

Liam Blunt Worksheet 1-5

by Liam Joseph Mark Blunt

FILE	4166_LIAM_JOSEPH_MARK_BLUNT_LIAM_BLUNT_WORKSHEET_1-5_100686_1545206842.DOCX (7.22M)		
TIME SUBMITTED	14-FEB-2018 04:37 PM (UTC+0000)	WORD COUNT	3666
SUBMISSION ID	83184572	CHARACTER COUNT	22027

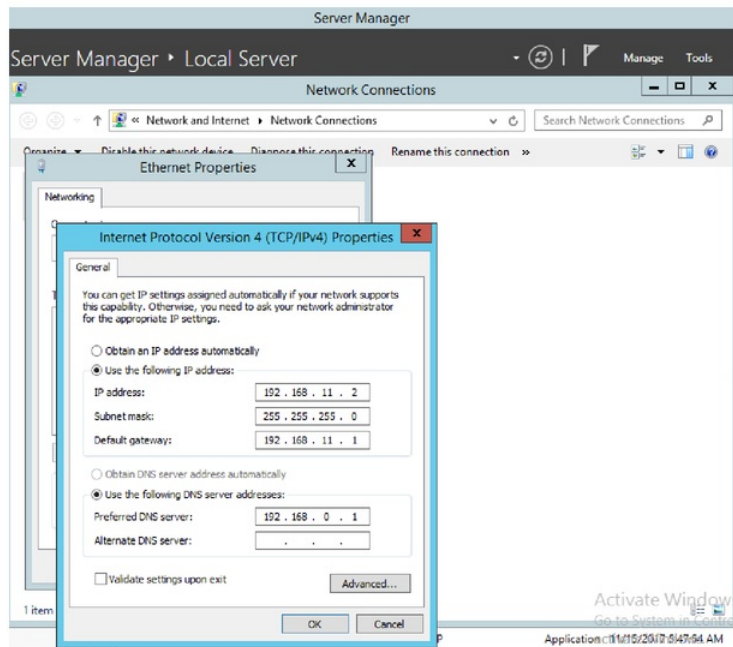
Table of Contents

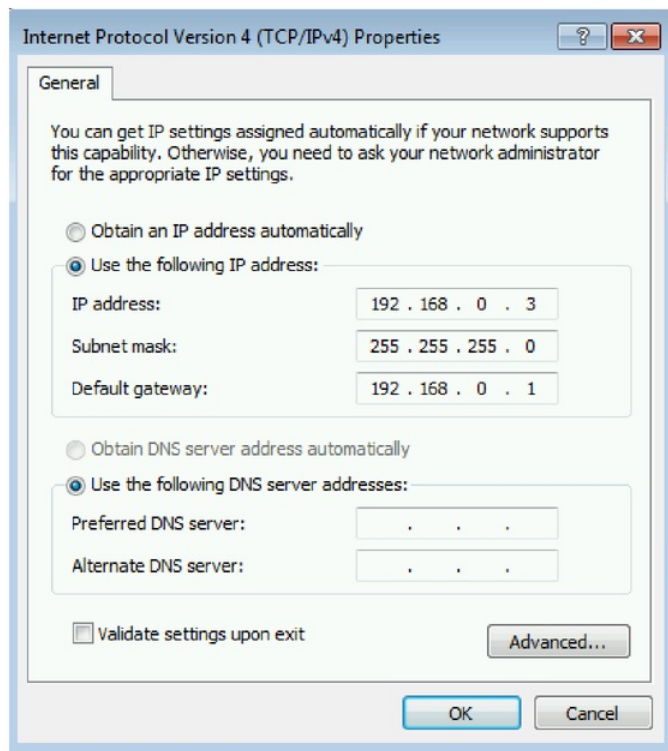
Worksheet 1	2
Task 1	2
Task 2	3
Task 3-	5
Task 4	7
Task 5	7
Worksheet 2	9
Task 2	9
Task 3	10
Task 4	13
Task 5-	16
Task 6-	17
Worksheet 3	18
Task 1	18
Task 2	18
Task 3	18
Task 4	19
Task 5-	20
Task 6	22
Worksheet 4	23
Task 1	23
Cardiff Tasks	23
Swansea Tasks	27
Task 2	28
Task 3	28
Task 4	29
Worksheet 5	31
Bibliography	32

Worksheet 1

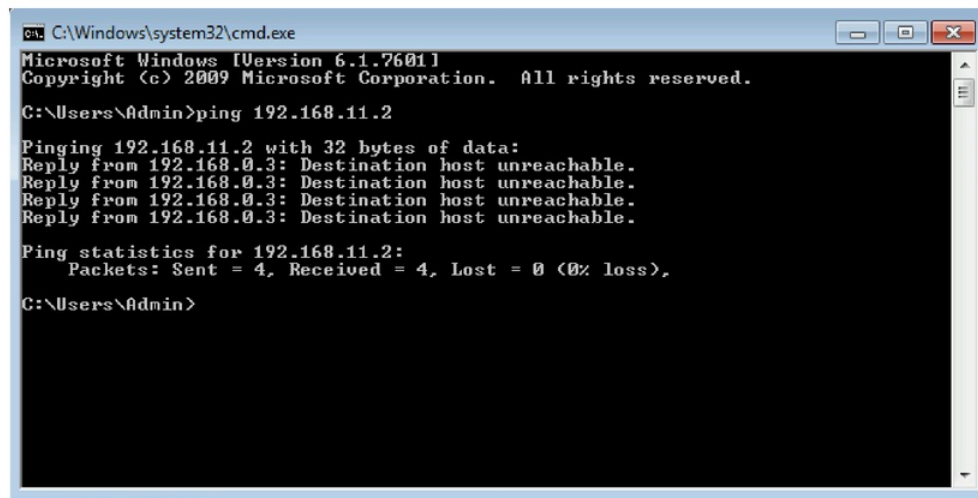
Task 1

Setting up IP and Gateway





Task 2- Unsuccessful ping to Servers



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

C:\Users\Admin>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Admin>
```

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

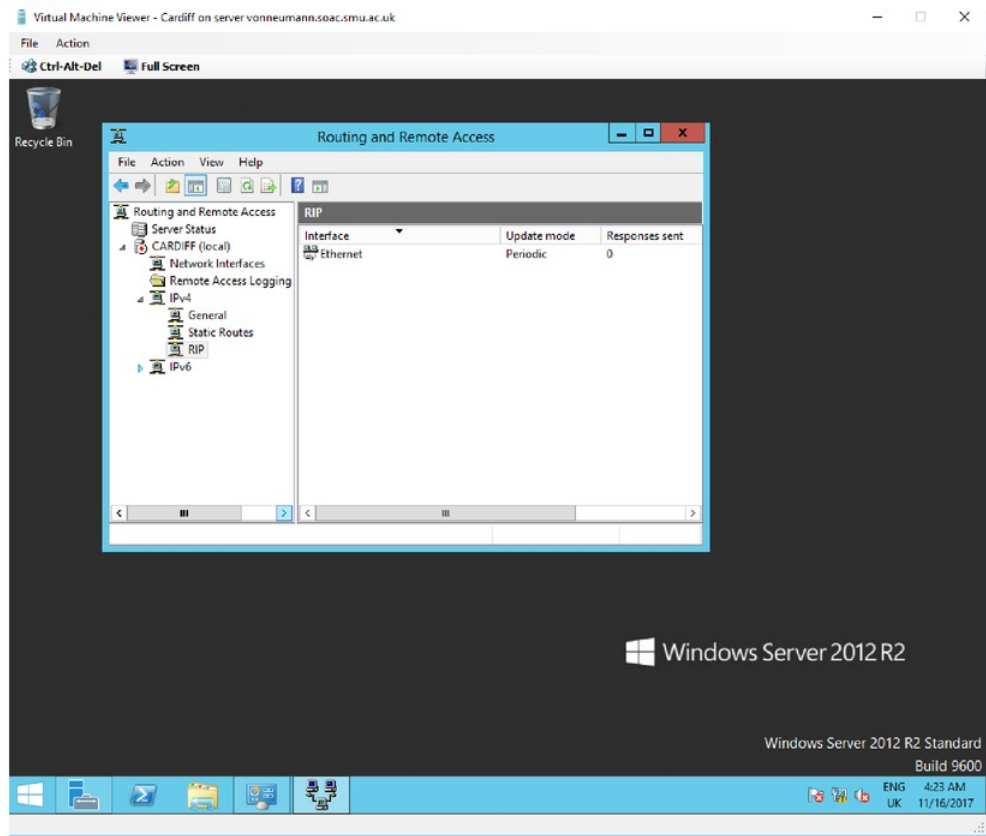
C:\Users\Admin>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.
Reply from 192.168.0.3: Destination host unreachable.

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

C:\Users\Admin>
```

