Implementation Manual for a Home Lab with:

Windows Server 2019

Windows 10 pro

Oracle Virtual Box

BEGINNER FRIENDLY

GABRIEL SANCHEZ

Introduction

Today, the administration of infrastructures based on Active Directory remains an essential skill for IT professionals, especially in areas such as system administration, cybersecurity, and enterprise support. With the aim of strengthening practical knowledge in these environments, a virtual laboratory (Home Lab) was developed to simulate a basic corporate infrastructure based on Windows Server.

This laboratory is designed to implement and configure a Domain Controller with fundamental network services: Active Directory Domain Services (AD DS), DNS, DHCP, and Remote Access (NAT/RAS). In addition, a Windows 10 client machine joined to the domain is integrated, allowing validation of proper communication and authentication within the environment.

The infrastructure was built entirely in a virtualized environment, making it possible to replicate real-world network administration scenarios without the need for additional physical hardware. This document describes step by step the creation, configuration, and validation of the laboratory, serving as a practical

Prerequisites and Requirements

Before beginning this laboratory, it is recommended that the reader possesses a foundational understanding of basic networking and system administration concepts. This includes familiarity with IP addressing, subnetting, DNS name resolution, and the general principles of client-server communication. Basic knowledge of Windows operating systems and their administrative tools is also beneficial, as the laboratory environment relies on Microsoft-based infrastructure services. While advanced expertise is not required, having prior exposure to virtualization and network configuration concepts will significantly facilitate the learning process.

From a technical perspective, the laboratory requires a host computer with sufficient hardware resources to support virtualization. A system with at least 16 GB of RAM, a multi-core processor with virtualization support enabled, and adequate storage space is recommended to ensure stable performance of the virtual machines. A virtualization platform such as VMware Workstation or Oracle VirtualBox must be installed to create and manage the virtual environment.

Additionally, official installation media for Windows Server 2019 and Windows 10 Pro are required. These operating systems will be deployed as virtual machines to simulate a real enterprise network. Network connectivity on the host system is necessary to allow the virtualized environment to access external networks when configuring routing and NAT services.

Meeting these prerequisites ensures that the laboratory can be deployed without technical limitations and that the reader can focus on understanding the implementation of core infrastructure services rather than troubleshooting environmental constraints.

Chapter 1: Topology Design and Laboratory Requirements

1.1 Laboratory Objective

The main objective of this laboratory is to implement a simulated corporate network environment, composed of:

- A Windows Server 2019 server acting as a Domain Controller.
- Essential network services: AD DS, DNS, DHCP, and NAT (Remote Access).
- A Windows 10 client computer joined to the domain.
- Automatic IP address assignment via DHCP.
- Internal communication between client and server.
- Internet access from the internal network through NAT.

This environment allows practicing common tasks performed by a Windows system administrator, such as domain creation, user administration, DNS resolution, and network service configuration.

1.2 Implemented Network Topology

The laboratory topology consists of two virtual machines connected through a virtualized internal network. The server has two network adapters to fulfill routing and external access functions.

Main components:

Virtual Machine 1 – Windows Server 2019

- **Role:** Domain Controller (DC)
- **Installed services:**

- Active Directory Domain Services (AD DS)
- DNS
- DHCP
- Remote Access (NAT/RAS)

Network adapters:

- **External NIC (Internet):** Obtains IP addressing from the home router via DHCP.
- **Internal NIC (Lab Network):** Static IP address manually configured.

Internal network configuration of the server:

- IP address: 172.16.0.1
- Subnet mask: 255.255.255.0
- Gateway: Not configured (isolated internal network)
- Preferred DNS: 127.0.0.1 (loopback, local DNS service)

Virtual Machine 2 – Windows 10 Pro

- **Role:** Domain client
- **Network adapter:**
  - Internal NIC: Obtains IP addressing automatically from the DC's DHCP server.

1.3 Implemented Network Services

Active Directory Domain Services (AD DS)
Enables centralized authentication and management of users and computers within the configured domain.

- Domain name (FQDN): mydomain.com

DNS (Domain Name System)
Resolves internal domain names, allowing computers to locate the domain controller and other network services.

DHCP (Dynamic Host Configuration Protocol)
Assigns dynamic IP addresses to client computers within the internal network.

- Address range: 172.16.0.100 – 172.16.0.200
- Subnet mask: 255.255.255.0
- Assigned gateway: 172.16.0.1
- Assigned DNS: 172.16.0.1

Remote Access (NAT/RAS)
Allows internal network devices to access the Internet by using the server's external interface as a gateway.

