

Manage and maintain network resources, and its services applying suitable policies and drafting security and redundancy practices.

1st Given Edward Patch

Software Engineer Student (of HND Year 2)

Network Operating Systems and Services

University of Wales Trinity St. Davids (of Nitheesh Murugan Kaliyamurthy)

Swansea, Wales

Student ID: 1801492

CONTENTS

I	Introduction	1
II	Worksheet Four - Practical	1
II-A	Windows Server I - Address Resolution Protocol (ARP) and Routing Tables . . .	1
II-B	Windows Server II - File Transfer Protocol Server	2
II-C	Windows Server II - Web Server	2
II-D	Windows Server II - Set File Transfer Protocol Permissions	3
II-E	Client II - FTP Service	3
II-F	Windows Server I - Add Roles and Features Wizard	4
II-G	Windows Server I - Routing and Remote Access Service	4
II-H	Windows Server I - Pings	6
II-I	Windows Server II - Pings	6
III	Worksheet Four - Observational	6
III-A	Fallover Clustering	6
IV	Head Network Administrator Suggestions	7
IV-A	Network Architecture	7
IV-B	Network Policy	7
IV-C	Network Topology	8
IV-D	Security Methods	8
V	List of Abbreviations	9
VI	Conclusion	9
VII	References	9

Abstract—Routing and packet filtering within core transmission control protocol or internet protocol services and critical failover/redundancy practices. The techniques of routing and packet filtering are displayed and explained below.

Index Terms—NTFS, FTP, Web Server (IIS)

I. INTRODUCTION

This report separates into two sections:-

- Worksheet Four - Practical.
- Worksheet Four - Observational.

II. WORKSHEET FOUR - PRACTICAL

A. Windows Server I - Address Resolution Protocol (ARP) and Routing Tables

Command Prompt **ARP -A** script generates data that displays any compromises within the machine. These are as followed:-

- Interface Network Interface Card's (NIC's) in Windows Server I.
- Physical Media Access Control (MAC) of the NIC interface within Windows Server I.
- Internet Access of this NIC.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ARP -A

Interface: 192.168.100.1 --- 0x7
Internet Address      Physical Address      Type
192.168.100.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.1.100 --- 0x9
Internet Address      Physical Address      Type
192.168.1.255         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

C:\Users\Administrator>route print

Interface List
0...{8B06F27D-4E8D-4A90-B8D6-585E5C01E398} Intel(R) PRO/1000 MT Desktop Adapter #2
1...{8B06F27D-4E8D-4A90-B8D6-585E5C01E398} Software Loopback Interface 1

IPv4 Route Table
Active Routes:
Network Destination  Netmask          Gateway           Interface Metric
127.0.0.0            255.0.0.0         On-link           127.0.0.1 331
127.0.0.1            255.255.255.255   On-link           127.0.0.1 331
127.255.255.255      255.255.255.255   On-link           127.0.0.1 331
192.168.1.0          255.255.255.0     On-link           192.168.1.100 281
192.168.1.100        255.255.255.0     On-link           192.168.1.100 281
192.168.1.255        255.255.255.255   On-link           192.168.1.100 281
192.168.100.0        255.255.255.0     On-link           192.168.100.1 281
192.168.100.1        255.255.255.255   On-link           192.168.100.1 281
192.168.100.255      255.255.255.255   On-link           192.168.100.1 281
224.0.0.0            240.0.0.0         On-link           127.0.0.1 331
224.0.0.1            240.0.0.0         On-link           127.0.0.1 331
255.255.255.255      255.255.255.255   On-link           127.0.0.1 331
255.255.255.255      255.255.255.255   On-link           192.168.1.100 281
255.255.255.255      255.255.255.255   On-link           192.168.100.1 281

Persistent Routes:
None

IPv6 Route Table
Active Routes:
If Metric Network Destination Gateway
1 331 ::::/128 :::: On-link
0 281 fe80::/64 fe80:: On-link
7 281 fe80::/64 fe80:: On-link
0 281 fe80::49b:fdb9:c0e0:c977/128 fe80::49b:fdb9:c0e0:c977 On-link
7 281 fe80::bd52:5baf:aac5:bf5a/128 fe80::bd52:5baf:aac5:bf5a On-link
1 331 ff00::/8 ff00:: On-link
0 281 ff00::/8 ff00:: On-link
7 281 ff00::/8 ff00:: On-link

