WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

VNet-to-VNet Connectivity (Classic)

Student Lab Manual

V1.0, November 24, 2015

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarked, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2014 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Exercise 1 – VNet-to-VNet Connectivity 5](#_Toc436122135)

[Prerequisites 5](#_Toc436122136)

[Task 1 – Create the Virtual Networks 5](#_Toc436122137)

[Task 2 – Define the Local Networks 9](#_Toc436122138)

[Task 3 – Connect Virtual Networks to Local Networks 12](#_Toc436122139)

[Task 4 – Create the Gateways 15](#_Toc436122140)

[Task 5 – Updating the Local Network VPN device settings 16](#_Toc436122141)

[Task 6 – Supply the Security Pre-Shared Key(s) 18](#_Toc436122142)

[Task 7 – Connect the networks together 19](#_Toc436122143)

[Task 8 – Checking the network status 20](#_Toc436122144)

**Introduction to VNet-to-VNet Connectivity**

In this lab, you will create two Azure virtual networks in different Azure regions, and connect these two networks together.

You'll learn:

* How to create two Azure virtual networks
* How to define two Azure “Local” networks
* How to connect the virtual networks to Local networks
* How to create two gateways
* How to update the VPN device address

# Exercise 1 – VNet-to-VNet Connectivity

## Prerequisites

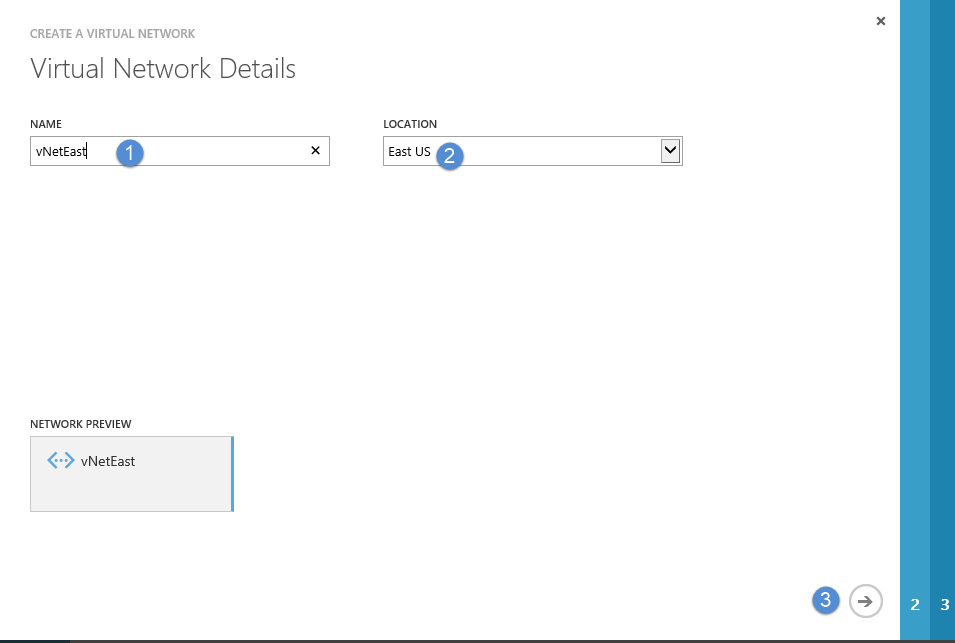
The following is required to complete this hands-on lab:

* Microsoft Azure PowerShell
* A Microsoft Azure subscription

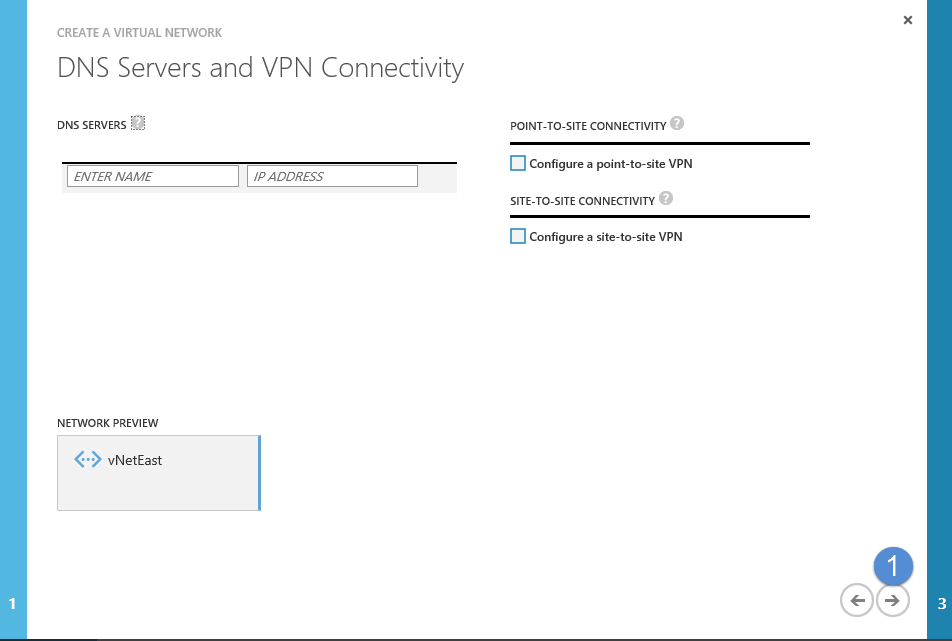
## Task 1 – Create the Virtual Networks

In this task, we will choose to create our virtual networks in two different regions, East US and Central US. You can choose whatever regions that you wish to use though, just remember to change your settings in the appropriate places while stepping through the exercise.

1. Log in to the Azure portal at <https://manage.windowsazure.com>.
2. Select the **Networks** menu item on the left side of the portal window and then select **New | Network Services | Virtual Networks | Custom Create**.
3. Enter the name of your first virtual network, the location/region and then select the **Next** arrow.

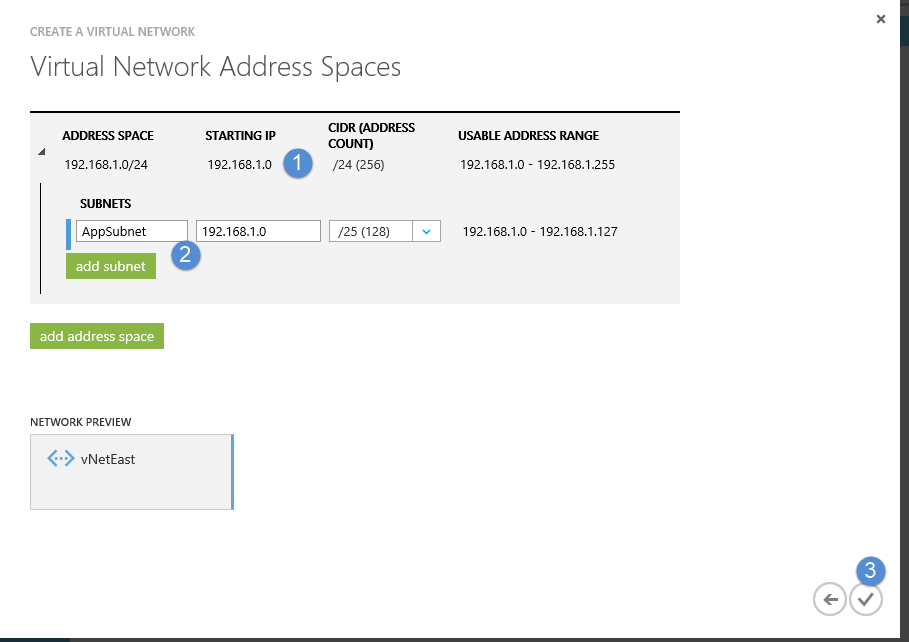


1. We will come back to the settings on this page at a later time. For now, just select the **Next** arrow.

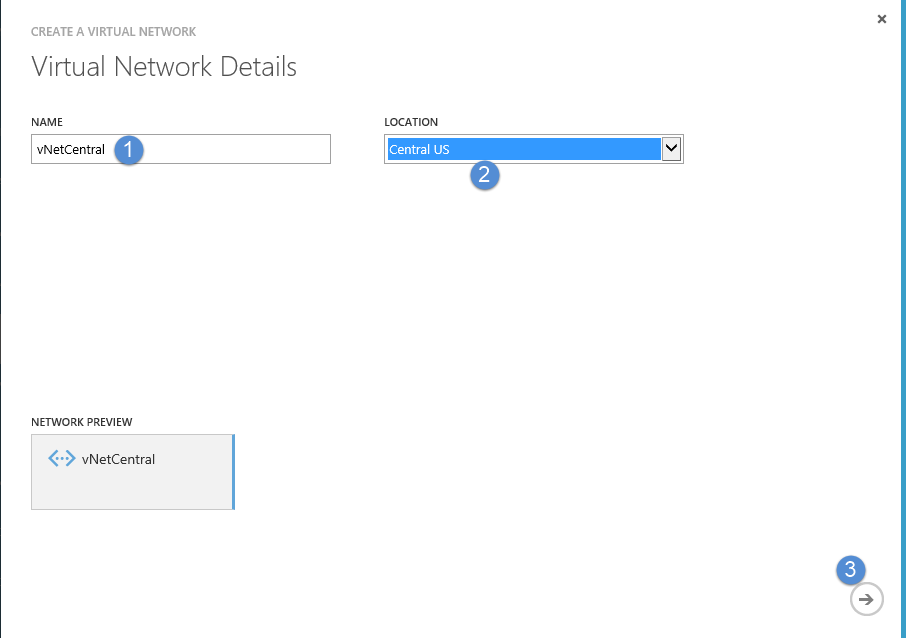


1. At this point, the internal IP address range that you choose does not matter, but, you need to make sure that whatever address range you choose will not conflict (overlap) with the address range of the other network you intend to connect to.