1.4 Software and Resources Used

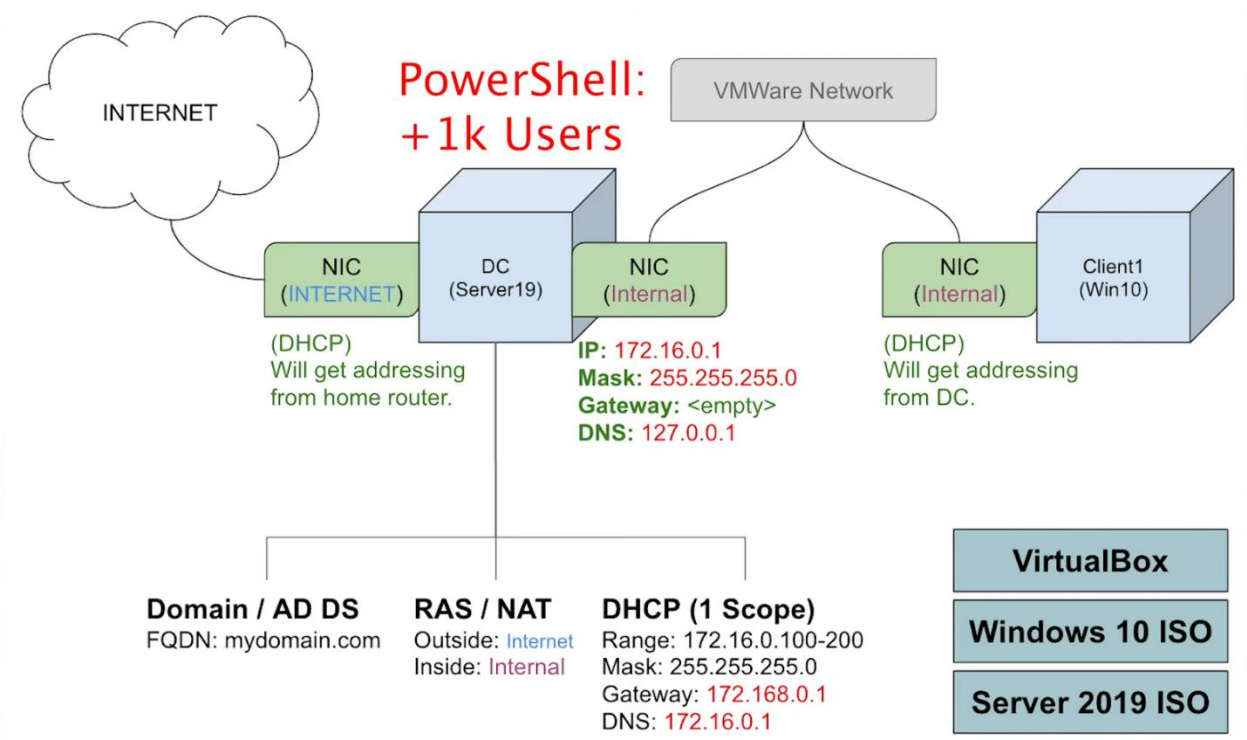
The following resources were used to implement the laboratory:

- Virtualizer: VirtualBox
- Windows Server 2019 ISO
- Windows 10 Pro ISO
- Host computer with virtualization support enabled

1.5 Expected Outcome of the Chapter

At the end of this chapter, the laboratory environment is fully designed and defined, establishing the foundation to begin the operating system installation and initial server configuration in the following chapters.

Topology/Diagram:



This diagram provides a clear and direct understanding of the laboratory topology, showing how the server acts as the central point of the network by connecting the internal network to the Internet while simultaneously providing domain and addressing services. The image clearly illustrates which network interfaces are used for each function, how IP addresses are assigned within the internal network, and how the client machine communicates with the server, serving as a visual reference that simplifies understanding of the overall structure and operation of the environment.

Chapter 2: Windows Server 2019 Installation and Initial Server Configuration

2.1 Purpose of This Chapter

The purpose of this chapter is to guide the installation of Windows Server 2019 on the virtual machine and perform the initial server configuration. This includes setting up network adapters, assigning a static IP address to the internal interface, and preparing the server to act as a Domain Controller with the necessary services for the laboratory environment. The chapter ensures that the server is correctly configured to support domain integration, DHCP, DNS, and NAT, forming the foundation for subsequent laboratory tasks.

