Module 5: Configuring and troubleshooting network connectivity

Lab: Configuring and troubleshooting network connectivity

**Scenario**

You’re working with the networking team. You’ve been asked to configure the network settings, including setting up a VPN, on a number of Windows 11 workstations. Later, back on the helpdesk, you are assigned some tickets relating to suspected networking issues. You decide to investigate.

**Objectives**

After completing this lab, you will be able:

* Configure IPv4 settings.
* Troubleshoot network connectivity.
* Troubleshoot name resolution.
* Configure a VPN.

Exercise 1: Configuring IPv4 settings

**Scenario**

The main tasks for this exercise are as follows:

1. Verify the IPv4 settings from the Settings app.
2. Verify the current IPv4 settings from the command line.
3. Test connectivity.
4. Reconfigure the IPv4 settings.
5. Test connectivity.
6. View the impact on the DHCP server.

Task 1: Verify the IPv4 settings from the Settings app

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm) using Virtual Machine drop down menu on the Home tab in the lab environment.
2. Open **Settings**.
3. In the navigation pane, select **Network & internet**.
4. In Network & internet, click **Ethernet**. Review the IPv4 settings. This window displays the same configuration information for this adapter as would the **Ipconfig** command.
5. Record the following information:
   * IPv4 address
   * IPv4 mask
   * IPv4 gateway
   * IPv4 DNS Server
6. Adjacent to the IPv4 settings, click **Edit**. You can configure protocols in this window. Click **Cancel**.
7. Close all open windows without modifying any settings.

Task 2: Verify the current IPv4 settings from the command line

1. Right-click **Start**, and then click **Windows Terminal (Admin)**.
2. At the Administrator: Windows PowerShell command prompt, type **Get-NetIPAddress**, and then press Enter. The IPv4 address should match what you recorded earlier.
3. Get-NetIPAddress
4. At the Windows PowerShell command prompt, type **netsh interface ipv4 show config**, and then press Enter. The current IPv4 configuration is displayed and should match what you recorded earlier.
5. netsh interface ipv4 show config
6. At the Windows PowerShell command prompt, type **ipconfig /all**, and then press Enter. Again, the information should match what you recorded earlier.
7. ipconfig /all
8. Leave the **Windows Terminal (Admin)** window open.

Task 3: Test connectivity

1. At the Windows PowerShell command prompt, type **test-connection LON-DC1**, and then press Enter.
2. test-connection LON-DC1
3. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter. Observe and describe the active connections to 172.16.0.10. Most connections to services are transient.
4. netstat -n

**Note:** See the next step if you do not see any connections.

1. If no connections appear, create a connection. To create a connection, on the taskbar, click Search, and then type [**\\LON-DC1**](urn:gd:lg:a:send-vm-keys), and then press Enter.
2. In **File Explorer**, double-click **netlogon**.
3. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter. Identify the services that **LON-CL1** had connections to on **LON-DC1**.
4. netstat -n

Task 4: Reconfigure the IPv4 settings

1. Open **Settings**.
2. In the navigation pane, select **Network & internet**.
3. In Network & internet, click **Ethernet**.
4. Adjacent to the IPv4 settings, click **Edit**.
5. In the **Edit IP settings** dialog box, click **Manual**, then select **Automatic (DHCP)**, and then click **Save**.
6. At the Windows PowerShell command prompt, type **ipconfig /all**, and then press Enter. Again, the information should match what you recorded earlier.
7. ipconfig /all
8. Verify that the IPv4 address is obtained from DHCP.

Task 5: Test connectivity

1. At the Windows PowerShell command prompt, type **test-connection LON-DC1**, and then press Enter.
2. test-connection LON-DC1
3. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter.
4. netstat -n
5. Observe and describe the active connections to 172.16.0.10. Most connections to services are transient.
6. If no connections appear, create a connection. To create a connection, on the taskbar, click Search, and then type [**\\LON-DC1**](urn:gd:lg:a:send-vm-keys), and then press Enter.
7. In **File Explorer**, double-click **netlogon**.
8. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter.
9. netstat -n
10. Identify the services that **LON-CL1** had connections to on **LON-DC1**.
11. Close all open windows except **Windows Terminal (Admin)**.

Task 6: View the impact on the DHCP server

1. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm) using the Virtual Machine drop down menu on the Home tab of the lab environemnt.
2. Click the [**CTRL+ALT+DEL**](urn:gd:lg:a:send-vm-key-combo) button on the home tab of the lab envirionment and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
3. Once **Server Manager** has loaded, click **Tools**, and then click **DHCP**.
4. In **DHCP**, expand **lon-dc1.adatum.com**, expand **IPv4**, expand **Scope [172.16.0.0] Adatum**, and then click **Address Leases**.
5. In the details pane, you should see the address lease for your Windows 11 client.

