# Windows Server – Setup and Configuration

# Section 5 – Network Services (DHCP, VPN)

Machines:

* 1 Windows Server 2016
* 1 Windows 10 Client Machine

## Part 1: Installing the DHCP role

Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses and other important IP configuration information to computers in a network. While it would be possible to run an IP network without using DHCP, the administrative effort would be prohibitive except in the smallest of networks.

DHCP is a non-authoritative protocol which means that (unlike DNS) you can’t restrict what computers are allowed to get DHCP information. Any computer sending a request to a DHCP server will get a response even if the computer is not a member of the Active Directory Domain.

Certain computers in a network will not use DHCP for configuration. These include the main infrastructure servers including domain controllers, DNS servers and DHCP servers. These machines should always have their IP configuration set manually with what are called Static IP address. Most of the other computers in the network will get their IP configuration data from a DHCP server.

* Start the **server** computer and log on with our personal administrative credentials.
* In Server Manager click on the **Manage** menu and select **Add Roles and Features.** This will take you to the Add roles and Features Wizard.

Graphical user interface, table

Description automatically generated

* Accept defaults as you work through the wizard until you get to the Server Roles section. When you click on the box to check DHCP you will immediately get a window asking if the DHCP management tools should also be installed. Click on Add Features to accept the management tools.

Graphical user interface, application, Word

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

* Click on Next after you have accepted the tools and you will be taken to the Features menu. Do not select any features. You only want the DHCP role and its associated management tools.
* You can click next to finish the wizard and at the last screen you click on Install to complete the wizard.
* You will get a progress bar after clicking install showing the status of the installation. The installation should only take a couple minutes. Note on completion that you are given a link to complete the DHCP configuration. Click on this link.

Graphical user interface, text, application, email

Description automatically generated

* The DHCP Post Install configuration wizard will start. The Description screen tells you about two new security groups that will be created in this process. Take note of them, then click Next.
* The next screen asks for credentials that will be used to “Authorize” this DHCP server to function in the Active Directory domain. Authorization is a process to help assure that the only DHCP server that will give out addresses on the network are those set up and controlled by administrators. You can accept the default of your own account as long as that account is member of the domain admins security group. You accept this by clicking on the Commit button.

Graphical user interface, text, application, email

Description automatically generated

* When finished you will be returned to the final page of the Add roles and Features wizard which you can now close.
* You will now notice a number 2 next to the flag icon on the Server Manager menu bar. When you click on this you should see that it shows that Feature installation was run and that the Post Deployment Configuration was completed.

Graphical user interface, text, application, chat or text message

Description automatically generated

## Part 2: Configuring DHCP

In order to give out IP addresses, the DHCP server needs to be given a “scope” which is a range of IP addresses that the server can administer. In a typical network, some addresses are always assigned statically such as those for the default gateway, domain controllers, DNS servers and DHCP servers. To prevent those numbers from being given to client computers, they will be excluded from the scope by being included in an Exclusion range. An Exclusion range is configured when you want certain addresses withheld by the server. In this lab you create a scope and then exclude a few addresses for static assignment.

* From the Tools menu of Server Manager select the DHCP option. This will open the DHCP module.

Graphical user interface, text, application

Description automatically generated

* In the left pane of the DHCP module expand the IPv4 icon. Then right click on the icon and select New Scope. This will open the New Scope wizard.
* You can give the scope any name and description you want. For lack of anything more original, you can call the scope LabScope and leave the description blank.
* The IP Address Range dialog box is very important. This page gives you critical settings that cannot be changed without deleting the scope and starting over, so you want to be sure the values are what you want.
* Use the entire Class C (/24) network for the scope. **The third octet of your network will be different than that shown in the screen shot below.** Use the correct IP addresses for your network.

Graphical user interface, text, application

Description automatically generated

* Set the Exclusion range for the first 20 address in your scope. This will prevent the DHCP server from giving these addresses out dynamically. They can be used for static IP addresses for servers.

Graphical user interface, text, application, email

Description automatically generated

* Take note of the default Lease duration in the next windows.
* At the **Configure DHCP options,** select **No, I will configure these options later**. The reason you do this is that the wizard doesn’t offer all the options you may need, and you must learn to add or change options manually.

