



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Network Operating Systems and Services (NOSS)

(ACCA5023)

Worksheet 4

ROUTING AND PACKET FILTERING WITHIN CORE
TCP/IP SERVICES AND CRITICAL
FAILOVER/REDUNDANCY PRACTICES

Objectives

- This component of the assessment is divided into two diverse areas.
- Firstly, you are expected to incorporate **Routing and Remote Access Services** into your scenario. The role of *ARP*, *Routing Tables* and *Routing Protocols* is demonstrated. This will also require the deployment of example core TCP/IP services. Then the role of *Firewalls* (software) through **IP Packet Filtering** is utilised to show how *inbound* and *outbound traffic* to the network can be filtered for enhanced security.
- The second part of the assessment requires an independent research element into the role of **Failover Clustering** in enterprise networks. This will require a more detailed understanding, by your attempting to configure the role and detailing the necessary 'prerequisite' technologies and resources for successfully implementing a high availability solution. NB: You are not expected to demonstrate a fully working Failover Cluster, but you are however expected to provide as much detail as possible as to 'how' this role can be implemented into the network. Also why it is of such critical importance.

KINDLY NOTE THAT, IN THIS WORKSHEET YOU HAVE TO RECORD YOUR OBSERVATIONS (WITH APPROPRIATE REFERENCES) IN THREE DIFFERENT TASKS. (3a, 5a & 6a)

NB: YOU ARE REQUIRED TO SCREEN CAPTURE THE COMPLETION OF THESE TASKS IN EVERY WORKSHEET AS YOUR EVIDENCE OF UNDERTAKING THE TASKS REQUIRED. PRACTICE USING THE SNIPPET TOOL AND CAPTURE EVIDENCE AND BUILD YOUR WORKSHEETS USING A WORD PROCESSING PACKAGE SUCH AS MICROSOFT WORD.

YOU SHOULD READ EVERY ELEMENT IN THE WORKSHEETS 'VERY CAREFULLY' AS THERE ARE PRE-REQUISITE SNIPPETS OF INFORMATION YOU WILL NEED TO UNDERSTAND, BEFORE UNDERTAKING EACH TASK.

YOU SHOULD PROVIDE SUITABLE NARRATIVE ALONGSIDE THE SCREEN CAPTURES TO IMPROVE THE QUALITY OF YOUR PRACTICAL TASKS.

Task 1: Utilising ARP and Routing Tables

IN ITS CURRENT FORM, OUR SIMULATED NETWORK ENVIRONMENT CONSISTS OF TWO, SEPARATE ISOLATED LOCAL AREA NETWORKS. THESE ARE SERVER 1 AND CLIENT 1, WHO ARE CONNECTED TO EACH OTHER ON 192.168.100.X AND SERVER 2 AND CLIENT 2, WHO ARE CONNECTED TO EACH OTHER ON 192.168.101.X

SERVER 1 AND SERVER 2 ALSO HAVE 1 ADDITIONAL NETWORK CONNECTION EACH TO THE PUBLIC NETWORK 192.168.1

We do not have any native routing capabilities set up in each of our private networks, other than each server having the capability to connect to the Internet. Recall, unless our private networks have a device known as a router setup, then it is impossible for one host on LAN 1 to connect to another host on LAN 2. This means that both servers can ping each other on the Public Network Connection 192.168.1 addresses, but clients are not able to ping each other on their networks (192.168.100.x and 192.168.101. respectively).

The ARP table 'maps' logical IP (Internet Addresses) to Physical Addresses of Network Interfaces, this is how a packet is sent/received on a Network Interface, or if you like, how packets arrive at your machine over the Internet.

[On the Server 1 VM]:

- o Click Start – run – cmd and at the command prompt type **ARP -A**

The information you see displayed comprises of:

- *The Interface (NIC's) in your Machine.*
- *The Physical (MAC) Address of this NIC*
- *The Internet Address of this NIC.*

You may not at present have any (or you may have very few entries). As you connect to, are connected to; other servers, this ARP Table (MAC Table) will be updated;

One common way to see this in practice, is by using an ICMP operation such as 'PING'

Attempt to ping other hosts in our 2 networks, note on successful attempts, check your ARP Table using the `arp -A` command, note the entries being updated as more servers connect/are connected to.

To verify what networks your host is connected to, you can use the ***route print*** command to print out the Routing Table information on your operating system.

- o Click Start – run – cmd and at the command prompt type **route print**

The information you see displayed comprises of:

Network Destination:	Destination Network Address
Netmask:	The subnet mask applied to each network.
Gateway:	The default gateway IP for reaching the destination network
Interface:	Which network IP on your host you are going to use to attempt to reach this network.
Metric	The 'cost' calculated for reaching destination network.

Task 2: Deploy core services (FTP Server)

Here we will install the FTP Server role on a server in the network. At present, only the client directly connected to this server (on the 192.168.101.x network) will be able to reach the FTP service.

[On the Server 2 VM]:

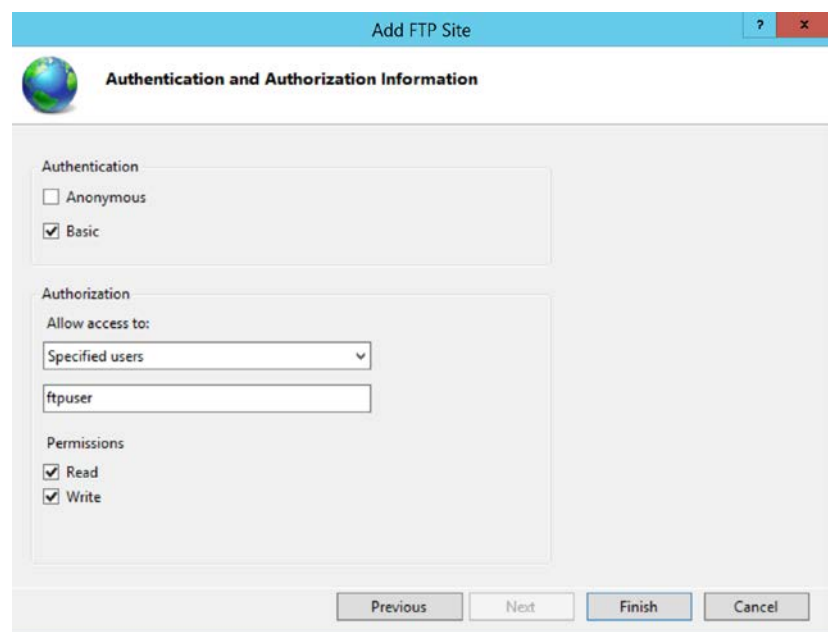
- o Launch Server Manager.
- o Click on Add Roles and Features.
- o Click Next.
- o Select Role based or Feature based installation - Next
- o At the 'Select Destination Server' screen ensure that you are the Server 2 VM (verify via name and IP address) – choose Next
- o At the Select Roles to install screen – check on the Web Server (IIS) Role
- o Click on the Add Features button
- o Click Next
- o In the **Select Features** screen simply click on **Next** and click on **Next** again in the **Web Server Role (IIS)** stage as well.
- o At the 'Select role services to install for Web Server (IIS) screen, find the checkbox for FTP Server (ensure that FTP Service option is also checked on). Now click Next and Install.
- o Here, we will create a test local user account that is authorised to FTP to the server
- o In Server Manager – click Tools – Computer Management
- o In the left hand menu, Expand Local Users and Groups – right click on Users and Choose New:

PLEASE READ: VERY IMPORTANT

Ensure that you **Check off** the '**user must change password at next logon setting**'.

