Class of '26-'27

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

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 A - Advanced Networking Fundamentals (CTS0099 - 150 Hours)
Cisco Networking Essentials - Ver. 3.0

COURSE DESCRIPTION

This course teaches the fundamentals of networking. It covers the foundation of networking and network devices, how to use different network applications and protocols to accomplish networking tasks, how to provide Internet Protocol (IP) addresses to devices both manually and automatically and understand how IP addresses are calculated and assigned, how the physical, data link, and network layers work together to provide end-to-end connectivity, how to provide basic network diagnostics and troubleshooting including endpoints, networks, for both local and remote scenarios, will teach foundations of security and about network and computer threats and attacks including application, cyber, wireless, and mobile device attacks, and how to perform basic secure wireless configuration.

GRADING SCALE

A = 90-100%
B = 80-89%
C = 70-79%
F = 0-69%

OCP A WEIGHTED GRADE CALCULATION

Canvas Lab Assignments and Skills Assessment = 35%
NetAcad Module Quizzes (Formative) = 10%
NetAcad CheckPoint and Final Exams (Summative) = 40%
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 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.
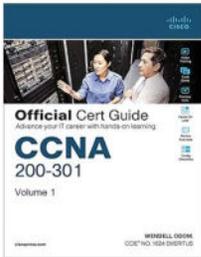
CCNA 200-301 Official Cert Guide, Volume 1 by Wendell Odom

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.

OVERALL COURSE OBJECTIVES

The Networking Essentials course is designed for people who want to learn the knowledge and skills they need to work in Information Technology (IT) and networking. These course materials will assist you in developing the skills necessary to do the following:

- Explain important concepts in network communication.

- Explain network types, components, and connections.

- Configure mobile devices for wireless access.

- Configure an integrated wireless router and wireless client to connect securely to the internet.

- Explain the importance of standards and protocols in network communications.

- Describe common network media.

- Explain how communication occurs on Ethernet networks.

- Explain the features of an IP address.

- Explain how IPv4 addresses are used in network communication and segmentation.

- Explain features of IPv6 addressing.

- Configure a DHCP server.

- Explain how routers connect networks together.

- Explain how ARP enables communication on a network.

- Create a fully connected LAN.

- Explain how clients access internet services.

- Explain the function of common application layer services.

- Use various tools to test and troubleshoot network connectivity.

- Explain components of a hierarchical network design.

- Explain the characteristics of virtualization and cloud services.

- Calculate numbers between decimal, binary, and hexadecimal systems.

- Explain how Ethernet operates in a switched network.

- Explain how routers use network layer protocols and services to enable end-to-end connectivity.

- Explain how ARP enables communication on a local area network.

- Explain how DNS and DHCP services operate.

- Compare the operations of transport layer protocols in supporting end-to-end communication.

- Use the Cisco IOS.

- Build a simple computer network using Cisco devices.

- Use various tools to test network connectivity.

- Explain how physical layer protocols, services, and network media support communications across data networks.

- Explain how media access control in the data link layer supports communication across physical and logical networks.

- Explain how routers use network layer protocols and services to enable end-to-end connectivity.

- Calculate an IPv4 subnetting scheme to efficiently segment a network.

- Implement an IPv6 addressing scheme.

- Explain how ND enables communication on a network.

- Describe Cisco routers and switches.

- Troubleshoot basic network connectivity issues.

- Demonstrate effective troubleshooting methodologies and help desk best practices.

- Explain common threats, vulnerabilities, and attacks on end points.

- Configure secure user access on a network.

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 - Communications in a Connected World	Explain important concepts in network communication. Explain the concept of a network. Describe network data. Explain the network transmission speed and capacity.
Module 2 - Network Components, Types, and Connections	Explain network types, components, and connections. Explain the roles of clients and servers in a network. Explain the roles of network infrastructure devices. Describe ISP connectivity options.
Module 3 - Wireless and Mobile Networks	Configure mobile devices for wireless access. Describe the different types of networks used by cell phones and mobile devices. Configure mobile devices for wireless connectivity.
Module 4 - Build a Home Network	Configure a wireless router and wireless client to connect securely to the internet. Describe the components required to build a home network. Describe wired and wireless network technologies. Describe Wi-Fi. Configure wireless devices for secure communications.
CheckPoint Exam: Build a Small Network	
Module 5 - Communication Principles	Explain the importance of standards and protocols in network communications. Describe network communication protocols.