2.2 Creation of the Server Virtual Machine

The laboratory was implemented using VirtualBox as the virtualization platform. VirtualBox allows the creation of internal and external virtual networks, simulating real enterprise infrastructure scenarios without additional hardware.

Steps performed:

- A new virtual machine was created with the name:

  DC-Server2019
- Operating system type selected:
  - Type: Microsoft Windows
  - Version: Windows 2019 (64-bit)
- Hardware resources assigned:
  - RAM: 4 GB
  - Processors: 2 cores
  - Virtual hard disk: 50 GB, dynamically allocated

Technical justification:

A Domain Controller requires sufficient resources to handle authentication, DNS, and DHCP services. Allocating appropriate memory and CPU avoids slowdowns during domain promotion and network service operation.

2.3 Network Adapter Configuration

To simulate a real environment where a server acts as a bridge between an internal and an external network, two network adapters were configured in the virtual machine.

Adapter 1 – External NIC (Internet)

- Network mode: Bridged Adapter
- Connected to the host computer's physical network card

Function:
This interface allows the server to obtain an IP address directly from the home router via DHCP. It provides Internet connectivity, which will later be shared with the internal network through NAT.

Technical justification:
In enterprise environments, servers acting as gateways typically have one interface connected to the external network (ISP) and another to the internal network. This setup replicates that scenario.

Adapter 2 – Internal NIC (Lab Network)

- Network mode: Internal Network
- Internal network name: LAB_INTERNAL

Function:
This interface connects the server exclusively to the lab client machines. It has no direct Internet access and depends on the server for network services.

Technical justification:
Separating the internal network from the external one allows full control of lab traffic and simulates an isolated corporate network where the server manages IP addressing, DNS, and authentication.

2.4 Windows Server 2019 Installation

once the virtual machine was created, the Windows Server 2019 ISO was mounted, and the installation process began.

Steps performed:

- The virtual machine was started from the ISO.
- Version selected: **Windows Server 2019 Standard (Desktop Experience)**
- Language and region configured.
- Clean installation performed on the allocated virtual disk.
- A secure password was set for the Administrator account.

Technical justification:
The Desktop Experience version was selected to facilitate visual server management, ideal for learning labs. Server Core can be used in enterprises, but Desktop Experience provides a more accessible learning curve.

2.5 Initial System Configuration

After the first login, basic configurations were performed before installing roles.

Server renaming:

- Assigned name: **DC01**

Technical justification:
Renaming the server before promoting it to a Domain Controller is best practice. Changing the name after installing Active Directory can cause infrastructure inconsistencies.

Updates configuration:

- Ensured essential system updates were installed.

Technical justification:
Keeping the server updated reduces vulnerabilities and ensures compatibility with network services.

2.6 Static IP Configuration on the Internal NIC

Assigning a static IP to the server's internal interface is critical before installing Active Directory.

Configuration applied:

- Interface: Internal NIC
- IP address: 172.16.0.1
- Subnet mask: 255.255.255.0
- Gateway: (Not configured)
- Preferred DNS: 127.0.0.1

Technical justification:

- **Static IP:** Ensures the Domain Controller is always reachable by clients. Dynamic IPs could cause authentication and DNS failures.
- **Subnet mask:** Defines the internal lab segment, supporting up to 254 devices in the 172.16.0.0/24 network.

- **Empty gateway:** Internal NIC belongs to an isolated network; Internet access uses the external NIC via NAT.
- **DNS 127.0.0.1:** Points to the server itself, which will later be configured as the domain's DNS server.

2.7 Internal Connectivity Verification

To validate the configuration:

- The external NIC obtained an IP automatically from the router.
- The internal NIC maintained the configured static IP.
- No network conflicts occurred between the two interfaces.

Technical justification:
Ensuring proper network separation before role installation prevents routing and DNS resolution issues during domain promotion.

2.8 Chapter Outcome

At the end of this chapter, the Windows Server 2019 server is:

- Correctly installed.
- Renamed as **DC01**.
- Equipped with two operational network interfaces.
- Configured with a static IP on the internal network.
- Ready for installation of Active Directory, DNS, DHCP, and Remote Access roles.

Chapter 2 — Chapter Outcome
By the end of this chapter, the Windows Server 2019 system was successfully installed, configured with internal and external network interfaces, and assigned a static IP address, leaving the server ready for the installation of infrastructure roles.

Chapter 3: Installation and Promotion of Active Directory Domain Services (AD DS)

3.1 Purpose of This Chapter

This chapter describes the process of installing the Active Directory Domain Services (AD DS) role and promoting the Windows Server 2019 server to a Domain Controller.

