

CompTIA Server+

Server Network Infrastructure Configuration

- Introduction
 - Lab Topology
 - Exercise 1 - Configure Various Network Settings on Windows Server 2019
 - Review
-

Introduction

Server+

Virtual Local Area Network (VLAN)

Default Gateways

Firewall

MAC Addresses

IP Configuration

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

For a server or any other computer system to interact with other systems on the network, it needs to be properly configured to work on the network it is being joined to. Depending on the use case of the server, the system might be configured to use a static IP address. Certain applications that may be installed on the server could require that specific firewall ports be opened. These are just a couple of considerations that the server administrator might have to take into account to adjust the server's network configuration to meet the needs of the business.

In this module, the configuration of network settings on Windows Server 2019 will be explored.

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Configure Various Network Settings on Windows Server 2019

After completing this module, you should be able to:

- Identify the Network Configurations of a Server

Exam Objectives

The following exam objectives are covered in this module:

2.2 Given a scenario, configure servers to use network infrastructure services

- IP configuration
- Virtual local area network (VLAN)
- Default gateways
- Name resolution
- Addressing protocols
- Firewall
- MAC addresses

Lab Duration

It will take approximately **1 hour** to complete this lab.

Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click **Next** to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.

Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01** - (Windows Server 2019 - Domain Controller)
- **PLABDM01** - (Windows Server 2022 - Domain Member Server)

- **PLABWIN10** - (Windows 10 - Domain Member Workstation)
- **PLABALMA** - (Alma Linux 8.7 - Stand-alone Linux Workstation)
- **PLABUBUNTU** - (Linux Ubuntu - Stand-alone Linux Server)

Click **Next** to proceed to the first exercise.

Exercise 1 - Configure Various Network Settings on Windows Server 2019

In this exercise, the configuration of network settings within Windows Server 2019 will be explored.

Learning Outcomes

After completing this exercise, you should be able to:

- Identify the Network Configurations of a Server

Your Devices

You will be using the following device in this lab. Please power this on now.

- **PLABDC01** - (Windows Server 2019 - Domain Controller)

Task 1 - Identify the Network Configurations of a Server

In this task, you will learn about the different types of network settings that can be configured on a server.

Step 1

Connect to **PLABDC01**.

Minimize the **Server Manager** window.

Click the **Start** charm and type the following:

command prompt

Select **Command Prompt** from the **Best match** pop-up menu.

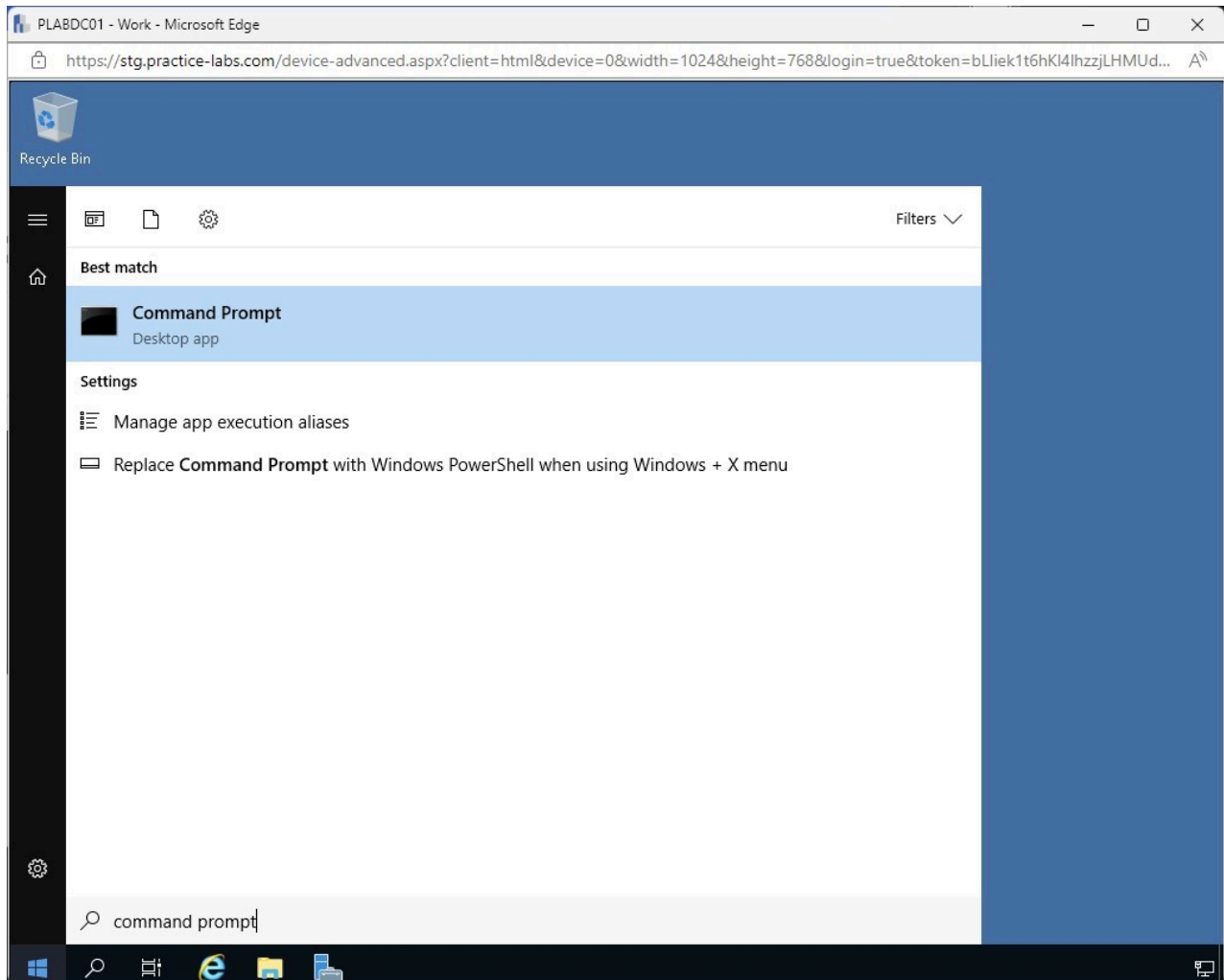


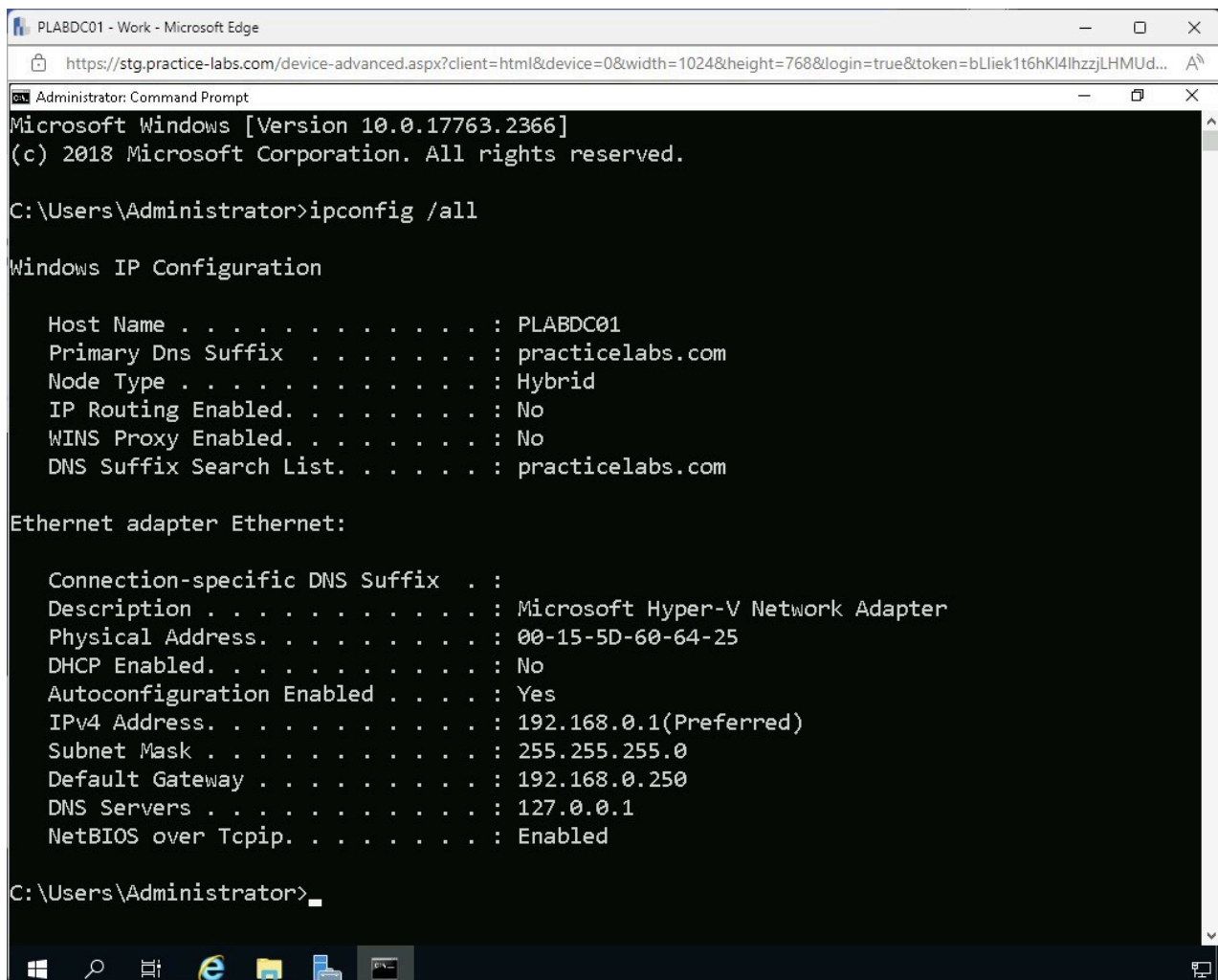
Figure 1.1 Screenshot of PLABDC01: Displaying selecting Command Prompt from the Best match menu.

Step 2

In the **Command Prompt** window, type the following:

ipconfig /all

Press **Enter**.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PLABDC01
    Primary Dns Suffix . . . . . : practicelabs.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : practicelabs.com

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Hyper-V Network Adapter
    Physical Address. . . . . : 00-15-5D-60-64-25
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.0.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.250
    DNS Servers . . . . . : 127.0.0.1
    NetBIOS over Tcpip. . . . . : Enabled