Task 3-



```
Virtual Machine Viewer - Swansea on server.babbage.soc.smu.ac.uk
File Action
Ctrl-Alt-Del Full Screen

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

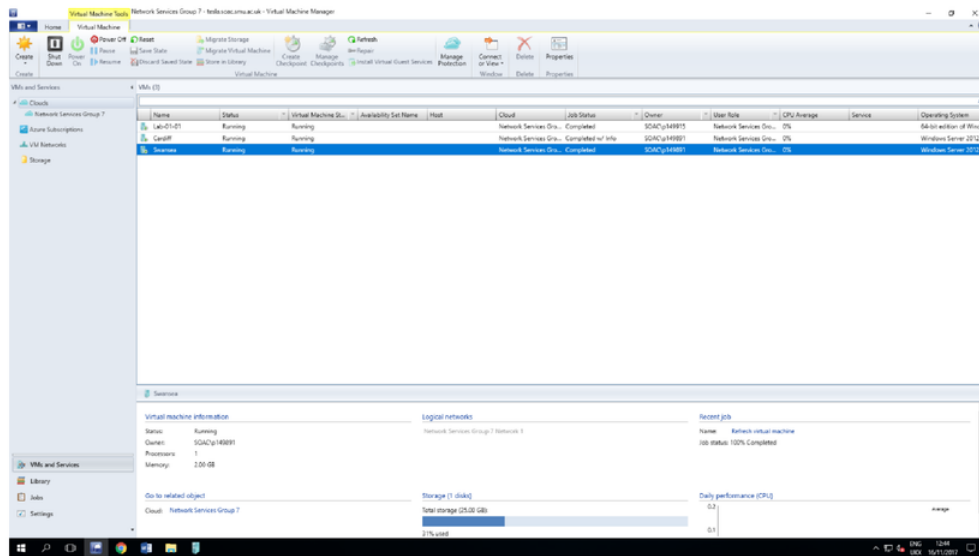
PS C:\Users\Administrator> ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:
Control-C
PS C:\Users\Administrator> ping 192.168.11.2
Pinging 192.168.11.2 with 32 bytes of data:
Reply from 192.168.11.2: bytes=32 time=1ms TTL=128
Reply from 192.168.11.2: bytes=32 time=1ms TTL=128
Reply from 192.168.11.2: bytes=32 time=1ms TTL=128
Reply from 192.168.11.2: bytes=32 time=1ms TTL=128
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 = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 192.168.11.1
Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.11.1: bytes=32 time=27ms 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 = 27ms, Average = 6ms
PS 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=33ms 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
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 = 1ms, Maximum = 33ms, Average = 8ms
PS C:\Users\Administrator> _
```

```
Virtual Machine Viewer - Swansea on server.babbage.soc.smu.ac.uk
File Action
Ctrl-Alt-Del Full Screen

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS 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=448ms TTL=127
Reply from 192.168.0.3: bytes=32 time=1ms TTL=127
Reply from 192.168.0.3: bytes=32 time=1ms TTL=127
Reply from 192.168.0.3: bytes=32 time=1ms 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 = 0ms, Maximum = 448ms, Average = 117ms
PS C:\Users\Administrator>
```



Task 4

The routing table consists of needed information to forward a packet along the best route to its destination. The routing table therefore includes Destination address, next hop address, interface, metric and routes. Depending on the protocols used this routing table's information is changed or created either manually or dynamically. Again, depending on the protocol used the router may send its own routing table out to surrounding routers and vice versa to create a whole-network routing table as opposed to a local one.

Task 5

- Identify the benefits of Type 1 Hypervisor software services and briefly evaluate some suitable products.
- Generally speaking, Type 1 hypervisors benefit from higher performance, security, availability and efficiency, when compared with their type 2 counterparts. This is because of the way it works, a type 1 runs directly off the system hardware bypassing the host OS, whereas a type 2 runs off the host OS, the OS being a middle-man of the process. While this provides the means to run a hypervisor easily off your own PC's OS it comes with lower speed overall, due to the fact that the info has to go;

Hardware>Host OS>Type 2 Hypervisor> Host OS> Hardware

As opposed to, on a type 1 hypervisor

Hardware> Type 1 Hypervisor > Hardware

Not to mention the fact that a breach in security on the host OS obviously affects the type 2 Hypervisor, but I digress.

- Define the role of Routers in the Network Architecture, what types can be used?
- The main role of a router is the forwarding/passing of packets/traffic around the network. This is done via Internet Protocol or IP, and using this IP, routers can direct traffic to its destination whether directly or indirectly. This is assisted by the use of a routing table, of which is detailed in a later question

When it comes to routers there are a few types, but for the most part they only vary a small amount. The types tend to be; wired, wireless, edge, core and virtual. A wired router is the basic version and the most common when referring to a router, barring the modem-router-switch combination that ISP's provide. A wireless router is the same as a wired but it, as you may guess, uses wireless technologies to connect to devices.

A core or edge router, while not technically a type of router like wired or wireless, they are a different way to categorize. A core router is a wired/wireless router that receives and sends packets within a network, an edge router on the other hand is one that sends and receives between two different networks, but not within.

A virtual router is a digital router protocol that 'kicks-in' should there be no physical router connected to the device, as a redundancy option should the router connected to the network fail, one of the computers can act as a router.

- Identify and discuss the usage of common Routing Protocols, what are the associated benefits of using Routing Protocols?
- Routing protocols are used to identify and value the routes available on a network, as well as build routing tables and make decisions based on the aforementioned values. Although there are many types of routing protocols they tend to end in two groups; Distance vector and Link-state.

A Distance vector protocol will first build its routing table using its directly connected interfaces then broadcast this table to its neighboring routers using the same protocol, the neighboring routers doing the same. Once the network has converged, all routers should have a matching routing table, detailing the network. When a line becomes unavailable the update will be received by all of the routers on the protocol network. An example of a distance vector would be EIGRP.

Link state on the other hand while similar, will only advertise an update when a change occurs, using bandwidth more effectively, and will only send the change, not the entire routing table. The routing protocol "will flood the network with link state advertisements to all neighbor routers per area in an attempt to converge the network". Link state is also able to use a variable subnet mask, making addressing more efficient. An example of link-state would be OSPF.

- Define the role of Routing Tables, what are they. Breakdown and analyze the information a Routing Table provides us with.
- A routing table contains the information needed for a router to successfully send received packets to their destination, whether directly or indirectly. A routing table includes; Destination, Next Hop, Interface, Metric & routes.

The destination is the destination/final IP, of which is stored in each packet, so that the router knows where to send it.

The next-hop is the IP where the packet must be forwarded to reach its destination, or failing that, it's next next-hop.

The interface is the interface on the router where the packet should be sent/forwarded.

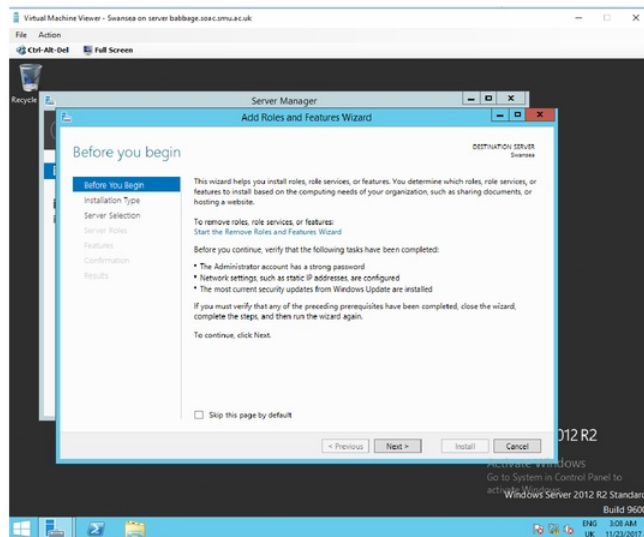
The Metric is the value assigned to different converging paths, the value of which determines the best or most convenient path for the packet to take to reach its destination in due time. Important thing to note is that a metric is subject to change both depending on the nature of the route, and the routing protocol used.

- What is the Subnet Mask, what is the significance of this in the Routing Table?
- A subnet Mask allows IP networks to be subdivided for security and performance purposes, meaning that a subnet mask can separate an IP address into the network portion and the host portion, or can be further divided into a (<network><subnet><host>) if needed. A subnet determines the amount of hosts an IP is given and tend to range from /24 giving 240,435,456 hosts to /30 that gives only 4. That being said this is for IPV4, IPV6 can easily give a much, much larger range of hosts.

