

NOSS assignment - Toby

by Thorbjorn Ravnaas Kristiansen

FILE	2652_THORBJORN_RAVNAAS_KRISTIANSEN_NOSS_ASSIGNMENT_-_TOBY_100686_2034844336.DOCX (5.85M)		
TIME SUBMITTED	14-FEB-2018 08:24 PM (UTC+0000)	WORD COUNT	4 122
SUBMISSION ID	83191311	CHARACTER COUNT	27 256

University of Wales, Trinity St. David

Investigating VM, Hypervisors and Networking

BEng Computer Systems and Electronics

Author/student: Thorbjørn R. Kristiansen
Lecturer: Dr. Tim Bashford, UWTSD
February 2018

Contents

Introduction	2
Worksheet 1 – IP addresses, RRAS and LAN	3
Task 1 – Static IP Addresses	3
Task 2 – Enabling RRAS	4
Task 3 – Adding Routing Protocols and Interfaces	5
Task 4 – Local Area Networking	7
Task 5 – Observational Tasks	8
Worksheet 2	10
Task 1 – Address Resolution Protocol	10
Task 2 – Setting up an FTP Server	11
Task 3 – Packet Filtering	14
Task 4 – Filtering FTP Services	15
Task 5 – Only Allow FTP	16
Task 6 – Observational Tasks	18
Worksheet 3	20
Task 1 – Understanding Different TCP/IP Configurations	20
Task 2 – Installing the DHCP Server	21
Task 3 – Authorising the DHCP Server	21
Task 4 – DHCP Scopes	21
Task 5 – Configuring Reservations	22
Task 6 – Observational Tasks	23
Worksheet 4	25
Task 1 – Understanding Active Directory and DNS	25
Task 2 – DNS zones	27
Task 3 – DNS Application	28
Task 4 – Observational Tasks	29
Worksheet 5 – Evaluation of Clustering Strategies	31
References	32

Introduction

The initial task was to create 3 virtual machines utilising SCVMM software.

Microsoft Server 2012 R2 was installed on two of the machines, and Microsoft Windows 7 was installed on the client machine.

The three machines were named as follows:

- Cardiff (server)
- Swansea (server)
- Lab (client)

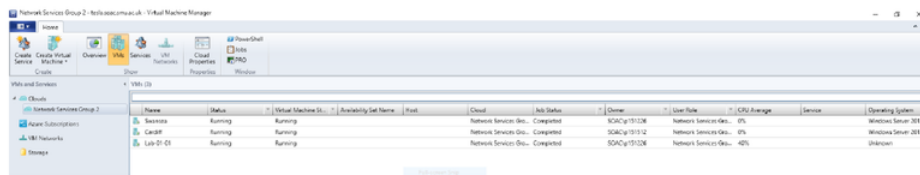


Figure 1 - Three virtual machines set up in SCVMM

Worksheet 1 – IP addresses, RRAS and LAN

Introduce scenario to worksheet. Copy/paste introduction?

Task 1 – Static IP Addresses

The goal for task 1 was in part to set up the virtual machines (see introduction) and to assign them static IP-addresses.

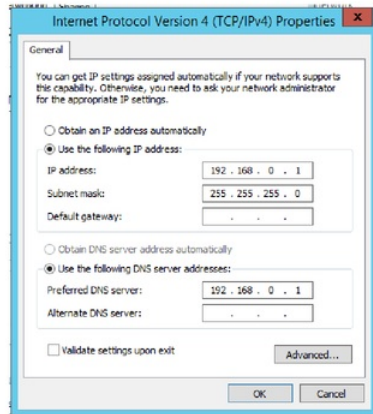


Figure 2 - Cardiff 0-network

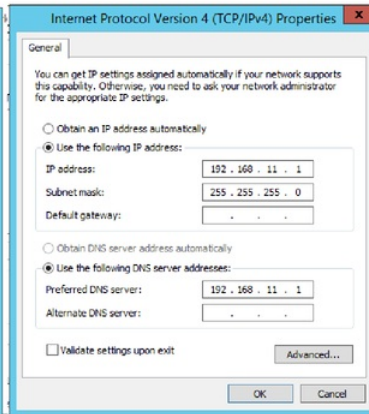


Figure 3 - Cardiff 11-network

As seen in figure 2 and 3, Cardiff was split into two networks. The 0-network exists primarily to communicate with Lab, and the 11-network communicates with the Swansea server.

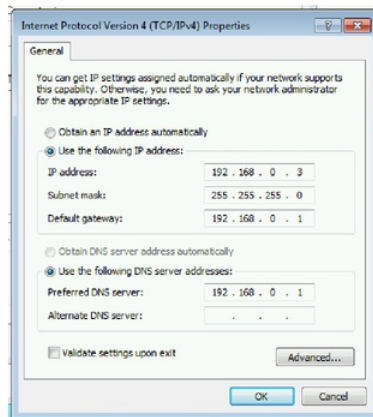


Figure 4 - Lab static IP

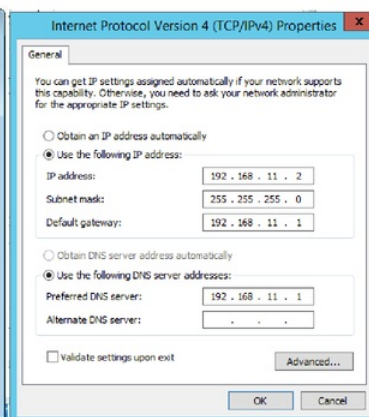


Figure 5 - Swansea static IP

In figure 5, we see the IP-configuration for the Windows 7 client. Its default gateway is Cardiff's 0-network. Figure 5 illustrates the Swansea server's connectivity, with Cardiff's 11-network as the default gateway.

Task 2 – Enabling RRAS

The next step was to enable the routing and remote access service (RRAS), to enable the machines to communicate without the need for a physical/external router.

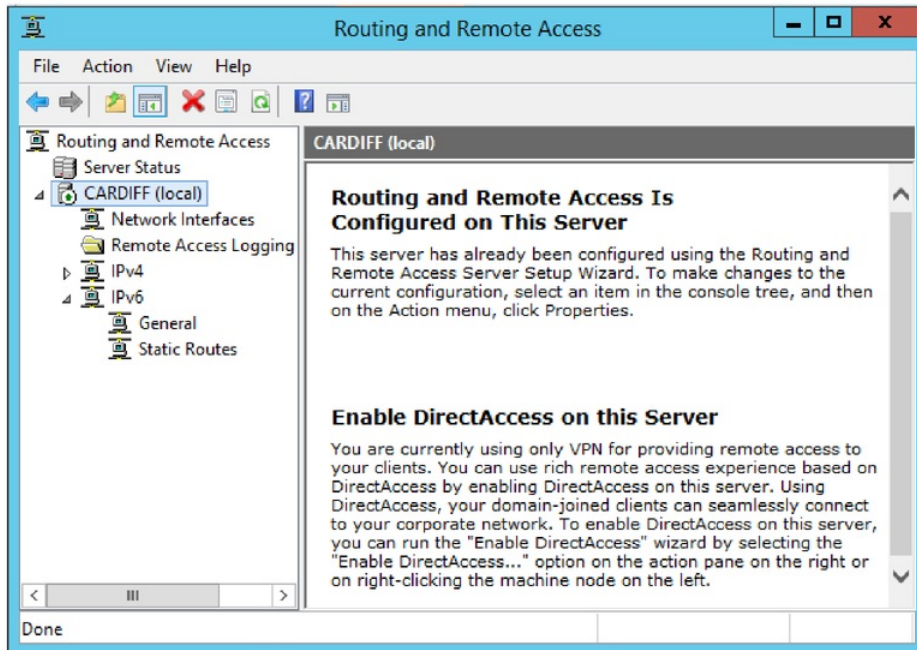


Figure 6 - RRAS enabled

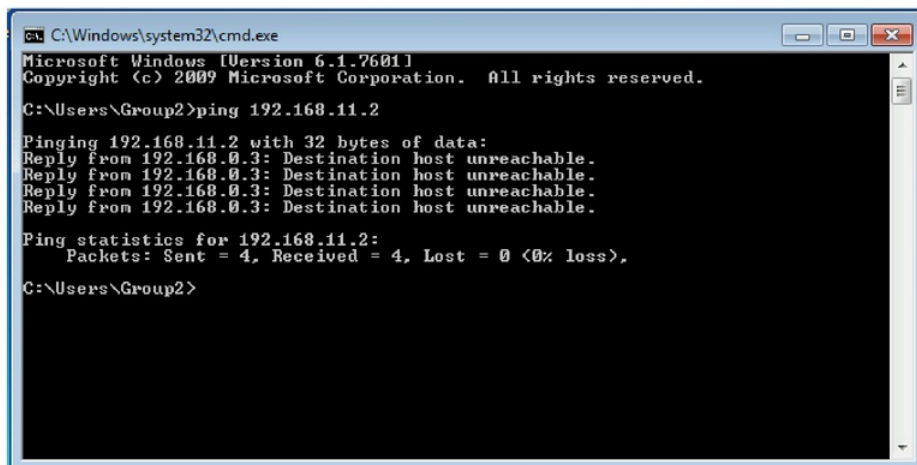


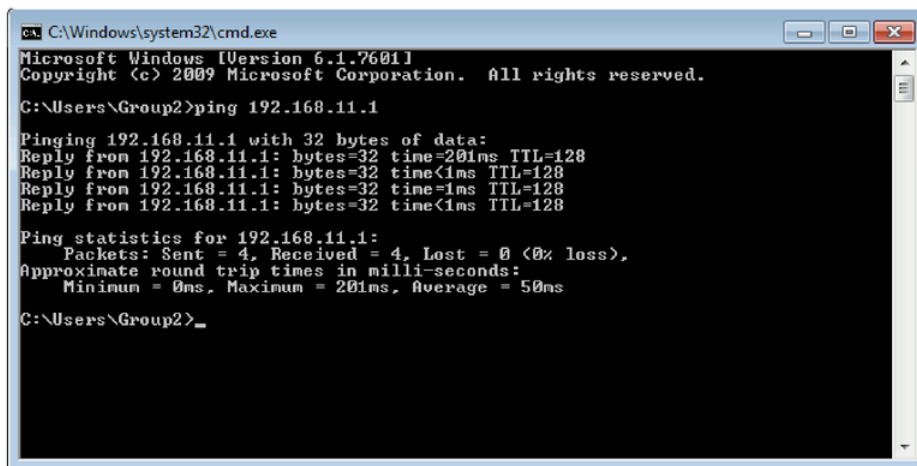
Figure 7 - Ping failed from Lab to Swansea

As seen in figure 6, the RRAS is enabled but unconfigured. This is reflected in figure 7, where the ping from Lab to Swansea failed.

