

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 262 – WIRELESS NETWORKING

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description

Covers WLAN (Wireless Local Area Network) topics including basic wireless principles, wireless technology concepts, wireless networking devices, 802.11 antenna technology, and WLAN Security. Introduces 802.11 WLAN communication technologies available today. Along with learning wireless technology terms, concepts and principles, students will get hands-on experience configuring a variety of WLAN networking devices and topologies. The CWNA certification is the foundation level enterprise Wi-Fi certification for the Certified Wireless Network Professional (CWNP) program, and is required for the Certified Wireless Security Professional (CWSP) and Certified Wireless Networking Expert (CWNE) certifications.

Prerequisite

“C” grade or higher or “Pass” in CIS120, CIS121, and CIS125; or successful completion of CIS 201; or equivalent or possess current CCNA or CCNET certification or two years verifiable network administration experience

Recommended Preparation

“C” grade or higher or “Pass” in CIS 190, 202 or equivalent

Entrance Skills

Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:

- 1) Describe and explain the concepts of networking and types of network topologies.
- 2) Demonstrate skill in planning, designing, implementing, optimizing and troubleshooting basic computer networks.
- 3) Describe the purpose and basic characteristics of each of the 7 layers of the OSI networking model.
- 4) Demonstrate skill in calculating and implementing IPv4 addressing and subnetting.
- 5) Describe and explain the implementation, structure, and use of LANs, MANs and WANs.
- 6) Describe and explain the functions of repeaters, hubs, bridges, switches, routers and gateways, and the OSI Model layers at which they operate.

Course Content

- 1) Radio Frequency (RF) Technologies
- 2) IEEE 802.11 Regulations and Standards
- 3) IEEE 802.11 Protocols and Devices
- 4) IEEE 802.11 Network Implementation
- 5) IEEE 802.11 Network Security
- 6) IEEE 802.11 RF Site Surveying

Course Objectives

Students will be able to:

- 1) Define and describe the concepts, protocols, standards, and regulations associated with IEEE 802.11 WLAN radio technologies and topologies.
- 2) Describe the 802.11 wireless radio system components and factors necessary for Wireless LAN communication.
- 3) Describe WLAN security threats, vulnerabilities and basic security mitigation features.
- 4) Describe the strengths, weaknesses, appropriate uses, and implementation of the IEEE 802.11 WLAN security-related mechanisms.
- 5) Install and configure basic IEEE 802.11 WLAN topologies consisting of access points, routers, switches, WLAN controllers and client adapters
- 6) Perform the basic elements of a site survey.

Method of Evaluation

A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.

- 1) Written quizzes and exams that measure students' ability to describe WLAN technologies, functions and characteristics, and analyze a scenario and choose the alternatives and troubleshooting options.
- 2) Scenario-based lab activities that measure students' ability to configure WLAN functions.
- 3) Practical application-based examinations that measure students' ability to install a scenario-based WLAN topology; analyze the topology and determine configuration requirements/problems; configure a WLAN topology using WLAN controller GUI to achieve the correct requirements of the scenario.

Special Materials Required of Student

Electronic storage media

Minimum Instructional Facilities

Computer lab: computers must have Internet connectivity, wired and wireless NICs, and appropriate software; VLAN connectivity not connected to school academic resources; WLAN controllers, wireless access points, wireless routers, wired switches or hubs, access routers, USB wireless client adapters, and interconnecting CAT 5E cabling; whiteboards; computers not connected to the school academic network resources; overhead computer projection system, screen, printer; computer server; storage cabinets.

Method of Instruction

- 1) Instructor and student mentoring
- 2) Practical application assignments
- 3) Topic-focused mini-lectures for small groups of students

Out-of-Class Assignments

May include the following:

- 1) Reading assignments
- 2) Technical skill labs using NetLabs
- 3) Technical skill labs using laboratory routers, switches, patch panels, access servers, computers, and virtualized PCs
- 4) Tests and quizzes

Texts and References

- 1) Required (representative example):
 - a. CWNA Certified Wireless Network Administrator Official Deluxe Study Guide: Exam CWNA-106 1st Edition; by David D. Coleman (Author), David A. Westcott (Author); Hardcover: 912 pages; Sybex; 1 edition (March 9, 2015); English; ISBN-10: 1119067766; ISBN-13: 978-1119067764
- 2) Supplemental: Optional Reference Text:
 - a. Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide*. 2nd edition. O'Reilly Media, 2005. ISBN-10: 0596100523, ISBN-13: 978-0596100520.

Exit Skills

Students having successfully completed this course exit with the following skills, competencies and/or knowledge:

- 1) Design, construct, and configure Adhoc Wireless LAN network topologies.
- 2) Design, construct, configure basic WLAN infrastructure network topologies.
- 3) Design, construct, configure point-to-point and point-to-multipoint wireless LAN network topologies consisting of wireless access points and wireless bridges.
- 4) Implement wireless security using MAC filtering, WEP, and WPA technologies.
- 5) Understand WLAN site survey fundamentals and conduct the basic elements required to accomplish a site survey.

Student Learning Outcomes

Upon successful completion of this course, students will be able to:

- 1) Successfully build and configure an instructor-defined secure WLAN scenario by implementing an 802.11 standards-based secure network solution using a wireless controller, access points, router, switch, and wireless clients