills Assessment	

NOTE: This syllabus may change at the instructor's discretion. It is the responsibility of the student to record changes.