Task 3 – Adding Routing Protocols and Interfaces

Now we add two routing protocols to Cardiff, making it the backbone of the network. These protocols allow for Swansea and Lab to get directions on where to send packets.

As we can see in the next 4 figures, the ping is now successful between all machines.



```
ca. C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

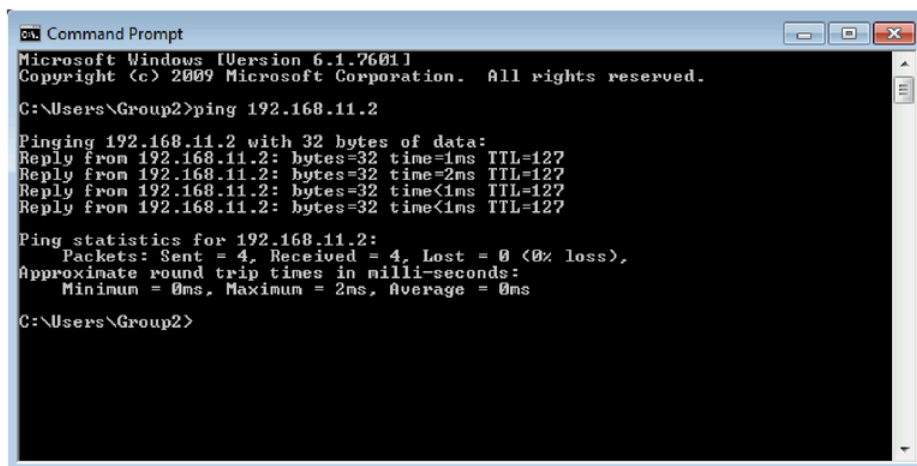
C:\Users\Group2>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.11.1: bytes=32 time=201ms TTL=128
Reply from 192.168.11.1: bytes=32 time<1ms TTL=128
Reply from 192.168.11.1: bytes=32 time=1ms TTL=128
Reply from 192.168.11.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 201ms, Average = 50ms

C:\Users\Group2>_
```

Figure 8 - Successful ping from Lab to Cardiff



```
ca. Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

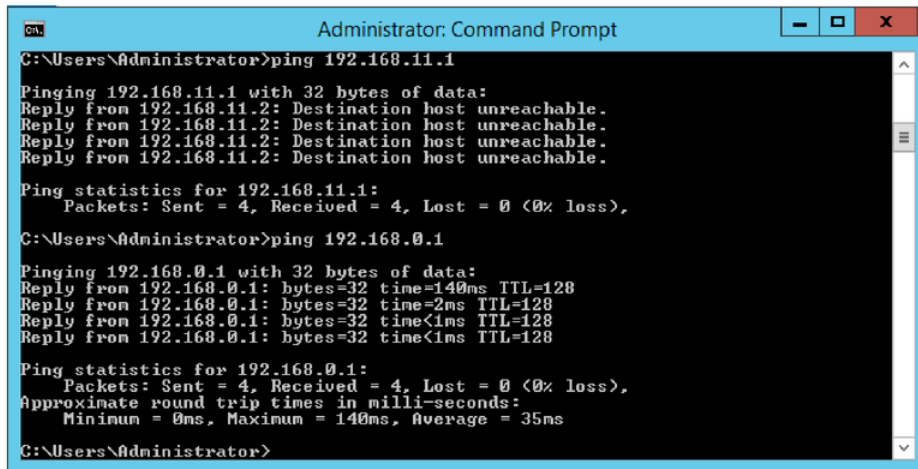
C:\Users\Group2>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:
Reply from 192.168.11.2: bytes=32 time=1ms TTL=127
Reply from 192.168.11.2: bytes=32 time=2ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Group2>
```

Figure 9 - Successful ping from Lab to Swansea (using Cardiff as router)



```
C:\Users\Administrator>ping 192.168.11.1
Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.11.2: Destination host unreachable.
Reply from 192.168.11.2: Destination host unreachable.
Reply from 192.168.11.2: Destination host unreachable.
Reply from 192.168.11.2: Destination host unreachable.

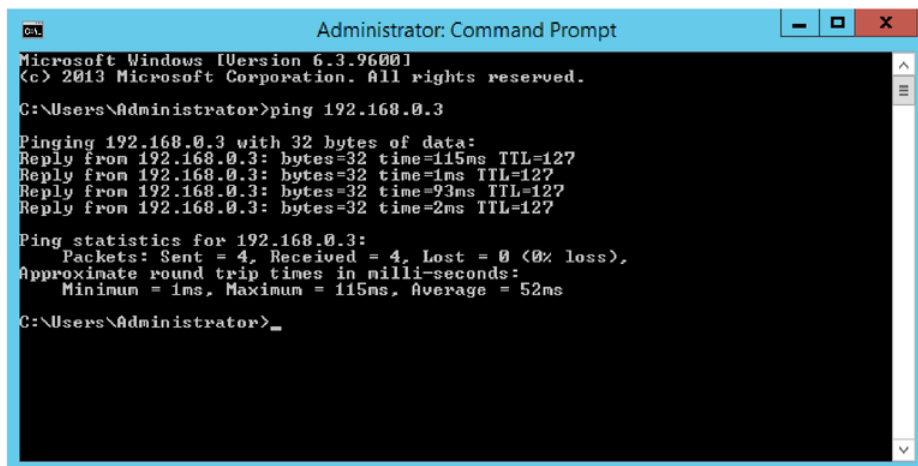
Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=140ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 140ms, Average = 35ms

C:\Users\Administrator>
```

Figure 10 - Successful ping from Swansea to Cardiff



```
C:\Users\Administrator>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time=115ms TTL=127
Reply from 192.168.0.3: bytes=32 time=1ms TTL=127
Reply from 192.168.0.3: bytes=32 time=93ms TTL=127
Reply from 192.168.0.3: bytes=32 time=2ms TTL=127

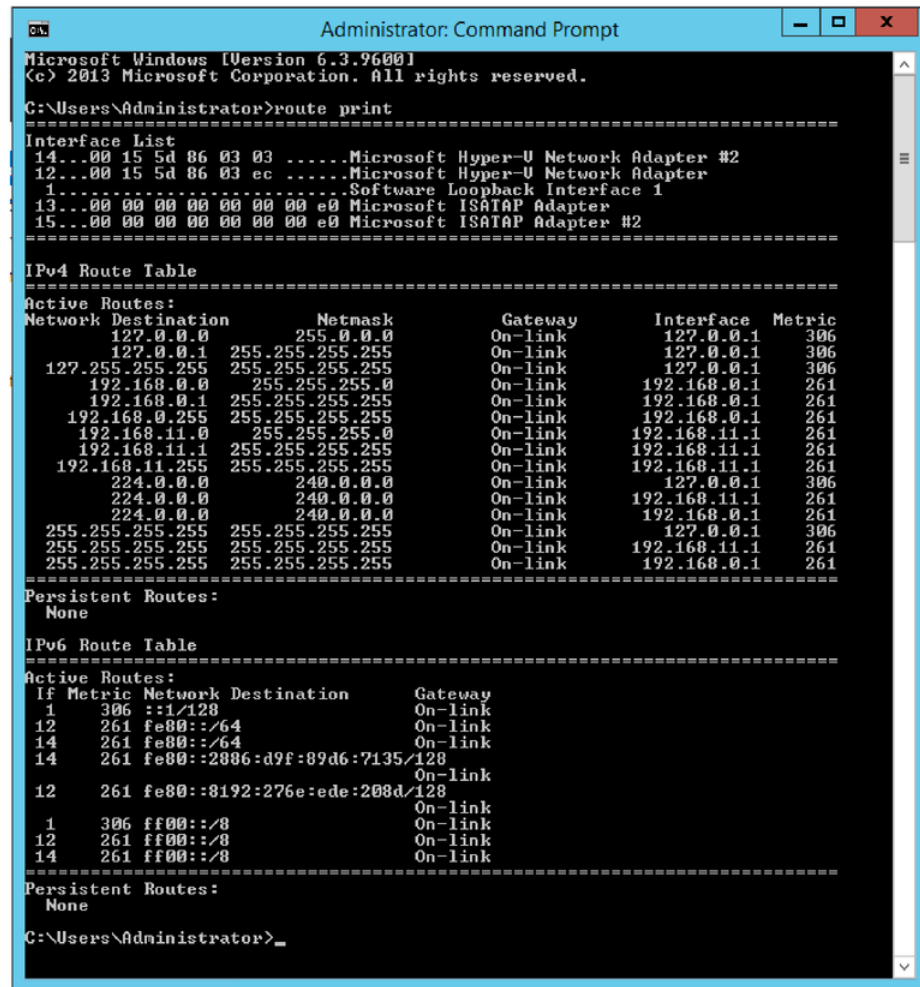
Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 115ms, Average = 52ms

C:\Users\Administrator>
```

Figure 11 - Successful ping from Swansea to Lab (using Cardiff as router)

Task 4 – Local Area Networking

By opening the route print window by running it from the command prompt on Cardiff using the command `route print`, we see the route table (figure 12).



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>route print

=====
Interface List
14...00 15 5d 86 03 03 .....Microsoft Hyper-V Network Adapter #2
12...00 15 5d 86 03 ec .....Microsoft Hyper-V Network Adapter
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
15...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
127.0.0.0                  255.0.0.0        On-link           127.0.0.1         306
127.0.0.1                  255.255.255.255  On-link           127.0.0.1         306
127.255.255.255           255.255.255.255  On-link           127.0.0.1         306
192.168.0.0                255.255.255.0    On-link           192.168.0.1       261
192.168.0.1                255.255.255.255  On-link           192.168.0.1       261
192.168.0.255              255.255.255.255  On-link           192.168.0.1       261
192.168.11.0               255.255.255.0    On-link           192.168.11.1      261
192.168.11.1               255.255.255.255  On-link           192.168.11.1      261
192.168.11.255             255.255.255.255  On-link           192.168.11.1      261
224.0.0.0                  240.0.0.0        On-link           127.0.0.1         306
224.0.0.1                  240.0.0.0        On-link           192.168.11.1      261
224.0.0.255                240.0.0.0        On-link           192.168.0.1       261
255.255.255.255            255.255.255.255  On-link           127.0.0.1         306
255.255.255.255            255.255.255.255  On-link           192.168.11.1      261
255.255.255.255            255.255.255.255  On-link           192.168.0.1       261
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128 On-link
12 261 fe80::/64 On-link
14 261 fe80::/64 On-link
14 261 fe80::2886:d9f:89d6:7135/128 On-link
12 261 fe80::8192:276e:ede:208d/128 On-link
1 306 ff00::/8 On-link
12 261 ff00::/8 On-link
14 261 ff00::/8 On-link
=====
Persistent Routes:
None