	Describe network communication standards. Compare the OSI and TCP/IP models.
Module 6 - Network Media	Describe common network media. Describe common types of network cables.
Module 7 - The Access Layer	Explain how communication occurs on Ethernet networks. Explain the process of encapsulation and Ethernet framing. Explain how to improve network communication at the access layer.
CheckPoint Exam: Network Access	
Module 8 - The Internet Protocol	Explain the features of an IP address. Explain the purpose of an IPv4 address. Explain how IPv4 addresses and subnets are used together.
Module 9 - IPv4 and Network Segmentation	Explain how IPv4 addresses are used in network communication and segmentation. Compare the characteristics of the unicast, broadcast and multicast IPv4 addresses. Explain public, private, and reserved IPv4 addresses. Explain how subnetting segments a network to enable better communication.
Module 10 - IPv6 Addressing Formats and Rules	Explain features of IPv6 addressing. Explain the need for IPv6 addressing. Explain how to represent IPv6 addresses.
Module 11 - Dynamic Addressing with DHCP	Configure a DHCP server. Compare static and dynamic IPv4 addressing. Configure a DHCPv4 server to dynamically assign IPv4 addresses.
CheckPoint Exam: The Internet Protocol	

Module 12 - Gateways to Other Networks	Explain how routers connect networks together. Describe network boundaries. Explain the purpose of Network Address Translation in small networks.
Module 13 - The ARP Process	Explain how ARP enables communication on a network. Compare the roles of the MAC address and the IP address. Explain why it is important to contain broadcasts within a network.
Module 14 - Routing Between Networks	Create a fully connected LAN. Explain the need for routing. Explain how routers use tables. Build a fully connected network.
CheckPoint Exam: Communication Between Networks	
Module 15 - TCP and UDP	Explain how clients access internet services. Compare TCP and UDP transport layer functions. Explain how TCP and UDP use port numbers.
Module 16 - Application Layer Services	Explain the function of common application layer services. Explain client and server interaction. Describe common network applications. Describe DNS. Describe HTTP and HTML. Describe FTP. Describe Telnet and SSH. Describe email protocols.
Module 17 - Network Testing Utilities	Use various tools to test and troubleshoot network connectivity. Troubleshoot using network utilities.

Module 18 - Network Design	Explain components of a hierarchical network design. Describe the four basic requirements of a reliable network. Explain the function at each layer of the 3-layer network design model.
Module 19 - Cloud and Virtualization	Explain the characteristics of virtualization and cloud services. Explain the characteristics of clouds and cloud services. Explain the purpose and characteristics of virtualization
Module 20 - Number Systems	Calculate numbers between decimal, binary, and hexadecimal systems. Calculate numbers between decimal and binary systems Calculate numbers between decimal and hexadecimal systems.
CheckPoint Exam: Characteristics of Network Design	
Module 21 - Ethernet Switching	Explain how Ethernet operates in a switched network. Explain the OSI model Layer 1 and Layer 2 functions in an Ethernet network. Explain how the Ethernet sublayers are related to the frame fields. Explain the types of Ethernet MAC addresses. Explain how a switch builds its MAC address table and forwards frames.
Module 22 - Network Layer	Explain how routers use network layer protocols to enable end-to-end connectivity. Explain how the network layer uses IP protocols for reliable communications. Explain the role of the major header fields in the IPv4 packet. Explain the role of the major header fields in the IPv6 packet.
Module 23 - IPv4 Address Structure	Calculate an IPv4 subnetting scheme to efficiently segment a network. Describe the structure of an IPv4 address (network ID, host ID, and the subnet mask).
CheckPoint Exam: Network Addressing	

