



Assignment Title: **Observational Tasks**

Module Title: **ACCC5003 Network Operating Systems and Security**

Lecturer: **Terry Walcott**

Student Number: **1815743**

Student: **Anghel Sandra-Stefania**

TABLE OF CONTENTS

List of figures.....	2
List of tables	2
Worksheet 1: Building the NOS infrastructure using Active Directory	1
Worksheet 2: Resource Management in Active Directory: Users, Computers and Groups.....	3
Worksheet 3: Resource Management in Active Directory: Managing access to files /folders and controlling domain user environments	4
Worksheet 4: Planning and Deploying DNS in the network infrastructure	6
Worksheet 5: Network Administration using DHCP	8
References	Error! Bookmark not defined.

LIST OF FIGURES

Figure 1: Difference between Hypervisor Type 1 and Hypervisor Type 2.....	1
Figure 2: Active Directory Forest, Trees, Parent and Child domains diagram	2
Figure 3: DHCP process [12]	7
Figure 4: Browser URL www.google.com	8
Figure 5: Command for displaying the content of the (DNS) resolver cache	8
Figure 6: Contents of the DNS resolver cache	8
Figure 7: Hosts file path	9
Figure 8: Local DNS server responses to DNS client.....	9
Figure 9: Iterative query between local DNS server and other DNS servers	10
Figure 10: Local DNS server returns response to DNS client.....	10
Figure 11: FQDN structure	11

LIST OF TABLES

Table 1: Active Directory Groups advantages/disadvantages	4
Table 2: NTFS vs FAT32 comparison.....	5
Table 3: DHCP advantages.....	6
Table 4: DHCP threats/dangers [13]	7

WORKSHEET 1: BUILDING THE NOS INFRASTRUCTURE USING ACTIVE DIRECTORY

“State the benefits of using Type 2 Hypervisor Virtualization software in your design.” [1]

Virtualization, simply explained by the capability of running multiple operating system at the same time on a single computer, would not be possible without the existence of a software called *hypervisor*. A hypervisor is responsible for creating a layer between physical resources of the computer and logical systems (virtual machines that runs on it). IBM [2] illustrates the difference between the existing hypervisor types in the following figure:

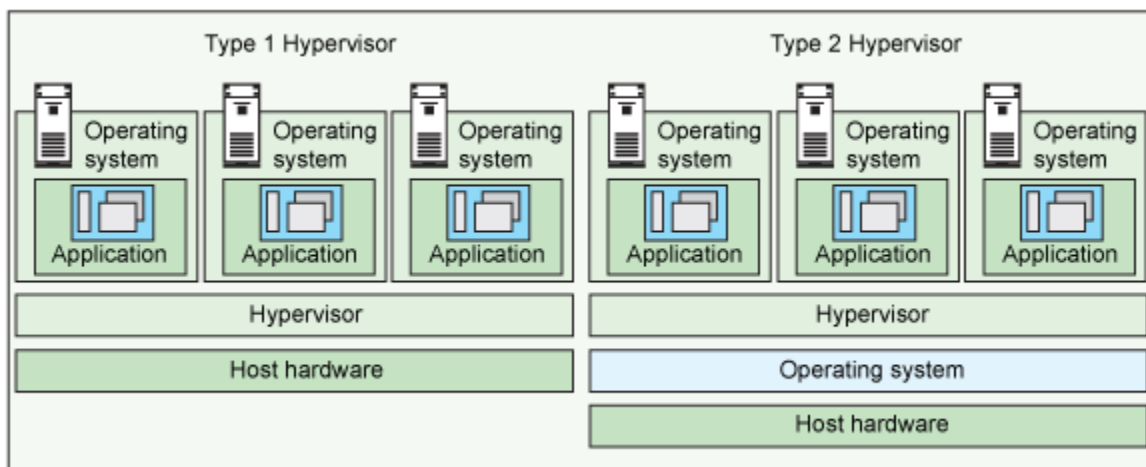


Figure 1: Difference between Hypervisor Type 1 and Hypervisor Type 2

Hypervisor Type 2 is running on a host operating system, in comparison with Hypervisor Type 1, which is running directly on the system hardware [3]. This aspect results into the advantage of running easily a virtual machine on a personal computer, without the need of a management console. Hypervisor Type 2 is usually suitable for personal computing devices or environments with a reduced number of servers [3].

