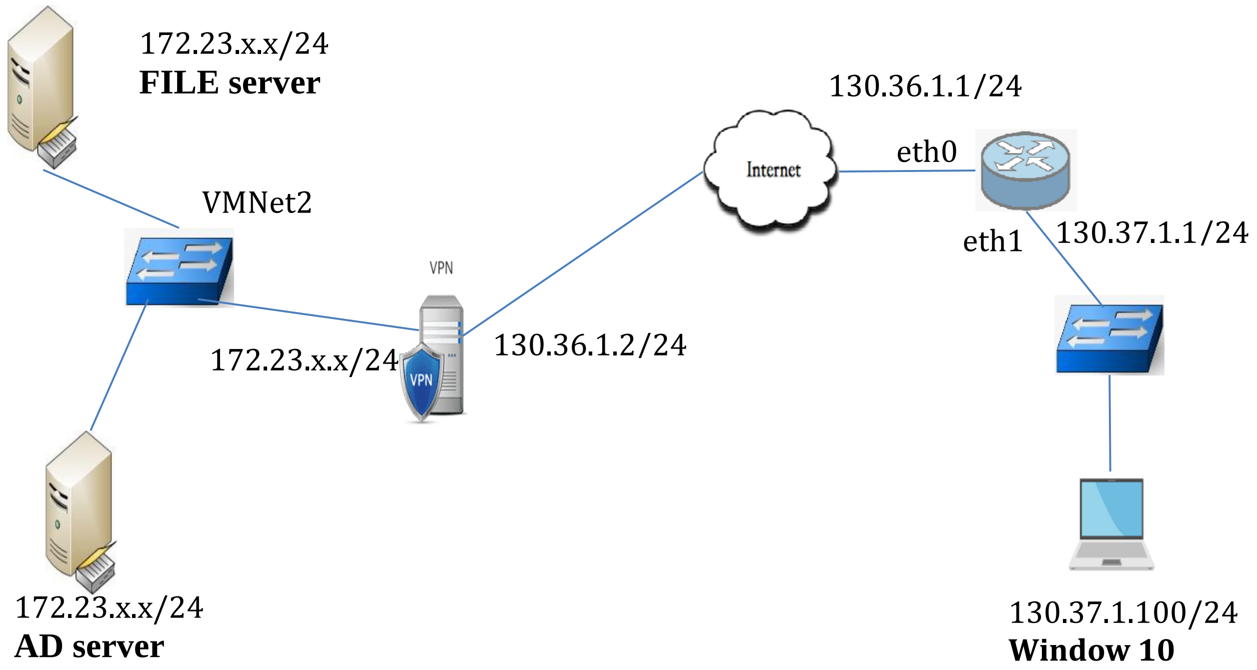
Lab 6

VPN AND DIRECTACCESS

In this lab, you are responsible for setting up a network as shown in the following figure.



EXERCISE 1: BUILD THE NETWORK USING VMWARE WORKSTATION

1. Add a windows 2016 server to play the Remote Access (RA) server role. Note that the VPN server has 2 network adapters
2. Connect host together to form the network as described in the Figure
3. Configure IP for all the host
4. For RA Server:
    a. Configure the **Internal network interface**: provide an IPv4 address and a subnet mask. DO NOT specify a default gateway! Provide the IP addresses for **DNS servers on the corporate LAN** as necessary.
    b. Configure **the External interface:**
        - Provide an IPv4 address, subnet mask, and default gateway. **DO NOT specify any DNS servers.**
        - Click on **Advanced...** and Select the **WINS** tab and **uncheck** the box next to **Enable LMHOSTS lookup**
        - Disable all protocols and services other than IPv4 and IPv6 to reduce the attack surface of the DirectAccess server.
5. Join RA server to domain controller
6. Using the Linux to act as the router into the network (the image of the router is provided by the teacher).
7. Print the routing table of the router

8. Check that the client can contact the RA server but make sure that the client cannot reach the internal server

EXERCISE 2: INSTALL AND CONFIGURE VPN SERVER

Step 1: Installing Remote Access role

1. On the RA server, install the **Remote Access** role
2. During the installation, select: DirectAccess and VPN (RAS)
3. Open the **Remote Access Management** Console (Tools -> **Remote Access Management**)
4. Select **Direct Access and VPN** on the left and then click to **Run the Remote Access Wizard**

Step 2: Configure and Enable Routing and Remote Access on Server 2016

5. Open **Remoting and Remote** Access
6. Right click on the Server's name and select **Configure and Enable Routing and Remote Access**
7. Choose **Custom configuration** and click **Next**
8. Select **VPN access only** in this case and click Next
9. Finally click **Finish**

Step 3: Configure VPN Server Settings (Security, IP Range, etc.)