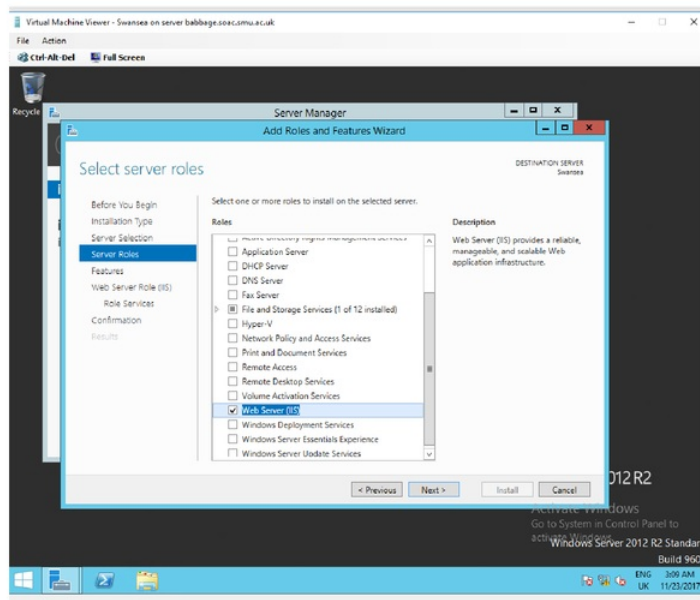
Worksheet 2

Task 2

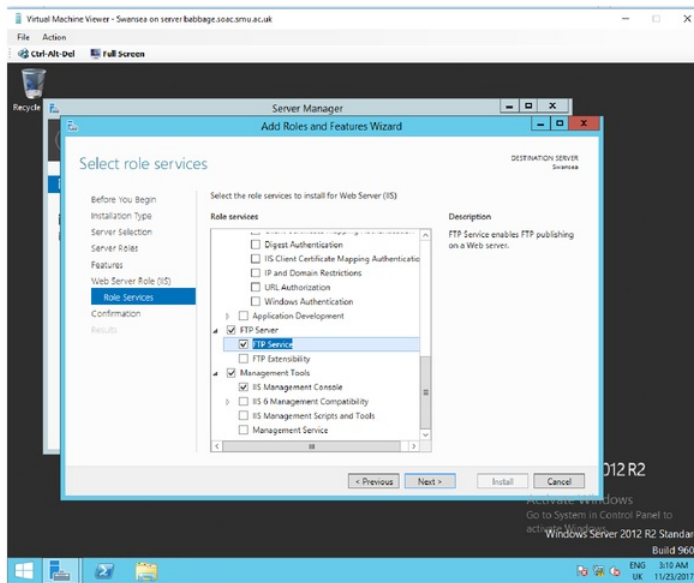
Setting up server roles



Setting up web server

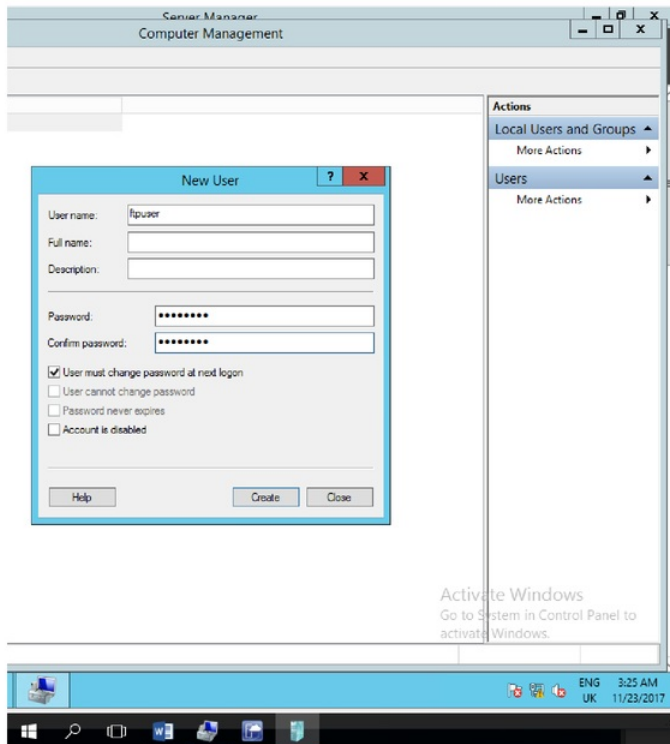


Setting up FTP service

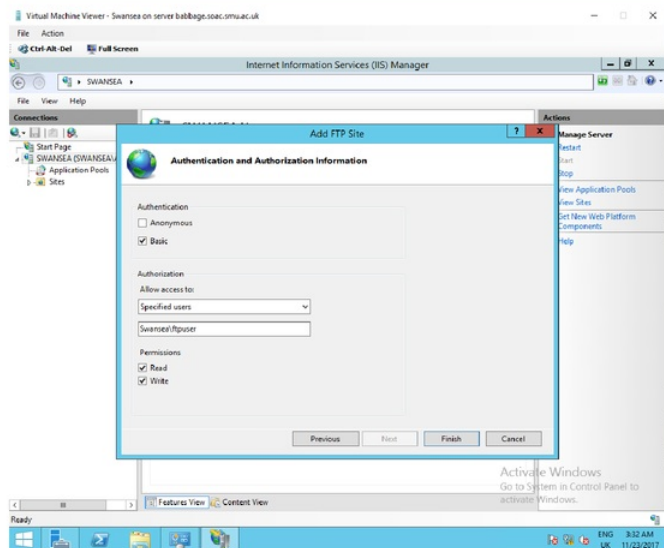
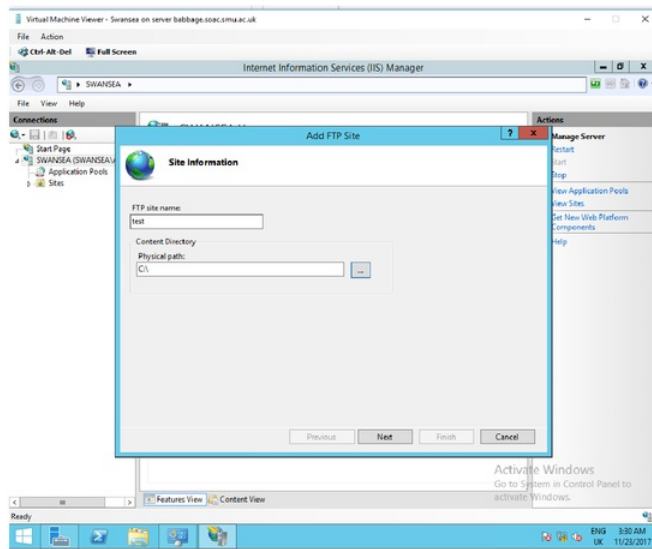


