masterskill
education through innovation

aci LEARNING | SKILL LABS

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

Course Specifications

Course Number: ACI76-002SL_rev1.0
Lab Length: Approximately 17 hours

Introduction to the OSI Model (N10-009)

Introduction
Objective

Welcome to the Introduction to the OSI Model Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

The OSI (Open Systems Interconnection) model comprises seven layers, each assigned a unique number from 1 to 7. These layers, from bottom to top, are:

- Layer 1 – The Physical Layer is responsible for the physical transmission of data over the network medium.
- Layer 2 – The Data Link Layer manages the reliable transfer of data frames between nodes on the same network.
- Layer 3 – The Network Layer handles routing and addressing to facilitate communication across multiple networks.
- Layer 4 – The Transport Layer ensures end-to-end delivery of data with error detection and correction.
- Layer 5 – The Session Layer establishes, manages, and terminates connections between applications.
- Layer 6 – The Presentation Layer is responsible for data translation, encryption, and compression.
- Layer 7 – The Application Layer provides network services and interfaces for user applications.

These layers collectively define the functions and interactions necessary for network communication and interoperability.

In this module, you will explore the functions and components of the OSI model layers.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – OSI Model Layers 1, 2, and 3
- Exercise 2 – OSI Model Layers 4 and 5
- Exercise 3 – OSI Model Layer 6
- Exercise 4 – OSI Model Layer 7

After completing this module, you should be able to:

- Examine a NIC at Layer 1
- Examine Interface Statistics and the ARP Table at Layer 2
- Examine Route Print at Layer 3
- Use Wireshark to Observe a TCP Connection

- Use Wireshark to Follow a TCP Stream
- Conduct File Compression and Encryption
- Use Nslookup

Exam Objectives:

The following exam objectives are covered in this module:

1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference mode.

- Layer 1 – Physical
- Layer 2 – Data link
- Layer 3 – Network
- Layer 4 – Transport
- Layer 5 – Session
- Layer 6 – Presentation
- Layer 7 Application

Networking Appliances and Functionality (N10-009)

Introduction
Objective

Welcome to the Networking Appliances and Functionality practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

VPNs (Virtual Private Networks) establish secure connections across public networks, enabling remote users to access internal private network resources from afar. Firewalls act as guards, monitoring and controlling both incoming and outgoing network traffic through an interface based on pre-established rules to protect against unauthorized access and malicious activities.

In this module, you will explore the setup and configuration of VPN connections and firewall rules to gain practical skills in establishing and securing network communications.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Configure OpenVPN
- Exercise 2 – Configure a VPN Client
- Exercise 3 – Connect and Inspect a VPN Connection

After completing this module, you should be able to:

- Create an OpenVPN Remote Access Server
- Create a VPN User
- Export a VPN User Package
- Install an OpenVPN Package on a Client
- Connect to the OpenVPN Server
- Inspect VPN Status and Firewall Rules

Exam Objectives:

The following exam objectives are covered in this module:

1.2 Compare and contrast networking appliances, applications, and functions

- Physical and virtual appliances
- Functions

Cloud Networking Concepts (N10-009)

Introduction
Objective

Welcome to the Cloud Networking Concepts practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

In cloud networking, Cloud Service Providers provide infrastructure and networking services over the Internet. They offer scalability, flexibility, and cost-effectiveness compared to traditional on-premises networking. In cloud networking, resources such as virtual machines, storage, and networking components are provisioned and managed centrally through web-based interfaces, allowing for rapid deployment and scalability on demand.

In this module, you will explore cloud networking concepts and understand the parallels between cloud and on-premises networking infrastructure.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Discover AWS Cloud Documentation
- Exercise 2 – Demonstrate NFV with pfSense

After completing this module, you should be able to:

- Review VPC, Internet Gateway, and Security Group Documentation
- Configure pfSense Firewall Rules
- Create a LAN Interface in pfSense
- Configure a Local Route Table
- Configure NAT on pfSense

Exam Objectives:

The following exam objectives are covered in this module:

1.3 Summarize cloud concepts and connectivity options

- Network functions virtualization (NFV)
- Virtual private cloud (VPC)
- Network security groups
- Cloud gateways

Networking Ports and Protocols (N10-009)

Introduction
Objective

Welcome to the Networking Ports and Protocols Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network ports and protocols are essential components of network communication, facilitating the exchange of data between devices. Ports are logical endpoints for communication, with each port corresponding to a specific service or application running on a device. Protocols, on the other hand, define the rules and formats for data exchange between devices.