10. At **Routing and Remote access** panel, right click on your server's name and select **Properties.**
11. At 'Security' tab, select the **Windows Authentication** as the Authentication Provider and then click the **Authentication Methods** button.
12. Make sure that the **Microsoft encrypted authentication version 2 (MS-CHAP v2)** is selected and then click **OK**
13. Now select the IPv4 tab, **choose** the **Static address pool** option and click **Add**.
14. Now type the **IP Address Range** that will be assigned to VPN clients and click **OK** twice to close all windows.

Step 4: Allow Routing and Remote Access Inbound Traffic in Windows Firewall

15. Go To **Control Panel -> All Control Panel Items** > **Windows Firewall**
16. Click **Advanced settings** on the left.
17. Select **Inbound Rules** on the left
18. At the right pane, double click at **Routing and Remote Access (PPTP-In)**
19. At 'General' tab, choose **Enabled**, **Allow the connection** and click **OK**.
20. Then double click at **Routing and Remote Access (GRE-In)**
21. At General tab, choose **Enabled**, **Allow the connection** and click **OK**.
22. **Close** the Firewall settings and **restart** your server

Step 5: Select which users will have VPN Access

23. On AD server open **Server Manager**
24. From **Tools** menu, select **Active Directory Users and Computers**
25. Select **Users** and double click on the user that you want to allow the VPN Access.
26. Select the **Dial-in** tab and select **Allow access**. Then click **OK**.

Note: In order for VPN client to communicate with internal servers (networks), internal router has to configure the route for the IP range of VPN networks

EXERCISE 3: SETUP VPN CONNECTION FOR CLIENT

1. On windows 10, From **Settings** click **Network and Internet** (OR, **right click** at the **Network** icon on the taskbar) and choose **Open Network & Internet settings**.
2. Click **VPN** on the left and then click + to Add a VPN connection.
3. At the next screen, fill out the following information and click **Save**:

   + **VPN provider**: Select **Windows (built-in).**
   + **Connection name**: Type a friendly name for the VPN connection. (e.g.. "VPN_OFFICE")
   + **Server name or address**: Type the VPN's server host name or the public IP address
   + **VPN Type**: Use the drop down arrow to select the type of the VPN connection that your company uses. {e.g. "Point to Point Tunneling Protocol (PPTP)"}.
   + **Type of sign-in info**: Use the drop down arrow and select the authentication type for the VPN connection. (e.g. "User name and password").
   + **User Name**: Type the VPN user name.
   + **Password**: Type the VPN password
   + **Check** the "Remember my sign-in info" checkbox, if you want to save your sign-in credentials for the VPN connection and then click **Save**

4. Under **Related settings**, choose **Change adapter options**
5. **Right click** on the **VPN connection** and choose **Properties**
6. At **Security** Tab, select **Allow these protocols,** and check the following protocols:

   - **Challenge Handshake Authentication Protocol (CHAP)**
   - **Microsoft CHAP Version 2 (MS-SHAP v2)**

7. At **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
8. Click **Advanced**.
9. Now you're ready to connect to your VPN Server 2016.

Note: verifying that VPN work and client can reach the internal server via VPN

EXERCISE 4: INSTALL AND CONFIGURE DIRECTACCESS

A. Creating DirectAccess OU & Group in Active Directory

1. Create a new OU named "**DirectAccess Clients**"
2. Create a Group named **"DA Clients"** inside OU "**DirectAccess Clients**"
3. Right-click **DA Clients,** and then click **Properties.**
4. In the **DA Clients Properties** dialog box, click the **Members tab**, and then click **Add** and then click **Object Types.**
5. Click **Computers** check box, and then click **OK.**
6. **Enter the** object names **to select (examples)** box, type **<computer name>** of DA clients, e.g., **DAClient1**, and then click **OK. (note:** These are computers allowed to use DirectAccess services

B. Installing the Remote Access server role

(Already done in Exercise 2)