Task 3

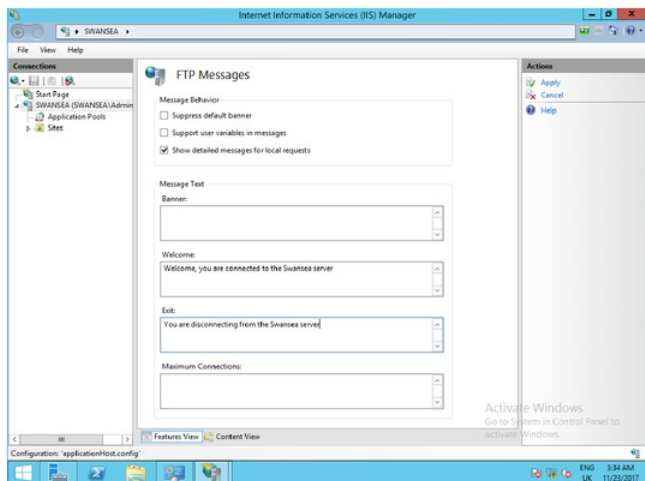
Setting up local users folder



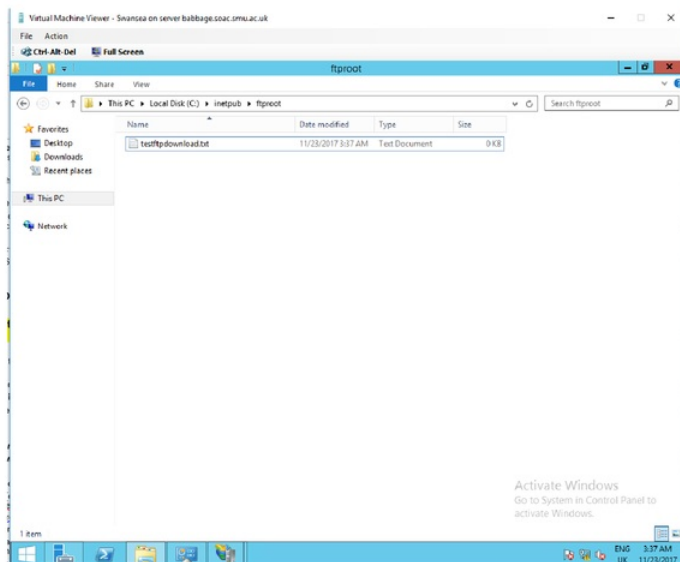
Setting up directory



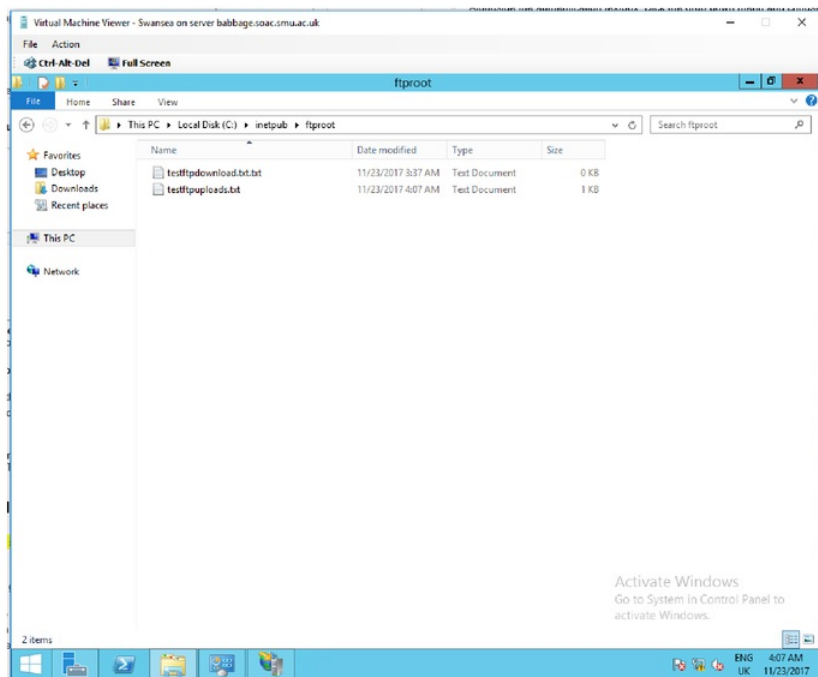
Creating banner messages



Proof of text file in folder

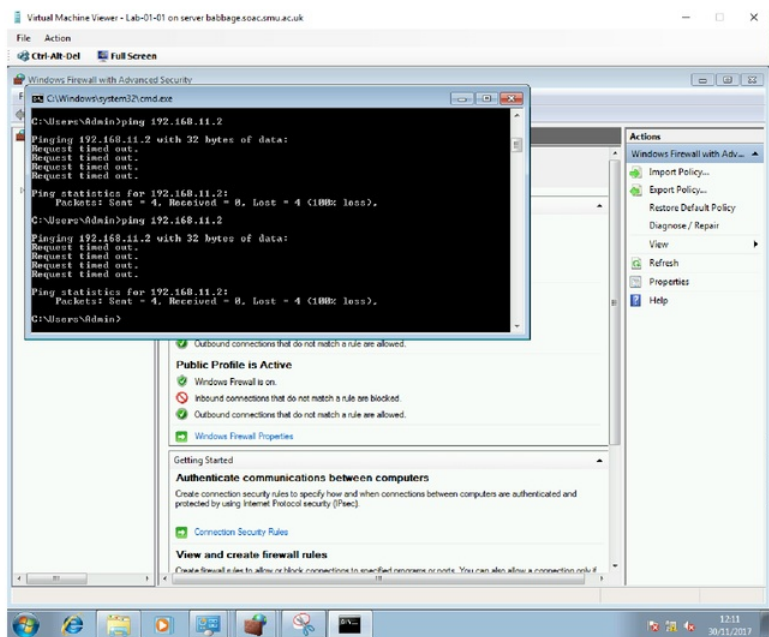


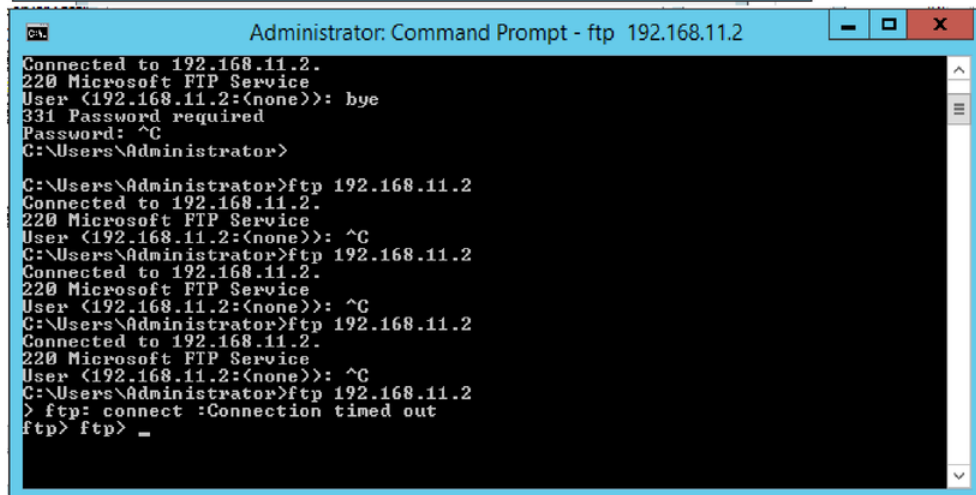
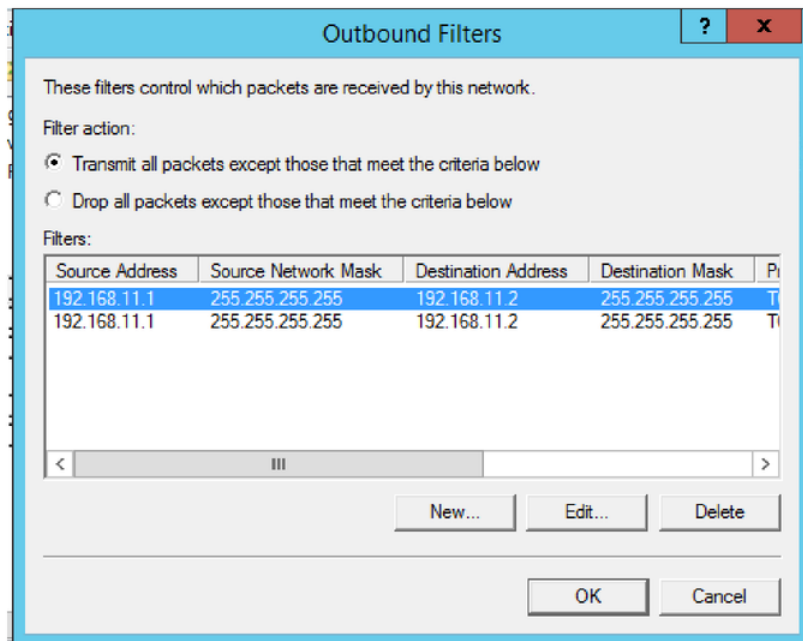
Proof of pinged file from Cardiff server in folder

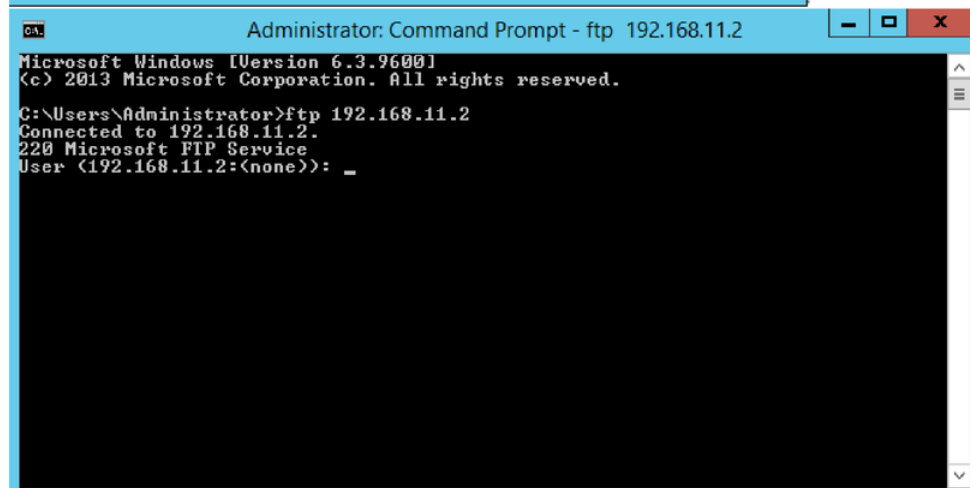
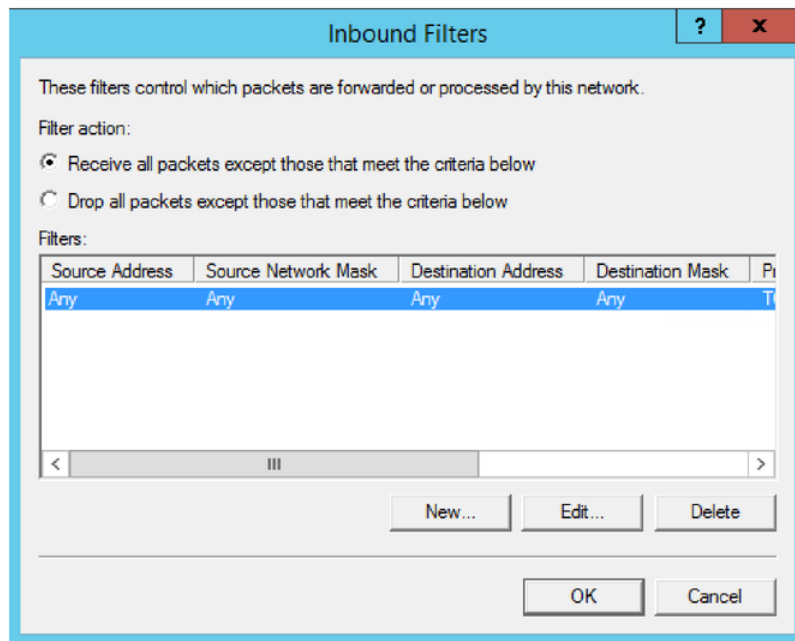


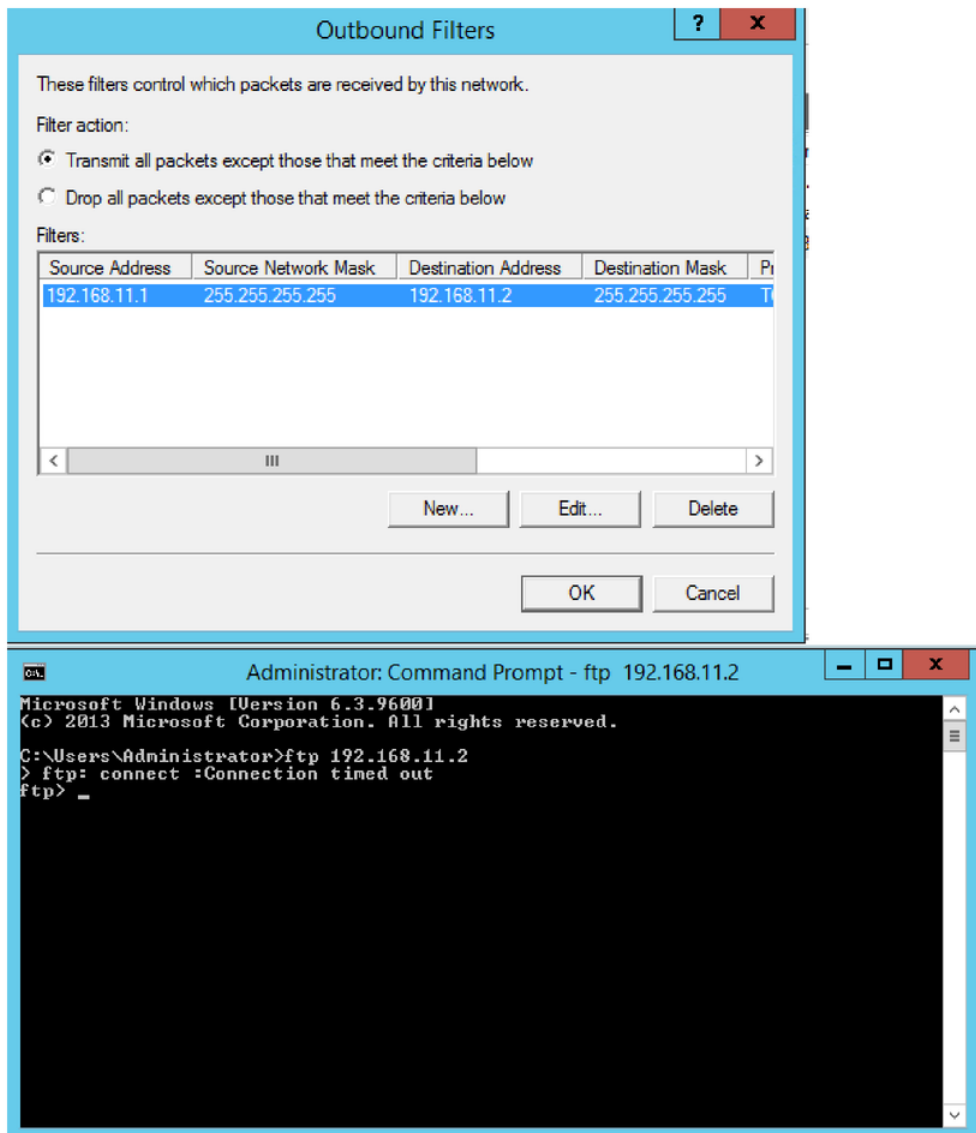
Task 4

Ping from Lab to FTP









Task 5-

Here we want to only allow our Router to FTP. All other traffic from our Router and all other traffic from other networks (including PINGS) must be blocked.