Persistent Routes:
None
```

Fig. 1. Figure of Windows Server I ARP -A and route print Scripts

B. Windows Server II - File Transfer Protocol Server

Addition of the Web Server Role Internet Information Services (IIS) role via the Add Roles and Features window.

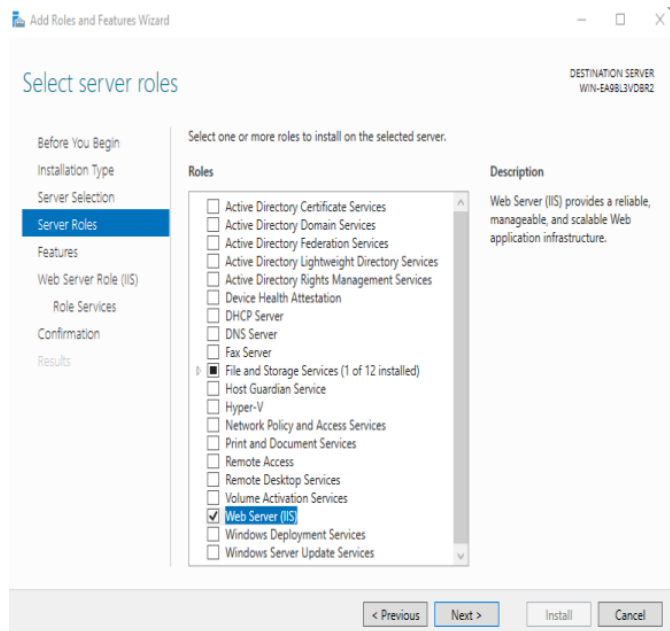


Fig. 2. Figure of Windows Server II - Add Roles and Features

Addition of the File Transfer Protocol (FTP) Server role via the Add Roles and Features window.

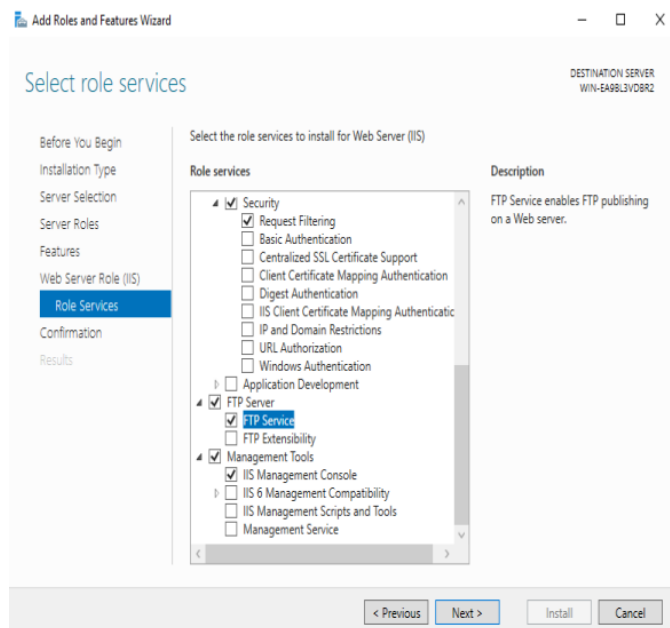


Fig. 3. Figure of Windows Server II - Add Roles and Features

C. Windows Server II - Web Server

Dialog shows a FTP Site is being set up. Within the *Add a FTP Site* window, named '1STFTPSITE' with the *Physical path*: set to 'C:\inetpub\ftproot'.

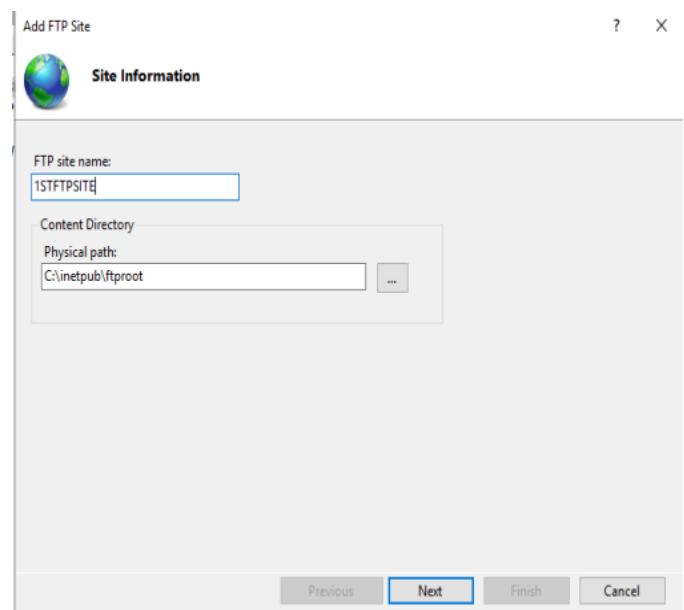


Fig. 4. Figure of Windows Server II - Web Server Configuration

