Weekly Schedule

The following is the weekly course schedule for OSM620. It includes topic schedules, assessment due dates, and course work weighting.

This is a working schedule and may be subject to change.

Week 1: September 1-7

Agenda/Topic	Reading	Assessment Due
Introduction to OSM620	Lab 1 - Environment Setup	
Introduction to Microsoft Server 2025 and Virtual Machines	Posted slides and lecture material	

Week 2: September 8-14

Agenda/Topic	Reading	Assessment Due
Microsoft Technologies, Windows Server, and Editions	Lab 2 - Hyper-V, NAT, and Windows Clients	Lab 1 – Environment Setup (2.5%)

Agenda/Topic	Reading	Assessment Due
Demo: Server Installation	Posted slides and lecture material	

Week 3: September 15-21

Agenda/Topic	Reading	Assessment Due
Basic Networking and Security Principles	Lab 3 – Security and Remote Connectivity	Lab 2 - Hyper-V, NAT, and Windows Clients (2.5%)
Demo: VM Interconnectivity and Troubleshooting	Posted slides and lecture material	

Week 4: September 22-28

Agenda/Topic	Reading	Assessment Due
DNS: Concepts and Implementation	Lab 4 - Implementing DNS	Lab 3 – Security and Remote Connectivity (5%)

Agenda/Topic	Reading	Assessment Due
Demo: Hosting DNS	Posted slides and lecture material	

Week 5: September 29 - October 5

Agenda/Topic	Reading	Assessment Due
DHCP: Concepts and Implementation	Lab 5 - Implementing DHCP	Lab 4 - Implementing DNS (5%)
Demo: Hosting DHCP	Posted slides and lecture material	

Week 6: October 6-12

Agenda/Topic	Reading	Assessment Due
Release and Discuss: Assignment 1	Assignment 1	Lab 5 - Implementing DHCP (5%)
Dedicated lab time and lab help (Work Week)	Posted slides and lecture material	Quiz 4

Week 7: October 13-19

Agenda/Topic	Reading	Assessment Due
Review and Lab Help	All previous material	**Midterm Test (15%)**
Midterm Test		Assignment 1 (15%)

Study Week: October 20-26

No classes this week. Campus is open.

Week 8: October 27 - November 2

Agenda/Topic	Reading	Assessment Due
Introduction to Active Directory	Lab 6 - Active Directory	
Demo: AD Creation	Posted slides and lecture material	

Week 9: November 3-9

Agenda/Topic	Reading	Assessment Due
Domain Controllers and RODCs	Lab 6 - Active Directory	
Assignment 2 Discussion: Group Project Creation	Posted slides and lecture material	

Week 10: November 10-16

Agenda/Topic	Reading	Assessment Due
Active Directory Users, Groups, and Group Policies	Lab 7 – Users, Groups, and Group Policies	Lab 6 - Active Directory (5%)
Demo: Applying Group Policies and Downstream Effects	Posted slides and lecture material	

Week 11: November 17-23

Agenda/Topic	Reading	Assessment Due
Server Storage and File Shares	Lab 8 – Configuring Storage	Lab 7 – Users, Groups, and Group Policies (5%)
Demo: Assigning and Mapping Storage	Posted slides and lecture material	

Week 12: November 24-30

Agenda/Topic	Reading	Assessment Due
Introduction to Microsoft Azure and Cloud Computing	Lab 9 – Introduction to Azure	Lab 8 – Configuring Storage (5%)
Demo: Introduction to Azure UI and Access	Posted slides and lecture material	

Week 13: December 1-7

Agenda/Topic	Reading	Assessment Due
Group Project Presentations	Posted slides and lecture material	Group Presentations
		Lab 9 – Introduction to Azure (5%)
		Assignment 2: Group Project (15%)

Week 14: December 8-12

Agenda/Topic	Reading	Assessment Due
Course Review	All previous material	**Final Test (15%)**

Lab 1 - Environment Setup

Lab Preparations

Purpose of Lab 1

In this lab you will stand up the base environment you'll use for the course. You'll obtain official installation media and keys, prepare VMware Workstation, and deploy two servers:

- srv1: **Windows Server 2025 Datacenter, GUI** (Desktop Experience)
- srv2: **Windows Server 2025 Datacenter, CLI** (Core)

You'll complete essential post-install tasks (time zone, naming, activation, updates), then place both servers on a two-NIC layout so they can talk to each other on a private subnet while still reaching the internet for updates.

By the end, the machines are clean, consistent, and ready for later labs (Hyper-V, security hardening, DNS, DHCP, and eventually AD).

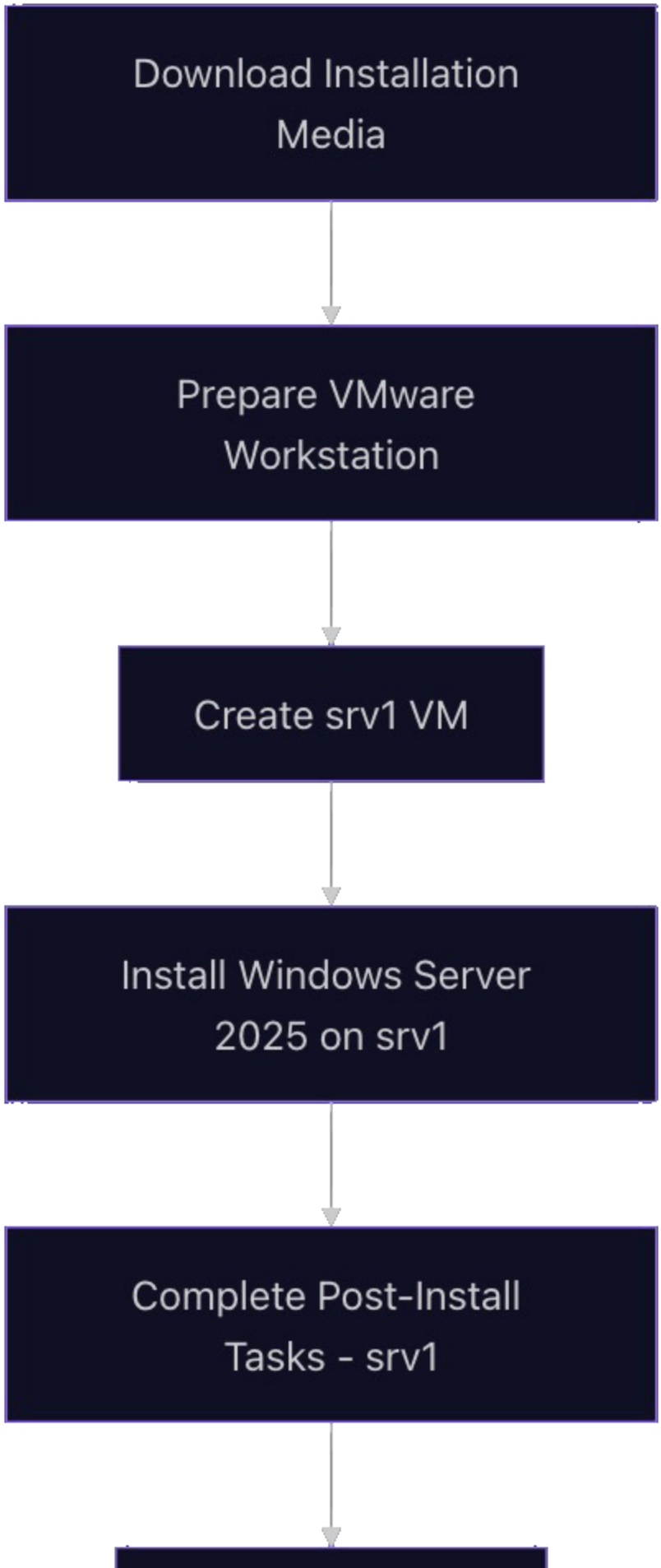
Objectives

By the end of this lab, you will be able to:

- Acquire **Windows Server 2025 Datacenter** installation media and your individual product key from Azure Education and store them securely.
- Access **VMware Workstation** on a Seneca lab PC (locally or via MyApps) or install it on a personal PC.

- Provision two VMs with the required specs and networks:
  - srv1-`senecaUsername` (GUI) with NAT + VMnet10 NICs.
  - srv2-`senecaUsername` (Core) with NAT + VMnet10 NICs.
- Complete essential post-install tasks on each server.
- Verify basic Internet connectivity prerequisites for later labs within each VM.

Here's a basic flowchart of what we'll be doing with Lab 1 to give you a visual overview:


Download Installation Media
Prepare VMware Workstation
Create srv1 VM
Install Windows Server 2025 on srv1
Complete Post-Install Tasks - srv1

Minimum Requirements

Before beginning, you must have:

1. Attended the Week 1 lecture.
2. Read through the Week 1 slides, and have them handy as a reference for concepts.
3. Working access to portal.azure.com with your Seneca credentials.
4. Access to VMware Workstation (Seneca lab PC or personal PC meeting course specs).
5. Your external SSD with at least 500 GB of dedicated space for this course.
6. Your assigned **UID** (from Blackboard Grades) handy for addressing.
7. Your physically printed **OSM620 Lab Logbook** for notetaking and saving commands.
8. Optional, but recommended: Caffeine delivery system.

Investigation 1: Downloading Installation Media

In this investigation, you will be downloading your Windows OS installation media by logging into your Seneca-based Azure account. You will also generate your personal serial keys.

1. Navigate to the Microsoft Azure site: portal.azure.com
2. Use your Seneca e-mail address and password to login.
3. Once on the main Azure page, look for the Search bar at the top of the page.
4. In the Search bar, type: **Education**, then hit Enter.

5. In the **Education | Overview** page, look to the left. You will see menu items already displayed on screen. (*Overview*, *Learning resources*, etc.)
6. Inside **Learning resources** in the left menu, click on **Software**.
7. In the main **Software** page, there is a Search bar just below the word Software (it says *Search* inside it.)
8. In that search field, type and enter: **Windows Server 2025 Datacenter**
9. In the item that appears below (there should only be one), click the link for **Windows Server 2025 Datacenter**.
10. On the right, an information box appears describing the software. Using your mouse to hover over this information box, scroll down to the bottom.
11. You should now see two items: **View Key** and **Download**
12. Click on **Download** first to begin downloading the Server 2025 ISO. You will need this for your operating system installation. (Don't forget where you've saved it!)
13. While the ISO file is downloading, click on **View Key**.
14. Copy this key into a text file that you save locally on your personal computer or personal USB key. You will need this for the Server installation and for any reinstalls later in the semester. **Do not lose this key and do NOT share it with anyone!**
15. Repeat steps 8-14 for the **Windows 11 Education** ISO and serial key. You will need that for later.

> **Reminder:** Always store all serial keys in a secure location only you have access to.

Investigation 2: Using VMware Workstation

The use of *VMware Workstation* is required for this course. You can either use a

Seneca Lab computer (Option 1a / Option 1b) or a personal computer (Option 2).

If you use an external SSD, you can use both!

> **WARNING:** Seneca Lab computers erase any locally saved data when restarted from their internal drives. Save all work to an external drive or online storage.

Option 1a: Seneca Lab Computers w/VMware Workstation Installed Locally

How do you know if your particular Seneca Lab classroom has VMware Workstation installed?

When you log in, the VMware Workstation icon will be visible on the desktop. If it is not, jump to *Option 1b*.

1. Log in to the Seneca workstation with your Seneca username (don't include @myseneca.ca) and password.
2. Once the desktop has fully loaded, double-click on the **VMware Workstation** icon on the desktop. (If not present, jump to *Option 1b* instructions.)
3. When the **VMware Workstation** application appears on screen, continue to the next Investigation.

Option 1b: Seneca Lab Computers *without* VMware Workstation Installed

Do not use this option if your lab computer already has *VMware Workstation* installed. Go back to *Option 1a*.

1. Log in to the Seneca workstation with your Seneca username (don't include @myseneca.ca) and password.
2. Once the desktop has fully loaded, double-click on the **Seneca MyApps** icon on the desktop.
3. In the browser that launches, log in with your Seneca credentials.
4. Do not ignore dialog boxes! Read them carefully instead of just clicking *Cancel* or randomly.
5. In the search bar in the middle of the screen, type *VMware* and hit **Enter.**
6. One result should show up, **VMware WS Pro**. Click this result.
7. In the new *VMware WS Pro* page, click on the version number (Example: 17.6.1). This will launch the application over the network.
8. Click on allow for any dialog boxes that appear. Remember, **do not ignore dialog boxes!**
9. Be patient. It can take a bit for the background files to transfer over the network.
10. When complete, the **VMware Workstation** application should appear on screen. (You will also see the **VMware Workstation** icon on the desktop. You can launch it from here if you accidentally close the program.)
11. Proceed to the next investigation.

Option 2: Personal Computer

Part 1: Computer Hardware Requirements

To run this course and its tech on a personal computer, it must meet the following minimum system requirements:

1. CPU: **6-core Intel/AMD**
2. RAM: **32 GB**
3. Storage: **500 GB SSD free**, *reserved for this course* (if external, USB3.0 or

higher)
4. Internet connection: **High speed, stable**

> **CPU architecture is vital.** You *cannot* use ARM or SnapDragon based computers for this course. This includes all Apple Silicon computers (M1/M2/M3/M4, etc).

Part 2: Registering Your Broadcom Account

Broadcom (formerly VMware) now requires account registration before you can download the VMware Workstation software. Follow the instructions below to do so. You only have to do this once. (If you already have an account using your Seneca e-mail, skip to Part 3.)

1. Visit the Broadcom registration site: profile.broadcom.com/web/registration
2. Provide your Seneca e-mail address and continue.
3. You will be sent a verification code. Check your Seneca e-mail and enter the code on the page.
4. On the *Complete your Registration* page, enter your information and click **Create Account.**
5. On the *Registered Successfully!* page, you can skip the rest and simply click **I'll do it later**.
6. At the top right of the screen, click on the **Login** button. (No, you aren't logged in automatically. Yes, it's annoying.)
7. Enter your Seneca e-mail address as your username and the password you chose on Part 4 as your credentials.
8. When complete, you should see your name in the top right of the screen instead of *Login.* If not, attempt to log in again or ask for help.

Part 3: Downloading VMware Workstation

1. Go to this link: Download VMware Workstation
2. Click on **VMware Workstation Pro 17 for Windows**
3. Click on the highest version available. (17.6.3 as of last update)
4. On the next screen, click on the blue link inside *I agree to the Terms and Conditions* to open a new tab with their terms and conditions. Do not close this window.
5. Back in the previous window/tab that's still open, now click the checkbox for *I agree to the Terms and Conditions*.
6. Click on the little cloud icon next to the name of the download file.
7. Click the **Yes** button when the dialog box pops up.
8. In the *Trade Compliance and Download Conditions* screen, fill in the following school information:
    i. Address1: **1750 Finch Ave E**
    ii. City: **North York**
    iii. State/Province: **Ontario**
    iv. Country: **Canada**
    v. Zip/Postal Code: **M2J 2X5**
9. ***Finally*** click on the cloud icon again to begin the actual download.
10. If you ever need to download the software again, you won't have to go through any of the registration mess. Follow Part 3, Steps 1-3, then Part 9.

Part 4: Install VMware Workstation

1. Find the downloaded .exe file and run the installer.
2. Follow all prompts and install.

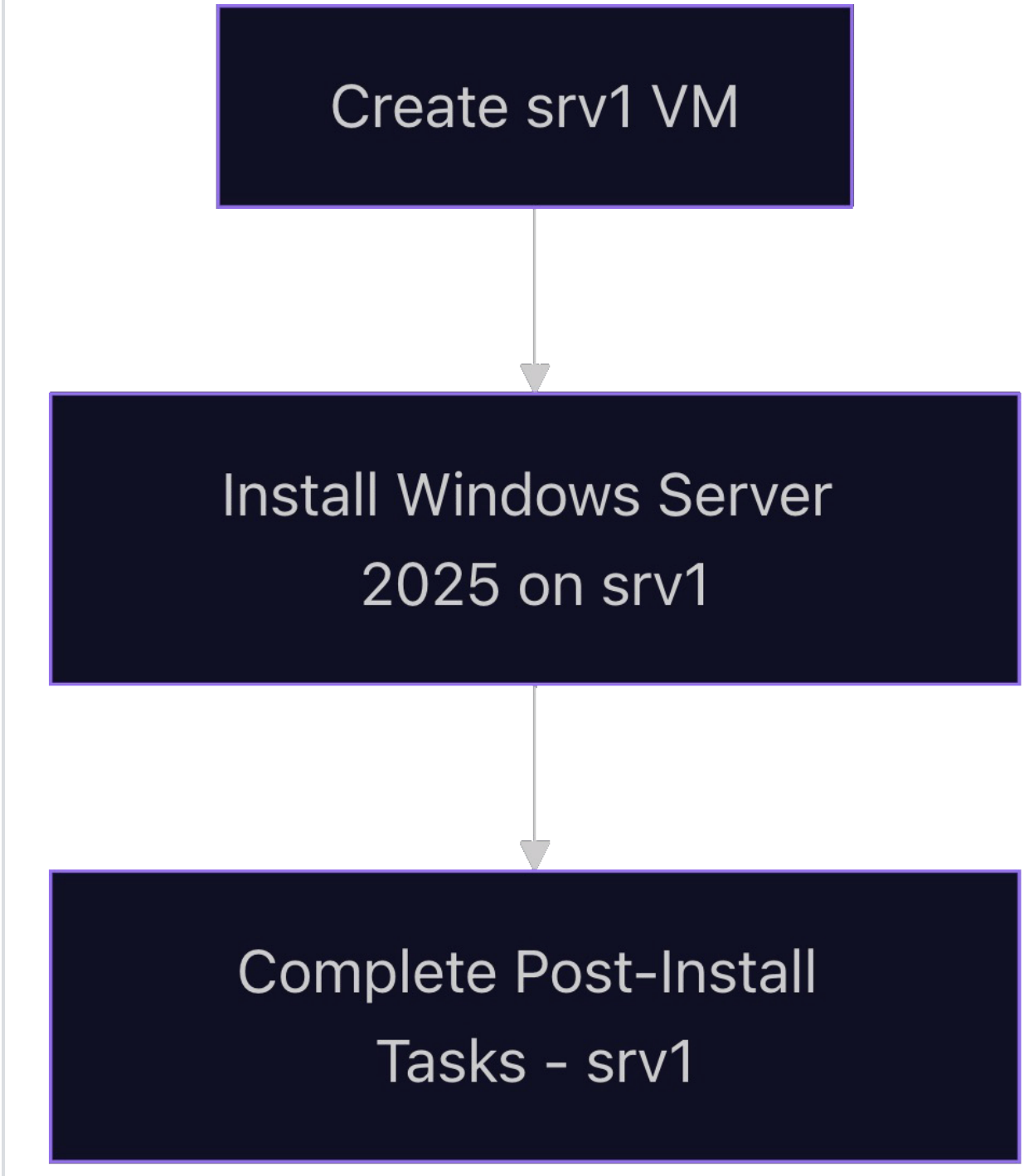
Part 5: Launch VMware Workstation

1. Open **VMware Workstation** from your desktop or the Start Menu.
2. When asked, paste in your serial key.
3. Proceed to the next Investigation.

Investigation 3: VM1 Installation - Windows Server 2025 Datacenter (*srv1*)

- Hypervisor: **VMware Workstation**
- Name: **srv1-cjohnson30**
- RAM: **16 GB**
- CPU: **6 cores**
- Storage: **250 GB**
- Networking: **2 NICs**
- ISO: **Windows Server 2025**

Flowchart Visualization of Investigation 3



Part 1: Setup Instructions

1. In the main window, you should see a large + symbol icon titled **Create a New Virtual Machine**. Click it.

2. In the new dialog box, keep *Typical* selected and click the **Next** button.

3. On the next screen, *Guest Operating System Installation*, do the following:

    i. Select *Installer disc image file (ISO):*

    ii. Now click **Browse**.

    iii. Navigate to where you saved your ***Windows Server 2025 Datacenter*** downloaded ISO and select it.

    iv. Once selected, the previous screen should now say:

    > **Windows Server 2025 detected.**
    >
    > This operating system will use Easy Install.

    v. If it doesn't, you haven't selected the right file, or your download was corrupted. **Ask for help.**

    vi. Click **Next**.

4. On the "Easy Install Information" screen, do the following:

    i. Paste in your serial key.

    ii. Version of Windows to install: Select *Windows Server 2025 Datacenter*

    iii. Personalize Windows:

        a. Full Name: **Administrator**

b. Password (both fields): Select a strong password **you will remember**. You will use this same password for all VMs in this course.
c. ***Do not select "Log on automatically"***.
d. Click **Next**.

5. On the "Name the Virtual Machine" screen, do the following:

i. Virtual machine name: **srv1-*senecausername***

> **Explanation:** For example, if my Seneca e-mail address is `cjohnson30@myseneca.ca`, then my Seneca username is *cjohnson30*. This would give me a VM name of *srv1-cjohnson30*.

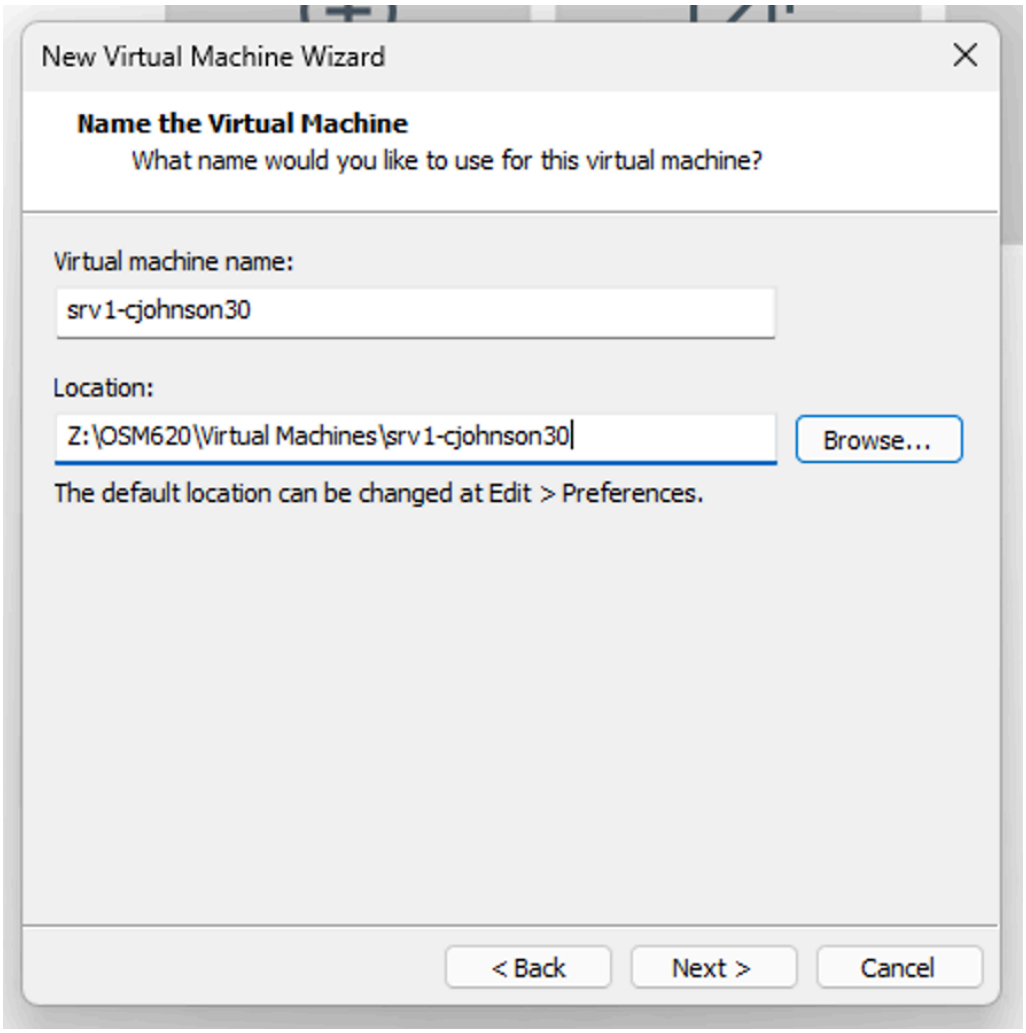
ii. Location: If using an external SSD (like with our lab computers), click **Browse** and navigate to your external SSD.

a. Create the following directory structure in your SSD: *OSM620 > Virtual Machines/srv1-cjohnson30*

b. Select this new *srv1-cjohnson30* folder.

c. Make sure you now see this change in the Location field.

> **Example:** *Z:\OSM620\Virtual Machines\srv1-cjohnson30*



iii. Click **Next**.

6. On the "Specify Disk Capacity" screen, do the following:

   i. Maximum disk size (GB): **250**
   ii. Select *Split virtual disk into multiple files*.
   iii. Click Next.

7. On the "Ready to Create Virtual Machine" screen, do the following:

   i. Click on **Customize hardware...**

8. On the new "Hardware" screen, do the following:
    i. Select *Memory*, and change the value to: **16384**
    ii. Select *Processors*, and change:
        a. Number of processors: **1**
        b. Number of cores per processor: **6**
        c. Virtualize Intel VT-x/EPT or AMD-V/RVI: **Checked**
        d. Virtualize CPU performance counters: ***Unchecked***
        e. Virtualize IOMMU (IO memory management unit): **Checked**
    iii. Select *Network Adapter* and confirm:
        a. *Connected at power on:* **Checked**
        b. *NAT*: **Checked**
    iv. Click on the ***Add...*** button on the bottom left of the *Hardware* window.
        a. Select *Network Adapter* and click **Finish**.
        b. Back in the *Hardware* window, click on *Network Adapter 2*.
        c. Under *Network connection*, click the **Custom: Specific virtual network** radio button.
        d. Just below that, click the drop-down (it likely says *VMnet0* by default). Find and select **VMnet10**.
        e. Click **Close**.
9. Back in the "Ready to Create Virtual Machine" screen, click **Finish**.
10. The virtual machine should launch.
11. If you get a dialog box about *Side channel mitigations*, check the box for *Do not show this hint again* and click **OK**.
12. Your new Virtual Machine should now finish creating and then turn on and begin the OS installation.

13. Windows installation is automated at this point and won't require any input from you. It may restart several times.

    > **Time Note:** Installation may take some time.
    >
    > Feel free to get some caffeine or make a sandwich.

14. Eventually, you will be presented with the desktop and the VMware Tools installer having completed and asking if you'd like to restart. Choose **Yes**.

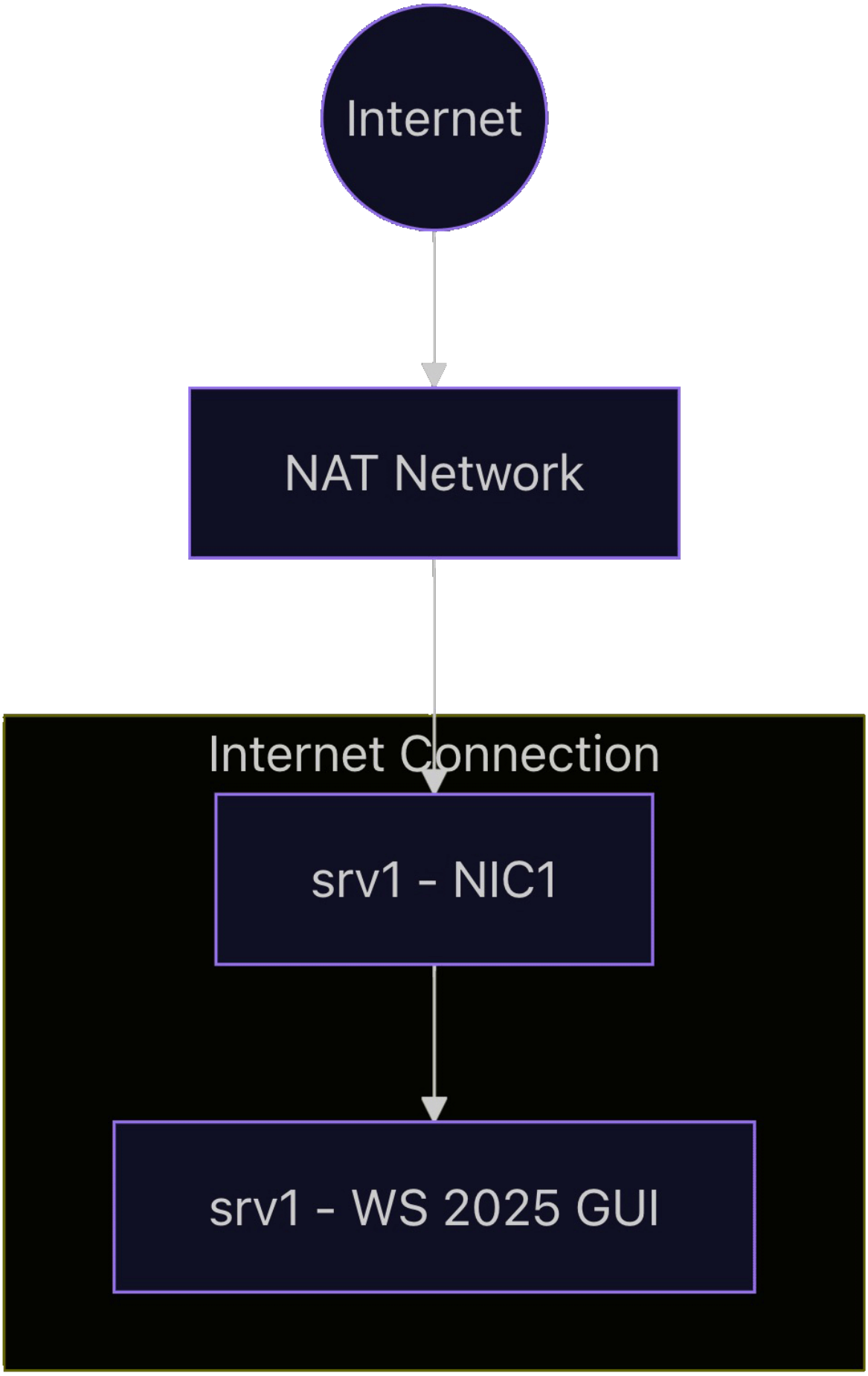
15. Once you've restarted, your installation is complete.

Investigation 4: Post-Installation Tasks (*srv1*)

After installing a new operating system, there are always a number of **post-installation tasks** to complete. **These aren't optional!**

Overview Check-In: *srv1* Internet Connection

Let's take a quick look at an overview of our NAT Internet connection as it currently stands. It's important to understand how everything is connected.


Internet
NAT Network
Internet Connection
srv1 - NIC1
srv1 - WS 2025 GUI

Part 1: Applying Time Zone Settings

This one is fairly straight-forward. Having the proper time zone set (EST) is essential for proper time keeping and ensuring encrypted webpages connect properly.

1. In the *Server Manager* application, click on **Local Server** in the left-hand menubar.
2. In the main *Properties* area, on the right-hand column, look for the *Time Zone* line. It should say **(UTC-05:00) Eastern Time (US & Canada)**.
3. If the *Time Zone* line item doesn't say the above, click on the displayed time zone and change it to UTC-05:00 as seen above.

Part 2: Server Name Change

The default name applied to your new server will be semi-randomized. For proper identification (and to not wonder which server you're on when you have several), we're going to change this.

1. In the *Server Manager* application, click on **Local Server** in the left-hand menubar.
2. In the main *Properties* area, on the left-hand column, look for the *Computer name* line.
3. Click the current computer name.
4. In the *System Properties* dialog box that pops up, find the **Change** button and click it. (Ignore the *Computer Description* field. It's tempting, but wrong!)
5. In the new *Computer Name/Domain Changes* dialog box that pops up, find the *Computer name* field. Replace it with **srv1-SenecaUsername**.
6. When you click **OK**, the system will warn you about restarting. Choose to

restart the system when asked.

7. Once you've restarted and logged back in, go back to the *Server Manager* from Part 1 and double-check your new computer name is correct. **Do not skip this step!**
8. If it is, you're done!

Part 3: Windows Activation

Activating Windows unlocks certain settings and features. Since you've used your valid serial key (right?), you can activate with Microsoft easily.

1. In the *Server Manager* application, click on **Local Server** in the left-hand menubar.
2. In the main *Properties* area, on the right-hand column, look for the *Product ID* line.
3. Click on the **Not activated** link.
4. Follow the instructions in the popup dialog box. If unable to activate easily, **ask your professor for help**.

Part 4: Installing OS Updates

A critical part of a security-conscious mindset is running regular updates. **This is NOT something you do only once at the start of installation.** You should be running these regularly to keep up to date with security fixes and zero-day exploits.

1. If you're already in the *Settings* application, look through the left menubar for **Windows Update** and click it. (Otherwise, click on the *Start* menu and search for **Updates**.)
2. In the *Windows Update* main screen, scroll down to **Advanced Options** and click it.

3. The very first option is *Receive updates to other Microsoft products*. Toggle this from **Off** to **On**.
4. At the top of the screen, where it says *Windows Update > Advanced Options*, click **Windows Update** to go back to the previous screen.
5. You will likely already see updates ready. Click on **Download & install all**.
6. As you might expect, this can take a while. Timing will depend on your Internet connection, how fast your computer is, how fast your SSD is, and how many updates there are. Please be patient. Your computer may restart.
7. Once updates have begun, take a break while it does its thing. Grab a drink, make a sandwich, text a friend.
8. After updates are complete, go back into *Windows Update* and click **Check for updates** again. There may be (and often times are) more.
9. If there are more updates, complete Steps 5-8 again until there are no more updates available.
10. In *Windows Update*, scroll back down to **Advanced options** again and click it.
11. Inside *Windows Update > Advanced options* scroll down to **Optional updates** and click it.
12. Select all available updates that appear (you may have to expand some lists).
13. Click **Download & install**.
14. Once all updates are complete, restart your VM if asked, then move onto the next section.

Part 5: Internet Connectivity Check w/Edge

We'll double-check we can access the Internet using the built-in Microsoft Edge application.

1. Open *Microsoft Edge*.
2. Go through the first-run questions.
3. When able, use the browser to navigate to **eff.org**.
4. If the website loads, move on to the next step. If not, **ask your professor for help**.

Part 6: Download and Install Firefox

There are a ton of feature and privacy reasons *not* to use Microsoft Edge. Instead, we'll download and install **Mozilla Firefox** and use that going forward.

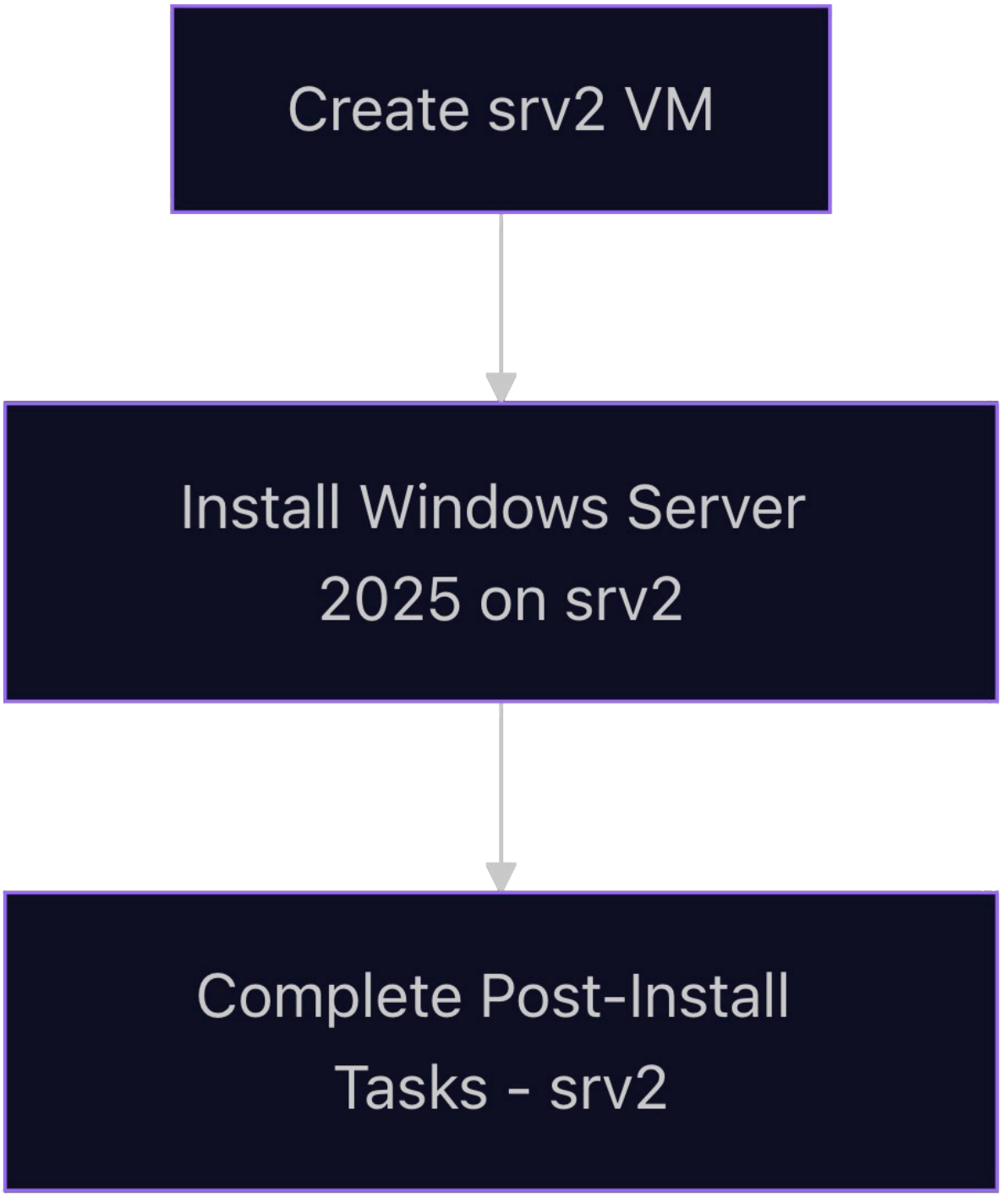
1. Open *Microsoft Edge*.
2. Navigate to: Download Mozilla Firefox
3. Wait for the installer to finish, then open it.
4. Follow the installer instructions.
5. Once complete, open *Firefox* and navigate to **eff.org** to check everything is okay.
6. Close *Microsoft Edge* forever.