This step is the core of the laboratory, as Active Directory will centralize user and computer authentication, manage security policies, and serve as the foundation for network services implemented later, such as DNS and DHCP.

At the end of this chapter, the server **DC01** will be fully operational as the primary Domain Controller for the **mydomain.com** environment.

3.2 Importance of Active Directory in Enterprise Environments

Active Directory Domain Services is the directory service used in Windows infrastructures to:

- Manage users, computers, and groups.
- Centralize authentication and authorization.
- Apply security policies through Group Policy.
- Integrate network services such as DNS and DHCP.
- Facilitate network resource administration.

In real corporate environments, Active Directory is the backbone of the infrastructure. This lab replicates that behavior on a smaller scale, allowing practice with real domain management configurations.

3.3 Prerequisites

Before installing AD DS, the following requirements were verified:

- Windows Server 2019 installed correctly.
- Server renamed as **DC01**.
- Internal NIC configured with a static IP:
    - IP: 172.16.0.1
    - Subnet mask: 255.255.255.0
    - DNS: 127.0.0.1
- External NIC obtaining IP automatically from the router.
- Stable network connectivity between both interfaces.

Technical justification:
Active Directory depends directly on DNS and a fixed IP address. If these requirements are not met, promotion to Domain Controller may fail or cause name resolution errors.

3.4 Installation of the Active Directory Domain Services Role

Procedure:

1. From Server Manager, select **Add Roles and Features**.
2. Choose **Role-based or feature-based installation**.
3. Select the server **DC01** as the destination.
4. In the roles list, check **Active Directory Domain Services (AD DS)**.
5. Accept installation of additional features (AD DS management tools).
6. Complete the wizard and start the role installation.

Technical justification:
Installing the AD DS role prepares the server to act as a Domain Controller. At this stage, only binaries and management tools are installed; the domain is not yet created. Domain creation occurs during promotion, described next.

3.5 Promoting the Server to Domain Controller

Once the role installation is complete, Server Manager shows a notification indicating the server must be promoted.

Procedure:

1. Select **Promote this server to a domain controller**.
2. Choose **Add a new forest**.
3. Enter the root domain name: **mydomain.com**.
4. Configure functional levels:
    - Domain Functional Level: Windows Server 2016 or higher
    - Forest Functional Level: Windows Server 2016 or higher
5. Check **Install DNS server**.
6. Set a password for **Directory Services Restore Mode (DSRM)**.
7. Accept default paths for the database and SYSVOL.
8. Run the prerequisite check and start the promotion.
9. The server restarts automatically upon completion.

3.6 Technical Justification of Selected Configuration

- **New forest:** A new forest was created because this lab simulates a greenfield infrastructure with no existing domains.
- **Domain mydomain.com:** Using a realistic FQDN mirrors enterprise naming conventions.
- **DNS installation:** AD requires DNS to locate Domain Controllers and other services; installing it with AD DS is standard practice.

- **Modern functional levels:** Enable advanced Active Directory features and ensure compatibility with Windows Server 2019.
- **DSRM password:** Used for recovery and maintenance in Safe Mode.

3.7 Domain Verification After Restart

After the automatic restart:

- Log in using: **MYDOMAIN\Administrator**
- Open **Active Directory Users and Computers** to verify:
    - Existence of the domain **mydomain.com**
    - Creation of default organizational units
- Verify that the DNS service is installed and running

3.8 Verification of DNS Integrated with Active Directory

From the DNS console, confirm:

- Existence of the forward lookup zone: **mydomain.com**
- Automatic creation of records:
    - **A (Host)**
    - **SRV (Service Records)**

Technical justification:
SRV records allow client machines to automatically locate the Domain Controller during the domain join process.

3.9 Chapter Outcome

At the end of this chapter, the server **DC01** is:

- Promoted as the primary Domain Controller.
- Domain created: **mydomain.com**

- DNS service integrated and operational.
- Active Directory database functioning correctly.

Chapter 3 — Chapter Outcome
By the end of this chapter, the server was successfully promoted to a Domain Controller, the mydomain.com domain was created, and the DNS service was integrated, establishing the central authentication and management platform of the laboratory.

Chapter 4: DNS Service Configuration and Validation

4.1 Purpose of This Chapter

The DNS (Domain Name System) service is an essential component in any Active Directory environment. Its main function is to enable name resolution—that is, translating human-readable domain names (e.g., **dc01.mydomain.com**) into IP addresses that computers can use to communicate.