C:\Users\Administrator>_
```

Figure 12 - Route print table

This gives us valuable information on which gateways the packets much use to arrive at its designated location. A great tool for troubleshooting, and, for the inclined, it also gives the opportunity to understand the network in a more advanced way.

Task 5 – Observational Tasks

Identify the benefits of Type 1 Hypervisor software services and briefly evaluate some suitable products

The main benefits of type-1 hypervisors is their ability to run directly on the hardware of the host machine[1]. Here, the overlying operating system shares resources with the underlying hypervisor, making it run faster and more efficient[2].

Define the role of Routers in the Network Architecture, what types can be used?

The routers are the different machines' tool for communicating with each other. They send the packets to their wanted destination, as instructed by the computer itself, guided by IP addresses[3]. Routers can be internal, like the type used in this assignment. They can also be wireless, with modem capabilities built in. Routers can be classified after what their job is, not only the way they are engineered. Edge routers and core routers are an example[4].

Identify and discuss the usage of common Routing Protocols, what are the associated benefits of using Routing Protocols?

According to Cisco, routing protocols can be classified by their purpose, operation and behaviour[5]. The different protocols allow for different characteristics in scalability, implementation complexity and resource usage among others. Using routing protocols are important because they offer a standardised communication language, which makes it easier for the end-user to operate the system efficiently[5].

Define the role of Routing Tables, and what they are. Break down and analyse the information a Routing Table provides us with.

The routing tables main role is to aid troubleshooting. Maintaining networks and fixing issues requires an in-depth understanding of the different paths machines use to communicate regardless of the users understanding of a specific routing protocol. This is the main purpose of a routing table[6]. As seen in figure 12, the routing table provides us information on what gateway an interface uses, as well as which subnet mask it is assigned to.

What is the Subnet Mask, what is the significance of this in the Routing Table?

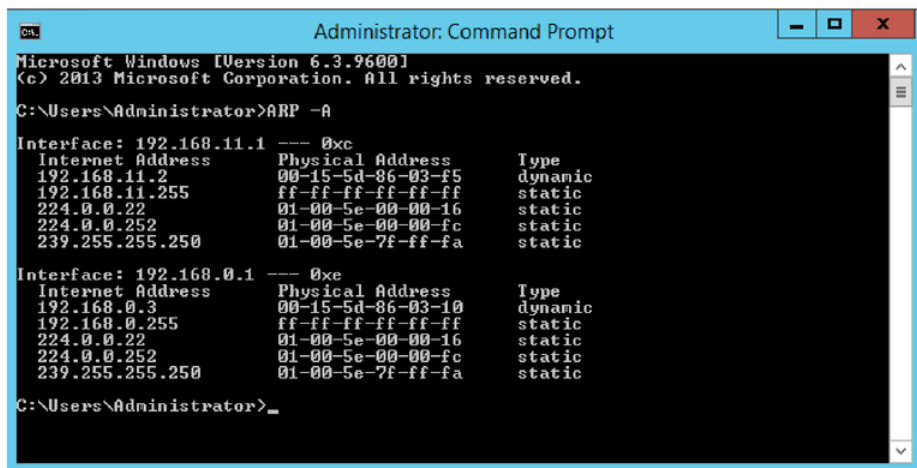
The subnet mask matches the IP address to the network ID. Since subnetting separates the host addresses from the network addresses, the routing table provides a way to visualise the way the network is interconnected[7].

Worksheet 2

This worksheet will explain the significance of advantages such as packet filtering, and the principles of FTP servers. It will also go through the ARP process in closer detail and explain through proper filtering techniques how to avoid contradictory filtering.

Task 1 – Address Resolution Protocol

This task demonstrates how to obtain network information on the link layer using the Address Resolution Protocol (ARP). The query ARP-A was ran in the command prompt on Cardiff, and the table in figure 13 got generated.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a

Interface: 192.168.11.1 --- 0xc
Internet Address      Physical Address      Type
192.168.11.2          00-15-5d-86-03-f5    dynamic
192.168.11.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.0.1 --- 0xc
Internet Address      Physical Address      Type
192.168.0.3           00-15-5d-86-03-10    dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\Administrator>
```

Figure 13 - ARP network link information

Figure 13 illustrates what IP address is associated with each physical address at the current moment, and their change depending on them being static or dynamic as also shown on the right.

Task 2 – Setting up an FTP Server

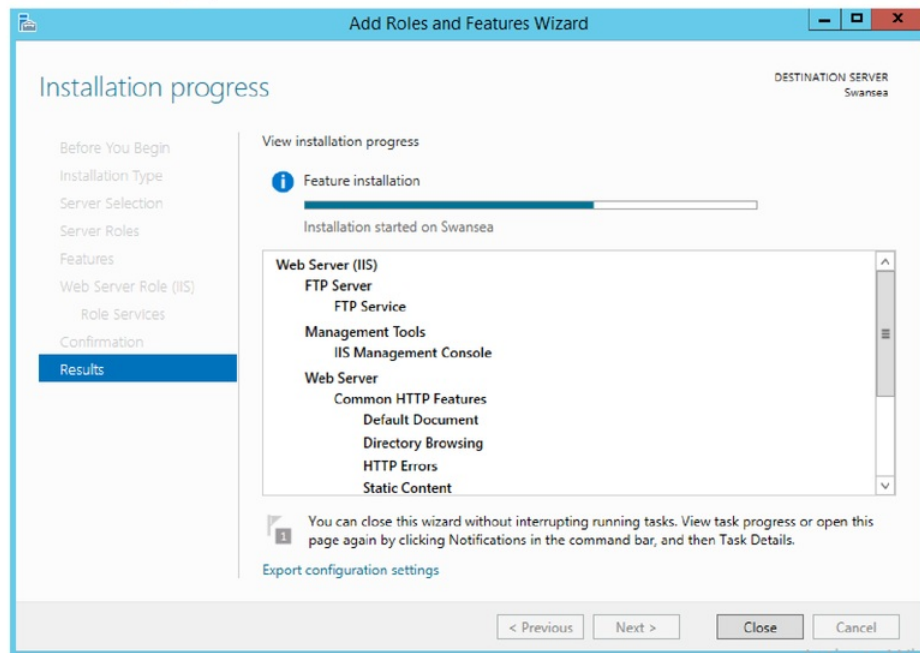


Figure 14 - FTP service installing

After installing the FTP service from the server manager dashboard on Swansea (figure 14), a new FTP user was created using the tools from the users and groups settings (figure 15), with the instructed username and password in the worksheet.

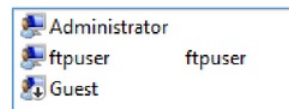


Figure 15 - New FTP user

A root folder was selected, as well as the authentication method (basic) and the Secure Sockets Layer (SSL) (turned off). The user was given read/write privileges over the Swansea server, and a banner was created to help identify the FTP server when connected to (figure 16). The working banner can be seen in figure 17.

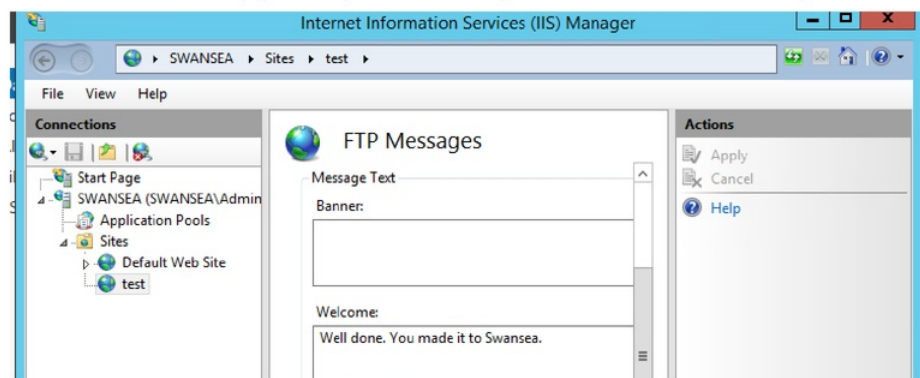
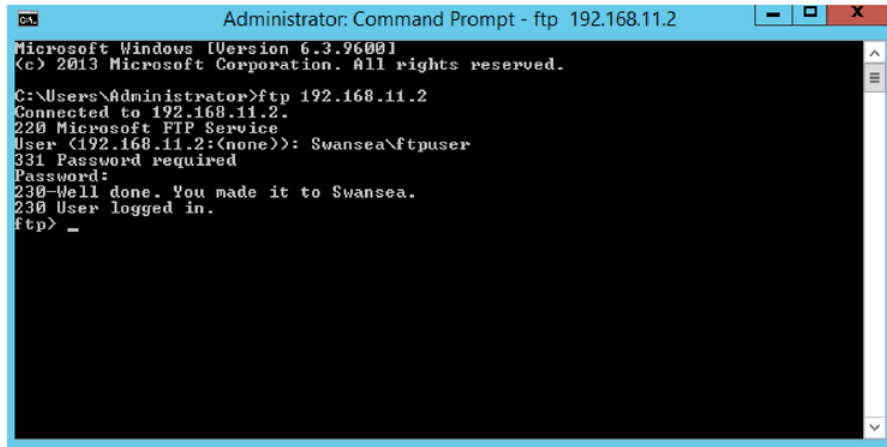


Figure 16 - FTP server welcome banner set

A new file was created in the root directory, so the actual FTP functionality could be assessed.

In the Cardiff server, a new folder dedicated for FTP downloads was created. Then, the command `ftp 192.168.11.2` was executed in the command prompt. The login credentials previously created were typed in (figure 17) and

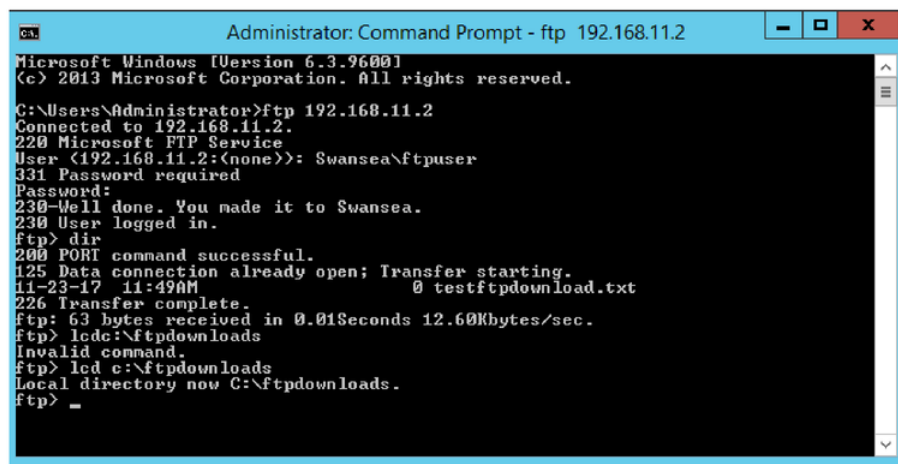


```
Administrator: Command Prompt - ftp 192.168.11.2
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.11.2
Connected to 192.168.11.2.
220 Microsoft FTP Service
User (192.168.11.2:(none)): Swansea\ftpuser
331 Password required
Password:
230-Well done. You made it to Swansea.
230 User logged in.
ftp> _
```

Figure 17 - Successful login to Swansea FTP server from Cardiff

the `dir` command was utilised to show the contents of the directory previously created. The host directory for downloads needed to be set with the command Local Directory Change: `lcd c:\ftpdnloads`, as seen in figure 18.