Investigation 5: VM2 Installation - Windows Server 2025 Core (*srv2*)

- Hypervisor: **VMware Workstation**
- Name: **srv2-cjohnson30**
- RAM: **4 GB**
- CPU: **2 cores**
- Storage: **250 GB**

- Networking: **2 NICs**
- ISO: **Windows Server 2025**

Flowchart Visualization of Investigation 5



Part 1: Setup Instructions

1. In the main window, you should see a large + symbol icon titled **Create a New Virtual Machine**. Click it.

2. In the new dialog box, keep *Typical* selected and click the **Next** button.

3. On the next screen, *Guest Operating System Installation*, do the following:

    i. Select *Installer disc image file (ISO):*
    ii. Now click **Browse**.

        a. Navigate to where you saved your ***Windows Server 2025 Datacenter*** downloaded ISO and select it.

        b. Once selected, the previous screen should now say:

        > **Windows Server 2025 detected.**
        >
        > This operating system will use Easy Install.

        c. If it doesn't, you haven't selected the right file, or your download was corrupted. **Ask for help.**

    iii. Click **Next**.

4. On the "Easy Install Information" screen, do the following:

    i. Paste in your serial key.
    ii. Version of Windows to install: Select *Windows Server 2025 Datacenter **(Core)***
    iii. Personalize Windows:
        a. Full Name: Administrator

b. Password (both fields): Select a strong password **you will remember**. You will use this same password for all VMs in this course.

iv. ***Do not select "Log on automatically"***.

v. Click **Next**.

5. On the "Name the Virtual Machine" screen, do the following:

   i. Virtual machine name: **srv2-*senecausername***

   > **Explanation:** For example, if my Seneca e-mail address is `cjohnson30@myseneca.ca`, then my Seneca username is *cjohnson30*. This would give me a VM name of *srv2-cjohnson30*.

   ii. Location: If using an external SSD (like with our lab computers), click **Browse** and navigate to your external SSD.

      a. Create the following directory structure in your SSD: *OSM620 > Virtual Machines > srv2-cjohnson30*

      b. Select this new *srv2-cjohnson30* folder.

      c. Make sure you now see this change in the Location field. (Example: *Z:/OSM620/Virtual Machines/srv2-cjohnson30*)

   iii. Click **Next**.

6. On the "Specify Disk Capacity" screen, do the following:

   i. Maximum disk size (GB): **250**

   ii. Select *Split virtual disk into multiple files*.

   iii. Click Next.

7. On the "Ready to Create Virtual Machine" screen, do the following:

   i. Click on **Customize hardware...**

8. On the new "Hardware" screen, do the following:
    i. Select *Memory*, and change the value to: **4096**
    ii. Select *Processors*, and change:
        a. Number of processors: **1**
        b. Number of cores per processor: **2**
        c. Virtualize Intel VT-x/EPT or AMD-V/RVI: **Checked**
        d. Virtualize CPU performance counters: ***Unchecked***
        e. Virtualize IOMMU (IO memory management unit): **Checked**
    iii. Select *Network Adapter* and confirm:
        a. *Connected at power on:* **Checked**
        b. *NAT*: **Checked**
    iv. Click on the ***Add...*** button on the bottom left of the *Hardware* window.
        a. Select *Network Adapter* and click **Finish**.
        b. Back in the *Hardware* window, click on *Network Adapter 2*.
        c. Under *Network connection*, click the **Custom: Specific virtual network** radio button.
        d. Just below that, click the drop-down (it likely says *VMnet0* by default). Find and select **VMnet10**.
        e. Click **Close**.
9. Back in the "Ready to Create Virtual Machine" screen, click **Finish**.
10. The virtual machine should launch.
11. If you get a dialog box about *Side channel mitigations*, check the box for *Do not show this hint again* and click **OK**.
12. Your new Virtual Machine should now finish creating and then turn on and begin the OS installation.

13. Windows installation is automated at this point and won't require any input from you. It may restart several times.

    > **Time Note:** Installation may take some time.
    >
    > Feel free to get some caffeine or make a sandwich.

14. Eventually, you will be presented with the Command Prompt window open to the *SConfig* text-based application, and the VMware Tools installer having completed and asking if you'd like to restart. Choose **Yes**.

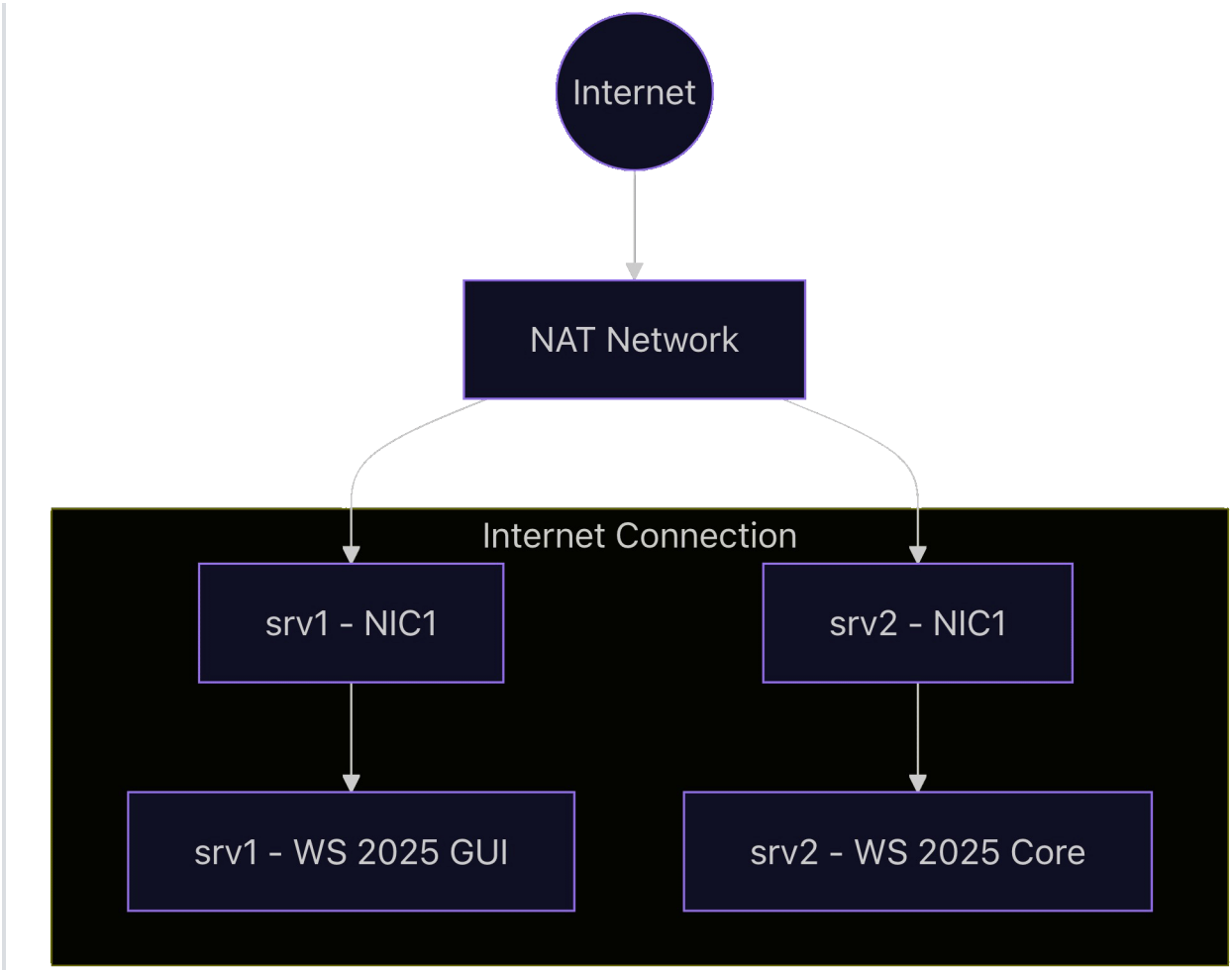
15. Once you've restarted, your installation is complete.

Investigation 6: Post-Installation Tasks (*srv2*)

After installing a new operating system, there are always a number of **post-installation tasks** to complete. **These aren't optional!**

Overview Check-In: srv2 Internet Connection

Let's take a quick look at an overview of our NAT Internet connection as it currently stands since our newest server addition. It's important to understand how everything is connected as we continue to build out our VMs.



Part 1: Applying Time Zone Settings

This one is fairly straight-forward. Having the proper time zone set (EST) is essential for proper time keeping and ensuring encrypted webpages connect properly.

1. In the *SConfig* application, select Option 9 (*Date and Time*). Use your keyboard.
2. The *Date and Time* dialog box pops up.
3. Look for the *Time Zone* line. It should say **(UTC-05:00) Eastern Time (US & Canada)**.
4. If the *Time Zone* line item doesn't say the above, click on the *Change time zone...* button and change it to UTC-05:00 as seen above.

5. Click **OK** to close out of *Date and Time*.
6. Back in *SConfig*, choose Option 9 again to confirm your changes have stuck. If yes, continue to Part 2.

Part 2: Server Name Change

The default name applied to your new server will be semi-randomized. For proper identification (and to not wonder which server you're on when you have several), we're going to change this.

1. In the *SConfig* application, select Option 2 (*Computer name*). Use your keyboard.
2. In the new *Computer name* screen, enter your new computer name in the waiting text field: **srv2-SenecaUsername**
3. Press **Enter** on your keyboard to confirm the change.
4. The system now asks you about restarting. Enter **Y** to choose yes and hit the **Enter** key to confirm.
5. Once you've restarted and logged back in, go back to the *Computer name* screen from Part 2 and double-check your new computer name is correct. **Do not skip this step!**
6. If it is, you're done!

Part 3: Windows Activation

Activating Windows unlocks certain settings and features. Since you've used your valid serial key (right?), you can activate with Microsoft easily.

1. In the *SConfig* application, select Option 11 (*Windows activation*). Use your keyboard.
2. In the new *Windows activation* screen, enter **2** (*Activate Windows*) and hit **Enter** to begin the activation process with Microsoft.
3. Follow the instructions on screen. If unable to activate easily, **ask your professor for help**.

Part 4: Installing OS Updates

A critical part of a security-conscious mindset is running regular updates. **This is NOT something you do only once at the start of installation.** You should be running these regularly to keep up to date with security fixes and zero-day exploits.

> **IMPORTANT:** If Windows Update fails with errors, you may have Internet connectivity issues. Ask your professor for help!

1. In the *SConfig* application, select Option 5 (*Update settings*). Use your keyboard.
2. In the new *Update setting* screen, enter **5** (*Opt-in to Microsoft Update*) and hit **Enter** to confirm.
3. The next screen will ask you confirm again. Enter **y** and hit **Enter** to continue. (Then, hit **Enter** again.)
4. In the *SConfig* application, select Option 6 (*Install updates*). Use your keyboard.
5. In the new *Install updates* screen, enter **1** (*All quality updates*) and hit **Enter** to confirm.
6. After a short check, you are asked which updates to install. Select **a** to install all updates and hit **Enter** to confirm.
7. As you might expect, this can take a while. Timing will depend on your Internet connection, how fast your computer is, how fast your SSD is, and how many updates there are. Please be patient.
8. Once updates have begun, take a break while it does its thing. Grab a drink, make a sandwich, text a friend.
9. If asked to restart, choose **yes**.
10. After updates are complete, go through Steps 4-6 again. Do so until the system tells you there are no new updates. (It may take a few cycles to get them all.)
11. When complete, shut down *srv2* safely. Use the on-screen menu options in

SConfig to do so.

That's it! Now you're done. Congratulations!

Lab 1 Sign-Off

It is extremely important that you complete Lab 1 correctly as these Windows Server installs will be the platform on which the rest of the course will be completed.

When you have completed Lab 1, ask your instructor to come and check your installation. This must be done in class. They will ask you to complete a set of tasks/commands. If everything has been completed correctly, your instructor will mark your Lab 1 as complete.

Sign-Off Checklist

1. Open VMware Hardware Settings window for *srv1* and *srv2*.
2. *srv1* is currently running and logged in.
3. *srv2* is currently running and logged in.
4. No new updates available for both VMs.
5. Server names have been applied correctly.
6. Time zone is in EST.
7. Servers have been properly activated.
8. *srv1*: Firefox installed and open.

Lab 2 - Hyper-V, NAT, and Windows Clients

Lab Preparations

Purpose of Lab 2

In this lab, you'll move beyond basic VM deployment and learn to create nested virtualization environments. This is a crucial skill for modern sysadmins and cloud architects. You'll enable the Hyper-V role on your Windows Server, build a secure internal network using Hyper-V switches, and deploy Windows 11 client VMs within your existing server VM. You'll also set up NAT and routing, allowing your nested clients to access the internet safely through your server.

By the end, you'll have a working mini-enterprise: one physical computer running a server VM, which itself is hosting client VMs. Just like real-world cloud and enterprise setups! You'll gain hands-on experience with Hyper-V, RRAS, and NAT, and build a technical foundation for future labs in DHCP, DNS, and security.

Objectives

By the end of this lab, you will be able to:

- Enable the Hyper-V role on a Windows Server 2025 VM and configure virtual networking.
- Build and configure a Hyper-V External Virtual Switch bound to a specific NIC.
- Set up Routing and Remote Access (RRAS) for network address translation

(NAT) between internal and external networks.

- Deploy Windows 11 client VMs inside Hyper-V, configuring hardware and storage as needed.
- Assign static IPs and ensure that internal client VMs can reach the internet via NAT on your server.
- Practice real-world sysadmin tasks: managing nested VMs, routing, and internal networks.

Minimum Requirements

Before beginning, you must have:

1. Completed Lab 1 in full, with both srv1 and srv2 working, activated, and updated.
2. Attended the Week 2 lecture, or carefully read through the Week 2 slides.
3. Downloaded the Windows 11 Education ISO and your product key (from Lab 1).
4. Access to VMware Workstation and your external SSD with at least 200 GB of free space remaining.
5. Your printed OSM620 Lab Logbook for notetaking and command recording.
6. A basic understanding of server roles, virtual networking, and Windows installation processes.
7. Caffeine or snack of your choice: nested virtualization can be a long process!

Investigation 1: Hyper-V Role Installation and Switch Setup *(srv1)*

In this investigation, you will install the Hyper-V role on srv1 and create a Hyper-V virtual switch that uses your existing Internal Network adapter.

Your Hyper-V switch will be named Internal Network (Hyper-V).

Part 1: Install the Hyper-V Role

1. Open the **Server Manager** application and go to **Add Roles and Features**.
2. **Installation Type:** Keep Role-based or feature-based installation selected.
3. **Server Selection:** Ensure your local server (*srv1*) is selected.
4. **Server Roles:** Check ***Hyper-V***.
    i. When prompted to "*Add features that are required for Hyper-V*", click **Add Features**.
5. **Features:** Leave defaults (the *Hyper-V Management Tools* are already included).
6. **Hyper-V page**:
    i. When asked about Virtual Switches, select **Internal Network** only.
    ii. Migration for live migrations: leave unchecked.
    iii. Default Stores: leave defaults.
7. Confirmation: Check "*Restart the destination server automatically if required*".
8. Click **Install**.
9. Wait for installation to complete. If prompted, allow the reboot. Log back in

when finished.

> **Note:** It’s normal for *Server Manager* to take a minute or two after reboot to show the Hyper-V tile.

Part 2: Rename the Hyper-V Virtual Switch

As part of our Hyper-V role installation, we selected the *Internal Network* (Part 1, Step 6.1).

This has created a virtual switch on the server. For easy management, we'll rename it.

Our new virtual switch name will be: `HQ Network`

1. In Server Manager, click Tools (top-right) and select Hyper-V Manager.
2. In the left pane, click your server name (e.g., srv1-...).
3. In the right Actions pane, click Virtual Switch Manager....
4. Under the Virtual Switches column on the left, look for the switch that's already been created. It will likely have a name similar to: `Intel(R) 82574L Gigabit Network Connection - Virtual Switch`
5. In the Virtual Switch Properties window:
    i. Name: Change to `HQ Network`
    ii. Ensure the **External network** radio button is selected.

    > **Reminder:** This is the adapter you renamed earlier to Internal Network and set to 10.0.`UID`.1.

iii. Ensure "*Allow management operating system to share this network adapter*" is checked.

iv. Click OK. If you see a warning about temporary network disruption, click Yes.

> **Naming note:** You are creating an External Hyper-V switch, but you're binding it to the Windows NIC you named Internal Network.
>
> That's correct.
>
> You will end up with a third network adapter called: `vEthernet (HQ Network)`

6. Go back to *Server Manager > Local Server* and refresh. You should now see the following two networks:
   - **External Network**: Assigned by DHCP
   - **vEthernet (HQ Network)**: IPv4 addess assigned by DHCP, IPv6 enabled

Part 3: Configure Network Setting for Hyper-V Switch

Now that we've created the Hyper-V network adapter, we have to give it an IP address. This will let our Hyper-V VMs talk to the server, and eventually, bridge our Internet connection.

1. In *Server Manager > Local Server*, click on the entry next to **vEthernet (HQ Network)**. This opens the *Network Connections* window.
2. Verify you now see a third network adapter: `vEthernet (HQ Network)`
3. Right-click it → Properties and do the following:

i. Internet Protocol Version 6 (TCP/IPv6): **Unchecked**
ii. Internet Protocol Version 4 (TCP/IPv4): Select and click **Properties**
    a. IPv4 Address: **10.0.`UID`.1**
    b. Subnet Mask: **255.255.255.0**
    c. Leave all other fields blank and click OK.
4. Back in *Server Manager > Local Server*, refresh. You should now see the following two networks:
    - **External Network**: Assigned by DHCP
    - **vEthernet (HQ Network)**: 10.0.`UID`.1

Investigation 2: RRAS and NAT

Our server now has access to two networks:

- **External Network**: Connection to the Internet
- **vEthernet (HQ Network)**: Internal network only between *srv1* and the Hyper-V VMs we'll create in Investigation 3. This network *does not* have access to the Internet.

If we want to give our Hyper-V machines Internet access, we need to route network traffic between the two networks using *srv1* as a bridge. This keeps our Hyper-V machines on a secure network, and Internet access is handled and monitored by our Windows Server.

This will involve setting up routing and network address translation (NAT).

Welcome to Microsoft's **Routing and Remote Server (RRAS)**.

Part 1: Installing the Remote Access Role

1. Open the **Server Manager** application and go to **Add Roles and**

Features.

2. **Installation Type:** Keep Role-based or feature-based installation selected.
3. **Server Selection:** Ensure your local server (*srv1*) is selected.
4. **Server Roles:** Check ***Remote Access***.
5. **Features:** Leave defaults (the *Hyper-V Management Tools* are already included).
6. **Remote Access page:** Click Next.
    i. The **Add Roles and Features Wizard** dialog box appears. Leave defaults and select *Add Features*.
7. **Remote Access > Role Services page:** Check the following and click *Next* when ready:
    - Direct Access and VPN (RAS)
    - Routing
8. Keep defaults and select *Next* on the following pages:
    i. Web Server Role (IIS)
    ii. Web Server Role (IIS) > Role Services
9. Confirmation: Click **Install**.
10. In the **Results** page: When installation has completed, click on the "*Open the Getting Started Wizard*" link.
11. The wizard opens. Make no changes and close it. (This just removes the system nagging.)
12. Back in **Results**, click Close.

Part 2: Enabling NAT with RRAS

You will now install the tools for routing and NAT bridging discussed at the top of this investigation using the **Routing and Remote Access Server** (RRAS) we've just installed.

1. Open the **Server Manager** application and go to **Tools > Routing and**

Remote Access.

2. This opens the *Routing and Remote Access* application.
3. In the right-hand column, find SRV1, right-click it, and select **Configure and Enable Routing and Remote Access**.
4. The setup wizard appears. Click *Next*.
5. **Configuration:** Select the *Custom configuration* radio button.
6. **Custom Configuration:** Select (checkbox) only the following:
    - NAT
    - LAN routing
7. **Summary window**: Click *Finish*.
8. The **Routing and Remote Access** service status dialog box appears. Click *Start service*.
9. It may take a few moments for the service to fully start. Be patient.
10. Once the *Routing and Remote Access* application reappears, move to the next part.

Part 3: Configuring NAT with RRAS

It's now time to configure the routing and NAT bridging between the two networks.

1. Open the **Routing and Remote Access** application.
2. In the right-hand column, expand *SRV1*, then expand *IPv4*.
3. Right-click on *NAT* and select *New Interface*.
4. Select the **External Network** entry and click *OK*.
5. In the *Network Address Translation Properties* window, select the following and click OK when ready:
    - Public interface connected to the Internet
    - Enable NAT on this interface

6. Right-click on *NAT* and select *New Interface* again.
7. Select the **vEthernet (HQ Network)** entry and click OK.
8. In the *Network Address Translation Propertie*s window, select the following and click OK when ready:
    - Private interface connected to private network
9. Back in the *NAT* window, you should see two created interfaces:
    - External Network
    - vEthernet (HQ Network)
10. Keep the application open on *NAT* and minimize. We'll come back to it later.
11. That's it! Move on to the next Investigation.

Investigation 3: Installing Windows Client 1 with Hyper-V *(client1)*

In this investigation, you'll create your first Hyper-V based virtual machines.

These will be Windows 11 client machines. Think of these as typical workstations in a corporate office.

Part 1: Creating the Hyper-V Virtual Machine

- Hypervisor: **Hyper-V**
- Name: **client1-**`SenecaUsername`
- RAM: **4 GB**
- CPU: **2 processors**
- Storage: **64 GB**
- NIC: **1** (default)
- Security: **Enable Trusted Platform Module**

- ISO: **Windows 11 Education**

1. Drag and drop the *Microsoft Windows 11 ISO* file from Lab 1 onto the desktop of *srv1*. It should copy the file there. If it doesn't, ask your professor for help before continuing.
2. Open the **Server Manager** application and go to **Tools > Hyper-V Manager**.
3. This opens the *Hyper-V Manager* application.
4. In the right-hand column, click on **New > Virtual Machine...**
5. The *New Virtual Machine Wizard* appears.
6. On the *Before You Begin* page, check the **Do not show this page again** option and click **Next**.
7. **Specify Name and Location**:
   - Name: **client1-**`SenecaUsername`
   - Leave the rest at their defaults.
8. **Specify Generation:** Leave defaults.
9. **Assign Memory:** 4096 MB
10. **Configure Networking:**
    - Connection: **HQ Network**
11. **Connect Virtual Hard Disk:**
    - **Create a virtual hard disk** selected.
    - Size: **64 GB**
    - Leave the rest at their defaults.
12. **Installer Options:**
    - Select **Install an operating system from a bootable CD/DVD-ROM**
    - Select **Image file (.iso):**
    - Click **Browse** and select the Windows 11 ISO image file you copied to *srv1*.

13. **Summary:** Click *Finish*.

> **WARNING:** Do not start the *client1* VM, yet! We need to modify it. See *Part 2*.

Part 2: Modifying *client1* VM for Windows 11

Despite Hyper-V being a Microsoft product and Windows 11 being a Microsoft product, Hyper-V doesn't automatically add everything needed to run Windows 11.

If you think this is silly... It is. Welcome to the wonderful world of IT.

1. In the **Hyper-V Manager** application, select the *client1* VM.
2. In the right-hand column, look for and click on the **Settings...* option.
3. This opens up the settings window for the *client1* VM. Change the following:
4. **Processor:**
    - Number of virtual processors: **2**
    - Make sure to click **Apply**!
5. **Security:**
    - Encryption Support > Enable Trusted Platform Module: **Checked**
    - Make sure to click **Apply**!
6. Click **OK** to close the VM settings window.

Part 3: Hyper-V Client Management

Knowing how to power on and off your Hyper-V VM is important and includes a few cool features.

In the **Hyper-V Manager** application, select the **client1** VM. (Single click. Do

not double-click.)

On the right-hand column, towards the bottom, you have:

- **Connect**: This *connects* to the VM. It will open a virtual monitor to the machine. Just like a normal computer, if the computer (VM) is off, connecting to it will do nothing but give you a blank screen.
- **Settings**: You used this in *Part 2*. Modify VM settings. Don't change anything unless told to.
- **Start**: Power on the VM. If you are already connected to it, you will see it power up. If not connected, it still powers up. Click on **Connect** to open a screen to it.

When the VM is powered on, you have additional options in that column:

- **Turn Off:** This is the equivalent of pulling the power plug. Don't do this unless the VM is fully frozen and not responding from commands. (This is the "*Nuke it from orbit.*" option. It works, but it's overkill and may cause damage.)

- **Shut down:** This is the polite version of the option above. Hyper-V will send a gentle "Please shut down." command to the Windows 11 client. If the Windows 11 client is working, it'll close all applications and shut down properly. Hyper-V detects the OS having shut down and then powers off the VM itself. (**This is your preferred option.**)

- **Reset:** Equivalent to pressing the *Reset* physical button on a computer. Yanks the power and then turns it back on. AKA "*Nuke and reload.*" (Again, don't use unless unresponsive.)

- The **Start** button disappears when the VM is on, which makes sense.

There are other options, but those are enough to get by for now.

> **IMPORTANT:** Always safely shut down all Hyper-V VMs before shutting down your Windows Server!

Part 4: Installing Windows 11 (*client1*)

1. Once the Windows 11 Setup screen appears:
2. On *Select language settings*, keep the defaults and click **Next**.
3. On *Select keyboard settings*, keep the defaults and click **Next**.
4. On *Select setup option*, do the following:
    i. Select *Install Windows 11*
    ii. Check the box next to *I agree everything will be deleted, including files, apps, and settings*
    iii. Click **Next**.
5. On the *Product key* page, enter your product key and click **Next**.
6. On *Applicable notices and license terms*, click **Accept**.
7. On *Select location to install Windows 11*, keep the defaults and click **Next**.
8. On *Ready to install*, click **Install**.
9. The Windows Installer will now install the OS. This may take some time, and the percentage may freeze at certain points. Be patient.
10. When the installer finishes, Windows 11 will start up and you will be launched into the First-Run Setup. Go to Part 3.

Part 5: First-Run Setup

1. On *Is this the right country or region?*, select **Canada** and click **Yes.**
2. On *Is this the right keyboard layout or input method?*, stick with the default and click **Yes**.
3. On *Want to add a secondary keyboard layout?*, click **Skip**.

> **Note:** If it has an Internet connection, Windows will now check for

> available updates from the Internet. If it finds any, it will install them automatically.
>
> If it doesn't have an Internet connection, this step will be skipped.

This process may take some time. Please be patient. Your VM may restart on its own.

Part 6: Account Creation

Now that language/keyboard and installer updates have been applied, it's time to create your account.

> **Note:** Steps 1-2 may not be necessary. If you're asked for a name, start with Step 3.

1. On *Let's set things up for work or school*, select **Sign-in options**.
2. On this next screen, click on **Domain join instead**.
3. On *Who's going to use this device?*, enter your **Seneca username**, (*Not* your full name), then click **Next**.
4. On *Create a super memorable password*, enter the same password you've used for your other VMs and click **Next**.
5. Confirm it on the next screen and continue.
6. On *Now add security questions*, fill out three security questions, clicking **Next** after each.
7. On *Let Microsoft and apps use your location*, select **No**, then click **Accept**.
8. On *Find my device*, select **No**, then click **Accept**.
9. On *Send diagnostic data to Microsoft*, scroll down to select **Required only**, then click **Accept**.
10. On *Improve inking & typing*, select **No**, then click **Accept**.
11. On *Get tailored experiences with diagnostic data*, select **No**, then click

Accept.

> **Note:** If it has a valid Internet connection, Windows will now check for *more* available updates. As before, if it finds any, it will install them automatically.
>
> If not, it will simply continue.

This process may take some time. Please be patient. Your VM may restart on its own.

Once complete, you will be presented with a login screen. Move to the next part to continue.

Investigation 4: Post-Installation Tasks *(client1)*

In this investigation, we'll log in for the first time and run through several post-installation tasks both necessary and for user comfort.

Part 1: First Login

1. Enter your password to login. First-login may take a few minutes as your profile is set up.

Part 2: Network Configuration

1. Click on the *Start* button and search for **Network Connections**. Open it when found.
2. Find the only Ethernet adapter (it may have different names).
3. Right-click it → Properties and do the following:

i. Internet Protocol Version 6 (TCP/IPv6): **Unchecked**
ii. Internet Protocol Version 4 (TCP/IPv4): Select and click **Properties**
    a. IPv4 address: **10.0.`UID`.11**
    b. Subnet mask: **255.255.255.0**
    c. Default gateway: 10.0.`UID`.1
    d. Preferred DNS server: 10.0.`UID`.1
    e. Alternate DNS server: 8.8.8.8
    f. Leave all other fields blank and click OK.
4. Open *Microsoft Edge* and nagivate to **eff.org**. If the page loads, you're done!

> **Check it out:** You are now using RRAS+NAT on your Windows Server to make this Internet connection happen.
>
> In *srv1*, go back to the **Routing and Remote Access** application. Inside, go to *SRV1 > IPv4 > NAT*. The **External Network** entry now has non-zero numbers under the 'packets translated' columns. This is your routing and NAT from *client1* at work! Refresh the page to see the count go up.

Part 2: Setting the Time Zone

1. Login again.
2. Find the time on the bottom right of the screen (in the VM, not your host machine!)
3. Right-click on the time and select **Adjust date and time**.
4. Check the displayed time and time zone.
5. The time should match current time, and the time zone should say "*(UTC-5:00) Eastern Time (US & Canada)*".
6. If the time zone is wrong, change it to the value above.
7. Confirm your time zone and time matches local time.

Part 3: Setting Internal Computer Name

When we created our VM, we gave it the name *client1-SenecaUsername*. This only applies to how VMware Workstation sees the VM, not to how the internal Windows OS sees itself. We need to change that to match.

1. In the *Settings* window you still have open (or reopen it from the Search bar), look to the left-hand menu bar and select **System**.
2. The very first thing you see at the top is the current computer name. This is what we're going to change.
3. Click on the **Rename** text link.
4. In the *Name your device* field, enter your VM's name: **client1-SenecaUsername** (replacing *SenecaUsername* with your actual username)
5. Click **Next**.
6. You will now be asked if you'd like to restart. Click **Restart now**.
7. After restarting and logging back in, go into *Settings* > *System* and confirm your computer name is now **client1-SenecaUsername**.

Part 4: Windows Updates

A critical part of a security-conscious mindset is running regular updates. **This is NOT something you do only once at the start of installation.** You should be running these regularly to keep up to date with security fixes and zero-day exploits.

1. If you're already in the *Settings* application, look through the left menubar for **Windows Update** and click it.
2. In the *Windows Update* main screen, scroll down to **Advanced Options** and click it.

3. The very first option is *Receive updates to other Microsoft products*. Toggle this from **Off** to **On**.
4. At the top of the screen, where it says *Windows Update > Advanced Options*, click **Windows Update** to go back to the previous screen.
5. You will likely already see updates ready. Click on **Download & install all**.
6. As you might expect, this can take a while. Timing will depend on your Internet connection, how fast your computer is, how fast your SSD is, and how many updates there are. Please be patient. Your computer may restart.
7. Once updates have begun, take a break while it does its thing. Grab a drink, make a sandwich, text a friend.
8. After updates are complete, go back into *Windows Update* and click **Check for updates** again. There may be (and often times are) more.
9. If there are more updates, complete Steps 5-8 again until there are no more updates available.
10. In *Windows Update*, scroll back down to **Advanced options** again and click it.
11. Inside *Windows Update > Advanced options* scroll down to **Optional updates** and click it.
12. Select all available updates that appear (you may have to expand some lists).
13. Click **Download & install**.

Investigation 5: Installing Windows Client 2 with Hyper-V *(client2)*

In this investigation, you'll create your second Hyper-V based virtual machine. This will be another Windows 11 client.

To conserve resources and speed up installation, it's helpful to shutdown *client1* while doing this.

Part 1: Creating the Hyper-V Virtual Machine

Create a second Hyper-V virtual machine with the following settings:

- Hypervisor: **Hyper-V**
- Name: **client2-`SenecaUsername`**
- RAM: **4 GB**
- CPU: **2 processors**
- Storage: **64 GB**
- NIC: **1** (default)
- Security: **Enable Trusted Platform Module**
- ISO: **Windows 11 Education**

Part 2: Installing Windows 11 (*client2*)

Set this up exactly as you did with *client1*, with **two important changes**:

1. Computer Name: **client2-`SenecaUsername`**
2. IP address: **10.0.`UID`.12**

Part 3: Post-Installation Tasks (*client2*)

Don't forget to run your **Post-Installation Tasks**! These are the same as for *client1*

Once *client2* is installed and has a working Internet connection, you're done!

Lab 2 Sign-Off

It’s essential to complete Lab 2 correctly, as the nested virtualization setup will be the core environment for all advanced labs. Everything you do from this point (DHCP, DNS, security, and domain controller work) will depend on this structure being solid and consistent.

When you finish Lab 2, ask your instructor for a sign-off. Your instructor will check your configuration, verify networking, and confirm all VMs are working as required.

Sign-Off Checklist

1. Hyper-V role is installed and running on srv1.
2. HQ Network (External Virtual Switch) exists and is bound to the correct NIC.
3. RRAS (Routing and Remote Access) is installed and NAT is configured for the two networks:
    i. External Network: **Internet access (DHCP-assigned)**
    ii. vEthernet (HQ Network): **10.0.`UID`.1/24**
4. client1 and client2 are both running inside Hyper-V, with the following:
    i. Static IPs set: **10.0.UID.11** and **10.0.UID.12**, respectively.
    ii. Default gateway set to **10.0.UID.1**
    iii. Both can access the internet (test by browsing to eff.org).
    iv. Both have correct computer names set.
    v. Both have time zone set to EST.
    vi. Both are fully updated via Windows Update.
5. Graceful shutdown: You can demonstrate safe start, shutdown, and reset procedures for Hyper-V VMs.
6. All relevant steps, commands, and decisions are recorded in your Lab Logbook.

Lab 3 - Security and Remote Connectivity

Lab Preparation

Purpose / Objectives of Lab 3

In this lab, you will conduct several Windows system administration tasks to secure your servers against would-be attackers and gain preliminary experience with the command line interface.

If you encounter technical issues, please contact your professor via e-mail or in your section's Microsoft Teams group.

Minimum Requirements

Before beginning, you must have:

1. Successfully completed Lab 2.
2. Attended the Week 3 lecture
3. Read through the Week 3 slides, and have them handy as a reference for concepts.
4. Your external SSD (or personal computer) with your VMs from Labs 1 and 2.
5. Your VM login credentials.
6. Optional, but recommended: Caffeine delivery system.

Key Concepts

Security: From the Beginning

In the not-too-distant past, companies would focus on getting their product and systems working and relegating security as their last step, often as an afterthought. When security is only considered at the end of a project, it's very difficult to remember all the ways in which your product interacts and things can get missed.