In this module, you will explore and learn about network ports and protocols.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Discover Protocols with Wireshark
- Exercise 2 – Network Port Scan

After completing this module, you should be able to:

- Conduct a Ping
- Conduct a DNS Query
- Make an SSH Connection
- Access an HTTP Web Server
- Conduct a Network Port Scan

Exam Objectives:

The following exam objectives are covered in this module:

1.4 Explain common networking ports, protocols, services, and traffic types

- Protocols
- Ports
- Internet Protocol (IP) types

Networking Topologies and Architecture (N10-009)

Introduction
Objective

Welcome to the Networking Topologies and Architecture Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network topologies and architecture refer to the structural layout of a computer network. A network topology can either be defined as a physical or a logical topology, whereas a physical topology describes the network's layout and how the devices are connected. A logical network topology defines the different devices and how these devices communicate with each other. Common topologies include star, bus, ring, and mesh. Network architecture encompasses the broader framework, addressing how components like routers, switches, and servers are organized and interconnected to facilitate data transfer.

In this module, you will use Windows Hyper-V to establish virtual topologies.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Star Topology
- Exercise 2 – Full Mesh Topology

After completing this module, you should be able to:

- Create a Star Topology with Hyper-V
- Create a Full Mesh Topology with Hyper-V

Exam Objectives:

The following exam objectives are covered in this module:

1.6 Compare and contrast network topologies, architectures, and types

- Mesh
- Star/hub and spoke

IPv4 Network Addressing (N10-009)

Introduction
Objective

Welcome to the IPv4 Network Addressing practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

IPv4 network addressing encompasses critical aspects of network configuration. It includes IPv4 address classes as defined by RFC1918, which defines private IPv4 address spaces such as Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16). Furthermore, in IPv4 network addressing, subnetting and Classless Inter-Domain Routing (CIDR) allow for efficient utilization of IP addresses by dividing networks into smaller subnetworks, enabling granular control over routing and addressing between the subnetworks.

Automatic Private IP Addressing (APIPA) assigns temporary IP addresses within the range of 169.254.0.0 to 169.254.255.255 when DHCP servers are unavailable to provide automatic IPv4 addresses and machines are configured for DHCP addressing.

Loopback addressing reserves the IP address range 127.0.0.0/8 for self-testing and local communication within a device. These components form the foundational framework for IPv4 network addressing, enabling the allocation of IP addresses within small and enterprise-level networks.

In this module, you will explore each of the concepts.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – APIPA Addressing
- Exercise 2 – Subnetting
- Exercise 3 – The Loopback Address

After completing this module, you should be able to:

- Investigate network adapter configuration.
- Check APIPA connectivity.
- Assign static IP addresses.
- Conduct subnetting.
- Ping and articulate the loopback address range.

Exam Objectives:

The following exam objectives are covered in this module:

1.7 Given a scenario, use appropriate IPv4 network addressing

- Subnetting
- IPv4 address classes

Software Defined Networking Concepts (N10-009)

Introduction
Objective

Welcome to the Software Defined Networking Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Software Defined Networking (SDN) decouples the network control plane from the data plane, providing a more flexible and programmable infrastructure. This is particularly useful as networks grow in size and complexity. In SDN, a centralized controller manages and directs network traffic flows over the data plane. This separation of control and data planes facilitates automation, agility, and scalability in network configuration, making it easier to deploy and manage networks, optimize resource utilization, and respond efficiently to changing business requirements.

In this module, you will explore the use of Ansible to deploy configuration changes and Git to manage code versioning.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Utilize Ansible
- Exercise 2 – Utilize Git

After completing this module, you should be able to:

- Install Ansible
- Deploy an Ansible Playbook
- Install and Utilize Git
- Manage a Version Change in Git

Exam Objectives:

The following exam objectives are covered in this module:

1.8 Summarize evolving use cases for modern network environments

- Software-defined network (SDN)
- Infrastructure as Code (IaC)

Routing Concepts (N10-009)

Introduction
Objective

Welcome to the Routing Concepts practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

In this module, you will explore fundamental routing concepts, including static routing techniques, to establish efficient data paths. Static routing involves manually configuring routing tables, thus providing a straightforward method for small-scale networks. Network Address Translation (NAT) will be implemented to enable private network devices to access the Internet using a single public IP address via port forwarding. Additionally, you will delve into the utilization of sub interfaces, a technique in which a single physical network interface is logically divided into multiple virtual interfaces, each assigned a unique IP subnet and IP address. This allows for the segmentation of network traffic and facilitates the creation of distinct broadcast domains within a single physical interface.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Static Routing
- Exercise 2 – NAT
- Exercise 3 – Sub interfaces

After completing this module, you should be able to:

- Configure pfSense.
- Configure a static soute.
- Configure port forwarding.
- Create a VLAN on a pfSense subinterface.