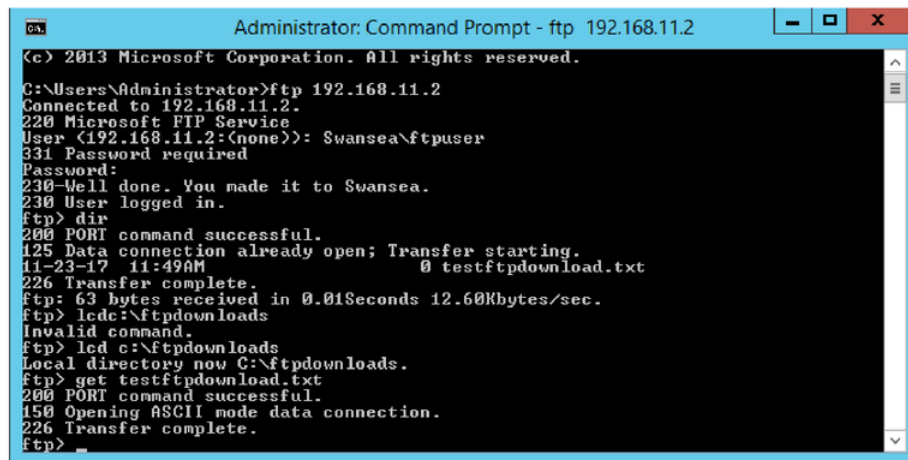
```
Administrator: Command Prompt - ftp 192.168.11.2
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.11.2
Connected to 192.168.11.2.
220 Microsoft FTP Service
User (192.168.11.2:(none)): Swansea\ftpuser
331 Password required
Password:
230-Well done. You made it to Swansea.
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-23-17 11:49AM 0 testftpdnload.txt
226 Transfer complete.
ftp: 63 bytes received in 0.01Seconds 12.60Kbytes/sec.
ftp> lcd c:\ftpdnloads
Invalid command.
ftp> lcd c:\ftpdnloads
Local directory now C:\ftpdnloads.
ftp> _
```

Figure 18 – Local Directory Change successful

After this was done, the FTP server was tested with the command `get testftpdnload.txt` (name of the file previously created). This initiated the

download, and the file appeared in the folder created for FTP downloads (figures 19).



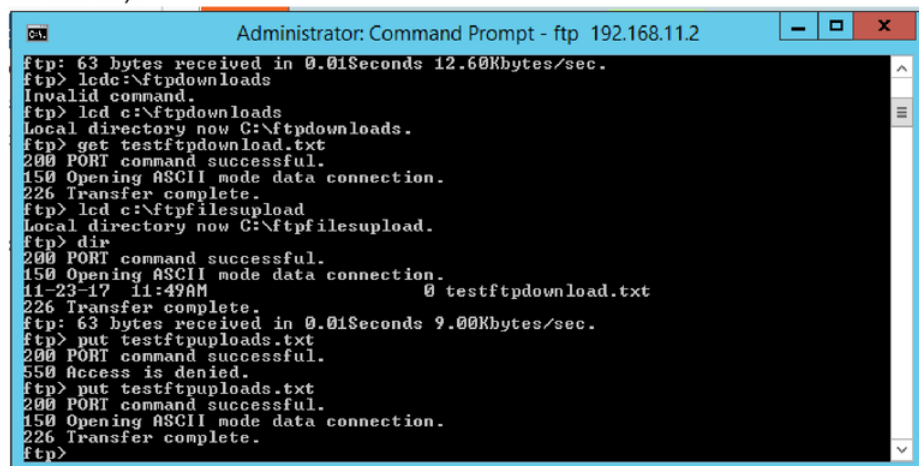
```

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.11.2
Connected to 192.168.11.2.
220 Microsoft FTP Service
User (192.168.11.2:(none)): Swansea\ftpuser
331 Password required
Password:
230 Well done. You made it to Swansea.
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-23-17 11:49AM 0 testftpdownload.txt
226 Transfer complete.
ftp> lcd c:\ftpdownloads
Invalid command.
ftp> lcd c:\ftpdownloads
Local directory now C:\ftpdownloads.
ftp> get testftpdownload.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp>
  
```

Figure 19 - Test file download complete

The upload was tested in the same manner, with a new folder created for uploading files on Cardiff, and the folder was chosen as the default folder using the lcd command. A new file was created, named testftpuploads.txt, and the command put testftpuploads.txt was used to upload the file to Swansea (figure 20 and 21).



```

ftp> 63 bytes received in 0.01Seconds 12.60Kbytes/sec.
ftp> lcd c:\ftpdownloads
Invalid command.
ftp> lcd c:\ftpdownloads
Local directory now C:\ftpdownloads.
ftp> get testftpdownload.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp> lcd c:\ftpfilesupload
Local directory now C:\ftpfilesupload.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
11-23-17 11:49AM 0 testftpdownload.txt
226 Transfer complete.
ftp> 63 bytes received in 0.01Seconds 9.00Kbytes/sec.
ftp> put testftpuploads.txt
200 PORT command successful.
550 Access is denied.
ftp> put testftpuploads.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp>
  
```

Figure 20 - FTP upload from Cardiff to Swansea completed

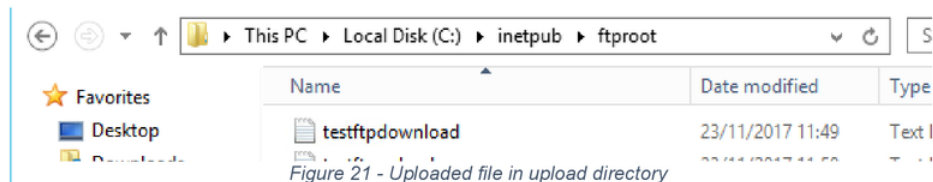


Figure 21 - Uploaded file in upload directory

Task 3 – Packet Filtering

The main purpose of this task was to demonstrate the capabilities of packet filtering and how to correctly set it up. For proof of concept, a ping from a client which has had its packet flow blocked by the inbound filter should fail.

The filter was set up on the 11-network on the router (Cardiff) to block packets coming from Lab to Swansea (figure 22). The 0-network was left untouched.

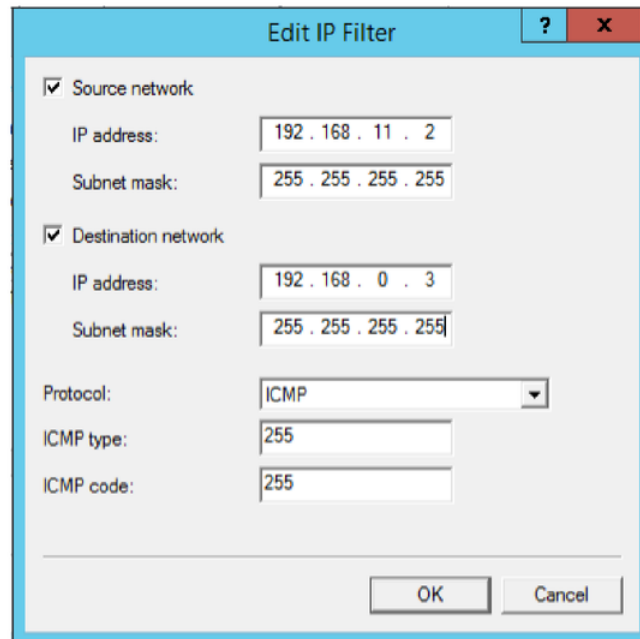


Figure 22 - Filter setup at Cardiff's 11-network interface

Then, two individual pings were performed to illustrate that only the 11-network interface had been affected by the packet filtering options. In figure 23, we see the ping being blocked by the filter when trying to communicate from Swansea to Lab. In figure 24, we see the packet arriving at Cardiff's unchanged 0-network interface as predicted.

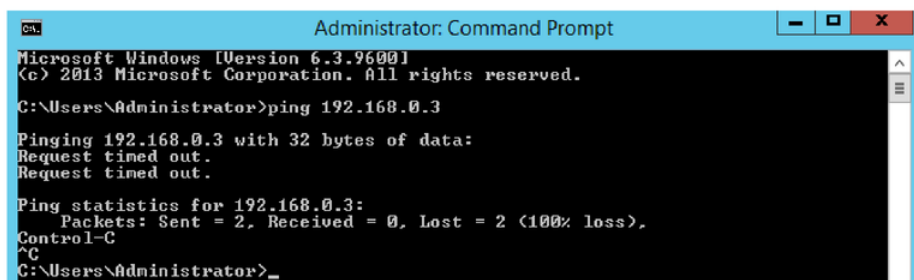


Figure 23 - Packets blocked by inbound filter

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=342ms TTL=127
Reply from 192.168.0.1: bytes=32 time=2ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 342ms, Average = 86ms

C:\Users\Administrator>
```

Task 4 – Filtering FTP Services

Before any new filters were created, the existing ones were removed to avoid contradictory filtering. The task at hand was to filter out all connections to the FTP server on Swansea. A new filter was created on the router (Cardiff) with these attributes (figure 25).

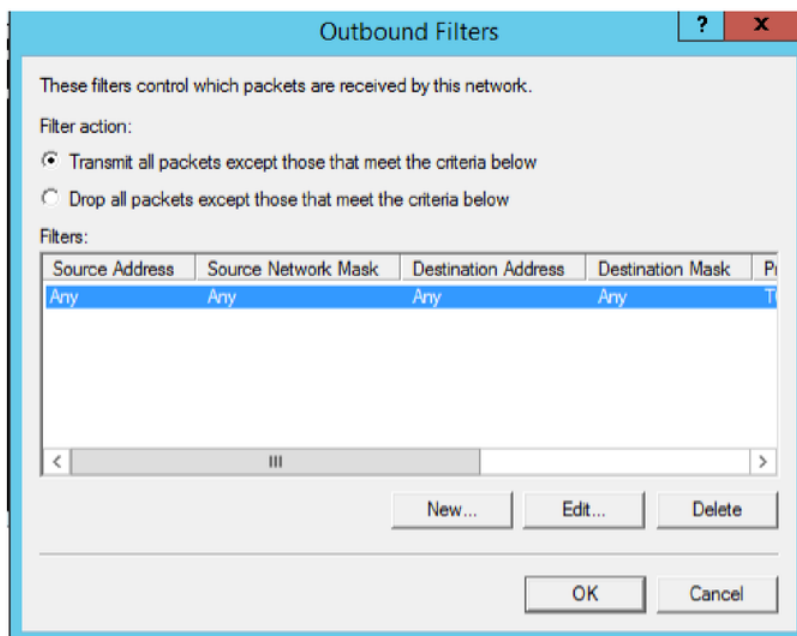


Figure 25 - Outbound filter set up on Cardiff

This was tested by attempting to connect to the server (figure 26).