Text

Description automatically generated

* When you finish the wizard, you will be taken back to the DHCP module and will be able to see your scope. Expand the Scope folder. [Note the very small red arrow on the Scope folder icon. This indicates that the scope has not been activated. That means that it will not give out addresses until you activate it.]
* Click on the **Address Pool** folder and you should see your address range and the exclusion range.

Graphical user interface, text, application, chat or text message

Description automatically generated

* Left click on **Scope Options** and you will get a description of the Scope Options in theright-hand pane.
* Right click on **Scope Options** and select **Configure Options.**
* Click on the check box for 003 Router. This is actually the Default Gateway setting that will be sent out to all the clients receive IP addresses from this scope.
* Enter the Default Gateway address for your network by filling in the IP Address line and clicking Add. Your default gateway address will not be the same as the screen shot.

Graphical user interface, text, application

Description automatically generated

* Scroll down through the options to option 006 DNS Servers and add the address of your server computer which is the DNS server for your small network.
* For Option 15 add the domain name of your network.
* Click OK to save your Scope Options.
* Now that your scope is ready, you can Activate it. Right click on the Scope folder and select Activate. The small red arrow should disappear after activation. Do not continue if you still see the red arrow

Graphical user interface, application

Description automatically generated

Your scope is now ready to give out IP configuration information to any requesting clients.

## Part 3: Testing DHCP

* Start the **client** and log on with your personal domain credentials.
* Open Network and Sharing center (Hint: icon on the taskbar near the clock) and click on Change adapter settings.
* Right click on the Ethernet icon and select Properties.

Graphical user interface, application

Description automatically generated

* Select Internet Protocol Version 4 and click the Properties button.
* Configure your static IP address so the last octet is 15. Your settings will not exactly match the screen shot. Use the correct IP addresses for your network if they are different from those shown in the screen shot.

Graphical user interface, text, application

Description automatically generated

* Save these settings.
* Now go back to the IPv4 Properties settings and click both radio buttons to Obtain an IP address automatically. This tells the system to use DHCP.

A picture containing graphical user interface

Description automatically generated

* Click OK and Close to save the settings.
* Run ipconfig again and see if the address has come from DHCP. The only change should be the last octet in the IPv4 address.

**IPv4 address:**

**Subnet Mask:**

**Default Gateway:**

If a DHCP client computer cannot reach a DHCP server it will assign itself and IP address in the Automatic Private Address range (APIPA) in the 169.254.0.0 /16 network. In the next steps you will see this happen.

## Part 5: Configuring a server VPN

Part 1: Install the VPN Role to SRV16

Before you can connect your client to the server VPN you must install the VPN role to your server. This is done through the Server Manager.

* Start your server and log on with your personal administrative credentials.
* Turn off the firewall

Graphical user interface, text, application, email

Description automatically generated

* From the Server Manager choose **Add roles and features**.
* Leave the default **Role-based or feature-based installation.**

Graphical user interface, text

Description automatically generated

* Select the **SRV16** server and click next

Graphical user interface, text, application, email

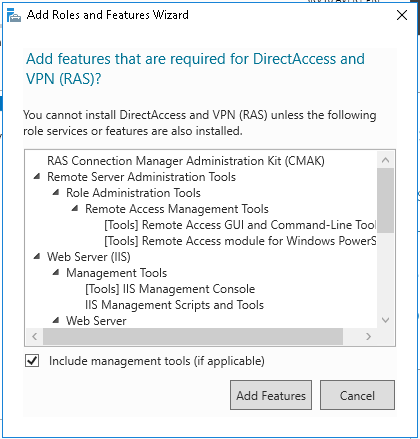
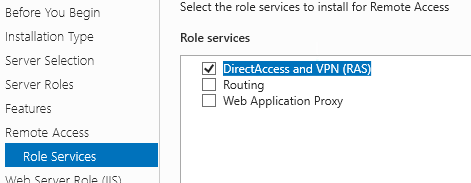
Description automatically generated

* From the list of server roles choose ‘**Remote Access’**

Graphical user interface, application

Description automatically generated

* Leave the ‘**features’** list as default and click ‘**Next’**
* Click ‘**Next’** to begin installing the **‘Remote Access’** services.
* Select the **‘DirectAccess and VPN (RAS)**’ role service and then click ‘Add Features’ on the next dialog box. Click ‘Next’ when finished.



