



C-ID Descriptor

Network Security and Automation

Descriptor Details

- **Descriptor Title:** Network Security and Automation
- **C-ID Number:** 152
- **Units:** 3
- **Date of Last Revision:** 2/26/2025 07:17:59 PM GMT+0000

General 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.

Prerequisites

None

Corequisites

None

Advisories

- ITIS 150 - Computer Network Fundamentals
- ITIS 151 - Switching, Routing and Wireless Essentials

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

Lab Activities

No information provided

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.

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

- Cisco Academy Program – CCNAv7: Enterprise Networking, Security, and Automation, Companion Guide, Cisco Press
- Odem, W., CCNA 200-301 Official Certification Guide, Cisco Press