```
Administrator: Command Prompt - ftp 192.168.11.2
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.11.2
> ftp: connect :Connection timed out
ftp>
```

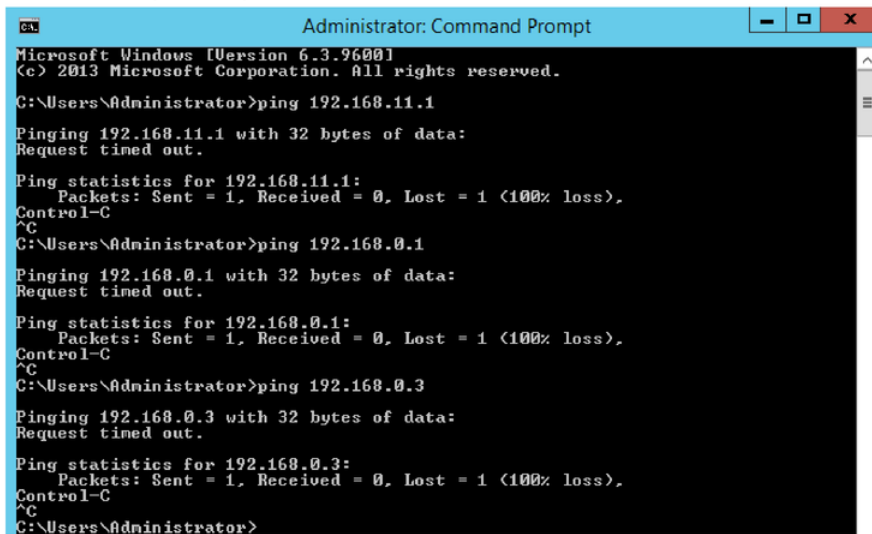
Figure 26 - Connection to the FTP failed

The filters were then removed again, preparing for the task of filtering out all access to the FTP-server, except for connections from Cardiff. This required an inbound filter blocking all TCP-ports used for FTP. The filter was tested by attempting to connect from Cardiff itself and the other machines. The screenshots for this are regrettably missing along with the rest of task 4, although the result for this experiment is the same as in figure 26.

The filters were again removed, and a new filter was put in place to block only Cardiff from accessing the FTP server.

Task 5 – Only Allow FTP

The Cardiff server was set up with inbound and outbound filters excluding all traffic except TCP-ports 20 and 21. This allowed for FTP-traffic to flow through.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.11.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    ^C
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    ^C
C:\Users\Administrator>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.3:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    ^C
C:\Users\Administrator>
```

Figure 27 – Swansea is unable to ping anywhere

```
Administrator: Command Prompt - ftp 192.168.11.2
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.11.2
Connected to 192.168.11.2.
220 Microsoft FTP Service
User (192.168.11.2:(none)): ftpuser
331 Password required
Password:
230-Well done. You made it to Swansea.
230 User logged in.
ftp>
```

Figure 28 - FTP request from Cardiff is still functional

```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Group2>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Control-C
^C
C:\Users\Group2>ping 192.168.11.1
Pinging 192.168.11.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.11.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Control-C
^C
C:\Users\Group2>ftpuser 192.168.11.2
'ftpuser' is not recognized as an internal or external command,
operable program or batch file.
```

Figure 29 - Lab cannot utilise FTP or Ping anywhere

As a result, pings are blocked in all directions, and only FTP traffic is allowed to flow (figures 27, 28 and 29).

Task 6 – Observational Tasks

Describe (using appropriate illustrations) how the ARP process operates in Networking

The address resolution protocol process resolves which interface a packet should be sent by utilising the MAC-address of the interface. This is shown below[8]:

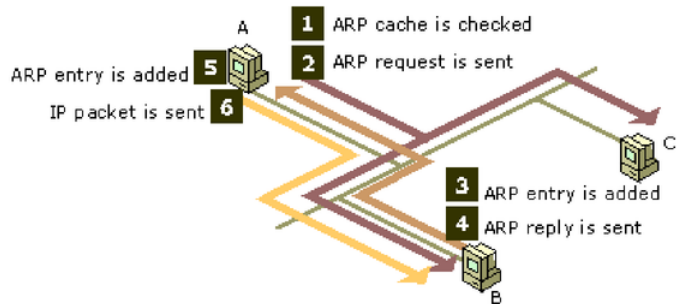


Image courtesy of Microsoft Technet[8]

This makes it possible to send data to a specific receiving party, as well as identifying where the data came from.

Explain what packet filtering is, and why it is called IP Packet filtering. Also explain why you would use packet filtering in your network and what the benefits are

Packet filtering is used to control which machines can receive/send packets, or more specifically, what types of packets are allowed through. Packet filtering can utilise the opening or closing of ports, or simply allowing or blocking different services depending on their type. It is an extremely important tool when connecting an intranet to the internet. This provides an extra layer of security, and works as a form of access control[9].

Why is it possible for contradictory filters to occur when you use packet filtering? Give an example of a Contradictory Filter:

Contradictory filters appear as a result of a breach in logic. Example: If a filter on Cardiff's 0-interface allows FTP data, and another filter on Cardiff's 11-interface blocks it, the packets can still get through the other channel to reach its destination. This renders both filters useless.

FTP Server is just one Role/Service we can configure our Server to provide? What other roles can the Server provide that would benefit our Infrastructure in both a local and remote context?

Several services are required for a network to operate smoothly. DNS services are important for resolving actual address names, making it easier for the end-user to remember URL's[10]. DHCP makes setting up new interfaces and peripherals easier, as it assigns IP-addresses automatically and keeps a record of the nodes connected to the network, reducing the administration effort[11]. RRAS gives the machine routing capabilities, which is useful for controlling packet flow over different interfaces[12].

Worksheet 3

Worksheet 3 will cover TCP/IP configuration utilising the DHCP protocol. As part of the pre-setup, each machine was given three network interfaces on its networks. The original static IP-addresses were written down for future use.

Task 1 – Understanding Different TCP/IP Configurations

Here, we set the 0-network on Lab client to automatic private IP addressing through the GUI. Then the command prompt was opened, and the ipconfig/release command was executed. This ensures that all static IP-addresses are removed. Then, the ipconfig/renew command was executed to renew the IP addresses. The machine now lacks a DHCP server (figure 30).

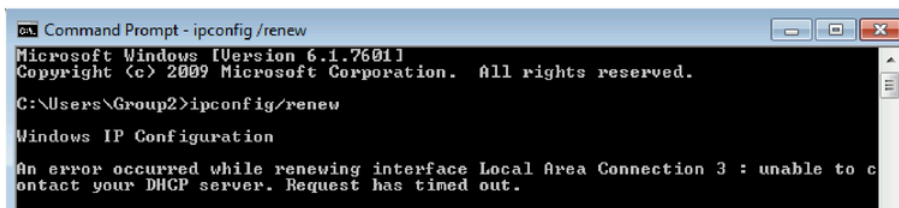


Figure 30 - Computer is unable to contact the non-existing DHCP-server.

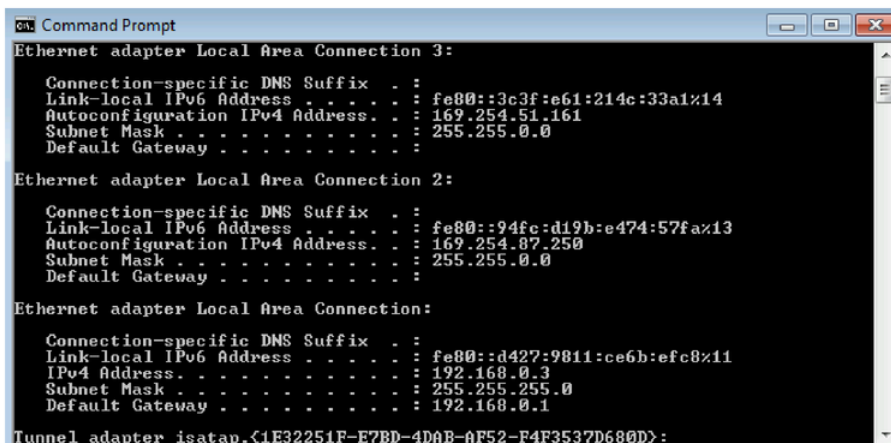


Figure 31 - Autoconfiguration enabled, see subnet masks

In figure 31, we see the subnet masks has changed to 255.255.0.0, and the IP-addresses are in the APIPA-range. There's also no default gateway, which means Autoconfiguration has been enabled.

Task 2 – Installing the DHCP Server

The cleared static IP-addresses from the previous task were now reinstated to their former values. Next was installing the DHCP server, this was done simply by using the post-install wizard for DHCP in the GUI of the Cardiff machine.

Task 3 – Authorising the DHCP Server

This task was simply authorising the DHCP server, to prepare it for Active Directory. This was also done in the Cardiff GUI. No screenshots are provided for this task and the previous due to their simplicity.

Task 4 – DHCP Scopes

A question posed in this task was: Why are reservations important when using DHCP? Reserved IP-addresses are often a good idea for hardware and units that never leave the network or units that require extra stability and continuous connections like servers and printers.

Part A – Creating Scope Lease

To set DHCP scopes on our network, we added a new DHCP scope in the IP configuration window of the Cardiff machine. The scope was set between 192.168.0.2 to 192.168.0.254.