This created several high-profile breaches in the 90s and early 2000s, and our approach to security had to be reconsidered.

As a result, we now consider security **from the beginning**. As you create applications, add users to databases, create links between services, you *must* keep security in mind at every step of development. Securing as you go is the best method, but even something as simple as simply documenting unsecured parts of your code as you go can be enough (assuming you go back and fix them!)

Generally, we apply the concept of Principle of Least Privilege to security. Essentially, this boils down to locking everything down as much as possible and only allowing what and who you need through. Open access makes you a target. You'll be applying this principle to the firewall later in this lab.

We also take a look at defaults. Most systems and software come with pre-configured defaults to make out-of-the-box setup easy. This can take the form of a default username and password, default ports, etc. In a well secured system, these are often changed to avoid hack attempts. If you know the default, there's a high chance that hackers know it as well. You'll be changing some defaults in this lab.

This is not an exhaustive list of applied security, but it does give us a bit of working knowledge. You'll need it for this lab as well as in our later work.

Firewalls

In short, **a firewall is a utility that sits on your computer between your network connection and the rest of your system.**

Any application, service, or other data that is sent or received by your computer goes through your firewall first. The dominant network protocol is TCP/IP, which means we're dealing with *packets*.

A firewall looks at these packets.

To be clear, the firewall doesn't look *inside* packets, but just at the outside data like IP address and/or port destination, etc. The actual transmitted data is still secure and unread.

Generally with firewalls, we apply the *Principle of Least Privilege* by dropping all new connections by default, and allowing a few exceptions. This is known as **whitelisting**.

Editing Text Files

As you will sometimes be working in the Windows PowerShell command line environment, it is useful to learn a least one common method of editing text files.

Although programmers and developers usually use graphical IDE's to code and compile programs (Visual Studio, Sublime, Eclipse, etc), they can create source code using a text editor and compile their code directly on the server to generate executable programs (without having to transfer them for compilation or execution).

Developers very often use a text editor to modify configuration files. In this course, you will become familiar with the process of installing, configuring, and running network services. Text editors are an important tool to help this setup, but are also used to "tweak" or make periodic changes in service configurations.

The most readily-available command line text editor built into Windows is **Notepad**.

However, Notepad is not available in Server Core. To edit a text file in that environment, we have three main options:

1. Use PowerShell's object-oriented programming to send an edit directly into a text file. This is cumbersome and is not interactive (you don't see the text file on screen), but it is the only built-in option.
2. Transferring the file to a different computer that does have a text editor (like your Windows 11 client), modifying the file there, and transferring it back to your Server Core machine.
3. Using **Visual Studio Code** to connect remotely the environment. This is by far the coolest and most convenient option.

We'll be doing all three in this lab to show you how, but going forward, VS Code will be our go-to for interacting with Server Core in most instances. (You will be tested on all three options, so don't skip them!)

Investigation 1: Windows Defender (Firewall)

In this investigation, we're going to take a look at the Windows Defender firewall to see how firewall rules can be applied to secure our servers and let the few things we want to allow through.

It should be noted that the Windows Defender firewall *should not be your only*

defense. Production environments will often have managed networks that restrict access on a larger scale, some of which you will get into with your networking courses.

These work together, though we will only be focusing (mostly) on the Windows firewall in this course.

Part 1: Setting Up *srv2*'s NIC2 - Internal Network

In this part, we'll rename the second NIC and then give it a 10.x.x.x address so we can use it to communicate with our other servers and clients.

1. Login to *srv2*.
2. In the `sfconfig` application, select Option 8 (Network Settings).
3. You will have two network adapters. We're going to change their names for easier identification.
4. Find the adapter that has the external network IP address. It's usually the first one in the list. If you're not sure, ask.
5. Select that entry's number from the first column to go into it's options.
6. In *Network Adapter Settings*, select Option 4 (Rename network adapter).
7. Type the following and hit Enter: `External Network`
8. Repeat steps 3-7 for the second network adapter, and call it: `Internal Network`
9. Go back to the main `sfconfig` screen.
10. Select Option 15 to exit to the command line.

We're now going to apply network settings to our Internal Network adapter using PowerShell.

11. First, confirm the names of your adapters with the following command:

```
Get-NetAdapter
```

12. Now, assuming they look correct, run the following:

```
New-NetIPAddress -InterfaceAlias "Internal Network" -IPAddress
10.0.UID.2 -PrefixLength 24
```

13. Double-check your work by running:

```
Get-NetIPAddress -InterfaceAlias "Internal Network"
```

If it has the proper 10.x.x.x IP address, well done! Move on to **Part 2**.

If the network information is wrong, you can remove it and try again by running:

```
Remove-NetIPAddress -InterfaceAlias "Internal Network"
-AddressFamily IPv4
```

> Tip: To return to `sfconfig`, either run that command or type `exit`.

Part 2: Windows Server GUI (srv1) - Testing the IIS Role

On this server, we will take a look at a role that was installed in our last lab as part of RRAS, **IIS (a web server)**. This will be used only for testing connectivity between your other VMs and working with the firewalls.

This role is already running after Lab 2 and doesn't need any configuration. We'll be using it later to test network connections and firewall rules.

Let's test it locally (from within the same machine). We'll do so by pointing a

web browser at ourselves.

1. Inside *srv1*, open Firefox.
2. Navigate to: `http://127.0.0.1`

If you see the *Internet Information Services* splash page, then this role is working. If you don't, ask your professor for help.

> **ℹ A note about servers, clients, Server Roles, and IIS:**
> The IIS Server Role installs a **web server** inside of *srv1*. A web server is one that serves many clients (web browsers). This one-to-many concept is known as the client-server model in IT spaces. Other VMs and computers can also access this test web page (though it is blocked by default, see the Investigations below).

Part 3: Testing VM Network Connectivity

As part of your Lab 1 environment setup, you tested your connection to the Internet from each of your 3 virtual machines.

It's now time to test if we can use each VM to connect to *each other*.

1. On your Windows Server GUI (srv1) VM, open Command Prompt.
2. Grab this VM's **Internal Network** IP address with the following command and write it down: `ipconfig`

   > Remember, your *Internal Network* is the non-Internet network you created with the 1**0.0.**`UID`**.1** address. We're running ipconfig to confirm it's still there.

3. On your **Windows Client (client 1) VM**, open Command Prompt.
4. Enter the following command to test our ability to talk to *srv1*: `ping`

`"srv1-ipaddress"` where *srv1-ipaddress* is the IP address from Step 2.

> Example: `ping 10.0.40.1`

5. It doesn't work, does it? That's normal at this stage and we'll fix it below. For now, we'll try connecting to our web server on *srv1*. That should show us the two VMs can talk to each other.

6. Open *Firefox* on your **Windows 11 Client (client1)** and use the IP address from Step 2 (your *srv1* IP address) as the URL.

> Example: `http://10.0.40.1`

7. Can you see the IIS splash page that you saw in *Investigation 1, Part 1, Step 2*? If so, you have connectivity!

8. Continue to **Part 4**.

Part 4: Windows Server GUI (srv1) - Applying Firewall Rules

We will now apply our security-conscious policy by configuring the firewall on this server.

At the moment, the server's firewall is configured using defaults. As mentioned above, **defaults are a security risk** as they are known to everyone and can be used against you. If an attacker *doesn't* know your configuration, it's harder for them to know what's open and what's not and how to attack.

As you saw from **Part 2**, ping between *client1* and *srv1* didn't work.

By default, the ability to ping a server is turned off. A ping (a type of ICMP packet) is typically used to see if you can get a response from a server. Having a server respond let's an attacker know there's a machine there that they can

then try to break into.

> **Imagine a burglar knocks on a random brick wall (sends a ping).** If you (the server) knock back (send a ping reply), the burglar now knows there's a person there who probably has some nice stuff! Don't knock back, and the burglar has no idea what's on the other side of that wall and will move on.

We want to turn on ping so we can test connections between our machines, but we have to be careful. Turning that on through the firewall too broadly opens us up to that vulnerability.

We are going to turn it on *only* for our local network. Our VMs will be allowed to ping each other, but anything outside of our subnet (10.0.`UID`.0/24) can't. Best of both worlds.

To do this, we're going to work with the **Windows Defender Firewall** on srv1.

1. In the *Server Manager* application, go to *Local Server*.
2. In the *Properties* section of this page, look for the **Microsoft Defender Firewall** line item.
3. Next to the line, it should say **Public: On**. Click on this.
4. The *Windows Security > Firewall & Network protection* application opens.
5. On this screen, you will see three networks: *Domain network*, *Private network*, and *Public network*.
6. We'll spend more time with these in later weeks, but for now, all three should say: **Firewall is on**.
7. Below this, click on the link that says: **Advanced settings**
8. This opens the *Windows Defender Firewall with Advanced Security* application.
9. On the first page, you'll notice the same three profiles: *Domain Profile*, *Private Profile*, and *Public Profile*.

10. All three have the same overall rules:
11. **Windows Defender Firewall is on**: This just confirms the firewall is active for this network profile.
12. **Inbound connections that do not match a rule are blocked**: This means that all incoming connections and requests (like trying to ping this machine) are blocked *by default*. If you want to allow a certain type of connection or service into your server, you have to make a specific rule for it. This is whitelisting and our *Principle of Least Privilege* in action.
13. **Outbound connections that do not match a rule are allowed**: This means all network data leaving the server is automatically allowed. The logic here is that if the server is the one deciding the send out information, it's likely fine. (Note: The only time we ever whitelist outbound connections is for specialized security settings like government compliance.)
14. At the moment, we're dealing with the *Public Profile* context. Let's allow ICMP ping!
15. On the left-hand menu bar, click **Inbound Rules**.
16. This loads a ton of already-defined rules. Thankfully, the one we need has already been defined. We just need to turn it on.
17. At the top of this area, click **Name** to order the list by name (this is not the default).
18. Now, scroll down until you can find the following and double-click it: **Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)**, **Private, Public**.
19. **Note:** There are two of these rules! Look for the one that has **Private, Public** under the Profile header. The wrong one says Domain.
20. This opens this rule's configuration window, starting on the *General* tab.
21. In the *General* tab, look for the following and check the box next to it: **Enabled**
22. Click **Apply**, then **OK**.
23. Back in the main *Inbound Rules* window, you should see that same rule line

now says **Yes** under the *Enabled* header.

24. You've enabled ICMP ping! Let's go test it.
25. Switch back to your client1 machine, and run the same ping you ran earlier pointing to srv1. (Refer to *Part 2, Step 4*.)
26. Does it work?
27. If it does, congratulations! You've just enabled ping for connectivity checking to *srv1* and gone through your first foray into the Windows Firewall.

> **ℹ A note for later labs:** By default, this rule is set to only allow incoming pings (ICMP requests) from computers on your **VM network**—that is, other virtual machines on the same VMware NAT or host-only network as your server—not from the wider Internet or any physical computers in the classroom.
>
> You can see this by checking the **Scope** tab in the rule's properties, where "Remote IP address" is set to "Local subnet."
>
> We'll spend more time on how **Scope** and **Private/Public profiles** affect your firewall rules in our *Secondary Network* assignment.

> 📝 **Lab Question:** Why did we *not* have to do this for our IIS web server setup?
>
> In the **Inbound Rules** list, scroll through to see if you can find the rule that's allowing web server pages to be requested from *srv1*.
>
> Write down the name of the rule in your Lab Logbook when you find it (it's not called IIS) and explain why you think you didn't have to enable this rule yourself. Think back to when you installed the IIS Server Role.

Part 5: Windows Server Core (srv2) - Applying Firewall Rules

Let's apply the same incoming ping firewall rule to our Server Core machine so we can check it's network connectivity as well.

1. Login to your Server Core *(srv2)* machine.
2. The *sfconfig* text-based application automatically launches.
3. Select option 8 to find this machine's **Internal Network** IP address. Write it down.
4. Back in your Windows 11 Client (*client1*), try to ping this address. Does it work?
5. Just as in *srv1*, it doesn't.
6. Go back to *srv2*.
7. If you're still in the *Network settings* page, leave the field blank and hit **Enter** to go back to the main screen.
8. Select option 15 to exit to PowerShell.
9. As there's no GUI, we need to use PowerShell for firewall management.
10. Let's take a look at the existing rules, just like in Part 2. Run the following PowerShell command:

```
Get-NetFirewallRule | Where-Object DisplayName -Like '*ICMPv4-In*'
```

11. Several results appear in the search. Look for the one with the name: **Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)**
12. This firewall rule object, starting from *Name* all the way down to *PackageFamilyName* lists all the configured properties for this rule.
13. Read through these properties. Recognize any from our GUI version?
14. This rule matches both our incoming ping requests and keeps to *Private,*

Public profiles. As with our GUI version, the scope is defaulted to local subnet only.

15. Let's turn on this incoming firewall rule by running the following command:

```
Enable-NetFirewallRule -Name CoreNet-Diag-ICMP4-EchoRequest-In
```

16. This selects the right rule and enables it.
17. One of the things you **must** get into the habit of doing with CLI commands is ***double-checking your work***.
18. Let's do that now by asking the system if it was actually enabled:

```
Get-NetFirewallRule -Name CoreNet-Diag-ICMP4-EchoRequest-In
```

19. Look for the *Enabled:* field. See how it's changed to **True**? It worked!
20. Optional: We can even check the scope for local subnet only as we did in the GUI version if we want with the following command:

```
Get-NetFirewallRule -Name CoreNet-Diag-ICMP4-EchoRequest-In | Get-
NetFirewallAddressFilter
```

Output:

```
LocalAddress  : Any
RemoteAddress : LocalSubnet4
```

21. Last, because there are two incoming ICMP rules (*Domain* profile and *Private, Public* profile), let's check that only the *Private, Public* rule is enabled:

Command:

```
Get-NetFirewallRule -DisplayName "Core Networking Diagnostics -
ICMP Echo Request (ICMPv4-In)" | Select-Object DisplayName,
Profile, Enabled
```

22. This shows a brief status of both rules. The *Domain* version should show **False** under the *Enabled* header, while the *Private, Public* version should show **True**.

Output:

```
DisplayName
Profile Enabled
-----------
------- -------
Core Networking Diagnostics - ICMP Echo Request
(ICMPv4-In)          Domain   False
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)
Private, Public    True
```

23. Now, let's test our ping. Switch over to your Windows 11 Client (client1).
24. Open a Command Prompt window, and run the following command: `ping srv2-ipaddress` (Refer to *Part 3, Step 3*).
25. Does it work?
26. **If it does, congratulations!** You've just enabled ping for connectivity checking to *srv2* and gone through your first foray into the PowerShell!

Part 6: Windows Client (client1) - Applying Firewall Rules

Finally, let's enable ping on our Windows Client machine.

1. Login to *client1*.

2. Click the **Start** button and type the following search: **firewall**
3. Of the options that appear, select: **Windows Defender Firewall with Advanced Security**
4. Just as in *Part 2* with *srv1*, navigate to **Inbound Rules**.
5. Click the *Name* header to sort by name.
6. Find the following rule:
7. Name: **Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)**
8. Profile: **Private, Public**
9. Double-click it to open the rule's configuration settings.
10. In the *General* tab, find and check the box next to **Enabled**.
11. Click **Apply**, then **OK**.
12. Open a *Command Prompt* window and run the following to get your client's IP address: `ipconfig`
13. Switch to your *Server Core (srv2)* machine.
14. In PowerShell, run the following command: `ping client1-ipaddress` (Where client1-ipaddress is the address from Step 10.)
15. Example: `ping 10.0.40.11`
16. Does it work?
17. **It if does, congratulations!** You've just enabled ping for connectivity checking to *client1* and have full connectivity checking for your entire environment! This will become ***very*** handy in Labs 3-4.

Investigation 2: Remote Management - Windows Server GUI (srv1)

While you have direct access to all three VMs from VMware, these days most

machines are remote. This means you typically do not have direct, physical access to the servers.

Even if you do, having remote access to allow you to manage your servers from the comfort of your office (or home!) instead of walking to each physical machine is far better.

In this investigation, we'll set up remote access to our Windows Server GUI (srv1) so we can connect to it using your Windows 11 Client VM.

Part 1: Enabling Remote Desktop Connections

In this part, we'll turn on Remote Desktop (RDP) on the server. This will allow you to remotely connect to *srv1* from your Windows 11 Client.

1. In the *Server Manager* application, navigate to *Local Server*.
2. In the main *Properties* window, find the line entry for: **Remote Desktop**
3. Click the link next to it: **Disabled**
4. In the new *System Properties* window, you should automatically be on the *Remote* tab.
5. Look down to the section on **Remote Desktop**.
6. Toggle the option for: **Allow remote connections to this computer**
7. Ensure the checkbox next to this is on: **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**
8. Click **Apply**, then **OK**.

Part 2: Adding your RDP Firewall Rules

In this part, we'll add a firewall rule to allow the connection over the local network.

1. On *srv1*, open **Windows Defender Firewall with Advanced Security**.
2. In the *Inbound Rules* section, look for the following rules:
    i. **Remote Desktop - Shadow (TCP-In)**
    ii. **Remote Desktop - User Mode (TCP-In)**
    iii. **Remote Desktop - User Mode (UDP-In)**
3. If they're all enabled (they should be), you're good to go!
4. Why check? Always check your firewall rules when enabling a new service, even if it *usually* enables the associated firewall rule automatically. **Never assume!**
5. If these rules are **not** enabled, enable them now.

Part 3: Connecting to Windows Server (srv1) from Windows 11

In this part, we'll verify our work by connecting to the server using our Windows 11 client VM.

1. Make sure you've got your *srv1* IP address from earlier. (You wrote it down, *right*?)
2. On *client1*, click the **Start** menu.
3. Search for and open: **Remote Desktop Connection**
4. In the newly opened application, in the *Computer* field, enter the IP address for *srv1*.
5. Click **Connect**.
6. Enter your *srv1* username and password, then click **OK**.
7. A security dialogue box pops up. **Check the box next to "*Don't ask me again for connections to this computer*" before the next step.**
8. Click **Yes**.
9. If you can see your *srv1* desktop, congratulations! You now have remote access.

10. To quit the remote session, find the floating HUD at the top of the screen with the IP address and click on the **X** icon.
11. Note: **This will not shutdown your *srv1* VM. It only ends your remote session.**
12. Note 2: A remote session will automatically lock your VM's direct session. You will need to unlock it again when you go back to it through VMware Workstation directly.

Investigation 3: Remote Management – Windows Server Core (srv2) with Remote Desktop

In this investigation, we'll set up remote access to our Windows Server Core (srv2) so we can connect to it using your Windows 11 Client VM.

Part 1: Enabling Remote Desktop Connections

In this part, we'll turn on Remote Desktop (RDP) on the Core server (*srv2*).

1. Login to *srv2*.
2. If you're at the PowerShell command prompt, run the following command to get back into the text-based *Server Manager* application: `sconfig`
3. Select option 7.
4. In the *Remote desktop* page, select option **E** to enable Remote Desktop.
5. It will ask you to select a security level. Select **Option 1**.
6. Press **Enter** to complete and go back to the main *Server Manager* page.
7. **Double-check your work.** Select option 7 again.
8. Is the *Remote desktop status* changed and correct?
9. If not, go through Steps 4-9 again.

10. If yes, press **Enter** without entering any options to go back to the main screen without making any changes.

Part 2: Adding a RDP Firewall Rules

In this part, we'll check that the RDP firewall rules have been enabled.

1. Select **Option 15** to exit to PowerShell.
2. Run the following PowerShell command to check the status of your RDP firewall rules:

Command:

```
Get-NetFirewallRule | Where-Object { $_.DisplayName -like '*Remote
Desktop*' -and $_.Direction -eq 'Inbound' } |
    Select-Object Name, DisplayName, Profile, Enabled
```

Output:

```
Name                          DisplayName
Profile Enabled
----                          -----------
------- -------
RemoteDesktop-In-TCP-WS       Remote Desktop - (TCP-WS-
In)            Any   False
RemoteDesktop-In-TCP-WSS      Remote Desktop - (TCP-WSS-
In)           Any   False
RemoteDesktop-Shadow-In-TCP   Remote Desktop - Shadow (TCP-
In)        Any    True
RemoteDesktop-UserMode-In-TCP Remote Desktop - User Mode (TCP-
In)     Any    True
RemoteDesktop-UserMode-In-UDP Remote Desktop - User Mode (UDP-
In)     Any    True
```

3. Check that your output matches the above. This is the same as on *srv1*, just at the command line. Notice which are enabled and which are not?
4. If you need to, grab the IP address for *srv2* here by running this command in PowerShell: `ipconfig`

Part 3: Connecting to Windows Server (srv2) from Windows 11 via RDP

In this part, we'll verify our work by connecting to *srv2* using our Windows 11 client VM. This is essentially the same as our instructions for *srv1*, but with a different IP address.

1. Make sure you've got your *srv2* IP address from earlier. (You wrote it down, *right*?)
2. On *client1*, click the **Start** menu.
3. Search for and open: **Remote Desktop Connection**
4. In the newly opened application, in the *Computer* field, enter the IP address for *srv2*.
5. Click **Connect**.
6. Enter your *srv2* username and password, then click **OK**.
7. A security dialogue box pops up. **Check the box next to "*Don't ask me again for connections to this computer*" before the next step.**
8. Click **Yes**.
9. If you can see your *srv2* Command Prompt window, congratulations! You now have remote access.
10. To quit the remote session, find the floating HUD at the top of the screen with the IP address and click on the **X** icon.
11. Note: **This will not shutdown your *srv2* VM. It only ends your remote session.**
12. Note 2: A remote session will automatically lock your VM's direct session.

You will need to unlock it again when you go back to it through VMware Workstation directly.

Investigation 4: Remote Management - Windows Server Core (srv2) with SSH

Part 1: Enabling SSH Connections

In this part, we'll turn on incoming SSH connections so we can connect to our server using Visual Studio Code from the Windows 11 client.

1. Login to your Server Core *(srv2)*.
2. Exit the *Server Manager* program by selecting **Option 15**.
3. In PowerShell, run the following command to install the OpenSSH Server

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

4. After it installs, we have to start the SSH service. Run the following:

```
Start-Service sshd
```

5. We now have to set the SSH service to start automatically every time the system boots. Run the following:

```
Set-Service -Name sshd -StartupType 'Automatic'
```

6. As with our other work, let's confirm the SSH service is running:

```
Get-Service sshd
```

7. You should have a response that looks like this:

```
Status   Name               DisplayName
------   ----               -----------
Running  sshd               OpenSSH SSH Server
```

Part 2: Adding an SSH Firewall Rule

1. We'll now add an SSH rule. One already exists, but it's only attached to the *Private* profile and would not work for us.
2. Instead, we'll create a custom rule. Run the following command:

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)'
-Enabled True -Direction Inbound -Protocol TCP -Action Allow
-LocalPort 22 -Profile Private,Public
```

3. This rule sets the following:
    i. Name: sshd
    ii. Display Name: OpenSSH Server (sshd)
    iii. Enabled: True
    iv. Profile: Private, Public
    v. Direction: Inbound
    vi. Action: Allow
    vii. Protocol: TCP
    viii. Port: 22
4. Verify your work! First, let's look at the firewall object by running the following command:

5. Now, let's verify the protocol and port with the following command:

Command:

```
Get-NetFirewallRule -Name 'sshd'
```

Output:

```
Name                          : sshd
DisplayName                   : OpenSSH Server (sshd)
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Private, Public
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully
from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

Command:

```
Get-NetFirewallRule -Name 'sshd' | Get-NetFirewallPortFilter |
Select-Object Name, Protocol, LocalPort
```

Output:

```
Name Protocol LocalPort
---- -------- ---------
     TCP      22
```

6. If your own output looks like the above, congratulations! If not, try your configuration commands again or ask for help.

Part 3: Connecting to Windows Server Core (srv 2) from Windows 11 via SSH

1. On your Windows 11 Client (*client1*), open Command Prompt.
2. Enter the following command: `ssh Administrator@srv2ipaddress` (Where *srv2ipaddress* is your actual *srv2* IP address.)

   > Example: `ssh Administrator@10.0.40.2`

3. The first time you connect, a prompt will ask you if you are sure. Type **yes** and hit **Enter**.
4. Type your password when asked and hit **Enter**.

   > **i Note:** By default, You will *not* see asterisks or other characters as you type. **This is normal.** It is taking your keyboard input. It may take you a few tries to get used to it.

5. Once logged in, you are now on *srv2*'s Command Prompt environment.
6. To get back into PowerShell (which you should), run: `powershell`

7. It is **not** recommended to run the *sconfig* program over an SSH connection. If you need to use the *sconfig / Server Manager* text-based program, connect through your RDP connection in Part 1.

> **ℹ A note about SSH and *Server Manager*:**
> Your SSH connection will allow you to run the *sconfig* Server Manager program and load it. However, many of it's functions fail over an SSH connection because it relies on background interactive processes that can't run on an SSH session. They must be run from the RDP connection, despite it *looking* the same.
>
> For an example of this, run `sconfig` from your SSH session and try to run Windows Updates. If it finds any and you try to install them, it will fail. This is an SSH+sconfig problem; run the same thing through RDP and it will work fine.

Lab 3 Sign-Off

It’s essential to complete Lab 3 correctly, as the networking setup will be required for all advanced labs.

When you finish Lab 3, ask your instructor for a sign-off.

Sign-Off Checklist

On *client1*:

1. Ping *srv1*
2. Ping *srv2*
3. SSH into *srv2*
4. RDP into *srv2*
5. In Firefox, load the IIS test page at: **10.0.`UID`.1**
6. In Firefox, test your Internet connection by loading: **eff.org**

Lab 4 - Implementing DNS

Lab Preparation

Purpose / Objectives of Lab 4

In this lab, you will deploy and validate a local DNS service on your Windows Server GUI VM (srv1), then configure all machines in your lab environment to use it. By the end, you will be able to:

1. Install the **DNS Server** role on *srv1*.
2. Create a **Forward Lookup Zone** for *yourSenecaUsername.com*.
3. Add *A records* for *srv1, srv2, client1* and *client2*.
4. Configure forwarders so *srv1* can resolve Internet names.
5. Point *srv1* to itself via loopback (127.0.0.1) for DNS.
6. Reconfigure *srv2*, *client1*, and *client2* to use *srv1* as their DNS.
7. Create a **Reverse Lookup Zone** and **PTR records**. Verify forward and reverse resolution with `nslookup`, `ping`, and browser tests.

If you encounter technical issues, please contact your professor via e-mail or in your section's Microsoft Teams group.

Minimum Requirements

Before beginning, you must have:

1. Successfully completed Lab 3.

2. Attended the Week 5 lecture
3. Read through the Week 5 slides and have them handy as a reference for concepts.
4. Your external SSD (or approved personal computer) with your VMs from Labs 1-3.
5. Your VM login credentials.
6. Optional, but recommended: Caffeine delivery system.

Key Concepts

What DNS Does - Domain Name System

DNS maps names to IP addresses. Humans remember reddit.com. The Internet only understands how to route to 151.101.193.140. It’s hierarchical and distributed, so no single server knows everything. **Authoritative servers** answer for their zones and resolvers figure the rest out.

Forward vs. Reverse Lookups

1. **Forward:** URL to IP (e.g., srv1.yourSenecaUsername.com converts to 10.0.UID.1) using A/AAAA records.
2. **Reverse:** IP to URL (e.g., 10.0.UID.1 to srv1.yourSenecaUsername.com) using PTR records in a Reverse Lookup Zone.

Reverse lookup is gold for troubleshooting and clean logs.

Zones and Authority

A zone is the authoritative dataset for a chunk of namespace. In this lab you create:

1. **Forward zone:** yourSenecaUsername.com
2. **Reverse zone:** 10.0.UID.0/24 (IPv4 reverse)

Each zone has an SOA (start of authority) and NS records defining who's in charge. We keep dynamic updates disabled here for control and repeatability.

Authoritative vs. Recursive (srv1 does both)

1. **Authoritative:** Answers with authority for names inside its zones.
2. **Recursive:** Chases down answers it doesn't know yet.

In our setup, *srv1* is **authoritative for your lab domain** and recursive for everything else (via forwarders).

Forwarders vs. Root Hints (and Conditional Forwarders)

1. **Forwarders:** send unknown queries to specific upstream resolvers (what we configure for the classroom).
2. **Root hints:** the built-in map to the DNS root—slower to "warm up."
3. **Conditional forwarders:** send only certain domains to specific DNS servers (handy in enterprises; not needed here).

We will only be using forwarders in this lab for ease of set up.

Records You'll Actually Touch

1. A: Hostname to IPv4.
2. PTR: IPv4 address to hostname (reverse).
3. CNAME (alias): points a name to another name.
4. Rule of thumb: a CNAME can't live alongside other records at the same name (no A+MX+CNAME pileups).

FQDNs and the DNS Suffix

1. Fully-Qualified Domain Name (FQDN): Full path (e.g., srv1.yourname.com.).
2. **Short names** (e.g., ping srv1) rely on a DNS suffix search list. To keep tests deterministic, we use FQDNs in this lab.

Caching and TTL

DNS answers are cached to reduce load. The TTL controls how long.

Tips:

1. After changing records, clear caches where relevant:
2. **Client:** `ipconfig /flushdns`
3. **Server:** DNS Manager > right-click server > Clear Cache

Ports and Firewall

DNS uses **UDP/53** for most queries, **TCP/53** for large responses and zone transfers. With the DNS Server Role installed, inbound DNS rules should be enabled (Private/Public).

Verify. Never assume.

Loopback and Why We Use It on *srv1*

The loopback interface (127.0.0.1) sends traffic to the local host. It is immune to network interface card (NIC) misconfigurations. Pointing *srv1* at **127.0.0.1** ensures it always asks itself first, which simplifies troubleshooting.

> Loop: srv1 > 127.0.0.1 > srv1

Split-Horizon (a.k.a. Split-Brain) DNS (just awareness)

Enterprises often serve different answers internally VS externally for the same name. In this lab your domain is internal-only. Don’t register it publicly.

Troubleshooting Toolkit

1. **nslookup** (classic): Quick forward/reverse tests.

2. **Resolve-DnsName** (PowerShell): Richer diagnostics (optional).
3. **Get-DnsClientServerAddress**: Confirm which DNS your client is using.
4. If names resolve but pings fail, think firewall (Lab 3), not DNS.

Investigation 1: Configuring DNS on Windows Server (*srv1*)

Part 1: Confirm a Static IP Address on *srv1*

As *srv1* will be our primary network services provider, we have to give it a **static IP address**. This is so it doesn't periodically change. If it did change, any other machines relying on this one would suddenly be unable to connect and lose access to all services provided, including the very DNS we're about to set up!

We already did this during *Lab 2, Investigation 1, Part 3*. Doing so is called **manual static network configuration**.

Let's confirm our work:

1. Open **Command Prompt**.
2. Run the following command: `ipconfig`
3. Confirm the *Internal Network* adapter uses: **10.0.`UID`.1**
4. Find the *External Network* adapter's current DNS address. **Write this down**. You will need it later in this lab.

Static IP addressing is always required for a computer or device providing network services. Remember that.

If the proper static IP is confirmed, move on to *Part 2*.

Part 2: Installing the DNS Server Role on *srv1*

Let's install the DNS Server Role.

1. **Login to srv1** with your Administrator account.
2. Open the **Server Manager** application (icon is on the taskbar or Start menu).
3. In the left menu, click on **Local Server** if you're not already there.
4. At the top right, click **Manage > Add Roles and Features**.
5. In the **Add Roles and Features Wizard** window:
    i. On *Installation Type*, select **Role-based or feature-based installation**, then **Next**.
    ii. On *Server Selection*, confirm **Select a server from the server pool** and choose **srv1**, then **Next**.
    iii. On *Server Roles*, scroll down and check the box for **DNS Server**.
    iv. A pop-up will ask to add required features, click **Add Features**.
    v. Back on the *Server Roles* page, click **Next**.
    vi. On the *Features* page, leave defaults, click **Next**.
    vii. On the *DNS Server* page, read and click **Next**.
    viii. On the *Confirmation* page, click **Install**.
    ix. Wait for installation to finish (may take a few minutes).
    x. When you see *Installation succeeded on srv1*, click **Close**.

Part 3: Configuring a New DNS Zone

We are now going to create a new DNS foward lookup zone. This is what allows us to put all of our machines under a single **domain name**. Just like *reddit.com* and *eff.org*, you will create your own domain name using *yourSenecaUsername.com*.

1. Back in **Server Manager**, in the top right, click **Tools > DNS** to open the DNS Manager.
2. In the left pane, expand **srv1** and then **Forward Lookup Zones**.
3. Right-click on **Forward Lookup Zones** and select **New Zone…**
4. In the **New Zone Wizard**:
    i. On *Zone Type*, select **Primary zone**, click **Next**.
    ii. On *Zone Name*, enter ***yourSenecaUsername*.com**, replacing *yourSenecaUsername* with your actual username.
    iii. For example, mine might be: **cjohnson30.com**
    iv. Click **Next**.
    v. On *Zone File*, keep **Create a new file** selected, click **Next**.
    vi. On *Dynamic Update*, keep **Do not allow dynamic updates** (default), then click **Next**.
    vii. Click **Finish** to create the zone.

Part 4: Adding Host (A) Records

A records (also known as host records) are the entries that allow us to say what name goes to what IP address. So, we can link the IP address *10.0.`UID`.1* with *srv1*, for example.

> **Note:** An A record adds to your domain name. If you make an A record called *srv1*, then the full path is *srv1.yourSenecaUsername.com*.
>
> The formula is always: *A_recordname+domainname*

1. In **DNS Manager**, expand your new **yourSenecaUsername.com** zone.
2. Right-click in the right pane and select **New Host (A or AAAA)…**
3. For each of your lab VMs, create a record:
    i. **srv1**
        - Name: `srv1`

        - IP address: `(Use the IPv4 address of srv1)`
        - Click **Add Host**
    ii. **srv2**
        - Name: `srv2`
        - IP address: `(Use the IPv4 address of srv2)`
        - Click **Add Host**
    iii. **client1**
        - Name: `client1`
        - IP address: `(Use the IPv4 address of client1)`
        - Click **Add Host**
    iv. **client2**
        - Name: `client2`
        - IP address: `(Use the IPv4 address of client2)`
        - Click **Add Host**
4. When finished, you should see all four names listed in the zone.

Part 5: Configure DNS Forwarders on *srv1*

We want *srv1* to answer local names (your zone which contains srv1, srv2, etc.) and resolve Internet names. If *srv1* isn’t authoritative for a name (i.e. doesn't have a definition for it), it *should* forward the query upstream.

At the moment, it's only set up to give the IP addresses of our VMs, not the Internet.

To fix this, we have to tell *this* server where to look if it doesn't have the answer locally. If it can't answer locally, it will forward the request to an Internet-based DNS server.

This is called a *Forwarder*. Let's set it up:

1. In **DNS Manager** on srv1, right-click on your server’s name in the left pane.
2. Select **Properties**.
3. Go to the **Forwarders** tab.
4. Click **Edit…** Investigation 1, Part 1, Step 4.
5. In the *IP address* field, enter the IP address from *Investigation 1, Part 1, Step 4*, then hit **Enter** for it to be verified. If it can reach it, you should see a domain name populate next to the IP address.
6. Add a second DNS for fallback, using CIRA's DNS:
    - **149.112.121.20**
7. Make sure CIRA's DNS is the **second** entry in the list.
8. Click **OK** to add.
9. Click **OK** again to close Properties.

> ℹ **Note:** In managed networks you might use *Root Hints* instead. We’re using Forwarders for predictable performance in a classroom environment.

Part 6: Configuring *srv1* To Use DNS From *srv1*

Now that we've set up our DNS server locally on *srv1*, we have to tell *srv1* to use itself for DNS resolution instead of what Seneca (or your ISP) provides.

We're going to do this by using the *Loopback Interface*. This is a special network interface on all modern operating systems that, when network traffic (like DNS!) is sent to it, will loop it back to itself. Hence, the name.

The *Loopback* interface's address is always **127.0.0.1** on all systems. (You may sometimes see **localhost** used for this. That's the URL version of the exact same network interface.)

This special interface is great for a number of reasons, but most importantly:

It's completely separate from our other networks and so isn't affected by network configuration mistakes. When you use loopback, you know you're getting the most direct link. Helpful in troubleshooting!

> **Network Flow with Loopback:** Send Traffic from *srv1* > *srv1* Loopback > Receive Traffic from *srv1*

1. To do this, open up the Network Properties for **External Network** and change its TCP/IPv4 settings to the following:
    - Preferred DNS server: **127.0.0.1**
    - Alternate DNS server: `<blank>`
2. Click OK on each open dialog box until you're back at *Network Connections*.
3. Repeat Steps 1-2 for **vEthernet (HQ Network)**.
4. Verify your work by opening **Command Prompt** and running: `ipconfig /all`
5. You should see both interfaces and their DNS settings set to 127.0.0.1.