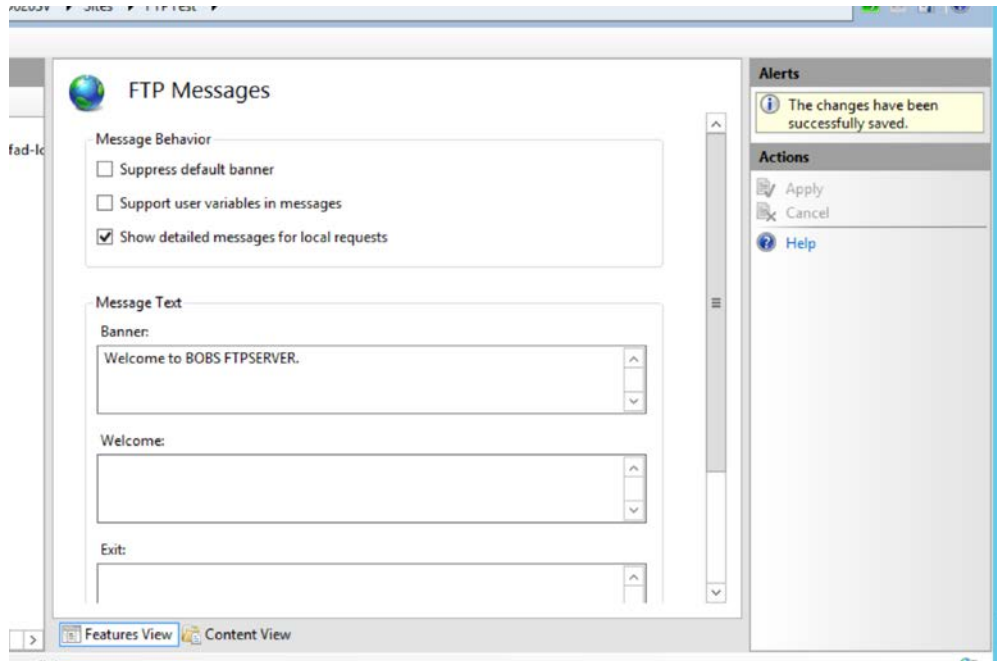
- o Name: ftpuser
- o Password: P@ssw0rd
- o Now that the ftpuser is created, go to Server Manager – Tools and then Internet Information Services (IIS) Manager.
- o Expand the Computer Name – Right click on Sites – choose Add FTP Site

- o In Site information type **1STFTPSITE**
- o Click on the browse button [...] next to Content Directory/Physical Path
- o Choose root drive (e.g. C:\inetpub\ftproot) - next
- o At the bindings and SSL settings page – choose **No SSL**
- o Take note of the Port Number **(21)** can be used via the TCP protocol when using the FTP Service.
- o Chose **Basic Authentication** as the preferred mode.
- o Alongside the Authentication menu, click the drop down menu and choose Specified Users.

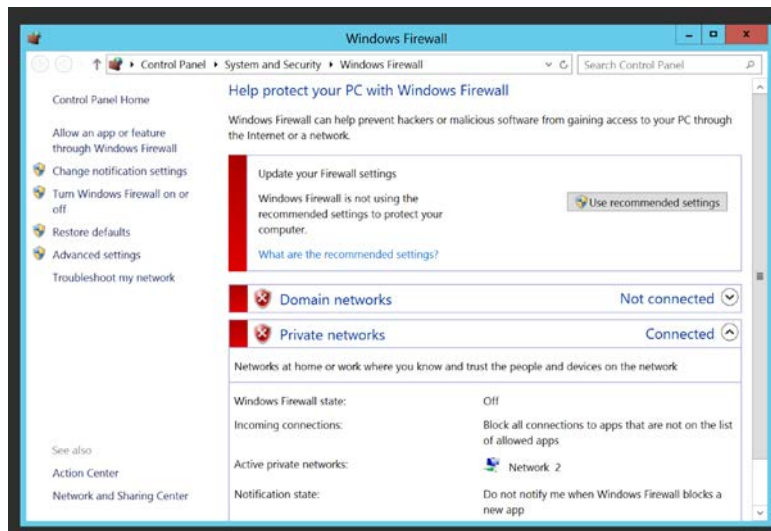


- o Here, type in the name of this server followed by the user account you created above (e.g. Server2\ftpuser). NB: The server name is the name of your computer in windows, check this by opening up a command prompt and typing in **hostname**:
- o **NB:** Ensure you check on both the Read\Write options. Choose Finish.
- o We can setup banners/welcome greetings as a way of knowing if we are connecting to the right server
- o To setup a banner – Server Manager – Tools – Internet Information Services (IIS Manager).
- o Expand the servername in the left hand side of the window – Expand sites click on your ftp site you created earlier **1STFTPSITE**

- o In the right hand window double click on FTP messages.
- o As shown in the image below, enter some text in the Banner field and click Apply.



- o There is one last permission to check to ensure we can use the FTPService ok.
- o In the file system, go to C:\inetpub and right click on **ftproot**, choose Properties.
- o Add in the user account you have just created (you do this by clicking on the Security Tab – Clicking the Edit button and then clicking the Add button.
- o Type in *ftpuser* and click *Check Names* button, you should notice the account is underlined when it is successfully found.
- o Choose Ok to confirm and close down all windows.
- o We now have the FTP Service running on Server 2.
- o Within the C:\inetpub\ftproot folder, create a New Folder – call it **Ftpuploads**
- o **Double check to ensure that there are NO FIREWALLS ENABLED ON SERVER 2**
- o Search for the Firewall Program (Windows Firewall and ensure that there are no Firewalls on for Public/Private profiles. It should resemble something similar to the image below:
- o You can click on **Turn Windows Firewall on or off** and then **disable on any of the profiles**, hint: it usually goes from green to red as in the image below.



[On the Client 2 VM]: Here we will attempt to connect to the FTP Service on Server 2 to upload a file, from client 1.

NB: You will need to login as a domain administrator level account, since you may well have disabled the command prompt for non-admin level users in your network. You should also ensure that the firewall on the Windows 10 client machine is disabled as per the instructions above in the previous section.