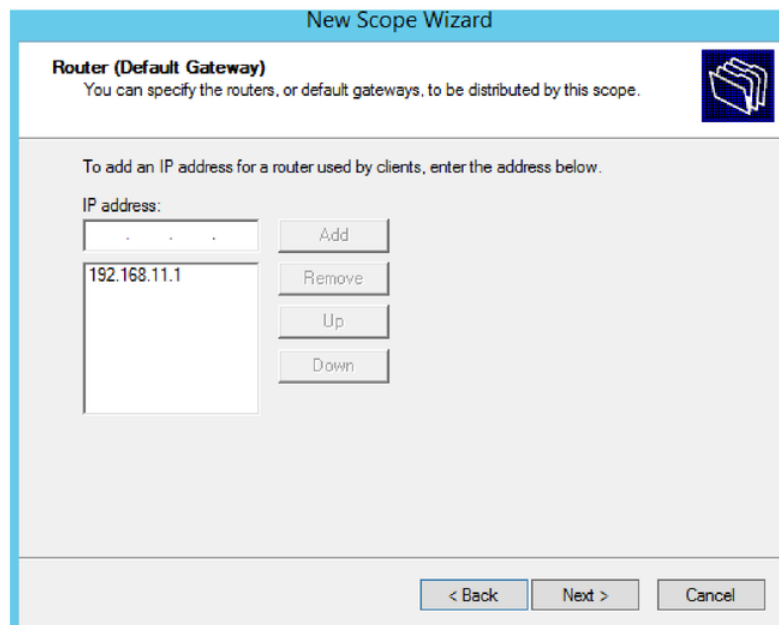


Figure 32 - DHCP scope window

Part B – Obtaining IP Address

In Swansea's TCP/IP settings, the server was set to obtain IP addresses and DNS servers automatically. The IP addresses were thereafter released and renewed through the command prompt.

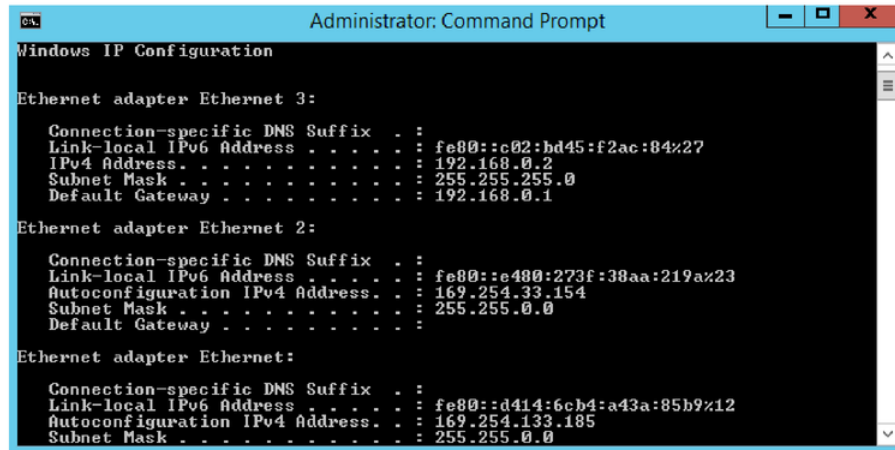


Figure 33 - Swansea's IP address after DHCP scope configuration. See Ethernet 3.

Task 5 – Configuring Reservations

The IP address lease for Swansea was changed to a reserved address. Thereafter, the 0-network on the client was changed to be reserved by using its MAC-address as a reference point. The new reserved IP address was set to 192.168.0.5, which we see after a renew in figure 34.

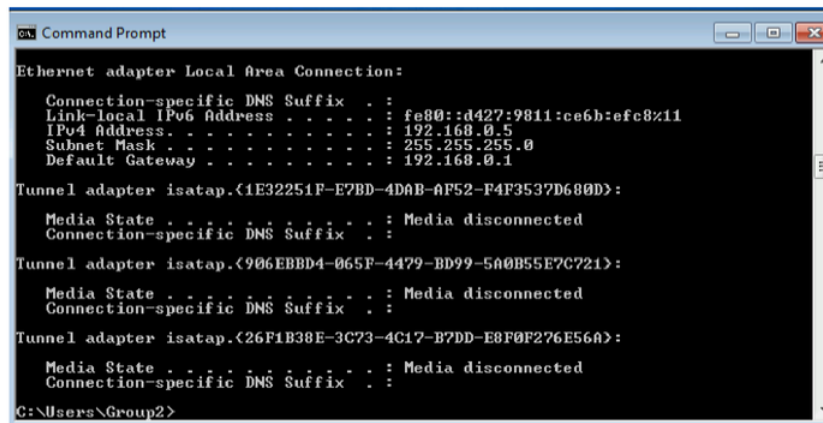
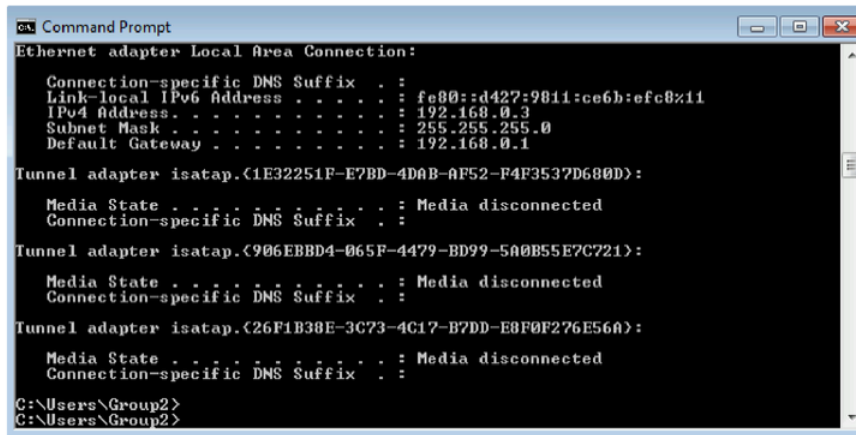


Figure 34 - Lab IP address 0.5

As a proof of concept and understanding, the IP reservation was changed manually to 0.3, and the renew revealed once again that the change had gone through. See figure 35.



```
Command Prompt
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::d427:9811:ce6b:efc8%11
    IPv4 Address. . . . . : 192.168.0.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{1E32251F-E7BD-4DAB-AF52-F4F3537D680D}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Tunnel adapter isatap.{906EBBD4-065F-4479-BD99-5A0B55E7C721}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Tunnel adapter isatap.{26F1B38E-3C73-4C17-B7DD-E8F0F276E56A}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\Group2>
C:\Users\Group2>
```

Figure 35 - Lab IP address as 0.3

Task 6 – Observational Tasks

Define the role of the DHCP Server in your Network?

The DHCP server assigns IP addresses to the different devices connected to the network. It also assigns default gateways and subnet masks. The main purpose of DHCP is to reduce the administration effort, making the network more autonomous[11].

What happens when we have dynamically configured TCP/IP for our NIC, but then consequently cannot contact a DHCP server?

If no DHCP server is available, Autoconfiguration is activated, and the NIC gets assigned an IP address in the APIPA range.

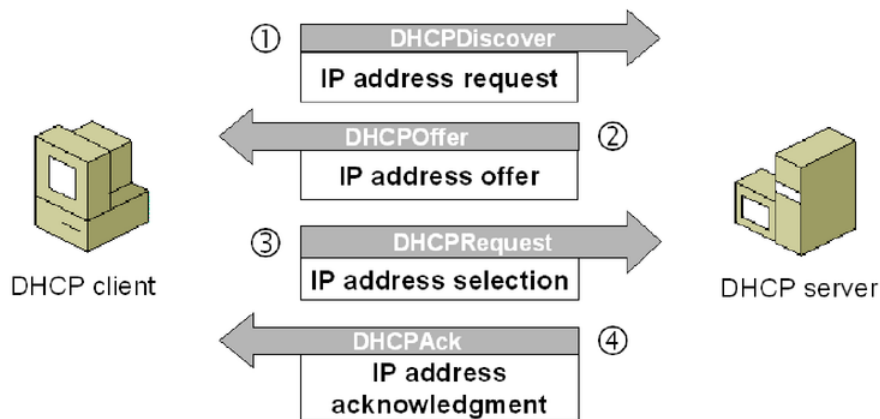
Illustrate, with illustrations, the 4-stage process involved when DHCP clients look to obtain an IP address via DHCP.

The DHCP clients talk to the server in 4 steps, known as the DORA-process. This is an abbreviation of Discover, Offer, Request and Acknowledge.

The client first broadcasts that it needs a DHCP server (discover).

The DHCP server then receives the broadcast and offers the client an available IP address (offer).

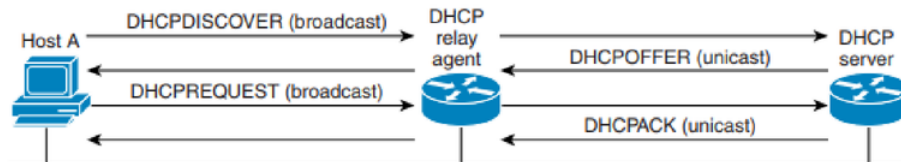
The client then requests this IP address, (request) and the server acknowledges the address assignment (acknowledge). See illustration below[13]:



DORA process. Image and information courtesy of imedita.com[13]

Describe the advantages of using a relay agent. Explain (with descriptions and illustrations) how and why we would setup the Relay Agent on our router?

The relay agent is the technique utilised by DHCP to communicate between the server and client. The messages sent include gateway information, link information for the different interfaces, etc. This is useful when communicating across differing subnets[14].



As seen in the figure above[14], this is how the DORA-handshake works on a macro-level. This also illustrates the basic setup location for a relay agent.

Worksheet 4

This worksheet will contain tasks utilising the Domain Name Service (DNS) system, and how to deploy Active Directory.

Task 1 – Understanding Active Directory and DNS

Firstly, Active Directory needed to be installed on the Cardiff server. The domain name was nwtraders.msft.

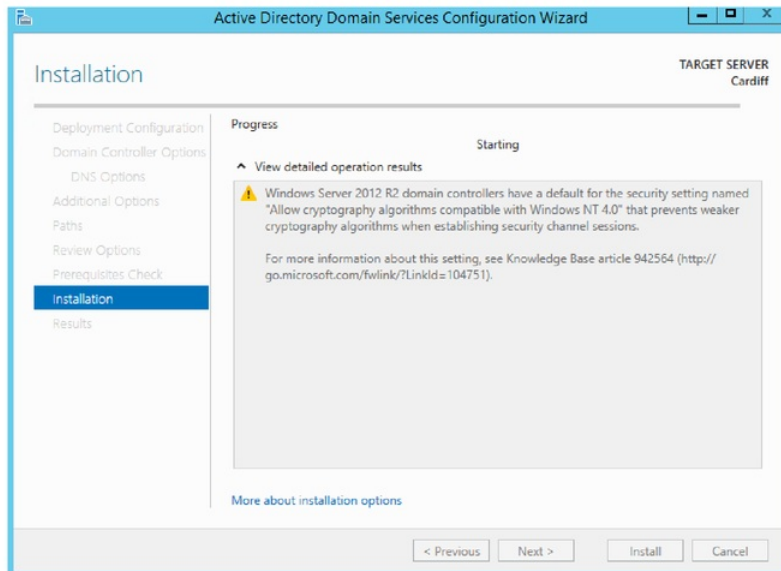


Figure 36 - Setting up Active Directory on Cardiff

The Swansea and Lab machine were added to the domain (figures 37, 38 and 39).

