CompTIA Network+ (Exam N10-009), Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-002VL_rev1.0
Video and Lab Length: Approximately 51 hours, 9 minutes

Course Introduction

This course provides the learner with a comprehensive exploration of networking, encompassing essential fundamental concepts, practical network implementations, and vital operational strategies. Learners will explore how to troubleshoot various network issues effectively. The course will examine critical aspects of network security necessary to protect against a wide range of threats.

Video Enhanced Learning

(34h 9m * 6 Modules * 117 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Course Overview
2. Introduction to Network Communications
3. Examining Network Standardization
4. Introduction to TCP_IP and the OSI Model
5. Comparing TCP_IP to the OSI Model
6. Encapsulation and Decapsulation
7. Examining Network Topologies and Traffic Flows
8. Networking Protocols and Services
9. Internet Protocol Number and Traffic Types
10. Examining Public and Private Addressing
11. Examining IPv4 Address Classes
12. Examining IPv4 Addressing

13. Introduction to Subnetting
14. Introduction to VLSM
15. Introduction to CIDR
16. Implementing IP Addressing
17. Examining Network Switches
18. Examining Network Routers
19. Examining Wireless Appliances
20. Examining Firewalls and IPSs
21. Examining Load Balancers and Proxies
22. Examining Network Storage
23. Examining VPNs and QoS
24. Examining the 802.11 Standard
25. Examining the 802.3 Standard
26. Examining Transceivers and Connector Types
27. Examining Wireless Communications
28. Examining Cloud Concepts
29. Examining Cloud Components
30. Examining SDN and SD-WAN
31. Examining VXLAN
32. Examining Zero Trust Architecture
33. Examining Infrastructure as Code
34. Examining IPv6 Addresses
35. Static Routing
36. OSPF
37. EIGRP
38. BGP
39. Route Selection
40. Address Translation
41. First Hop Redundancy Protocols
42. Subinterfaces
43. VLANs
44. Interface Configuration
45. Spanning Tree Protocol
46. MTU

47. Frequencies and Channels
48. SSIDs
49. Network Types
50. Encryption
51. Authentication
52. Guest Networks
53. Antennas
54. Access Points
55. Installation Implications
56. Power
57. Environmental Factors
58. Common Documentation
59. Configuration/Change Management
60. Life-cycle Management
61. SNMP
62. Flow Data and Packet Captures
63. Baseline Metrics
64. Log Aggregation
65. API Integration
66. Port Mirroring
67. Network Monitoring Solutions
68. DR Metrics
69. DR Sites
70. HA Approaches-DR Testing
71. DHCP
72. DNS
73. Time Protocols
74. VPNs
75. Connection Methods
76. Jump Boxes
77. In-Band vs Out-of-Band Management
78. Data Security Concepts
79. Examining Digital Certificates
80. Examining Public Key Infrastructure

81. Examining Identity and Access Management
82. Examining Authentication Factors
83. Examining Single Sign On
84. Authentication with LDAP
85. Examining AAA
86. TACACS
87. Time-Based Auth and Geofencing
88. The Principle of Least Privilege
89. Examining Authorization and Access Control Models
90. Examining Physical Security
91. Examining Deception Technologies
92. Risks, Vulnerabilities, and Threats
93. Examining the Principles of Security
94. Regulatory Compliance and Audits
95. IoT and SCADA
96. Network Segmentation
97. Network Based Threats
98. Indicators of Network Attacks
99. Malware and Social Engineerings
100. Network Security Defenses
101. Implementing a Troubleshooting Methodology
102. Identifying the Problem in Troubleshooting
103. Establishing and Testing Theories in Troubleshooting
104. Establishing an Action Plan in Troubleshooting
105. Implementing a Solution in Troubleshooting
106. Verification and Documentation in Troubleshooting
107. Examining Network Cabling Issues
108. Examining Physical Interface Issues
109. Examining Switching and Routing Issue
110. Examining IP Addressing Issues
111. Examining Network Traffic Issues
112. Examining Wireless Network Issues
113. Examining Network Commands in Windows
114. Examining Network Commands in Linux

115. Examining Hardware-based Tools
116. Examining Software-Based Tools
117. Examining Basic Network Device Commands

Skill Labs

(17h * 17 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. Introduction to the OSI Model (N10-009)
2. Networking Appliances and Functionality (N10-009)
3. Cloud Networking Concepts (N10-009)
4. Networking Ports and Protocols (N10-009)
5. Networking Topologies and Architecture (N10-009)
6. IPv4 Network Addressing (N10-009)
7. Software Defined Networking Concepts (N10-009)
8. Routing Concepts (N10-009)
9. Switching Concepts (N10-009)
10. Network Monitoring Concepts (N10-009)
11. Disaster Recovery Concepts (N10-009)
12. Implementing IPv4 Network Services (N10-009)
13. Network Access and Management (N10-009)
14. Network Security Concepts (N10-009)
15. General Network Attacks (N10-009)
16. Network Hardening Techniques (N10-009)
17. Network Troubleshooting Tools and Techniques (N10-009)