If you do, move on to the next part!

Part 7: Test *srv1* DNS Resolution

Our first task is to confirm this works locally by telling the server to talk to itself first for DNS resolution. This lets us test our DNS service and records while removing the network and firewall pieces. (See the explanation above in Part 6.)

1. Open **Command Prompt**.
2. To test DNS resolution functionality on your local network, run the following

commands one at a time:

```
nslookup srv1.cjohnson30.com
nslookup srv2.cjohnson30.com
nslookup client1.cjohnson30.com
nslookup client2.cjohnson30.com
```

3. Now, let's run a lookup for an address on the greater Internet:

```
nslookup eff.org
nslookup reddit.com
```

4. If each returns the proper IP address value, you're done! If not, revisit your earlier configuration steps and check to see what might be missing.
5. Don't be afraid to ask for help!
6. **If *any* of your lookups above failed, ask for help! Do not move onto the next Investigation if failed.**

Investigation 2: Configuring Other Machines For DNS Use

In this investigation, we will configure our other VMs to use *srv1* as the DNS server for all DNS resolution.

> **ℹ A note about the *loopback* address from Investigation 1**
> The *loopback address* we used on *srv1* only works locally. You cannot use this address outside of *srv1*. You must use its **Internal Network** address.

Part 1: Windows Server Core (srv2)

1. Turn on the following VMs:
    - srv2
    - client1
    - client2
2. On *srv2*, log in as Administrator.
3. At the prompt, run:

```
Get-NetIPAddress
```

3. Look for the section that contains *srv2*'s normal **Internal Network** IP address. Make a note of the **InterfaceIndex** number just below it. (For example, 4. Yours may differ.)
4. Set the DNS server to srv1’s IP (replace X.X.X.X with srv1’s actual address, and 4 with your NIC’s ifIndex):

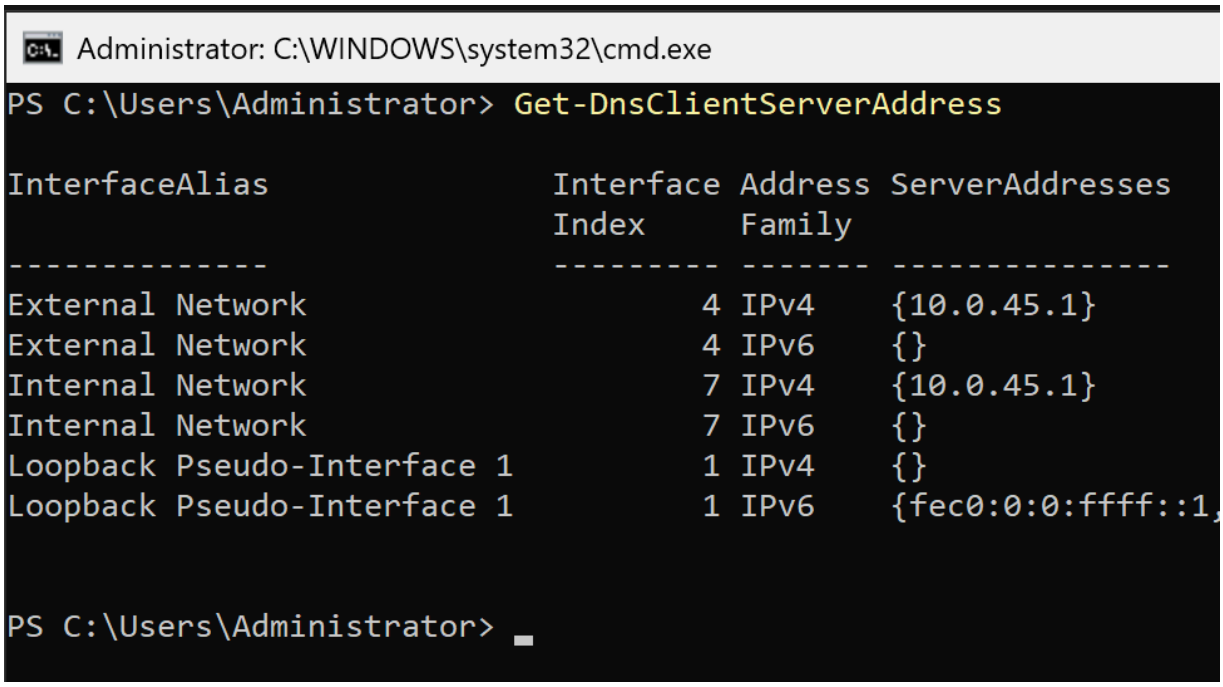
```
Set-DnsClientServerAddress -InterfaceIndex 4 -ServerAddresses
`10.0.UID.1`
```

5. Confirm the change:

```
Get-DnsClientServerAddress
```

6. Repeat Steps 2-5 for the **External Network** address/network interface.

7. When done, the command on Step 5 should provide a similar output to this:



8. To test DNS resolution functionality, run the following commands one at a time:

```
nslookup srv1.cjohnson30.com
nslookup srv2.cjohnson30.com
nslookup client1.cjohnson30.com
nslookup client2.cjohnson30.com
nslookup eff.org
```

7. If each returns the proper IP address value, you're done! If not, revisit your earlier configuration steps and check to see what might be missing.
8. Don't be afraid to ask for help!
9. Last, ping each other machine to prove you no longer need to remember IP addresses:

```
ping srv1.cjohnson30.com
```

13. Cool, right?

Part 2: Windows 11 Client (client1)

1. Login as Administrator.
2. Right-click the **Network** icon in the system tray, click **Network and Internet settings**.
3. Click **Ethernet**.
4. Scroll down to *DNS server assignment* and click the **Edit** button next to it.
5. In the *Edit DNS settings* pop-up window, click the drop-down menu to change it from *Automatic (DHCP)* to **Manual**.
6. Find the new *IPv4* option and toggle it **On**.
7. In the *Preferred DNS* field, enter the *srv1* IP address.
8. Leave all others on their defaults and click **Save**.
9. Remove saved DNS cache. Open **Command Prompt** and type:

```
ipconfig /flushdns
```

9. To test DNS resolution functionality, run the following commands one at a time:

```
nslookup srv1.cjohnson30.com
nslookup srv2.cjohnson30.com
nslookup client1.cjohnson30.com
nslookup client2.cjohnson30.com
nslookup eff.org
nslookup reddit.com
```

10. If each returns the proper IP address value, you're done! If not, revisit your earlier configuration steps and check to see what might be missing.

11. Don't be afraid to ask for help!
12. Last, ping each server to prove you no longer need to remember IP addresses:

```
ping srv1.cjohnson30.com
ping srv2.cjohnson30.com
ping client2.cjohnson30.com
```

13. In Firefox, browse to your *srv1* IIS splash page by name:

```
http://srv1.cjohnson30.com
```

14. Also cool, right?

Investigation 3: Configuring Reverse Lookup (PTR) Records

In this investigation, we will set up Reverse Lookup (PTR) records so we can look up a server by its IP address and get a FQDN address back. Very helpful in troubleshooting and a best practice.

You'll also see how it helps for self-identification a little later.

Part 1: Create a Reverse Lookup Zone

1. In **DNS Manager** on *srv1*, right-click **Reverse Lookup Zones** in the left pane.
2. Click **New Zone…**
3. In the **New Zone Wizard**:

i. On *Zone Type*, select **Primary zone**. Click **Next**.
ii. On *Reverse Lookup Zone Name*, choose **IPv4 Reverse Lookup Zone**. Click **Next**.
iii. On *Network ID*, enter the first three octets of your VMs' subnet (for example, if your VMs' IPs are 10.0.45.x, enter 10.0.45). Click **Next**.
iv. On *Zone File*, keep defaults. Click **Next**.
v. On *Dynamic Update*, keep defaults (Do not allow dynamic updates). Click **Next**.
vi. Click **Finish** to create the zone.

Part 2: Add PTR Records for Each VM

1. We're going to automatically add PTR records using our existing A records for ease of use.
2. Inside the *Forward Lookup Zones*, in the **cjohnson30.com** zone, right-click each A record you created (srv1, srv2, client1, client2) and select **Properties**.
3. Check the box next to **"Update associated pointer (PTR) record"** and click **OK**.
4. If the box was already checked, uncheck it, click **Apply**, check it again, then click **Apply** again. This forces the PTR generation.
5. This should automatically create PTR records in your new reverse zone.
6. Double-check your work. Click on the folder inside *Reverse Lookup Zone* to see its contents. If empty, right-click on the folder and click *Refresh*.
7. They should now appear. If they do not, retrace your steps or ask for help.

Part 3: Test Reverse DNS Resolution

1. On *srv2*, open PowerShell.
2. Run **nslookup** on each VM's IP address:

```
nslookup 10.0.UID.1
nslookup 10.0.UID.2
nslookup 10.0.UID.11
nslookup 10.0.UID.12
```

3. You should see the PTR record and corresponding hostname for each IP address.

Example Output:

```
Server:  srv1.cjohnson30.com
Address:  10.0.45.1

Server:  srv2.cjohnson30.com
Address:  10.0.45.2

Name:    client1.cjohnson30.com
Address:  10.0.45.11

Name:    client2.cjohnson30.com
Address:  10.0.45.12
```

4. Notice that the server entry no longer says "UnKnown" as it did before. Now it can identify itself!

Congratulations, you've now set up basic DNS services from *srv1* to each VM in your environment and allowed for local resolution to your other VMs by name!

Troubleshooting and Common Pitfalls

1. **Forwarders not working:** Verify upstream DNS IPs are reachable from

srv1 and listed in the Forwarders tab (not just in adapter DNS settings).

2. **Wrong adapter DNS:** On srv1, both adapters should use 127.0.0.1. On other machines, adapters should use 10.0.UID.1.
3. **Names resolve, but pings fail:** That's likely firewall (Lab 3). The important bit for this lab is that nslookup returns correct answers.
4. **PTRs missing:** Re-toggle "Update associated PTR" on each A record, Apply, then Refresh the reverse zone.
5. **Typo domain:** Be consistent (e.g., cjohnson30.com everywhere).
6. **UID mismatch:** Ensure all A/PTR records and tests use your UID subnet (10.0.UID.x).

Lab 4 Sign-Off

It's essential to complete Lab 4 correctly. All later labs assume working forward and reverse name resolution.

When you finish Lab 4, ask your instructor for a sign-off.

Sign-Off Checklist

Please have the following on screen and ready to show.

On srv1:

1. `nslookup srv1.yourdomain`: Returns 10.0.`UID`.1
2. `nslookup eff.org`: Returns a public IP (forwarder working)
3. Both adapters show 127.0.0.1 as DNS in `ipconfig /all`
4. Your **Forward Lookup Zone** page open for review.
5. Your **PTR Records** page open for review.

On srv2:

1. `Get-DnsClientServerAddress`: Shows 10.0.`UID`.1 for Internal and External network adapters.
2. `nslookup client1.yourdomain` and `nslookup client2.yourdomain`: Correct IPs
3. `nslookup 10.0.UID.1`, `nslookup 10.0.UID.11` and `nslookup 10.0.UID.12`: Correct PTR to FQDN.

On client1:

1. DNS set to 10.0.`UID`.1 (Manual/IPv4)
2. `nslookup srv1.yourSenecaUsername.com`: Resolves to 10.0.`UID`.1
3. In Firefox: `http://srv1.yourSenecaUsername.com` loads the IIS splash page.
4. `nslookup reddit.com`: Resolves a public IP (forwarder working)
5. In Firefox: `http://www.reddit.com` loads the Reddit main page.

Lab 5 - Implementing DHCP

Lab Preparation

Purpose / Objectives of Lab 5

In this lab, you will deploy **DHCP** on *srv1* to automatically provide IP configuration for your internal lab network.

By the end, you will:

1. Install the **DHCP Server** role on *srv1*.
2. Create an IPv4 **scope** for your internal subnet **10.0.`UID`.0/24** with proper **options** (Router, DNS servers, DNS Suffix).
3. Create **reservations** so *srv2*, *client1*, and *client2* receive predictable addresses that match prior labs.
4. Flip *srv2*, *client1*, and *client2* from **static** addressing to **DHCP**, then verify leases.
5. Validate **DHCP + DNS** end-to-end with `ipconfig`, `nslookup`, and `ping`.

Minimum Requirements

Before beginning, you must have:

- Successfully completed **Lab 4 – Implementing DNS**, with *srv1* resolving internal names and using loopback for local DNS testing.
- Your **UID** value handy.

- All four VMs present from earlier labs: *srv1* (GUI), *srv2* (Core), *client1*, *client2*.

Key Concepts

- **DHCP** automatically assigns IP addressing (IPv4 address, subnet mask), **Default Gateway (Option 003)**, **DNS servers (Option 006)**, and **DNS Suffix (Option 015)** to clients on a subnet.
- **Scope** defines the usable address pool on a network. **Reservations** ensure specific MAC addresses always receive the same IP.
- In this course, your internal network remains **10.0.`UID`.0/24**; *srv1* is the router at **10.0.`UID`.1**.

> **Design Note:** We will keep client addresses consistent with Labs 2–4 using **reservations** so your existing DNS host records remain correct.

Investigation 1: Install the DHCP Server Role on *srv1*

Part 1: Add the DHCP Server Role

In this investigation, we'll install the DHCP role on our server so other machines on our network can get their IP address and network configuration from *srv1*.

1. **Login to srv1** with your Administrator account.
2. Open **Server Manager → Manage > Add Roles and Features**.
3. **Installation Type**: *Role-based or feature-based installation* → **Next**.
4. **Server Selection**: choose **srv1** → **Next**.

5. **Server Roles**: check **DHCP Server** → **Add Features** if prompted → **Next** through *Features* and *DHCP Server* pages.
6. **Confirmation**: **Install** and wait for completion.

Part 2: Post-Install Configuration

1. In **Server Manager**, click the yellow **!** → **Complete DHCP configuration**.
2. In the wizard, click **Commit** → **Close**.

Once fully complete, move on to the next investigation.

Investigation 2: Create Scope and Options (10.0.`UID`.0/24)

In this investigation, we'll configure the **scope**.

A DHCP scope is , basically, what slice of the network are we going to use and define. (Example are 10.0.45.0/24, 192.168.1.0/24, 172.16.0.0/16, etc.)

Here, we're going to tell DHCP we want to manage the **10.0.`UID`.0/24** network. Any machine that connects to our *Internal Network* will get its IP address, subnet mask, default gateway, and DNS using what we set up below.

In short: *srv1* will give other machines their IP addresses automatically, along with other network configuration.

Part 1: Create a New IPv4 Scope

1. **Tools > DHCP**.

2. Expand your server (srv1) → **IPv4** → **Right-click > New Scope…**

3. **Scope Name**: `OSM620 HQ`
4. **IP Address Range**:
    - **Start**: `10.0.UID.1`
    - **End**: `10.0.UID.254`
    - **Subnet mask**: `255.255.255.0`
5. **Add Exclusions and Delay**: Add the following:
    - `10.0.UID.1`
    - `10.0.UID.200` to `10.0.UID.254`
    - Leave the delay blank.
6. **Lease Duration**: default (8 days) → **Next**.
7. **Router (Default Gateway) – Option 003**: `10.0.UID.1` → **Add** → **Next**.
8. **Domain Name and DNS Servers – Option 006/015**:
    - **Parent domain** (Option 015): `yourSenecaUsername.com` *(replace with your lab domain from Lab 4)*
    - **DNS Servers** (Option 006):
        - `10.0.UID.1` *(srv1)*
        - **149.112.121.20** *(CIRA)*
9. **WINS Servers**: leave blank → **Next**.
10. **Activate Scope**: select **Yes, I want to activate this scope now** → **Finish**.

> **Why start at `.2`?** `.1` is the gateway on *srv1*. We want to make sure our DHCP server can't give out the IP address that *srv1* already uses!

Investigation 3: Reservations for Predictable Addresses

By default, a DHCP server will assign IP addresses to other machines randomly from the range you defined earlier. (10.0.`UID`.2 - 10.0.`UID`.254)

Every time one of your other machines connect, it could get *any* IP address inside that range. It will always start with 10.0.`UID`., but that last number (octet) could be anything between 2-254. It can and will change from day to day.

In this investigation, we're going to use **Reservations** to let us decide, from *srv1*, what IP addresses each of our machines should *always* have. After we're done, when srv2 gets an IP address, it won't be random. It will be what we decide.

We'll bind specific IPs to each machine's **MAC address** so they keep the same addresses used in Labs 2–4.

Part 1: Collect Physical Addresses From Each NIC

To set this up, we need to grab the physical address (otherwise known as MAC address) of each network card on each computer. This is how *srv1* will known which machine is which when it needs to give out IP addresses.

Write down the physical address for each:

1. On **srv2** (Core): `ipconfig /all` → record the **Physical Address** for the **Internal Network** adapter.

2. On **client1**: `ipconfig /all` → record Physical Address.
3. On **client2**: `ipconfig /all` → record Physical Address.

Part 2: Create Reservations on *srv1*

In this part, we'll know create a DHCP reservation for each computer. This is how we make sure they get the specific IP address we want them to have, instead of a random one.

Each computer will have its own reservation. This is like a record.

In **DHCP Manager → IPv4 > OSM620 HQ > Reservations → Right-click > New Reservation…**

Create the following (replace `UID` and MACs):

- **srv2**
  - **IP address**: `10.0.UID.2`
  - **MAC**: `<srv2 MAC>`
  - **Description**: `Windows Server 2025 Datacenter Core`
  - **Supported types**: **Both → Add**
- **client1**
  - **IP address**: `10.0.UID.11`
  - **MAC**: `<client1 MAC>`
  - **Description**: `Windows 11 Education`
  - **Supported types**: **Both → Add**
- **client2**

- **IP address**: `10.0.UID.12`
- **MAC**: `<client2 MAC>`
- **Description**: `Windows 11 Education`
- **Supported types**: **Both → Add**

Verify all three appear under **Reservations**.

Investigation 4: Switch from Static to DHCP

Right now, you're other computers are using **manual static network configuration**. You set up their IP addresses manually.

In this investigation, we'll switch our other machines back to using DHCP so they can get their network information, including IP address, from *srv1*.

Part 1: Swtiching *srv2* (Server Core)

1. Login as **Administrator**.
2. In PowerShell, identify the interface index of your network adapter (look for **IfIndex**):

   ```
   Get-NetIPInterface
   ```

3. Enable DHCP for IPv4 (replace `4` with your **IfIndex** on the Internal Network adapter):

   ```
   Set-NetIPInterface -InterfaceIndex 4 -Dhcp Enabled
   ```

4. Run `ipconfig /all` to confirm the following: **IPv4 Address = 10.0.UID.2**, **Default Gateway = 10.0.UID.1**, **DNS = 10.0.UID.1**.

Part 2: *client1* (Windows 11)

1. **Settings > Network & Internet > Ethernet > Edit** next to **IP assignment → Automatic (DHCP) → Save**.
2. **Edit** next to **DNS server assignment → Automatic (DHCP) → Save**.
3. Command Prompt:

```
ipconfig /release
ipconfig /renew
ipconfig /all
```

4. Confirm **IPv4 = 10.0.UID.11**, **Gateway 10.0.UID.1**, **DNS 10.0.UID.1**.

Part 3: *client2* (Windows 11)

Repeat the exact steps as client1. Confirm **IPv4 = 10.0.UID.12**.

> If a machine doesn’t pick up the reserved address, re-check the MAC you entered in the reservation and ensure the NIC you changed to DHCP is the **Internal** (HQ) adapter.

Investigation 5: Verify Leases and Name Resolution

In this investigation, we'll run checks to confirm that our machines are:

- Using DHCP
- Have an IP address
- Can connect to other machines
- Can connect to the Internet

Part 1: Check Leases in DHCP Manager

1. On *srv1*: **DHCP Manager → IPv4 > OSM620 HQ > Address Leases**.
2. Confirm entries for **srv2**, **client1**, **client2** with correct **Reservation** type and IPs.

Part 2: Test DHCP + DNS

From **client1** (or **client2**):

```
ipconfig /all
nslookup srv1.yourSenecaUsername.com
nslookup client2.yourSenecaUsername.com
nslookup eff.org
ping srv1.yourSenecaUsername.com
```

- All should resolve and ping (ICMP allowed per Lab 3). If `nslookup` for Internet names fails, revisit **DNS Forwarders** on *srv1*.

Troubleshooting

- **Client keeps old static IP**: ensure **IP assignment = Automatic (DHCP)**; on Core, run `Set-NetIPInterface -Dhcp Enabled` then `ipconfig /release` + `/renew`.
- **Gets wrong pool address**: verify the **reservation MAC** matches the

Internal adapter; remove/re-add reservation if needed.

- **No default gateway**: re-check **Option 003** in scope options.
- **DNS wrong**: verify **Option 006** points to `10.0.UID.1` and **Option 015** is your lab domain.
- **No Internet**: confirm *srv1* still NATs traffic between Internal and External (Lab 2 RRAS) and that **Forwarders** work (Lab 4).

Lab 5 Sign-Off

To complete Lab 5, show your instructor:

1. **Scope** `10.0.UID.2–199` active with Options **003**, **006**, **015** set.
2. **Reservations** for **srv2 (10.0.UID.2)**, **client1 (10.0.UID.11)**, **client2 (10.0.UID.12)**.
3. On each client, `ipconfig /all` showing **DHCP Enabled = Yes** and the correct leased address.
4. In Address Leases, entries for all three machines marked as **Reservation**.
5. `nslookup` for `srv1.yourSenecaUsername.com` **and** an Internet site returns addresses successfully.

> **You're done!** Your lab environment now uses **DHCP** correctly while keeping earlier labs' addressing and DNS intact.

Lab 6 – Active Directory

Lab Preparation

Purpose of Lab 6

In this lab, you'll redesign and configure your environment to a more realistic, low-footprint, on-premises design. You'll move core network services off **srv1** and into **Active Directory** by promoting **srv2** to **Domain Controller (DC1)** with integrated **DNS** and **DHCP**, manage everything remotely from **srv1** using **RSAT**, and prove end-to-end client functionality by joining **laptop1** to the domain.

You'll also prepare a clean clone (**srv3**) and promote it to **DC2** for redundancy.

The lightweight **router** VM you'll create replaces RRAS/NAT, mirroring how real sites use a dedicated edge device.

Objectives

By the end of this lab, you will be able to:

- Build a minimal **VyOS router** VM and configure LAN/WAN, default route, and NAT for Internet access.
- Configure a consistent **IP plan** (gateway 10.0.UID.254, statics for servers, DHCP range for clients).
- Promote **srv2** to **AD DS** as the first domain controller for **yourSenecaUsername.com** with integrated **DNS**.

- Configure **DNS forwarders** and create a **reverse lookup zone** with **Secure only** dynamic updates.
- Convert **srv1** into a **management server** (RSAT only) and manage **srv2** remotely via **Server Manager**.
- Join **srv1** and **laptop1** to the domain and verify **Kerberos + name resolution** end-to-end.
- Validate DNS registration: confirm **A** and **PTR** records for servers and client populate correctly.
- Use GUI tools (**DNS**, **DHCP**, **ADUC/AD DS**) to administer services from **srv1**.
- Clone **srv3**, join it to the domain, promote it to **DC2 (GC + DNS)**, and verify DNS replication.

Minimum Progression Requirements

Before beginning, you must have:

1. **Successfully graded *Labs 1-5* and *Assignment 1*.**
2. Attended the **Week 8 - Active Directory** lecture.
3. Your external SSD (or personal computer) with your VMs.
4. Your OSM620 Lab Logbook.
5. Optional, but recommended: Caffeine delivery system.

Before You Begin

Time to Backup! *You will be making major changes to all virtual machines.* This is a good time to backup these VMs so you can restore from them if

something catastrophic occurs.

With all VMs turned off, copy the entire `Virtual Machines` folder on your SSD to a separate location. This can be a backup directory on your SSD, or even a separate physical drive. Leave the copy be and use the original going forward. (If you need space, compress the backup folder.)

Do not continue until the copy has fully completed.

Investigation 1: Adding the *router* VM

In this investigation, we'll be adding a Linux-based router to our setup. This low-footprint virtual machine will take the place of the RRAS NAT work you did in previous labs. Most on-premises installations (offices, warehouses, schools) will have a physical router that does this instead of relying on Windows Server to do that work.

Setting this up is extremely easy and should only take a few minutes.

After you're done, you will need to have this VM powered on during all lab work. I'll remind you of this often.

VM Specifications

Setting	Value
VM Name	router
Role	Router / NAT (edge)

Setting	Value
OS / Image	VyOS (current stable ISO)
vCPU	1
RAM	512 MB
Disk	20 GB
NICs	2
NIC1	VMware NAT
NIC2	VMnet10
NIC2 IPv4	**10.0.`UID`.254/24** (static)

Instructions to set this up are provided below.

Part 1: Create *router* VM

Here we'll create the VM hardware and install the VyOS operating system. This is very quick process.

> **Reminder**: Remember to create a new *router* folder on your SSD for the VM files!

1. Download the VyOS ISO: https://community-downloads.vyos.dev/stream/1.5-stream-2025-Q2/vyos-1.5-stream-2025-Q2-generic-amd64.iso
2. Create a new VMware VM with the following:

    i. ISO: **VyOS ISO image**
    ii. Type: **Debian 12.x 64-bit**
    iii. Boot firmware: **UEFI**
    iv. Name: **router**
    v. CPU: **1 core**
    vi. RAM: **512 MB**
    vii. CPU > IOMMU: **Enable**
    viii. CPU > Enable hypervisor: **Disabled**
    ix. Storage: **20 GB**
    x. NIC1: **NAT**
    xi. NIC2: **VMnet10**
3. Power on VM.
4. In the boot menu, select the first option: **Live system (vyos)**
5. Login with these credentials:
    i. Username: **vyos**
    ii. Password: **vyos**
6. Install VyOS on the disk using this command: `install image`
    i. Would you like to continue?: **y**
    ii. What would you like to name this image?: **Just hit Enter to select the default**
    iii. Please enter a password for the "vyos" user: *yourNormalAdminPassword*
    iv. What console should be used as default?: **Hit Enter to select default**
    v. Which one should be used for installation?: **Enter to select default**
    vi. Installation will delete all data on the drive. Continue?: **y**
    vii. Would you like to use all the free space on this drive:? **y**
    viii. What would you like to use as boot config?: **Enter to select default**
7. The installation proceeds (it's very fast). When finished, reboot: `sudo`

`reboot`

8. Wait for the machine OS to boot up again.
9. Use the following credentials for your new VM:
    i. Username: ***vyos***
    ii. Password: ***yourNormalAdminPassword***

Part 2: Configuring Routing

Now that our new virtual machine is installed and running, we need to configure it to do our routing. This is a one-time process.

1. Power on router VM and login. (If you haven't already.)
2. Run the following commands ONE AT A TIME (**Replace UID!**):

```
configure
set interface ethernet eth0 address dhcp
set system name-server eth0
set interface ethernet eth1 address 10.0.UID.254/24
set nat source rule 20 outbound-interface name eth0
set nat source rule 20 source address 10.0.UID.0/24
set nat source rule 20 translation address 'masquerade'
set system ipv6 disable
commit
save
exit
```

> *Figure 1. Example of VyOS commands*

3. Check your router can access the Internet: `ping eff.org`

> *Figure 2. Proper ping completion*

4. If it receives proper ping, move on to the next step. If not, ask for help!

5. Log out: `exit`
6. Keep this VM up! Minimize and move on to the next Investigation.

Congratulations! You now have a NAT router VM that uses minimal resources.

> Note: After this lab, whenever you have other Windows VMs turned on, turn this one on first. (You don't need to log into it, just let it do its thing.)

Investigation 2: Create srv3 VM

In this investigation, we're going to clone *srv2*, reset it to defaults, then configure the clone with *srv3* information.

Do not create the VM below from scratch! This is just for quick reference.

Setting	Value
VM Name	srv3
Role	Windows Server Core #2
vCPU	2
RAM	4 GB
Disk	250 GB
NICs	1
NIC1	*Removed*

Setting	Value
NIC2	VMnet10
NIC2 IPv4	**10.0.`UID`.3** (static)

Part 1: Cloning in VMware

1. Shut down ALL VMs except the router.
2. Create a new folder inside Virtual Machines on your SSD and call it: *srv3-yourSenecaUsername*
3. In VMware Workstation, right-click on *srv2* and select: **Create Full Clone**
4. Rename when asked to: **srv3-yourSenecaUsername**
5. Save it inside: **Virtual Machines/srv3-yourSenecaUsername/**
6. This may take several minutes to complete.
7. Once complete, change the following hardware (do not power on):
    i. Remove NIC1 (External Network)
    ii. Confirm hardware:
        a. CPU: **2 cores**
        b. RAM: **4 GB**

Part 2: Cleaning the Clone (srv3)

1. Power on and login.
2. Exit to PowerShell.
3. Run the following command: `C:\Windows\System32\Sysprep\Sysprep.exe /oobe /generalize /shutdown`
4. This will take a *very* long time, around 10 minutes. When complete, the

computer will shut down.

5. Power on *srv3* again.
6. It will ask you to change the login password. Just use the same you've been using before. (Tab to go to the next field, then Enter to send both fields.)
7. When asked about diagnostics, select option 1 (Required only)
8. Your scrubbed *srv3* will now start up.

Part 3: Configuring srv3

1. Login to *srv3*.
2. Stay in *sconfig*.
3. Change the computer name to to *srv3*. (***not srv3-yourSenecaUsername!***)
4. The computer restarts.
5. After restart, log back in.
6. Change your network adapter settings to the following:
    i. Name: **Internal Network**
    ii. IP address: **10.0.`UID`.3**
    iii. Subnet: **255.255.255.0**
    iv. Gateway: **10.0.`UID`.254**
    v. DNS1: **10.0.`UID`.2**
    vi. DNS2: ***Blank***
    vii. DNS3: ***Blank***
7. Exit to PowerShell

8. Check Internet connection by running: `ping 173.239.79.200`

   > **Note:** DNS won't work yet, that's okay.

9. If Step 8 worked, go back to sconfig and shutdown the system.

10. Keep this VM powered off until told otherwise.

Investigation 3: Convert srv1 to a Management Server

In this investigation, we'll remove all our network services from Labs 1-5 and turn *srv1* into a **Management Server**. Essentially, a GUI that lets us control other servers remotely from the **Server Manager** application.

This is a very normal on-prem setup, and you'll see why later on in the lab. It makes everything far easier and it's more secure.

Part 1: Removing Old Roles

1. Turn off all VMs.
2. Power on *srv1* and login.
3. In *Server Manager > Remove Roles*:
   i. Roles > Select these roles (Remove features when asked):
      a. DHCP
      b. DNS
      c. Remote Access
      d. Hyper-V
      e. IIS
4. **Do NOT select restart this server.**

5. This may take a while!
6. When complete, shut down *srv1*.

Part 2: Hardware Changes for srv1

1. Go into srv1's hardware properties in VMware (do not power on!)
2. Remove NIC1 (External Network)
3. Reduce hardware:
    i. CPU: **4 cores**
    ii. RAM: **8 GB**

Part 3: Network Configuration (srv1)

1. Turn on *router* VM.
2. Power on *srv1* and login.
3. Set static network configuration for Internal Network NIC:
    i. IP address: **10.0.`UID`.1**
    ii. Subnet: **255.255.255.0**
    iii. Gateway: **10.0.`UID`.254**
    iv. DNS: **149.112.121.20**
4. Confirm Internet connection.
    i. In Command Prompt, run: `ping eff.org`
    ii. Confirm it works. If not, ask for help!
5. Shut down *srv1*.

Investigation 4: Promote srv2 to AD DC1

In this investigation, we're going to promote *srv2* to an **Active Directory Domain Controller**. As the first Core machine, we have to do this purely from the command line with PowerShell.

Part 1: Network Reconfiguration (srv2)

Let's configure the server to get it ready for Active Directory.

1. Remove NIC1 (External Network)
2. Confirm hardware:
    i. CPU: **2 cores**
    ii. RAM: **4 GB**
3. Power on.
4. Change computer name from *srv2-yourSenecaUsername* to *srv2*. **Restart**.
5. Log back in.
6. Set static network configuration for Internal Network NIC:
    i. IP address: **10.0.`UID`.2**
    ii. Subnet: **255.255.255.0**
    iii. Gateway: **10.0.`UID`.254**
    iv. DNS: **10.0.`UID`.2**
        a. Note: If DHCP won't be removed, go to PowerShell and run: `Set-NetIPInterface -InterfaceAlias "Internal Network" -Dhcp disabled`
        b. Go back to *sconfig* and rerun Step 6.
7. Exit to PowerShell.

8. Check Internet connection by running: `ping 173.239.79.200`
9. If ping is successful, move on to the next Investigation. If not, ask for help!

Part 2: Installing AD and DC Promotion

Here, we install the Active Directory server role and then promote *srv2* to be an AD Domain Controller.

1. Install the Active Directory role:

```
Install-WindowsFeature AD-Domain-Services
```

2. **This can take a while!** Be patient.
3. Promote srv2 to a domain controller:

```
Install-ADDSForest -DomainName 'yourSenecaUsername.com'
-DomainNetbiosName 'YOURSENECAUSERNAME' -InstallDNS -Force
```

4. When asked for a password, use the same one you've used for your Administrator accounts.
5. **This will take several minutes!** Your VM will restart and take a few more minutes. Be patient.
6. Once you can, login with: `YOURSENECAUSERNAME\Administrator`
7. In sconfig, confirm you can see:
    i. Computer name: **srv2**
    ii. Domain: **yourSenecaUsername.com**
8. Minimize srv2 VM but keep it on!

Investigation 5: Manage srv2 from

srv1 GUI

Let's use *srv1*'s **Server Manager** to manage and configure *srv2*!

Part 1: Join srv1 to the new domain

We now have an Active Directory domain, but we need to join *srv1* to it.

1. Double-check the following VMs are already powered on:
    i. router
    ii. srv2
2. Power on *srv1* and login.
3. Change "Internal Network" NIC DNS to: `10.0.`UID`.2`
4. In *Computer Properties*, change the computer name from *srv1-yourSenecaUsername* to *srv1*.
5. Restart and log back in.
6. Open *Computer Properties* again, and click on **Workgroup**.
7. Select *Domain* and enter: *yourSenecaUsername.com*
8. When asked for credentials, use your Administrator username and password.
9. When it adds properly, you'll get a welcome message.
10. The computer will now restart.
11. When the computer is up again, login using: **Other > YOURSENECAUSERNAME\Administrator**

Part 2: Setup srv1 as a GUI Management Server for srv2

This is where we add *srv2* to *Server Manager* for remote control. We also install a few features that help with that remote control.

1. In *Server Manager*, go to **All Servers**.
2. Go to *Manage > Add Servers*
3. Click on **Find Now**.
4. Select *srv2*.
5. Click **OK**.
6. It may take a few moments to appear properly. **Ensure it says "Online - Performance counters not started."**
7. Go to *Manage > Add Roles and Features*
8. Select **srv1** from the list.
9. Skip *Roles*, and select the following *Features*:
10. *Remote Server Administration Tools > Role Administration Tools:*
    i. **AD DS and AD LDS Tools**
    ii. **DHCP Server Tools**
    iii. **DNS Server Tools**
11. Click **Next** through the rest of the wizard and then **Install**.
12. Any other message, ask for help!

Part 3: Configure DNS on srv2 with srv1

We're now going to set up Active Directory DNS on *srv2*. This is much more advanced than the previous standalone DNS service we installed in a previous lab, and you'll see that shortly.

1. Go to *Server Manager > Tools > DNS*
2. When asked to connect to a DNS server, select "The following computer" and enter: `srv2`
3. You will now be connected to the DNS server on *srv2* remotely, using the GUI on *srv1*.
4. Find *srv2* in the list, right-click, and select **Properties**.
5. Add forwarders: **149.112.121.20**
6. Right-click on **Reverse Lookup** and select **New Zone**.
7. Stick with the wizard defaults until *Network ID*.
8. Enter Network ID: `10.0.`UID``
9. Click **Next** and then **Finish** through the rest of the wizard.
10. Go to *Reverse Lookup Zones > `UID`.0.10.in-addr.arpa*
11. Notice the list is currently empty.
12. Run `ipconfig /registerdns` on both *srv1* and *srv2*.
13. Refresh the view in reverse lookup and confirm the two server entries.
14. Check the *Forward Lookup Zone > yourSenecaUsername.com*. Your two servers are already there!
15. On *srv1*, open **Command Prompt** and run:

```
ipconfig /flushdns
nslookup srv2
nslookup srv1
nslookup eff.org
ping srv2
ping eff.org
```

16. Open Firefox and go to: **reddit.com**
17. If those two steps worked, you now have full Internet using the DNS service on *srv2*!