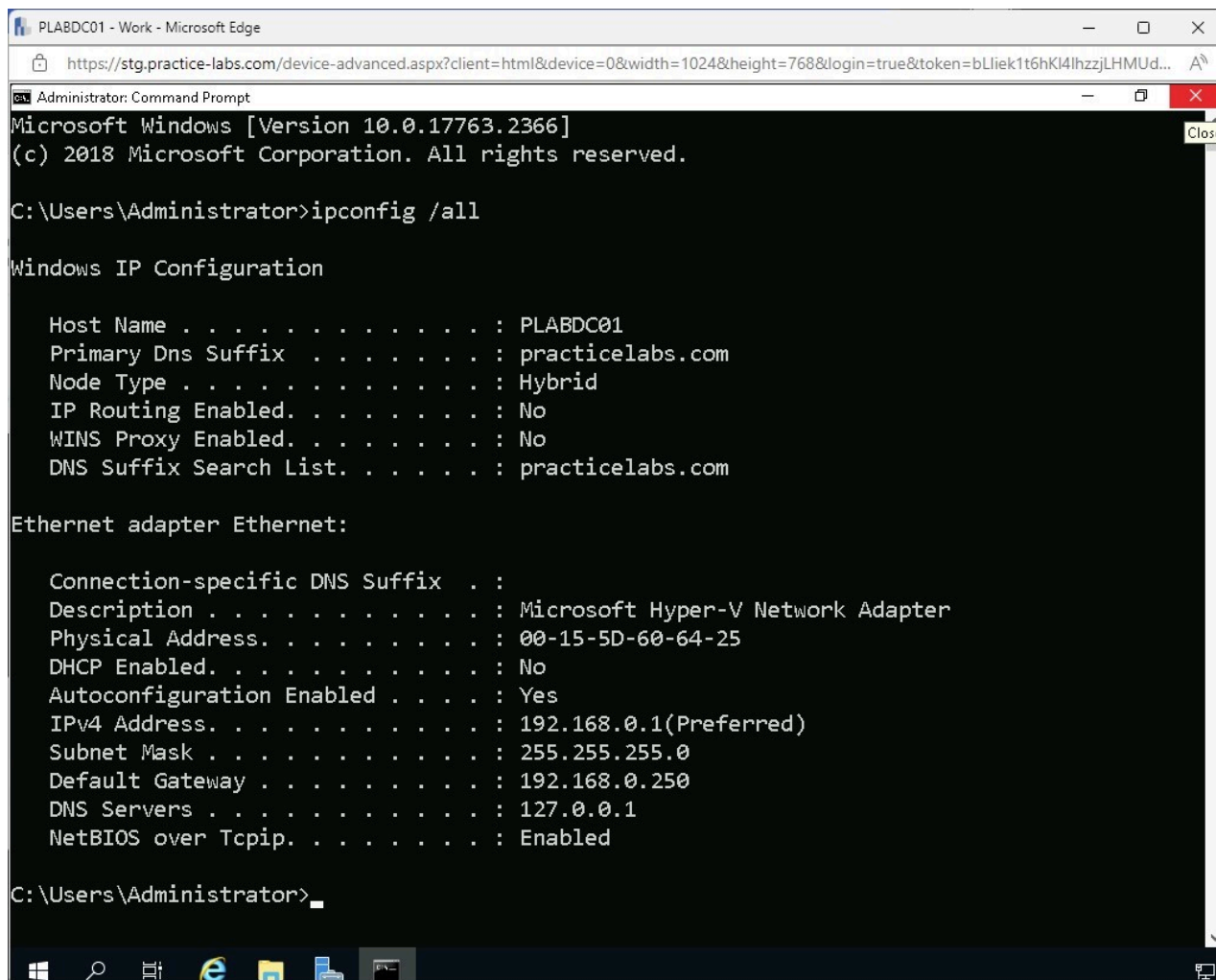
C:\Users\Administrator>
```

Figure 1.2 Screenshot of PLABDC01: Displaying the Command Prompt window with the ipconfig command entered and executed.

- Note:** The results displayed in this window provide you with the following information:
- The Host Name is listed as **PLABDC01**.
 - The Primary DNS Suffix shows that the system is joined to the **practicelabs.com** domain. Combining this information with the hostname, you can determine that this system's Fully Qualified Domain Name (FQDN) is **PLABDC01.practicelabs.com**. FQDN is the hostname followed by the domain name that the host is joined to.
 - The Physical Address is specified as **00-15-5D-60-64-79**. This is the unique identifier of hexadecimal digits that is associated with the physical network adapter. The physical address never changes but can be manually modified on virtual devices. The physical address is commonly referred to as the **MAC Address**.
 - IP address details.

Step 3

Close the **Command Prompt** window.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PLABDC01
    Primary Dns Suffix . . . . . : practicelabs.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : practicelabs.com

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Hyper-V Network Adapter
    Physical Address. . . . . : 00-15-5D-60-64-25
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . : Yes
    IPv4 Address. . . . . : 192.168.0.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.250