- o First create a folder and a text file in the C:\ directory of client 2, create the folder call it **FTPFiles** go into the folder and create a text file here, name it: **ftpfile2upload.txt**
- o Now, connect to the ftpservice, launch command prompt
- o In command prompt type in: **ftp 192.168.101.1**
- o Then use server1name\ftpuser as the username and
- o P@ssw0rd is the password.
- o You should now be connected to the FTPServer (denoted by an ftp prompt)
- o Now type in: **lcd C:\FTPFiles** (* This will change to the directory on the client that stores the file you want to upload to the FTPServer
- o Type in: **dir** (* This gives a listing of what is stored in the directory above, you should see the text file we created there).
- o Now type in: **put ftpfile2upload.txt**

[On the Server 2 VM]:

- Go to the c:\inetpub\ftproot folder and verify that the file has been uploaded

Task 3: Installing and configuring the Routing and Remote Access Service

At this stage we will expand our initial network design, here, we will build two remotely connected local area networks (e.g. a Wide Area Network), but using Layer 3 devices and protocols referred to as Routers and Routing Protocols. We are able to deploy a software routing service on Windows Server which will enable our disconnected networks to communicate with each other.

Recall our initial configuration from Worksheet 1:

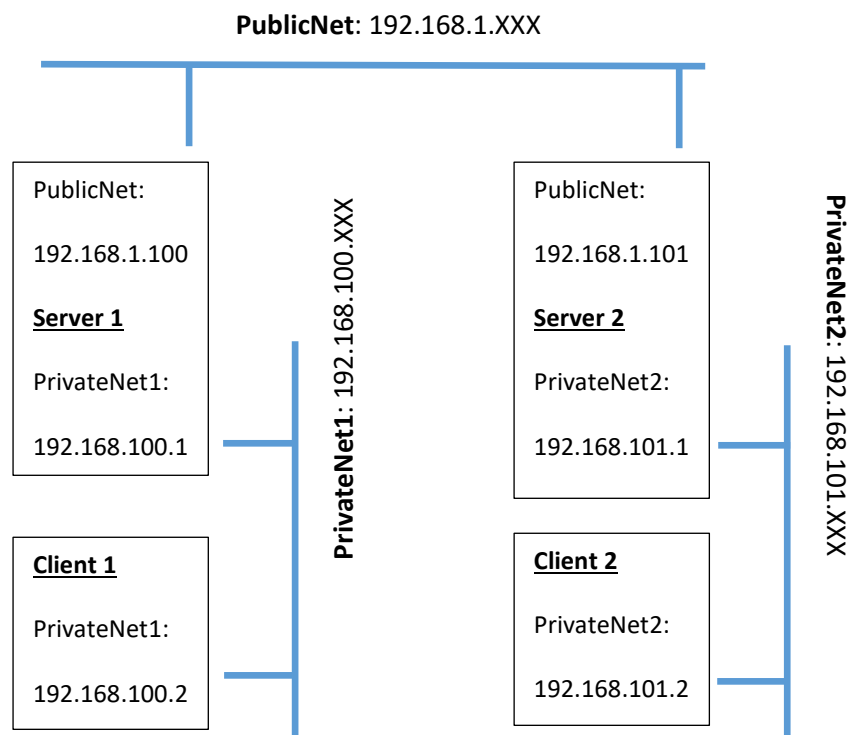


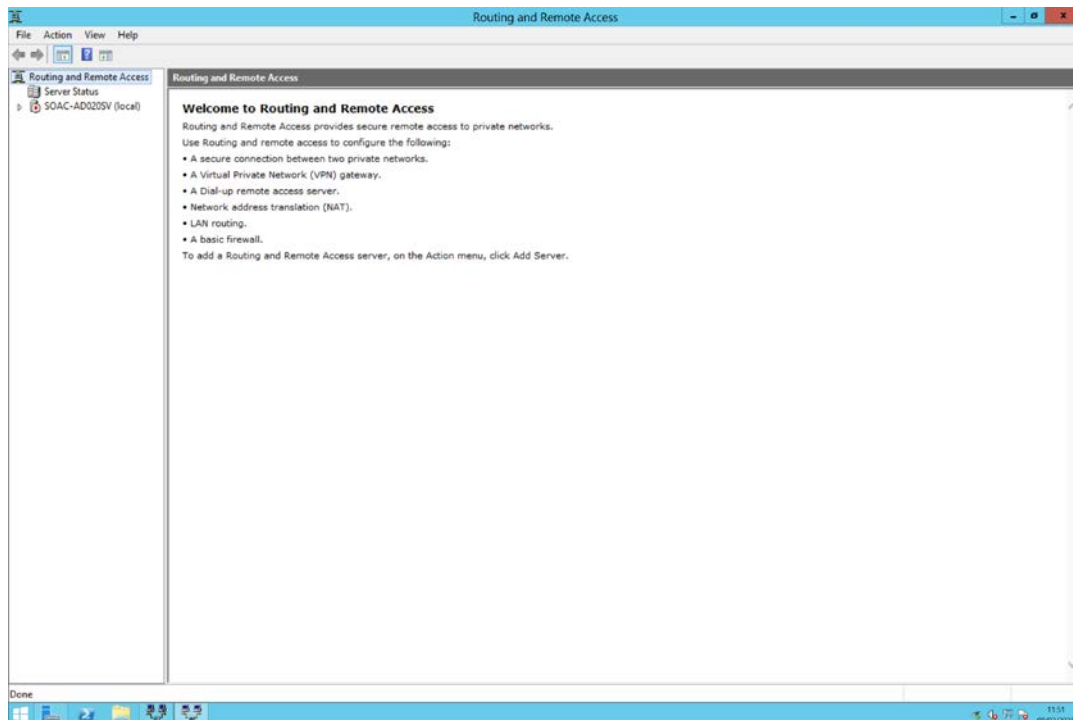
Figure 1: Trial Network Configuration

Here we are going to ensure that hosts inside of each of our Local Area Networks are able to communicate with each other, by providing a Routing Service on both **PrivateNet1** and **PrivateNet2**.