Notice how you didn't have to create any A or PTR records! The servers self-registered. *How cool is that?*

Part 4: Configure DHCP on *srv2* with *srv1*

We're now going to set up Active Directory DHCP on *srv2*. As with DNS, this is much more advanced than the standalone we did earlier.

Unlike DNS, which was installed along with the AD Domain Controller, the DHCP role isn't currently on *srv2*. We have to install it and then configure.

1. Go to *Server Manager > Manage > Add Roles and Features*
2. Select **srv2** from the list.

> **WARNING:** Make sure you select *srv2*! Not *srv1*!

3. Select the DHCP role.
4. Go through the DHCP wizard and finish.
5. When installation is complete, click on **Complete DHCP configuration**.
6. Click **Next** and then **Commit**.
7. Close the window.
8. Go to *Server Manager > Tools > DHCP*
9. Right-click the DHCP entry in the left and select **Manage authorized servers...**
10. Select *srv2*, then click **OK**.
11. In the new *srv2* entry, create a new scope.
12. Configure it with the following:
    i. Name: **OSM620 Fall 2025 - AD DHCP**
    ii. Range: **10.0.`UID`.1 - 10.0.`UID`.254**
    iii. Exclude:
        a. **10.0.`UID`.1-10.0.`UID`.9**

        b. **10.0.`UID`.254**
    iv. Router: **10.0.`UID`.254**
    v. DNS:
        a. DNS1: **10.0.`UID`.2**
        b. DNS2: **10.0.`UID`.3**
    vi. WINS: **Leave defaults**
    vii. Select **Activate now**.
13. Back in the main DHCP window, go to the *IPv4* folder, right-click, and select **Properties**.
14. Click the DNS tab.
15. Select **Always dynamically update DNS records**
16. Click **OK**
17. That's it, you're done!

Investigation 6: Add laptop1 to Domain

Now that we've set up our AD Domain Controller on *srv2* and remote control on *srv1*, it's time to add a normal client machine to our Active Directory domain. We'll use *laptop1* for this.

The initial "join to AD" is typically done by an administrator such as yourself. After the laptop is part of the AD domain, you would then give it to the employee.

Part 1: Setting Proper Network Configuration

1. Have the following VMs powered on:
    i. router

    ii. srv2
    iii. srv1 (if you have the hardware resources)
2. Before powering on *laptop1*, check NIC1 in VMware. Make sure it's set to **VMnet10**.
3. Power on *laptop1* and login.
4. If you named this machine *laptop1-yourSenecaUsername*, change it to *laptop1* and restart.
5. Check Windows NIC1 network settings. They should be set to **DHCP**.
    i. If it was static until now, open **Command Prompt** and run to check it has an Internet connection:
        a. `ipconfig /release`
        b. `ipconfig /renew`
6. In Command Prompt, run: `ipconfig /all`
7. Check the information. You should have a 10.0.`UID`.x address, DNS as *srv2*, and gateway as 10.0.`UID`.254.
8. In Command Prompt, run:

```
ipconfig /flushdns
nslookup srv1
nslookup srv2
nslookup eff.org
ping srv1
ping srv2
ping eff.org
```

9. Back on *srv1*, go to *Server Manager > Tools > DHCP*
10. In the DHCP window, go to: *srv2 > IPv4 > Scope > Leases*
11. You should see your *laptop1* in the leases section.
12. If all this works, continue to the next section!

Laptop1 now has a stable Internet connection using DHCP and DNS from *srv2*, and is routing to the Internet through the *router* VM.

Part 2: Domain Join for laptop1

Now, it's time to join *laptop1* to our AD domain.

1. Open *Settings* > *System* > *About* (at the very bottom)
2. Click on the **Domain or workgroup** link.
3. In the new *System Properties* > *Computer Name* tab, click on **Change**.
4. Change from workgroup to domain: **yourSenecaUsername.com**
5. Authenticate the same as you did with *srv1*.
6. After the congratulations message, allow the machine to restart.
7. Do not log in with your normal account.
8. Click on Other, and use: **YOURSENECAUSERNAME\Administrator**
9. Your profile may take a minute to setup. That's normal.
10. Once you see the desktop, minimize this VM.

Part 3: Confirm laptop1 is in DNS

Let's check that *laptop1* auto-registered to DNS after the AD join.

1. On *srv1*, open the DNS tool.
2. Go to *srv2* > *Forward Lookup Zones* > *yourSenecaUsername.com*
3. Do you see laptop1? If yes, congrats! It auto-registered, just as we wanted.
4. If not, ask for help. Do not continue.

Investigation 7: Promote *srv3* to AD DC2

In this investigation, we'll create a second AD Domain Controller by using *srv3*. This is a much simpler process than *srv2*, as we can use *srv1* for part of it.

Part 1: Domain Join for *srv3*

Time to add *srv3* to our new AD domain.

1. Power on *srv2* and *router* (if not already on). Leave all other VMs off.
2. Power on *srv3* and login.
3. Change workgroup to domain: **yourSenecaUsername.com**
4. Authenticate with your Administrator credentials when asked.
5. The computer will restart. This will take some time.
6. Once you can, login with `YOURSENECAUSERNAME\Administrator` by hitting the ESC key on your keyboard. (Twice.)
7. When it says *Select a user*, select **Other user**.
8. In the next page, use the following credentials to login (tab on your keyboard to go to the next field):
    i. User name: **YOURSENECAUSERNAME\Administrator**
    ii. Password: ***yournormalpassword***
9. If it asks you about diagnostics again, select **1**.
10. In sconfig, confirm you can see:
    i. Computer name: **srv3**
    ii. Domain: **yourSenecaUsername.com**
11. Minimize *srv3* VM but keep it on!

Part 2: Install AD and DC Promotion (srv3)

Now, let's use *srv1*'s **Server Manager** to install the Active Directory role on *srv3* and promote *srv3* to a secondary Domain Controller. All remotely through the GUI.

1. Power on srv1 and login using: **YOURSENECAUSERNAME\Administrator**

> **NOTE:** You **must** login as the domain administrator. Otherwise, none of this will work!

2. In Server Manager, go to All Servers.
3. Click on *Manage > Add Servers*
4. Add *srv3*.
5. This will take a few minutes to process. **Wait until the SRV3 line says: "Online - Performance counters not started."**
6. In Server Manager, add a new role. (*Manage > Add Roles and Features*)
    i. Select: **srv3**
    ii. Select: **Active Directory Domain Services**
    iii. Go through wizard and select defaults until you get to the *Confirmation* page.
    iv. On the *Confirmation* page, select the option **"Restart the destination server automatically if required"**, then click **Install**
    v. Active Directory will now install onto *srv3*.
    vi. When complete, the **Promote this server to a domain controller** link is active on the *Results* page. **Click it**.

7. The *Active Directory Domain Services Configuration Wizard* now opens.

    i. Keep the defaults on the first page, but click on the **Change...** button. We need to authorize this connection.

    ii. The credentials window opens. Enter the following:

        a. User name: **Administrator**
        b. Password: ***yournormalpassword***

    iii. Back in the main wizard, click **Next**,

    iv. On the next page, its asking for a *DSRM password*. Enter the same password you've been using for all your admin accounts.

    v. Keep all other defaults and click **Next**.

    vi. The DNS page gives you a warning. Don't worry about it and click **Next**.

    vii. On the *Additional options* page, for the *Replicate from:* field, select *srv2* from the drop down. Click **Next**.

    viii. Click **Next** on the rest of the pages to accept defaults until you arrive on *Prerequisites Check* page.

    ix. Look for the green check mark that says: **"*All prerequisites checks passed successfully. Click Install to begin installation.*"**

    > **NOTE: If you do NOT see the green check mark, do not continue! Ask for help!**

    x. Click **Install**.

xi. It will now install. The DNS warning will come up again. Continue to ignore it.

xii. Once it finishes, click **Close**.

8. Give it a few minutes as it processes.
9. When the *srv3* VM is back to the login screen, go to *srv1*. (This will take a few minutes.)
10. Open **Server Manager** on *srv1*.
11. Go to **AD DS** and confirm *srv3* is there.
12. It may take a few moments to appear properly. **Ensure it says "Online - Performance counters not started."**
13. Any other message, ask for help!

You have now converted *srv3* into our second AD Domain Controller, mostly using the GUI remotely!

Part 3: Confirm DNS replication

Always confirm your work. Let's check on DNS.

1. In *srv1*, open the DNS tool.
2. When asked, tell it to connect to **srv3**.
3. In the new window, right-click on DNS and select **Connect to DNS Server**.
4. Add *srv2* to your list of servers in DNS.
5. Open *IPv4 > Forward Lookup Zones* in both *srv2* and *srv3*.

6. They should look identical.
7. If they do, then DNS replication is working.
8. Find *srv3* in the list, right-click, and select **Properties**.
9. Add forwarders: **149.112.121.20**
10. Congratulations, you now have two Domain Controllers!

This confirms *srv2* and *srv3* are communicating and syncing information, including DNS records.

Investigation 8: Test Without srv1

In this investigation, we'll explore the consequences of what we've set up in this lab and how much more efficient on hardware resources it is.

1. Shut down *srv1* and *srv3*.
2. Have the following VMs powered on:
    i. router
    ii. srv2
3. Power on *laptop1*.
4. Login to *laptop1* with: **YOURSENECAUSERNAME\Administrator**
5. Use Command Prompt and run: `ipconfig /all`
6. Does it look correct? If so, move to the next step.
7. Open *Firefox* and go to: **reddit.com**
8. Did that work? If so, move to the next step. **Otherwise, ask for help.**
9. In Command Prompt, run:

```
ipconfig /flushdns
nslookup srv1
nslookup srv2
```

10. Why did some of these work and not the others?

Congrats! You now have a low profile Domain Controller. Resource usage is at a minimum.

> **A note about Hyper-V:** In a real production environment, we could use *srv1* to install Hyper-V VMs on *srv2*, allowing us to run these VMs on a lower resource Core machine. That's beyond the scope of this course, but something cool to know.

Lab 6 Sign-Off

It’s essential to complete Lab 6 correctly. All later labs assume working Active Directory Domain Controllers and its services.

When you finish Lab 6, ask your instructor for a sign-off.

Sign-Off Checklist

Please have the following on screen and ready to show. You will need to power on ALL VMs for the check.

On srv1

1. *Server Manager > All Servers*: Shows *srv1*, *srv2*, and *srv3*
2. *Server Manager > AD DS*: Shows *srv2* and *srv3*
3. `ipconfig /all` shows the correct information.
4. Firefox loads: **eff.org**

On srv2

1. Sconfig shows:
    i. Name: **srv2**
    ii. Domain: **yourSenecaUsername.com**

2. In PowerShell, `ipconfig /all` shows the correct information.
3. You can ping:
    i. srv1
    ii. srv3
    iii. laptop1
    iv. eff.org
    v. reddit.com

On srv3

1. Sconfig shows:
    i. Name: **srv3**
    ii. Domain: **yourSenecaUsername.com**
2. In PowerShell, `ipconfig /all` shows the correct information.
3. You can ping:
    i. srv1
    ii. srv3
    iii. laptop1
    iv. eff.org
    v. reddit.com

On laptop1

1. System Properties shows:
    i. Name: **laptop1**
    ii. Domain: **yourSenecaUsername.com**
2. In Command Prompt, `ipconfig /all` shows the correct information.
3. You can ping:
    i. srv1
    ii. srv2
    iii. srv3
    iv. eff.org

    v. reddit.com
4. In Firefox: `http://www.reddit.com` loads the Reddit main page.

Lab 7 - AD Users, Groups, Computers, and GPOs

Lab Preparation

Purpose of Lab 7

In this lab, you'll reshape your domain into something closer to real life:

- Build a clean **OU (Organizational Unit)** structure for **people** and **computers**.
- Stop using the built-in **Administrator** and switch to a **personal admin** account.
- Use **GPOs** (Group Policy Objects) to control **how things behave**.
- Use **Groups + Delegation** to control **who is allowed to do what** in Active Directory.
- You'll prove the difference between "policy" and "permission" with three concrete users:
  - **Bob (Accounting)** — a normal employee who gets a **lockdown** user policy.
  - **Enzo (IT L1)** — can **reset passwords** in a department.
  - **Dot (IT L2)** — can **create/modify/move/delete** users in department OUs.
- Finally, you'll create the start of a **Computers OU** structure so **device-level** settings have a proper home.

Objectives

By the end of this lab, you will be able to:

- Create a tidy **HQ\Users** scaffold and a starter **HQ\Computers** scaffold.
- Create a **personal domain admin account**, verify access, and **disable** the built-in **Administrator** safely.
- Create a **User-scope GPO** (**User – Employee Lockdown**), link it to a specific **Accounting** OU, and verify that it follows the user (Bob) wherever he signs in.
- Create a **User-scope GPO** for IT (**User – IT Environment**), link it to **HQ\Users\IT**, and verify that Enzo/Dot get the intended desktop experience.
- Create ***Global Groups (GG_)*** to represent **who people are** and **Role Groups (RG_)** to represent **what a role can do**; wire them together and **delegate**:
  - **L1**: reset passwords in a department OU (e.g., Accounting).
  - **L2**: create/modify/move/delete users in department OUs (not IT).
- Build the first **Computers OUs** by hand, then complete the scaffold with a small **CSV > PowerShell script**; move *srv1* and *laptop1* into place.

Concepts

This section is your mental model. Read it once now; refer back while you work.

Users vs Computers (two different kinds of objects)

- **User object** = a person. When a **User-scope** GPO applies, it **follows the person** to any domain-joined machine they sign in to.

  Example: Bob gets “no Control Panel” everywhere he signs in.

- **Computer object** = a device. When a **Computer-scope** GPO applies, it **sticks to that device**, no matter who signs in.

  Example: Laptop sleep/USB rules apply for every user on that laptop.

> **Checkpoint:** If the question is “Does this follow the person or the device?” — you already know which scope to use.

OUs: what they are (and are not)

- An **OU (Organizational Unit)** is a folder inside AD used for **targeting** and **delegation**:
  - You **link GPOs** to OUs to target either the **users in that OU** (User-scope) or the **computers in that OU** (Computer-scope).
  - You **delegate control** on an OU to allow a group to perform tasks (like reset passwords) **for the objects inside that OU**.
- An OU is **not** a security principal. You cannot “give permissions to an OU.” You always grant permissions to **groups** (or users), then point those groups at an OU via **delegation**.

> **Analogy:** Think of OUs as labeled **folders**. Policies and delegation are **rules on the folder**. Groups are the **keyrings** you hand to people.

Groups: Global Groups VS Role Groups

We use a simple naming convention to keep your head clear:

- `GG_*` **(Global Group)** = **who they are** (identity buckets).
  You put **users** into **GGs**.

  Examples: `GG_IT_L1`, `GG_IT_L2`.

- `RG_*` **(Role Group)** = **what they can do** (delegated abilities).
  You assign **rights** to **RGs** by using the **Delegation of Control** wizard on an OU.

  Examples: `RG_PasswordReset`, `RG_OUAdmin_AllDepts`.

Wiring rule: *Put the GG inside the RG.*

- You never delegate directly to a user in production.
- You delegate to an **RG** on the target **OU**, then make the **GG** a **member** of that **RG**.
- Users gain the delegated ability by being in the **GG**.

> **Example (you'll do this):**
> Delegate **"Reset user passwords"** on `HQ\Users\Accounting` **to** `RG_PasswordReset`.
>
> Make `GG_IT_L1` a **member of** `RG_PasswordReset`.
>
> Add **Enzo** to `GG_IT_L1`.
>
> Result: Enzo can reset passwords **in that OU**.

Delegation of Control (where + what + who)

- **Where:** right-click the **target OU** (e.g., `HQ\Users\Accounting`) > **Delegate Control…**
- **What:** pick the task(s) (e.g., **Reset user passwords**, or **Create, delete, and manage user accounts**).
- **Who:** choose the **RG** (e.g., `RG_PasswordReset`, `RG_OUAdmin_AllDepts`).

> **Important:** The rights you delegate **apply only to objects in that OU (and its child OUs)**.

> If you want the same right in another department, you repeat the delegation on that department's OU.

GPOs: two halves, linked to an OU

A **GPO** is a bundle of settings with two halves:

- **User Configuration** — shapes the **user session** (Start menu, Control Panel access, etc.).
  Link it to a **Users** OU to target those users.
- **Computer Configuration** — shapes the **device** (firewall, power settings, removable storage).
  Link it to a **Computers** OU to target those devices.

We avoid advanced tricks in this lab (no **Block Inheritance**, no **Enforced**). We simply **link at the lowest sensible OU** so there's no ambiguity.

> **Examples you'll build:**
>
> - **User – Employee Lockdown** *(User)* > link to `…\Users\Accounting`.
> - **User – IT Environment** *(User)* > link to `…\Users\IT`.
> - **Computer – Workstations Baseline** *(Computer)* > link to `…\Computers\Workstations`.
> - **Computer – Laptops Baseline** *(Computer)* > link to `…\Computers\Laptops`.

Policies VS Permissions (why both exist)

- **Policy** = **configuration/behavior** the system adopts.

  Example: "Hide Control Panel" (policy) changes the UI for Bob.

- **Permission** = **authority** to perform an action in AD.

Example: “Reset passwords in Accounting” (delegation) gives Enzo the right to change those user objects.

They solve **different problems** and often work together:

- policies make the environment safe and consistent
- permissions define who can administer AD

Minimum Progression Requirements

Before beginning, you must have:

1. **Successfully graded *Lab 6***.
2. Attended the **Week 10 - AD Users, Groups, Computers, and GPOs** lecture.
3. Your external SSD (or personal computer) with your VMs.
4. Your OSM620 Lab Logbook.
5. Optional, but recommended: Caffeine delivery system.

Pre-Flight Check

Have the following VMs turned on:

1. router
2. srv1
3. srv2
4. srv3

Investigation 1: Create Personal

Domain Controller User

We’re going to give the domain a proper identity backbone before we do anything clever. That means building a clean **HQ\Users** OU path, creating a named administrator for yourself, and retiring the **built-in Administrator** account. Named admins are audit-friendly and safer. OUs (not the default *Users* container) are where policy and delegation behave predictably.

You’ll create your personal admin, verify it on both DCs, add a break-glass backup admin, and then disable the built-in Administrator.

From this point on, every right you have will be applied purpose, and every policy we link later will land exactly where we intend.

Part 1: First OU Scaffolding Setup

Before we make any accounts, we need a proper home for them. The built-in **Users** container isn’t an OU, so you can’t link GPOs to it or delegate neatly. Building **HQ\Users** (with an **IT** branch) gives us a clean, predictable place where policy and delegation will behave the way we want.

1. On *srv1*, open **Active Directory Users and Computers** (ADUC).
2. Open your domain name from the list. (Example: *cjohnson30.com*)
3. Right-click your domain name and select: **New > Organizational Unit** (Do not use the built-in Users folder!)
4. Name this new OU: **HQ**
5. Using the same **New > Organizational Unit** function, create the following hierarchy:

```
HQ
└─ Users
   └─ IT
      ├─ Helpdesk
      ├─ SecAdmins
      └─ SysAdmins
```

6. Verify your work. Does your HQ object hold the above items in the correct levels?

7. If so, move on to the next part. If not, fix your mistakes or ask for help.

Part 2: Create Personal User

Admins shouldn't live and work in the default *Administrator* account. A named admin is safer (auditing, accountability) and lets us save the built-in Administrator for emergencies. We'll create your personal admin under **HQ\Users\IT\SysAdmins** so any IT-specific policy we link there applies to you automatically.

1. On **srv1** in ADUC, navigate to: **HQ\Users\IT\SysAdmins**
2. Right-click on *SysAdmins* (or the whitespace to the right) and select: **New > User**
3. Fill out the following in the *New Object - User* dialog box:
   i. **First name:** *Your Proper First Name*
      > Example: Chris
   ii. **Last name:** *Your Proper Last Name*
      > Example: Johnson
   iii. **User login name:** *firstname.lastname*
      > Example: chris.johnson

iv. Click **Next**.

4. Fill out the following in the next page:
   i. **Password:** *same strong password as your other accounts*
   ii. **Confirm password:** *same strong password as your other accounts*
   iii. Check/uncheck the following:
      a. **User must change password at next logon:** *Unchecked*
      b. **User cannot change password:** *Unchecked*
      c. **Password never expires:** *Checked*
      d. **Account is disabled:** *Unchecked*
   iv. Click **Next**.
5. On the final page, review your settings and click **Finish**.

Part 3: Add New Personal User to Domain Controllers

Now we grant your account the rights to actually run the domain. Adding it to **Domain Admins** makes the change global.

> **NOTE:** For your new personal user to have those rights *applied*, you need to log off of that account and log back in. In this case, we haven't logged on to the account yet, so we can skip this step. But it's important to note for changes made to accounts currently logged on.

We'll also open Server Manager under your new personal account and re-add the other DCs (*srv2/srv3*).

1. On **srv1** in ADUC, navigate to: **HQ\Users\IT\SysAdmins**
2. Right-click on the user you created in Step 2 and click **Properties**.
3. In the *Properties* dialog box, click on the tab: **Member Of**
4. In the list, you should already see one entry, *Domain Users*. Click **Add**.
5. In the *Select Groups* dialog, type: **Domain Admins**

6. To verify an object named *Domain Admins* exists, click on the **Check Names** button. If it's correct, you'll see *Domain Admins* become underlined. (If not, check for typos or ask for help!)
7. Click **OK** to add.
8. Back in the *Member Of* tab, you should now see two entries. If so, click **OK** to fully apply.
9. On *srv1*, log out of your Administrator account and log back in using your new personal account by clicking on **Other user**.
   > Logging in using *firstname.lastname* should be sufficient, but if not, you can use either `yourSenecaUsername\firstname.lastname` or `firstname.lastname@yourSenecaUsername.com`.
10. Open *Server Manager > All Servers* and add *srv2* and *srv3*.

You now have full domain admin access using your personal account instead of the default Administrator account. This is far more secure and best practice.

Going forward, always log into your servers using this personal account, never the default Administrator account.

Part 4: Create a Secondary Backup Administrator

This is your break-glass admin. If your main account gets locked or broken, this one saves the day. It should work everywhere the primary does. We'll test it right away so you know it works before you ever need it.

1. On **srv1** in ADUC, create a new user in: **HQ\Users\IT\SysAdmins**
2. Same steps as Part 3, but use the following values:
   i. **Full name:** *Backup Admin*
   ii. **User login name:** *backup.admin*
   iii. All others the same as Part 3.

3. In this user's *Member Of*, add **Domain Admins**
4. Logout of srv1, log back in with this new user, and add *srv2/srv3* to Server Manager.
5. On **srv2**, log on with `backup.admin` to confirm you have backup access to your DCs.
6. If the previous step worked, congrats! Keep going. If not, stop and ask for help.

Part 5: Disable Default Administrator Account

The built-in Administrator is a well-known target for attackers. Disabling it removes a giant bullseye without taking away any capability. Your named admin replaces it (as does your backup admin).

From now on, do everything with your personal account. **Make sure you're logged on to your *firstname.lastname* admin account before continuing!**

1. On **srv1** in ADUC, navigate to: **yourSenecaUsername.com\Users** (this is *not* inside HQ)
2. Find the **Administrator** account and right-click it.
3. From the drop-down menu, select: **Disable Account**

You've now disabled the default admin account and prevented a possible attack vector.

Investigation 2: Bob from Accounting

Now we add a real employee so we can see user-scope policy do real

work. We'll carve out **HQ\Users\Accountants** and create **Bob Smith** as a standard user: no special rights, just a normal person who should get normal restrictions.

With that in place, we'll link a **User-scope GPO** to the **Accountants OU** and watch the settings follow Bob wherever he signs in.

This is the first half of the model: people live under Users OUs, and user policy follows the person. It also sets us up to delegate tasks to IT without giving them domain-wide power in the next investigations.

Part 1: Add Accountants OUs

Departments deserve their own space. By carving out **HQ\Users\Accountants**, we get a tidy spot to place real people and a perfect target for user-scope GPOs and delegation. Policies linked here will follow accountants wherever they sign in.

1. On **srv1** in ADUC, navigate to: **HQ\Users**
2. Using the **New > Organizational Unit** function, ***add*** the following to your existing hierarchy:

   ```
   HQ
   └─ Users
      └─ Accountants
   ```

3. Verify your work. Does your HQ object hold the above items in the correct levels?
4. If so, move on to the next part. If not, fix your mistakes or ask for help.

Part 2: Create User - Bob Smith

Bob is our test user for “normal staff”. We’ll give him standard settings (password change at next logon, no special rights) so we can see our **Employee Lockdown** user-GPO take effect exactly where we expect later in this investigation.

1. Create a new user in the following location: **HQ\Users\Accountants**
2. Sse the following values:
    i. **First name:** *Bob*
    ii. **Last name:** *Smith*
    iii. **User login name:** *bob.smith*
3. Fill out the following in the next page:
    i. **Password:** *same strong password as your other accounts*
    ii. **Confirm password:** *same strong password as your other accounts*
    iii. Check/uncheck the following:
        a. **User must change password at next logon:** *Checked*
        b. **User cannot change password:** *Unchecked*
        c. **Password never expires:** *Checked*
        d. **Account is disabled:** *Unchecked*

> **Note:** Modern views on passwords are to always enable *Password never expires*. In the past, we disabled this option to deal with security issues where users would write down passwords, share them, lose them, etc. A password would become invalid after a certain amount of time (say, 90 days).
>
> These days, we use **Multi-factor Authentication (MFA)** instead. We

> won't set that up in this lab, but it's a very typical addition to managed user accounts.

Part 3: Create GPO, *User - Employee Lockdown*

Bob from Accounting is a *terrible* user. He ignores written computer polices and likes to mess around with settings due to boredom and 'fixing things' instead of contacting IT support. So, we create a **Group Policy Object (GPO)** to disable his ability to change important system settings.

We have to create the GPO first before we can have it applied to Bob (and other users we want).

1. On *srv1*, open the **Group Policy Management** application.
2. In the left-hand column, expand the following: **Forest: yourSenecaUsername.com > Domains > yourSenecaUsername.com > Group Policy Objects**
3. Right-click *Group Policy Objects* and select: **New**
    i. **Name:** *User - Employee Lockdown*

Part 4: Edit GPO, *User - Employee Lockdown*

Let's add those restrictions to our new **User - Employee Lockdown** GPO.

1. In the *Group Policy Objects* list, right-click on your newly created Group Policy Object (GPO) and click **Edit**.
2. This opens the **Group Policy Management Editor** application, and loads the **User - Employee Lockdown** GPO automatically.
3. We are now going to turn on certain restrictions.
4. Prohibit access to Control Panel and PC settings.
    i. Navigate to: **User Configuration > Policies > Administrative Templates > Control Panel**.

   ii. Find **Prohibit access to Control Panel and PC settings** in the list and double-click it to open.
   iii. Click **Enabled** then **OK** to apply.
5. Repeat for the following:
   i. User Configuration > Policies > Administrative Templates > System > **Prevent access to the command prompt = Enabled**
   ii. User Configuration > Policies > Administrative Templates > System > **Prevent access to registry editing tools = Enabled**
   iii. User Configuration > Policies > Administrative Templates > Start Menu and Taskbar > **Remove Run menu from Start Menu = Enabled**
   iv. User Configuration > Policies > Administrative Templates > Windows Components > File Explorer > **Remove “Map Network Drive” and “Disconnect Network Drive” = Enabled**
   v. User Configuration > Policies > Administrative Templates > Control Panel > Printers > **Prevent addition of printers = Enabled**

Part 5: Link the *User - Employee Lockdown* GPO to Accounting

Now that we have our GPO with all the restrictions added, it's time to apply it.

The best method is to apply it at the *HQ\Users\Accounting* OU so **any** accounting employee will inherit this GPO and its restrictions, including Bob.

Much better than applying it to 50 different employees one at a time!

1. Back in the *Group Policy Management* application, right-click on: **HQ\Users\Accounting**
2. Click **Link an existing GPO**
3. Select **User - Employee Lockdown** from the list and click **OK**.
4. You should now see it in the list in the main *Linked Group Policy Objects*

pane for *Accounting*. If you don't, double-check your work and ask for help before proceeding.

Part 6: Verify Bob's Restrictions

We should check that our restrictions have worked.

1. Logout of your account on *srv1*.
2. Log on to Bob's account: **bob.smith**
    i. You will be asked to reset the password on first login. This is normal. Pick something complex but basic and **write it down in your Lab Logbook**.
3. Once logged in, try to open up **Settings**. Does it let you?
4. If not, nicely done! Move on to the next part of the lab.

This is a good example of applying settings to a user account. No matter what HQ workstation Bob logs into, these restrictions will *follow him*.

> **Note:** Normally, we'd use a workstation to test Bob's account, not a server. We're using *srv1* here to conserve lab resources. We'll test with *laptop1* towards the end of this lab.

Investigation 3: Enzo Matrix - IT Helpdesk

We're going to create a user that provides Level 1 IT support to employees in the rest of the company.

Unlike Bob, who we only needed to restrict what access he had to computers he logged into directly, with Enzo, we have to grant him *specific* admin privileges in Active Directory so he can manage certain things.

A Level 1 Helpdesk employee always has the same terrible job: Reset passwords for employees who have forgotten their own.

This requires some extra steps beyond what we did with Bob from Accounting.

Let's set that up.

Part 1: Create GPO, *User - IT Environment*

The previous GPO we created is far too restrictive for an IT employee. They can be trusted to make changes to their own system.

Remember, Group Policy Objects (GPOs) are about modifying *default behaviour*. Think about when you log into a normal Windows machine you own. You can access Control Panel, right? So, to allow it here, all we need to do is **not** disable it. The default is to allow access. Same with the other restrictions we placed on the previous GPO.

Instead of adding restrictions, we're going to add some shortcuts for common AD management tools to the IT users' desktops.

1. Open the **Group Policy Management** and navigate to: **Forest: yourSenecaUsername.com > Domains > yourSenecaUsername.com > Group Policy Objects**
2. Create a new GPO here called: **User - IT Environment**
3. **User Configuration > Preferences > Windows Settings > Shortcuts > *Right-Click* > New > Shortcut**
4. Add the following shortcuts:
    i. Server Manager
        a. **Name:** *Server Manager*
        b. **Location:** *Desktop*
        c. **Target Path:** *%SystemRoot%\System32\ServerManager.exe*

    d. Keep all other fields as defaults.
ii. Active Directory Users and Computers
    a. **Name:** *Active Directory Users and Computers*
    b. **Location:** *Desktop*
    c. **Target Path:** *%SystemRoot%\System32\dsa.msc*
    d. Keep all other fields as defaults.
iii. Group Policy Management
    a. **Name:** *Group Policy Management*
    b. **Location:** *Desktop*
    c. **Target Path:** *%SystemRoot%\System32\gpmc.msc*
    d. Keep all other fields as defaults.

Part 2: Create User - Enzo Matrix

Enzo is our **Level 1 Helpdesk** employee. He needs an IT-friendly desktop (shortcuts, fewer restrictions than Bob) and, soon, the ability to reset passwords in a specific department.

We'll set him up now so the GPO and group wiring we do next has a real user to affect.

1. Create a new user in the following location: **HQ\Users\IT\Helpdesk**
2. See the following values:
    i. **First name:** *Enzo*
    ii. **Last name:** *Matrix*
    iii. **User login name:** *enzo.matrix*
3. Fill out the following in the next page:
    i. **Password:** *same strong password as your other accounts*
    ii. **Confirm password:** *same strong password as your other accounts*
    iii. Check/uncheck the following:

a. **User must change password at next logon:** *Checked*
b. **User cannot change password:** *Unchecked*
c. **Password never expires:** *Unchecked*
d. **Account is disabled:** *Unchecked*

Part 3: Link the *User - IT Environment* GPO to IT

Now that we have our GPO with all our additions included, it's time to apply it. We'll apply it to the *IT* OU, since it should apply to everyone there (all IT employees).

1. Back in the *Group Policy Management* application, right-click on: **HQ\Users\IT**
2. Click **Link an existing GPO**
3. Select **User - IT Environment** from the list and click **OK**.
4. You should now see it in the list in the main *Linked Group Policy Objects* pane for *IT*. If you don't, double-check your work and ask for help before proceeding.

Part 4: Global Groups

This is where we get into personal desktop environment settings VS Active Directory admin settings. GPOs are for personal desktop environments that a user sees when they login.

By contrast, we use Global Groups+Role Groups to grant certain AD admin tasks to groups of users.

For reference:

1. **GPO+User OU** = Desktop settings and restrictions on the local machine a user logs into.
2. **Global Groups+Role Groups** = Combinations of AD administrative tasks assigned to groups of users. This is to allow certain users to change Active Directory settings and configuration, not local computers.

A **Global Group *(GG)*** is, essentially, an *identity group*. We use Global Groups to add users together, and then apply a role to the group. Each user in that group then gets that role applied. (We do the roles part a bit later.)

Let's create an AD admin-type group (Global Group, GG) for IT Level 1. Remember, this is just a group of users.

1. In ADUC, navigate to: **HQ**
2. Using the **New > Organizational Unit** function, ***add*** the following to your existing hierarchy:

   ```
   HQ
   └─ Groups
      └─ Global
   ```

3. In *HQ\Groups\Global*, create a new **Group** object with the following settings:
   i. **Group name:** *GG_IT_L1*
   ii. **Group scope:** *Global*
   iii. **Group type:** *Security*

Part 5: Role Groups

In contrast to Global Groups, a **Role Group *(RG)*** is a collection of AD admin

privileges under a single profile. You can have many RGs, each with different sets of AD admin privileges.

Let's create our first RG and then add a single AD admin privilege to it: Reset passwords.

1. In ADUC, navigate to: **HQ**
2. Using the **New > Organizational Unit** function, ***add*** the following to your existing hierarchy:

   ```
   HQ
   └─ Groups
      └─ Roles
   ```

3. In *HQ\Groups\Roles*, create a new **Group** object with the following settings:
   i. **Group name:** *RG_PasswordReset*
   ii. **Group scope:** *Domain Local*
   iii. **Group type:** *Security*
4. In *HQ\Users\Accounting*, right-click and select: **Delegate control...**
5. In the *Delegation of Control Wizard*'s > *Users or Groups* page, add: **RG_PasswordReset**
6. In *Delegation of Control Wizard > Tasks to Delegate*, select: **Reset user passwords and force password change at next logon**
7. Review your settings on the last page, then click **Finish**.

Part 6: Wire Global Group to Role Group

We'll now assign our new RG from *Part 5* to our Global Group **GG_IT_L1**. This means that anyone who's a part of *GG_IT_L1* will get the AD admin privilege assigned in *RG_PasswordReset*.

1. In ADUC, navigate to: **HQ\Groups\Roles**
2. Double-click on **RG_PasswordReset** to open its Properties.
3. In the *Properties* window, go to the **Members** tab and click on: **Add...**
4. In the *Select Users, Contacts, Computers, Service Accounts, or Groups* window, type: **GG_IT_L1**
5. Click **OK** and verify it shows up in the *Members* tab.

The Global Group of users *GG_IT_L1* now has all the AD admin privileges given to Role Group *RG_PasswordReset*.

Part 7: Add Enzo to GG IT Helpdesk Level 1

And now we put it all together. We add Enzo to the Global Group *GG_IT_L1*. Once we do that, Enzo will be able to reset passwords for all users inside *HQ\Users\Accounting*.

1. In ADUC, navigate to: **HQ\Groups\Global**
2. Double-click on **GG_IT_L1** to open its Properties.
3. In the *Properties* window, go to the **Members** tab and click on: **Add...**
4. In the *Select Users, Contacts, Computers, Service Accounts, or Groups* window, type: **Enzo Matrix**
5. Click **OK** and verify it shows up in the *Members* tab.

That's it! If we ever want to add more IT employees to Helpdesk Level 1, we'd just repeat Part 7 with the new user. The rest is already setup.

Part 8: Verify Enzo's Access and Environment

We should check that our new Enzo account works, has our user GPO applied (those desktop shortcuts), and our Helpdesk Level 1 admin access applied.