“Evaluate the strengths and weaknesses of the VirtualBox platform used in your network.” [1]

VirtualBox [4]	
Advantages	Disadvantages
It is open-source and free (licensed GNU General Public License V2)	Support and documentation can be improved
It offers a friendly user interface being easy to installed and use	32-bit operating system support can be increased
It has a consolidated infrastructure by using a reduce amount of resources	3D Graphics support can be increased
It supports multiple 64-bit operating systems (Windows, Mac OS X or Linux)	It can be a bit slow when multiple virtual machines are running in the same time
It offers the option to take as many as needed snapshots and restore them quickly	Error messages can be improved to offer the user a better understanding of the failure reason

“Explain with use of diagrams the significance of the following terms, Active Directory Forests, Trees, Parent and Child Domains.” [1]

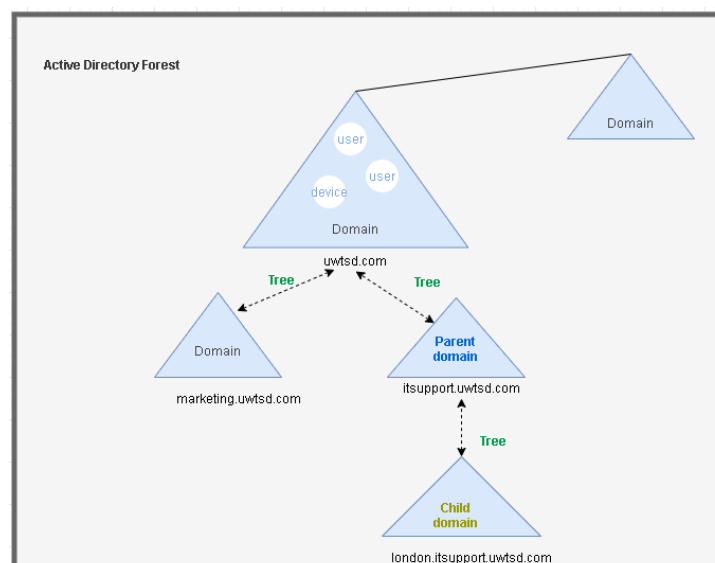


Figure 2: Active Directory Forest, Trees, Parent and Child domains diagram

As Figure 2 shown, a logical grouping of all users, devices and computers that are using one Active Directory database defines the concept of domain (e.g. uwtsd.com contains a collection of users, devices). A group of domains can be group together and form a tree (e.g. relationship between uwtsd.com and marketing.uwtsd.com). There is a hierarchical relationship between domains existing in a tree. A child domain is linked to a parent domain (e.g., there is a child-parent relationship between london.itsupport.uwtsd.com and itsupport.uwtsd.com domain). A collection of trees results into a forest [5].

“Investigate and document the main roles and responsibilities of an Active Directory Domain Controller.” [1]

The Active Directory Domain Controller is responsible for validation and authentication of users. It checks the user’s credentials (e.g. username, password) when a login request is performed. It is also responsible for user’s data encryption [5].

“What actions could we take in the event of a Domain Controller becoming unavailable?” [1]

When the Active Directory Domain Controller is changing the status to “Unavailable”, I have to check the IPv6 network connectivity. It needs to be enable, if not then I have to re-enable the IPv6 on the network card used by the domain controller [6].