    DNS Servers . . . . . : 127.0.0.1
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

Figure 1.3 Screenshot of PLABDC01: Displaying closing the Command Prompt window.

Step 4

Click the **Start** charm and select **Control Panel** from the Quick Access section.

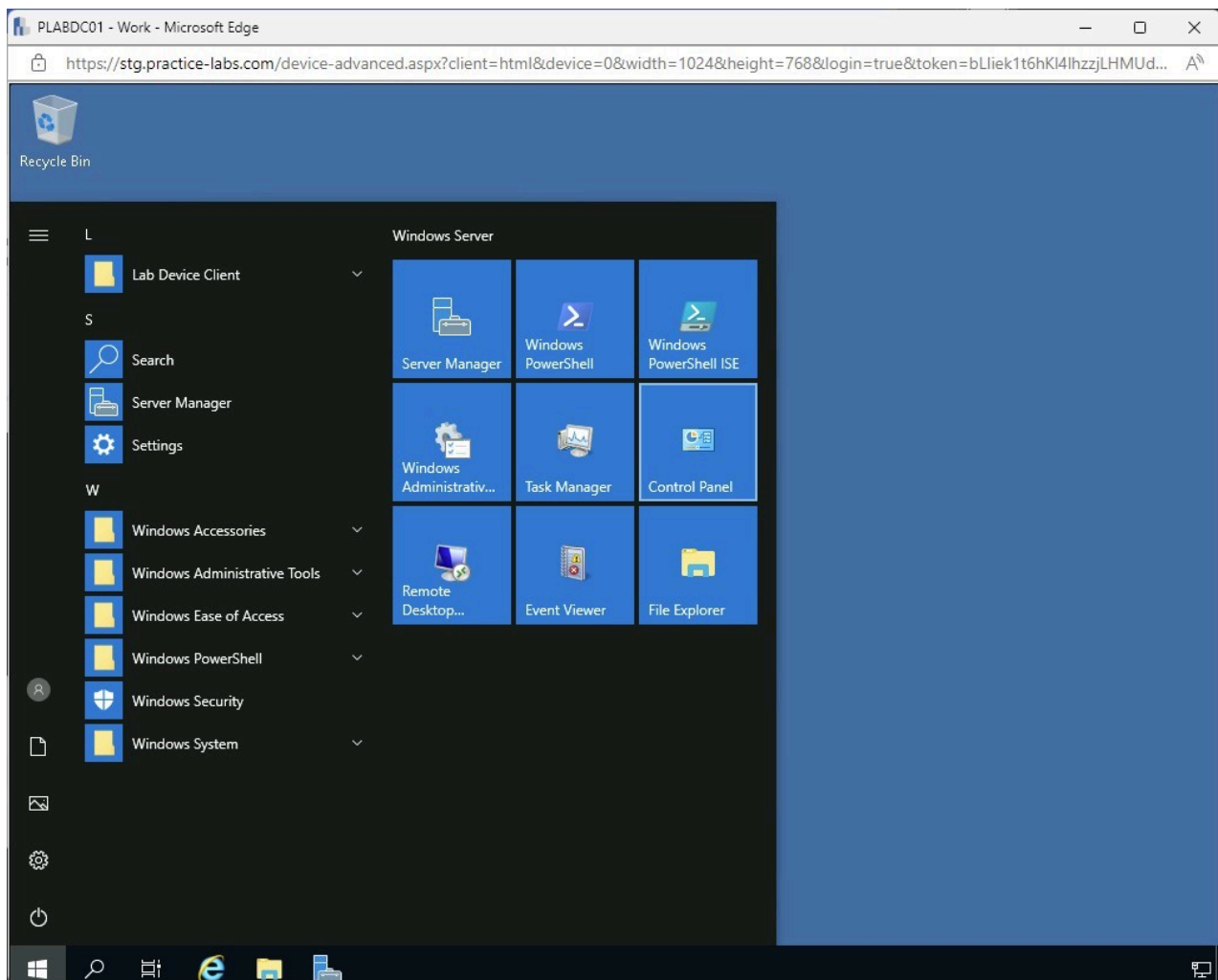


Figure 1.4 Screenshot of PLABDC01: Displaying selecting Control Panel from the Start menu.

Step 5

In the **Control Panel** window, select **Network and Internet**.

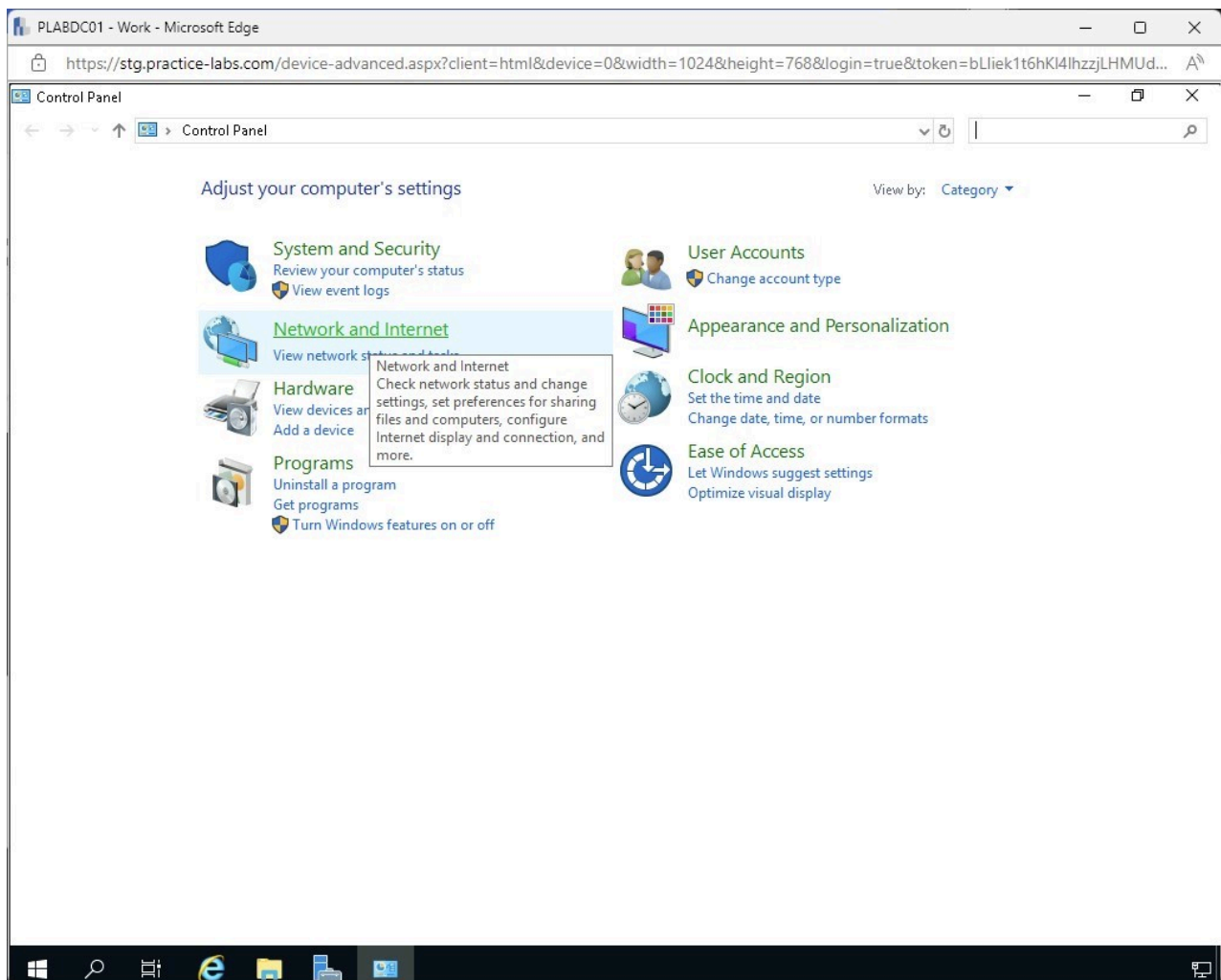


Figure 1.5 Screenshot of PLABDC01: Displaying the Control Panel window with Network and Internet selected.

Step 6

In the **Network and Internet** window, select **Network and Sharing Center**.

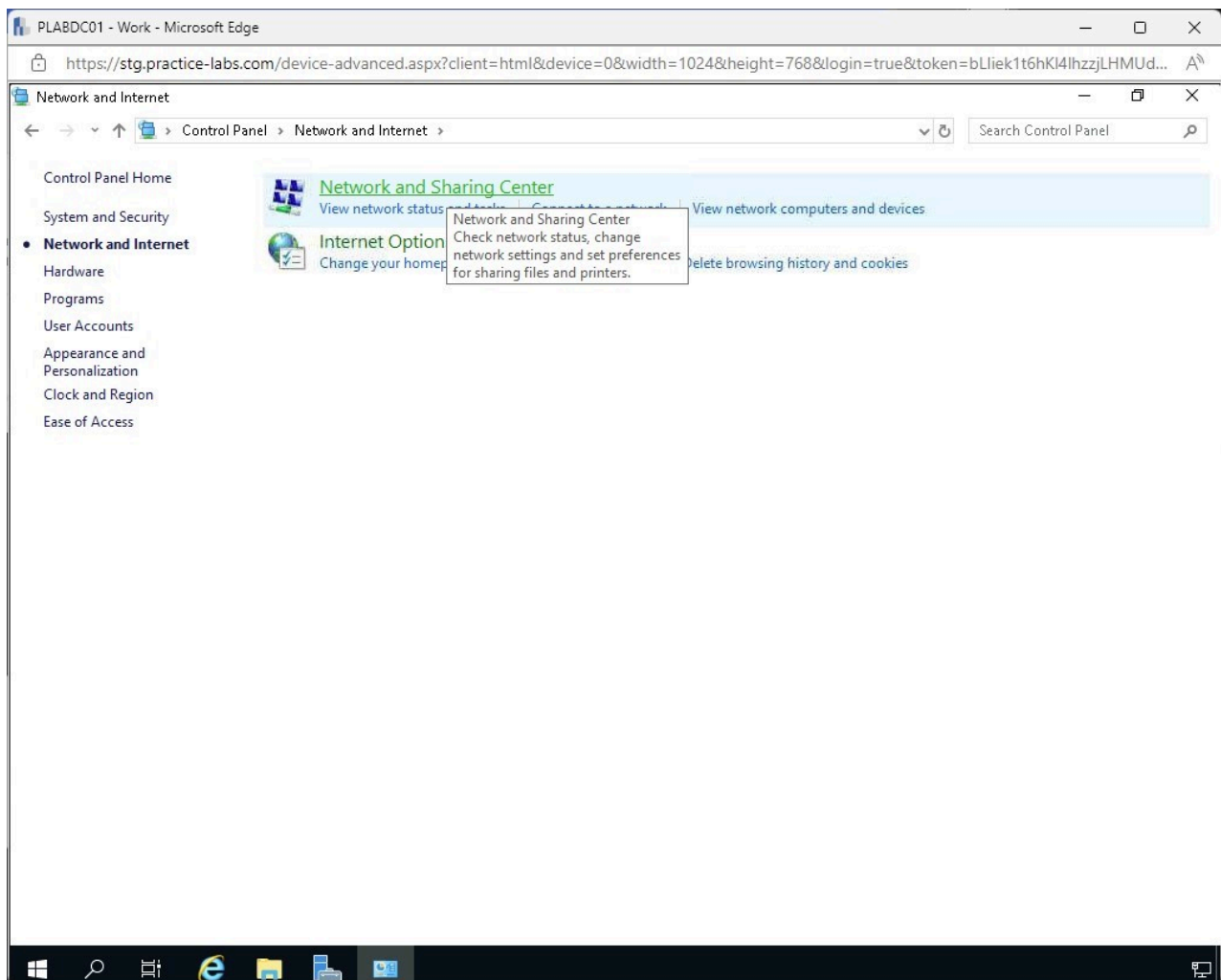


Figure 1.6 Screenshot of PLABDC01: Displaying the Network and Internet window with Network and Sharing Center selected.

Step 7

On the **Network and Sharing Center** window, select the **Change adapter settings** link on the left pane.

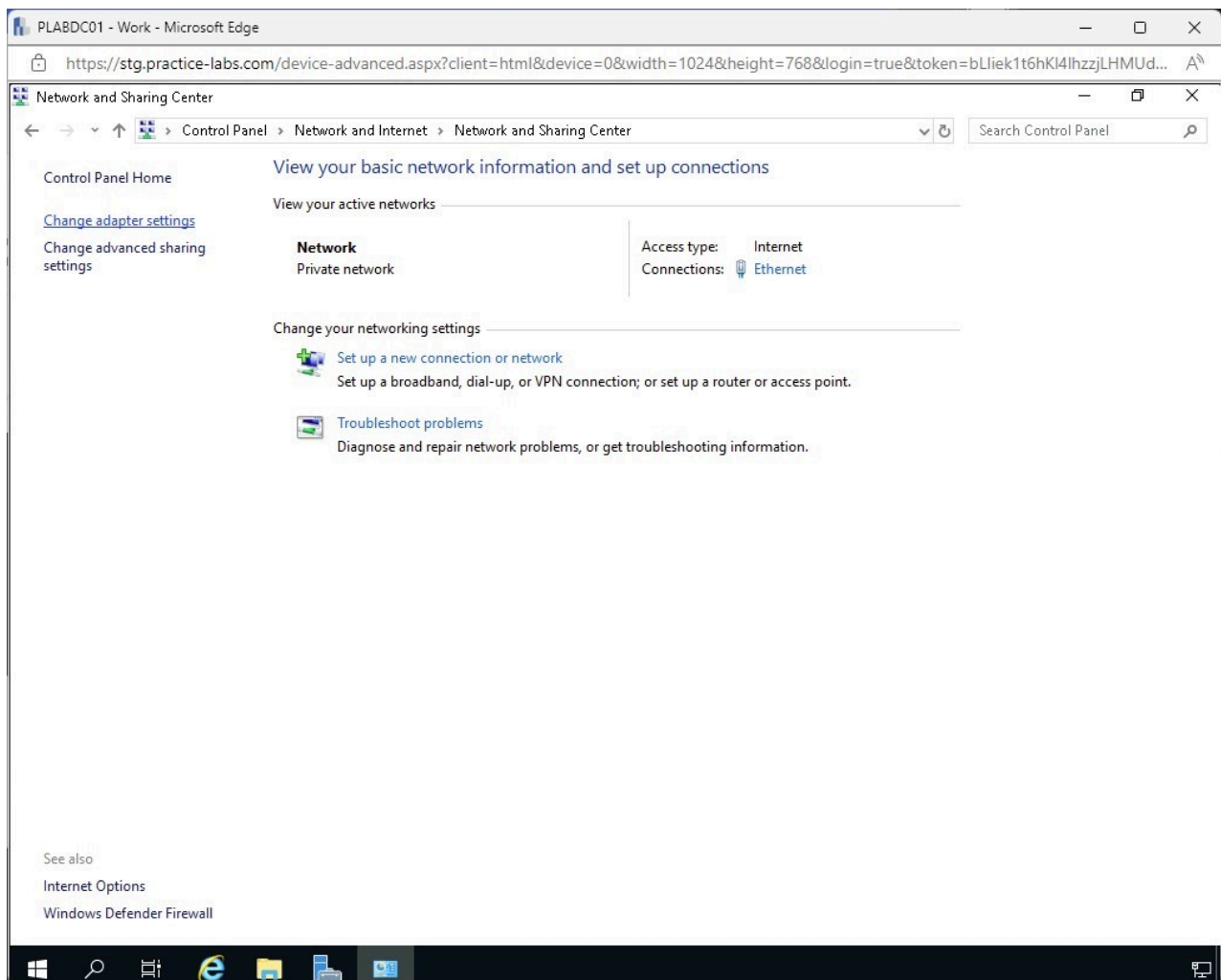


Figure 1.7 Screenshot of PLABDC01: Displaying the Network and Sharing Center window with the Change adapter settings link selected.

Step 8

From the **Network Connections** window, right-click on the **Ethernet** adapter and select **Properties**.

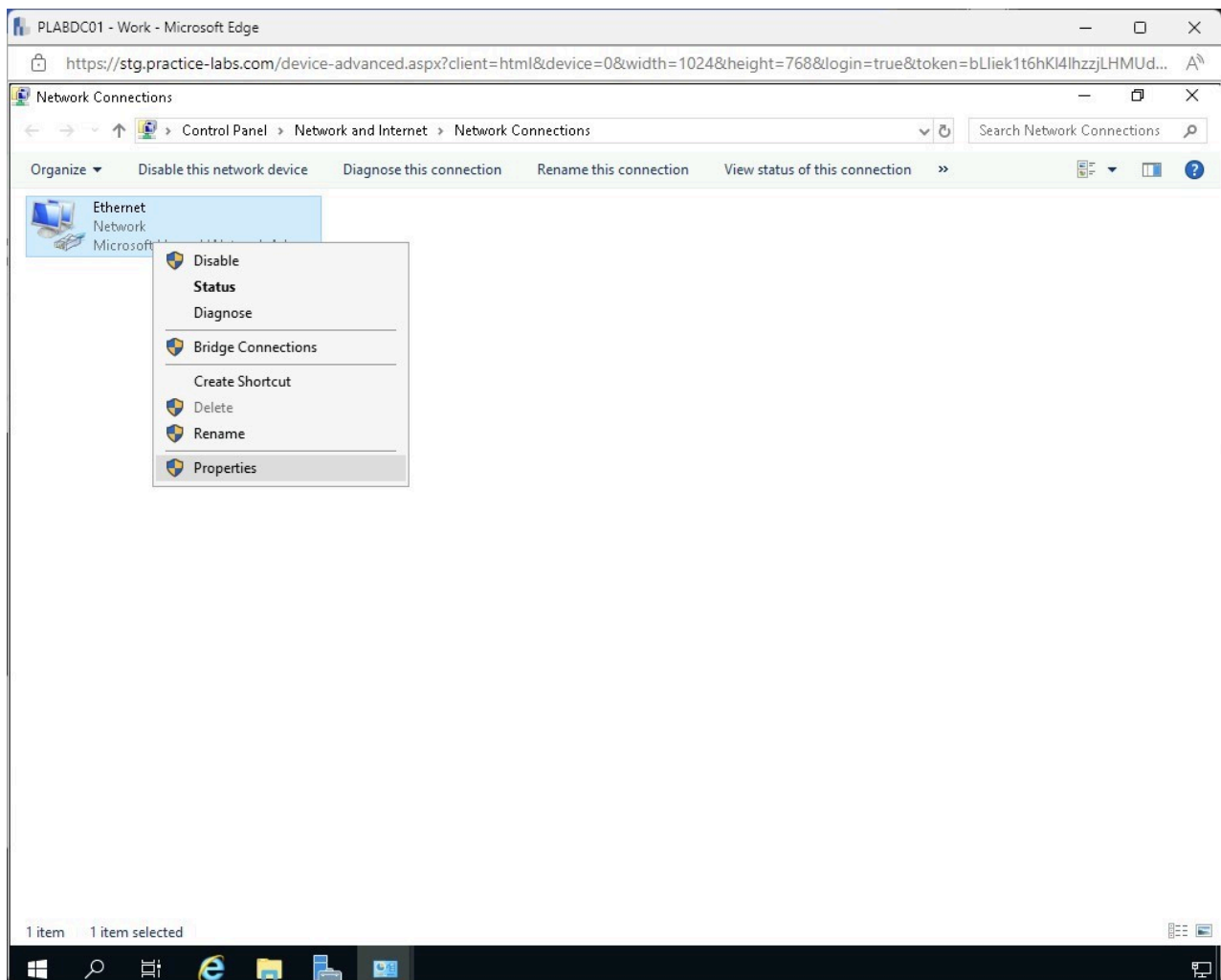


Figure 1.8 Screenshot of PLABDC01: Displaying the Network Connections window with Ethernet right-clicked and Properties selected.