Exam Objectives:

The following exam objectives are covered in this module:

2.1 Explain characteristics of routing technologies

- Static routing
- Address translation
- Subinterfaces

Switching Concepts (N10-009)

Introduction
Objective

Welcome to the Switching Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Switching is a fundamental networking concept that involves the efficient forwarding of data within a local area network (LAN). In this context, Virtual Local Area Networks (VLANs) provide a mechanism to logically segment a network into multiple networks, enhancing network flexibility and security. Maximum Transmission Unit (MTU) is a key parameter specifying the maximum size of data packets that can be transmitted over a network. Proper MTU configuration ensures efficient data transmission and avoids fragmentation issues. Knowing these concepts is essential for designing and managing modern network infrastructures, enabling efficient traffic control, segmentation, and optimal data transmission.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – VLANs
- Exercise 2 – MTU

After completing this module, you should be able to:

- Install and Configure VMs in Hyper-V
- Configure VLAN Communications
- Modify the MTU

Exam Objectives:

The following exam objectives are covered in this module:

2.2 Given a scenario, configure switching technologies and features

- Virtual Local Area Network (VLAN)
- Interface configuration
- Maximum Transmission Unit (MTU)

Network Monitoring Concepts (N10-009)

Introduction
Objective

Welcome to the Network Monitoring Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network monitoring involves the observation and analysis of traffic to ensure optimal performance, security, and reliability. Packet capture, a fundamental aspect of network monitoring, includes intercepting and recording data packets as they traverse the network through an interface, allowing administrators to inspect and troubleshoot issues at the packet level.

Network discovery plays a crucial role in understanding the network's topology, identifying connected devices, and mapping interconnections, aiding in efficient resource management and security enforcement.

In this module, you will explore the networking monitoring concepts of packet capture and network discovery.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Packet Capture
- Exercise 2 – Network Discovery

After completing this module, you should be able to:

- Utilize Wireshark
- Utilize pfSense Packet Capture
- Conduct an Ad hoc Host Discovery
- Conduct a Scheduled Host Discovery

Exam Objectives:

The following exam objectives are covered in this module:

3.2 Given a scenario, use network monitoring technologies

- Methods

Disaster Recovery Concepts (N10-009)

Introduction
Objective

Welcome to the Disaster Recovery Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Disaster recovery and high availability enable a resilience strategy. Disaster recovery describes the recovery and restoration of essential systems and data following some type of large-scale disruptive incident, such as a natural disaster. High availability focuses on minimizing downtime to ensure continuous operation of systems by deploying redundant components, failover mechanisms, and load balancing. Together, these concepts safeguard against disruptions, providing organizations with the ability to swiftly recover from disasters and maintain uninterrupted access to essential services, enabling business continuity and minimizing financial and operational impacts.

In this module, you will explore the load balancing component of high availability.

Overview
Learning Outcomes:

In this module, you will complete the following exercise:

- Exercise 1 – Load Balancing

After completing this module, you should be able to:

- Install IIS Server and Load Balancing Feature
- Configure Load Balancing Cluster
- Validate Load Balancing Configuration
- Review Load Balancer Logs

Exam Objectives:

The following exam objectives are covered in this module:

3.3 Explain disaster recovery (DR) concepts

- High-availability approaches
- Testing

Implementing IPv4 Network Services (N10-009)

Introduction
Objective

Welcome to the Implementing IPv4 Network Services practice lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

The implementation of essential Internet Protocol (IP) services is critical. IPv4, the foundational protocol that has long been the backbone of the internet, continues to play a crucial role in aiding the

communication between devices by assigning unique addresses to each one. As the demand for IP addresses grew exponentially, the adoption of IPv6 became increasingly important to address the limitations of IPv4 and ensure the continued expansion of the digital infrastructure. Additionally, services like Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) enhance network functionality by automating IP address allocation and translating user-friendly domain names into numerical IP addresses, respectively.

In this module, you will explore the implementation of DHCP, DNS records, and IPv6 in the network environment.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – DHCP
- Exercise 2 – DNS Records
- Exercise 3 – IPv6 Configuration

After completing this module, you should be able to:

- Install a DHCP Server
- Configure and Test the DHCP Server
- Add a CNAME Record
- Enable SLAAC IPv6 Addressing

Exam Objectives:

The following exam objectives are covered in this module:

3.4 Given a scenario, implement IPv4 and IPv6 network services

- Dynamic addressing
- Name resolution

Network Access and Management (N10-009)

Introduction
Objective

Welcome to the Network Access and Management Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network access management is a critical aspect of maintaining secure connections within a network infrastructure, with SSH (Secure Shell) serving as a fundamental protocol for secure communication. SSH ensures encrypted connections between clients and servers, preventing unauthorized access and safeguarding sensitive data transmission over untrusted networks.

