Beginner-Friendly Lab Guide: Building an AD & DNS Lab (Static IP Only)

Part 0: Lab Environment Overview

Before we begin, let's understand what we are building:

Your Server VM (Windows Server 2016/2019/2022):

This will be the brain of the lab.
It will act as:

- **Domain Controller (AD DS)** → Stores user accounts, groups, computers, and applies rules (Group Policy).
- **DNS Server** → The "phonebook" that lets computers find each other by name instead of IP address.

Your Client VM (Windows 10/11):

A workstation that will later join the domain.

It will:

- Get a manually assigned static IP.
- Use the Server VM as its DNS server.
- Join the domain and receive Group Policy rules.

Network Setup:

- Set both VMs to use a **Host-Only** or **Internal Network** in your virtualization software (VirtualBox, VMware, Hyper-V).

Why?

- Creates a private, isolated network where only your Host PC and the VMs can communicate.
- Keeps the lab safe and separate from your home/office internet.

Important:

- **Do NOT connect the server to your real home network with DHCP enabled**, otherwise it may conflict with your home router.
- Keep this lab environment isolated.

Lab 1: Detailed Setup – Static IP, AD, and DNS

Step 1: Configure a Static IP Address on Server

Why?
A Domain Controller must always have the same IP address so clients can reliably connect.

Actions:

1. Start your Windows Server VM and log in as **Administrator**.
2. Open **Server Manager** (auto-starts after login, or search in Start Menu).
3. In the left panel, click **Local Server**.
4. On the right side, find the **Ethernet** link (likely says “IPv4 address not assigned”). Click it.
5. The **Network Connections** window opens.
6. Right-click your active **Ethernet adapter** → Select **Properties**.
7. In the list, select **Internet Protocol Version 4 (TCP/IPv4)** → Click **Properties**.
8. Configure:
    - Select **Use the following IP address**:
        - **IP address**: 192.168.10.1
        - **Subnet mask**: 255.255.255.0
        - **Default gateway**: (leave blank)
    - Select **Use the following DNS server addresses**:
        - **Preferred DNS server**: 192.168.10.1 (points to itself).
9. Click **OK** → Close all windows.

Tip: Run ipconfig in Command Prompt to confirm.

Step 2: Install Active Directory Domain Services (AD DS) & Promote Server

Why?
AD DS turns the server into a Domain Controller. The Domain Controller will store accounts, enforce policies, and control access.

Actions:

1. Open **Server Manager**.

2. Click **Manage** → **Add Roles and Features**.
3. Wizard steps:
    - **Before You Begin** → Next.
    - **Installation Type** → Role-based or feature-based installation → Next.
    - **Server Selection** → Your server → Next.
    - **Server Roles** → Check **Active Directory Domain Services**.
        - Pop-up asks to add features → Click **Add Features** → Next.
    - **Features** → Next.
    - **AD DS Info** → Next.
    - **Confirmation** → Install.
4. Wait for install. Do NOT close the wizard.
5. After install, click the **yellow warning flag** at top → Select **Promote this server to a domain controller**.
6. In **AD DS Configuration Wizard**:
    - **Deployment Configuration**: Select **Add a new forest**.
        - Root domain name: CyberLab.local → Next.
    - **Domain Controller Options**:
        - Forest Functional Level: **Windows Server 2016 (or later)**.
        - Domain Functional Level: **Windows Server 2016**.
        - Ensure **DNS Server** and **Global Catalog (GC)** are checked.
        - Enter a **DSRM password**: Password1! → Next.
    - **DNS Options**: Ignore warning about delegation → Next.
    - **Additional Options**: NetBIOS name should auto-fill as **CYBERLAB** → Next.
    - **Paths**: Leave defaults → Next.
    - **Review** → Confirm → Next.
    - **Prerequisites Check** → Wait until “All prerequisite checks passed”.
    - Click **Install**.
7. Server restarts automatically.

8. Log in with:
    - **Username**: CYBERLAB\Administrator
    - **Password**: (what you set earlier).

You now have a **Domain Controller with DNS installed**.

Step 3: Configure Static IP on Client VM

Actions:

1. Start your **Windows 10/11 Client VM**.
2. Right-click the **Network icon** → **Open Network & Internet Settings**.
3. Click **Change adapter options**.
4. Right-click your Ethernet adapter → **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)** → Click **Properties**.
6. Configure as follows:
    - **Use the following IP address**:
        - **IP address**: 192.168.10.101
        - **Subnet mask**: 255.255.255.0
        - **Default gateway**: 192.168.10.1 (Server's IP).
    - **Use the following DNS server addresses**:
        - Preferred DNS server: 192.168.10.1 (Server's IP).
7. Click **OK** → Close all windows.
8. Open **Command Prompt** → Run ipconfig /all.
    - Confirm:
        - IP = 192.168.10.101
        - DNS = 192.168.10.1.

Step 4: Join Client VM to the Domain

Actions:

1. On the Client VM:

    - Right-click **This PC** → **Properties**.
    - Click **Rename this PC (Advanced system settings → Computer Name tab)**.
    - Click **Change…**.
2. Under **Member of** → Select **Domain**.
3. Enter: CyberLab.local.
4. When prompted:
    - Username: CYBERLAB\Administrator
    - Password: (your password).
5. Success message appears → Restart client.
6. After reboot, log in with a domain account.

