COURSE OUTLINE: CYB204 - CISCO TECHNOLOGIES

Prepared: IT Studies
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	CYB204: CISCO TECHNOLOGIES (CCNA)
Program Number: Name	2198: CYBERSECURITY 5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2024-2025
Course Description:	In this course, students learn key LAN, WAN, and WLAN concepts, as well as their configuration using Cisco routers and switches. Moreover, students learn how to manage IP configuration, mitigate security threats, and automate the configuration of networks. Through this course, students will be introduced to topics included on the Cisco Certified Network Associate (CCNA) certification exam.
Total Credits:	6
Hours/Week:	6
Total Hours:	84
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2198 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security VLO 4 Select and deploy optimal security appliances and technologies to safeguard an organization’s network **5911 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data. VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and2.incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization. VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security solutions. VLO 4 Select and deploy optimal security appliances and technologies to safeguard an organization’s network.

Essential Employability Skills (EES) addressed in this course:	EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 10 Manage the use of time and other resources to complete projects.
Course Evaluation:	Passing Grade: 50%, D A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation & Assessment Requirements:	A+ = 90-100% A = 80-89% B = 70-79% C = 60-69% D = 50-59% F < 50% Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test. If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test. Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information. In order to qualify to write a missed test, the student shall have: a.) attended at least 75% of the classes to-date. b.) provide the professor an acceptable explanation for his/her absence. c.) be granted permission by the professor. NOTE: The missed test that has met the above criteria will be an end-of-semester test. Labs / assignments are due on the due date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in advance, during class. Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable. It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade. Students are expected to be present to write in-classroom quizzes. There are no make-up

options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which can be up to 50 minutes after class starts or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Books and Required Resources:

Cisco CCNA Certification: Exam 200-301, 2 Volume Set by Todd Lammie
Publisher: Sybex (Wiley)
ISBN: 978-1-119-67761-1

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
1. Explore fundamental network concepts and configure network components.	1.1 Explain the role and function of network components. 1.2 Describe the characteristics of network topology architectures. 1.3 Compare physical interface and cabling types. 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed). 1.5 Compare TCP to UDP. 1.6 Configure and verify IPv4 addressing and subnetting. 1.7 Describe the need for private IPv4 addressing. 1.8 Configure and verify IPv6 addressing and prefix. 1.9 Compare IPv6 address types. 1.10 Verify IP parameters for Client OS (Windows, macOS, Linux). 1.11 Describe wireless principles. 1.12 Explain virtualization fundamentals (virtual machines). 1.13 Describe switching concepts.
Course Outcome 2	**Learning Objectives for Course Outcome 2**
2. Configure and verify network access protocol standards and best practices.	2.1 Configure and verify VLANs (normal range) spanning multiple switches. 2.2 Configure and verify inter-switch connectivity. 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP). 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP). 2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations. 2.6 Compare Cisco Wireless Architectures and AP modes. 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG). 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS). 2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation,

	security settings, QOS profiles, and advanced WLAN settings.
Course Outcome 3	**Learning Objectives for Course Outcome 3**
3. Interpret the components of a routing table and configure and verify IP connectivity.	3.1 Interpret the components of routing table. 3.2 Determine how a router makes a forwarding decision by default. 3.3 Configure and verify IPv4 and IPv6 static routing. 3.4 Configure and verify single area OSPFv2. 3.5 Examine the purpose of first hop redundancy protocol.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
4. Configure and verify various IP services.	4.1 Configure and verify inside source NAT using static and pools. 4.2 Configure and verify NTP operating in a client and server mode. 4.3 Explain the role of DHCP and DNS within the network. 4.4 Explain the function of SNMP in network operations. 4.5 Describe the use of syslog features including facilities and levels. 4.6 Configure and verify DHCP client and relay. 4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping. 4.8 Configure network devices for remote access using SSH. 4.9 Describe the capabilities and function of TFTP/FTP in the network.
Course Outcome 5	**Learning Objectives for Course Outcome 5**
5. Assess security concepts and program elements and configure multiple security features.	5.1 Elaborate key security concepts (threats, vulnerabilities, exploits, and mitigation techniques). 5.2 Describe security program elements (user awareness, training, and physical access control). 5.3 Configure device access control using local passwords. 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics). 5.5 Describe remote access and site-to-site VPNs. 5.6 Configure and verify access control lists. 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security). 5.8 Differentiate authentication, authorization, and accounting concepts. 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3). 5.10 Configure WLAN using WPA2 PSK using the GUI.
Course Outcome 6	**Learning Objectives for Course Outcome 6**
6. Evaluate the impact of automation and programmability on network	6.1 Explain how automation impacts network management. 6.2 Compare traditional networks with controller-based networking.

	management.	6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric). 6.4 Compare traditional campus device management with Cisco DNA Center enabled device management. 6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding). 6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible. 6.7 Interpret JSON encoded data.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Labs and Assignments	40%
Quizzes	10%
Test #1	25%
Test #2	25%

Date: June 16, 2024

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.