* Leave the Web Server (IIS) role services as default and click ‘Next’.
* Leave the ‘Confirmation’ dialog as default and click ‘Install’
* When the installation is finished click ‘Open the Getting Started Wizard’.

Graphical user interface, text, application, email

Description automatically generated

* Select ‘Deploy VPN only’

Graphical user interface, text, application

Description automatically generated

* On the ‘**Routing and Remote Access’** snap-in right-click on the ‘SRV16 (local) server and select ‘**Configure and Enable Routing and Remote Access’**

Graphical user interface, text, application, email

Description automatically generated

* Click ‘Next’ on the initial screen dialog box then select ‘Custom configuration’ on the Configuration dialog box.

Graphical user interface, text, application

Description automatically generated

* Choose ‘VPN access’ then click ‘Next’

Graphical user interface, text, application

Description automatically generated

* Click ‘Finish’
* Click [Start service]

Graphical user interface, text, application, email

Description automatically generated

* In the ‘Routing and Remote Access’ snap-in right-click the server (local) system and select ‘Properties’.

Graphical user interface, text, application, email

Description automatically generated

* From the ‘IPv4’ tab, select ‘Static address pool’ and [**Add**] the range of 5 addresses in your network. Example for a 192.168.1.0 network:

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text

Description automatically generated

* Once again right-click the <domain controller> (local) system > All Tasks > Restart.

Graphical user interface

Description automatically generated with low confidence

* Once done, go to ‘Active Directory Users and Computers’ and go to the properties of the **Administrator** account. On the ‘Dial-in’ tab set the ‘Network Access Permission’ for (\*) Allow access.

Graphical user interface, text, application

Description automatically generated

* Now you’ll need to ensure that ALL VPN traffic from the client machine goes through this connection. Do this by editing the ‘Local Group Policy’ with: **GPEDIT.MSC:**  
  **Computer Configuration\Administrative Templates\Network\Network Connections\Route all traffic through the internal network > Disable.**
* Now All of the Win10 network traffic will be forced through the secure VPN traffic. We’ll check this later.

## Part 4: Create Client VPN Network Connection to the domain controller

* Log into the client system with your personal domain administrative account.
* Open the ‘Network’ connections settings and click ‘VPN’ in the left side menu and click ‘Add a VPN connection’

Graphical user interface, application

Description automatically generated

* Configure the VPN connection for the server as shown below and click [Save] when finished.

Graphical user interface

Description automatically generated

* Once done, click ‘**Change adapter options’** in the ‘Related settings’ section.
* Right-click on the <servername>-VPN network connection and select ‘Properties’.

Graphical user interface, text, application

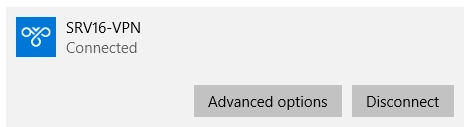
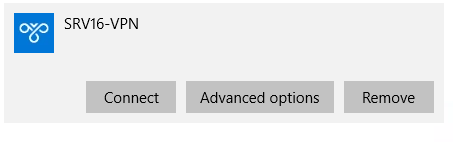
Description automatically generated

* On the ‘Security’ tab ensure the settings for ‘Data encryption:’ is set for ‘Optional encryption (connect even if no encryption) and that the ‘Authentication’ is set for ‘Use Extensible Authentication Protocol (EAP) is selected, as shown. Click ‘OK’ when done.

Graphical user interface, text, application, email

Description automatically generated

* Return to the VPN network settings page and click the ‘<domaincontroller>-VPN’ connection and then click [Connect].



* Once connected to the VPN, open a Command Prompt (CMD) and run ‘ipconfig’. You should see the VPN connection with an IPv4 Address within the configuration range set on the domain controller earlier.

Text

Description automatically generated

* Open the ‘Network Connections’ control panel and right-click the ‘Ethernet0’ connection and select ‘Status’. Do the same for the VPN connection.

Verify that network traffic bytes are being ‘sent’ and ‘received’ across both connections.