Note: In this window, additional adapters will be listed if the system has multiple network interface cards or other types of adapters, such as a wireless internet adapter or a Bluetooth adapter.

Step 9

On the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

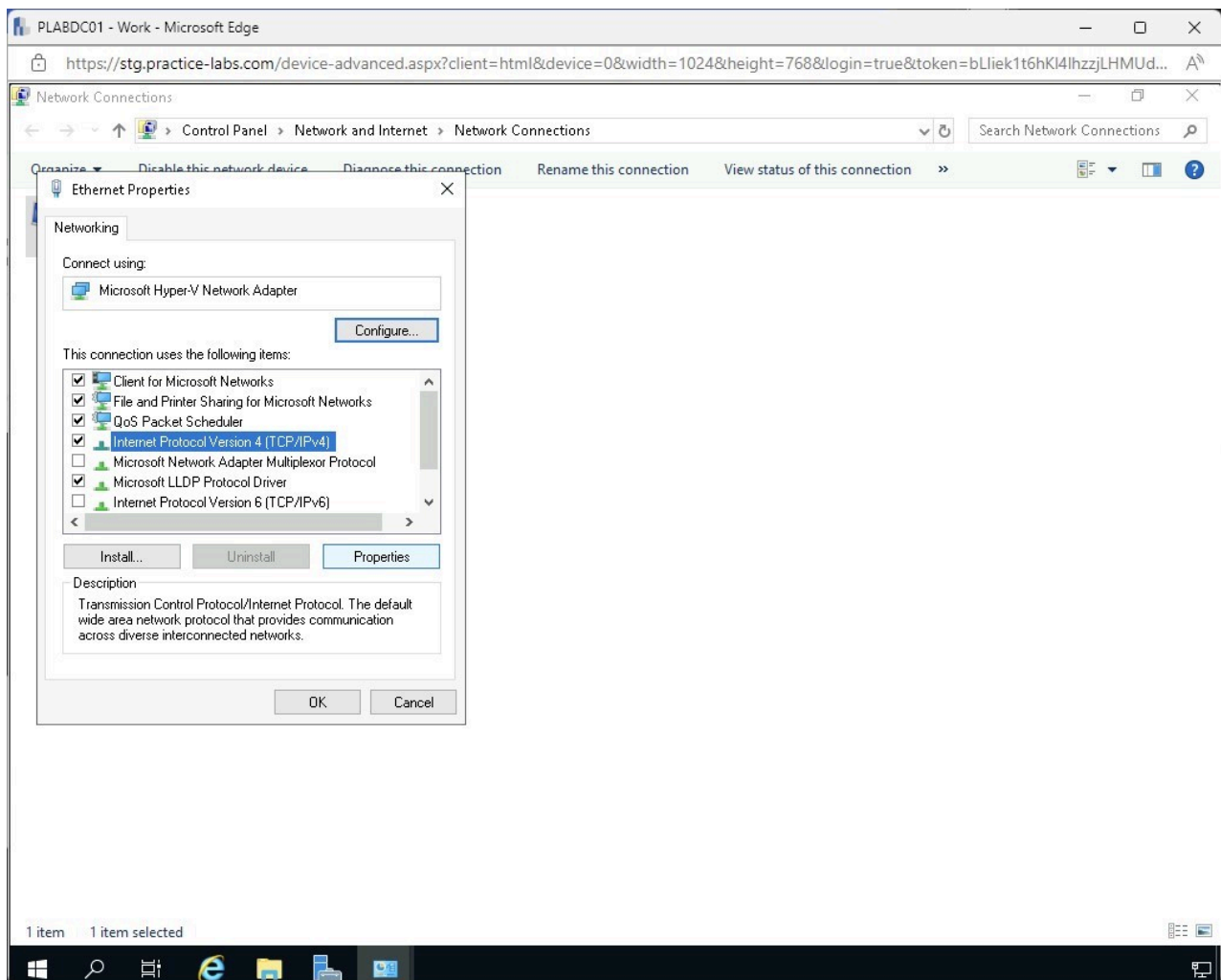


Figure 1.9 Screenshot of PLABDC01: Displaying the Ethernet Properties dialog box with Internet Protocol Version 4 (TCP/IPv4) selected and the Properties button highlighted.

Step 10

The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box is displayed.

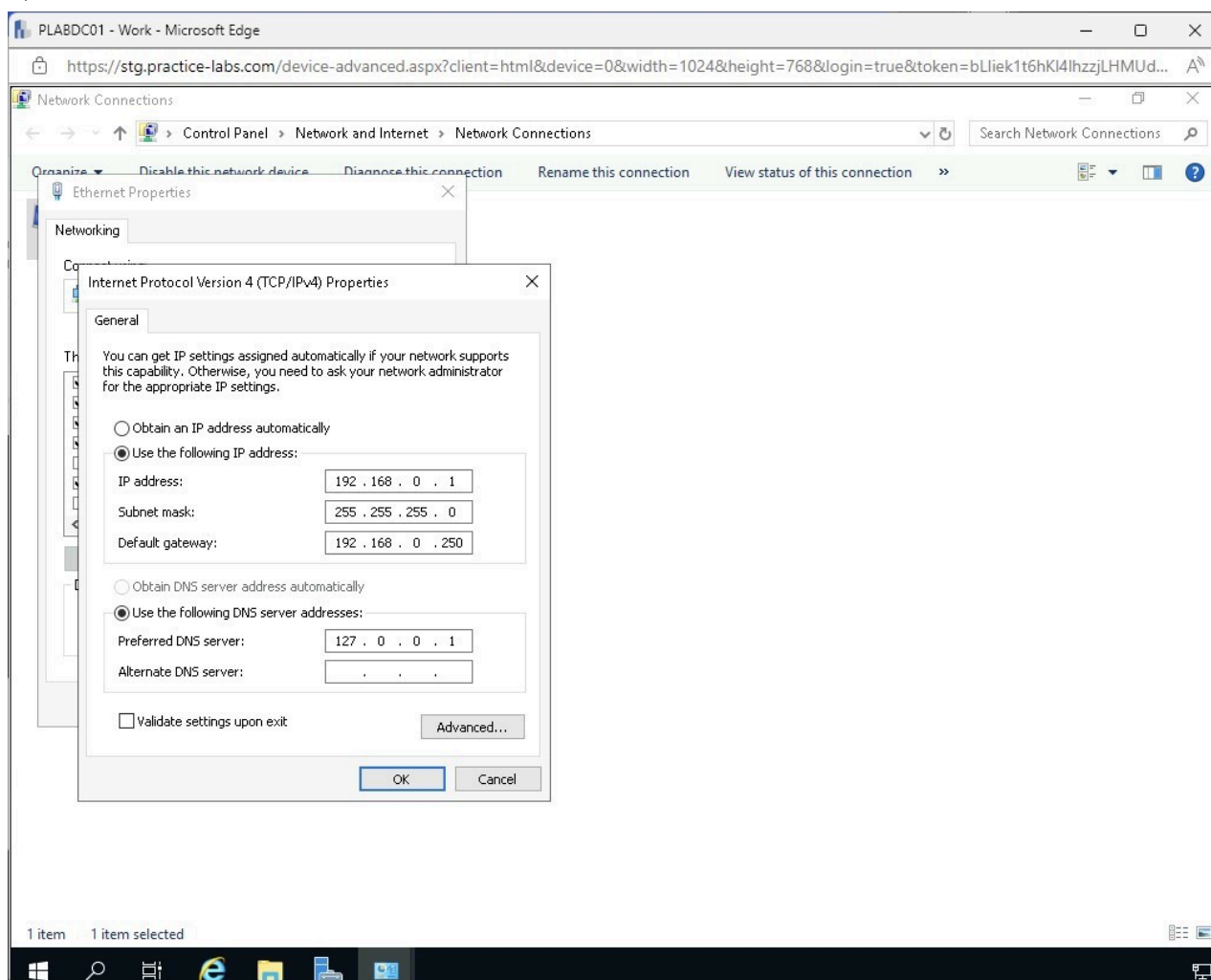


Figure 1.10 Screenshot of PLABDC01: Displaying the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

Note: The following options can be configured on this window:

- If you select to obtain an IP address automatically, the system will attempt to query a DHCP server in order to be assigned an **IP address**. In the above screenshot, a static address of **192.168.0.1** has already been assigned. You can also change the IP address in this window.
- A **Default gateway** of **192.168.0.250** has been assigned to the system. The Default gateway is the device traffic will need to reach if the system needs to communicate with other devices outside the subnet it is assigned to. The default gateway device is often a Router or Layer 3 switch.