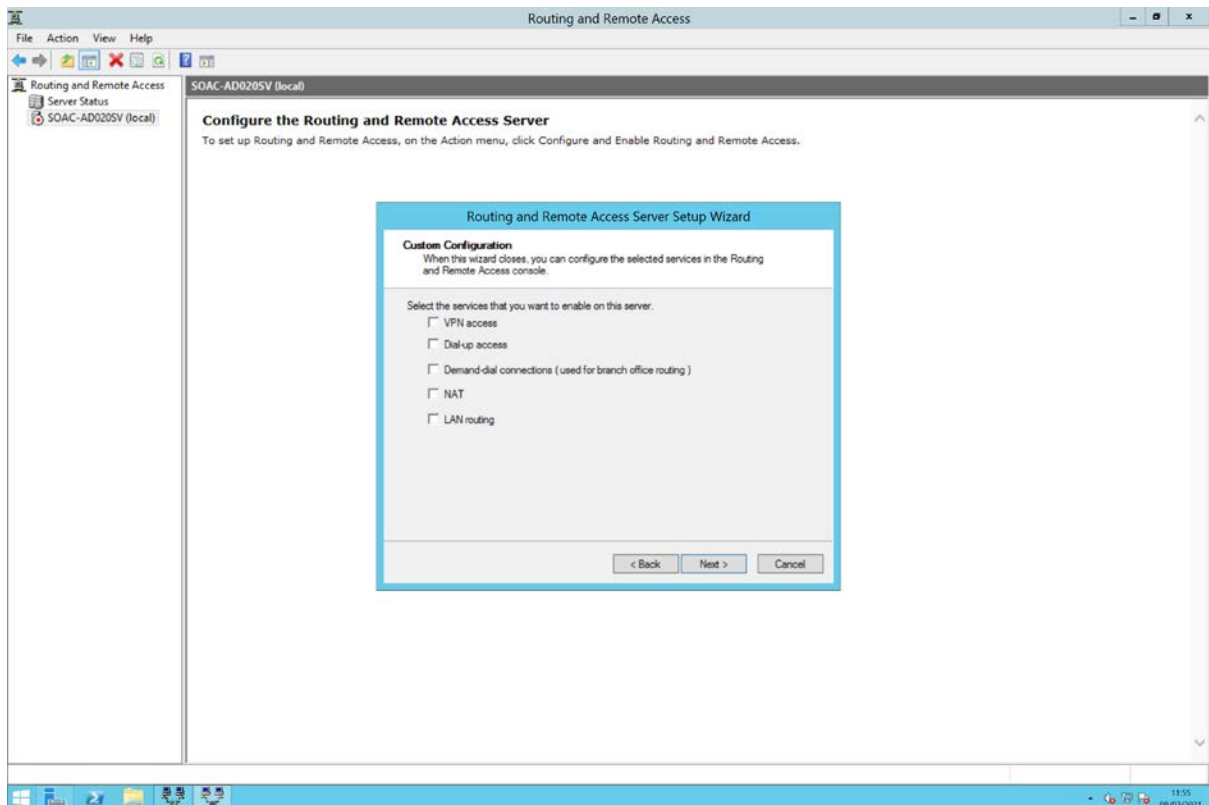
[On the Server 1 VM]:

- o Open Server Manager – Add roles and features.
- o Role based or feature based installation – Click Next
- o Select a Server from the Server pool (choose your server1 Server) - click Next
- o At the Select Server Roles screen – check on Remote Access choose Next
- o Do not make any changes in Features and click on Next.

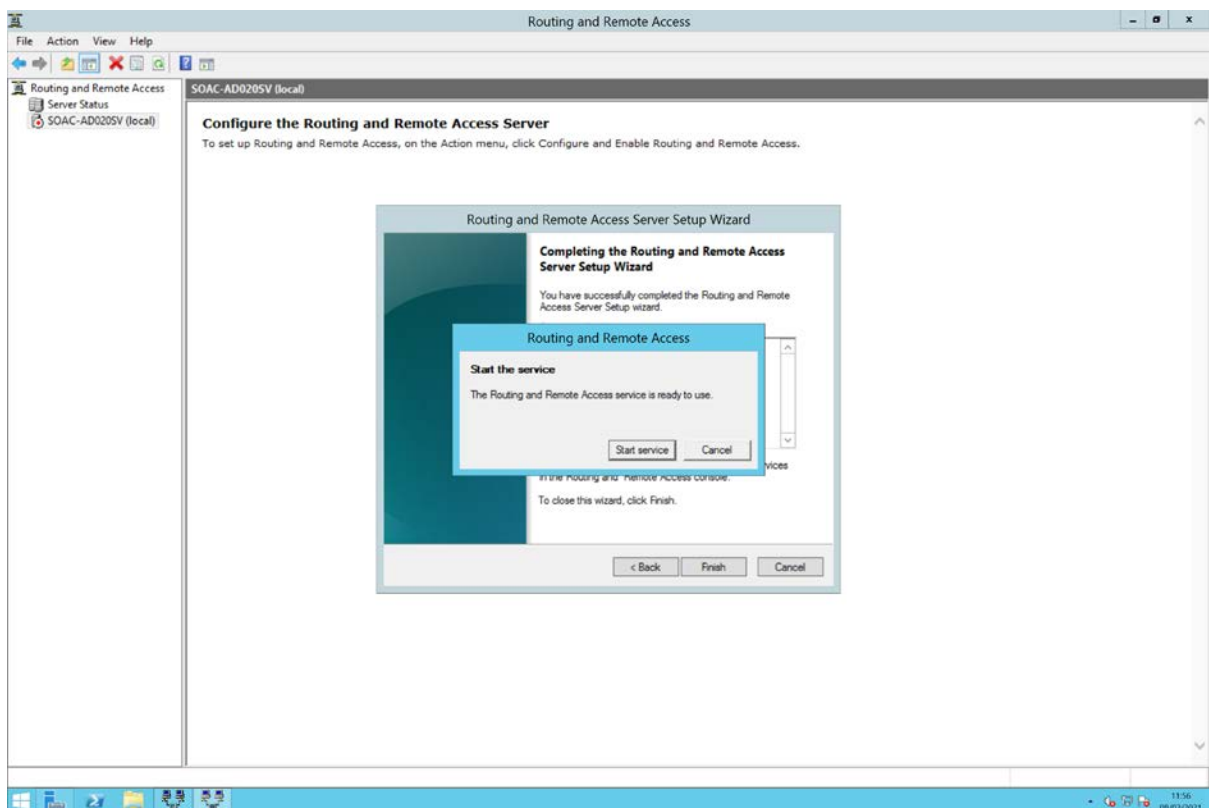
- o In Role services, select DirectAccess and VPN, Routing services and click on Next.
- o Review installation page and click on install once you are ready.
- o Once the installation is completed, click the link '*Open the Getting Started Wizard*'
- o At the '**Configure Remote Access**' wizard screen - click on **Deploy VPN only**
- o You should now be brought to the Routing and Remote Access Window:



- o Right click on the icon with your Servername listed – choose Enable and Configure Routing and Remote Access.
- o Choose Next at the Welcome wizard
- o At the Configuration wizard screen, select 'Custom Configuration'