1. Logout of your account on *srv1*.
2. Log on to Enzo's account: **enzo.matrix**
    i. You will be asked to reset the password on first login. This is normal. Pick something complex but basic and **write it down in your Lab Logbook**.
3. Once logged in, try to open up **Settings**. Does it let you? It should, this time.
4. Does the desktop contain the three shortcuts we configured:
    i. **Server Manager**
    ii. **Active Directory Users and Computers**
    iii. **Group Policy Management**
5. Open ADUC and go to: **HQ\Users\Accounting**
6. Right-click on **Bob Smith** and select *Disable Account*. It doesn't work, does it? It shouldn't; Enzo doesn't have permissions to do that.
7. Right-click on **Bob Smith** and select *Reset Password*.
8. Reset Bob's password. Can you?
9. If so, move on to the next part of the lab.

Investigation 4: Dot Matrix - IT Helpdesk L2

We're going to create a user that provides **Level 2 IT support** to employees in the rest of the company.

A Level 2 Helpdesk employee has their own special AD admin privileges, along with those in Level 1.

In theory, a Level 2 Helpdesk employee shouldn't be contacted for password resets, but she may be asked to do that after completing some L2 tasks for an employee. It happens.

Fortunately, most of the work here is already done. All we need to do is create a new user, and the L2 GG and RGs.

Part 1: Global Group - GG_IT_L2

Let's create an AD admin-type group (Global Group, GG) for IT Level 2. Remember, this is just a group of users.

1. In ADUC, navigate to: **HQ\Groups\Global** and create a new **Group** object with the following settings:
    i. **Group name:** *GG_IT_L2*
    ii. **Group scope:** *Global*
    iii. **Group type:** *Security*

Part 2: Role Group - RG_OUAdmin_AllDepts

Remember, a **Role Group *(RG)*** is a collection of AD admin privileges under a single profile.

Let's create an RG that allows L2 staff to create, modify, move, and delete users in other departments.

As an example, if Bob from Accounting gets reassigned to a different department, a Level 2 specialist like Dot would be the one to move him from one department to the next in the AD structure.

Or disable his account if he gets fired. (*He is terrible, after all.*)

1. In ADUC, navigate to: **HQ\Groups\Roles** and create a new **Group** object with the following settings:
    i. **Group name:** *RG_OUAdmin_AllDepts*
    ii. **Group scope:** *Domain Local*
    iii. **Group type:** *Security*
2. In *HQ\Users\Accounting*, right-click and select: **Delegate control...**
3. In the *Delegation of Control Wizard*'s *> Users or Groups* page, add: **RG_OUAdmin_AllDepts**
4. In *Delegation of Control Wizard > Tasks to Delegate*, select: **Create, delete, and manage user accounts**
5. Review your settings on the last page, then click **Finish**.

Part 3: Wire Global Group to Role Group

We'll now assign our new RG from *Part 2* to our Global Group **GG_IT_L2**. This means that anyone who's a part of *GG_IT_L2* will get the AD admin privilege assigned in *RG_OUAdmin_AllDepts*.

1. In ADUC, navigate to: **HQ\Groups\Roles**
2. Double-click on **RG_OUAdmin_AllDepts** to open its Properties.
3. In the *Properties* window, go to the **Members** tab and click on: **Add...**
4. In the *Select Users, Contacts, Computers, Service Accounts, or Groups* window, type: **GG_IT_L2**
5. Click **OK** and verify it shows up in the *Members* tab.

The Global Group of users *GG_IT_L2* now has all the AD admin privileges given

to Role Group *RG_OUAdmin_AllDepts*.

Part 4: Create User - Dot Matrix

Time to create our L2 user, Dot Matrix.

1. Create a new user in the following location: **HQ\Users\IT\Helpdesk**
2. Sse the following values:
    i. **First name:** *Dot*
    ii. **Last name:** *Matrix*
    iii. **User login name:** *dot.matrix*
3. Fill out the following in the next page:
    i. **Password:** *same strong password as your other accounts*
    ii. **Confirm password:** *same strong password as your other accounts*
    iii. Check/uncheck the following:
        a. **User must change password at next logon:** *Checked*
        b. **User cannot change password:** *Unchecked*
        c. **Password never expires:** *Unchecked*
        d. **Account is disabled:** *Unchecked*

Part 5: Add Dot to GG IT Helpdesk Level 1 *and* Level 2

As mentioned, a Level 2 Helpdesk staff should have L2 AD admin privileges *and* L1 AD admin privileges. **Let's add both.**

1. In ADUC, navigate to: **HQ\Groups\Global**
2. Double-click on **GG_IT_L1** to open its Properties.
3. In the *Properties* window, go to the **Members** tab and click on: **Add...**
4. In the *Select Users, Contacts, Computers, Service Accounts, or Groups*

window, type: **Dot Matrix**

5. Click **OK** and verify it shows up in the *Members* tab.
6. Go back to ADUC and navigate to: **HQ\Groups\Global**
7. Double-click on **GG_IT_L2** to open its Properties.
8. In the *Properties* window, go to the **Members** tab and click on: **Add...**
9. In the *Select Users, Contacts, Computers, Service Accounts, or Groups* window, type: **Dot Matrix**
10. Click **OK** and verify it shows up in the *Members* tab.

That's it! Dot has now been granted the AD admin privileges for Level 1 ***and*** Level 2.

Part 6: Verify Dot's Access and Environment

We should check that our new Dot account works, has our user GPO applied (those desktop shortcuts), and our Helpdesk Level 1/Level 2 admin access applied.

> **Note:** We didn't have to do anything with GPOs this time, as we applied our IT GPO to the IT folder in Users earlier. So, when Dot was created there, she inherited that GPO. **Cool, right?**

1. Logout of your account on *srv1*.
2. Log on to Dot's account: **dot.matrix**
    i. You will be asked to reset the password on first login. This is normal. Pick something complex but basic and **write it down in your Lab Logbook**.
3. Once logged in, try to open up **Settings**. Does it let you? It should, this time.
4. Does the desktop contain the three shortcuts we configured:
    i. **Server Manager**

    ii. **Active Directory Users and Computers**
    iii. **Group Policy Management**
5. Open ADUC and go to: **HQ\Users\Accounting**
6. Right-click on **Bob Smith** and select *Disable Account*. It works now, doesn't it? It should. Enzo didn't have permissions to do that, but Dot does.
7. Right-click and Enable the Bob account again so we can keep using it.
8. Verify your L1 permissions: Right-click on **Bob Smith** and select *Reset Password*.
9. Don't reset his password again. Opening the window is enough
10. If all these work, move on to the next part of the lab.

Investigation 5: Computers - OUs and GPOs

In this investigation, we'll create computer-based OUs and GPOs.

Until now, we've been working with User OUs and GPOs. Complicated as they may get, at the end of the day, these are all about settings and permissions that **follow a user**.

Computer OUs, by contrast, are applied at the computer level regardless of who's logged on.

An easy example: Network settings, like configuring an IP address, are applied at the computer level, not the user level. (Can you imagine if network settings changed every time a different user logged in?)

The following investigation allows us to organize the computers we have joined to our Active Directory domain and what settings to apply to each.

Part 1: First OU Scaffolding Setup

1. On *srv1*, open **Active Directory Users and Computers** (ADUC).
2. Open your domain name from the list. (Example: *cjohnson30.com*)
3. Open the **HQ** OU as before.
4. Inside it, right-click **HQ** and select: **New > Organizational Unit**
5. Name this new OU: **Computers**
6. Using the same **New > Organizational Unit** function, ***add*** the following to your existing HQ\Computers hierarchy:

   ```
   HQ
   └─ Computers
      └─ Workstations
         ├─ Accounting
         └─ IT
      └─ Laptops
         ├─ Accounting
         └─ IT
      └─ Servers
         └─ Members
   ```

7. Verify your work. Does your HQ object hold the above items in the correct levels?
8. If so, move on to the next part. If not, fix your mistakes or ask for help.

Part 2: Move Computers into the Correct OUs

1. In ADUC, click the built-in Computers container (CN=Computers) and your domain root to find machine accounts.

2. Move (drag and drop) to the new OUs:

    i. *srv1* > **HQ\Computers\Servers\Members**

    ii. *laptop1* > **HQ\Computers\Laptops\Accounting**

    > **Note:** Do not move *srv2* and *srv3*! Keep them where they are.

3. Verify your work. Are your *srv1* and *laptop1* computers in the correct OUs?

4. If so, move on to the next part. If not, fix your mistakes or ask for help.

> **Why not move *srv2* and *srv3*?**
> Domain Controllers live in a special **Domain Controllers** OU with their own built-in GPO (`Default Domain Controllers Policy`).
>
> In real environments, DCs are usually managed separately from normal servers, so we're leaving them where they are.

Part 3: Create Computer Baseline GPOs

Now that we have our Computers OUs, we'll create **Computer-scope** GPOs that can apply to devices in those OUs.

We'll make two simple baseline GPOs:

- **Computer – Workstations Baseline**
- **Computer – Laptops Baseline**

In a real company, these would eventually diverge (different sleep policies, USB

rules, etc.). For this lab, we'll give them the same simple setting so you can *see* a device-level policy in action on `laptop1`.

We'll add a standard **logon banner**. This is a message that appears before anyone logs in. Because it's a **Computer** setting, it will apply to *any* user who signs in on that device. (In this case, before anyone logs in at all, too.)

1. On *srv1*, open **Group Policy Management**.
2. In the left pane, navigate to:
   Forest: yourSenecaUsername.com > Domains > yourSenecaUsername.com > Group Policy Objects
3. Right-click **Group Policy Objects** > **New…**
4. Create a new GPO:
   i. **Name:** `Computer – Workstations Baseline`
5. Repeat **Step 3–4** to create a second GPO:
   i. **Name:** `Computer – Laptops Baseline`

Now we'll edit **both** GPOs to add the same logon message.

6. Right-click **Computer – Workstations Baseline** > **Edit…**
7. In the *Group Policy Management Editor* window, go to:

   Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

8. In the right pane, find the following two policies:

   i. **Interactive logon: Message title for users attempting to log on**
   ii. **Interactive logon: Message text for users attempting to log on**

9. Double-click **Interactive logon: Message title for users attempting to log on**:

    i. Set **Security Setting** to something like:
    `OSM620 HQ – Authorized Use Only`
    ii. Click **OK**.

10. Double-click **Interactive logon: Message text for users attempting to log on**:

    i. Set **Security Setting** to something like:

    `This system is for authorized use only. Activity may be monitored. By signing in, you agree to comply with company policy.`

    ii. Click **OK**.

11. Close the *Group Policy Management Editor* window.

12. Repeat **Steps 6–11**, but this time for **Computer – Laptops Baseline** so that both GPOs have the same logon banner configured.

> **Why a logon banner?**
> It's a **Computer-scope** setting that shows up *before* anyone signs in. That makes it a perfect visual example of "policy sticks to the device, not the person."

Part 4: Link Computer GPOs to the Computers OUs

Now we'll link our new Computer GPOs at the correct places in the **HQ\Computers** tree.

1. In **Group Policy Management**, expand:
   Forest: yourSenecaUsername.com > Domains >

yourSenecaUsername.com > yourSenecaUsername.com > HQ > Computers

2. Right-click **Workstations** > **Link an Existing GPO…**
3. Choose **Computer – Workstations Baseline** > **OK**.
4. Right-click **Laptops** > **Link an Existing GPO…**
5. Choose **Computer – Laptops Baseline** > **OK**.

You should now see:

- `Computer – Workstations Baseline` linked at **HQ\Computers\Workstations**
- `Computer – Laptops Baseline` linked at **HQ\Computers\Laptops**

Remember from **Part 2**:

- `srv1` is in **HQ\Computers\Servers\Members**
- `laptop1` is in **HQ\Computers\Laptops\Accounting**

So right now, **only** `laptop1` will actually inherit **Computer – Laptops Baseline**.

Part 5: Verify Laptop Baseline on *laptop1*

Let's prove that this GPO is really a **Computer-scope** policy that "sticks" to `laptop1`.

1. On *laptop1*, sign in with your normal domain account (*yourSenecaUsername*).
2. Open **Command Prompt** using *Run as Adminstrator*.
3. Run: `gpupdate /force`
   This forces the new Computer policy to apply right away instead of waiting.
4. When it completes, confirm your work by running the following: `gpresult`

`/r /scope computer`

5. You should see something similar to the following:

```
C:\Windows\System32>gpresult /r /scope computer

Microsoft (R) Windows (R) Operating System Group Policy Result
tool v2.0
© Microsoft Corporation. All rights reserved.

Created on 2025-11-22 at 4:47:29 PM


RSOP data for  on LAPTOP1 : Logging Mode
-----------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26200
Site Name:                   Default-First-Site-Name
Roaming Profile:
Local Profile:
Connected over a slow link?: No


COMPUTER SETTINGS
------------------

CN=LAPTOP1,OU=IT,OU=Laptops,OU=Computers,OU=HQ,DC=cjohnson30,DC=com
    Last time Group Policy was applied: 2025-11-22 at 4:37:30 PM
    Group Policy was applied from:      srv2.cjohnson30.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        CJOHNSON30
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Computer - Laptop Baseline
```

> **Notice the line: *Computer - Laptop Baseline***

1. Once confirmed, restart `laptop1`.
2. After the restart, look carefully at the **logon screen**:
    i. Do you see the **title** and **message text** you configured in Part 3?
3. Sign in as a different domain user (for example, Enzo or Dot, once their accounts are set up).
4. Confirm that the **same logon banner** appears for them as well.

If the banner shows up before *any* user signs in, you've just seen a **Computer-scope** GPO in action:

- It follows the **device (`laptop1`)**, not the individual user.
- Every domain user on that device must see and acknowledge the message.

If you **don't** see the message:

1. Double-check that:
    i. `laptop1` is in **HQ\Computers\Laptops\Accounting** in ADUC.
    ii. **Computer – Laptops Baseline** is linked at **HQ\Computers\Laptops**.
2. Run `gpupdate /force` again on *laptop1* and restart one more time.
3. If it still doesn't work, ask your instructor for help.

> **Note:** In a real environment, admins can trigger a *Group Policy Update* remotely from GPMC on the domain or OU, but for this lab you'll run `gpupdate /force` locally on *laptop1*.

Lab 7 Sign-Off

It's essential to complete Lab 7 correctly. Lab 8 assumes you have your users, groups, and computers properly organized in Active Directory.

When you finish Lab 7, ask your instructor for a sign-off.

Sign-Off Checklist

Please have the following on screen and ready to show. You will need to power on the following VMs:

- srv1
- srv2
- laptop1

On srv1:

Using your `firstname.lastname` Domain Administrator account, show the following in *Active Directory Users and Computers*.

HQ\Users OU structure

1. In Active Directory Users and Computers, show:
    i. Bob Smith in HQ > Users > Accountants
    ii. Enzo Matrix in HQ > Users > IT > Helpdesk
    iii. Dot Matrix in HQ > Users > IT > SysAdmins

HQ\Computers OU structure

1. In HQ > Computers, show:
    i. srv1 in Servers > Members
    ii. laptop1 in Laptops > Accounting
    iii. User and Computer GPOs
2. In Group Policy Management, show that:
    i. Your Employee user GPO (for example, User – Employee Lockdown) is linked at HQ > Users > Accountants.
    ii. Your IT user GPO (for example, User – IT Environment) is linked at HQ > Users > IT.
    iii. Your Laptop computer GPO (for example, Computer – Laptops Baseline)

is linked at HQ > Computers > Laptops.

If all of the above are present, your directory structure and GPO links are considered correct for this lab.

Test your user accounts:

1. Log into Enzo Matrix.
2. Log into Dot Matrix.

On laptop1:

1. Log into Bob Smith.
2. Log into your `firstname.lastname` Domain Administrator account.

Assignment 1 - Roaming Employee Laptop

Lab Preparation

Purpose of Assignment 1

In this assignment, you will provision a new Windows 11 “office laptop,” validate how it behaves **on premises** (HQ Network) versus **remote** (over the Internet via VPN), and explain routing/DNS differences between the two scenarios.

Scenario Overview: A new employee has been hired and you are in charge of onboarding them. This means provisioning a new company laptop for them to use for their work.

Scenario 1 - On-Premises: Your employee will be in the office with their new company laptop, physically connected to the internal network.

Scenario 2 - Remote: Your new employee also needs to work from home. Their remote work requires access to the company's internal network resources.

This is a technical assignment with a reflection component. Your deliverable will be online inside a single PDF through Blackboard. (Check the *Submission* section at the end of this assignment.)

You will produce screenshots and short written explanations (“why/why not?”) to prove each step. The assignment instructs you when to do each with the following notes:

> **Screenshots:** Heads up of screenshots you will need to take shortly, with a list at which steps each screenshot should be taken.
>
> **Reflection:** Questions you will answer to show some thought and understanding of the overall effects of what you're doing.

If you encounter technical issues, please contact your professor via e-mail or in your section's Microsoft Teams group.

Objectives

By the end, you will:

1. Distinguish **on-prem** VS **remote** access paths and when VPN is required.
2. **Enable and configure L2TP/IPsec (PSK)** in RRAS (RRAS is already installed).
3. Connect a client to your server using VPN over the Internet.
4. Prove DNS/web reachability to internal services **using FQDNs**.
5. Use `tracert` and `nslookup` output to explain routing/DNS behavior.

Minimum Progression Requirements

Before beginning, you must have:

1. Successfully completed Lab 1-5.
2. Watched the *Introduction to Assignment 1* recorded lecture available through Blackboard.
3. Your external SSD (or personal computer) with your VMs.

4. Optional, but recommended: Caffeine delivery system.

Minimum Hardware Requirements

It is *possible* to run Assignment 1 on a non-lab computer. I have done my best to reduce requirements. You may be able to run A1 on your personal computer. You will need an Intel/AMD-based computer with VMware Workstation installed. Check the grid below.

Lab computers are available on campus during Study Week and outside of class time.

Absolute Minimum Hardware

This may result in slow performance and disruptions, but is possible.

VM	OS	Cores	RAM
srv1	Windows Server 2025, Desktop Experience	2 cores	4 GB
srv2	Windows Server 2025, Core	2 cores	4 GB
laptop1	Windows 11 Education	2 cores	4 GB
Total:	-	4-6 cores	8-12 GB

> **Note:** Most of your work only requires *srv2* to be on temporarily. The absolute minimum would be 4 cores and 8 GB of RAM. I cannot guarantee stability under these settings. Use at your own risk.

Recommended Minimum Hardware

This is the recommended minimum hardware requirements for A1.

VM	OS	Cores	RAM
srv1	Windows Server 2025, Desktop Experience	4 cores	8 GB
srv2	Windows Server 2025, Core	2 cores	4 GB
laptop1	Windows 11 Education	2 cores	4 GB
Total:	-	6-8 cores	12-16 GB

> **Note:** Most of your work only requires *srv2* to be on temporarily. The absolute **recommended** minimum would be 6 cores and 12 GB of RAM.

Investigation 1: Installing *laptop1* VM

In this investigation, you will create and install a new VM called *laptop1*. This VM will be created **in VMware Workstation**, *not* Hyper-V.

Scenario: You are setting up a company laptop for a new employee.

Before You Begin

Time to Backup! You will be making major changes to *srv1*. This is a good time to backup the *srv1* VM so you can restore from it if something catastrophic occurs.

With *srv1* turned off, copy the entire **srv1** folder in your SSD to a separate location. This can be a backup directory on your SSD, or even a separate physical drive. Leave the copy be and use the original going forward. (If you need space, compress the backup folder.)

Do not continue until the copy has fully completed.

Part 1: Creating *laptop1* VM

In this part, you will create a new Windows 11 virtual machine using the hardware specifications below.

> **Note:** Keep all other VMs off until told otherwise.

Virtual Machine Specifications:

- Hypervisor: **VMware Workstation**
- Name: **laptop1**
- Location: **OSM620/Virtual Machines/laptop1**
- Encrytiption Information: **See note below.**
- RAM: **4 GB**
- CPU: **2 processors**
- Storage: **64 GB**
- NIC: **1**, set to **NAT**

- ISO: **Windows 11 Education**

If you can't remember how to create a VMware virtual machine, please refer back to Lab 1.

Encryption Information Page

Like with *client1* and *client2*, this VM's Windows 11 uses a TPM to encrypt certain important files. Unlike Hyper-V, VMware Worksation adds the TPM module automatically.

- Choose Encryption Type: **Only the files needed to support a TPM are encrypted.**
- Password: **Your normal VM password.**

You do need to choose the encryption type and give it a password. **Use the same password you've used for all other VMs in this course.**

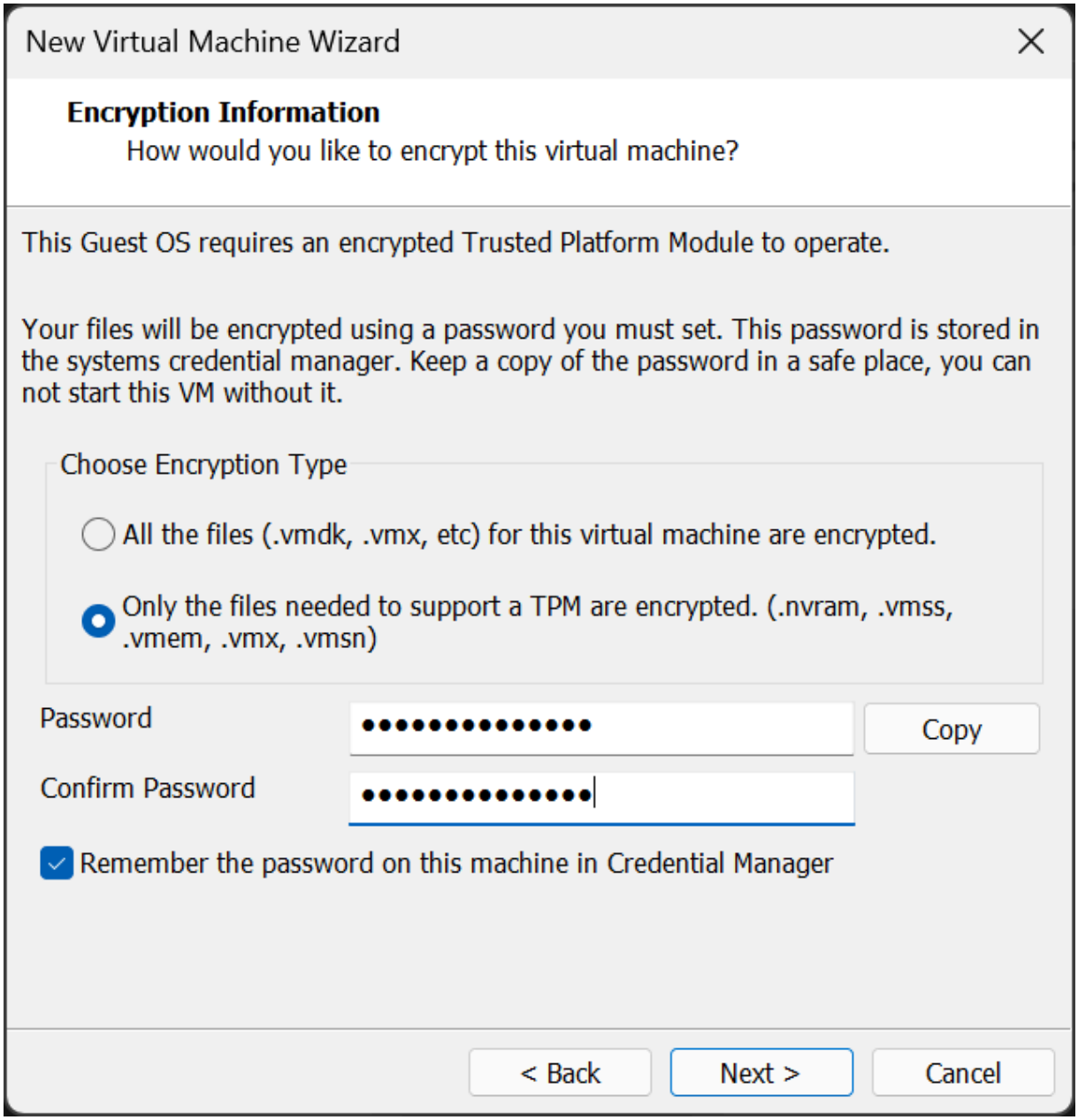


Figure 1. The Encryption Information page for creating a new Windows 11 VM in VMware.

Part 2: OS Installation and Configuration

Use the following instructions to install the OS and run post-installation tasks on your new *laptop1* VM.

1. Create the VM with the specifications above.
2. When creating the user, use `firstname.lastname`
3. Run through the standard **Post-Installation Tasks** you ran in *Lab 2*.
4. When complete (including internal name and updates!), shut down the VM.

Investigation 2: Add `laptop1` to Local HQ Network

Here, we'll connect our new `laptop1` machine to office HQ network and access some local resources.

Scenario: A physical laptop connected to Ethernet inside our company's physical office.

Before You Begin

We will *not* be using our Hyper-V VMs in this assignment. To make things easier, change *srv1*'s hardware settings in VMware Workstation while the VM is powered off.

On *srv1:*

1. CPU: **Change from 6-cores to 4-cores.**
2. RAM: **Change from 16 GB to 8 GB**

On *srv2*:

1. Disconnect the NAT NIC, leaving only the NIC with the 10.0.`UID`.2 online. *srv2* should only be reachable though the 10.0.`UID`.0/24 network (HQ Network). (Refer to *Fig. 2* and *Fig. 3* below.)

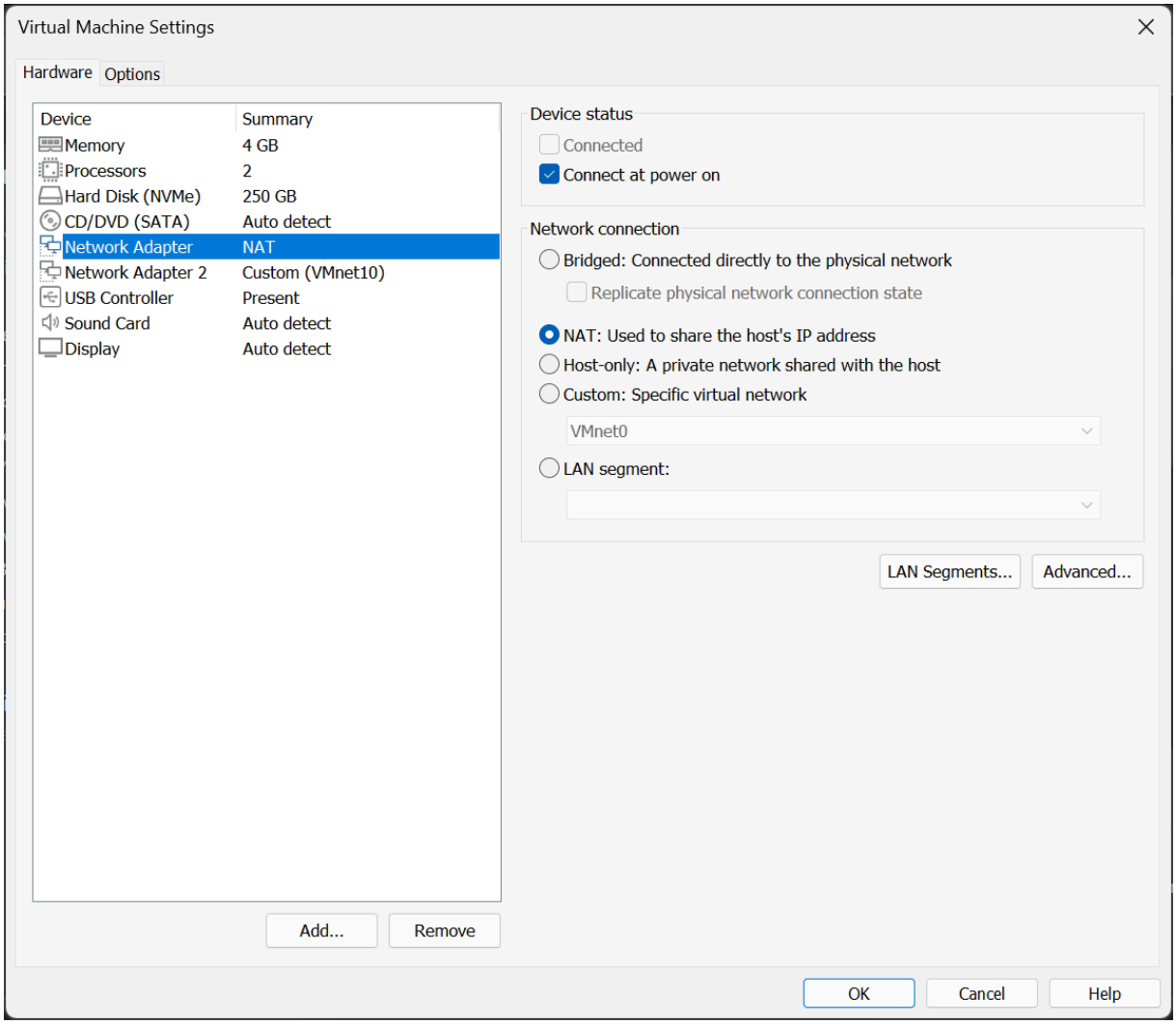


Figure 2. NIC1 connected in VMware's Hardware Settings.

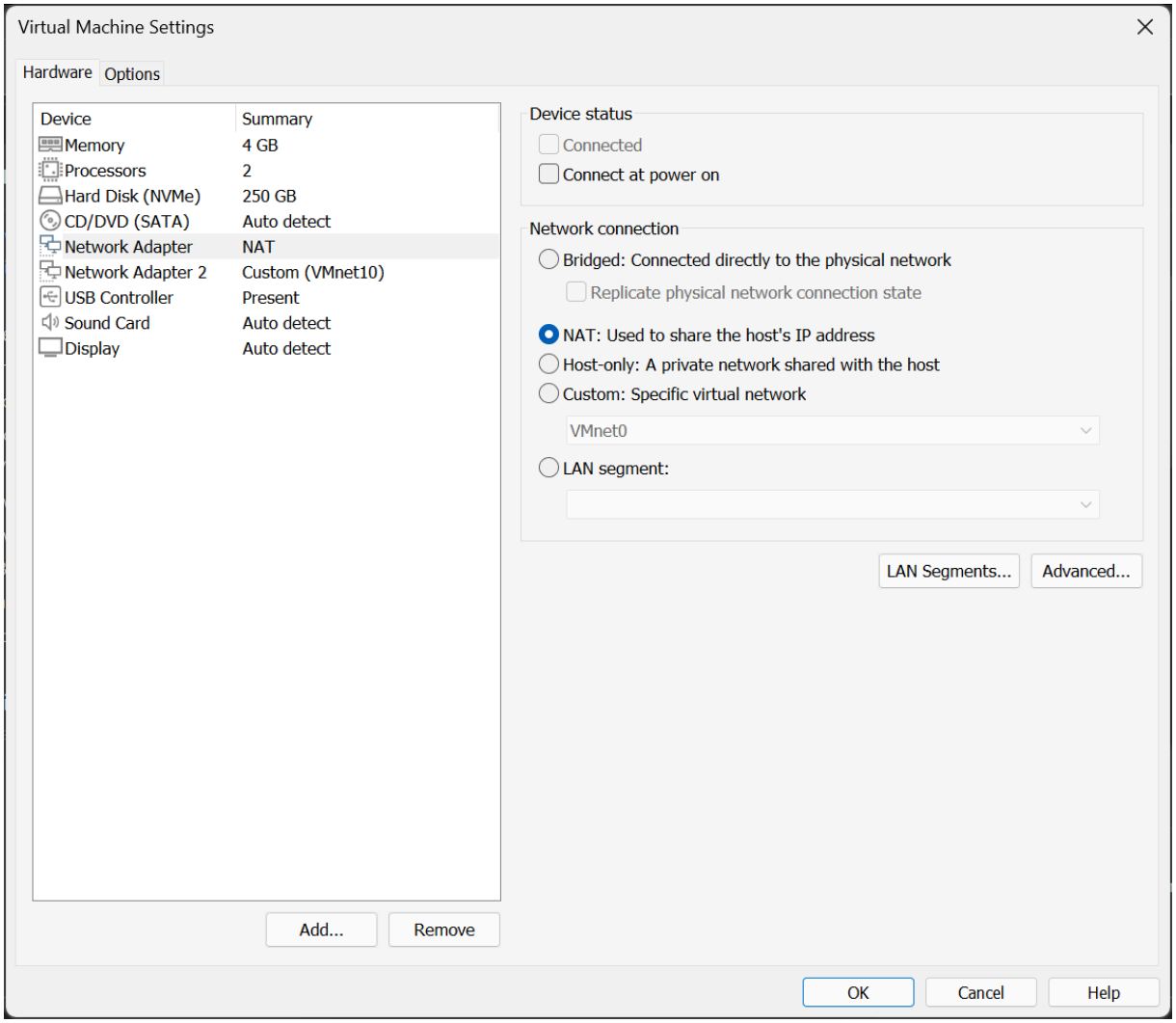


*Figure 3. NIC1 **disconnected** in VMware's Hardware Settings.*

Part 1: Switching the Network

We need to switch `laptop1`'s network connection from the basic Internet to our office's internal network.

1. Power on `srv1`.
2. Power on `srv2`.
3. Power on `laptop1` and login with your `firstname.lastname` credentials.
4. In VMware's hardware settings for `laptop1`, change NIC1 from **NAT** to

VMnet10.

5. Wait for the changes to apply. This may take a few moments.

Part 2: Testing Connections to HQ Resources

Let's see if we can access all the HQ resources we were able to with our other VMs in previous labs.

> **Screenshots:** Take full desktop screenshots of the end of the following steps:
>
> 1. Step 4 (Screenshot 1)
> 2. Step 5 (Screenshot 2)
> 3. Step 6 (Screenshot 3)

1. Switch to `laptop1`.
2. Open *Command Prompt*.
3. Reset DNS cache: `ipconfig /flushdns`
4. Let's check DNS resolution. Run the following:
    i. `nslookup srv1.YourSenecaUsername.com`
    ii. `nslookup srv2.YourSenecaUsername.com`
    iii. `nslookup eff.org`

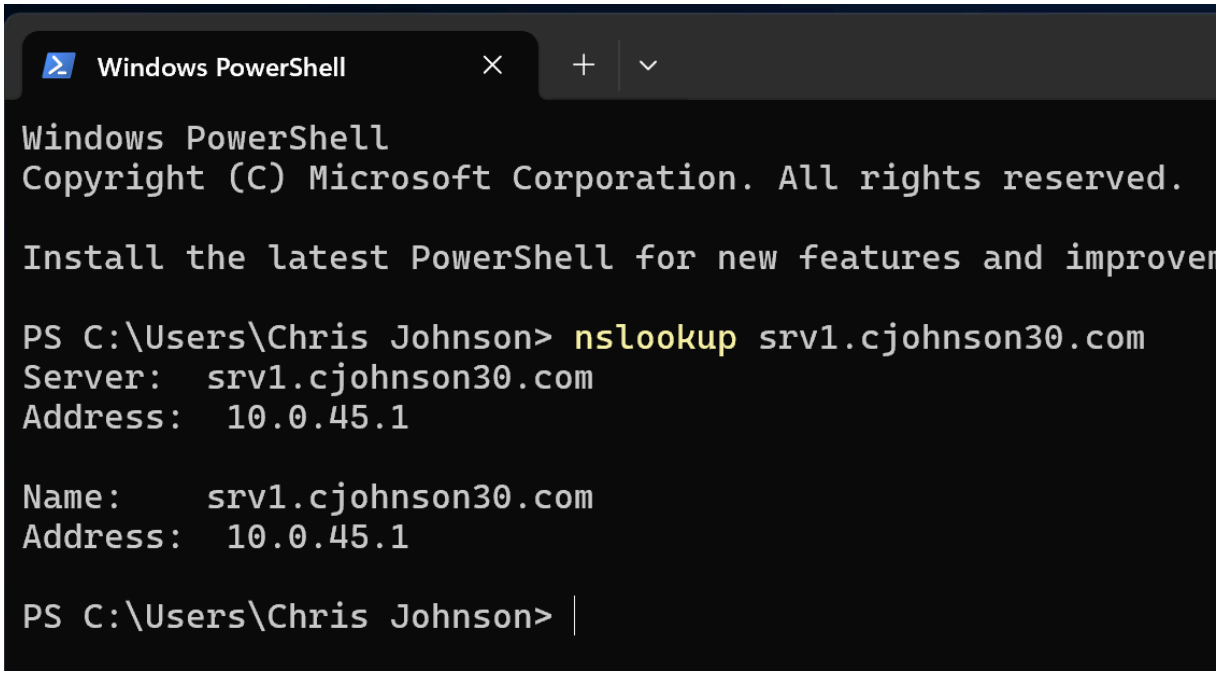


Figure 4. Example of a successful DNS lookup using srv1.