Enter an address range and a subnet name/address range and then select the **Finish** check button.

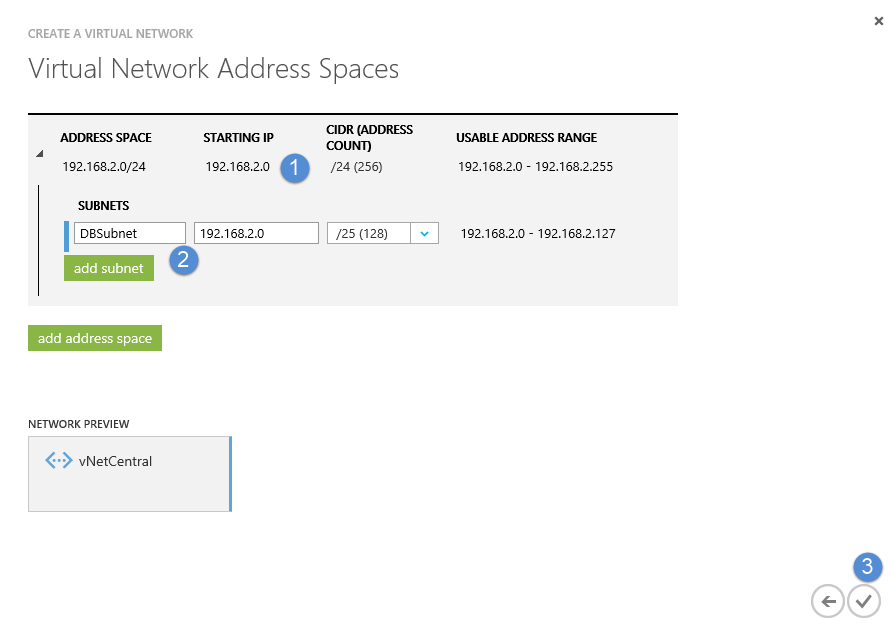


1. Select the **Networks** menu item on the left side of the portal window and then select **New | Network Services | Virtual Networks | Custom Create**.
2. Enter the name of your next virtual network, the location/region and then select the Next arrow.



1. Click the **Next** arrow on the *DNS Servers and VPN Connectivity* page.
2. Enter the IP address range and subnet for the virtual network. You will notice that this internal IP address range does not conflict with the first virtual network we created.

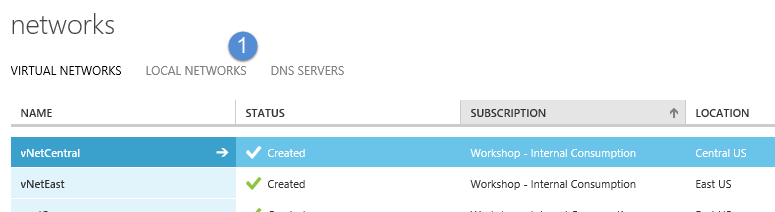
Enter the information and then select the **Finish** check button.



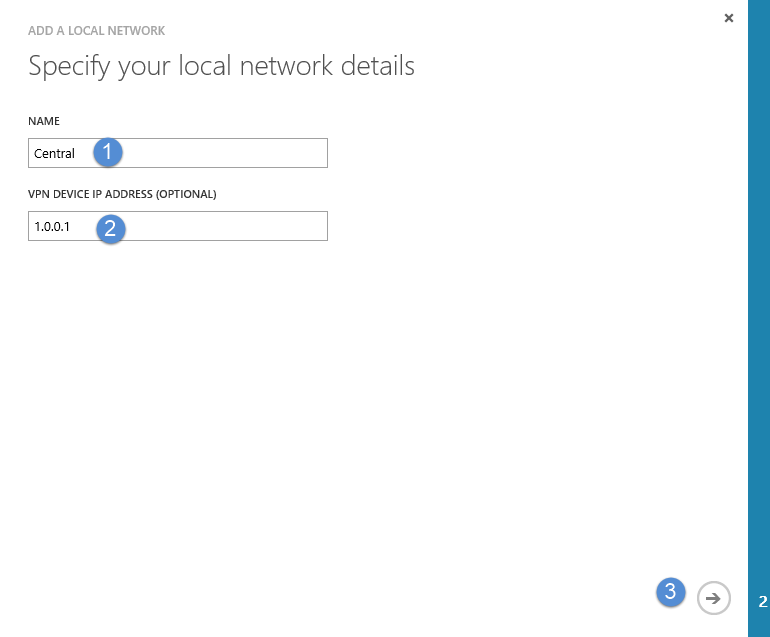
## Task 2 – Define the Local Networks

We will first define a local network that represents the virtual network we create in the Central US region. We need local networks to represent the range of addresses that the virtual networks can communicate with inside of each virtual network.