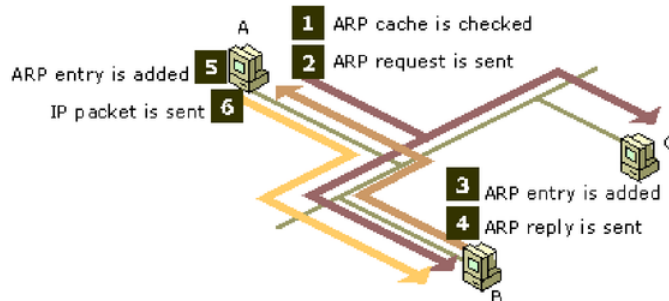
Explain your method for achieving this:

To start, FTP uses the port 21 by default, therefore we place an inbound filter allowing only FTP aka port 21, as well as an outbound filter restricting all but port 21 again. This is because While we are trying to block near everything, FTP is still a two way communication, meaning it must have access back to the router.

Task 6-

Observational Tasks:

Q1). Describe (using appropriate illustrations) how the ARP process operates in Networking Contexts?



The ARP process works similar to an acknowledgement communication. As shown in the diagram above, first of all the ARP cache is checked, seeing whether an ARP request needs to be sent. Then an ARP broadcast request is sent out, requesting the IP of the associated host. The host that matches the request will then send a unicast confirmation, any other hosts that don't match the request will drop the packet. Once the original host receives this confirmation, it has all the information needed to forward the IP packet and does so.

Q2). What is Packet Filtering? In our context, why is Packet Filtering termed 'IP Packet' Filtering? Why would you use Packet Filtering in your Network? What are the perceived benefits?

Packet filtering is the firewall process of allowing or blocking, depending on configuration, certain packets depending on their source, destination, ports or protocols, and this can be ingoing or outgoing to the system.

Packet filtering is called 'IP Packet' filtering as for the most part, packets are allowed or denied access based on their Internet Protocol address. Packet filtering is often used in networks as it is cheap in terms of implementation, although this comes at the cost of a lower level of security when compared to application security or the like. Not to mention that not only is it cheap filters can be placed on a router by router basis. It is often used to segment networks, meaning that one section of the network cannot easily access another section. Although bear in mind when it comes to sensitive data this security measure, although useful, is not enough.

Q3). Why is it possible for contradictory filters to occur when you use packet filtering? Give an example of a Contradictory Filter:

A contradictory filter occurs when an inbound and outbound filter conflict, meaning that the data cannot pass through the router. For example, should a user place a filter allowing all traffic of a sort, but then on the outbound filter blocks said traffic, this means that the entire traffic flow of that definition cannot pass through the router.

Q4). 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?

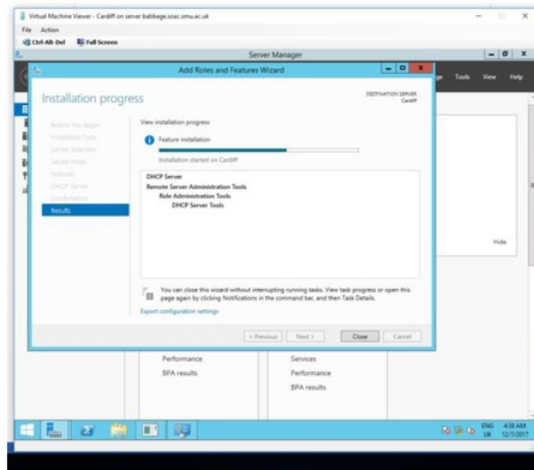
While an FTP server is a useful and common use of a server, it is only one of many, for example it could be used as a web server, SMTP server, print server, DHCP server and while there are more this would end up rambling. Important to note is that while these roles are normally one per server, using virtualisation it is possible for a server to have multiple roles.

Worksheet 3

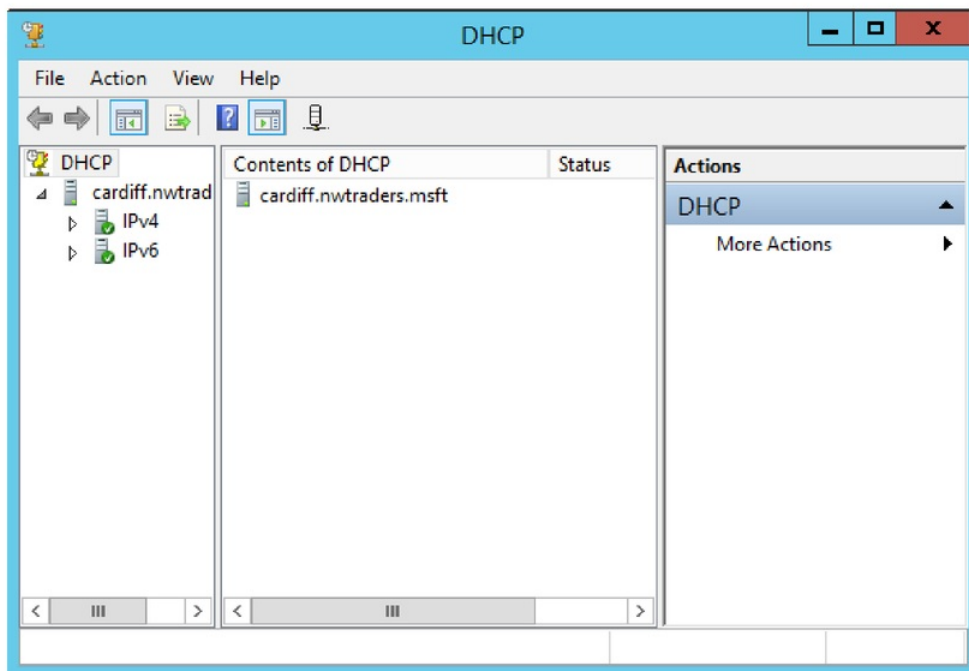
Task 1

screenshot unnecessary

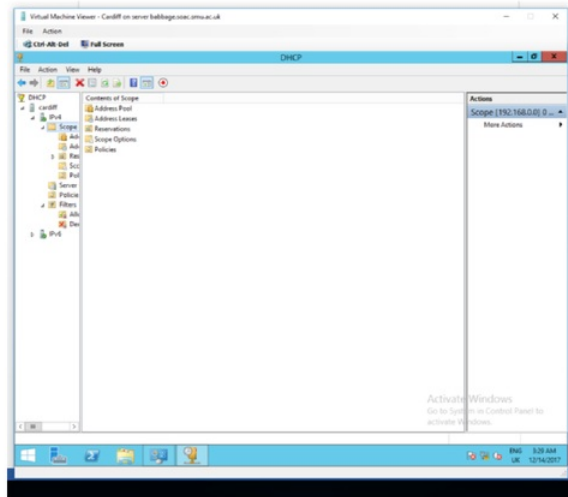
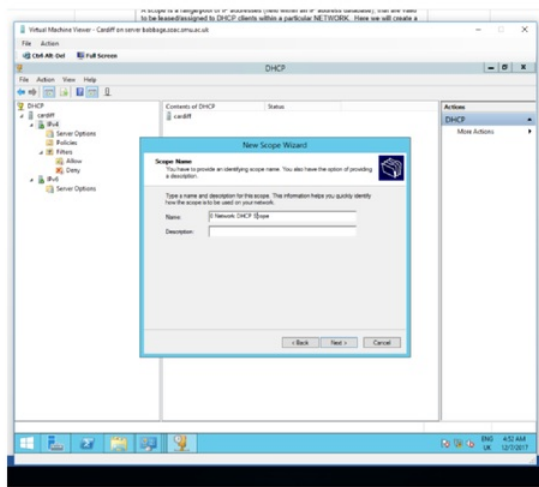
Task 2- Installation of DHCP server