5. Now, let's confirm we have connections to these resources:
   i. `ping srv1.cjohnson30.com`
   ii. `ping srv2.cjohnson30.com`
   iii. `ping eff.org`
6. Finally, let's take a look at the **path through the network** that our connection to these resources is taking. `tracert` is a utility that tracks each hop taken between your computer and the destination and shows any others it travelled through to get there. Run the following:
   i. `tracert srv1.cjohnson30.com`
   ii. `tracert srv2.cjohnson30.com`
   iii. `tracert eff.org`

Reflection 1: Why do these tests work? Be specific.

Part 3: Connecting to HQ Network Resources

In this part, we'll connect to actual resources on the HQ network. Remember, in this scenario, we are in the office and connected to the HQ network directly.

We will be connecting to the following services from *laptop1*:

- RDP
- SSH
- Webpage

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 3 (Screenshot 4)
> 2. Step 5 (Screenshot 5)
> 3. Step 8 (Screenshot 6)
> 4. Step 10 (Screenshot 7)
> 5. Step 11 (Screenshot 8)

1. Power on `laptop1` and login.
2. Open the **Remote Desktop Connection** application.
3. Connect with to *srv1* with: `srv1.YourSenecaUsername.com`
4. If you see the Server1 desktop, congrats! Close the RDP connection.
5. Back on *laptop1*: Open an RDP connection directly to: `srv2.YourSenecaUsername.com`
6. If you see the Server2 desktop with the `sconfig` window, congrats! Close the RDP connection.
7. Open **Command Prompt** and login to *srv2*'s SSH connection: `ssh Administrator@srv2.YourSenecaUsername.com`
8. To confirm your work, run the following commands in your SSH session:

    i. `hostname`
    ii. `whoami`
9. Close the connection.
10. In Firefox, navigate to: `http://srv1.cjohnson30.com`
11. In Firefox, navigate to: `http://www.eff.org`

> **Reflection 2:** Why did these connections work? Be specific. What's happening when we connect to `srv2` based on our `tracert` output? What's happening when we connect to `eff.org`?

Investigation 3: Virtual Private Networking (VPN)

In this investigation, you will configure a VPN service on *srv1*. This will allow *laptop1* to log into the local HQ network over the Internet and access internal office resources like *srv2* from outside the office.

Before You Begin

Only the following VMs need to be turned on:

- *srv1*

Shut down the rest for now (including *laptop1*).

Check the following on *srv1* when online:

1. In **Network Connections**, all three adapters (*External Network*, *Internal Network*, and *vEthernet (HQ Network)*) have ***IPv6 disabled***.
2. At the VMware level, check the hardware settings for *srv1*:

    i. NIC1: **NAT** (Internet)
    ii. NIC2: **VMnet10** (local network)
3. DNS is running.
4. DHCP is running.
5. RRAS is running.

Part 1: Adding VPN to RRAS

Routing and Remote Access (RRAS) is a service you worked with in previous labs to set up NAT. It also offers VPN services, but our earlier setup didn't include it.

In many services, you can simply add a function or additional configuration. In others, like RRAS, you can't. We have to delete the configuration and start again. This isn't as daunting as it sounds! You aren't uninstalling the Server Feature; this is just reconfiguration within the RRAS tool.

Let's begin.

1. Open the **Routing and Remote Access** window. (*Server Manager application -> Tools -> Routing and Remote Access*)
2. Find your local server in the column list on the left (likely *SRV1-SENECAUSERNAME (local)*).
3. Right-click it and select **Disable Routing and Remote Access**.
    i. You will get a warning that this will remove its configuration. This is what we want. Select **Yes**.
    ii. This may take a few moments. Be patient.
4. Once complete, the left-hand column list should refresh, showing almost nothing aside from the server name. The server name will also have a **red status icon** next to it showing you it's disabled. (If the left-hand column list is unchanged, refresh the view.)

5. Right-click *SRV1* and select **Configure and Enable Routing and Remote Access**
6. You're brought back into the *Routing and Remote Access Server Setup Wizard* from earlier in the course.
7. Select **Next** on the first info page. You are now in the **Configuration** page.
8. In the **Configuration** page, select: *Custom configuration* and click **Next**.
9. In the **Custom Configuration** page, select the following options and click **Next**:
    i. VPN Access
    ii. NAT
    iii. LAN routing
10. The last page is the confirmation page. If the above selections show up in the display, click **Finish** to complete. (If not, hit the **Back** button and fix your selection. Feel free to ask for help!)
11. A popup window will appear asking if you'd like to start the service. **Select *Cancel***. We have more configuration to do before starting it up.

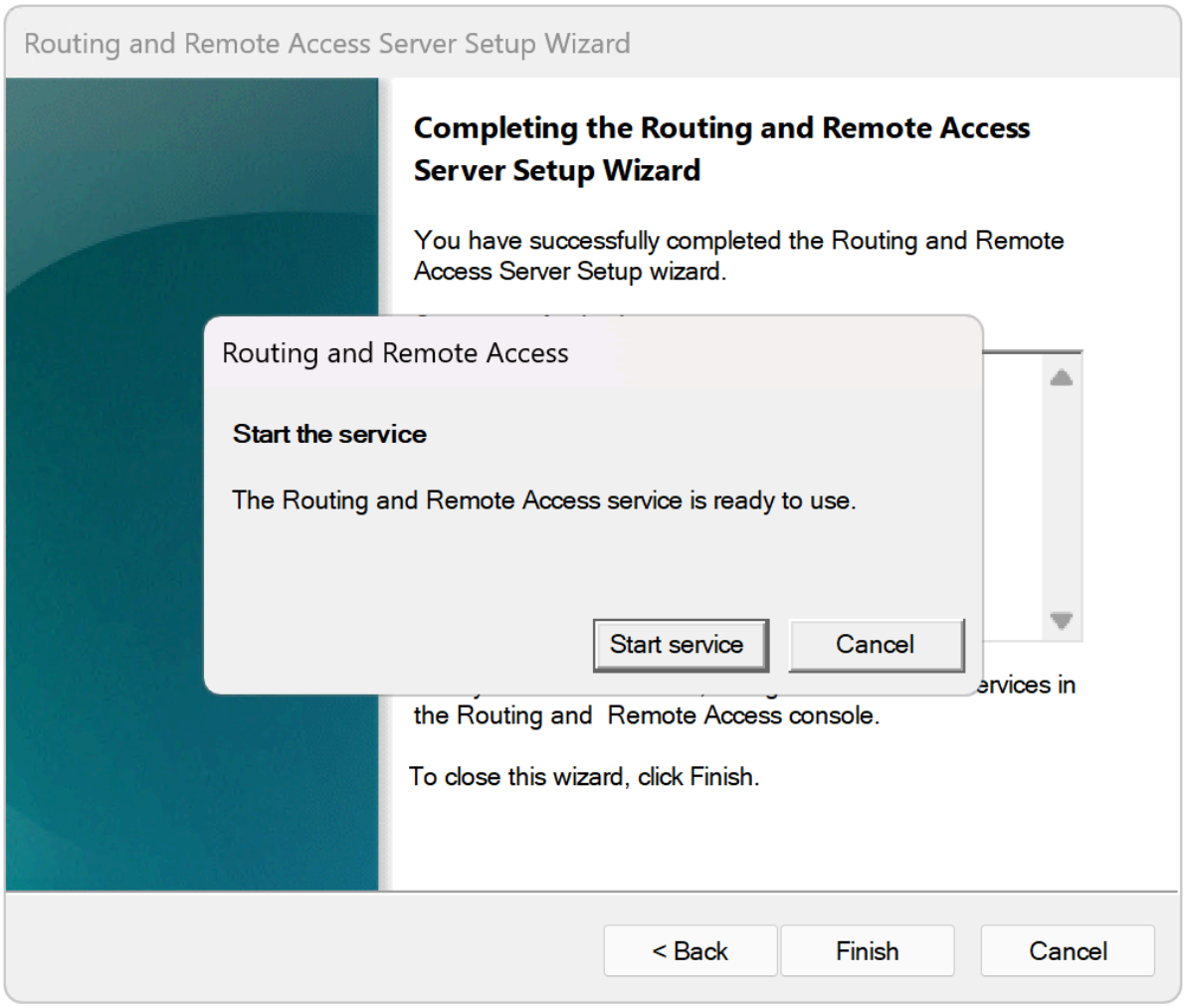


Figure 2. ***Select CANCEL on this screen!***

> **Note:** Keeping the RRAS server offline for now allows us to make additional changes without having to restart the service every time we make a change. This saves us a ton of time and frustration.

12. You should now see the familiar list of items in the left-hand menu column, with two new additions:
    i. Ports
    ii. Remote Access Clients
13. **Check:** The RRAS service should still be offline. Look for the red status icon over SRV1.

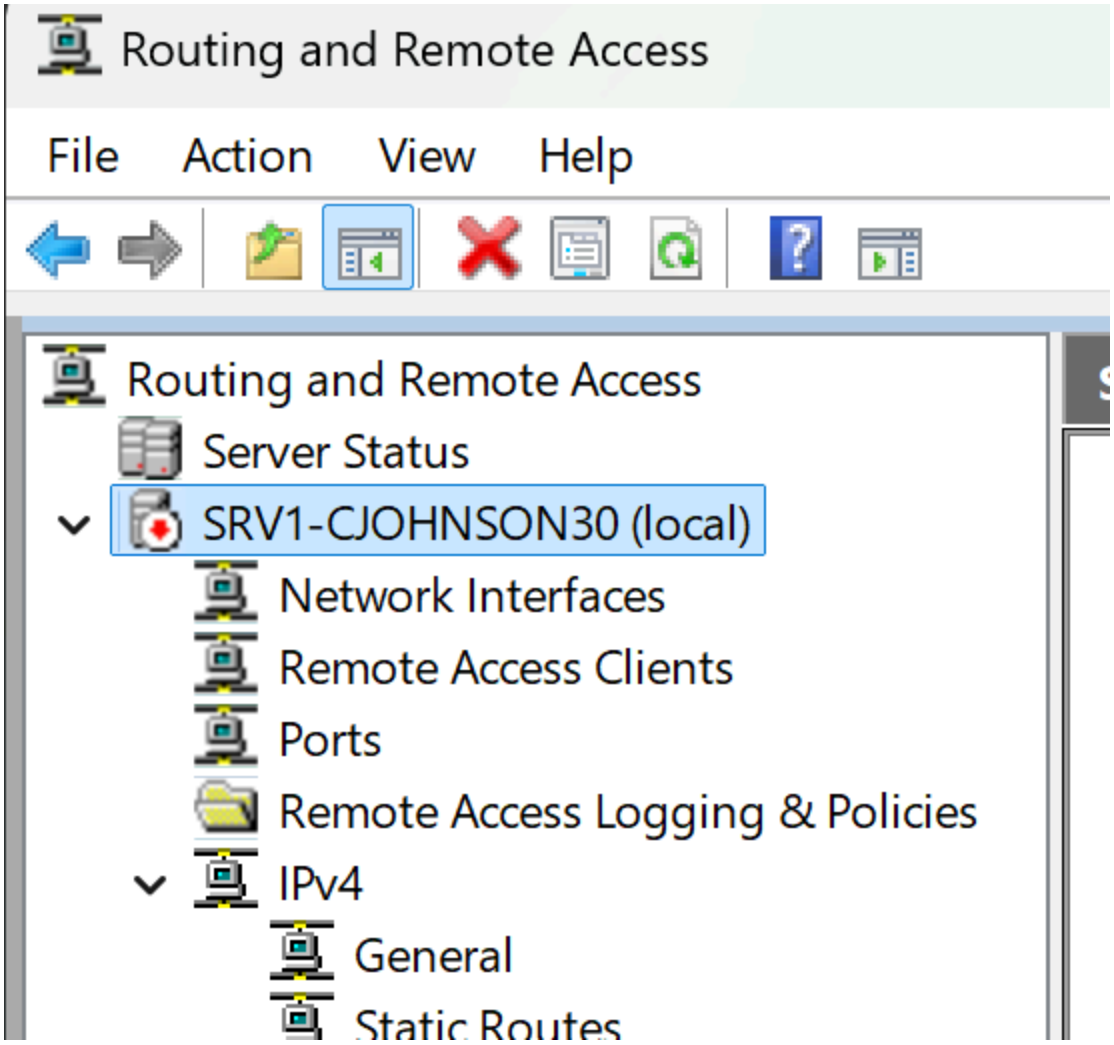


Figure 3. RRAS service offline with red status icon.

14. If the service is online (green), right-click it and go to: **All Tasks > Stop**

Part 2: Reconfiguring NAT

In this part, we'll reconfigure NAT to what we had set up before.

1. In the left-hand column, click on and expand the **IPv4** entry.
2. Click on **IPv4 -> NAT**.
3. Inside the NAT main window, right-click in the white space and select *New Interface*. Add the following:

    i. External Network -> Interface Type: Public interface connected to the Internet -> Enable NAT on this interface checked.
    ii. vEthernet (HQ Network) -> Interface Type: Private interface connected to private network

Part 3: Configuring the Server for IPv4 and Local Networks

In this part, we'll configure the RRAS service to only use IPv4 and to take network information from our vEthernet (HQ Network) where our DHCP and DNS live.

1. Back in the left-hand column, right-click on **SRV1** and select **Properties**.
2. In the *Properties* window, click on the **IPv6** tab.
3. Disable those pesky IPv6 options by ***unchecking*** the following:
    i. Enable IPv6 Forwarding
    ii. Enable Default Route Advertisement
4. Click in the **IPv4** tab.
5. Near the bottom of the tab, look for the *Adapter* entry and click on the drop-down menu.
    i. Select **vEthernet (HQ Network)**
6. Click **Apply** (not **OK**!). We have more work to do here.

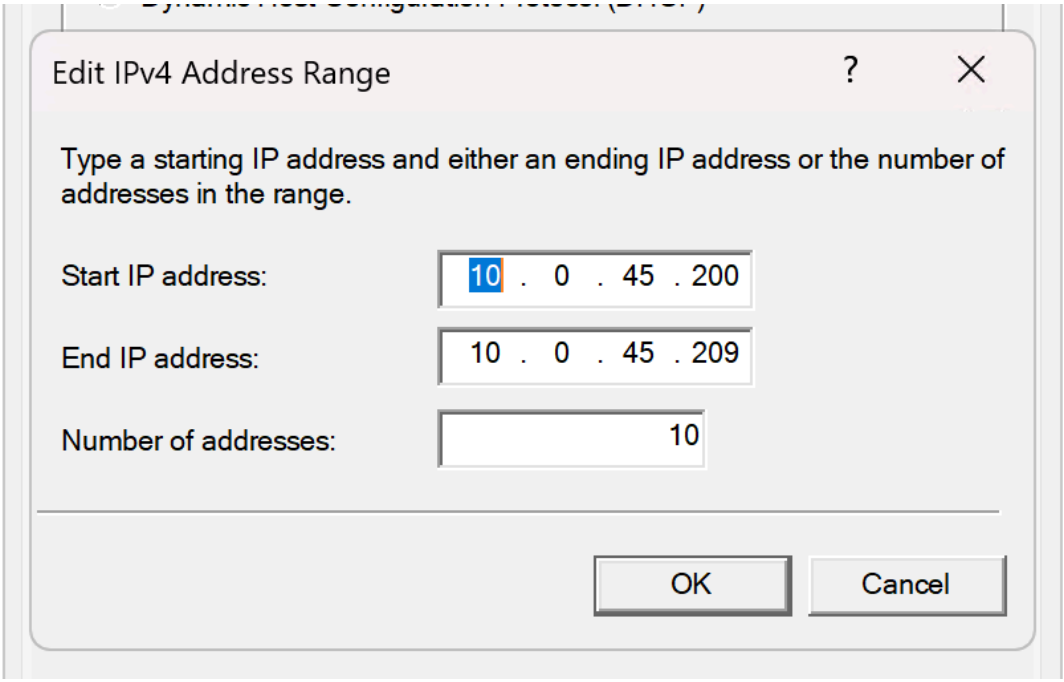
Part 4: Assigning IP Ranges for VPN Clients

In this part, we're going to assign IP addresses that the VPN can use. When a client (like *laptop1*) connects to the server using VPN, it'll be given an internal 10.0.`UID`.x address so it's part of the local network. That's how *laptop1* will be able to access internal network resources.

Remember in our DHCP lab where we specified that the DHCP could only use

10.0.`UID`.2-10.0.`UID`.199, even though we could have gone up to .254? That wasn't arbitrary! We'll use those remaining addresses here.

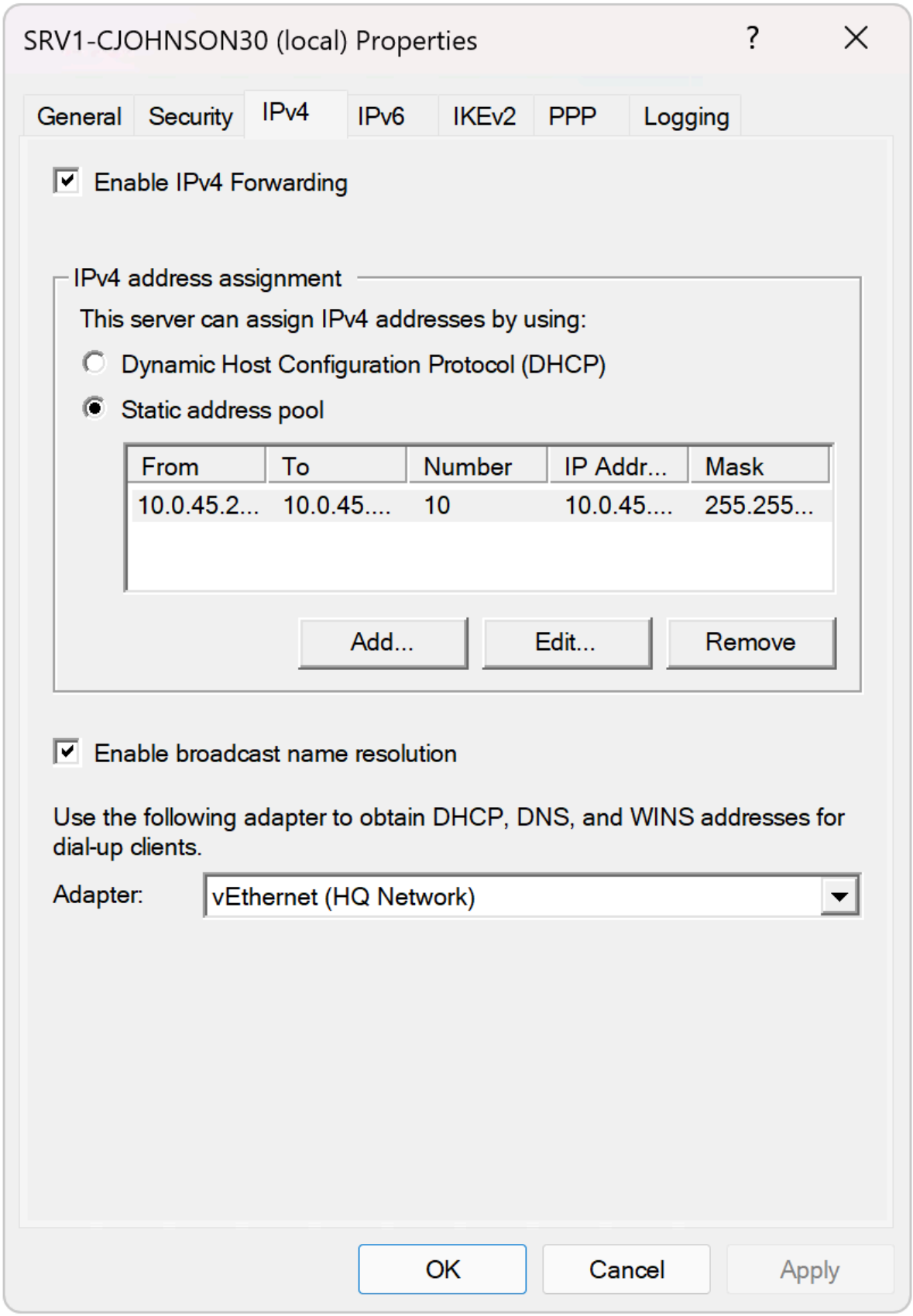
> **Screenshots:** Take screenshots of the following:
>
> 1. Step 2.v (Screenshot 9)

1. In RRAS, open the **Properties** window of *SRV1-SENECAUSERNAME (local)* and click on the **IPv4** tab. (If this is already open from *Part 3*, skip to Step 2.)
2. Look for the *IPv4 address assignment* section in this tab.
   i. Change the selection from **Dynamic Host Configuration Protocol (DHCP)** to **Static address pool**.
   ii. Below that, click the **Add** button.
   iii. The *New IPv4 Address Range* window pops up.
   iv. Enter the following:
      a. Start IP address: **10.0.`UID`.200**
      b. End IP address: **10.0.`UID`.209**
      c. 

d. This should give you **10** in the field below automatically. Click **OK**.

v. You should now see that IP address range in the *Static Address pool* table. (See *Figure 4* below.)

vi. Click **Apply** (not **OK**!). We have just a little more work to do here.


SRV1-CJOHNSON30 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Enable IPv4 Forwarding
IPv4 address assignment
This server can assign IPv4 addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From
To
Number
IP Addr...
Mask
10.0.45.2...
10.0.45....
10
10.0.45....
255.255...
Add...
Edit...
Remove
Enable broadcast name resolution
Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.
Adapter:
vEthernet (HQ Network)
OK
Cancel
Apply

> *Figure 4. Completed IPv4 tab.*

Part 5: VPN Security and Authentication

Here, we'll decide how clients (like *laptop1*) will authenticate to *srv1* when using VPN. These are security settings and must match on both the server and the client.

> **PROD NOTE:** We'll be using an older protocol called **L2TP** and a **Shared passphrase**. This is an older, deprecated setup with security flaws and should not be used in normal production environments! We're using it here in an educational environment for simplicity.
>
> In a production environment, we'd use certificate-based **IKEv2** instead of L2TP. It's more sophisticated, secure, and Microsoft recommended. We'll look at this briefly after Active Directory is installed in a later lab.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 6 (when all changes complete) (Screenshot 10)

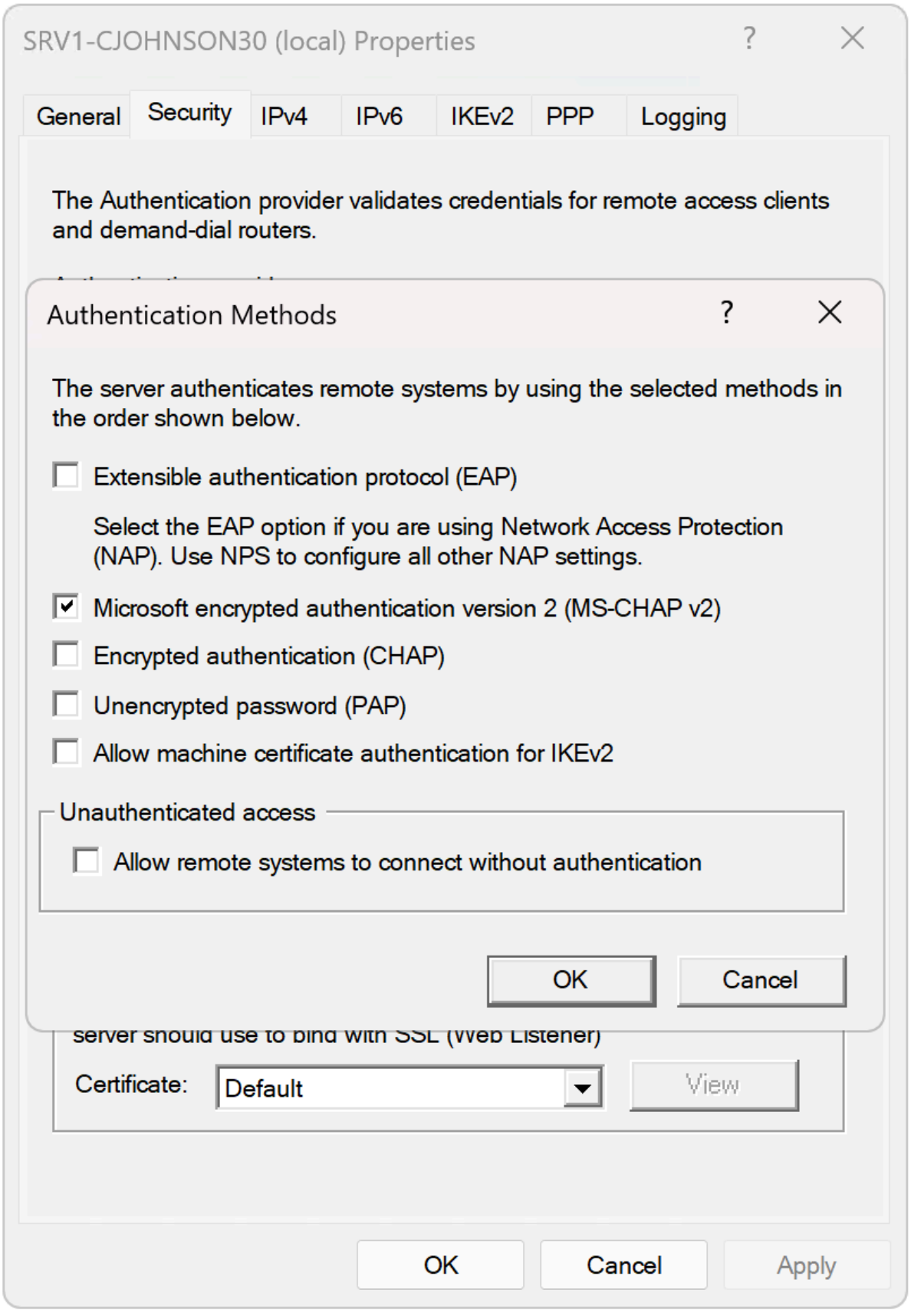
Let's begin our setup.

1. In RRAS, open the **Properties** window of *SRV1-SENECAUSERNAME (local)*. (If this is already open from *Part 3*, skip to Step 2.)
2. Change to the **Security** tab.
3. One of the first things you can see is *Authentication provider*. It's set to **Windows Authentication**. Leave it as is.
4. Just below that, there's a button labelled **Authentication Methods...**. Click it.
5. The *Authentication Methods* pop-up window appears. We're going to be changing a few settings here
6. Verify the following settings, and change the ones on your setup that don't

match the values below (Refer to *Figure 5* below):

i. Extensible authentication protocol (EAP): **Unchecked**
ii. Microsoft encrypted authentication version 2 (MS-CHAP v2): **Checked**
iii. Encrypted authentication (CHAP): **Unchecked**
iv. Unencrypted password: **Unchecked**
v. Allow machine certificate authentication for IKEv2: **Unchecked**
vi. Allow remote systems to connect without authentication: **Unchecked**

7. Click **OK** when done.
8. Click **OK** on the *Properties* **->** *Security* tab to close the window.


SRV1-CJOHNSON30 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication Methods
The server authenticates remote systems by using the selected methods in the order shown below.
Extensible authentication protocol (EAP)
Select the EAP option if you are using Network Access Protection (NAP). Use NPS to configure all other NAP settings.
Microsoft encrypted authentication version 2 (MS-CHAP v2)
Encrypted authentication (CHAP)
Unencrypted password (PAP)
Allow machine certificate authentication for IKEv2
Unauthenticated access
Allow remote systems to connect without authentication
OK
Cancel
server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply

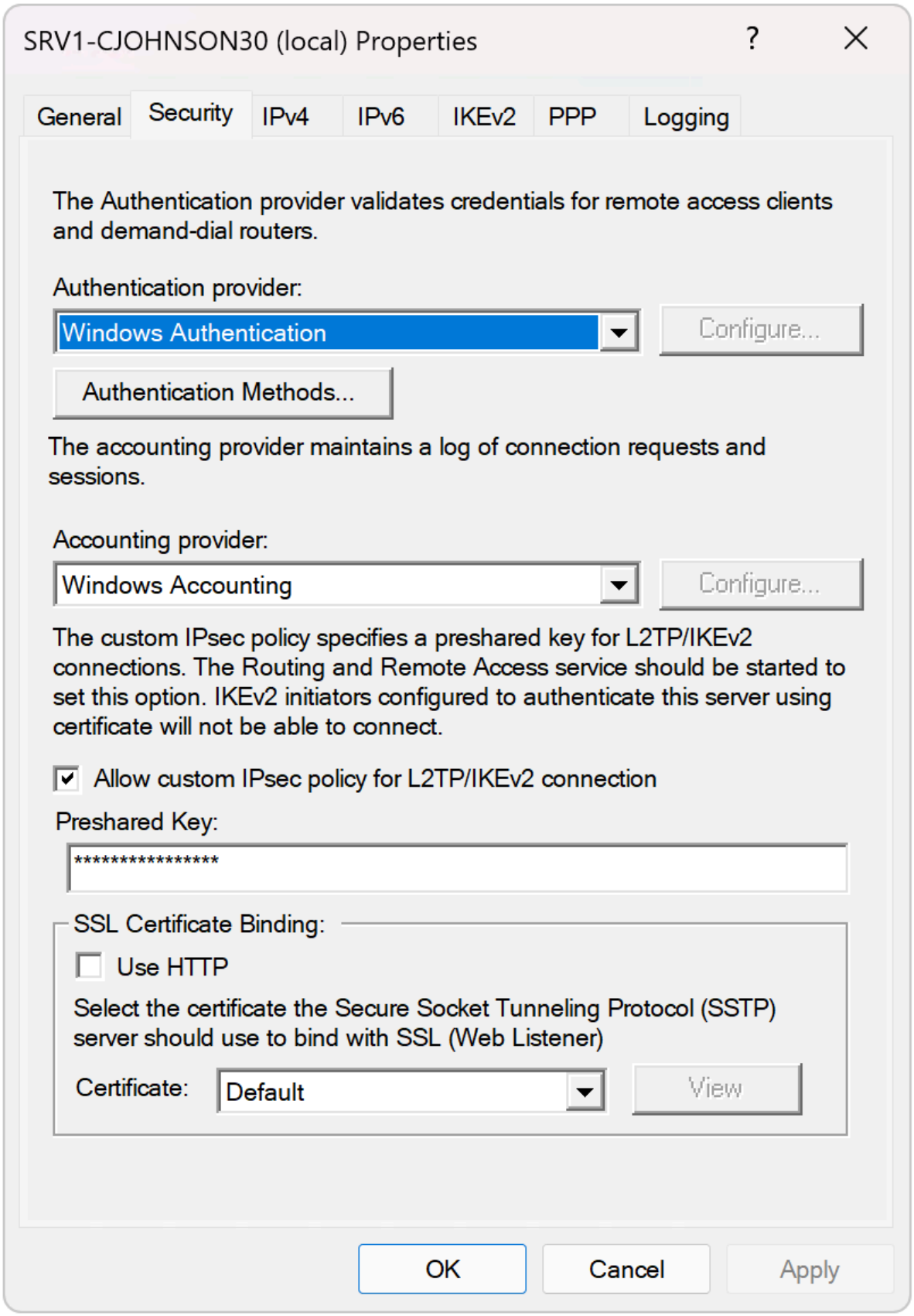
> *Figure 5. Properly selected authentication methods.*

Part 6: Starting up the RRAS service with VPN

In this part, we'll start up the RRAS service, check our VPN work, and make a small change to our VPN configuration we couldn't do until the service was running.

First, let's start up the RRAS service.

1. In RRAS, find the *SRV1-SENECAUSERNAME (local)* entry and right-click it.
2. In the drop-down context menu, click **All tasks**, then **Start**. This may take a few moments to start up.
3. When complete, the local server entry should now have a green icon.
4. Right-click *SRV1* again and select **Properties**.
5. In the **Security** tab, change the following:
    i. Allow custom IPsec policy for L2TP/IKEv2 connection: **Checked**
    ii. Preshared Key: **OSM620-2025F-L2TP-ONLY-DoNotReuse!**


SRV1-CJOHNSON30 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
Windows Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
Windows Accounting
Configure...
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.
Allow custom IPsec policy for L2TP/IKEv2 connection
Preshared Key:
****
SSL Certificate Binding:
Use HTTP
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply

> *Figure 6. Example of an entered Preshared Key value.*

6. Click **OK** to apply and close the window.
7. It may ask you to restart the service. Click **OK**.

Part 7: Creating Available Ports for VPN Connections

In this part, we'll create a pool of ports that can be used for individual VPN client connections. Each connection must have its own unshared port. These are recycled after disconnect.

In production environments, decisions have to be made from a business perspective at this point. How many people do we expect to be logging in to the VPN at any given time? We need to have enough ports available for that number, otherwise ports will run out and additional people won't be able to connect.

For us, we're going to stick with a demo number of 10 ports. **That means we will support 10 simultaneous active VPN client connections.** (If an 11th person tried to connect when 10 others were online, they'd get a connection error.)

> **IMPORTANT:** The RRAS service must be in a *Started* state (green icon)! Adding the ports below when the service is disabled will cause configuration damage that is very difficult to fix.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 8 (Screenshot 11)

Let's set this up.

1. In RRAS, verify that the service is online (look for the green icon.) If it isn't,

right-click and select: **All Tasks > Start**.

2. Find the *Ports* entry.
3. Right-click and select **Properties**.
4. The *Ports Properties* window appears.
5. We have some major changes to make here. To make changes, you'll click on one of the entries and then select the **Configure...** button. When you change the number of ports, a popup asking if you're sure will appear when you hit **OK**. Select **Yes**.
6. Verify the following settings, and change the *Number of ports* on your setup that don't match the values below:
    i. WAN Miniport (SSTP): **0**
    ii. WAN Miniport (IKEv2): **0**
    iii. WAN Miniport (PPTP): **0**
    iv. WAN Miniport (PPPoE): **1** (Though we don't need it, server will not let you set this to zero.)
    v. WAN Miniport (GRE): **0**
    vi. WAN Miniport (L2TP): **10**
        a. **Note:** Select *Remote access connections (inbound only)* in this window.
        b. **Note:** When you make this change, a popup will ask if you want to restart the RRAS server. Select **Yes**.
        c. **Your *srv1* computer will restart.** This is normal.
7. When you've finished restarting and logged back in, reopen the RRAS application.
8. In the main *Ports* window, the list in the main window should only contain the 10 L2TP ports (and 1 PPPoE).

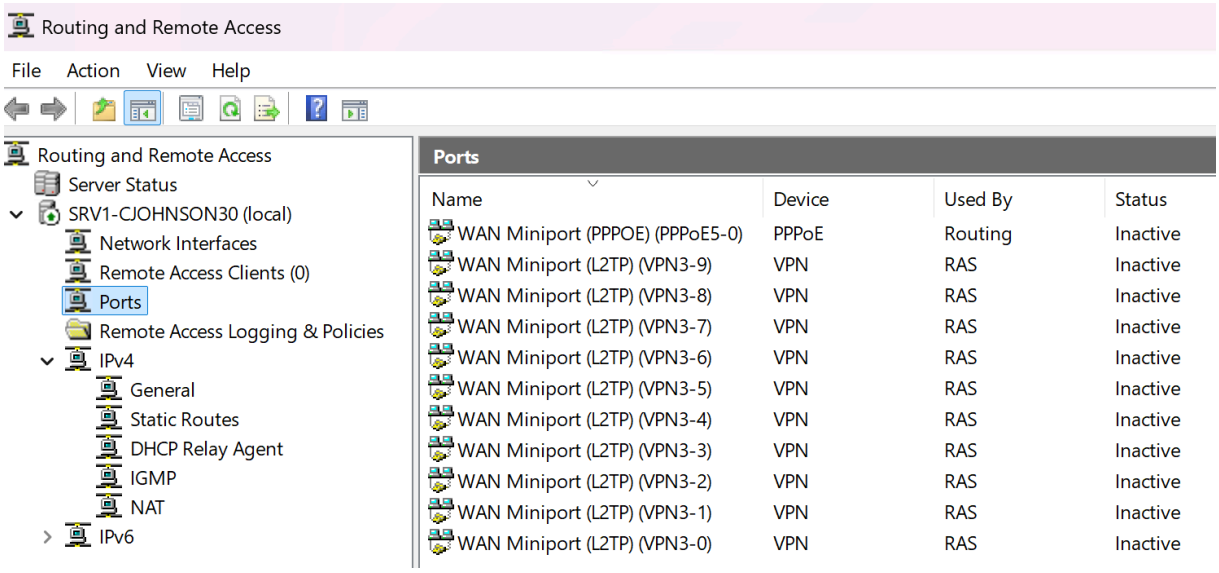


Figure 7. Completed L2TP ports listing.