1. Inside the portal window, click on the **Local Networks** tab.

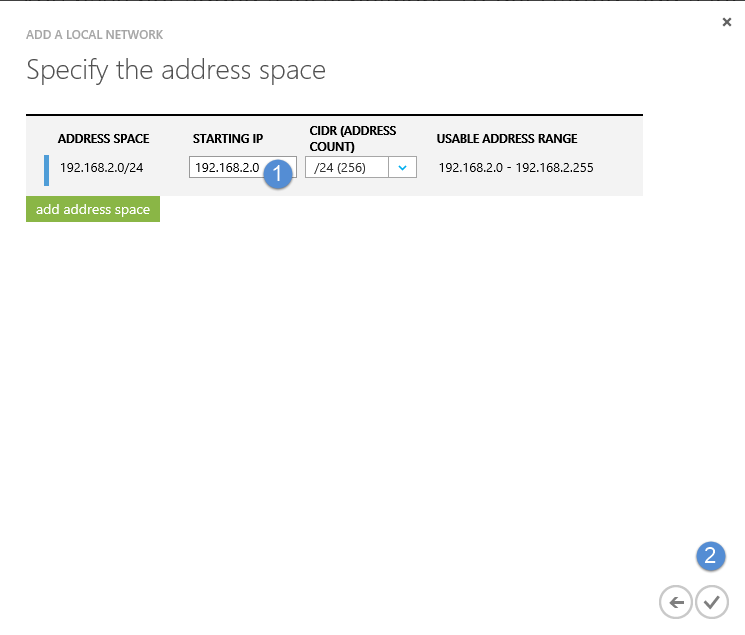


1. Click on **Add a Local Network**.
2. Enter a name for your local network and then a temporary internal IP address. This IP address is just used as a placeholder for the real, internet addressable gateway address we will supply later on. Click on the **Next** arrow. This first local network will represent the Central US virtual network.

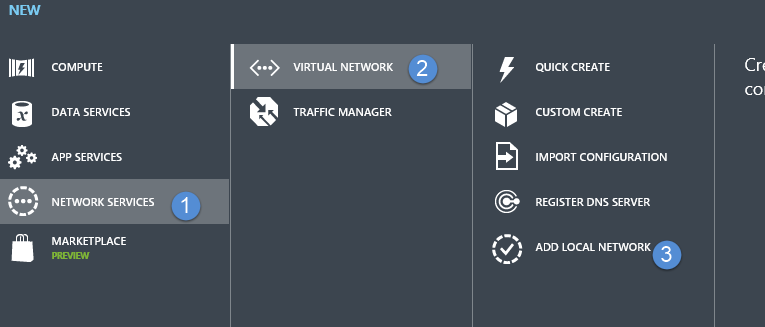


1. For the address space, enter the same address space that you created when you created your Central US virtual network. This address range signifies that we will allow the other connecting network to communicate with the entire range of IP addresses that we have in our Central US virtual network.

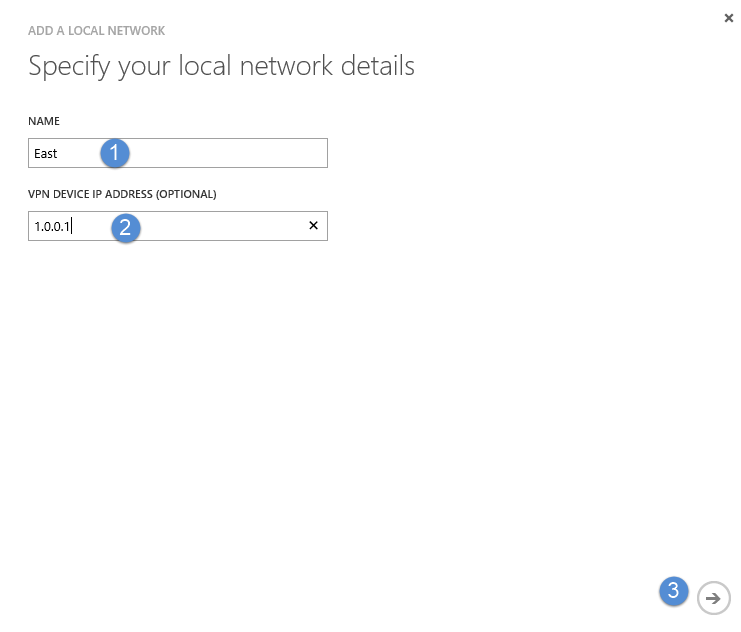
Enter the address range/starting IP address and then select the **Finish** check button.