Your client is now a member of the **CyberLab.local** domain.

Verification & Troubleshooting

- On **Server**:
    - Run ipconfig → Confirm static IP = 192.168.10.1.
    - Open **Server Manager** → Left panel shows **AD DS** and **DNS** installed.
- On **Client**:
    - Run ipconfig /all → Confirm IP = 192.168.10.101, DNS = 192.168.10.1.
    - Try ping cyberlab.local.
    - Try logging in with CYBERLAB\Administrator.

Beginner-Friendly Lab Guide: Building an AD, DNS (Static IP Only) & Managing OUs, Users, Computers, and GPOs

---

Part 0: Lab Environment Overview

Lab 1: Configure Server with Static IP & Install AD DS/DNS

(already updated – no DHCP, Server = 192.168.10.1, Client = 192.168.10.2, both manual IPs)

Lab 2: Create and Organize OUs

Why?
OUs (Organizational Units) help organize users, computers, and groups. They also let you apply different policies (GPOs) to different departments.

Actions:

1. Log into your **Domain Controller (CYBERLAB\Administrator)**.
2. Open **Server Manager** → Tools → **Active Directory Users and Computers (ADUC)**.
3. In the left pane, expand your domain: CyberLab.local.
4. Right-click the domain name → **New → Organizational Unit**.
5. Enter the name (e.g., "IT", "HR", "Finance", "Computers").
6. Repeat to create multiple OUs:
    - OU=IT
    - OU=HR
    - OU=Finance
    - OU=Computers

Now you have a structure to organize accounts.

Lab 3: Create Users

Why?
Users are the accounts people will log in with on client PCs.

Actions:

1. In ADUC, expand CyberLab.local → Right-click on an OU (e.g., IT) → **New → User**.
2. Fill in details:
    - First name: John
    - Last name: Smith
    - User logon name: jsmith → Next.
3. Enter password (e.g., Password1!).
4. Uncheck "User must change password at next logon" (optional for lab).
5. Finish.

Repeat to create a few test users in different OUs.

Example:

- IT: jsmith
- HR: mjones
- Finance: akhan

Lab 4: Create and Add Computers

Why?
When client machines join the domain, they appear as computer objects in AD. You can pre-create them or let them appear automatically.

Actions:

1. In ADUC, right-click the Computers OU (or your custom "Computers" OU).
2. Select **New → Computer**.
3. Enter a name: CLIENT01 → OK.

*(When you join your Windows 10/11 VM to the domain, it will appear here. You can also move it to another OU by right-click → **Move**.)*

Lab 5: Create a Security Group

Why?
Groups make it easy to assign permissions to multiple users at once.

Actions:

1. In ADUC, right-click an OU (e.g., IT) → **New → Group**.
2. Name: IT_Share_Access.
3. Group scope: **Global**.
4. Group type: **Security**.
5. Click OK.

Now add members:

1. Right-click group → **Properties** → Members → Add.
2. Enter username (e.g., jsmith) → OK.

Now John Smith is part of the IT group.

Lab 6: Create and Link a GPO (Group Policy Object)

Why?
GPOs allow you to enforce rules and settings (e.g., desktop wallpaper, password rules, software installs).

Actions:

1. Open **Group Policy Management** (Server Manager → Tools → Group Policy Management).
2. Expand Forest: CyberLab.local → Domains → CyberLab.local.
3. Right-click your OU (e.g., IT) → **Create a GPO in this domain, and Link it here**.
4. Name the GPO: IT-DesktopPolicy.
5. Right-click the new GPO → **Edit**.

Example Policy: Set Desktop Wallpaper

1. In GPO Editor, go to:
   User Configuration → Administrative Templates → Desktop → Desktop → Desktop Wallpaper.
2. Enable it → Enter path to an image file (e.g., C:\Wallpapers\labwallpaper.jpg).
3. Close editor.

Apply policy:

- On a client machine (joined to domain), log in as a user in the IT OU.
- Run gpupdate /force in Command Prompt.
- The wallpaper should update.

Lab 7: File Sharing with Group Permissions

Why?
Users in a group (like IT) can have access to shared resources.

Actions:

1. On the DC, create a folder: C:\Shares\ITDocs.
2. Right-click → Properties → Sharing → Advanced Sharing.
3. Check **Share this folder** → Share name: ITDocs.
4. Click **Permissions** → Remove "Everyone".
5. Add your group (IT_Share_Access).
6. Give them **Read/Write** → OK → Close.
7. On client PC, log in as jsmith (IT user).
8. Open Run (Win+R) → type:
   \\CYBER-DC\ITDocs
9. You should see and be able to create files in the folder.

Now only IT group members can access the shared folder.

Verification Steps

- Users exist in proper OUs.
- Client PCs appear in the Computers OU.
- GPO applies to correct users (test with different OUs).
- File shares only work for correct groups.

At this point, you've built a **fully functional Active Directory lab** with:

- **Static IP addressing**
- AD DS + DNS (no DHCP)

- OUs for organization
- Users, Computers, and Groups
- GPOs linked to OUs
- Group-based File Sharing