Part 8: Network Policy Server

In this section, we'll open the **Network Policy Server** application and enable the profile that allows VPN authentication. This is an easy security task. This feature is installed by default through our previous lab work.

1. Open **Server Manager**.
2. Click *Tools -> Network Policy Server*
3. In the *Network Policy Server* application, use the left-hand column to go to **Policies > Network Policies**.
4. In the main window, find the policy entry listed as **Connections to Microsoft Routing and Remote Access Server**.

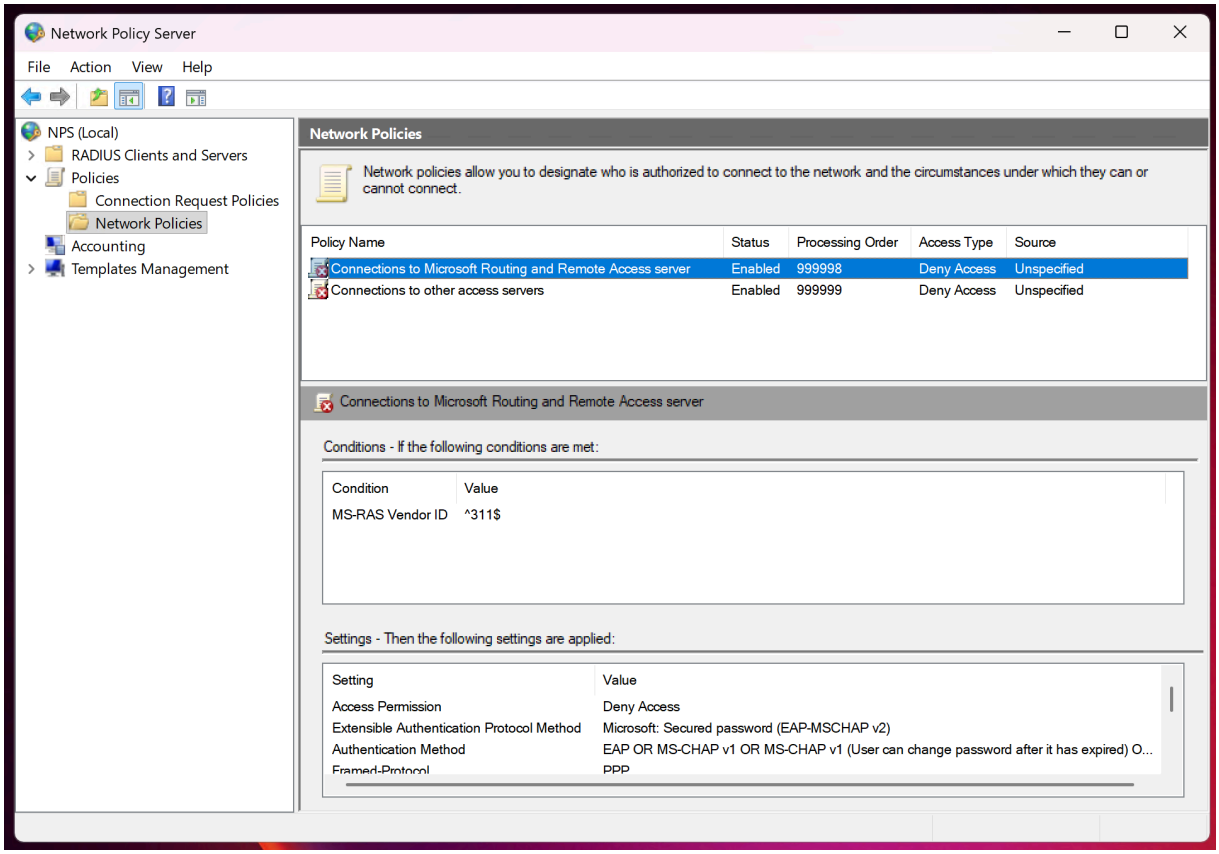


Figure 8. Network Policy Server application with the correct profile selected to edit.

5. Double-click this entry.
6. In the new *Properties* window, stay on the *Overview* tab.
7. Find the section on that tab labelled *Access Permission*.
8. Select: **Grant access. Grant access if the connection matches this policy.**

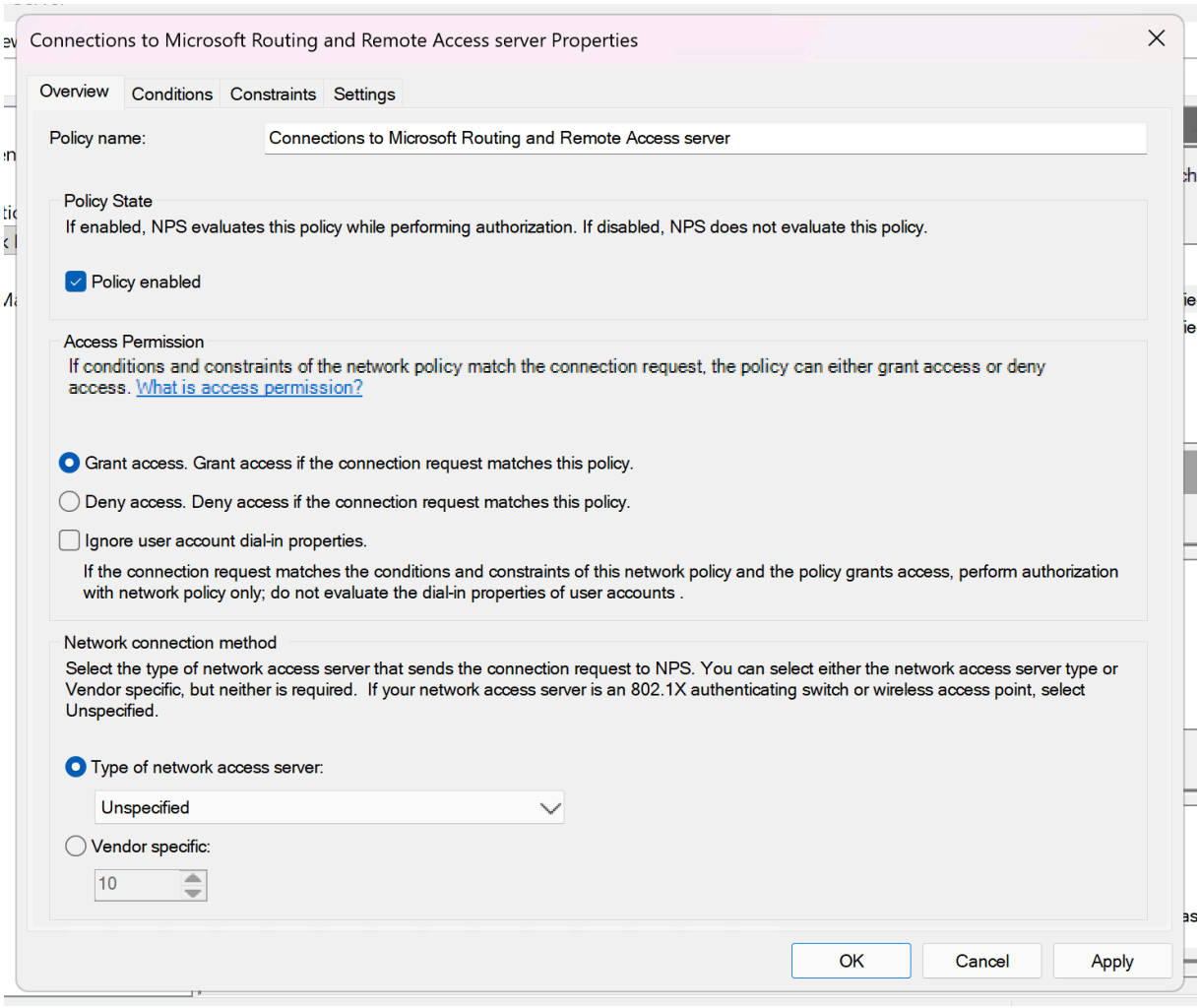


Figure 9. Granting access to the defined policy we're editing.

9. Click **OK** to apply and close the window.
10. The policy name in the main window should now have a green icon next to it.
11. You can now close the *Network Policy Server* application.

Part 9: Creating a Local User

Up to this point, you've been using the basic **Administrator** account. As the name implies, it has administrative privileges and can modify the system and access other users' files. The laptop we've set up is for a normal employee, not

someone on the admin team. Giving our normal employee admin access is a ***terrible*** security choice, so we won't!

For the employee to connect to *srv1*, we need to give them an account on that server. We'll create one for them below. It's a quick process. (There are other ways of creating VPN users, but this is easiest.) A new local account is, by default, not an admin.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 7 (Screenshot 12)

1. On *srv1*, open **Server Manager**.
2. Click *Tools -> Computer Management*
3. In the *Computer Management* application, use the left-hand column to go to **Local Users and Groups > Users**.
4. Right-click the *Users* folder and select **New User...**

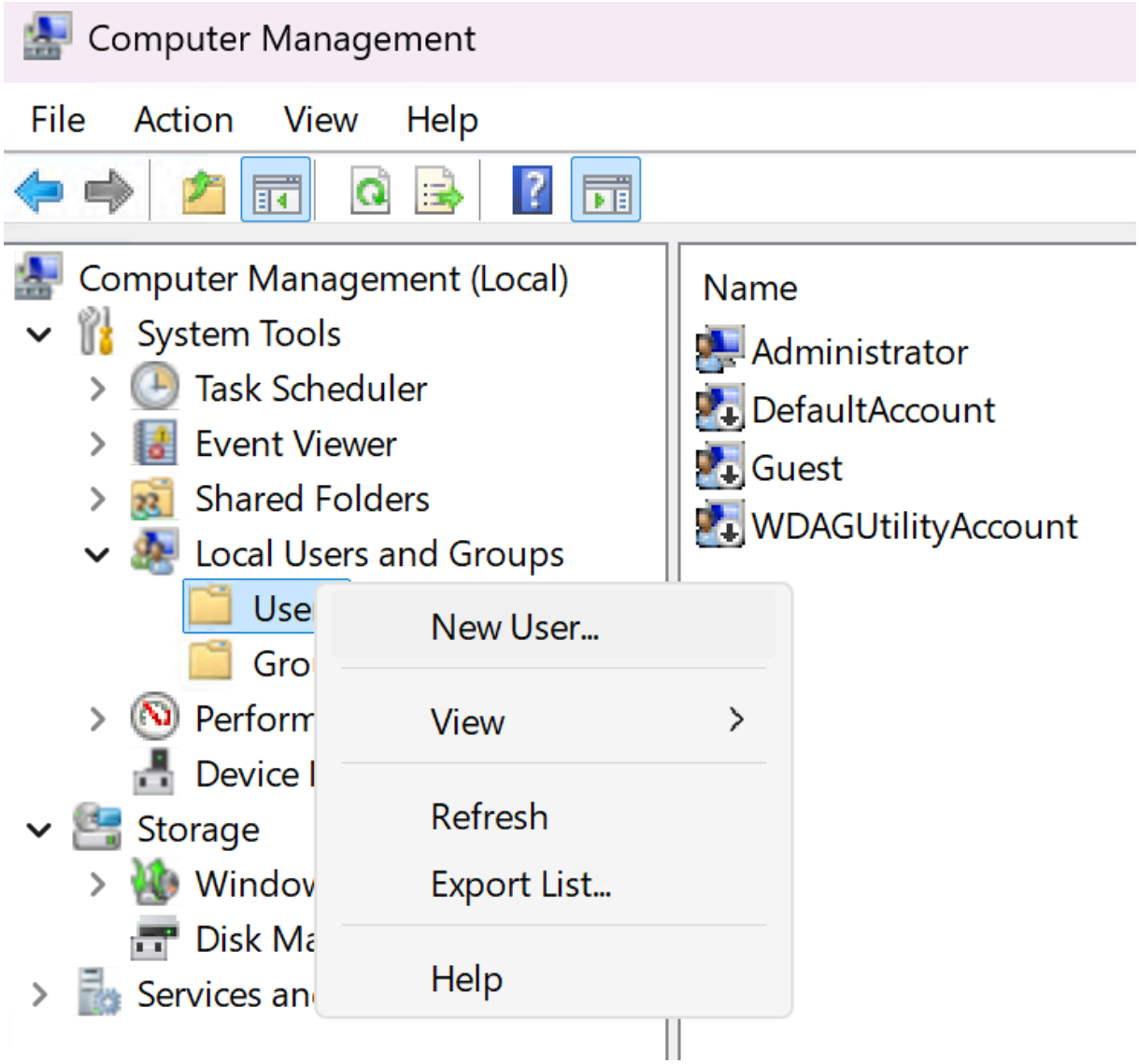


Figure 10. New User selection from context menu.

5. In the *New User* popup window, fill out the following values:
    i. User name: `firstname.lastname` (This is the same as you used for *laptop1*)
    ii. Full name: **Enter your full name** (Example: Chris Johnson)
    iii. Description: **VPN User**
    iv. Password: **Same as *laptop1***
    v. Confirm password: **Same as *laptop1***

vi. User must change password at next login: **Unchecked**

vii. User cannot change password: **Unchecked**

viii. Password never expires: **Checked**

ix. Account is disabled: **Unchecked**

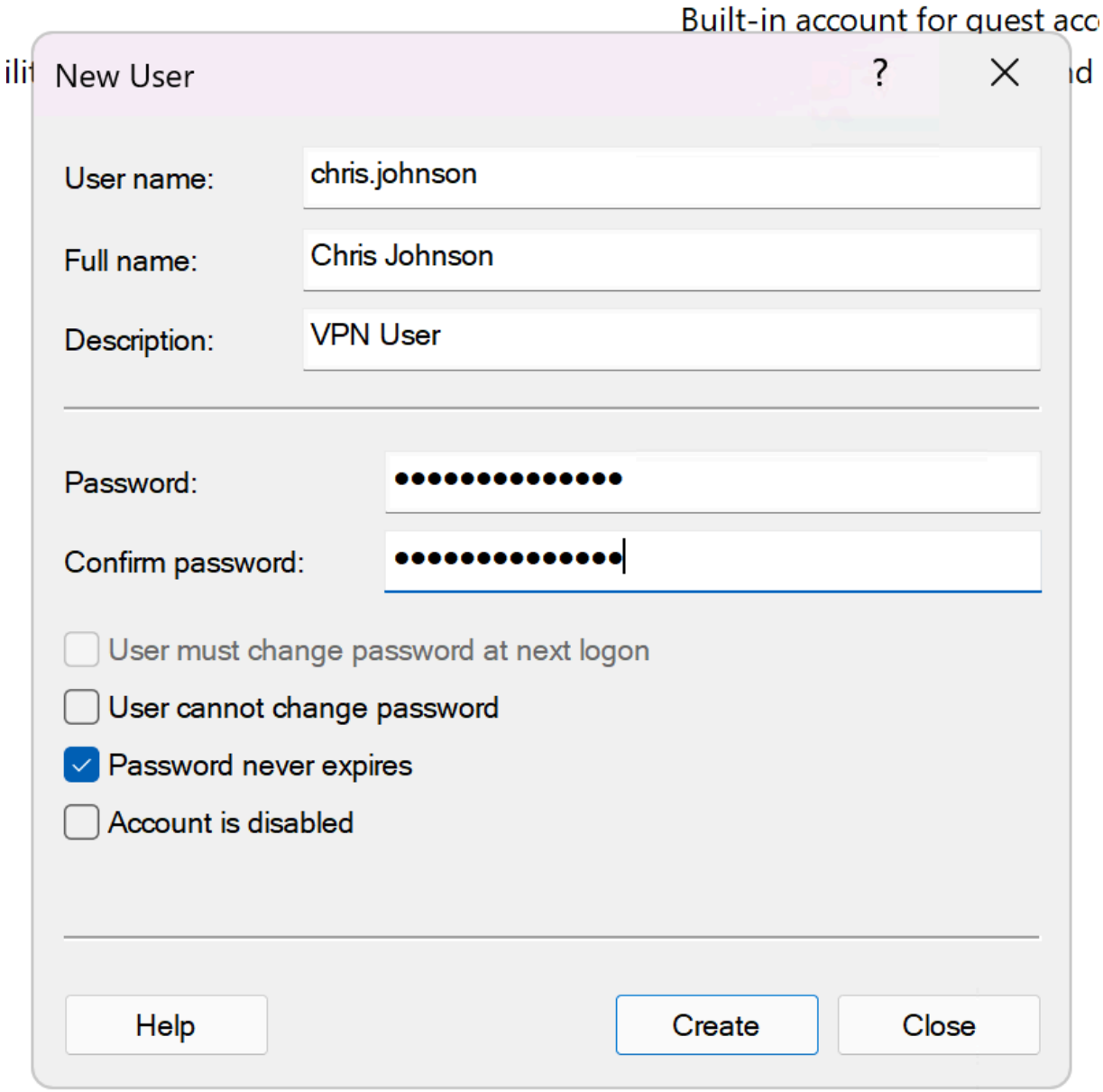


Figure 11. New User Dialog Box - Filled Out.

6. Confirm your settings are correct and click **Create**.

7. Confirm you can see your new user in the list. If so, move on to the next Investigation!

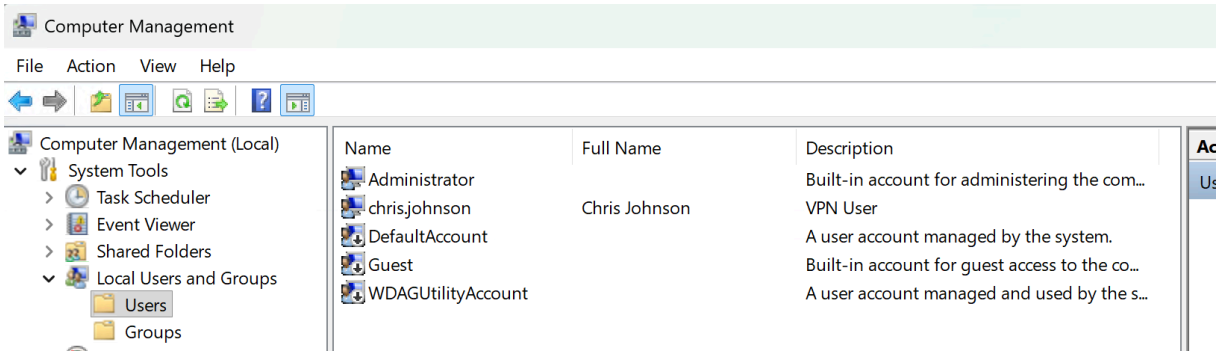


Figure 12. New user successfully added to list.

Investigation 4: Connecting to the VPN with *laptop1*

In this investigation, we will set up *laptop1* to connect to the VPN service we configured on *srv1*.

Scenario: Our new employee wants to connect to office resources from home. Let's make sure they can.

Before You Begin:

Turn on the following VMs:

- *srv1*
- *srv2*
- *laptop1*

> **IMPORTANT!** Check the following on *laptop1*:

> In **Network Connections**, the single adapter **Ethernet0** has ***IPv6 disabled***.

This should already be set from previous labs, but now is a good time to check. Missing this will break this investigation in interesting and very frustrating ways.

Part 1: Switching *laptop1*'s Network

Here, we'll emulate taking our new laptop home. This means removing it from the HQ network and putting it on NAT. Basically, giving it a standard Internet connection you'd get if you used it at home with your normal setup.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 2 (Screenshot 13)
> 2. Step 8 (Screenshot 14)

1. Turn on *laptop1*.
2. Once logged in, open Command Prompt and run: `ipconfig`
3. Observe the IP address and other network information. This will be important later.
4. In VMware Workstation, open *laptop1*'s Settings.
5. Find the **Network Adapter** and click on it.
6. Change the network selected from **VMnet10** to **NAT**.
7. Give it a few moments to apply the change.
8. Back inside *laptop1*, run the `ipconfig` command again.
9. Has the IP address changed from the 10.0.`UID`.x address? Good!

> **Reflection 3:** Why has the IP address changed and what does it mean for what *laptop1* can now access compared to *Investigation 2*?

Part 2: Testing Connections to Resources Under NAT

We will now check our ability to connect to several HQ network and Internet resources to see the difference between our on-premises (ie. in office) connection and a typical out-of-office Internet connection.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 3 (Screenshot 15)
> 2. Step 4 (Screenshot 16)

1. On *laptop1*, open *Command Prompt*.
2. Reset DNS cache: `ipconfig /flushdns`
3. Let's check DNS resolution. Run the following:
    i. `nslookup srv1.YourSenecaUsername.com`
    ii. `nslookup srv2.YourSenecaUsername.com`
    iii. `nslookup eff.org`
4. Now, let's check our connections to these resources:
    i. `ping srv1.cjohnson30.com`
    ii. `ping srv2.cjohnson30.com`
    iii. `ping eff.org`

> **Reflection 4:** Why can't you connect to certain things but can connect to others?

Part 3: Creating the FQDN: vpn.`YourSenecaUsername`.com

In this part, we'll create a local entry on *laptop1* that points a new FQDN (URL),

vpn.`YourSenecaUsername`.com to *srv1*. **This is necessary for our VPN connection in *Part 3*.**

Why are we doing this?

Normally, in a production or corporate environment, we'd have a registered domain name that works on the Internet. So, an address like `vpn.cjohnson30.com` would point to our *srv1*'s External Network NIC. This is the one that has an IP address that allows Internet connections, so it can be reached through the Internet from anywhere.

We don't have a purchased domain name like `cjohnson30.com`. We're doing everything local. So, we have to cheat a little.

We trick *laptop1* into thinking `vpn.YourSenecaUsername.com` is a valid Internet address.

> **PROD NOTE**: This is only done in lab testing environments! Never do this on production.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 9 (Screenshot 17)

Let's trick *laptop1*:

1. First, on *srv1*: Open *Command Prompt* and run: `ipconfig`
    i. Write down the IP address of the **External Network**. We'll need this shortly.
2. Over on *laptop1*: Open the folder: `C:\Windows\System32\drivers\etc`
3. There are several files here, including one called: `hosts`

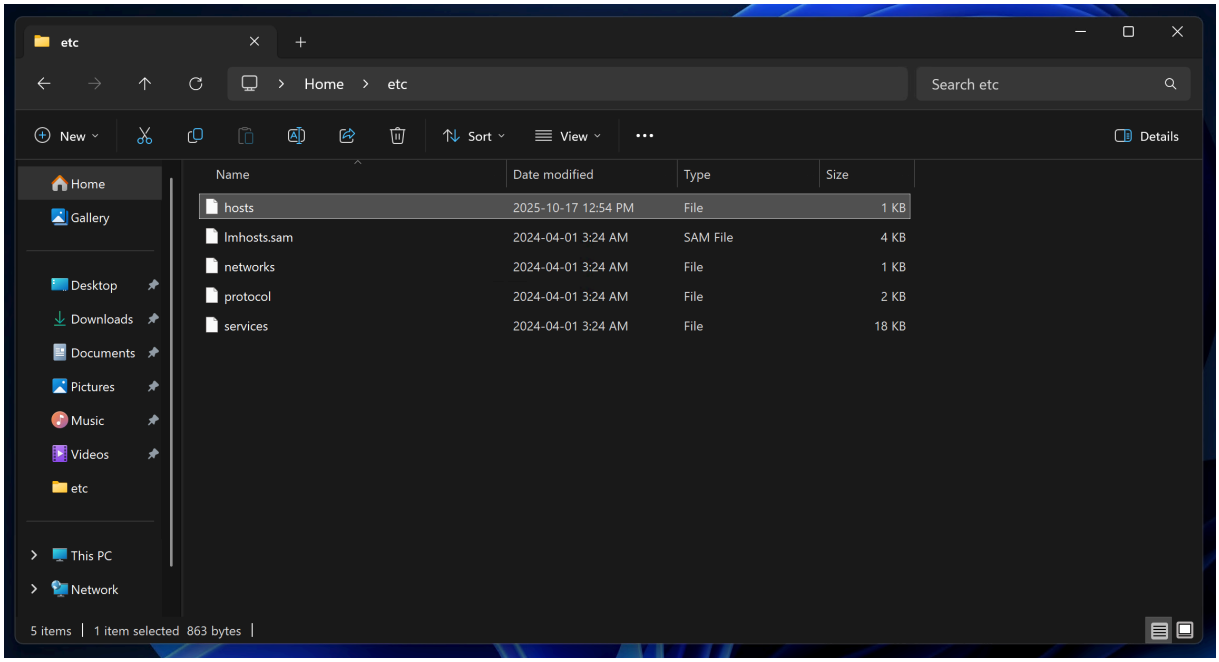


Figure 13. List of files in: C:\Windows\System32\drivers\etc

4. Copy the `hosts` file to your *laptop1* desktop.
5. Double-click it to open it. The system will ask you what application to use. Choose **Notepad**.
6. At the very bottom of the text document, add the following line (and change it according to your setup!):
    i. *srv1 External Network IP address* vpn.`YourSenecaUsername`.com

    > **Example:** `192.168.122.105 vpn.cjohnson30.com`

Figure 14. Example VPN entry in hosts file.

7. Save this file. When the dialog box comes up asking for a name, use this:
   i. `"hosts"`
   ii. **Those double-quotes are necessary.** This ensures it doesn't add *.txt* to the end.
8. Copy the file back to: `C:\Windows\System32\drivers\etc`
9. Check your work by opening *Command Prompt* and running the following command: `ping vpn.YourSenecaUsername.com`
10. If you received a response pointing for your *srv1* external IP address, congrats! Move to **Part 4**.

Part 4: Configuring a VPN Connection on

laptop1

In this part, we'll use our *laptop1* client VM to connect to the VPN on *srv1*. This involves creating a VPN profile and then connecting.

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 3 (completed) (Screenshot 18)
> 2. Step 7 (Screenshot 19)

1. On *laptop1*, open: *Settings* > *Network & internet* > *VPN*
2. Click on **Add VPN**
3. Use the following settings:
    i. VPN Provider: **Windows (built-in)**
    ii. Connection name: **SRV1 VPN**
    iii. Server name or address: **vpn.YourSenecaUsername.com** (replace with *your* domain)
    iv. VPN type: **L2TP/IPsec with pre-shared key**
    v. Pre-shared key: **OSM620-2025F-L2TP-ONLY-DoNotReuse!**
    vi. Type of sign-in info: **Username and password**
    vii. Username: `firstname.lastname`
    viii. Password: `password you used for the above account on srv1`
    ix. Remember my sign-in info: **Checked**

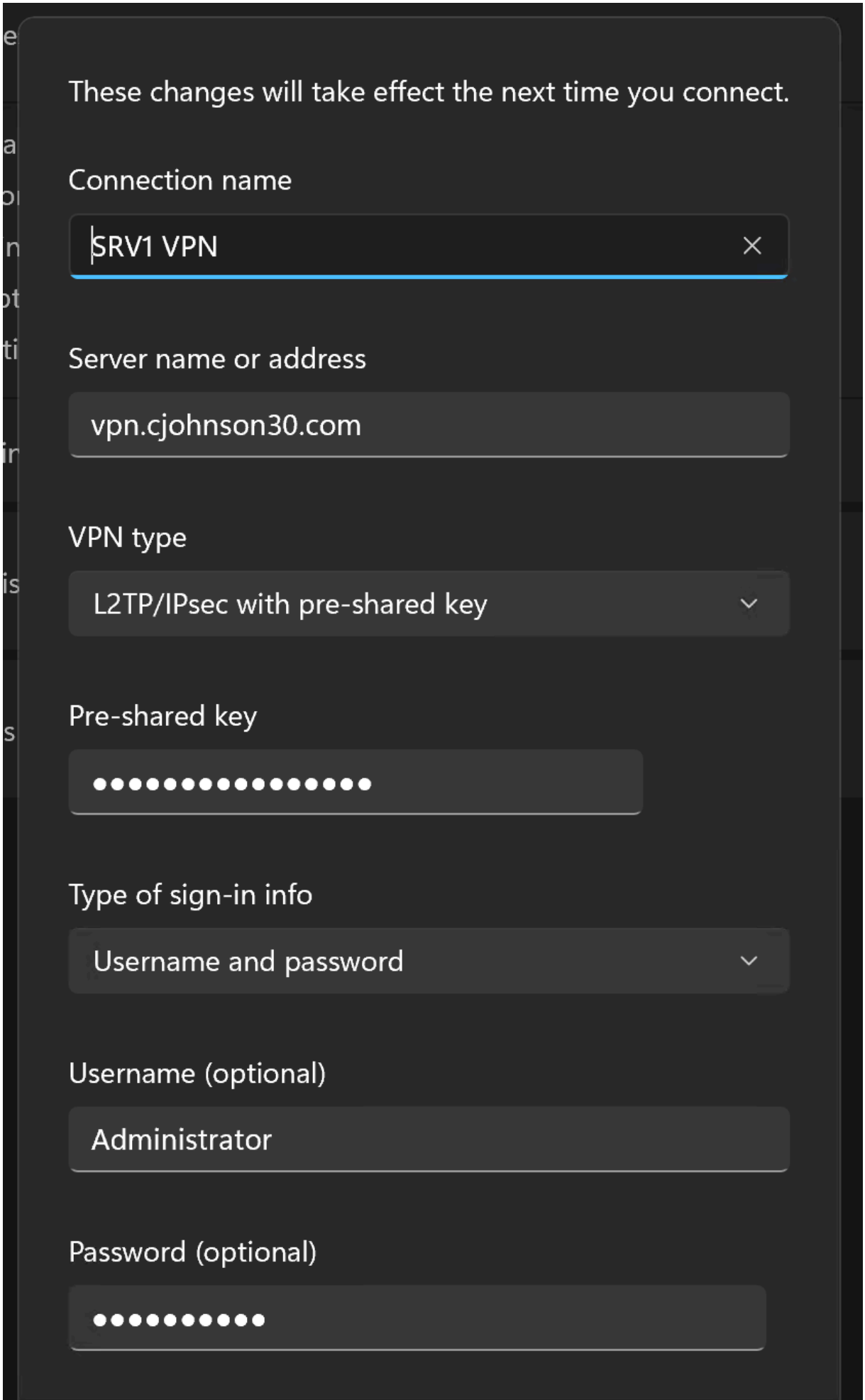

These changes will take effect the next time you connect.
Connection name
SRV1 VPN
Server name or address
vpn.cjohnson30.com
VPN type
L2TP/IPsec with pre-shared key
Pre-shared key
Type of sign-in info
Username and password
Username (optional)
Administrator
Password (optional)

Figure 15. Example of filled out VPN client information.

4. Double-check the above information, then click **Save**.
5. Back in the *VPN* window, a new entry has appeared: **SRV1 VPN**
6. Click the **Connect** button.
7. After a few moments, it should say *Connected*.

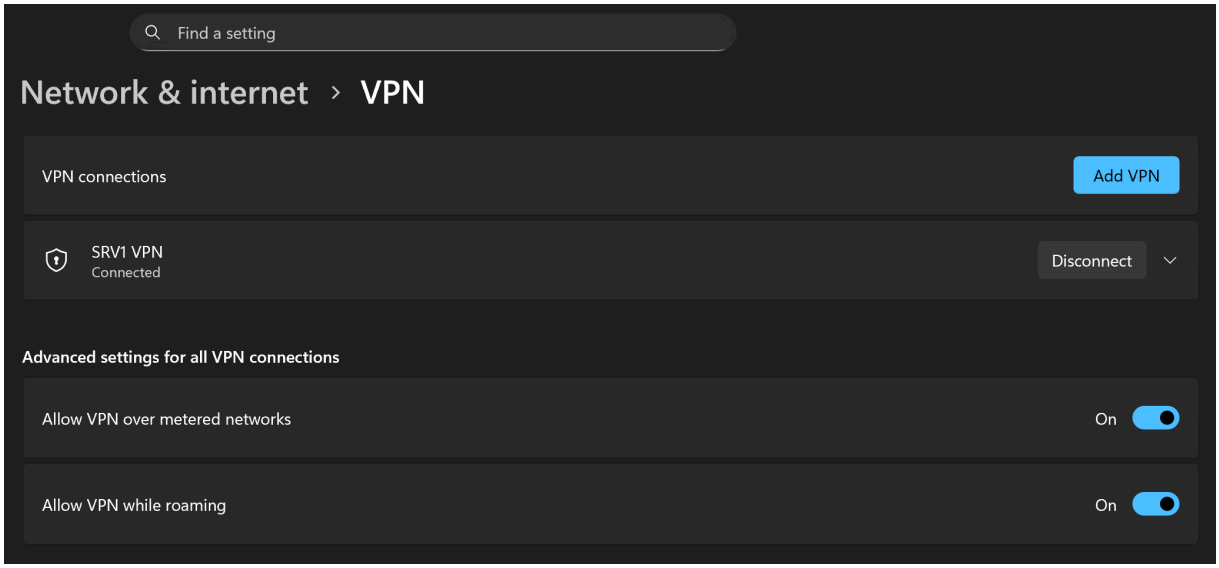


Figure 16. VPN connected.

8. If not, review your previous settings and/or ask for help.
9. Check your work once more by opening *Command Prompt* and running: `ipconfig`

> **Reflection 5:** What do you notice that's different? Why do you think this is? What might this mean?

Part 5: Testing Connections to HQ Network Resources

This is the fun part. Let's test our connection to HQ network resources, things that *aren't* accessible through a normal Internet connection.

> **Screenshots:** Take screenshots of the following:

> 1. Step 3 (Screenshot 20)
> 2. Step 4 (Screenshot 21)
> 3. Step 5 (Screenshot 22)

1. On *laptop1*, open *Command Prompt*.
2. Reset DNS cache: `ipconfig /flushdns`
3. Let's check DNS resolution. Run the following:
    i. `nslookup srv1.YourSenecaUsername.com`
    ii. `nslookup srv2.YourSenecaUsername.com`
    iii. `nslookup eff.org`
4. Now, let's confirm we have connections to these resources:
    i. `ping srv1.cjohnson30.com`
    ii. `ping srv2.cjohnson30.com`
    iii. `ping eff.org`
5. Finally, let's take a look at the **path through the network** that our connection to these resources is taking:
    i. `tracert srv1.cjohnson30.com`
    ii. `tracert srv2.cjohnson30.com`
    iii. `tracert eff.org`

These should all work! If they don't, start troubleshooting.

> **Reflection 6:** How are these results different from when you ran them in *Investigation 2*? How are they not? How are these results different from when you ran them in *Part 2* above? ***Why?***

Part 6: Connecting to HQ Network Resources

In this final part, we'll connect to actual resources on the HQ network through the VPN. Remember, in this scenario, we are at home and not on the HQ network directly.

We will be connecting to the following services from *laptop1*:

- RDP
- SSH
- IIS (Website)

> **Screenshots:** Take screenshots of the following:
>
> 1. Step 3 (Screenshot 23)
> 2. Step 5 (Screenshot 24)
> 3. Step 8 (Screenshot 25)
> 4. Step 10 (Screenshot 26)
> 5. Step 11 (Screenshot 27)

1. On *laptop1*, connect to the SRV1 VPN. (If you already are, skip to *Step 2*.)
2. Open the **Remote Desktop Connection** application.
3. Connect to *srv1* with: `srv1.YourSenecaUsername.com`
4. If you see the Server1 desktop, congrats! Close the RDP connection.
5. Back on *laptop1*, open an RDP connection directly to: `srv2.YourSenecaUsername.com`
6. If you see the Server2 desktop with the `sconfig` window, congrats! Close the RDP connection.
7. Open **Command Prompt** and login to *srv2*'s SSH connection: `ssh Administrator@srv2.YourSenecaUsername.com`
8. To confirm your work, run the following commands in your SSH session:
    i. `hostname`
    ii. `whoami`
9. Close the connection.
10. Open Firefox and navigate to: `http://srv1.YourSenecaUsername.com`
11. Open Firefox and navigate to: `http://www.eff.org`
12. Now, disconnect from the VPN and re-run the RDP, SSH connections and

Firefox steps.

> **Reflection 7:** Why did these connections only work while the VPN was running? What still works with the VPN off? What's happening when the VPN is connected? *Hint: Think about the* `ipconfig` *and* `tracert` *results you saw earlier.*

Submission

Submission for assignments is a bit different from labs. Instead of live checks, you will be submitting a **report**.

You will submit to Blackboard with a single PDF document that includes the following:

1. Title page that includes:
    i. Full name
    ii. Student ID Number
    iii. Course code and section
    iv. Calendar Semester (Fall 2025)
    v. Date
2. For each Investigation:
    i. The requested screenshots.
    ii. The reflection questions and your answers to each.
    iii. Each Investigation should start on a new page, and screenshots/ reflection answers should be placed in the appropriate Investigation pages.
    iv. Number your pages!

Export to PDF from your editor with images embedded. **No external links!**

Assignment 2

To be released on Week 9.