Within the *Binding and Secure Sockets Layer (SSL) Settings* set the binding *Internet Protocol (IP) Address*: field to 'All Unassigned' and *Port*: to 21. *No SSL* is selected as there is no SSL Certificate available, this is not recommended in proper network setups, refer to SSLShopper [1] Why SSL? The Purpose of using SSL Certificates to learn why.

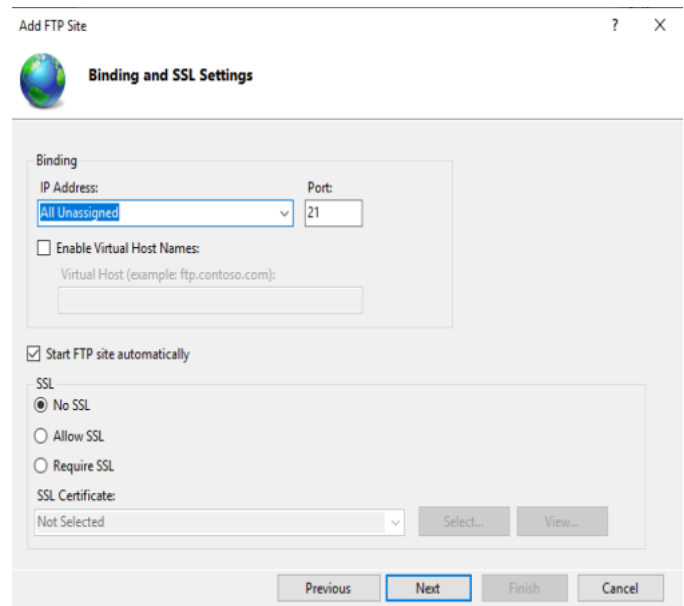


Fig. 5. Figure of Windows Server II - Web Server Configuration

Figure 6 shows that under *Authentication* the *Basic* checkbox was selected. Under *Authentication, Allow access to: Specified Users* was selected and configured to 'WIN-EA9BL3VDBR2\ftpuser' and *Read and Write* permission were selected.

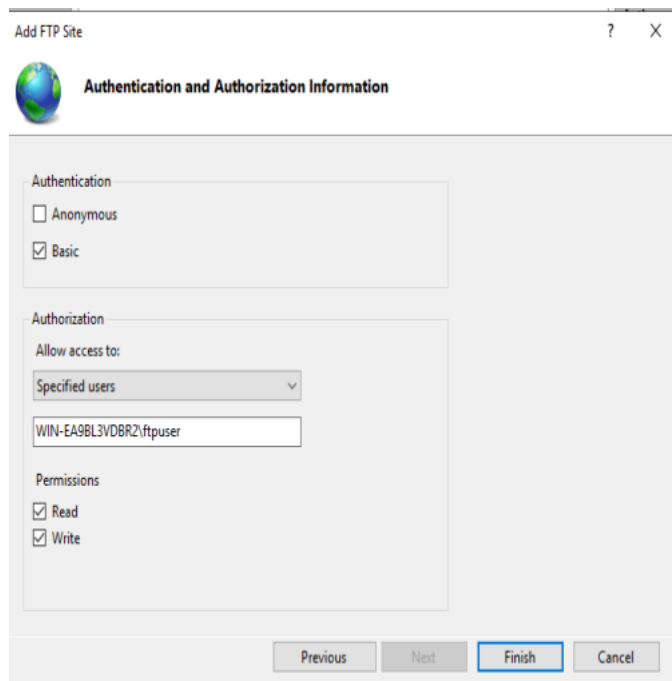


Fig. 6. Figure of Windows Server II - Web Server Configuration