**Results**: After completing this exercise, you should have successfully configured IPv4 settings.

Exercise 2: Troubleshooting network connectivity

**Scenario**

A user has reported a networking problem to the help desk. You must investigate and attempt a resolution.

| **Incident Record** |
| --- |
| **Incident Reference Number:** 823012 |
| Date of Call：September 21 |
| Time of Call：14:02 |
| User：Max Pennekamp (Research Department) |
| Status：OPEN |
| **Incident Details** |
| Max called the help desk. He is unable to connect to a server resource. |
| **Additional Information** |
| The resource is \\LON-DC1\Research. It is unavailable to Max, but other users also are affected. |
| Max restarted his computer when he returned from lunch. Prior to lunch, he had no problem. |
| **Plan of Action** |
| **Resolution** |

Task 1: Review the help-desk Incident Record for incident 823012

* Review the help-desk Incident Record 823012 in the Student Handbook Exercise Scenario.

Task 2: Discuss recommendations

1. Review the **Additional Information** section of the Incident Record in the Student Handbook Exercise Scenario.
2. Discuss your recommendations with other students:
   * Visit the user's computer.
   * Verify the problem by attempting to connect to the specific resource.
   * Attempt to connect to the same resource from other computers in the Research department.
   * Verify the network configuration on Max's client computer.
3. The fact that other users are affected suggests a server-side problem.

Task 3: Simulate the problem

1. On [**LON-CL1**](urn:gd:lg:a:select-vm), run the **D:\Labfiles\Mod05\Scenario1.vbs** script.
2. Wait while **LON-CL1** restarts.

Task 4: Attempt to resolve the problem

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm) and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
2. Right-click **Start** and then select **Windows Terminal (Admin)**.
3. At the Windows PowerShell command prompt, run the following command:
4. ipconfig /all

**Note:** Notice that the IPv4 address has the prefix **169.254**.

1. At the Windows PowerShell command prompt, run the following command:
2. ipconfig /renew

**Note:** Notice that this is unsuccessful.

1. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm) and login as [**Adatum\Administrator**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. In Server Manager, select **Tools**, and then select **DHCP**. Notice that the server is not available.
3. Close DHCP.
4. Select **Start**.
5. Enter [**services.msc**](urn:gd:lg:a:send-vm-keys), and then select Enter.
6. In the **Services** list, right-click **DHCP Server** and then select **Start**.
7. In Server Manager, select **Tools**, and then select **DHCP**. The server is available.
8. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm).
9. At the Windows PowerShell command prompt, enter [**ipconfig /renew**](urn:gd:lg:a:send-vm-keys),and then select Enter.

**Note:** The command runs successfully.

1. Select **File Explorer**.
2. In the File Explorer address bar, enter [**\\LON-DC1\Research**](urn:gd:lg:a:send-vm-keys),and then select Enter.
3. Close File Explorer.
4. Update the **Resolution** section of the Incident Record with the following comments:
   * The client was unable to contact the dynamic host configuration protocol (DHCP) server to obtain an IP configuration.
   * Restarted the DHCP service, and then renewed the IP configuration on the client.

**Results**: After completing this exercise, you should have resolved the network-related problem.

Exercise 3: Troubleshooting name resolution

**Scenario**

Name resolution is a critical part of your network infrastructure. You must ensure that you have correctly configured the Windows 11 devices for name resolution. Then you must test the name resolution process.

The main tasks for this exercise are as follows:

1. Verify current DNS settings on the client.
2. View and clear the DNS resolver cache.
3. Test name resolution.
4. Create and test a hosts file entry.
5. Troubleshoot name resolution.

Task 1: Verify current DNS settings on the client

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm).
2. Open **Settings**.
3. In the navigation pane, select **Network & internet**.
4. In Network & internet, click **Ethernet**. Review the IPv4 settings. Notice the **IPv4 DNS servers** address.

