**DESCRIPTOR: ITIS 152**

|  |  |  |  |
| --- | --- | --- | --- |
| Discipline: Information Technology/ Information Systems | Proposed Sub-discipline (if applicable): | | |
| General Course Title:  **Network Security and Automation** | | | Min. Units 3 |
| General Course Description:  This third course in the Cisco Certified Networking Associate (CCNA) curriculum describes the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation. Students learn how to configure, troubleshoot, and secure enterprise network devices and understand how application programming interfaces (API) and configuration management tools enable network automation. | | | |
| Proposed Number: ITIS 152 | Proposed Suffix: | | |
| Required Prerequisites[[1]](#footnote-1): None | | | |
| Required Co-Requisites: None. | | | |
| Advisories/Recommended Preparation[[2]](#footnote-2):     * ITIS 150 - Computer Network Fundamentals * ITIS 151 - Switching, Routing and Wireless Essentials | | | |
| Course Content:   1. Single-Area Open Shortest Path First (OSPF) Concepts 2. Single-Area Open Shortest Path First (OSPF) Configuration 3. Network Security 4. Concepts 5. Access Control List (ACL) Concepts 6. ACLs for Internet Protocol, Version 4 (IPv4) 7. Configuration 8. Network Address Translation (NAT) for IPv4 9. Wide Area Network (WAN) Concepts 10. Virtual Private Network (VPN) and Internet Protocol Security (IPsec) Concepts 11. Quality of Service (QoS) Concepts 12. Network Management 13. Network Design 14. Network Troubleshooting 15. Network Virtualization 16. Network Automation | | | |
| Course Objectives: *At the conclusion of this course, the student should be able to:*   1. Configure single-area OSPFv2 in both point-to-point and multi-access networks. 2. Explain how to mitigate threats and enhance network security using access control lists and security best practices. 3. Implement standard IPv4 ACLs to filter traffic and secure administrative access. 4. Configure NAT services on the edge router to provide IPv4 address scalability. 5. Explain techniques to provide address scalability and secure remote access for WANs. 6. Explain how to optimize, monitor, and troubleshoot scalable network architectures. 7. Explain how networking devices implement QoS. 8. Implement protocols to manage the network. 9. Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks. | | | |
| Methods of Evaluation:  Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments. | | | |
| Sample Textbooks, Manuals, or Other Support Materials (do not include editions or publication dates):   * Cisco Academy Program – CCNAv7: Enterprise Networking, Security, and Automation, Companion Guide, Cisco Press * Odem, W., CCNA 200-301 Official Certification Guide, Cisco Press | | | |
| FDRG Lead Signature: Markus Geissler, PhD Date: 01Jan2021 | | | |
| [For Office Use Only] | | **Internal Tracking Number** | |
|  | | | |
|  | | | |

1. Prerequisite or co-requisite course need to be validated at the CCC level in accordance with Title 5 regulations; co-requisites for CCCs are the linked courses that must be taken at the same time as the primary or target course. [↑](#footnote-ref-1)
2. Advisories or recommended preparation will not require validation but are recommendations to be considered by the student prior to enrolling. [↑](#footnote-ref-2)