- You can also set the **DNS Server**. The system queries the DNS Server using the hostname to find other devices on the network. The server maintains a record of hostnames and associated IP addresses. The DNS Server is set to **127.0.0.1** on this device. The address is a loopback address that tells the system to use itself as the DNS Server. Since this system is a Domain Controller and has the DNS role installed, there is no need to point to a different DNS server. Other systems joined to this domain would use 192.168.0.1 as their DNS server.

Step 11

Click **Cancel** in the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.

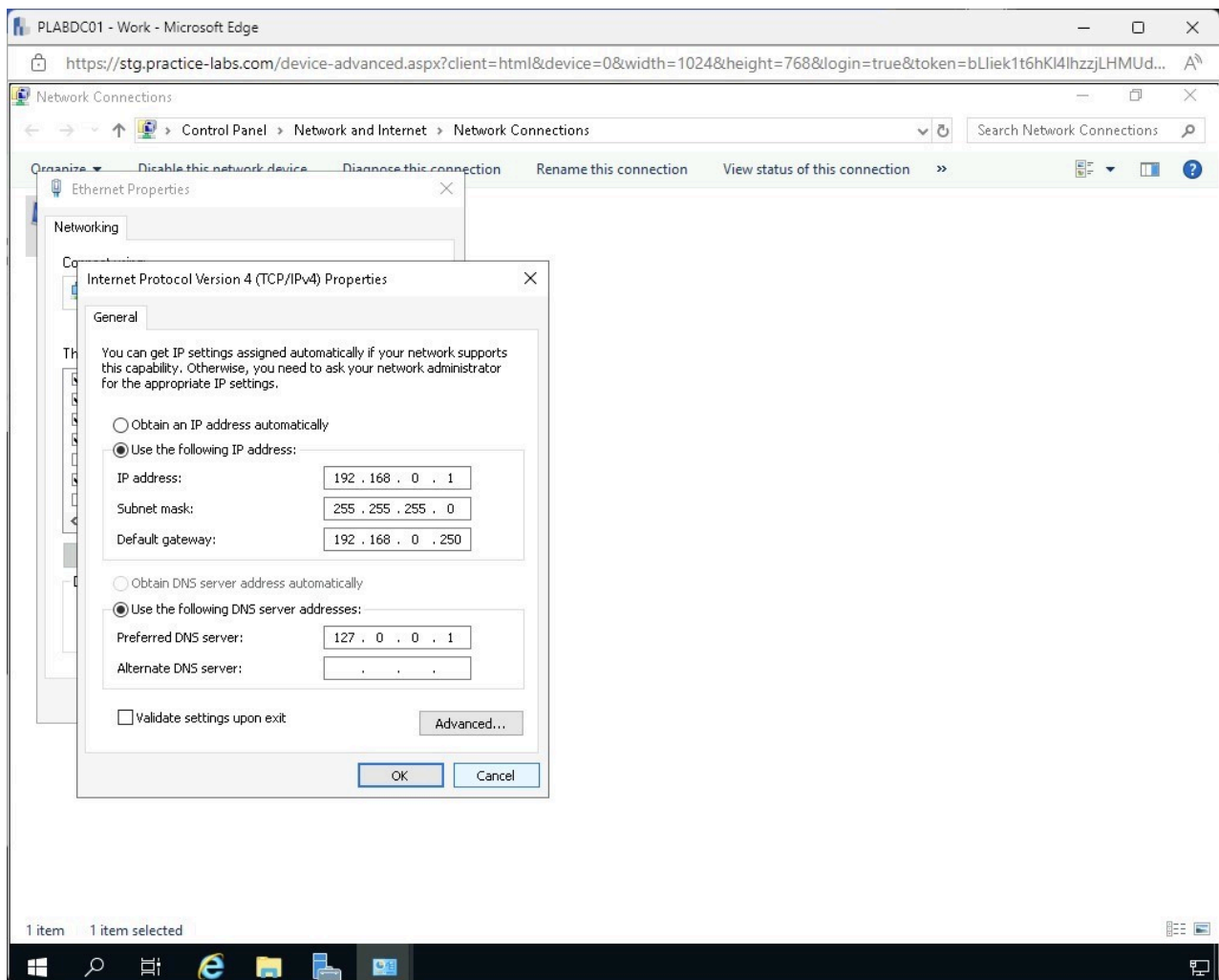


Figure 1.11 Screenshot of PLABDC01: Displaying the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box with Cancel selected.

Step 12

Back on the **Ethernet Properties** dialog box, click the **Configure...** button.

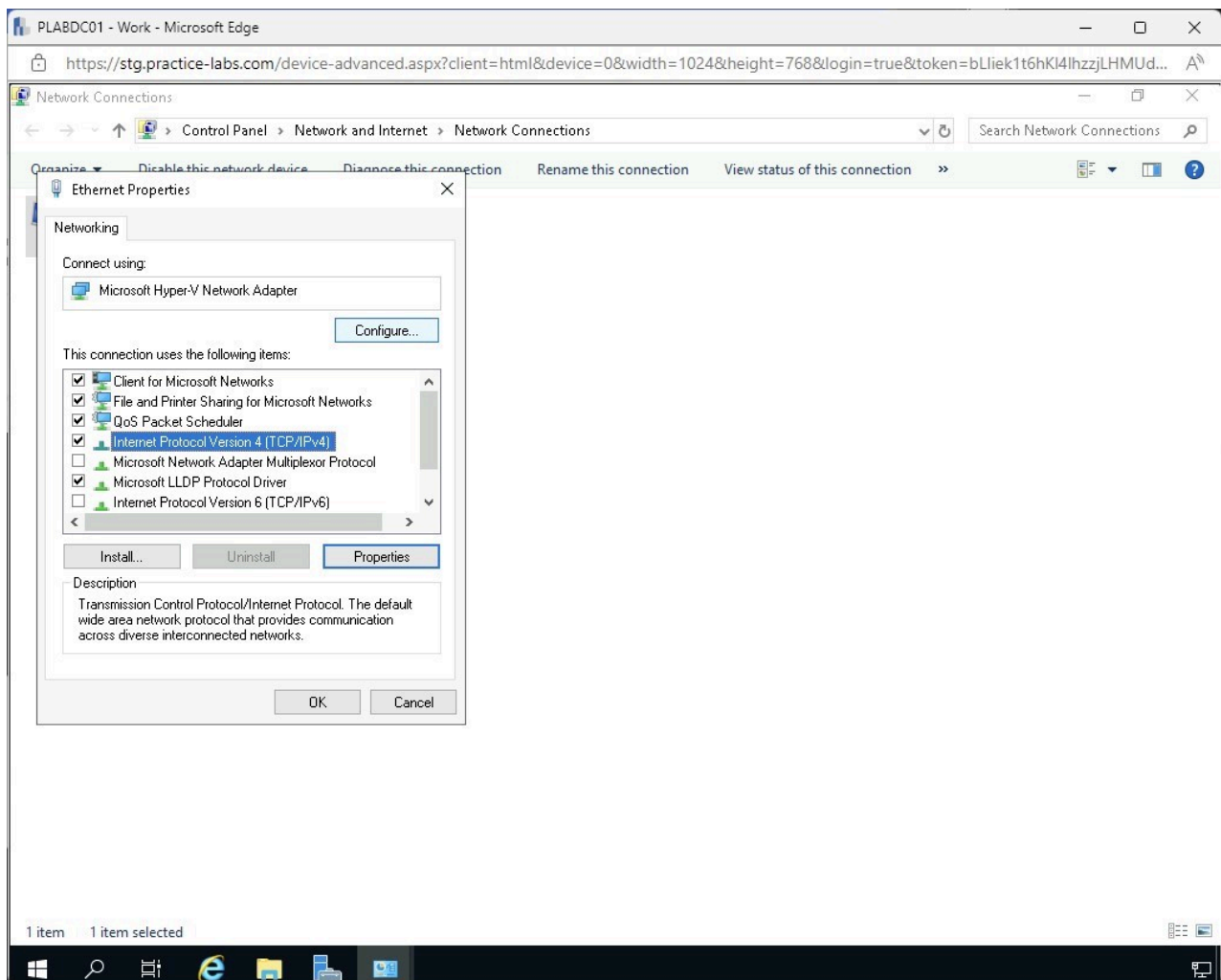
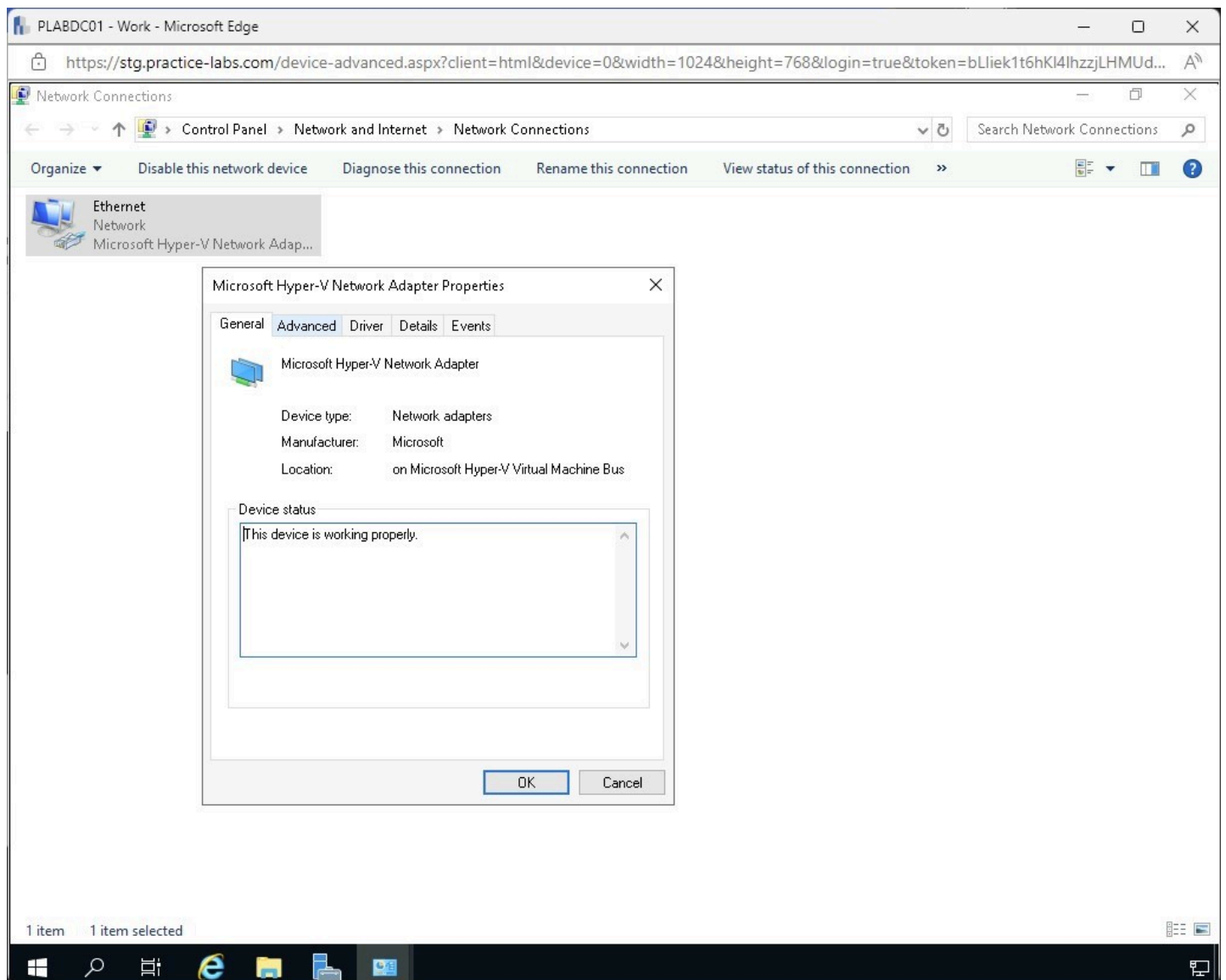


Figure 1.12 Screenshot of PLABDC01: Displaying the Ethernet Properties dialog box with Configure selected.

Step 13

In the **Microsoft Hyper-V Adapter Properties** dialog box, click the **Advanced** tab.



Step 14

From the **Advanced** tab, scroll down to **VLAN ID** under the **Property** field.

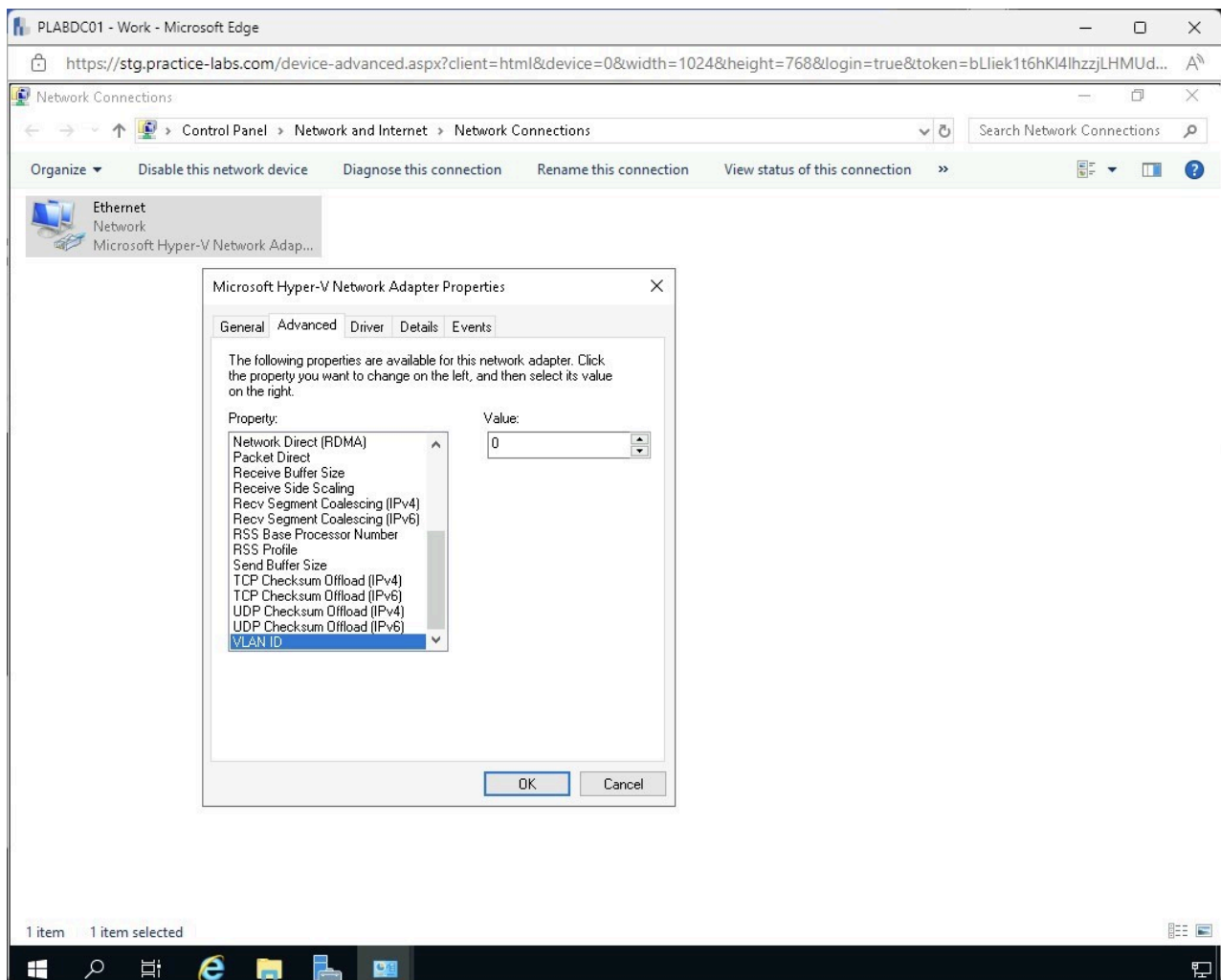


Figure 1.14 Screenshot of PLABDC01: Displaying the Microsoft Hyper-V Adapter Properties - Advanced tab with VLAN ID selected.