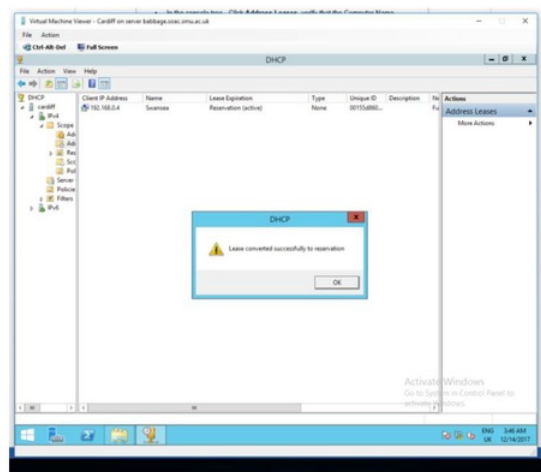
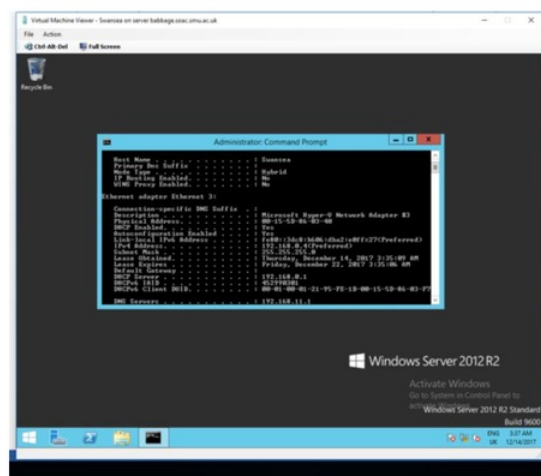


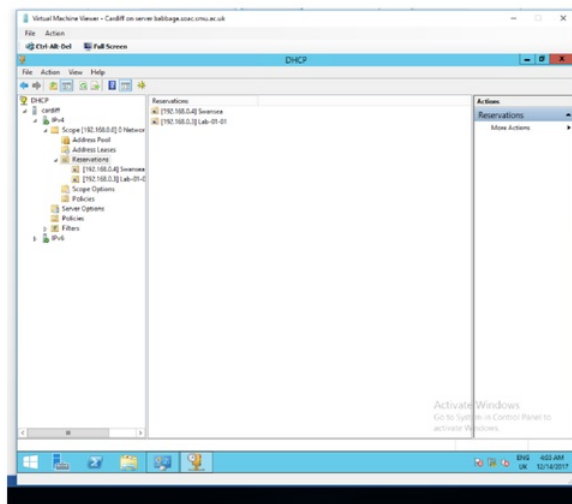
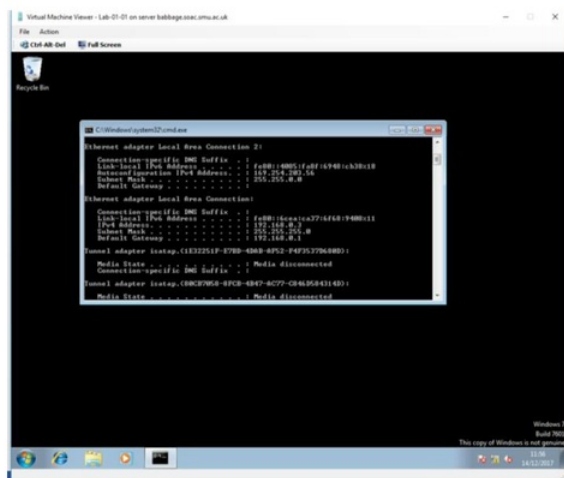
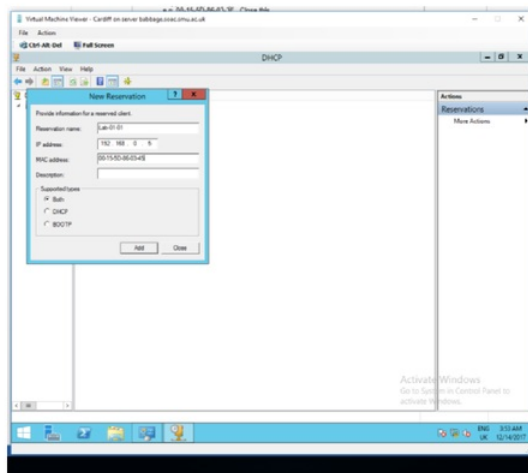
Task 3- DHCP Authentication



Task 4- DHCP Scope







Task 6

Q). Define the role of the DHCP Server in your Network?

The role of the DHCP server in any server is to automatically provide a connect host with an IP address, and any other configuration necessary, such as default gateway and subnet mask. Due to the fact that all, bar reservations and statics, IPs are controlled and managed by the DHCP server this reduces administration time and errors significantly. Important to note is that because DHCP is dynamic, IPs are assigned on time allotments, meaning that host IPs are subject to change unless statically defined manually, this static address of which is "attached" to the hosts MAC address.

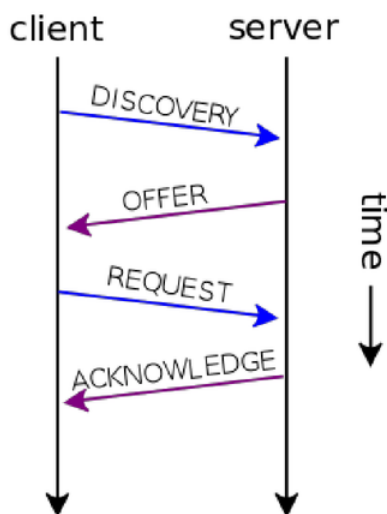
The way the time allotments work is that every x time has passed the server will check if the IP is still in use by the device, if so it will reset the time allotment and said host will continue with its IP. If the IP address is no longer in use by the host, then the DHCP server will give it to the next host requiring an IP address. So should the original host reconnect to the network, it is highly likely to be given a different IP address.

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

When a DHCP server is not reachable, at least on a windows PC one of two things can happen; IPAuto-configuration starts up, or Windows will act as a DHCP server for the network. As the former is more likely, we will start with that. IPAuto configuration is a protocol provided as default in windows PCs and should a DHCP server not be accessible then IPAC will configure the interface using an IP from the "Microsoft reserved Class B network (169.254.0.0), subnet mask 255.255.0.0.". Auto configuration is only used as long as necessary, should a DHCP server be located and accessed then IPAC will be immediately abandoned for the latter.

Q). Illustrate (with illustrations!!) the 4 stage process involved when DHCP clients look to obtain an IP address via DHCP?

The DHCP client server connection is a pretty basic two stage request-acknowledge communication, easily seen in the diagram below. At first the host finds the DHCP server, the DHCP server replies back saying that it is a DHCP server. Once the host receives the reply it requests and IP, of which the DHCP should be happy to provide given it can do so, and then the connection is complete, as the host has its IP.



Q). 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 main advantages of using a router as a relay agent is the fact that it can provide relay services for multiple UDP services and it reduces strain on the network as a whole. Starting with the latter, the reason for this is that as opposed to each router having its own DHCP server running on its local network, using relays you can put the entire network DHCP strains onto one router, of which will end up being much more efficient in its DHCP management.

To configure a DHCP relay agent, do the following;

R1(config)# ip dhcp relay enable

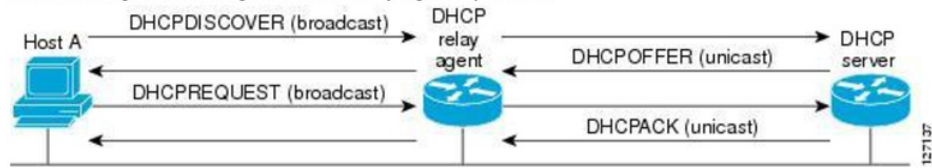
R1(config)# ip dhcp relay server 0.0.0.0 (DHCP server address)

(optional)

R1(config)# ip dhcp relay information policy replace

(allows the router to decide what to do if packet received is from another DHCP relay.)

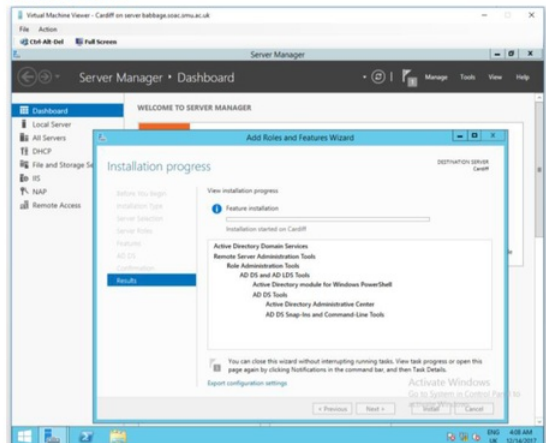
Below is diagram detailing the DHCP relay agent's process;

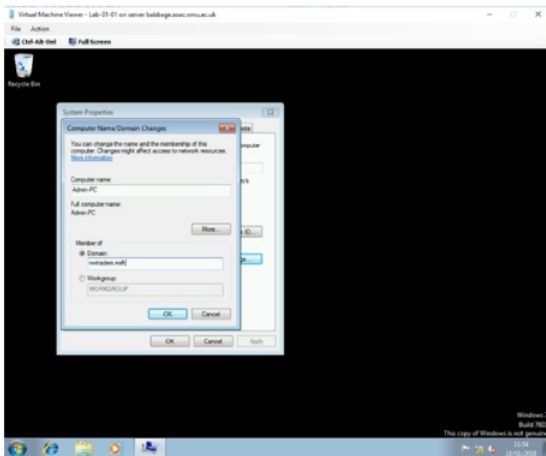
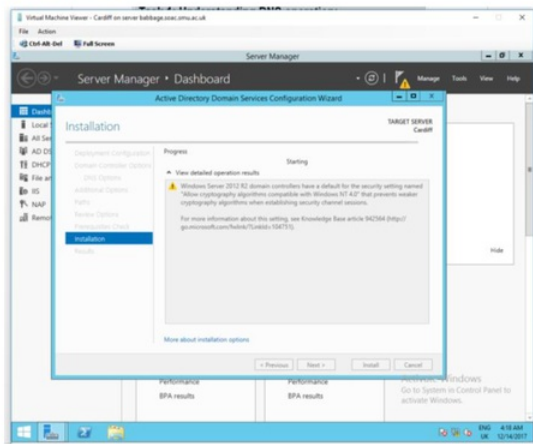
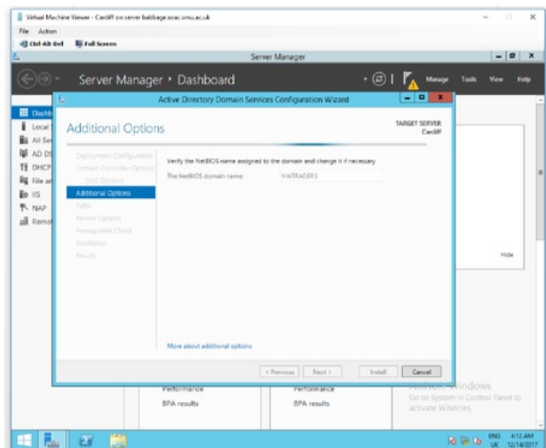