This chapter details the verification and configuration of the DNS service installed alongside Active Directory, as well as the necessary tests to confirm proper name resolution within the lab.

At the end of this chapter, **DC01** will function as the authoritative DNS server for the **mydomain.com** domain.

4.2 Importance of DNS in Active Directory

Active Directory relies entirely on DNS to:

- Locate Domain Controllers.
- Allow clients to join the domain.
- Resolve internal services via SRV records.
- Facilitate communication between domain computers.

Technical justification:
If DNS is not correctly configured, clients will not find the Domain Controller, causing authentication failures and errors when joining machines to the domain.

4.3 Initial DNS Service Verification

After promoting the server to Domain Controller, the DNS role is installed automatically. To confirm proper operation, the following checks were performed:

- Open **DNS Manager** from:
  Server Manager → Tools → DNS
- Verify the existence of the forward lookup zone:
  mydomain.com
- Within the zone, check automatically created records:
  - **A record** for **DC01** pointing to IP 172.16.0.1
  - **SRV records** for Active Directory services

4.4 Verification of Essential DNS Records

A Record (Host)

- Name: **DC01**
- IP Address: 172.16.0.1
- Function: Allows clients to resolve the server name **DC01** to its IP address.

SRV Records (Service Records)

- Indicate the location of specific domain services such as:
  - LDAP
  - Kerberos
  - Global Catalog

- Function: Clients query these records to automatically locate the Domain Controller during domain join.

4.5 Creation of Reverse Lookup Zone

Although optional, a reverse lookup zone allows IP-to-name resolution, useful for network diagnostics.

Procedure:

1. In **DNS Manager**, right-click **Reverse Lookup Zones** → **New Zone**.
2. Choose **Primary Zone**.
3. Select **IPv4 Reverse Lookup Zone**.
4. Enter the network ID: **172.16.0**.
5. Complete the wizard.
6. Verify that a **PTR record** for **DC01** is created automatically.

4.6 Technical Justification for Reverse Zone

The reverse zone allows diagnostic tools such as **nslookup** or security logs to identify hostnames from IP addresses. In enterprise environments, this facilitates auditing, monitoring, and troubleshooting.

4.7 DNS Resolution Tests from the Server

Test 1: Forward Resolution

- Command: nslookup dc01.mydomain.com
- Expected Result: Response with IP **172.16.0.1**

Test 2: Reverse Resolution

- Command: nslookup 172.16.0.1
- Expected Result: Response with name **dc01.mydomain.com**

4.8 Configuring DNS Forwarders

To allow domain clients to resolve Internet names, a DNS forwarder was configured.

Procedure:

1. In **DNS Manager**, right-click **DC01** → **Properties**.
2. Go to the **Forwarders** tab.
3. Add forwarder servers:
    - Home router DNS
    - Public DNS: 8.8.8.8, 1.1.1.1
4. Apply changes.

4.9 Technical Justification for Forwarders

The internal DNS server is authoritative only for **mydomain.com**.
When a client requests an external domain (e.g., google.com), the internal DNS forwards the query to a public DNS server, receives the response, and returns it to the client.

This enables Internet access from the lab's internal network.

4.10 Chapter Outcome

At the end of this chapter:

- DNS is correctly installed and configured.
- The forward lookup zone **mydomain.com** functions properly.
- The reverse lookup zone is enabled.
- **DC01** resolves both internal and external names.
- Active Directory can locate domain services without errors.

Chapter 4 — Chapter Outcome
By the end of this chapter, the DNS service was fully operational, resolving internal domain names and external queries through forwarders, ensuring proper location of services and devices within the network.

Chapter 5: DHCP Service Installation and Configuration

5.1 Purpose of This Chapter

The DHCP (Dynamic Host Configuration Protocol) service automatically assigns IP addresses and other network settings to client machines. In enterprise environments, DHCP eliminates the need for manual configuration on each device and reduces addressing errors.

In this lab, **DC01** acts as the DHCP server for the internal network **172.16.0.0/24**, automatically providing IP address, gateway, and DNS settings to domain-joined machines.

At the end of this chapter, any device connected to the internal network will receive its network configuration automatically from the Domain Controller.

5.2 Importance of DHCP in the Lab Infrastructure

Without DHCP, each client machine would require manual IP configuration. This is not scalable or efficient in real environments. Implementing DHCP in the lab replicates a corporate network behavior, where devices obtain connectivity dynamically and centrally.

Additionally, DHCP works together with DNS and Active Directory to automatically register machines in the domain and keep name resolution up to date.