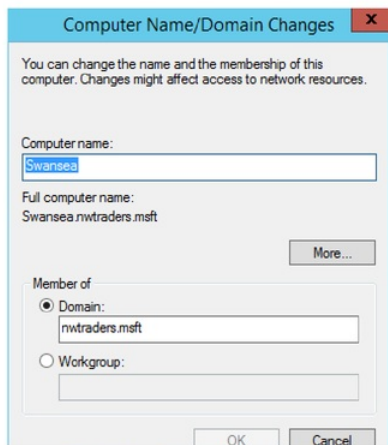


Figure 37 - Swansea added to the nwtraders.msft domain

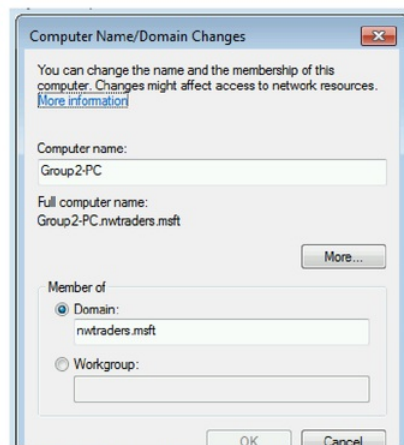


Figure 38 – Lab added to nwtraders.msft domain

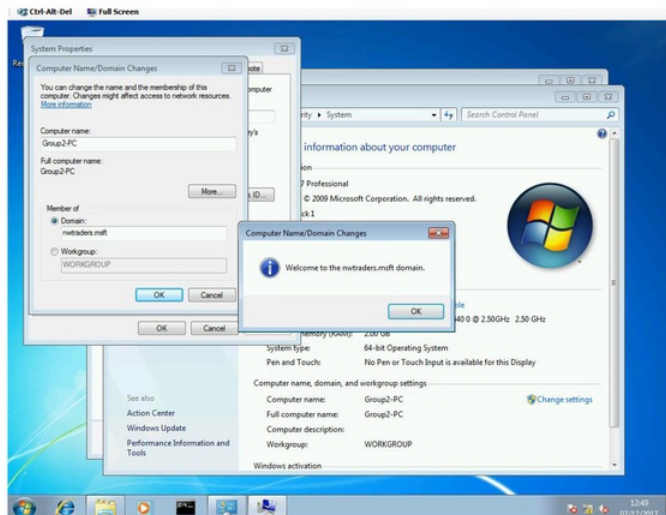


Figure 39 - Lab successfully joined nwtraders.msft domain

Now, we can confirm that the server and client are on the same domain from the Cardiff server's Active Directory settings (figure 40).

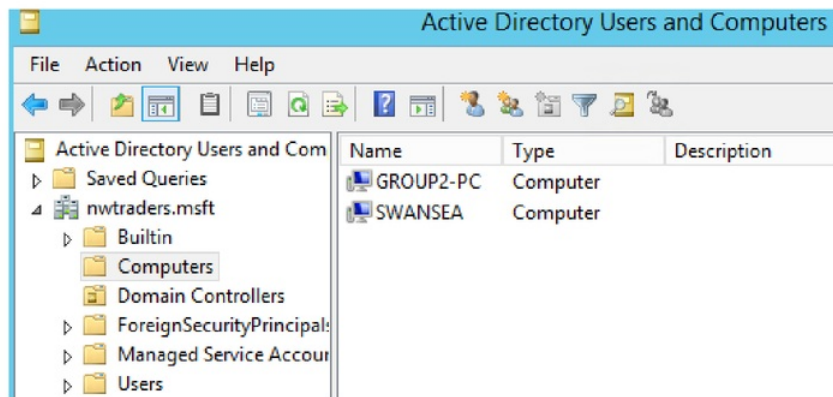


Figure 40 - Active Directory listing for the nwtraders.msft domain

The DNS server service was installed on Swansea. In Cardiff, we made the DNS server a client of itself (figure 41)

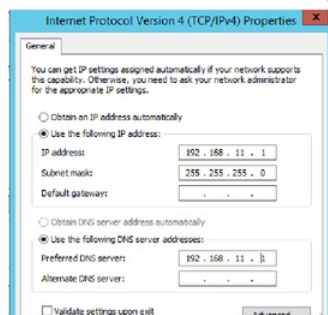


Figure 41 – Cardiff DNS server client of itself

The next step was to configure the DNS server to use a DNS forwarder (figure 42). The root hints were then updated, and the DNS cache cleared (figures 43 and 44).

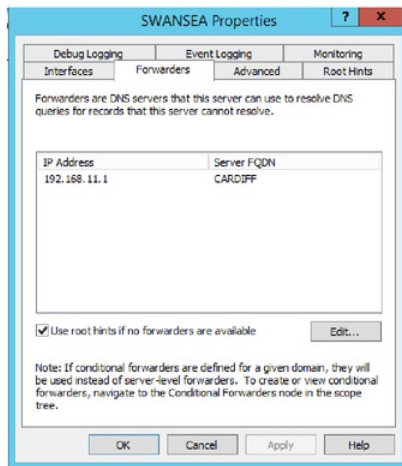


Figure 42 - DNS forward enabled for Cardiff

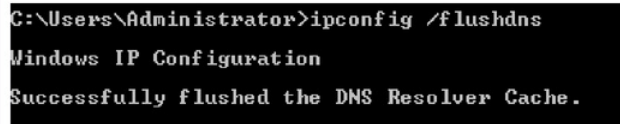


Figure 44 - DNS cache cleared

Server Fully Qualified Domain Name (FQDN)	IP Address
192.168.11.2.	[192.168.11.2]
a.root-servers.net.	[198.41.0.4]
b.root-servers.net.	[192.228.79.201]
c.root-servers.net.	[192.33.4.12]
d.root-servers.net.	[199.7.91.13]
e.root-servers.net.	[192.203.230.10]

Figure 43 - Root hint table

There are scenarios where having control over the DNS cache and being able to clear it is useful. These scenarios include server migration, privacy issues, maintenance scenarios etc[15].

Task 2 – DNS zones

A secondary forward lookup DNS zone was created in Swansea, and was named nwtraders.msft. Zone transfers were then enabled, as seen in figure 45.

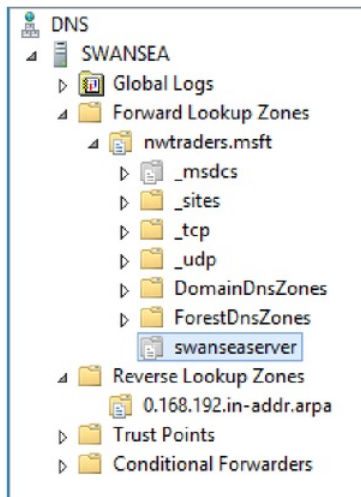


Figure 45 - Zone transfer enabled

Now, we configure the reverse lookup zone in Swansea. This was done through the previously installed DNS console, with the preferred DNS server on Cardiff as a reference (figure 46)

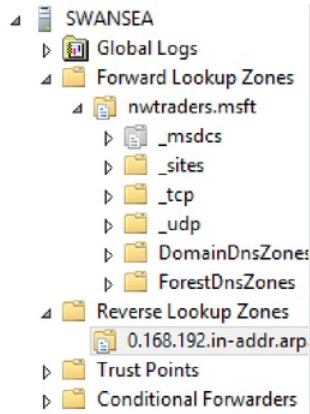


Figure 46 - Reverse lookup zone on Swansea. Zone transfer works.

Now, a new primary forward lookup zone was created, with the prefix swanseaserver. The FQDN was now swanseatraders.nwtraders.msft.

Task 3 – DNS Application

A Virtual directory was created on Swansea, with the name “test”. A default root directory for a website was created, and its location was set to the highest priority in the Virtual Directory.

Finally, a simple HTML script was created[16] and added to the root folder to output “hello world” when entering the URL in a browser on Lab. (figure 47).

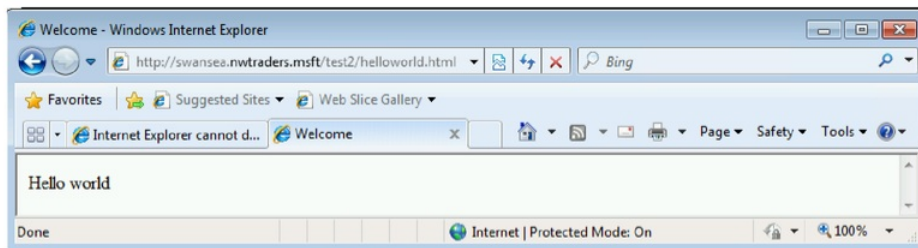


Figure 47 - Script working, page loaded

Task 4 – Observational Tasks

What steps does a client take (what is the process involved) when trying to resolve a Name to an IP address?

Anecdotally, the human brain is extremely bad at remembering numbers. This requires a service that converts IP addresses to intelligible text, e.g. google.com. The DNS server resolves names from IP addresses and vice versa. The process is as follows: The user inputs google.com into the browser. The computer does not know where or what google.com is, so it contacts a DNS resolver. The DNS resolver speaks to other DNS resolvers, hoping that one of the resolvers knows where “google” on the “com” domain is. When a result is acquired, the “google.com” query is translated to the destination IP address, and communication is established between the client (user) and the host (Google)[17].

Describe how the Recursive Query and Iterative Query Processes resolve DNS Client Requests?

The recursive query is the initial query from the host. A recursive query expects either an address or an error in return, as it is the first step of resolving an address or a name[18]. The iterative query takes it one step further, as the response must either be a location, name or address[18].

Explain the significance of root hints and how this process enables us to resolve names that are not managed (or kept in an authoritative DNS server in our network)?

The root hint file is a record of host destinations useful when querying locations or addresses outside the scope of the DNS server. If a query hits a dead-end, the query goes to the root hint list and finds an appropriate destination for the packet[19].

We have a Server called Server1, this server will be hosted in a subdomain called ‘subcontA’ with a root domain called nwtraders.msft, answer the following questions:

(1). What is the exact FQDN for this host.

The full FQDN is Server1.subcontA.nwtraders.msft.