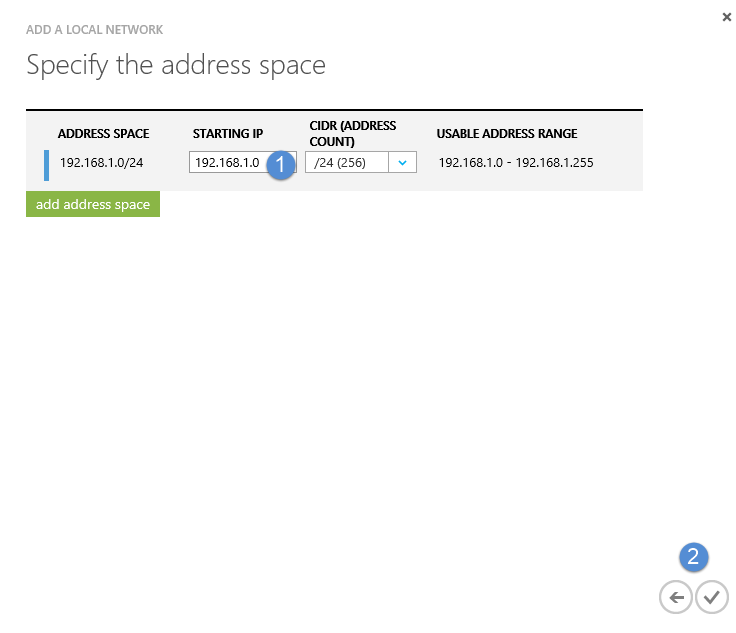
1. To create your next local network, select **New | Network Services | Virtual Network | Add a Local Network**.



1. Enter the name of your second local network and again enter the temporary placeholder IP address. Select the **Next** arrow button.



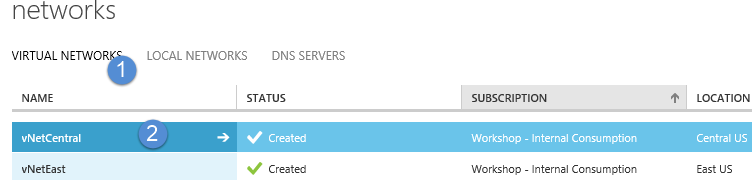
1. Enter the address range of your first virtual network, much in the same we you did for the previously created local network. Click on the **Finish** check button.



## Task 3 – Connect Virtual Networks to Local Networks

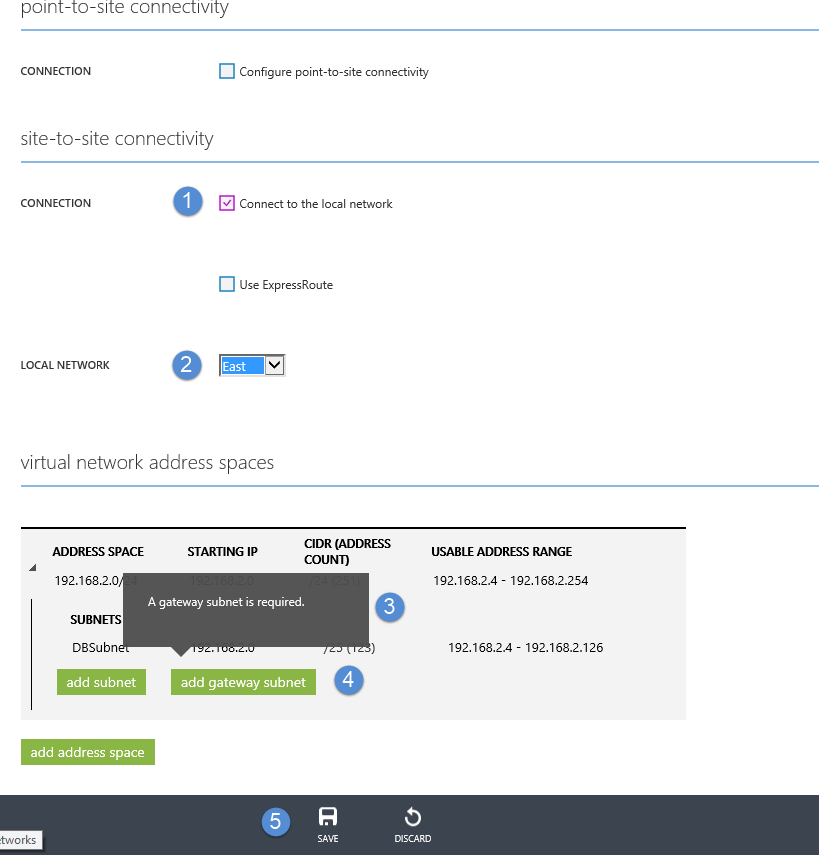
In this step, in order to connect the virtual networks together, you will follow a process where you connect the virtual networks to the *other* virtual networks LOCAL network.