Note: The **Virtual Local Area Network (VLAN) ID** can be specified in the **Value** field. This is frequently used in virtual environments where a server administrator may need to connect a hypervisor host to multiple network segments or VLANs over the same physical network interface.

Step 15

Click **Cancel**.

Close the **Network Connections** and **Network and Sharing Center** windows.

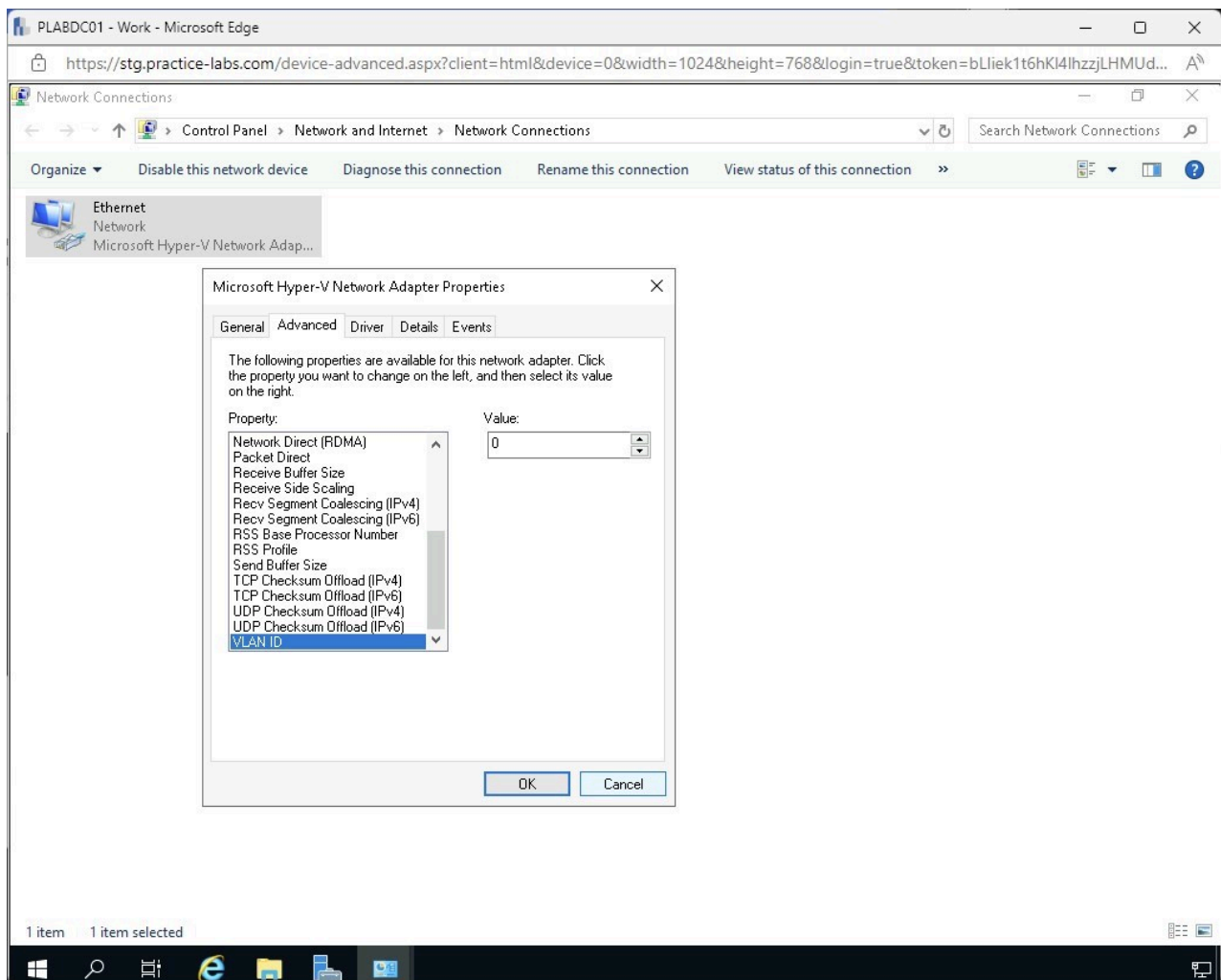


Figure 1.15 Screenshot of PLABDC01: Displaying the Microsoft Hyper-V Adapter Properties - Advanced tab with the Cancel button selected.

Step 16

Click the **Start** charm and type:

Firewall

Select **Windows Defender Firewall** from the **Best match** pop-up menu.

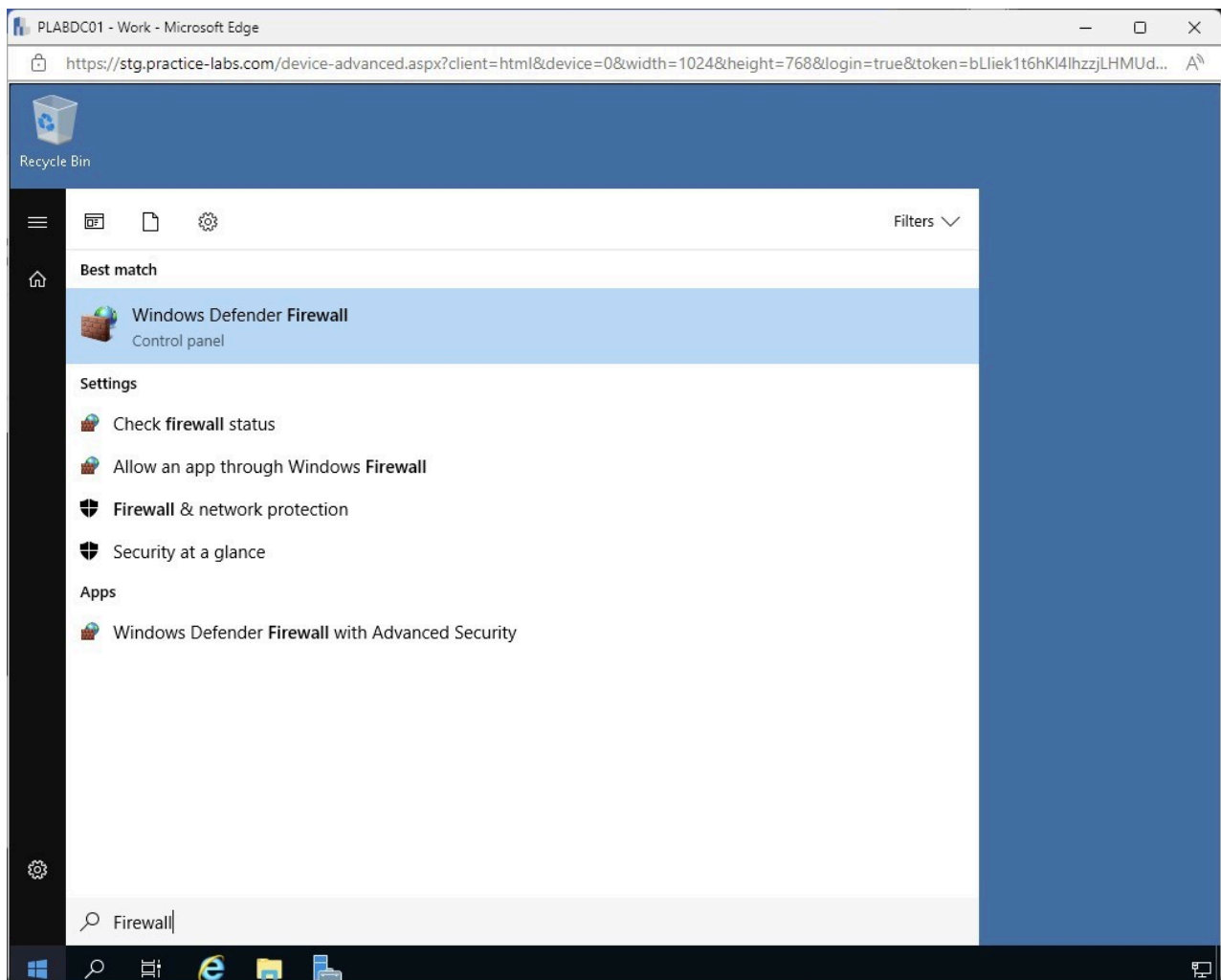


Figure 1.16 Screenshot of PLABDC01: Displaying selecting Windows Defender Firewall from the Best match pop-up menu.

Step 17

In the **Windows Defender Firewall** window, notice the system firewall is enabled.

Select the **Advanced settings** link on the left pane.

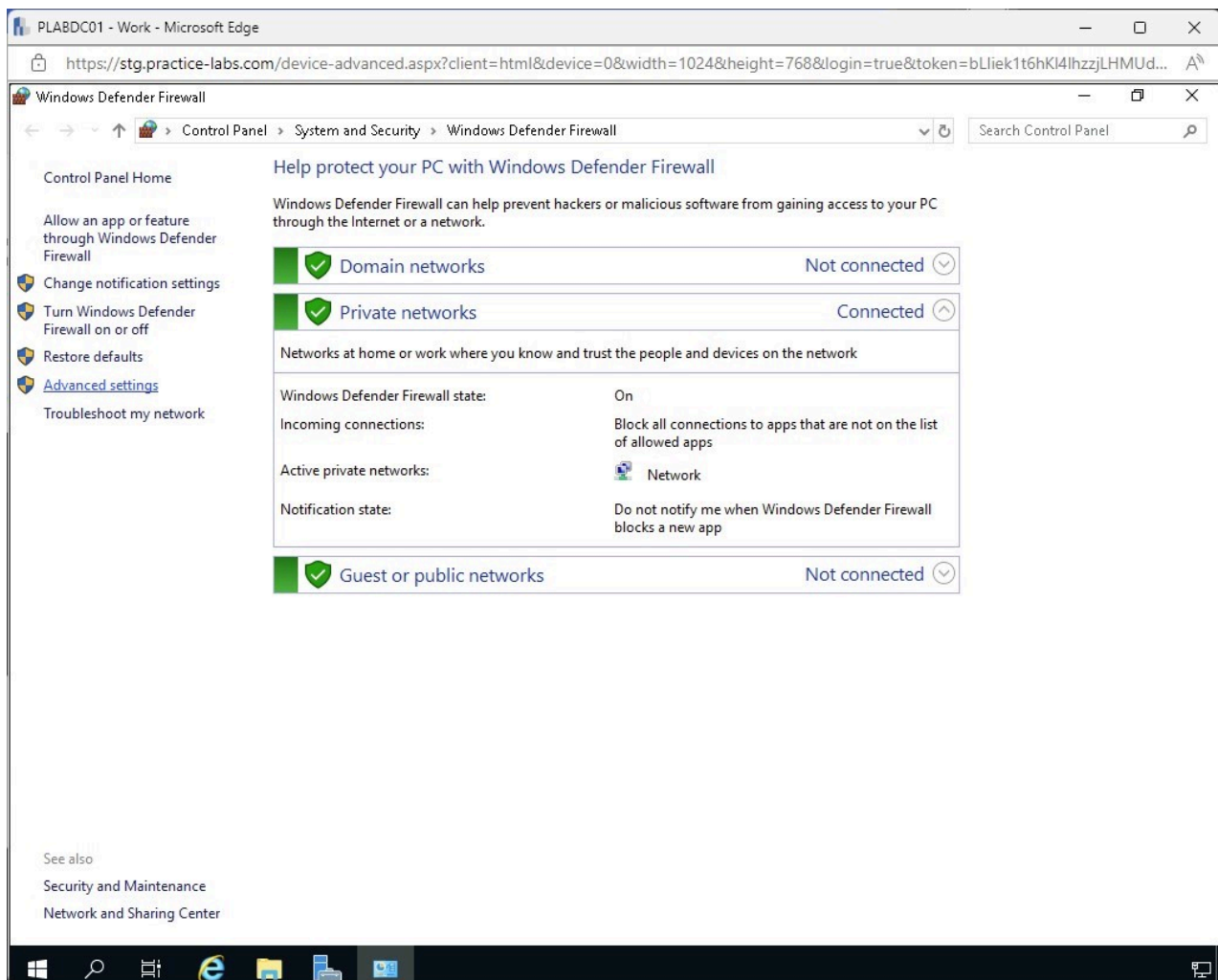


Figure 1.17 Screenshot of PLABDC01: Displaying the Windows Defender Firewall window with the Advanced settings link selected.

Step 18

In the **Windows Defender Firewall with Advanced Security** window, select **Inbound Rules** on the left pane

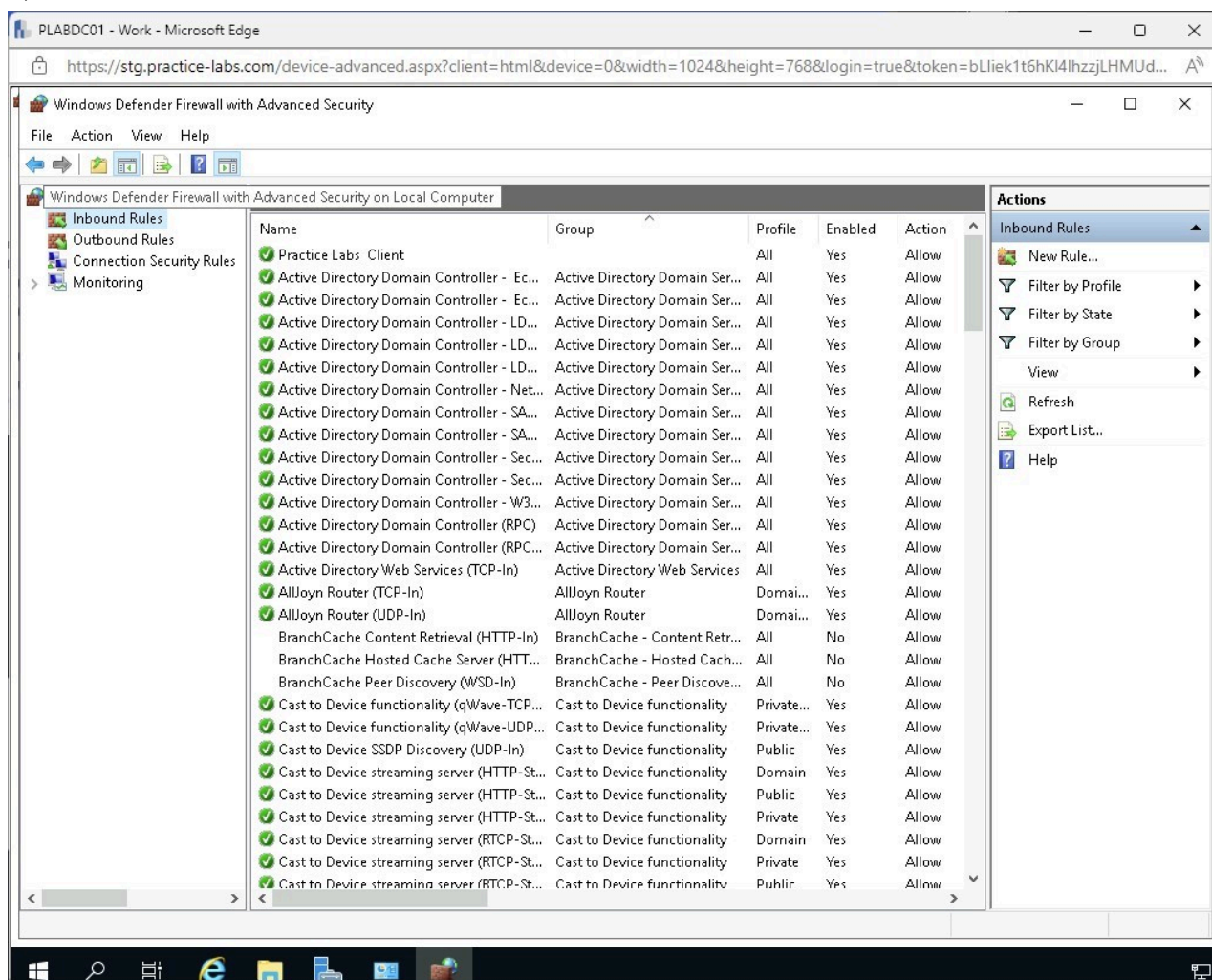


Figure 1.18 Screenshot of PLABDC01: Displaying the Windows Defender Firewall with Advanced Security window with Inbound Rules selected.

Note: On the **Inbound Rules** pane, rules that govern what types of inbound traffic are allowed to communicate with the server are displayed. Some newly installed applications might require additional ports to be opened on the system's firewall.