WORKSHEET 2: RESOURCE MANAGEMENT IN ACTIVE DIRECTORY: USERS, COMPUTERS AND GROUPS

“Investigate the minimum password complexity requirements required as part of modern Network Operating System implementations.” [1]

Nowadays, security becomes a very important aspect of any system, including Network Operating System implementations. In order to address this challenge, National Institute of Standards and Technology defined a set of minimum requirements for passwords’ complexity [7]. The following rules are part of the guideline:

- The length of the password should contains at least eight alphanumeric characters
- Simple words, well-known words or repetitive characters/words are not recommended (e.g. password123, aaaaa1)
- Words specific to a context are not recommended (e.g. is not recommended to have a virtual machine with password same as username or same as machine name)

“State the advantages and disadvantages of using Groups in Active Directory.” [1]

Usage of Groups in Active Directory Domain [5]	
Advantages	Disadvantages
Configurations and permissions rules can be applied for multiple users at once – advantage	Groups and Groups Policies management may require knowledge of scripting languages (e.g. PowerShell)
Users management is much easier using groups	Possible cyberattacks could be hard to detect without having a monitoring solution implemented
Time and effort is reduced for Active Directory administrators	
Security can be easily enforced by defining group policies	

Table 1: Active Directory Groups advantages/disadvantages

WORKSHEET 3: RESOURCE MANAGEMENT IN ACTIVE DIRECTORY: MANAGING ACCESS TO FILES /FOLDERS AND CONTROLLING DOMAIN USER ENVIRONMENTS

“Discuss the two different types of permissions in use within windows network environments.” [1]

There are two types of permissions: *share permissions* and *NTFS* (New Technology File System) *permissions*. Share permissions refers to the decision of what and who can access directories/files over a network (e.g. “*Read*” permission – a user can view the content of a specific directory shared over the network; “*Write*” permission – a user can create a new file into a specific directory etc.). On the other hand, NTFS permissions refers to the decision of what and who can access the directories/files stored in NTFS system files (e.g. “*Full Control*” – a logged in user can perform any operation, such as read content or properties, create, remove, modify on a specific directory stored on that server). In order to be able to perform different operation on a directory using NTFS permissions the user must be logged in the server [8] [9].

“Evaluate the benefits of the NTFS File system in comparison with other network operating system’s file systems.” [1]

File systems comparison [8] [10]		
Comparison metric	NTFS (New Technology File System)	FAT32 (File Allocation Table)
Security	High security by using NTFS permissions (local and network security)	Low security (only network security)
Folder/File encryption	✓	✗
Max file size	16TB	4GB
Max file name length	255 chars	8.3 chars
Compression	✓	x

Table 2: NTFS vs FAT32 comparison

“Identify the main benefits of using groups in an Active Directory domain.” [1]

As it was mention in the previous worksheet, the main benefit of using groups in the context of Active Directory Domain is scalability. For example, in companies with a huge number of departments, employees etc. the management of accounts, policies (including permissions) can be a taught work. Using groups, it can be easy to decide that Lecturers group can access all students submitted assessments, while Students groups (users assigned into Students group – even if there are 2000 registered students) can access only their own assessment. Another advantage is the authentication mechanism. A user, using AD account, can automatically log in other tools like Outlook, Teams etc.

On the other hand, when an employee leave the company, his Active Directory account is easily removed without having any security breaches if the user is part of a group, which has access to financial documents, once removed then that user is no longer able to access any forbidden documents [11].

“Discuss the benefits of using Group Policy and Organizational Units to manage a domain’s resources.” [1]

Group Policies are used to define a set of configurations. An example of possible configuration is the decision of what actions can users can perform on their computers (e.g., only administrators can run .exe files, users cannot access facebook.com). In addition, a company can apply same policies to all employee’s computers (e.g. all users will have the same desktop wallpaper with the company’s logo, all users need to change the password at least once at 3months etc.) Based on these examples, results that Group Policies offers the advantage of having an easy management over a huge amount of objects registered in Active Directory domain. It increase the security as the administrator can decide security policies, can apply restrictions or grant permissions or can perform software updates automatically (e.g. Windows Updates). It has also the advantage of reducing the time and cost of possible travel expenses for configuring machines existing in different locations [11].

WORKSHEET 4: PLANNING AND DEPLOYING DNS IN THE NETWORK INFRASTRUCTURE

“State some principal advantages of using the DHCP service in network infrastructures.”