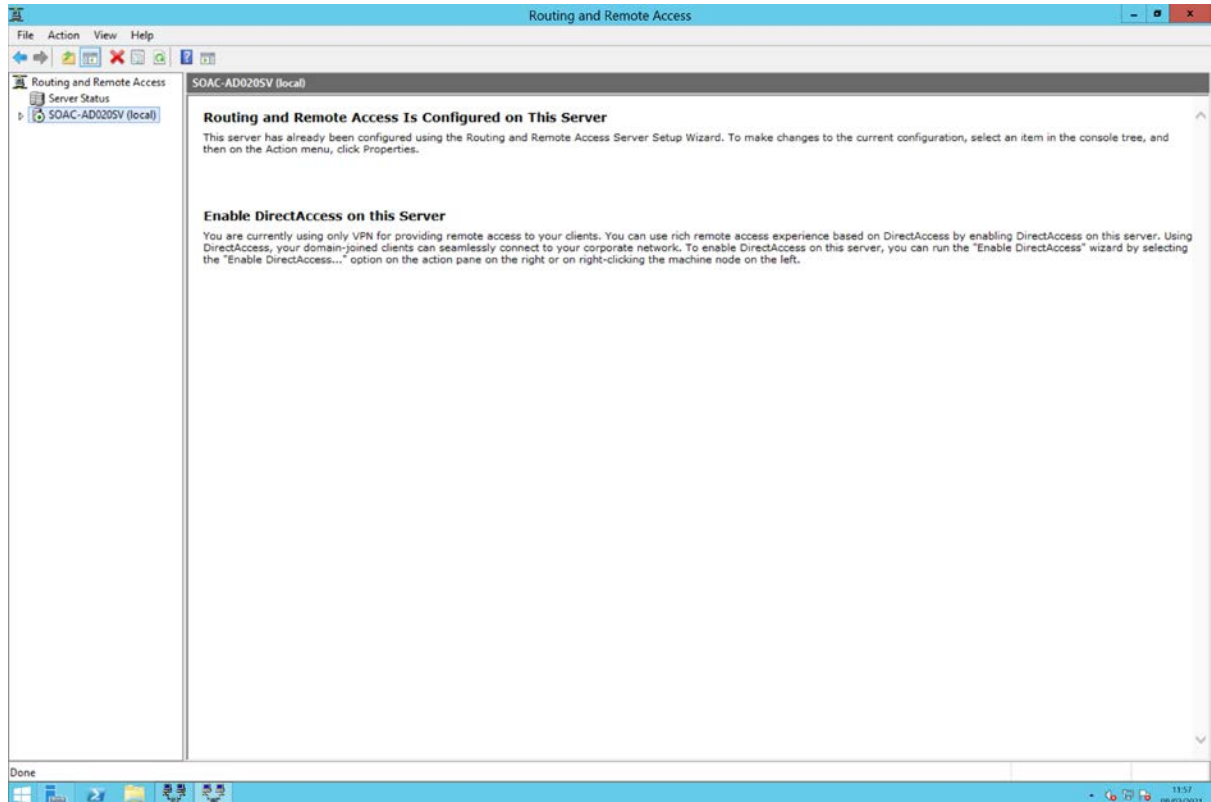


- o Choose **LAN Routing** – click Next



- o Click on **Start service**.

- o You should now be informed that the Service is started and running and the Server icon we click on in the left hand console windows should have a green arrow next to it to denote that the service is running.

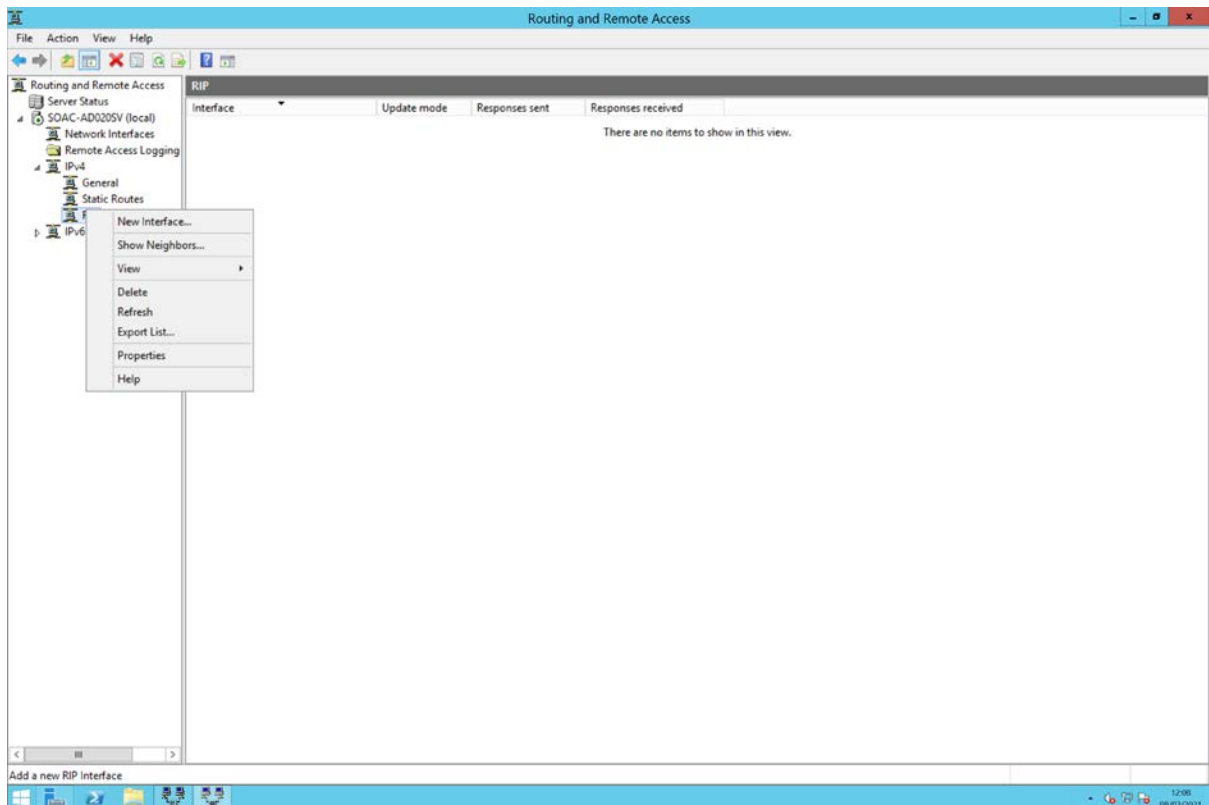


Here we will enable Routing Protocols on the network interfaces in our networks, so that the systems in our networks can 'learn about new networks', which may now be reachable utilising the routing protocols in the WANs. This is how the internet functions.