In this module, you will explore SSH and the differences between unsecure and secure network access and management connections.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Unsecure Connections

- Exercise 2 – Secure Connections

After completing this module, you should be able to:

- Use the Copy Command
- Utilize SFTP
- Utilize SCP

Exam Objectives:

The following exam objectives are covered in this module:

3.5 Compare and contrast network access and management methods.

- Connection methods

Network Security Concepts (N10-009)

Introduction

Objective

Welcome to the Network Security Concepts Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network security concepts encompass a range of strategies and technologies aimed at safeguarding data transmission and communication within networks. Alongside these measures, employing full disk and file encryption techniques ensures data confidentiality and integrity. Full disk encryption secures the entire contents of a storage device, rendering it unreadable without the appropriate decryption key. Similarly, file encryption selectively encrypts individual files or folders, offering granular control over data protection.

In this module, you will explore full disk and file encryption with a Linux machine.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Full Disk Encryption
- Exercise 2 – File Encryption

After completing this module, you should be able to:

- Create and Mount a LUKS Partition
- Use OpenSSL to Encrypt and Decrypt a File

Exam Objectives:

The following exam objectives are covered in this module:

4.1 Explain the importance of basic network security concepts

- Logical security

General Network Attacks (N10-009)

Introduction

Objective

Welcome to the General Network Attacks Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

In a general network attack, an on-path attack strategy could involve techniques like ARP poisoning and DNS poisoning. In ARP poisoning, the attacker manipulates ARP messages to associate their MAC address with the IP address of a legitimate device, intercepting and manipulating traffic passing through the network. This allows for eavesdropping, session hijacking, or data modification. Concurrently, DNS poisoning involves corrupting the DNS lookup process to redirect users from their intended destinations, spoofing legitimate domains, and leading to unauthorized access or phishing attempts.

The tools and techniques used during this lab should not be used outside of a lab environment.

Overview

Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – On-path Attack
- Exercise 2 – ARP Poisoning
- Exercise 3 – DNS Poisoning

After completing this module, you should be able to:

- Spoof the ACIDC01 MAC Address
- Configure Bettercap
- Launch an ARP Poisoning Attack
- Modify the HOSTS File

Exam Objectives:

The following exam objectives are covered in this module:

4.2 Summarize various types of attacks and their impact to the network

- On-path attack
- Address Resolution Protocol (ARP) poisoning
- ARP spoofing
- DNS poisoning

Network Hardening Techniques (N10-009)

Introduction
Objective

Welcome to the Network Hardening Techniques Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Network hardening implements security measures to protect a network from unauthorized access, attacks, and data breaches. Techniques include disabling unused ports on network devices such as switches, routers, and firewalls to reduce the attack surface, configuring Access Control Lists (ACLs), as well as changing default passwords to help prevent unauthorized access and lower the risk of credential-based attacks.

In this module, you will explore various network hardening techniques.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Disable an Unused Port
- Exercise 2 – Configure an ACL Rule
- Exercise 3 – Change Default Configuration

After completing this module, you should be able to:

- Block a Port
- Block an IP Address
- Change Default Password for a Guest Account
- Disable Account

Exam Objectives:

The following exam objectives are covered in this module:

4.3 Given a scenario, apply network security features, defense techniques, and solutions.

- Device hardening
- Security rules

Network Troubleshooting Tools and Techniques (N10-009)

Introduction
Objective

Welcome to the Network Troubleshooting Tools and Techniques lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

In network troubleshooting, various tools are utilized to diagnose and resolve connectivity issues. Ping verifies connectivity between devices. Tracert and traceroute trace the route packets take to reach a destination. Nslookup and dig are used to query DNS records. Nmap performs network scanning. Tcpdump and Wireshark are packet sniffers that capture and analyze network traffic. These tools collectively provide comprehensive insights into network behavior, enabling efficient troubleshooting and the resolution of network problems.

In this module, you will explore network troubleshooting tools and techniques.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Ping, Tracert, and Traceroute
- Exercise 2 – Nslookup and Dig
- Exercise 3 – Nmap
- Exercise 4 – Tcpdump and Wireshark

After completing this module, you should be able to:

- Conduct Ping and Tracert
- Conduct Ping and Traceroute

- Achieve an Authoritative Lookup with Nslookup
- Achieve an Authoritative Lookup with Dig
- Conduct Host Discovery Scan, Default Scan, and Host Enumeration
- Use Tcpdump to Capture Packets
- Analyze a Tcpdump Packet Capture with Wireshark

Exam Objectives:

The following exam objectives are covered in this module:

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

- Software tools