Task 2: View and clear the DNS resolver cache

1. At the Windows PowerShell (Admin) command prompt, type **ipconfig /displaydns**, and then press Enter. This displays the current DNS resolver cache.
2. ipconfig /displaydns
3. At the Windows PowerShell command prompt, type **Get-DnsClientCache**, and then press Enter. This displays the current DNS resolver cache.
4. Get-DnsClientCache
5. At the Windows PowerShell command prompt, type **ipconfig /flushdns**, and then press Enter. This flushes the current DNS resolver cache.
6. ipconfig /flushdns
7. At the Windows PowerShell command prompt, type **Clear-DnsClientCache**, and then press Enter. This flushes the current DNS resolver cache. It is not necessary to run this in addition to the preceding command.
8. Clear-DnsClientCache
9. At the Windows PowerShell command prompt, type **ipconfig /displaydns**, and then press Enter. This verifies that you have no entries in the cache.
10. ipconfig /displaydns

Task 3: Test name resolution

1. At the Windows PowerShell command prompt, type **test-connection lon-dc1**, and then press Enter.
2. test-connection lon-dc1
3. At the Windows PowerShell command prompt, type **Get-DnsClientCache | fl**, and then press Enter.
4. Get-DnsClientCache | fl
5. At the Windows PowerShell command prompt, type **ipconfig /displaydns**, and then press Enter. This should display similar information to the preceding command.
6. ipconfig /displaydns

Task 4: Create and test a hosts file entry

1. At the Windows PowerShell command prompt, type **notepad C:\windows\system32\drivers\etc\hosts**, and then press Enter.
2. notepad C:\windows\system32\drivers\etc\hosts
3. Scroll to the end of the file, type [**172.16.0.10 www**](urn:gd:lg:a:send-vm-keys), and then press Enter.
4. Click **File**, and then click **Save**.
5. Close Notepad.
6. At the Windows PowerShell command prompt, type **test-connection www**, and then press Enter.
7. test-connection www
8. At the Windows PowerShell command prompt, type **Get-DnsClientCache | fl**, and then press Enter.
9. Get-DnsClientCache | fl
10. View the www record in the cache.

Task 5: Troubleshoot name resolution

1. At the Windows PowerShell command prompt, type **nslookup LON-DC1**, and then press Enter.
2. nslookup LON-DC1
3. At the Windows PowerShell command prompt, type **Resolve-Dnsname LON-DC1 | fl**, and then press Enter.
4. Resolve-Dnsname LON-DC1 | fl
5. At the Windows PowerShell command prompt, type **nslookup -d1 LON-DC1 > file.txt**, and then press Enter.
6. nslookup -d1 LON-DC1 > file.txt
7. At the Windows PowerShell command prompt, type **notepad file.txt**, and then press Enter.
8. notepad file.txt
9. Review the information. Note that you might have to scroll to the section starting with **Got answer**.
10. What was the question that was asked of the DNS server?

**QUESTIONS: lon-dc1.Adatum.com, type = A, class = IN**

* 1. What was the response?

ANSWERS: lon-dc1.Adatum.com internet address = 172.16.0.10 ttl = 3600 (1 hour)

* 1. How long will the record be cached?

1 hour

* 1. What is the fully qualified domain name (FQDN) for the primary name server?

lon-dc1.Adatum.com

* 1. Close all open Windows.

**Results**: After completing this exercise, you should have successfully verified your DNS settings and tested name resolution.

Exercise 4: Configuring a VPN

**Scenario**

Many of your users want to be able to work from home, at least for part of the working week. It's decided to implement VPNs in the organization to facilitate this remote working. As part of this process, you decide to test VPNs in Windows 11.

The main tasks for this exercise are as follows:

1. Create a VPN.
2. Test the VPN.

Task 1: Create a VPN

1. Switch to [**LON-CL2**](urn:gd:lg:a:select-vm).
2. Open **Control Panel**, click **Network and Internet**, and then click **Network and Sharing Center**.
3. Click **Change adapter settings**, and then right-click and disable the **Ethernet** adapter.
4. Right-click and enable the **Internet** adapter.
5. Open **Settings**.
6. In the navigation pane, select **Network & internet**.
7. Select **VPN**.
8. On the VPN page, click **Add VPN**.
9. In the Add a VPN connection window, enter the following information and then click **Save**:

* VPN provider: Windows (built-in)
* Connection name: [**Adatum HQ**](urn:gd:lg:a:send-vm-keys)
* Server name or address: [**131.107.0.1**](urn:gd:lg:a:send-vm-keys)
* VPN type: Automatic

1. Click **Save**.

Task 2: Test the VPN

1. In Settings, click **Connect**.
2. In the **Windows Security** dialog box, sign in as [**Adatum\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys) and click **OK**.
3. Switch to [**LON-RTR**](urn:gd:lg:a:select-vm).
4. In Server Manager, select **Tools**, and then click **Remote Access Management**.
5. In Remote Access Management, click **Remote Client Status**. Double-click and review the connection information for your VPN client.
6. Click **Close**.

**Results**: After completing this exercise, you will have successfully created and tested a VPN connection using Windows 11.

**Congratulations!** You have now completed this lab. To continue to the next lab click End Lab in the Tools Menu . If you wish to contiue with this lab at a later date ensure you save the lab environment rather than ending it.