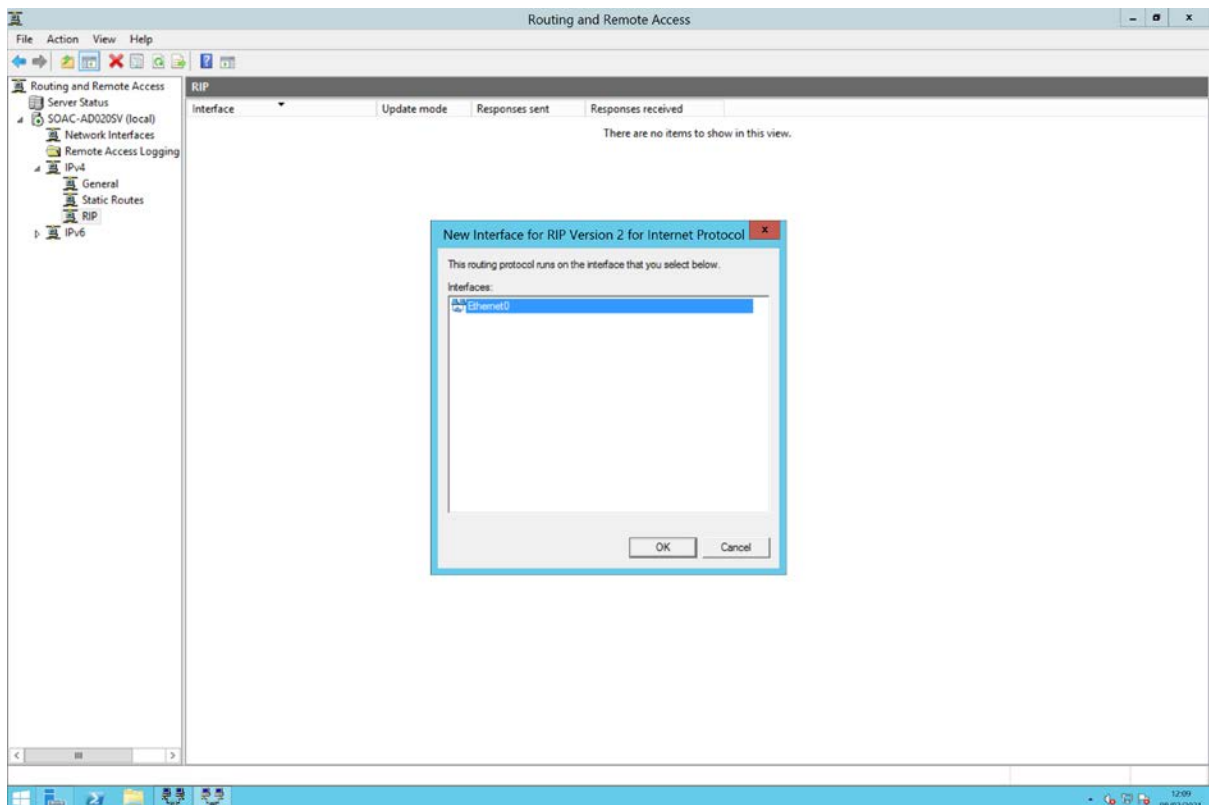
- o Click on the Server icon to expand it – choose **IPV4**
- o Right click on General – choose **New Routing Protocol**.
- o Choose RIP V2, next and then finish.
- o You should now see RIP listed as an available protocol on the IPV4 stack within our Windows Server.

We now need to add the routing protocols to the network interfaces that the Server uses to connect to both the **PublicNet** and **PrivateNet1** networks.

- o Right click on RIP – select **New Interface**



- o You need to add in any interfaces that are listed in the console window, you should see two listed for your Server: Choose Ok



[On the Server 2 VM]:

You now need to repeat the steps outlined the task above on the Server 2 VM, Server 2 needs to be configured as a Routing and Remote Access Service (RRAS). It will also need RIP.V2 configured and both of its interfaces added to the RIP/IPV.4 stack.

When you have completed these tasks, you will need to test Wide Area Network Connectivity by doing the following.

[On the Server 1 VM]:

- o Verify that you can 'ping' Server 2 on its 'PublicNet' IP address.
- o If you can, it means that at least the Routers themselves are connected to the same network, now you will need to check that the LAN hosts inside each PrivateNet LAN are able to ping each other as they are NOW connected to Routers in their respective networks:

[On the Client 1 VM]:

- o Ping the Client 2 VM, on its PrivateNet2 IP address (ping 192.168.101.2), are responses being received? It may take a while for the Routers to learn about the other Routers that they are connected to.

Task 3 Record your Observation:

3 a) How do Routers reference which networks they are able to connect to?

Task 4: IP Packet Filtering

IP Packet filtering is Microsoft's basic firewall configuration service. It is able to restrict packet flow by utilising a combination of source/destination ports and the protocol that these services use. Packet filtering uses two concepts known as ***Inbound*** and ***Outbound Filters***.

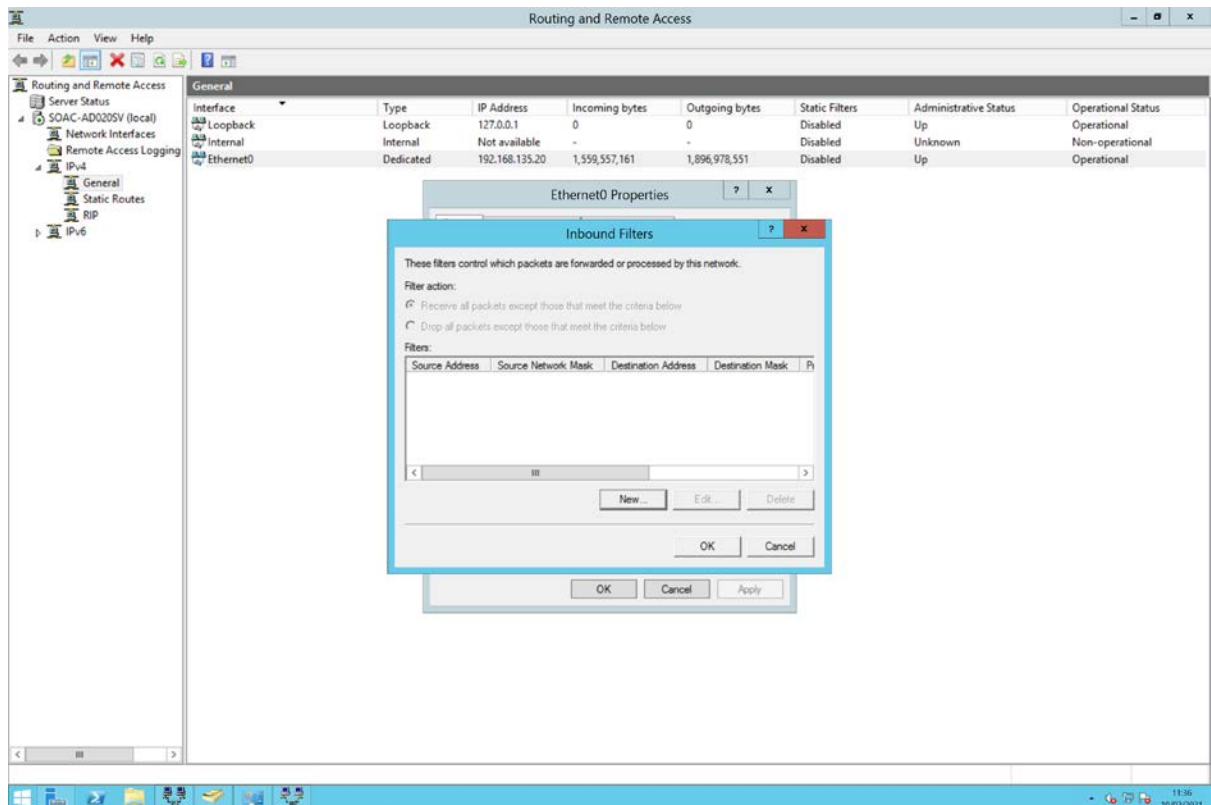
Inbound Filters are a rule which apply to the Firewall/Router (In our case, Server 1 and Server 2 in our two simulated networks). Inbound filters are placed on a particular interface (for us this could be the PublicNet interface or the PrivateNet interface(s). Inbound filters deal with packets that are arriving 'INTO or INWARDS into our Router or network. So for example if we built an inbound filter on Server 1's PublicNet Interface, it would investigate all packets coming into Server 1 on that network. In our scenario, these packets could only originate from Server 2's network (NB: though note, that Client 2 is on Server 2's network).