Module 24 - Address Resolution	Explain how ARP enables communication on a local area network. Describe the purpose of ARP.
Module 25 - IP Addressing Services	Explain how DNS and DHCP services operate.
Module 26 - Transport Layer	Compare the operations of transport layer protocols in supporting end-to-end communication. Explain the purpose of the transport layer in managing the transportation of data in end-to-end communication. Explain characteristics of TCP. Explain characteristics of UDP. Explain how TCP and UDP use port numbers. Explain how TCP session establishment and termination processes facilitate reliable communication. Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery. Describe the UDP client processes to establish communication with a server.
CheckPoint Exam: ARP, DNS, DHCP and the Transport Layer	
Module 27 - The Cisco IOS Command Line	Use the Cisco IOS. Use correct commands to navigate the Cisco IOS modes. Explain how to navigate the Cisco IOS to configure network devices. Use show commands to monitor device operations.
Module 28 - Build a Small Cisco Network	Build a simple computer network using Cisco devices. Configure initial settings on a Cisco switch. Configure initial settings on a router. Configure devices for secure remote management. Configure devices to use the default gateway.

Module 29 - ICMP	Use various tools to test network connectivity. Explain how ICMP is used to test network connectivity. Use ping and traceroute utilities to test network connectivity.
CheckPoint Exam: Configure Cisco Devices	
Module 30 - Physical Layer	Explain how physical layer protocols, services, and network media support communications across data networks. Describe the purpose and functions of the physical layer in the network. Describe characteristics of the physical layer. Identify the basic characteristics of copper cabling. Explain how UTP cable is used in Ethernet networks. Describe fiber-optic cabling and its main advantages over other media.
Module 31 - Data Link Layer	Explain how media access control in the data link layer supports communication across physical and logical networks. Compare the characteristics of physical and logical topologies. Explain how devices access a LAN in order to send frames.
Module 32 - Routing at the Network Layer	Explain how routers use network layer protocols and services to enable end-to-end connectivity. Explain how network devices use routing tables to direct packets to a destination network. Explain the function of fields in the routing table of a router.k.
CheckPoint Exam: Physical, Data Link, and Network Layers	
Module 33 - IPv6 Addressing	Implement an IPv6 addressing scheme. Compare types of IPv6 network addresses. Explain how to configure static global unicast and link-local IPv6 network addresses. Explain how to configure global unicast addresses dynamically.

	Configure link-local addresses dynamically. Identify IPv6 addresses.
Module 34 - IPv6 Neighbor Discovery	Explain how ND enables communication on a network. Describe the operation of IPv6 neighbor discovery.
CheckPoint Exam: IP Addressing	
Module 35 - Cisco Switches and Routers	Describe Cisco routers and switches. Describe Cisco LAN switches. Describe switch forwarding methods and port settings available on Layer 2 switch ports. Describe the Cisco LAN switch boot process. Describe Cisco small business routers. Describe the Cisco router boot process.
Module 36 - Troubleshoot Common Network Problems	Troubleshoot basic network connectivity issues. Describe some of the approaches used to troubleshoot networks. Describe the process of detecting physical layer problems. Troubleshoot a wireless network problem. Explain common internet connectivity problems. Explain how to use outside sources and internet resources for troubleshooting.
CheckPoint Exam: Cisco Devices and Troubleshooting Network Issues	
Module 37 - Network Support	Demonstrate effective troubleshooting methodologies and help desk best practices. Demonstrate effective troubleshooting methodologies. Create network documentation. Explain help desk best practices. Explain how to verify network connectivity in the operating systems of Linux, Mac, Android, and Apple devices.

	Troubleshoot a Network. Explain how to troubleshoot connectivity remotely.
Module 38 - Cybersecurity Threats, Vulnerabilities, and Attacks	Explain common threats, vulnerabilities, and attacks on end points. Explain the threats, vulnerabilities, and attacks that occur in the various domains. Describe the different deception methods used by attackers to deceive their victims. Describe common types of network attacks. Describe common types of wireless and mobile device attacks. Describe types of application attacks.
Module 39 - Network Security	Configure secure user access on a network. Explain foundational security concepts. Configure access control. Explain cybersecurity processes and procedures that protect systems. Explain methods of mitigating malware. Explain how firewalls operate to filter traffic and recommend endpoint security measures. Configure basic wireless security on a home router (WPAx).
Networking Essentials: Course Final Exam	

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