DHCP (Dynamic Host Configuration Protocol) [12]	
Advantages	
It reduce the exposure to errors caused by manual configurations of IP addresses	
It allows a centralized configuration of TCP/IP	
It offers an efficient mechanism of handling IP addresses’ changes	

Table 3: DHCP advantages

“With the aid of diagrams, explain the four stages process involved with assigning DHCP Clients with IP addresses. You should describe the stages that both client and server enter, and the processes involved.” [1]

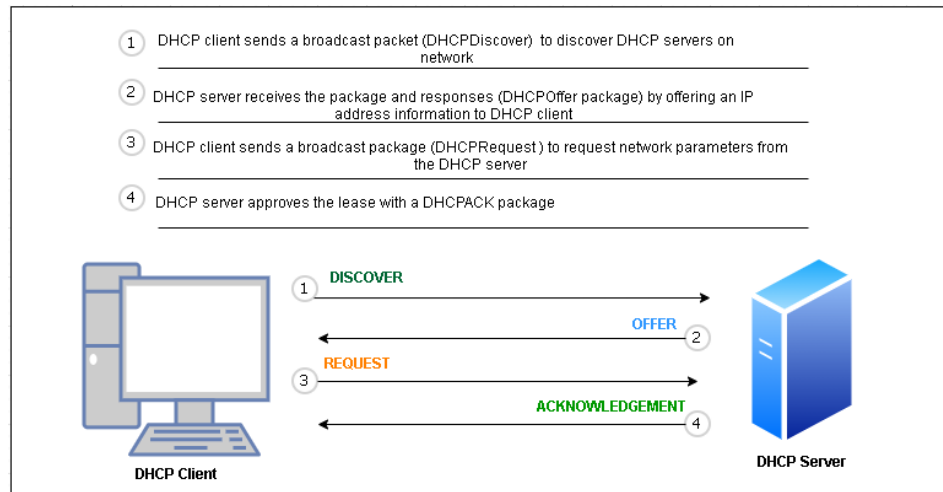


Figure 3: DHCP process [13]

“What are some of the potential threats/dangers that could occur when using a DHCP service?” [1]

DHCP
Threats/Dangers
Valid DHCP records can be overridden with wrong data
IP addresses can be obtained by unauthorized clients
Unauthorized DHCP servers can configure TCP/IP information to clients

Table 4: DHCP threats/dangers [13]

WORKSHEET 5: NETWORK ADMINISTRATION USING DHCP

“Describe how the Recursive Query and Iterative Query Processes resolve DNS Client Requests.” [1]

Recursive Query

A recursive query is happening between a DNS (Domain Name System) client and its local DNS server. [14]

Process steps:

1. Search for www.google.com in the browser

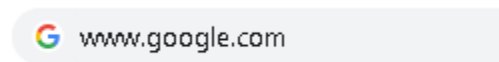


Figure 4: Browser URL www.google.com

2. The browser is looking for the name resolution into computer's cache memory

Run cmd:

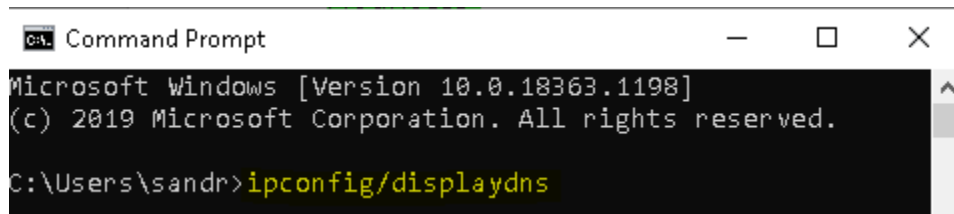
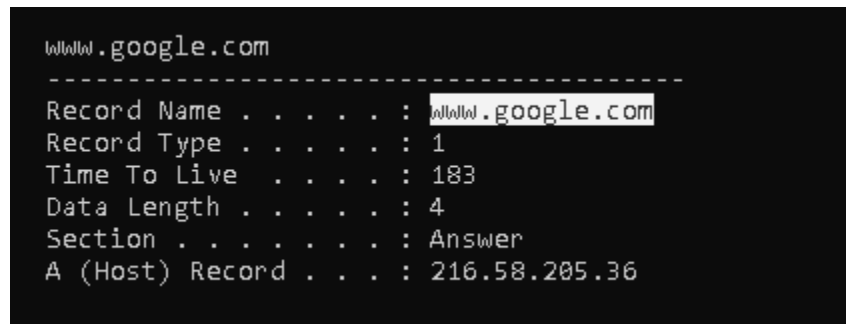
A screenshot of a Windows Command Prompt window. The title bar reads 'Command Prompt'. The window content shows the following text: 'Microsoft Windows [Version 10.0.18363.1198]', '(c) 2019 Microsoft Corporation. All rights reserved.', and the command 'C:\Users\sandr>ipconfig /displaydns' entered at the prompt.

Figure 5: Command for displaying the content of the (DNS) resolver cache

Output:

A screenshot of the output from a Windows Command Prompt. It displays the DNS resolver cache for 'www.google.com'. The output is as follows:
www.google.com

Record Name : www.google.com
Record Type : 1
Time To Live : 183
Data Length : 4
Section : Answer
A (Host) Record . . . : 216.58.205.36

Figure 6: Contents of the DNS resolver cache

3. If it is not in computer's cache memory, it is looking into hosts file

This PC > OS (C:) > Windows > System32 > drivers > etc				
Name	Date modified	Type	Size	
hosts	9/15/2018 8:31 AM	File	1 KB	
lmhosts.sam	3/19/2019 4:49 AM	SAM File	4 KB	
networks	9/15/2018 8:31 AM	File	1 KB	
protocol	9/15/2018 8:31 AM	File	2 KB	
services	9/15/2018 8:31 AM	File	18 KB	

Figure 7: Hosts file path

4. If we assume it cannot be find in any of the previous two locations, then the computer will ask about the IP to the local DNS server



Figure 8: Local DNS server responses to DNS client

Iterative Query

An iterative query is happening between a local DNS server and other DNS servers [14].

Based on the same scenario, if we assume local DNS is a new machine, which does not have any record of IP address for www.google.com, and then local DNS will communicate with other DNS servers in order to find the IP address.

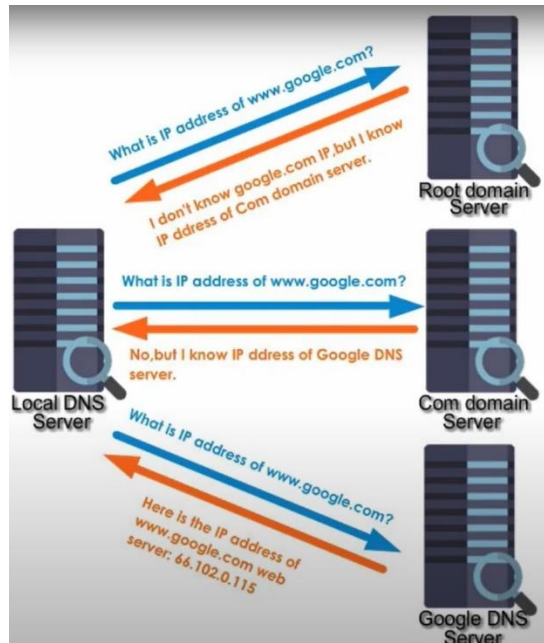


Figure 9: Iterative query between local DNS server and other DNS servers

Firstly, the local DNS server will ask the Root domain server, which can point to Com domain server and if it still does not know the IP address, can point to Google DNS server, which will be able to resolve it and then local DNS server will return the response to the DNS client:



Figure 10: Local DNS server returns response to DNS client

"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)." [1]

Root hints are a collection of existing DNS servers that is used for resolving queries. If a DNS server is not able to resolve a query it will use its root hints to forward the query to other DNS servers [14].