1. Within the Azure portal, click on the **Virtual Networks** tab and then select the *vNetCentral* virtual network.

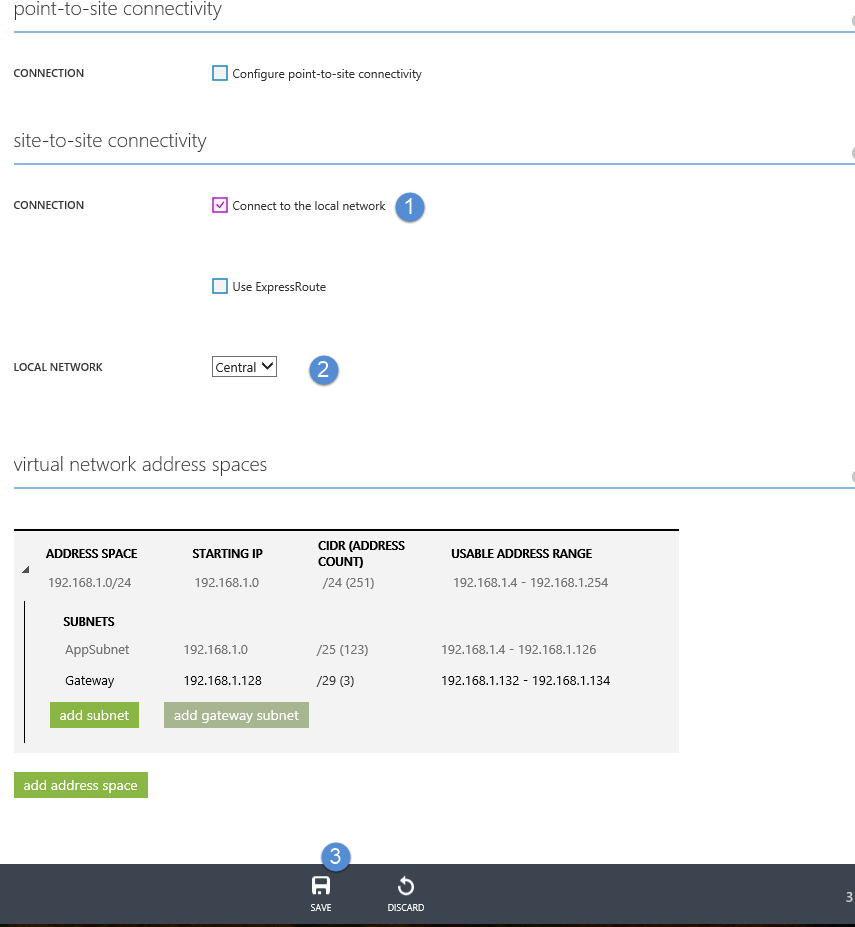


1. Go to the **Configure** tab and select **Connect to the Local Network**. Select **East** in the *Local Network* dropdown. You will also notice at the bottom of the screen a box that appears that says ‘A gateway subnet is required’.

Just under that pop-up, there is a button you need to click ‘**add a gateway subnet’**. You do not need to enter an address range, just select the button and then click the **Save** icon in the bottom toolbar. The IP address range in the gateway subnet is used internal by Azure for the two gateway machines Azure will build to handle the traffic flow.



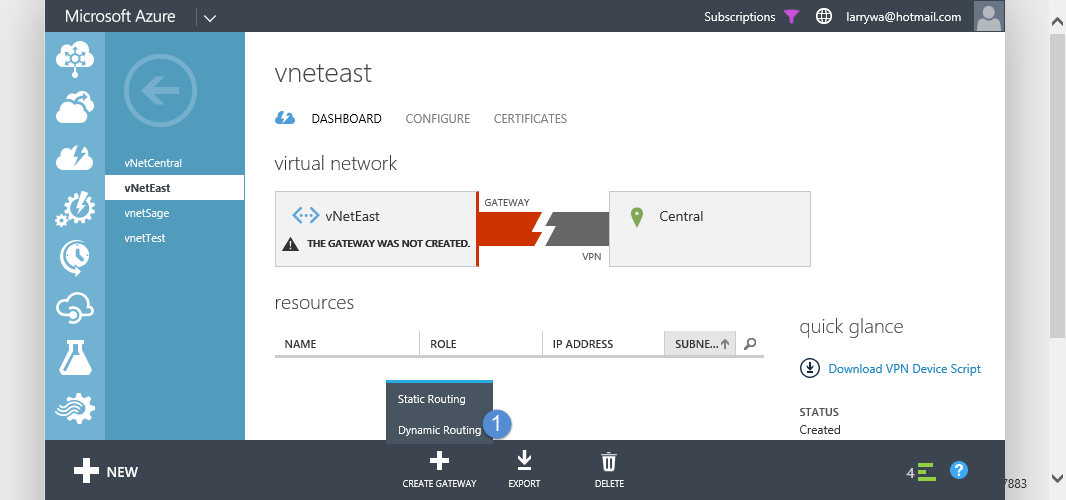
1. Next, from the Azure portal, select the **vNetEast** virtual network.
2. Select the **Configure** tab and then select **Connect to the local network** and **Central** in the *Local Network* dropdown. Notice that this time, you do not need to add a gateway subnet. That’s because we just went through the steps in the *vNetCentral* network to create a gateway subnet and now we’ve told the *vNetEast* network we’ll be connecting to that network. Select the **Save** button.