Step 19

Click **New Rule** on the **Actions** pane.

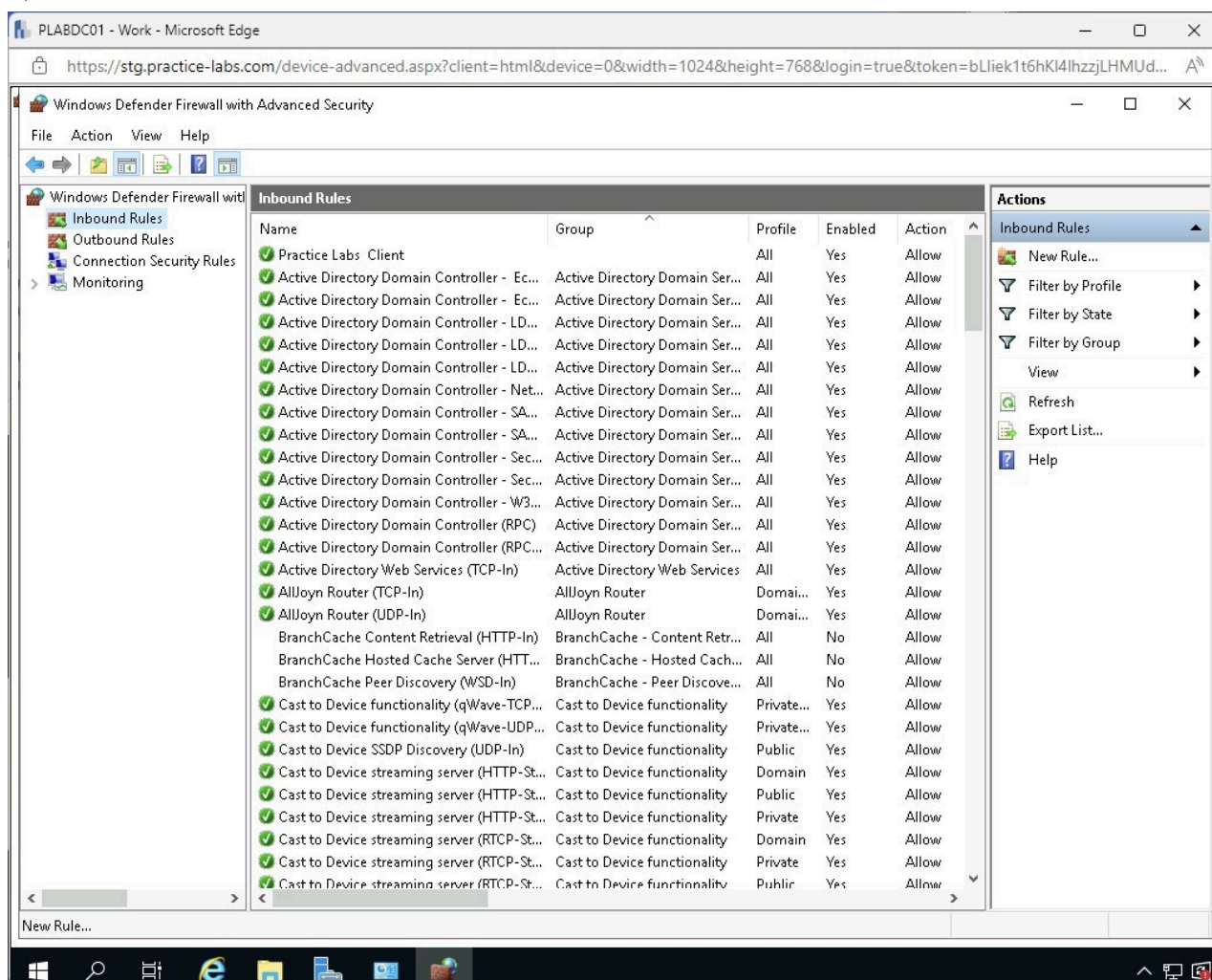


Figure 1.19 Screenshot of PLABDC01: Displaying the Windows Defender Firewall with Advanced Security window with Inbound Rules selected.

Step 20

On the **New Inbound Rule Wizard - Rule Type** page, select the **Port** option and click **Next**.

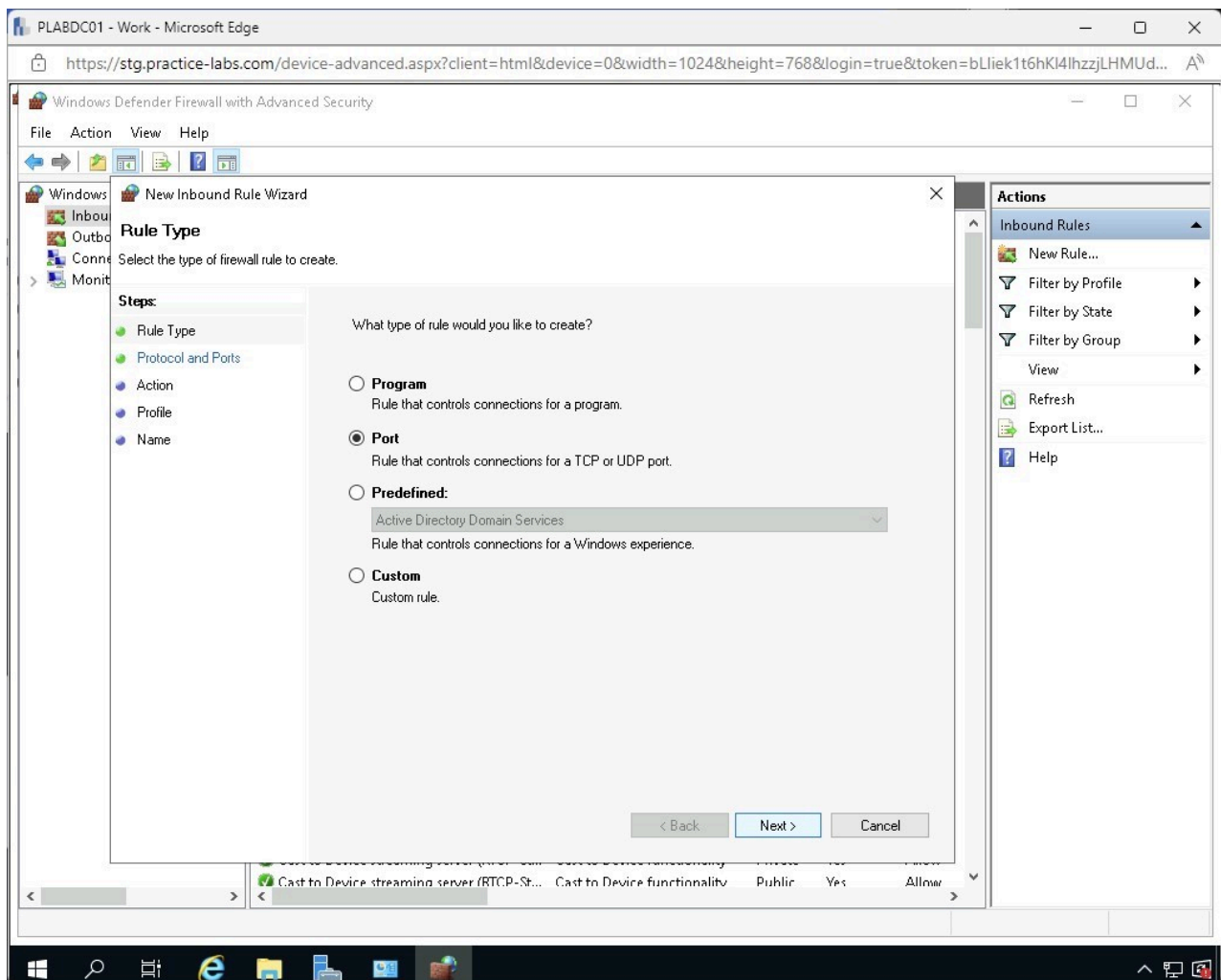


Figure 1.20 Screenshot of PLABDC01: Displaying the New Inbound Rule Wizard - Rule Type page with the Port option selected and the Next button highlighted.

Step 21

On the **Protocol and Ports** page, under the **Does this rule apply to all local ports or specific local ports?** section, select the **Specific local ports** option and type:

80

Click **Next**.

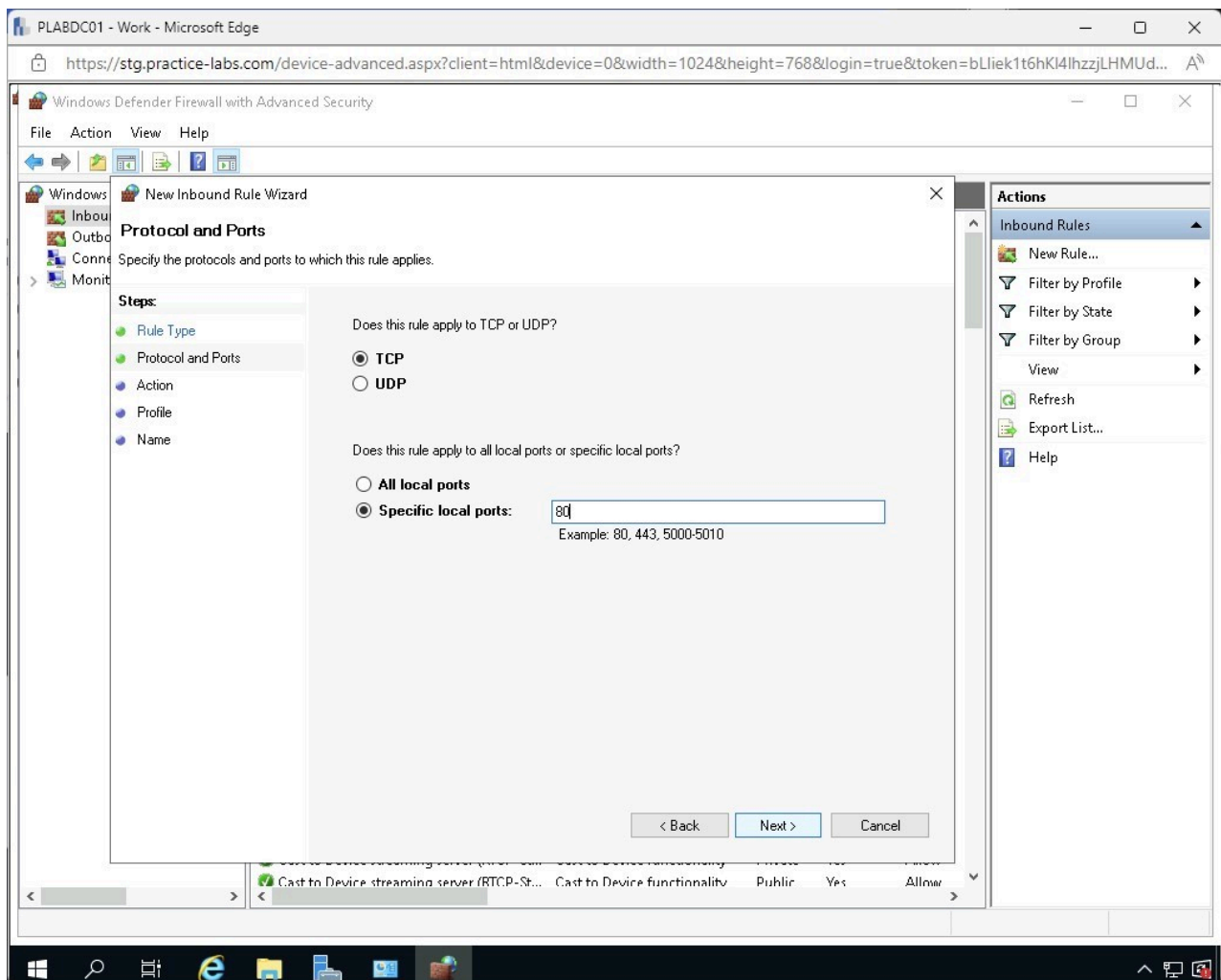


Figure 1.21 Screenshot of PLABDC01: Displaying the Protocol and Ports page with the required settings performed and the Next button highlighted.

Note: On the **Protocol and Ports** page, you can select either **TCP** or **UDP**. This can vary depending on the type of traffic expected. You can also choose to allow all ports or choose specific ports.

Step 22

On the **Action** page, keep the default settings and click **Next**.

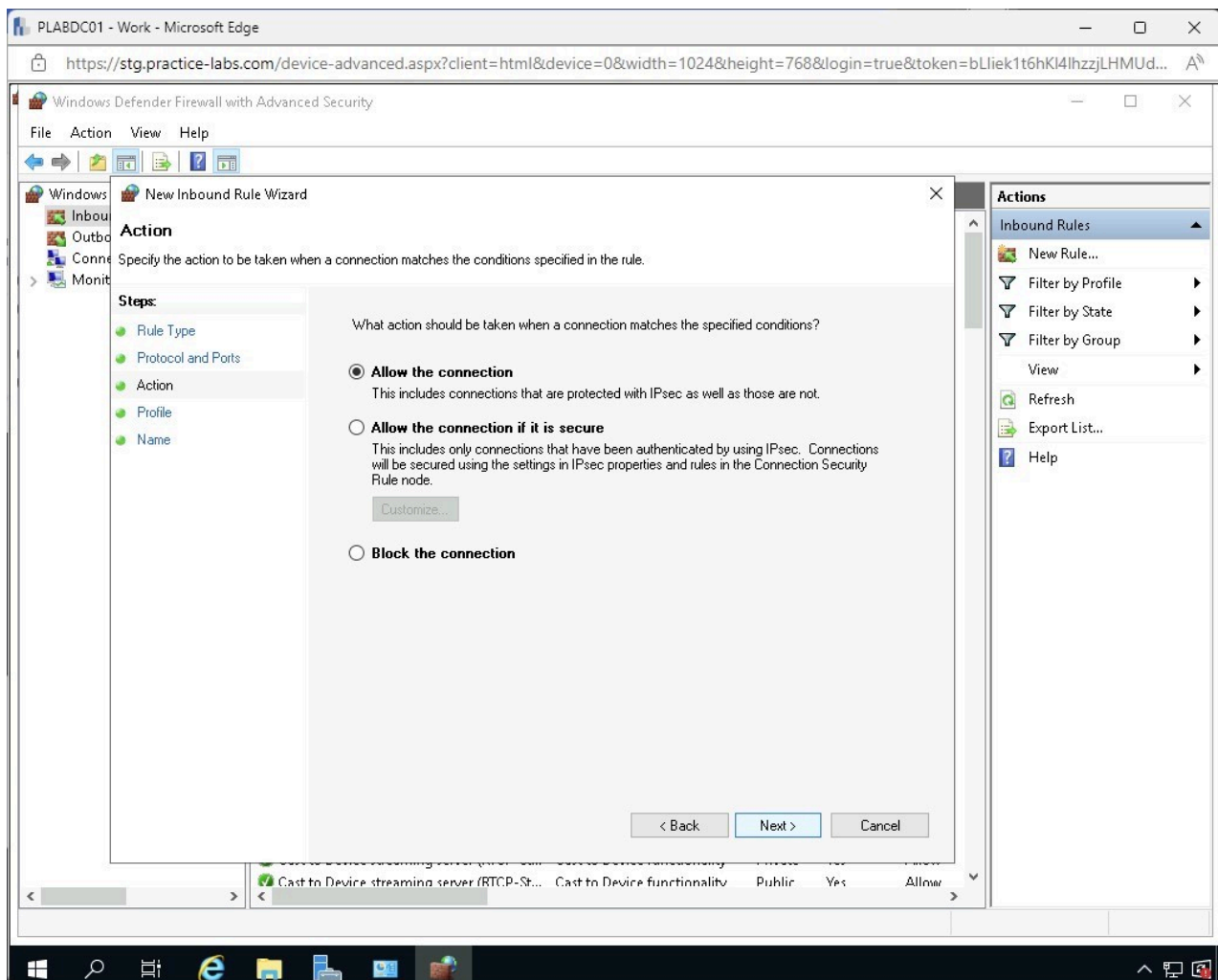


Figure 1.22 Screenshot of PLABDC01: Displaying the Action page with the Next button highlighted.

Step 23

