Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 204 – CISCO NETWORKING ACADEMY IV

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description
This is the fourth of four courses designed to provide knowledge, experience and skills in current and emerging networking technology. This course is also designed to help students prepare for the professional certification as a Cisco Certified Network Associate (CCNA) using the current Cisco Academy curriculum. Connected Networks discusses the WAN technologies and network services required by converged applications in a complex network. The course enables students to understand the selection criteria of network devices and WAN technologies to meet network requirements. Students learn how to configure and troubleshoot network devices and resolve common issues with data link protocols. Students will also develop the knowledge and skills needed to implement virtual private network (VPN) operations in a complex network.

Prerequisite
"C" grade or higher or "Pass" in CIS 203 or completion of CCNA3 Version 6 at another Cisco Networking Academy, or explicit instructor permission

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Basic understanding of routing and switching principles using the following networking protocols: single-area and multi-area OSPF, EIGRP, RIP, VLANs, VTP, STP, TCP/IP, EtherChannel, HSRP, DHCP, NAT. The ability to design and configure simple classful and classless network topologies consisting of workstations, switches and Cisco routers.

Course Content
1) Hierarchical Network Design
2) Connecting to the WAN
3) Point-to-Point Connections
4) Frame Relay
5) Network Address Translation for IPv4
6) Broadband Solutions
7) Securing Site-to-Site Connectivity
8) Monitoring the Network
9) Troubleshooting the Network

Course Objectives
Students will be able to:
1) Describe different WAN technologies and their benefits.
2) Describe the operations and benefits of virtual private networks (VPNs) and tunneling.
3) Describe, configure, and troubleshoot serial connections.
4) Describe, configure, and troubleshoot broadband connections.
5) Describe, configure, and troubleshoot tunneling operations.

6) Describe, configure, and troubleshoot Network Address Translation (NAT) operations.
7) Monitor and troubleshoot network operations using syslog, SNMP, and NetFlow.
8) Describe network architectures.

Method of Evaluation

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

1) Chapter exams that measure students' ability to define and appropriately use networking technology concepts and terminology to describe networking processes, protocols, functions and features.
2) Comprehensive final exam that measures students' ability to synthesize and apply course concepts to a variety of networking scenarios.
3) Comprehensive skills exam that measures students' ability to practically apply network, design, configuration and hardware connectivity techniques to LAN/WAN environments.
4) Lab exercises that require students to apply course concepts and skills in order to implement LAN/WAN solutions, compute IPv4 network addressing to network problems defined by the instructor, and connect and configure LAN/WAN devices.

Special Materials Required of Students

USB flash drive

Minimum Instructional Facilities

Smart computer lab with whiteboards, Internet Browser, Internet connectivity, software, printer; network connection not connected to school academic resources; 19" equipment racks populated with cross-connect patch panels, Cisco Access routers and switches, interconnecting CAT 5E and serial cabling; lab desks with computers not connected to the school academic network resources; computer server; storage cabinets

Method of Instruction

1) Online computer-based reading assignments
2) Instructor and individual student mentoring
3) Practical application assignments
4) Topic-focused mini-lectures for small groups of students

Out-of-Class Assignments

1) Read online curriculum and assignment instructions
2) Complete Packet Tracer assignments and online quizzes
3) Review online resources, including reference materials and videos

Texts and References

1) Required (representative example): Text is provided online at *www.netacad.com*
2) Supplemental (optional reference texts):
   a. Cisco Networking Academy, *Connecting Networks Companion Guide*. 1st edition. Cisco Press, 2014.
   b. Cisco Networking Academy, *Connecting Networks Lab Manual*. 1st edition. Cisco Press, 2013.
   c. Empson, Scott. *CCNA Routing and Switching Portable Command Guide*. 3rd edition. Cisco Press, 2013.
   d. Odom, Wendell. *CCNA Routing and Switching 200-120 Official Cert Guide*. 1st edition. Cisco Press, 2013.

Exit Skills

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

1) Ability to describe different WAN technologies and their benefits.
2) Ability to describe the operations and benefits of virtual private networks (VPNs) and tunneling.
3) Ability to configure and troubleshoot serial connections.
4) Ability to configure and troubleshoot broadband connections.
5) Ability to configure and troubleshoot IPsec tunneling operations.
6) Ability to monitor and troubleshoot network operations using syslog, SNMP, and NetFlow.
7) Ability to describe network architectures, dynamic NAT, and NAT overload.

Student Learning Outcomes

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

1) Build a basic LAN/WAN topology consisting of Cisco routers, Cisco switches and workstations. Configure a multiple router WAN topology by creating connections using GRE Tunnels, Frame Relay, PPPoE, NAT, and PAT. Manage and monitor network operations by configuring NTP, Syslog, SNMP, and NetFlow.