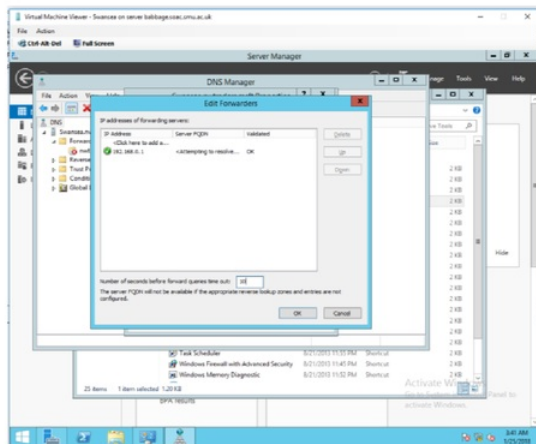
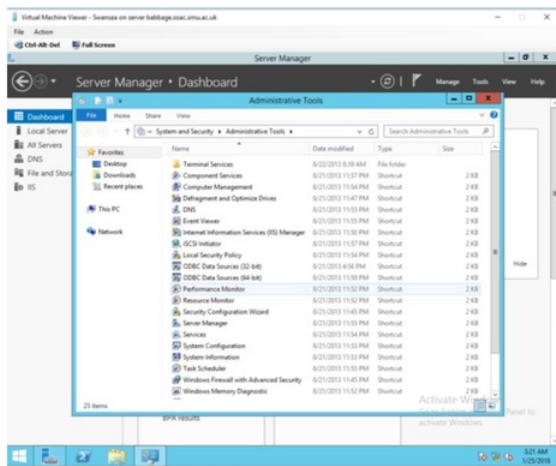
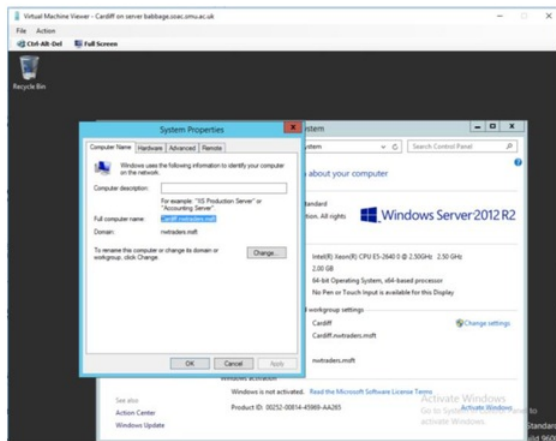
Worksheet 4

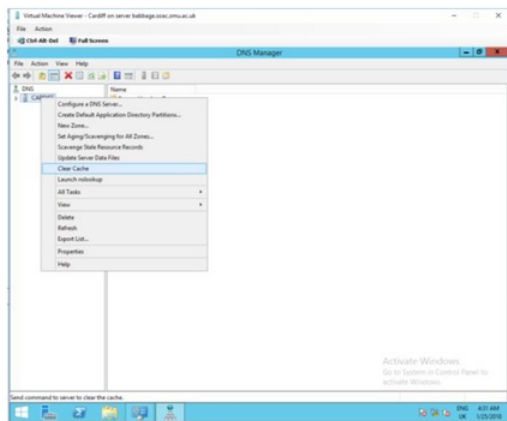
Task 1- Planning & Deploying DNS

Cardiff Tasks

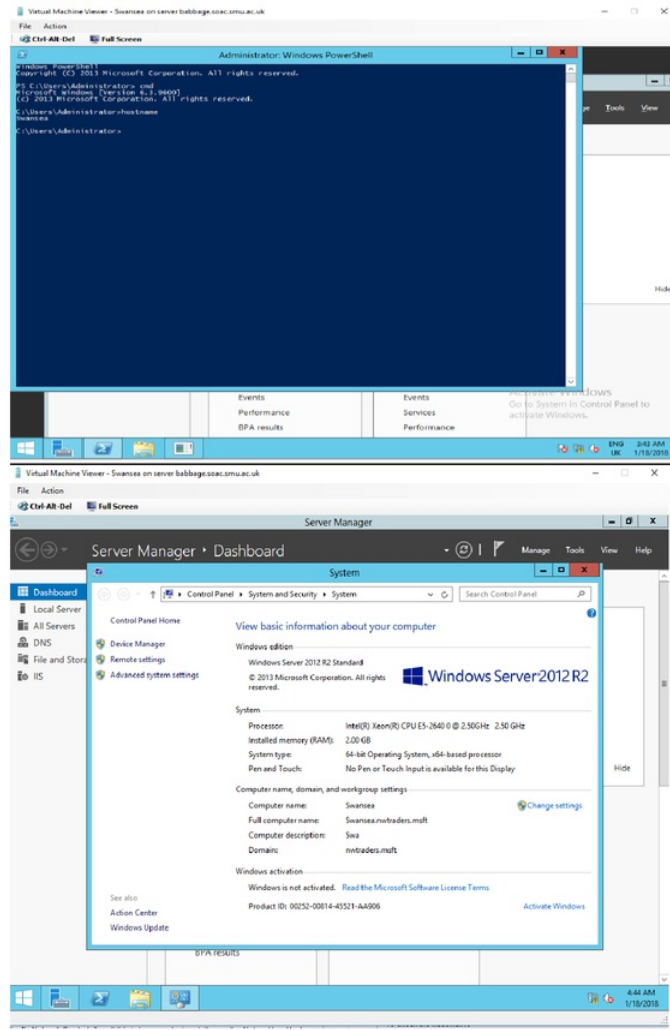




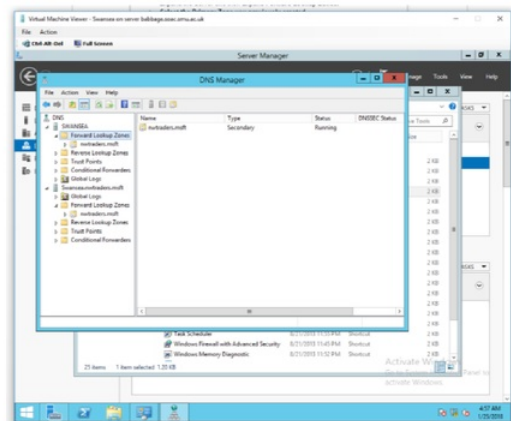
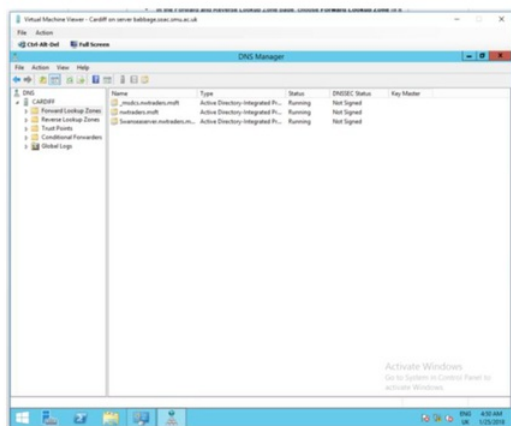
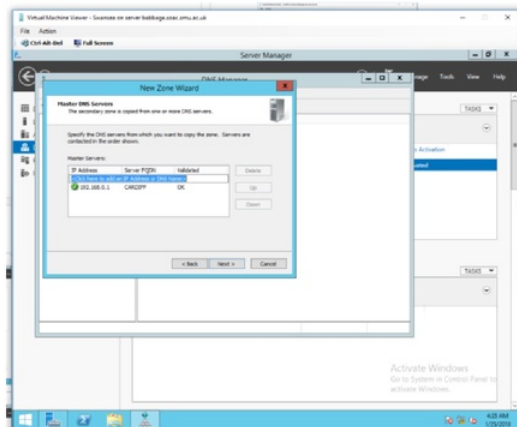