“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:

- What is the exact FQDN for this host?” [1]

FQDN (Fully-Qualified Domain Name) is **subcontA.nwtraders.msft**

- “Illustrate how the Domain Name System breaks up this FQDN into Host and Domain Namespace.” [1]

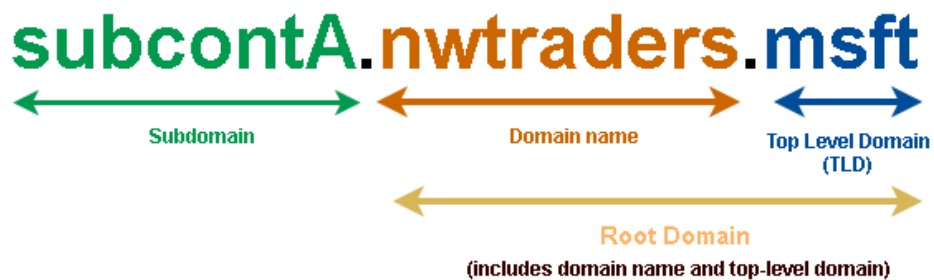


Figure 11: FQDN structure

“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.” [1]

A DNS zone represents a unique part of a domain namespace [15] used for performing a DNS lookup (finding an IP address on a DNS server that is managing the DNS zone for a specific hostname).

Each domain level (e.g. TLD: .msft, subdomain: subcontA) can be a DNS zone. For example, nwtraders.msft may be allocated to Nwtraders Corporation and it is responsible for managing the DNS server that stored the correct DNS records for this domain [15].

REFERENCES

- [1] University of Wales, Trinity Saint David, "Network Operating Systems and Security (ACCC5003_LON)," [Online]. Available: <https://moodle.uwtsd.ac.uk/course/view.php?id=3760>.
- [2] B. P. Tholeti, "Learn about hypervisors, system virtualization, and how it works in a cloud environment," IBM, 24 09 2011. [Online]. Available: <https://developer.ibm.com/articles/cl-hypervisorcompare/>.
- [3] A. W. Altaher, Virtualization Hypervisor Servers: Basics, Concepts, Methods, LAP LAMBERT Academic Publishing, 2017.
- [4] Oracle, "Oracle VM VirtualBox," 22 04 2016. [Online]. Available: <https://www.virtualbox.org/wiki/Documentation>.
- [5] B. Desmond, Active Directory, 5th Edition, O'Reilly Media, Inc., 2013.
- [6] ITExpert, "Microsoft Technical Expert Blog," 15 12 2015. [Online]. Available: <http://itexpert4ever.blogspot.com/>.
- [7] National Institute of Standards and Technology, "Digital Identity Guidelines - Authentication and Lifecycle Management," *NIST Special Publication 800-63B*, 2017.
- [8] Microsoft, "NTFS overview," Microsoft, 30 03 2020. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview>.
- [9] LSoft Technologies Inc., "NTFS Permissions," LSoft Technologies Inc., 2020. [Online]. Available: <https://www.ntfs.com/ntfs-permissions.htm>.
- [10] Microsoft, "Description of the FAT32 File System," Microsoft, 03 09 2018. [Online]. Available: <https://support.microsoft.com/en-gb/help/154997/description-of-the-fat32-file-system>.
- [11] B. Svidergol and R. Allen, Active Directory Cookbook: Solutions for Administrators & Developers, O'Reilly, 2013.
- [12] Microsoft, "Dynamic Host Configuration Protocol (DHCP)," Microsoft, 07 08 2020. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>.
- [13] Cisco, "IP Addressing: DHCP Configuration Guide," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-mt/dhcp-15-mt-book/dhcp-overview.html.
- [14] Microsoft, "Reviewing DNS Concepts," Microsoft, 08 08 2018. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/reviewing-dns-concepts>.
- [15] A. Liska and G. Stowe, DNS Security - Defending the Domain Name System, Syngress, 2016.