Outbound filters are concerned with packets that are trying to leave the Router's themselves (packets could leave the Router on the PublicNet interface and again, on PrivateNet1 or PrivateNet2 connections for Server 1 and Server 2 respectively).

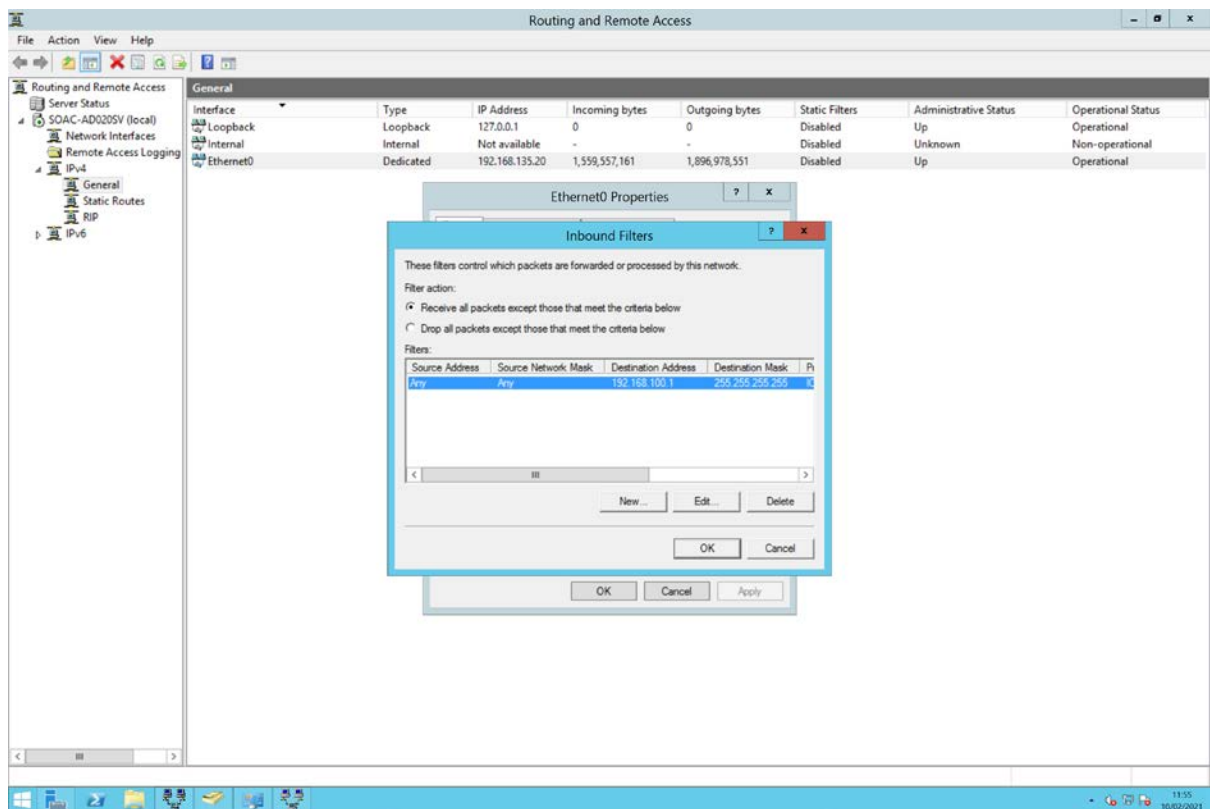
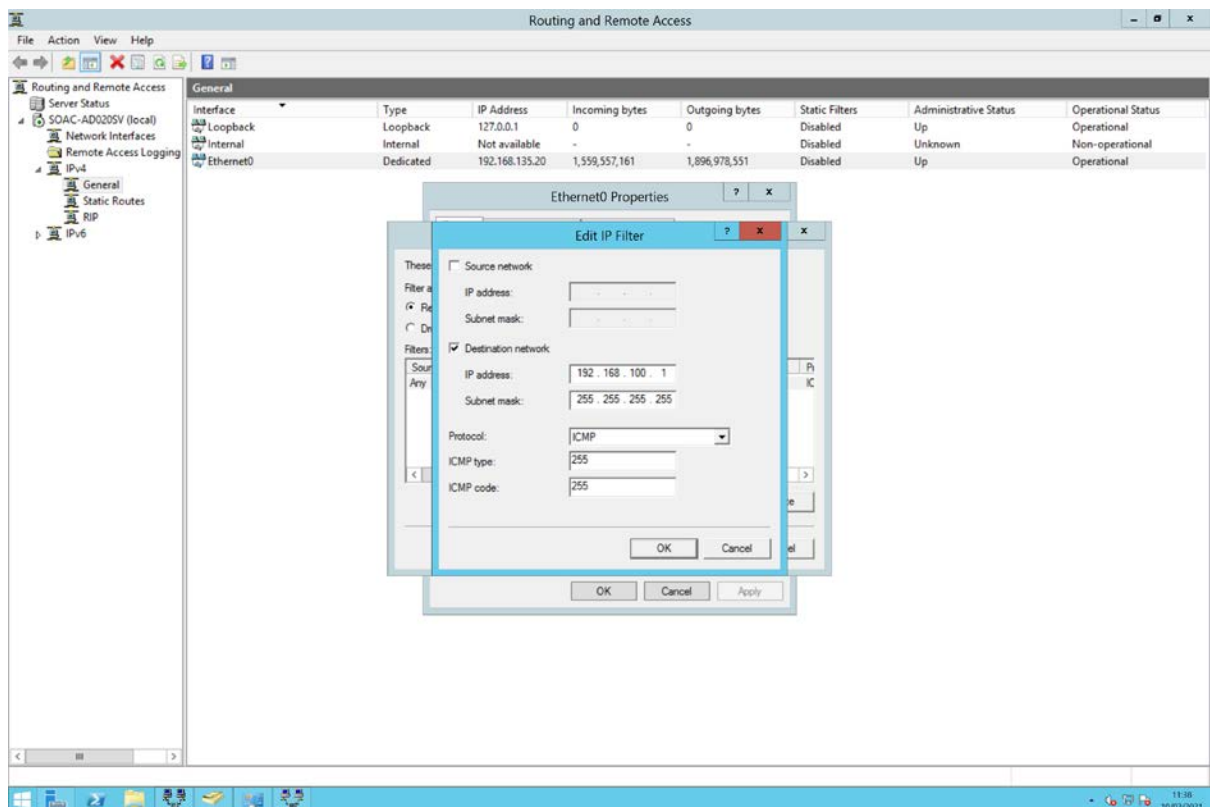
Here we are going to implement a few rules using both types of filters to govern access to some important services and protocols on the network.

Filter 1: Stopping 'anyone' in PrivateNet 1 from Pinging the Router Firewall Service.

- o Open Server Manager – Tools – **Routing and Remote Access**.
- o In the left hand console window, expand your ServerName if needed and click to expand **IP Routing** – Then Click **General**
- o Right click the **PrivateNet1 Connection interface**, click **Properties**.
- o Click **Inbound Filter** (anything coming into the Router on the PrivateNet1 Connection interface).



