# Lab Answer Key:  Module 5: Virtual Networking

## Lab 1: Configuring User Defined Routes

### Exercise 1: Configuring User Defined Routes

The tasks for this exercise are as follows:

1. Deploy a resource group template
2. Review the template deployment
3. Configure Routing and Remote Access for an Azure VM
4. Reset the lab environment (optional)

#### Task 1: Deploy a resource group template

1. Login to your Azure account at https://portal.azure.com
2. You will use a template from the GitHub quickstart repository to set up the lab environment. Launch a browser and navigate to https://github.com/Azure/azure-quickstart-templates/tree/master/201-userdefined-routes-appliance.
3. Click the **Deploy to Azure** button at the bottom of the page
4. Specify the following values:

* Subscription: the name of your Azure subscription
* Resource group: ensure that the **Create new** option is selected and assign the name **UDR** to the new resource group
* Location: the closest Azure region to your location
* New Storage Account Name: provide unique storage account name (lower case letters and digits only)
* Admin Username: **demouser**
* Admin Password: **DemoPa$$w0rd**
* Unique Dns Prefix for VM: a unique prefix that will be used to generate public DNS name for VMs. You might need to attempt a few names in order to pass the validation stage
* Vm Name Prefix: **vm**
* Public IP Address Type: **Dynamic**
* Windows OS Version: **2012-R2-Datacenter**
* I agree to the terms and conditions stated above: checked on

1. Click **Purchase** to start the deployment. Wait until the deployment completes. This should take about 5 minutes.

#### Task 2: Review the Template Deployment

In this task we will review the deployment to understand the virtual machines and routes that were created.

In the Azure portal, click **More Services**. In the list of services, click **Route tables**. On the **Route tables** blade, click **BasicNVA** and then, on the **BasicNVA** blade, click **Routes**. Next, click the entry represeting the route in the route table. This will show you that traffic to the 10.1.2.0/24 subnet (**BackEndSubnet**) originating from **FrontendSubnet**, with which the route table is associated, is supposed to flow via 10.1.1.4. This is the IP address of **vm1**, which will function in this case as a router (once you configure it later in this exercise). If you look at the resource template file that we used for this deployment, avalable at https://github.com/Azure/azure-quickstart-templates/blob/master/201-userdefined-routes-appliance/azuredeploy.json, IP forwarding is enabled on the vm1.

#### Task 3: Configure Routing and Remote Access for the Appliance VM

1. Login to the **vm0** (FrontEndSubnet) VM with the credentials you specified during the template deployment
2. Once logged in, start Command Prompt by right clicking on the Windows logo in the bottom left corner and clicking **Command Prompt (Admin)**.
3. From the command prompt on **vm0**, run tracert vm2. Based on the routing table you would expect to reach vm2 on the BackendSubnet via vm1 on NVASubnet. However, at this point, tracert returns Request timed out. There are two reasons for it:

* You need to configure **vm1** (NVASubnet) as a router.
* You need to allow for ICMP traffic on both **vm1** (NVASubnet) and **vm2** (BackendSubnet).

1. Minimize vm0 RDP session window and connect via RDP to the **vm1** VM with the credentials you specified during the template deployment.
2. Once you are connected to vm1, right-click on the Windows Logo in the bottom left corner, click **Run** and enter **Services.msc**.
3. In the Services console, locate **Routing and Remote Access** service, right-click on it and click **Properties**. Change the **Startup** type from **Disabled** to **Automatic** and click **OK**. Then right-click on the service and click **Start**. This service implements routing over LAN and WAN.
4. Right click on the Windows Logo in the bottom left corner, click **Run** and enter **wf.msc**.
5. In the **Windows Firewall with Advanced Security** console, click **Inbound Rules**. Locate the **File and Printer Sharing (Echo Request – ICMPv4-In)** rule, right-click on it and click **Enable Rule**.
6. Minimize vm1 RDP session window and connect via RDP to the vm2 VM.
7. Once you are connected to vm2, right-click on the Windows Logo in the bottom left corner, click **Run** and enter **wf.msc**.
8. In the **Windows Firewall with Advanced Security** console, click **Inbound Rules**. Locate the **File and Printer Sharing (Echo Request – ICMPv4-In)** rule, right-click on it and click **Enable Rule**.
9. Minimize vm2 RDP session window and switch back to the vm0 VM and run tracert vm2 again. This time you can see the traffic reaching vm2, with vm1 as the hop 1.

#### Task 4: Reset the lab environment (optional)

Note: To minimize charges associated with running the lab environment, you should consider removing its resources. This is the purpose of this task.

Note: If you want to keep your lab environment in place, then you might want to consider stopping both virtual machines. This will eliminate compute charges associated with keeping these virtual machines online. To ensure that these charges do not accrue, stop the virtual machines from the Azure portal and ensure that they are listed on the Virtual machines blade with the Stopped (deallocated) state (rather than Stopped).

1. In the Azure portal, in the hub menu, click **Resource groups**
2. On the Resource groups blade, click **UDR**
3. On the **UDR** blade, click **Delete**
4. On the **Are you sure you want to delete "UDR"?** blade, type **UDR** in the **TYPE THE RESOURCE GROUP NAME** text box, and click **Delete**