## Task 4 – Create the Gateways

The gateways will represent the public IP address that the two networks can communicate through. Inside of Azure, load balanced virtual machines are created and the IP address you will be given represents that load balancer address.

1. Within the vNetEast virtual network dashboard (click on the Dashboard tab), you will see a diagram that shows that no gateway has been created.



You will also notice a button at the bottom of the screen ‘**Create Gateway**’. You MUST choose the **Dynamic Routing** option. You will then be prompted to confirm that you want to create the gateway. Select **Yes**.

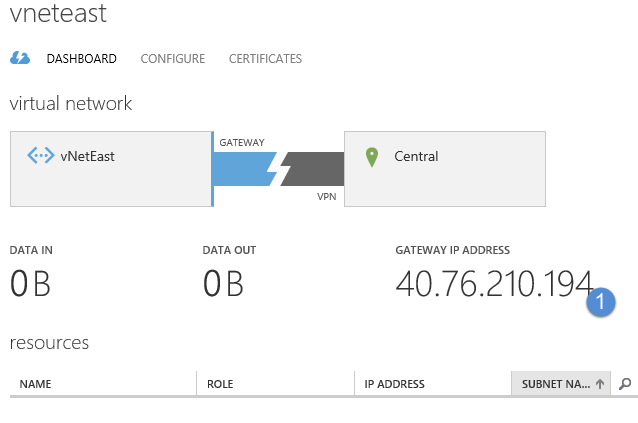
While this gateway is being created, you can go to the vNetCentral virtual network and perform the same steps.

The process of creating the gateways can take 15 to 20 minutes. You cannot proceed with the exercise until the gateway creation process has completed. You will know the process has been completed when you see a public IP address appear in the dashboard of each virtual network.

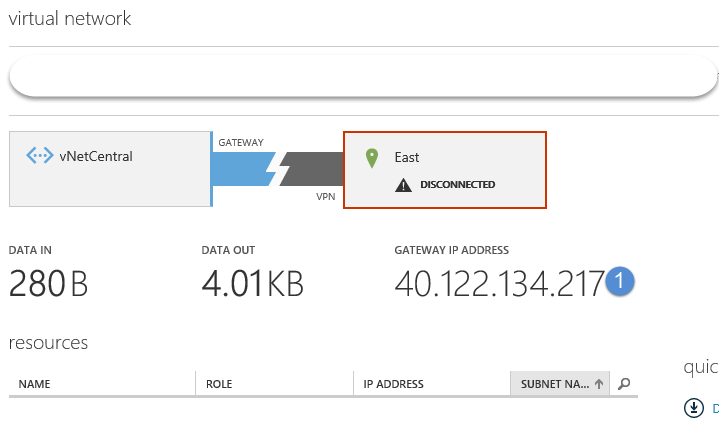
## Task 5 – Updating the Local Network VPN device settings

Once both virtual network gateways have been created, you will have two different public IP addresses that represent the entry point into the virtual networks from outside of Azure.

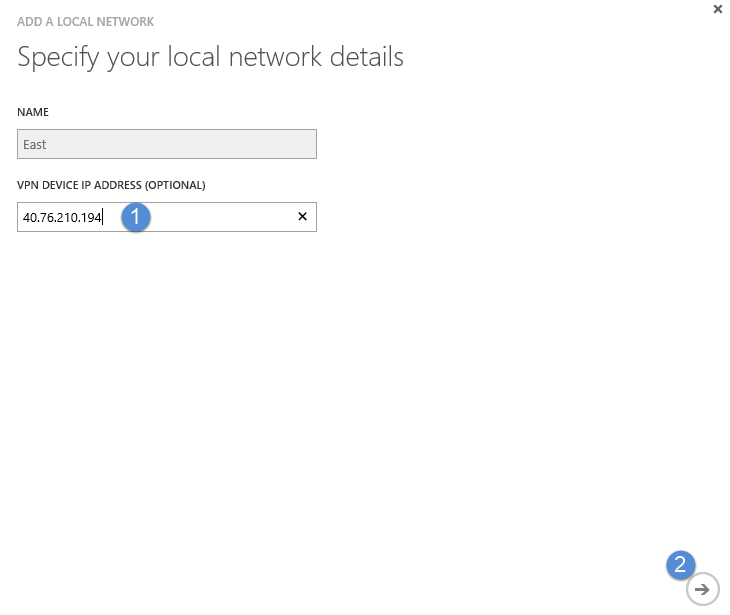
1. Go to the dashboard of *vNetEast* network. Record the value of the Gateway IP address.