- o Choose **New**
- o Check on **Destination Network**
- o **IP Address: 192.168.100.1**
- o **Subnet Mask: 255.255.255.255** (This mask value is applied, since we know the EXACT HOST that we want to affect by our rule).
- o **Protocol: ICMP**
- o **Click Ok** (leave the last two fields ICMP code and type empty, the filter will include these itself).
- o Ensure that the following option is checked '**Receive all packets, except those that meet the criteria below**'



NB:

[On the Client 1 VM]:

You now need to test your filter. First try 'pinging' 192.168.100.1 you should find that there is no reply. Now try pinging other networks, you should find that you can reach them, since only destination 192.168.100.1 (the Router) is denying you ping access.

Rationale:

There are several ways we could restrict LAN hosts from 'pinging' our Router (Server1), there really isn't only one answer. Using this method just assumes that anyone on the same source network as the PrivateNet1 is affected by the rule. Obviously, we only have one host here, Client 2, but if we had say 500 hosts, then this rule would cover all of them. It is just rule which cuts out ambiguity and the amount of additional rules that would be required to do the same thing. It is important to carefully consider your firewall rules, perhaps even more so when using a software firewall such as this. This is because software firewalls are not as quick as processing the rules and rely on work done by the TCP/IP protocol stack within the operating system. The lesser the number of rules and the less ambiguous their structure, the more efficient the routing/firewall service.

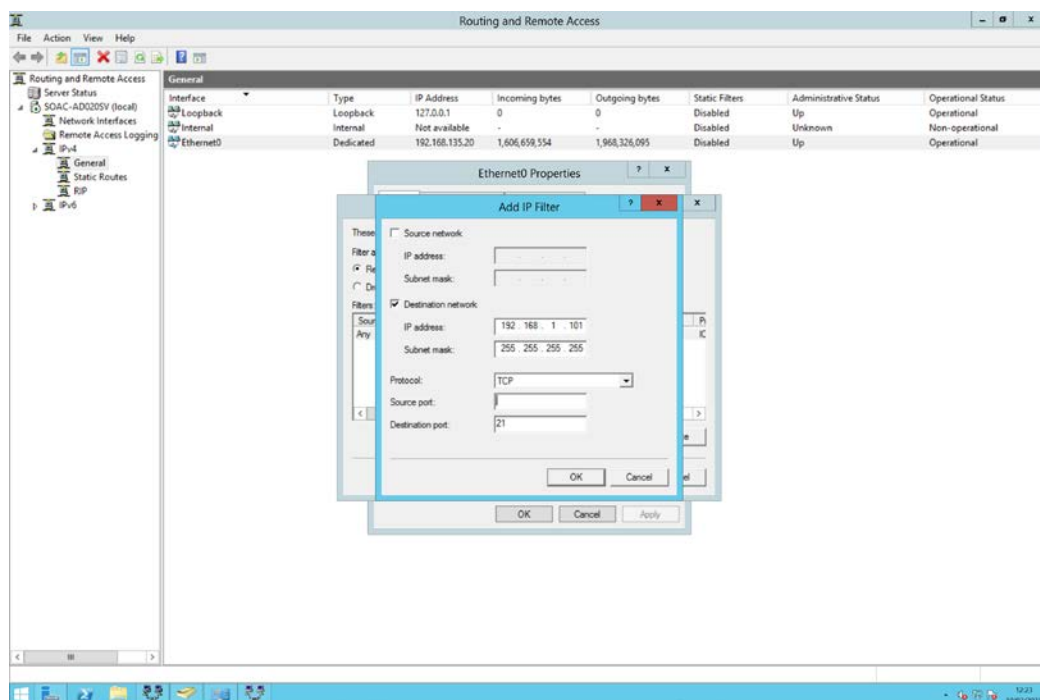
Filter 2: Restrict Access to FTP Service running on Server2 to only hosts in PrivateNet2.

Here we demonstrate, another possible, slightly unorthodox method of using an 'Outbound' filter to restrict access to hosts on our network (PrivateNet1) from accessing the FTP Service running on another network (Server2). The question is, will it work?

[On the SERVER 1 VM]:

- o Open Server Manager – Tools – **Routing and Remote Access**.
- o In the left hand console window, expand your ServerName if needed and click to expand **IP Routing** – Then Click **General**
- o Right click the **PublicNet Connection** interface, click **Properties**.
- o Click **Outbound Filter** (anything leaving the Router on the PublicNet Connection interface).

- o **New**
- o Check on **Destination Network** (again we don't need source network, since theoretically all our hosts in PrivateNet1 will try to connect to Server 2 through the Routing Service on Server 1 to reach the Network on Server2.
- o **IP Address: 192.168.1.101**
- o **Subnet Mask: 255.255.255.255**
- o **Protocol: TCP**
- o **Destination Port:** (the port on the destination we are trying to reach): **21**
- o **Click Ok**



- o Ensure that the following option is checked '**Receive all packets, except those that meet the criteria below**'

[On the Client 1 VM]:

NB: You now need to test this filter, you should try and access the ftp service running on Server 2 (as discussed in the steps in task 2: Can you still access the FTP server? If you can, you may need another identical filter but focusing on destination port 20, since FTP can run on two binding ports. If you are still able to connect, it is possible to use an inbound filter on Server 2 to deal with this requirement. Construct a rule to show this.

Filter 3: Only allow specific hosts in PrivateNet1 to access the FTPService running on Server2

This task requires you to construct your own 'rule' to restrict FTP access to EVERYONE except 192.168.100.1 (Client 1). Note that when a rule is constructed, you can either 'Receive all packets except those that meet the criteria below' or you can 'Drop all packets except those that meet the criteria below'. With this in mind, you should show how your rule is constructed and give the rationale of how it works. Also demonstrate the testing process.

For Task 5 and 6, You should use a proper referencing style here when submitting your answers.

Task 5: Failover Clustering for high availability systems/services

A failover cluster is a set of physical or virtual computer systems that work together to facilitate a High Availability (HA) or Continuous Availability (CA) environment for the various applications and services that run within enterprise networks.

5 a) Give a detailed explanation of the concepts that need careful consideration when considering the usage of such a system. Also show one possible role within the Window Server OS environment that could provision these requirements. You should breakdown the aspects that need consideration when attempting to deploy this role/service. **(Hint: Give screen shots of the role being configured and discuss these steps).** YOU DO NOT HAVE TO BUILD, DEPLOY OR TEST A FAILOVER CLUSTER.

Task 6: Observational Tasks

6 a) Assume that you are the Head - Network Administrator of an Enterprise Network which operates in multiple locations nationwide. Draft a network policy, Critical business applications high availability practices and security practices for your network. State all assumptions made. **(Hint: In your draft, address (not limited to) the architecture/ topology/ design/ layout of the network, network access, security team, enforcement of security policies, analysis of security risks, scope of security changes (if needed), monitoring the security operations, mitigations in the event of violations, etc)**