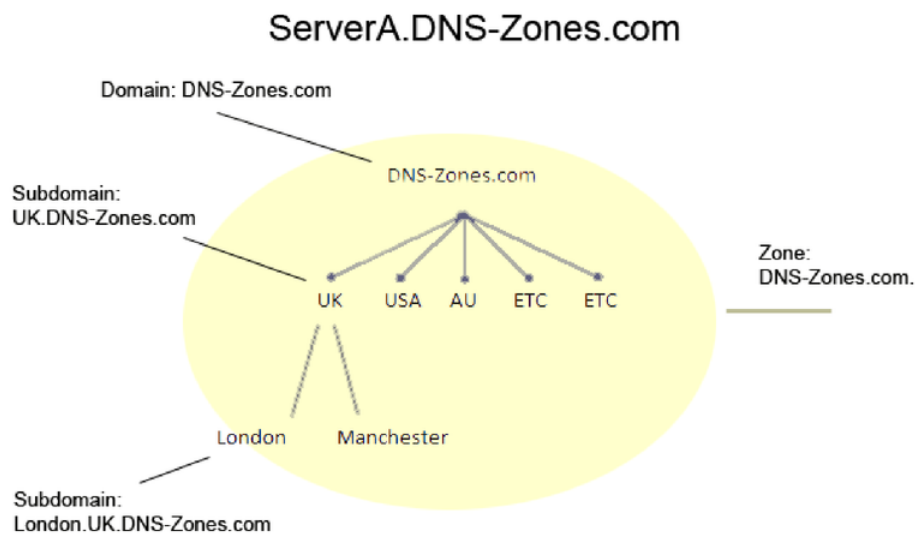
(2). Illustrate how the Domain Name System breaks up this FQDN into Host and Domain Namespace.

This FQDN is broken up into 3 separate entities, which are as follows[20]:

1. Host name (Server1)
2. Subdomain (subcontA)
3. Primary domain (nwtraders.msft)

Explain how DNS Zones are used in DNS, give examples to illustrate the use of multiple zones and how these can be used to manage resource records of domains. What important factors/characteristics do we need to be aware of?

DNS zones is a system of delegations which simplify finding specific addresses within a network. Since the internet is vast, finding a specific address is a complex task. Therefore, DNS is split up into different physical zones, each referring to the next zone. An abstraction of this can be the following: If you call a customer support hotline at any company and ask to speak to Dan in the warranty section, the person who picks up the phone doesn't know Dan or his number. What he does know, is the number for the warranty section. The call gets forwarded to warranty, and they have their own list of numbers pointing you in the direction of Dan[21]. This abstraction also works for IP addresses and routing. The different layers of a domain name are resolved through a system of subdomains, and the different DNS servers handling them. See image below[22] for reference.



Worksheet 5 – Evaluation of Clustering Strategies

Clustering is the splitting of workload between multiple servers. A web-development system can be split in to three layers. The client tier, application tier and the data tier. Here, the client layer interacts with the user, and handles requests like ordering and site navigation. The application tier contains the applications running in the background to complete these requests. This tier uses data from the data tier, which contains all the necessary information to make the distribution do something useful[23].

This makes clustering ideal. Each tier can be handled by a separate server, in order to increase efficiency, as each tier requires different levels of server performance. These machines (nodes) work together to make the application appear seamless for the end-user, making a virtual machine[24]. The machines in the clusters are also fulfilling tasks like making the system redundant, utilising failover clusters[24]. A good example of resource delegation is the Google search engine. Google handles millions upon millions of search queries every day. This is too much for one machine to handle, so the workload is split up over several machines placed around the globe[25].

References

- [1] B. Golden, *Virtualization for dummies*. Wiley, 2007.
- [2] S. Meier, "IBM Systems Virtualization: Servers, Storage, and Software." [Online]. Available:
<http://www.redbooks.ibm.com/redpapers/pdfs/redp4396.pdf>. [Accessed: 14-Feb-2018].
- [3] Cisco Networking Academy, "Introduction - Cisco Networking Academy's Introduction to Routing Concepts," *Cisco Press*, 2014. [Online]. Available:
<http://www.ciscopress.com/articles/article.asp?p=2180208&seqNum=3>. [Accessed: 14-Feb-2018].
- [4] D. Thakur, "Types of Routers." [Online]. Available:
<http://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-routers-explain-types-of-routers>. [Accessed: 14-Feb-2018].
- [5] Cisco Networking Academy, "Types of Routing Protocols - Cisco Networking Academy's Introduction to Routing Dynamically," 2014. [Online]. Available:
<http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7>. [Accessed: 14-Feb-2018].
- [6] Cisco Networking Academy, "The Routing Table (3.5) Cisco Networking Academy's Introduction to Routing

Dynamically,” 2014. [Online]. Available:
<http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=12>. [Accessed: 14-Feb-2018].

[7] IPlocation.net, “What is a Subnet Mask?” [Online]. Available:
<https://www.iplocation.net/subnet-mask>. [Accessed: 14-Feb-2018].

[8] Microsoft Technet, “ARP Process.” [Online]. Available:
<https://technet.microsoft.com/en-gb/library/cc940010.aspx>.
[Accessed: 14-Feb-2018].

[9] Microsoft Technet, “IP Packet Filtering.” [Online]. Available:
<https://technet.microsoft.com/en-gb/library/cc957881.aspx>.
[Accessed: 14-Feb-2018].

[10] M. Brain and S. Crawford, “How Domain Name Servers Work
| HowStuffWorks.” [Online]. Available:
<https://computer.howstuffworks.com/dns.htm>. [Accessed:
14-Feb-2018].

[11] Microsoft technet, “What Is DHCP?: Dynamic Host
Configuration Protocol (DHCP),” 2003. [Online]. Available:
[https://technet.microsoft.com/en-gb/library/cc781008\(v=ws.10\).aspx](https://technet.microsoft.com/en-gb/library/cc781008(v=ws.10).aspx). [Accessed: 14-Feb-2018].

[12] Microsoft Developer Network, “Routing and Remote Access

Service.” [Online]. Available:

<https://msdn.microsoft.com/en-us/library/Aa446768>.

[Accessed: 14-Feb-2018].

- [13] S. Singh, “DHCP Concepts and Configuration in Real Cisco Router,” 2015. [Online]. Available:
<http://imedita.com/blog/dhcp-in-cisco-packet-tracer/>.
[Accessed: 14-Feb-2018].
- [14] Cisco, “Cisco Application Control Engine Module Routing and Bridging Configuration Guide Configuring the DHCP Relay Cisco Application Control Engine Module Routing and Bridging Configuration Guide DHCP Server and Client Overview.”
- [15] S. Laverty, “Is There a Need to Clean the DNS Cache? | It Still Works | Giving Old Tech a New Life.” [Online]. Available:
<https://itstillworks.com/there-need-clean-dns-cache-25636.html>. [Accessed: 14-Feb-2018].
- [16] mkyong, “Html Tutorial Hello World,” 2012. [Online]. Available: <https://www.mkyong.com/html/html-tutorial-hello-world/>. [Accessed: 14-Feb-2018].
- [17] Cisco, “Understanding the Domain Name System - Cisco,” *Cisco tech support*, 2005. [Online]. Available:
<https://www.cisco.com/c/en/us/support/docs/ip/domain->

name-system-dns/12683-dns-descript.html. [Accessed: 14-Feb-2018].

- [18] Catchpoint, "Name to IP Address," *Catchpoint blog*, 2014. [Online]. Available: <http://blog.catchpoint.com/2014/07/01/dns-lookup-domain-name-ip-address/>. [Accessed: 14-Feb-2018].
- [19] Microsoft technet, "Root Hints Files," *Technet*. [Online]. Available: <https://technet.microsoft.com/en-us/library/cc958982.aspx>. [Accessed: 14-Feb-2018].
- [20] Indiana University, "About fully qualified domain names (FQDNs)," *IU Knowledge Base*, 2017. [Online]. Available: <https://kb.iu.edu/d/aiuv>. [Accessed: 14-Feb-2018].
- [21] ISO Training Institute, "DNS - what are DNS ZONES ? - YouTube," 2017. [Online]. Available: <https://www.youtube.com/watch?v=Jlwi6ii-rzI>. [Accessed: 14-Feb-2018].
- [22] "DNS Zones Explained | Think Like A Computer." [Online]. Available: <https://www.think-like-a-computer.com/2011/06/11/dns-zones-explained/>. [Accessed: 14-Feb-2018].
- [23] Microsoft Developer Network, "Three-Tiered Distribution." [Online]. Available: <https://msdn.microsoft.com/en->

us/library/ff647546.aspx. [Accessed: 14-Feb-2018].

- [24] ESDS, "Cluster Computing: Definition and Architecture of a Cluster." [Online]. Available:
<https://www.esds.co.in/blog/cluster-computing-definition-and-architecture-of-a-cluster/#sthash.vBg3fjN9.dpbs>.
[Accessed: 14-Feb-2018].
- [25] C. S. Yeo, R. Buyya, H. Pourreza, R. Eskicioglu, P. Graham, and F. Sommers, "Cluster Computing: High-Performance, High-Availability, and High-Throughput Processing on a Network of Computers."

NOSS assignment - Toby

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

61 / 100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20



Comment 1

No apostrophe here. "unique resource locators" not "unique resource locator's" - it's a plural, not a possessive.

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

GRADING FORM: SMU GENERIC_GJ

THORBJORN RAVNAAS KRISTIANSEN

61

RESEARCH-INFORMED LITERATURE

- | | | |
|---|--|----------|
|  | A very good number of sources used, though a massive over-reliance on dubious web sources. You should aim to rely primarily on peer-reviewed material (journal articles are good) where possible. Some web sources can be acceptable - e.g. you've used TechNet in a fair few places. Microsoft can be considered authoritative, though not necessarily objective on their technologies - fine to cite, though caution must be taken when talking about anything potentially subjective. | 6 |
|---|--|----------|

KNOWLEDGE AND UNDERSTANDING

- | | | |
|---|---|----------|
|  | Good knowledge and understanding displayed - however, worksheet 5 is extremely brief for the number of marks assigned to it. This is a real shame - the work is otherwise largely worthy of a first, but limited by the lack of detail in this section. | 9 |
|---|---|----------|

ANALYSIS

- | | | |
|---|---|----------|
|  | Some evidence of analysis clear - synthesis of material in places. You could be more explicit in this, however - cite a number of sources you've read to form a single argument. Again, limited by the lack of detail in worksheet 5. | 9 |
|---|---|----------|

PRACTICAL APPLICATION AND DEP.

- | | | |
|---|---|-----------|
|  | Some very good practical work, worksheets completed to a reasonable standard. Comments are generally good. A few key images would also help - | 29 |
|---|---|-----------|

e.g. other than one obscure screenshot, there's a lack of depiction of the other side of the DHCP process.

SKILLS FOR PROFESSIONAL PRAC.



You write very well. Be a little careful combining apostrophes with acronyms, and take care to avoid run-on sentences. A well-presented document.

8