1. Now, go to the dashboard of the *vNetCentral* virtual network and record the IP address of that gateway.



1. Click on the **Local Networks** tab in the Azure portal.
2. Select the **East** local network and then select the **Edit** button at the bottom of the screen.
3. Edit the **VPN device IP Address (optional)** field and put in the public IP address that Azure provided when the gateway was created. Click the **Next** button.



1. Click the **Finish** check button since no IP addresses need to be modified at this point.
2. Repeat this process for the **Central** local network using the public IP address provided for its gateway creation.

## Task 6 – Supply the Security Pre-Shared Key(s)

When the gateway was created for each virtual network, a pre-shared security key was also created for each gateway. A different key is automatically created for each virtual network.

In our case, to communicate between the virtual networks, we want the keys to be the same. We can do this either through the REST API or PowerShell..

There is no UI option for *entering* the pre-shared key values, so we must do this using PowerShell.

1. Open PowerShell ISE as an administrator.
2. Within the PowerShell ISE command window, log in to Azure using the command:  
     
   Add-AzureAccount.
3. If you have more than one subscription, you will have to select the subscription you are working with (that contains your virtual networks) into the running PowerShell instance. To do this, enter the following commands:

Select-AzureSubscription –SubscriptionId <yoursubscriptionId>

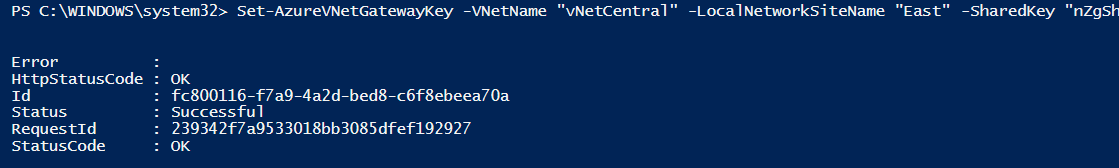
1. Enter the following commands. Note, what you can do is just make up a key or you can grab one of the already existing keys. It may be easier just to make up a simple key for testing, like ABCI23XYZ.

Set-AzureVNetGatewayKey -VNetName "vnetCentral" -LocalNetworkSiteName "East" -SharedKey "<yourSecretKey>"

Then…

Set-AzureVNetGatewayKey -VNetName "vnetEast" -LocalNetworkSiteName "Central" -SharedKey "<yourSecretKey>"

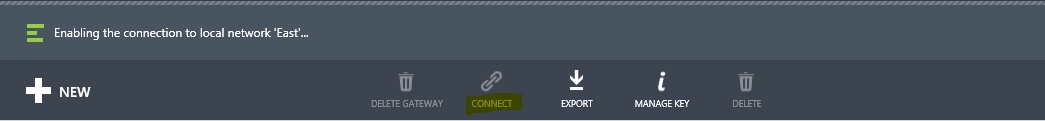
Example output:



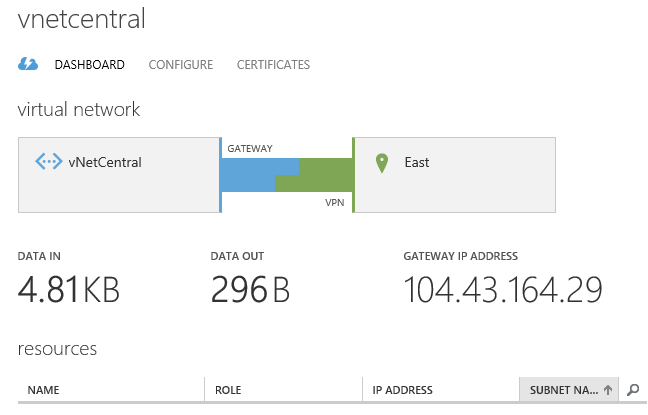
## Task 7 – Connect the networks together

Now that each virtual network has the other virtual networks IP address and pre-shared key, we can connect them together.

1. Go it to each virtual networks dashboard and click the “**Connect**” button at the bottom of the screen



As an example, when the vNetCentral virtual network successfully connects to the vNetEast network, you should see something like:

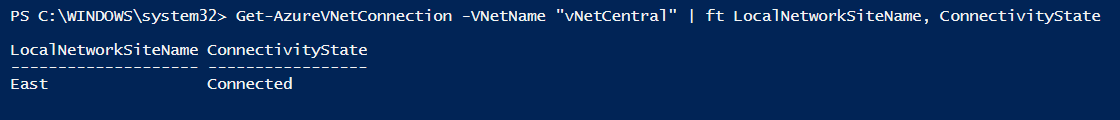


## Task 8 – Checking the network status

Another way to check connectivity between the networks is through PowerShell. Once the networks are connected together, we can check the connectivity via PowerShell commands.

1. Within the previously logged in PowerShell ISE session, enter the following commands.

Get-AzureVNetConnection -VNetName "vNetCentral" | ft LocalNetworkSiteName, ConnectivityState



Get-AzureVNetConnection -VNetName "vNetEast" | ft LocalNetworkSiteName, ConnectivityState