C. Configure DirectAccess

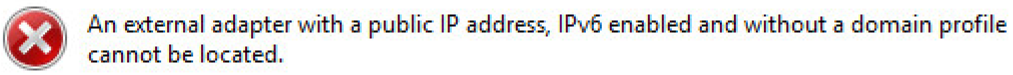
1. On RA Server. Open Server Manager: **Tools -> Remote Access Management**

2. Click on **VPN** under the Configuration and the double-click on **Enable DirectAccess** on the right-side pane to open **Enable DirectAccess** Wizard. This Wizard will get us through steps in settings DirectAccess

3. In **DirectAccess Client Setup page**, in the **Select Groups** click **Add…** to add the group containing clients computers that will be enabled for DirectAccess (created at the previous step i.e., DA Clients)

4. **On the Network Topology** page, verify that **Edge** is selected**,** in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server, *type 130.36.1.2,*** and then click **Next.**

   *If you get the following error, you need to resolve is routing between your DMZ and Domain for this server by disabling **Routing and Remoting Access** (and Disbaled and tehnEnable the External network interface)*

   An external adapter with a public IP address, IPv6 enabled and without a domain profile cannot be located.

   After the **DirectAccess setup** Wizard finish, click on the **DirectAccess and VPN** to edit the configuration

5. **Step 3 – Infrastructure Servers**: Click on **Edit…** button under the Step 3 Infrastructure Servers

   Click the Radio next to **"The network location server is deployed on a remote web server (recommended)** and input the URL for NLS server, e.g., https://nls.clc.com

Network Location Server ***(NLS)*** *– is a server through which the client can determine that it is on the internal network of the organization, i.e. you do not need to use DA to connect. NLS server can be any internal web server (even with a default IIS page), the main requirement is that the NLS server must not be accessible from outside the corporate network. This web site doesnot require any special content (Only the Web server installed and running).*

To create a Certificate for NLS serrevr using the following Powershell Cmdlets

New-SelfSignedCertificate –DnsName ***nls.clc.com*** *–certStoreLocation cert:\LocalMachine\My*

D. Test Direct Access on the Windows Client

DirectAccess only works on Windows 10 Enterprise of Windows 10 Education

For each client, we need to do 2 steps:

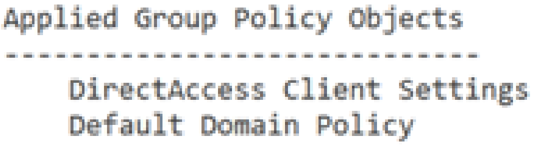
1) Join to the domain locally (from inside network)
2) Move the client outside (Access the network from home, i.e., from Internet)

For this exercise, we first plug our computer into the internal network. To do this, we connect Windows 10 computer to VMNet2 and change the IP address accordingly. Then, do the following:

1. Log on windows 10 client and join to the domain (ensure that the computer name must be belong to the **DA Clients** group) the restart the windows 10 when requested.
2. Sign in again using the domain account (e.g., clc\administrator)
3. Open a **Command Prompt window,** and then type the following commands, pressing **Enter at the end of each line:**

```
Gpupdate /force
gpresult /R
```

4. Verify that **DirectAccess Client Settings** GPO displays in the list of **Applied Group Policy objects** for the Computer Setting, **Close the** Command Prompt window.



```
Applied Group Policy Objects
-----------------------------
    DirectAccess Client Settings
    Default Domain Policy
```

Note:

If the ***DirectAccess Client Settings*** *GPO displays in the list of* ***Applied Group Policy objects, log in the DC*** *and add the computer to DA Clients group, then repeat step 4.*