A FTP Welcome Message is set within the FTP Messages dialog.

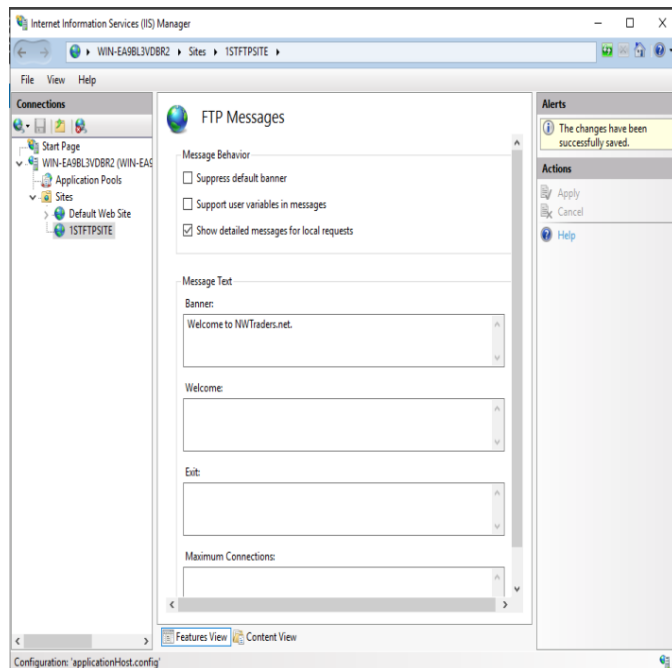


Fig. 7. Figure of Windows Server II - Web Server Configuration

D. Windows Server II - Set File Transfer Protocol Permissions

Set the following permissions of 'ftpuser':

- Read & execute.
- List folder contents.
- Read.
- Write.

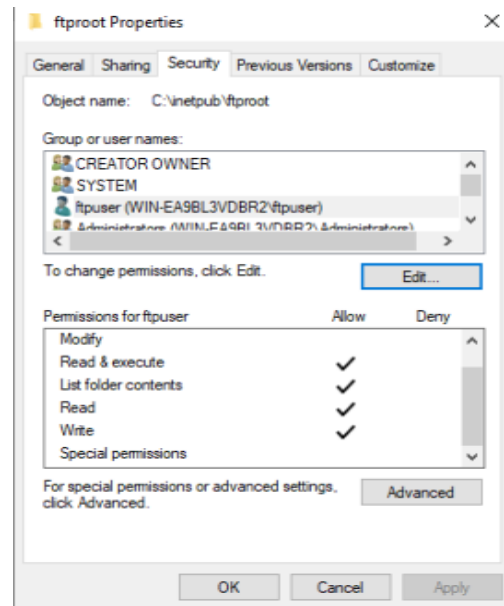


Fig. 8. Figure of Windows Server II - FTP Permissions

E. Client II - FTP Service

Uploaded text file called 'fptupload' to the fptfiles folder.

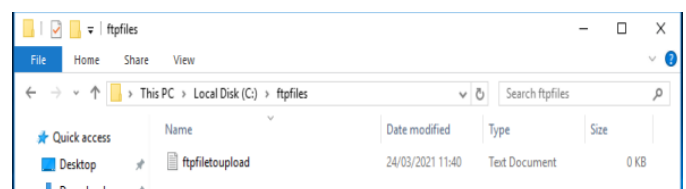


Fig. 9. Figure of Windows Client II - FTP File

Logged into ftpuser via the Windows Server I network.

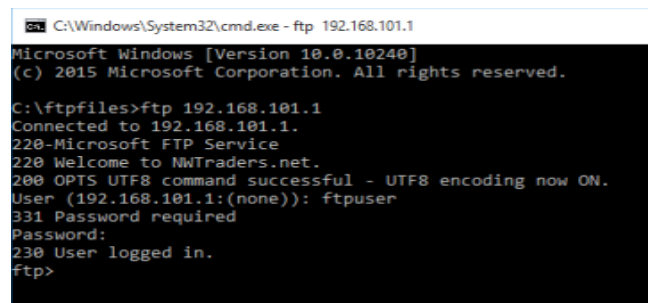


Fig. 10. Figure of Windows Client II - Login to FTP Server

Transferred the *ftpfileupload.txt* to Windows Server II.