Swansea Tasks

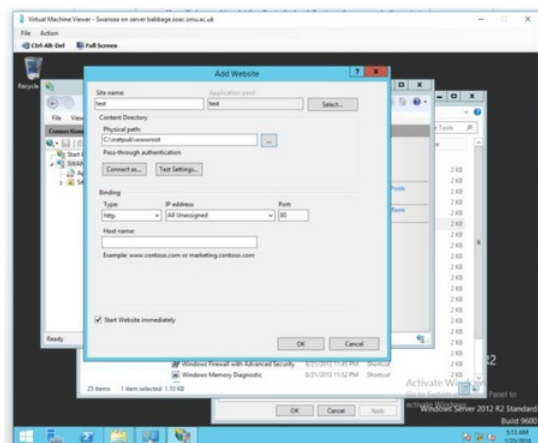


Task 2

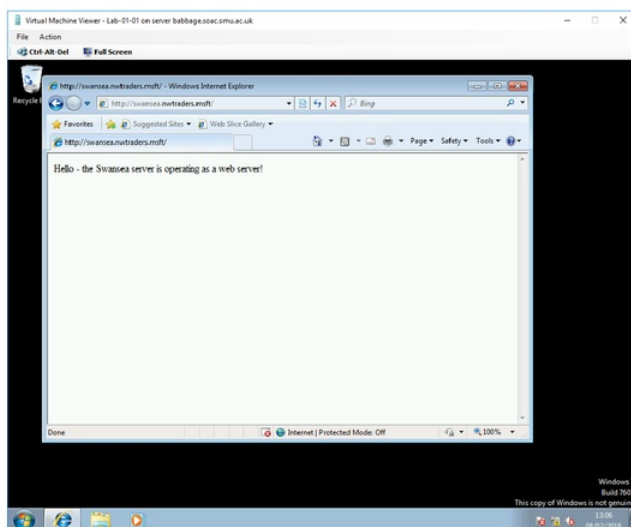


Task 3

Web creation



Evidence of Website

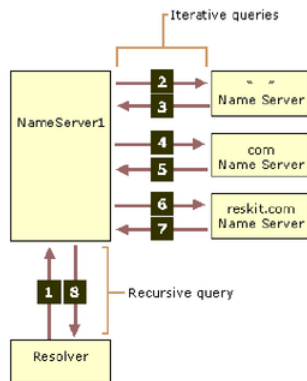


Task 4

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

Of the two types of name > IP address, hostname resolution is more likely than NetBIOS, for this example we will use the former. First the client will check whether the name to be resolved is its own, if not then it will check its local hosts files (IP address list with associated names). Should that fail, the DNS server is then queried. Should that fail, NetBIOS is then used as a backup process. Windows will try to use both methods, but should both fail then the user should get an error similar to "Client is unable to resolve a host name."

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



First the host will contact the server with a query for "test.testing.com", for example. The server will first check its local cache for the answer, failing that it will contact a root server with an iterative query for "test.testing.com". As the root server will not know the answer it will refer the query to the server for the next domain, in this case the .com domain. The server then contacts the .com domain, but again this fails as, while closer the .com domain doesn't know the full address, and refers to the testing.com domain server. Again the original server will request the address from the testing.com server, and it should be successful given the original name was correct. The original server now has the IP address and forwards it to the host.

Q). 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)?

Root hints are the cache files contained on a host server that are relied on before contact is made with a DNS server and contain the names and associated addresses needed to contact root DNS servers.

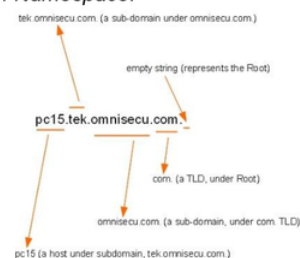
Root hint files, as specified by the name, can be used as pointers for DNS servers, so should they fail to resolve a query, it can be pointed to the network with an internal DNS, given the right instructions are given in root hint file.

Q). 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.

Server1.subcontA.nwtraders.msft.com.

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

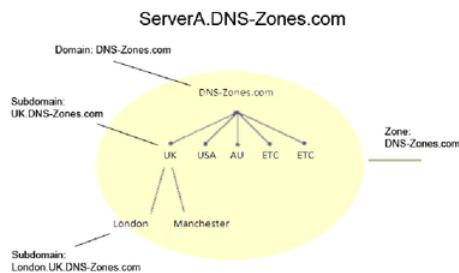


DNS breaks down the above address in part one into multiple parts, host, sub-domain, domain and root. In this case;

- 'Server1' is the host section.
- 'SubcontA' is the sub-domain.
- 'nwtraders.msft' is the domain.
- '.com' is the root.

Along the same lines, google.com would be a simple 'google' being the domain, and .com being the root again, admittedly that is a very simple address, although it is always the first one that comes to mind.

- Q). 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?



A DNS zone is a zone/section of the domain in the DNS range of which administration has been given to a singular manager, the internet being a common example of which has multiple DNS zones ("multiple" being the understatement of the year).

In the illustration above for example, while there are multiple domains and subdomains, they all are part of a singular DNS zone, and therefore are all managed by a singular entity/server. This singular management server will have access to resource records of nearly every server in its zone, or at least those directly under it, and another DNS zone will keep similar records of it's zone.

Worksheet 5

When it comes to clustering strategies there are two main strategies that come to mind that can be used for the aim of this worksheet; hosting a '3-tier web development system.', that being either a failover cluster or a Network Load balancing cluster. While there are other forms of clusters, for this task we will only be looking at these two as they can both fit the objectives, just to different degrees. Of course there is also Quorum, another cluster type it was quickly disregarded by this writer as cost per reliability seemed to be much more than the two strategies mentioned previously.

Looking that what a '3-tier web development system' would require; reliability and redundancy, these are the two main factors as a web dev. system would require near continuous uptime, a common attribute needed for corporate/business centred servers. These being the main factors to incorporate, failover should be the better choice, but then comes the factor of scalability, of which separates the two cluster configurations, NLB offers much better scalability at the slight cost of fault-tolerance, whereas failover clusters tend to be better at fault-tolerance but are much more difficult to scale, usually limited by port number. Barring physical limitations of the configurations, the software needed also varies, but both can be achieved/set-up on a windows server 2012 configuration, and should this objective need to be put into practise it is very likely said OS would be this author's first choice, and the fact that it comes with a 'Failover cluster manager' and 'NLB Manager'. [1]-[3]

When deciding which configuration to use, this author would likely end up using a failover server, the reason of which will be later explained. While they both share their similarities in terms of fault-tolerance and availability, the scalability and such of an NLB cluster wouldn't be needed as much in this web development system, and would only bring with it additional costs of hardware, should the objective be one that requires a lot more resources such as a high-load server farm, then NLB would be the choice, but alas. A failover cluster was

chosen as it provides the availability and fault tolerance required, without the costs that come with scalability, mainly because scalability shouldn't be a huge factor here as the 3-4 servers that are normally set-up with a 3-tier failover cluster should be more than enough for the objective. For this objective's instance, this writer would recommend a 3-node setup, such as the one detailed in the diagram below, as it provides increased reliability compared to a minimum failover cluster configuration, aka one that only has 2 nodes.

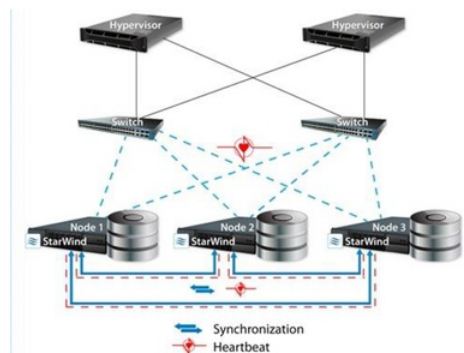


Figure 1[4]

As you can see from the design, it comes with 3 nodes or NAS servers, 2 switches, and 2 servers/hypervisors. This should be the minimum in terms of reliability, as in this case there should be fair warning of trouble as it would take significant loss of hardware for this cluster to fail. Also with 3 NAS devices connected, this cluster can roughly abide by the 'Computer Backup Rule of Three', meaning the data *should* be secure, at least from a statistics perspective. Of course this setup can be expanded, the limiting factor being cost and ports, but as this writer doesn't know the specific hardware being used he cannot give a maximum number of hypervisors allowed. Although, with this objective instance of a 3-tier web server, scalability shouldn't be a problem to a certain degree.

Bibliography

- [1] J. Gerend, "Failover Clustering | Microsoft Docs," *Windows IT Pro Center*. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview>. [Accessed: 14-Feb-2018].
- [2] J. McIllece, "Network Load Balancing | Microsoft Docs," *Windows IT Pro Center*. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/network-load-balancing>. [Accessed: 14-Feb-2018].
- [3] ITProToday, "Windows Server 2012: Building a Two-Node Failover Cluster | IT Pro." [Online]. Available: <http://www.itprotoday.com/windows-8/windows-server-2012-building-two-node-failover-cluster>. [Accessed: 14-Feb-2018].
- [4] A. Alvarez, "3 Node design." [Online]. Available: https://augustoalvarez.files.wordpress.com/2014/03/3node_big.jpg.
- [5] S. Ben-David and M. Ackerman, "Measures of Clustering Quality: A Working Set of Axioms for

Clustering," *Adv. Neural Inf. Process. Syst.* 21, pp. 121–128, 2009.

- [6] C. Hennig, "Clustering strategy and method selection," pp. 1–34, Mar. 2015.

Liam Blunt Worksheet 1-5

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

43/100

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7



Comment 1

colon, not semicolon.

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

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

GRADING FORM: SMU GENERIC_GJ

LIAM JOSEPH MARK BLUNT

43

RESEARCH-INFORMED LITERATURE



A relatively low number of sources used, and of somewhat low academic credibility overall. Some web sources can be acceptable - e.g. you've used TechNet twice. 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

3

subjective. Try to diversity your reading and focus more on peer-reviewed material.

KNOWLEDGE AND UNDERSTANDING



Some reasonable knowledge and understanding evident, though you're rather low on description in the worksheet documentation. The observational tasks are of a high quality, however worksheet 5 is extremely brief for the amount of marks assigned to it.

9

ANALYSIS



Some moderate analysis - a bit of a lack of synthesis due to a lack of sources in general. It'd also be beneficial to see some concluding remarks in the report.

7

PRACTICAL APPLICATION AND DEP.



Worksheets are complete, though the mark here is limited by the lack of description associated with them.

18

SKILLS FOR PROFESSIONAL PRAC.



Reasonable good spelling, punctuation and grammar through the report. Be careful to avoid contractions, and to proof-read your work. A well-presented document.

6