5.3 DHCP Role Installation

Procedure:

1. From **Server Manager**, select **Add Roles and Features**.

2. Choose **Role-based or feature-based installation**.
3. Select **DC01** as the destination server.
4. In the roles list, check **DHCP Server**.
5. Accept additional features when prompted.
6. Complete the wizard and start the installation.
7. Click **Complete DHCP Configuration** at the end.

5.4 Authorizing the DHCP Server in Active Directory

In Active Directory environments, every DHCP server must be authorized to prevent unauthorized servers from assigning incorrect IP addresses.

Procedure:

- When prompted, select **Authorize DHCP Server in AD**.
- Use credentials: **MYDOMAIN\Administrator**.
- Complete the wizard.

Technical justification:
Only authorized DHCP servers can operate within an Active Directory domain. This prevents attacks or network errors caused by misconfigured or malicious DHCP servers.

5.5 Creating the DHCP Scope

The **Scope** defines the range of IP addresses the DHCP server can assign to clients.

Procedure:

1. Open **DHCP Manager** from **Server Manager → Tools → DHCP**.
2. Expand: **DC01 → IPv4**.
3. Right-click **IPv4 → New Scope**.
4. Configure scope parameters:
    - **Scope Name:** LAB_INTERNAL_SCOPE

    - **IP Range:** 172.16.0.100 – 172.16.0.200
    - **Subnet Mask:** 255.255.255.0
    - **Lease Duration:** 8 days (default)
5. No exclusions configured at this stage.

5.6 Configuring DHCP Options

After creating the scope, configure the network options clients will receive:

- **003 Router (Gateway):** 172.16.0.1
- **006 DNS Servers:** 172.16.0.1
- **015 DNS Domain Name:** mydomain.com

Technical justification:

- **Gateway 172.16.0.1:** Points to the internal NIC of DC01, which will later act as the NAT gateway.
- **DNS 172.16.0.1:** Ensures clients use the internal domain DNS for Active Directory name resolution.
- **Domain mydomain.com:** Allows clients to automatically register their names in DNS within the domain.

5.7 Activating the Scope

Once options are configured:

- Right-click the created scope → **Activate**.

5.8 DHCP Service Verification

To confirm proper operation:

- Verify the **DHCP Server** service is running.

- Check in **DHCP Manager** that the scope is active and no authorization errors exist.

5.9 IP Assignment Test

Final validation will occur when the Windows 10 client connects to the internal network in **Chapter 7**.
From the server, it was confirmed that the service is ready to assign dynamic addresses.

5.10 Chapter Outcome

At the end of this chapter:

- The DHCP role is installed.
- The DHCP server is authorized in Active Directory.
- An active scope exists with IP range 172.16.0.100 – 172.16.0.200.
- Clients will automatically receive correct IP, DNS, and Gateway settings.
- The internal network is ready to accept client machines.

Chapter 5 — Chapter Outcome
By the end of this chapter, the DHCP server was installed, authorized, and configured with a dynamic address scope, enabling automatic assignment of network parameters to laboratory devices.

Chapter 6: Remote Access Service Configuration (NAT/RAS)

6.1 Purpose of This Chapter

In a real corporate network, internal devices typically access the Internet through a server or device acting as a gateway. To replicate this behavior in the lab, the **Remote**

Access service with NAT (Network Address Translation) was configured on the **DC01** server.

This service allows devices on the internal network **172.16.0.0/24** to access the Internet using the server's external interface as the exit point.

By the end of this chapter, the lab's internal network will have controlled external connectivity through Windows Server 2019.

6.2 Importance of NAT in Network Environments

NAT allows multiple devices within a private network to share a single public IP address to access the Internet.

Main benefits:

- Hides internal IP addresses.
- Reduces the number of public IP addresses required.
- Centralizes control of outgoing traffic.

Technical justification:
Implementing NAT in this lab simulates a basic corporate architecture where the server acts as a router between the internal and external networks.

6.3 Remote Access Role Installation

Procedure:

1. In **Server Manager**, select **Add Roles and Features**.
2. Choose **Role-based or feature-based installation**.
3. Select **DC01** as the destination server.
4. In the roles list, check **Remote Access**.
5. In role services, select **Routing**.
6. Complete the wizard and start the installation.

6.4 Configuring Routing and Remote Access (RRAS)

Once installation is complete:

1. Open **Routing and Remote Access** from **Server Manager → Tools**.
2. Right-click **DC01 → Configure and Enable Routing and Remote Access**.
3. In the wizard, choose **Network Address Translation (NAT)**.
4. Select the external interface: NIC connected to the Internet (Bridged Adapter).
5. Confirm the internal interface: NIC with IP **172.16.0.1**.
6. Finish the wizard and enable the service.