On the **Profile** page, click **Next**.

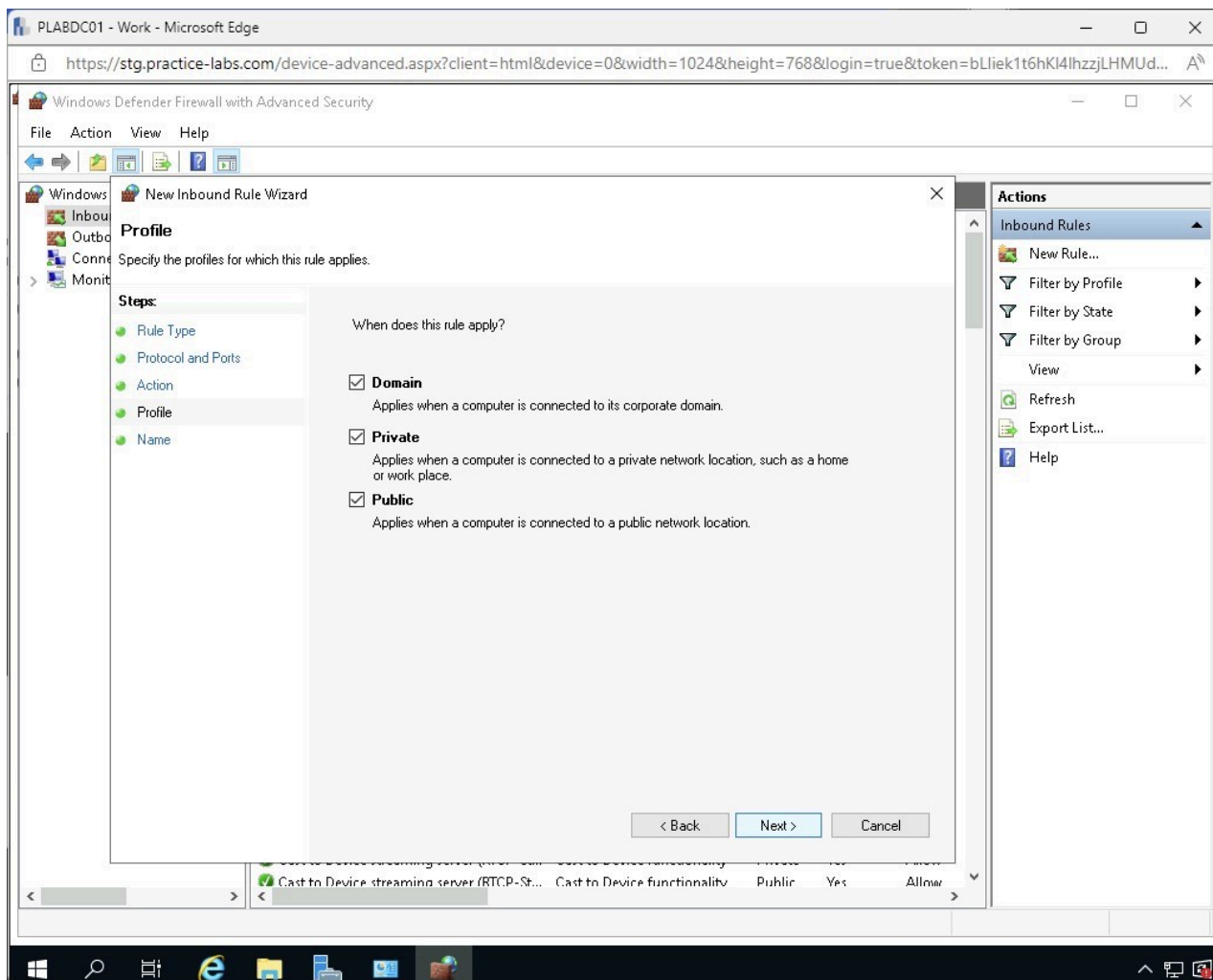


Figure 1.23 Screenshot of PLABDC01: Displaying the Profile page with the Next button selected.

Note: On the **Profile** page, you can choose when the rule applies. Some rules may pose a security risk if connections are made from networks other than the corporate network. In that case, just the **Domain** checkbox should be selected.

Step 24

On the **Name** page, complete the following:

Name: **Port 80 Inbound**
Description: **New App**

Click **Finish**.

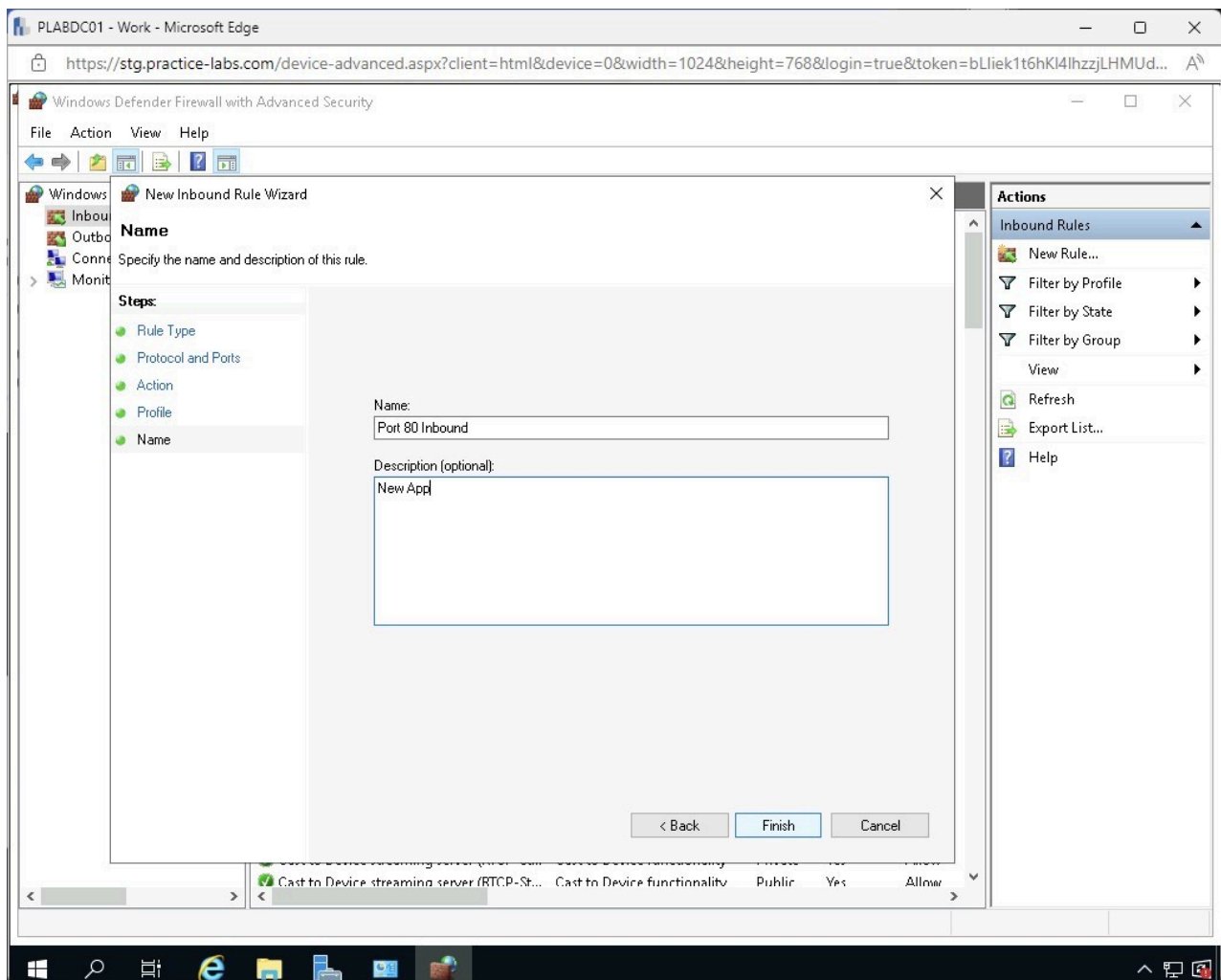


Figure 1.24 Screenshot of PLABDC01: Displaying the Name page with the required settings performed and the Finish button highlighted.

Step 25

The newly created firewall rule **Port 80 Inbound** is displayed in the **Inbound Rules** list.

Close all open windows.

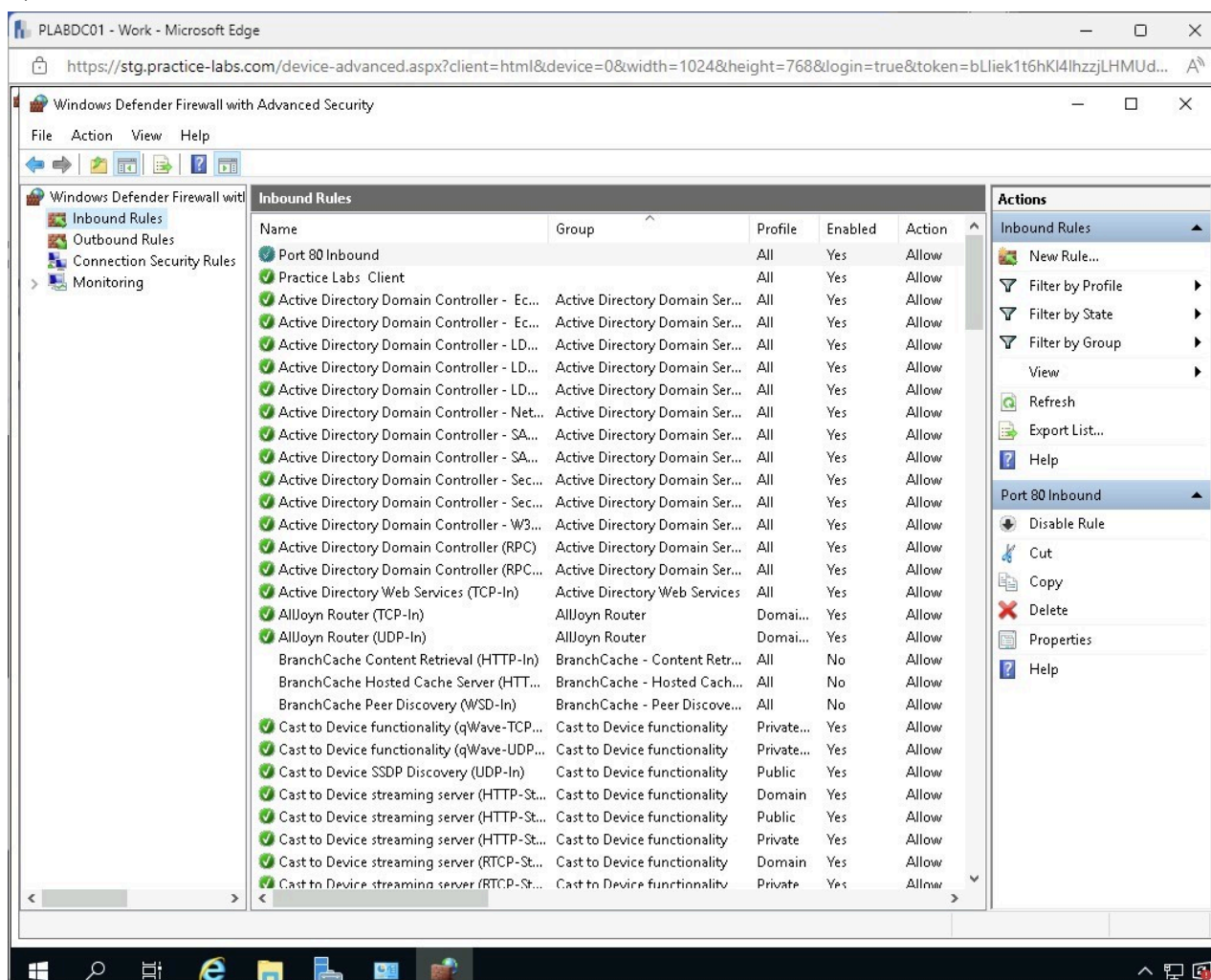


Figure 1.25 Screenshot of PLABDC01: Displaying the Windows Defender Firewall with Advanced Security window with the newly created Inbound Rule.

Keep all devices that you have powered on in their current state and proceed to the review section.

Review

Well done, you have completed the **Server Network Infrastructure Configuration** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Configure Various Network Settings on Windows Server 2019

You should now be able to:

- Identify the Network Configurations of a Server

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.