ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSN 2242: CCNA Capstone

Effective Date: Fall 2026 **Submitted Date:** Spring 2024

Credit Hours: 3 **IAI Number (if applicable): N/A**

Complete all that apply or mark "None" where appropriate:

Prerequisite(s): CSN-2241

Enrollment by assessment or other measure? ☐ Yes ☒ No
If yes, please describe:

Corequisite(s): None

Pre- or co-requisite(s): None

Consent of Instructor: ☐ Yes ☒ No

Delivery Method:		
	☒ **Lecture**	**2 Contact Hours** (1 contact = 1 credit hour)
	☐ **Seminar**	**0 Contact Hours** (1 contact = 1 credit hour)
	☒ **Lab**	**3 Contact Hours** (2-3 contact = 1 credit hour)
	☐ **Clinical**	**0 Contact Hours** (3 contact = 1 credit hour)

Offered: ☒ **Fall** ☒ **Spring** ☐ **Summer**

CATALOG DESCRIPTION and IAI NUMBER (if applicable):

The course focuses on preparing to pass the CCNA Certification Exam. Students identify areas of opportunity for growth and development. They practice testing of targeted areas of knowledge and configurations. Equipment and content will be organized to improve students understanding, skills, and ability to demonstrate during testing. Students will improve their ability and performance during tests.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:

1. Improve knowledge and skills to test in the subject matter.
    - Network Fundamentals
    - Network Access
    - IP Connectivity
    - IP Services
    - Security Fundamentals
    - Automation and Programmability
2. Identify Opportunities for improvement in learning.
3. Improve ability to perform during tests.
4. Improve confidence in student's knowledge and skillset to pass Certification Exam.

INSTRUCTIONAL METHODS:
Utilization of physical equipment and simulation software to engage students in comprehensive lab activities challenging their understanding and ability to work collaboratively / individually to overcome challenges and develop their skillset.

EVALUATION OF STUDENT ACHIEVEMENT:
Variety of labs
Quizzes
Written and Practical Final

INSTRUCTIONAL MATERIALS:

Textbooks: None

Resources
Cisco's Learning Management System
Cisco's Packet Tracer (Simulation software)
Cisco's hardware Devices (Routers and Switches)

LEARNING OUTCOMES AND GOALS:
Institutional Learning Outcomes
☒ 1) Communication – to communicate effectively.
☐ 2) Inquiry – to apply critical, logical, creative, aesthetic, or quantitative analytical reasoning to formulate a judgement or conclusion.
☐ 3) Social Consciousness – to understand what it means to be a socially conscious person, locally and globally.
☐ 4) Responsibility – to recognize how personal choices affect self and society.

Course Outcomes and Competencies

1. Network Fundamentals
   - 1.1. Explain the role and function of network components
     - 1.1.1. Routers
     - 1.1.2. Layer 2 and Layer 3 switches
     - 1.1.3. Next-generation firewalls and IPS
     - 1.1.4. Access points
     - 1.1.5. Controllers (Cisco DNA Center and WLC)
     - 1.1.6. Endpoints
     - 1.1.7. Servers
     - 1.1.8. PoE
   - 1.2. Describe characteristics of network topology architectures
     - 1.2.1. Two-tier
     - 1.2.2. Three-tier
     - 1.2.3. Spine-leaf
     - 1.2.4. WAN
     - 1.2.5. Small office/home office (SOHO)
     - 1.2.6. On-premise and cloud
   - 1.3. Compare physical interface and cabling types
     - 1.3.1. Single-mode fiber, multimode fiber, copper
     - 1.3.2. Connections (Ethernet shared media and point-to-point)
   - 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. Describe IPv6 address types
     - 1.9.1. Unicast (global, unique local, and link local)
     - 1.9.2. Anycast
     - 1.9.3. Multicast
     - 1.9.4. Modified EUI 64
   - 1.10. Verify IP parameters for Client OS (Windows, Mac OS, Linux)
   - 1.11. Describe wireless principles
     - 1.11.1. Nonoverlapping Wi-Fi channels
     - 1.11.2. SSID
     - 1.11.3. RF
     - 1.11.4. Encryption
   - 1.12. Explain virtualization fundamentals (server virtualization, containers, and VRFs)
   - 1.13. Describe switching concepts
     - 1.13.1. MAC learning and aging
     - 1.13.2. Frame switching
     - 1.13.3. Frame flooding
     - 1.13.4. MAC address table

2. Network Access

- 2.1. Configure and verify VLANs (normal range) spanning multiple switches
  - 2.1.1. Access ports (data and voice)
  - 2.1.2. Default VLAN
  - 2.1.3. InterVLAN connectivity
- 2.2. Configure and verify interswitch connectivity
  - 2.2.1. Trunk ports
  - 2.2.2. 802.1Q
  - 2.2.3. Native VLAN
- 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. Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
  - 2.5.1. Root port, root bridge (primary/secondary), and other port names
  - 2.5.2. Port states (forwarding/blocking)
  - 2.5.3. PortFast
- 2.6. Describe 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. Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

3. IP Connectivity
   - 3.1. Interpret the components of routing table
     - 3.1.1. Routing protocol code
     - 3.1.2. Prefix
     - 3.1.3. Network mask
     - 3.1.4. Next hop
     - 3.1.5. Administrative distance
     - 3.1.6. Metric
     - 3.1.7. Gateway of last resort
   - 3.2. Determine how a router makes a forwarding decision by default
     - 3.2.1. Longest prefix match
     - 3.2.2. Administrative distance
     - 3.2.3. Routing protocol metric
   - 3.3. Configure and verify IPv4 and IPv6 static routing
     - 3.3.1. Default route
     - 3.3.2. Network route
     - 3.3.3. Host route
     - 3.3.4. Floating static
   - 3.4. Configure and verify single area OSPFv2
     - 3.4.1. Neighbor adjacencies
     - 3.4.2. Point-to-point
     - 3.4.3. Broadcast (DR/BDR selection)
     - 3.4.4. Router ID
   - 3.5. Describe the purpose, functions, and concepts of first hop redundancy protocols

4. IP Service
   - 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 operation
   - 4.5. Describe the use of syslog features including facilities and level
   - 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, and shaping
   - 4.8. Configure network devices for remote access using SSH
   - 4.9. Describe the capabilities and functions of TFTP/FTP in the network
5. Security Fundamentals
   - 5.1. Define 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 and verify 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 IPsec remote access and site-to-site VPNs
   - 5.6. Configure and verify access control lists
   - 5.7. Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
   - 5.8. Compare authentication, authorization, and accounting concepts
   - 5.9. Describe wireless security protocols (WPA, WPA2, and WPA3)
   - 5.10. Configure and verify WLAN within the GUI using WPA2 PSK.
6. Automation and Programmability
   - 6.1. Explain how automation impacts network management
   - 6.2. Compare traditional networks with controller-based networking
   - 6.3. Describe controller-based, software defined architecture (overlay, underlay, and fabric)
   - 6.4. Separation of control plane and data plan
   - 6.5. Northbound and Southbound APIs
   - 6.6. Compare traditional campus device management with Cisco DNA Center enabled device management
   - 6.7. Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
   - 6.8. Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
   - 6.9. Recognize components of JSON-encoded data