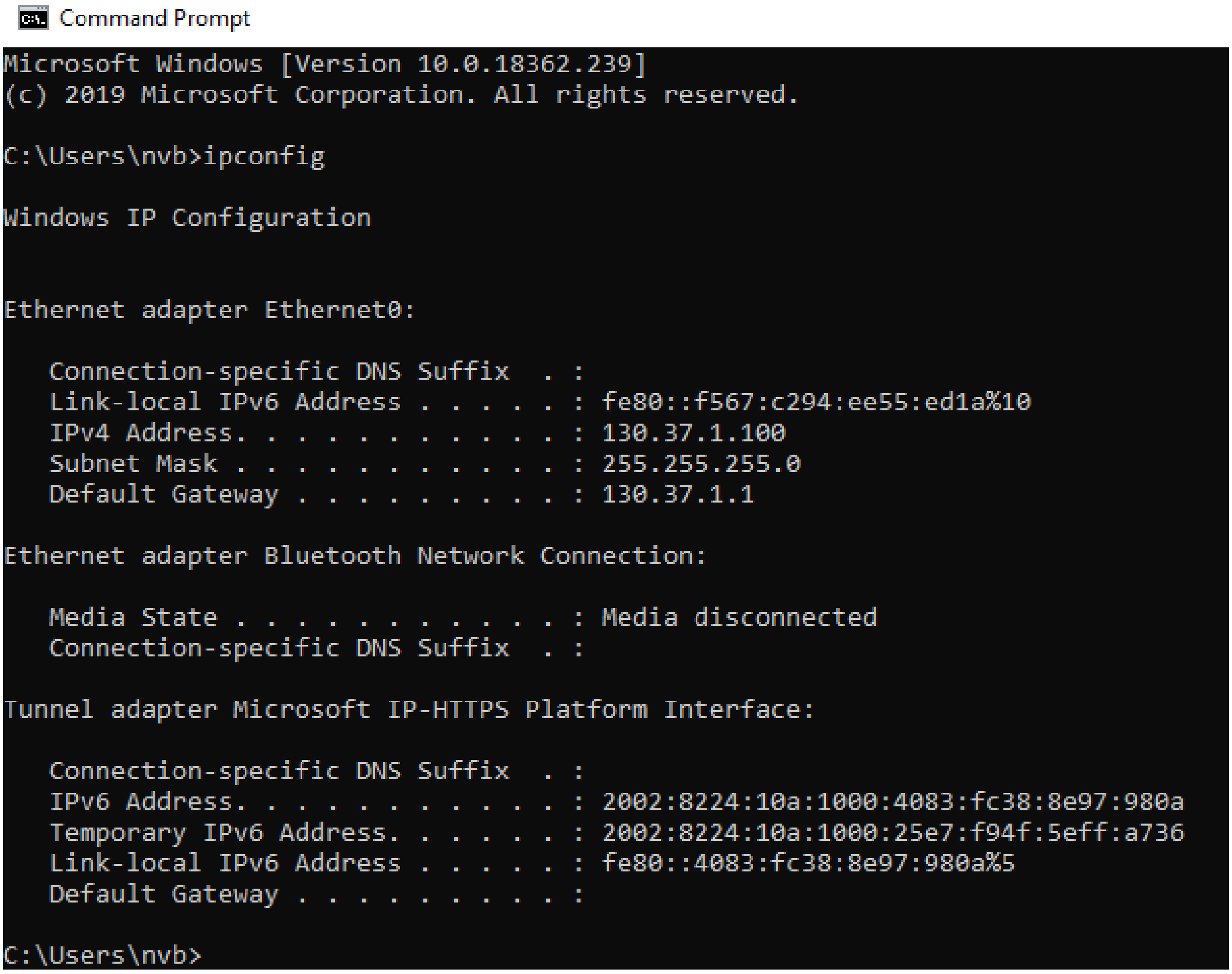
If it is still not working, Log in to Domain controller and do the following steps:

ii) *Open Active Directory Users and Computers, then move the DA client computer to OU "Direct Access Client"*

iii) *Open Group Policy Management Tools, Right-click on OU DirectAccess Client and choose Group Policy Update ...*

iv) *Repeat step 4*

6. Move the computDAClienter to external network, i.e., change the connection off Windows 10 computer to VMNet4 and change IP address as shown in the above figure.
7. Login to Windows 10 using, open a **command prompt,** type the following command, and then press Enter: **ipconfig**



```
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\nvb>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f567:c294:ee55:ed1a%10
   IPv4 Address. . . . . . . . . . . : 130.37.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 130.37.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Microsoft IP-HTTPS Platform Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:8224:10a:1000:4083:fc38:8e97:980a
   Temporary IPv6 Address. . . . . . : 2002:8224:10a:1000:25e7:f94f:5eff:a736
   Link-local IPv6 Address . . . . . : fe80::4083:fc38:8e97:980a%5
   Default Gateway . . . . . . . . . :

C:\Users\nvb>
```

Notice the IPv6 address that starts with 2002. This is an IP-HTTPS address

8. At the command prompt, type the following command, and then press Enter:

Netsh name show effectivepolicy

9. In Settings, select Network & Internet**,** and then click DirectAccess

Verify connectivity to the **DirectAccess** server

Note: testing to make sure that VPN work: outside client can reach the internal server