6.5 NAT Interface Configuration

After completing the wizard, verify:

- **External interface:** Marked as **Public interface connected to the Internet** and enabled for NAT.
- **Internal interface:** Marked as **Private interface**.

6.6 Technical Justification

- The external interface obtains an IP from the physical router, enabling Internet access.
- The internal interface remains isolated in the lab network.
- NAT translates private internal addresses (**172.16.0.x**) to the server's public external IP.
- This allows internal clients to browse the Internet without direct exposure to the external network.

6.7 RRAS Service Verification

To confirm RRAS is functioning properly:

- Check that **Routing and Remote Access** service is **Running**.
- Verify in the RRAS console that:
    - Both internal and external interfaces are active.
    - NAT is enabled.

6.8 Chapter Outcome

By the end of this chapter:

- The **Remote Access** role is installed.
- RRAS is configured in **NAT mode**.
- DC01 acts as a gateway between the internal and external networks.
- The lab network is ready for Internet access from client machines.

Chapter 6 — Chapter Outcome
By the end of this chapter, the Remote Access service was configured with NAT, establishing the server as the gateway between the internal and external networks and enabling Internet access from the laboratory environment.

Chapter 7: Windows 10 Installation and Client Domain Join

7.1 Purpose of This Chapter

This chapter documents the creation and configuration of a **Windows 10 Pro virtual machine**, acting as a client within the **mydomain.com** domain.

The goal is to integrate the client into the previously built infrastructure, verifying that it:

- Receives network configuration from DHCP.
- Resolves names using the internal DNS.
- Can authenticate against Active Directory.

By the end of this chapter, the lab will have a fully domain-joined client functional within the simulated corporate network.

7.2 Creating the Windows 10 Virtual Machine

Using VirtualBox, a second virtual machine was created with the following specifications:

- **Name:** CLIENT-W10
- **Type:** Microsoft Windows
- **Version:** Windows 10 (64-bit)
- **RAM:** 4 GB
- **Processors:** 2 cores
- **Virtual Hard Disk:** 40 GB (dynamically allocated)

Technical justification:
Windows 10 Pro was selected because it supports domain join, which is not available in Home editions.

7.3 Client Network Adapter Configuration

- **Network mode:** Internal Network

- **Network name:** LAB_INTERNAL

Technical justification:
Using the same internal network as the server's internal NIC isolates the client from the Internet, making it fully dependent on DC01 for connectivity, replicating a real corporate environment.

7.4 Windows 10 Installation

The Windows 10 Pro ISO was mounted, and a clean installation was performed:

- Boot from ISO.
- Select language and region.
- Install Windows 10 Pro.
- Create a temporary local user.

7.5 Obtaining an Automatic IP Address

After installation:

- Verified network settings to ensure the adapter was set to obtain an IP automatically.

Expected result:

- IP assigned by DHCP: 172.16.0.100 (or within configured range)
- Subnet mask: 255.255.255.0
- Gateway: 172.16.0.1
- DNS: 172.16.0.1

Technical justification:
This confirms DHCP is working, the client receives correct network parameters, and server-client communication is operational.

7.6 Verifying Server Connectivity

Basic tests from the client:

- **IP connectivity:**
- ping 172.16.0.1

Expected result: Successful reply from DC01.

- **DNS resolution:**
- nslookup dc01.mydomain.com

Expected result: Resolves correctly to 172.16.0.1.

7.7 Joining the Client to the Domain

Procedure:

1. Open **System Properties** → **Computer Name** → **Change**.
2. Select **Domain** and enter **mydomain.com**.
3. Provide credentials:
    - User: MYDOMAIN\Administrator
    - Password: domain password
4. System confirms: *Welcome to the mydomain.com domain*.
5. Reboot the client.

7.8 Logging in to the Domain

After restart:

- Select **Other user**.
- Enter credentials: MYDOMAIN\Administrator / domain password.
- Login successful.

7.9 Verification from Active Directory

From DC01:

- Open **Active Directory Users and Computers**.
- Confirm that **CLIENT-W10** appears in the **Computers** organizational unit.

7.10 Chapter Outcome

By the end of this chapter:

- Windows 10 Pro is correctly installed.
- Client obtains IP automatically via DHCP.
- Internal DNS resolves domain names.
- CLIENT-W10 is joined to the **mydomain.com** domain.
- The domain successfully authenticates users.

Chapter 7 — Chapter Outcome
By the end of this chapter, the Windows 10 client was installed, received automatic network configuration, and successfully joined the mydomain.com domain, validating integration between client and server.

Chapter 8: Final Validation and Lab Testing

8.1 Purpose of This Chapter

After implementing all the lab services, it is essential to perform final tests to verify the proper operation of each component. This chapter documents the validations carried out to ensure that **Active Directory, DNS, DHCP, and NAT** work together in an integrated and stable manner.

The goal is to confirm that the environment accurately simulates a basic corporate infrastructure and is ready for use as a practical learning platform.

8.2 Active Directory Service Validation

Domain Authentication Test

From the client **CLIENT-W10**:

- Log in using domain credentials:
    - User: MYDOMAIN\Administrator

Expected result:

- Successful login and domain profile load.

Technical justification:

- Confirms the client can communicate with the Domain Controller and that Kerberos authentication is functioning correctly.

Administration Test from DC01

From the server:

- Open **Active Directory Users and Computers**.
- Verify:
    - Existence of the domain **mydomain.com**
    - Registration of the **CLIENT-W10** machine

Expected result:

- Client appears correctly registered in the domain.

8.3 DNS Service Validation

Internal Name Resolution

From **CLIENT-W10**:

nslookup dc01.mydomain.com

Expected result:

- Resolves successfully to IP 172.16.0.1

External Name Resolution

From **CLIENT-W10**:

nslookup google.com

Expected result:

- Resolves successfully via the configured DNS forwarder

Technical justification:

- Confirms that:
    - Internal DNS resolves domain names correctly.
    - DNS can forward external queries to public DNS servers.

8.4 DHCP Service Validation

From **CLIENT-W10**:

ipconfig /all

Expected result:

- IP address within range 172.16.0.100 – 172.16.0.200
- Gateway: 172.16.0.1
- DNS: 172.16.0.1
- Domain: mydomain.com

Technical justification:

- Confirms the client is receiving automatic network configuration from the authorized DHCP server.

8.5 NAT and Internet Access Validation

External Connectivity Test

From **CLIENT-W10**:

ping 8.8.8.8

Expected result:

- Successful reply

Web Browsing Test

- Open a web browser
- Access an external site (e.g., https://www.google.com)

Expected result:

- Web page loads correctly

Technical justification:

- Confirms that NAT is translating internal addresses correctly and the internal network can access the Internet through server DC01.

Chapter 8 — Final Laboratory Summary

By the completion of this final chapter, the entire home lab infrastructure was successfully designed, deployed, and validated, simulating a real enterprise network environment. The Windows Server 2019 system now operates as a fully functional Domain Controller providing Active Directory, DNS, DHCP, and Remote Access services, while the Windows 10 client is properly integrated into the domain.

This laboratory demonstrates the end-to-end implementation of core Microsoft network services, establishing a solid foundation for further security testing, system administration practice, and enterprise infrastructure development.

Conclusion

This guide presented the complete design and deployment of a Windows-based home lab environment, replicating the fundamental components of a corporate network infrastructure. Throughout each chapter, the laboratory was built step by step, from initial planning and network design to the installation and integration of Active Directory, DNS, DHCP, and Remote Access services, as well as the successful incorporation of a Windows 10 client into the domain.

By completing this project, a functional and scalable environment was achieved, suitable for practicing system administration, network management, and security testing in a controlled setting. This laboratory not only reinforces technical knowledge of Microsoft server technologies, but also provides a strong foundation for future expansions such as Group Policy management, centralized logging, security monitoring, and advanced domain configurations.

This concludes the implementation of the home lab, leaving a fully operational platform ready for continued learning and professional development.

Objectives

The main objective of this project is to design, implement, and validate a functional Windows-based home lab that simulates a real enterprise network environment. This includes deploying a Windows Server 2019 system as a Domain Controller, configuring core infrastructure services such as Active Directory, DNS, DHCP, and Remote Access, and integrating a Windows 10 client into the domain. Additionally, this laboratory aims to provide a practical environment for developing skills in system administration, network configuration, and infrastructure management.

Scope

The scope of this laboratory covers the creation of a virtualized network environment composed of one Windows Server 2019 machine and one Windows 10 client machine. The project includes the installation and configuration of server roles and services,

network interface setup, IP addressing, domain creation, client-domain integration, and validation of service functionality. External enterprise services, advanced security hardening, and cloud-based integrations are outside the scope of this implementation but may be considered for future expansions.