```
C:\Windows\System32\cmd.exe - ftp 192.168.101.1

Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\FTPFiles>ftp 192.168.101.1
Connected to 192.168.101.1.
220-Microsoft FTP Service
220 Welcome to NWTraders.net.
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.101.1:(none)): DC1-NWT\ftpuser
331 Password required
Password:
230 User logged in.
ftp> put ftpfileupload.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

Fig. 11. Figure of Windows Client II - Upload File to FTP Server

Evidence:

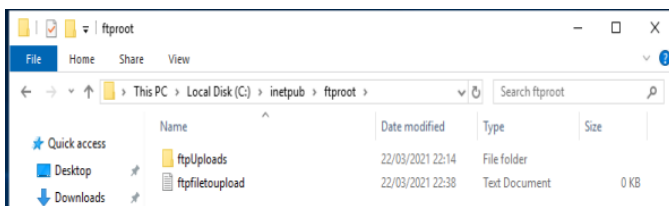


Fig. 12. Figure of Windows Server II - FTP Upload from Client II Evidence

F. Windows Server I - Add Roles and Features Wizard

Add's the **Remote Access** role from Add Roles and Features Wizard.

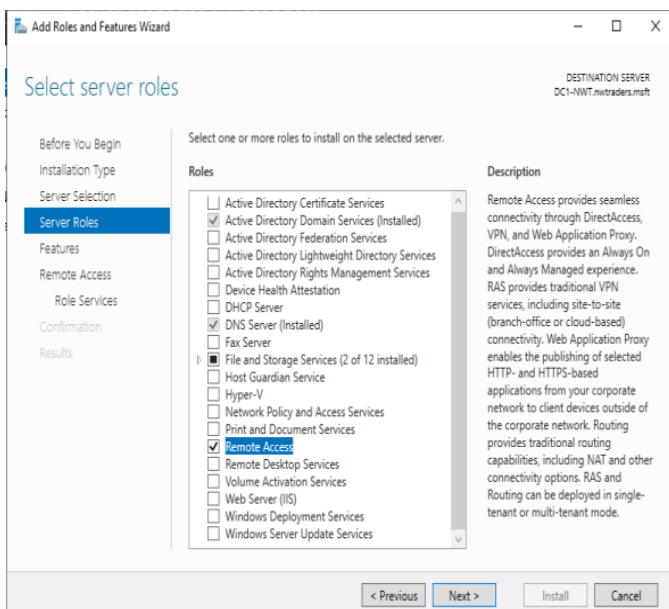


Fig. 13. Figure of Windows Server I - Addition of Remote Access

Selected **DirectAccess and Virtual Point Network (VPN) Network Attached Service (NAS)** within the Select role services menu.

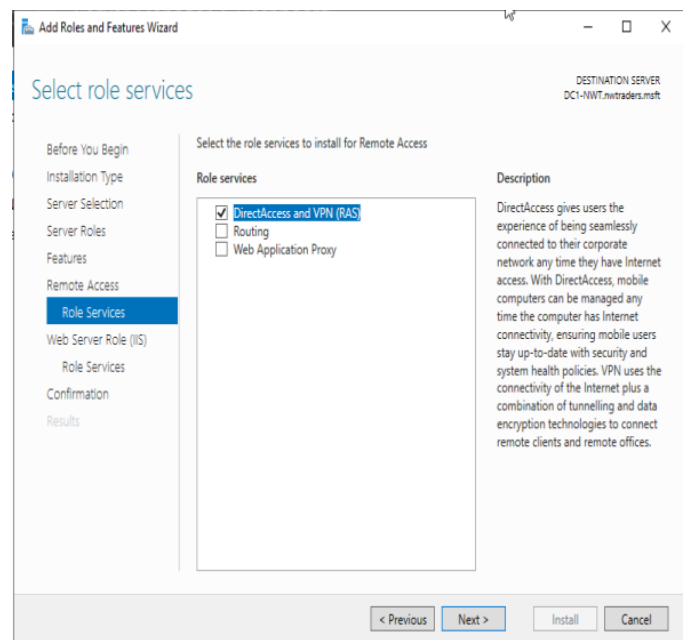


Fig. 14. Figure of Windows Server I - Configuration of Remote Access

G. Windows Server I - Routing and Remote Access Service

Selected **Deploy both DirectAccess and VPN (recommended)** option within Configure Remote Access window.

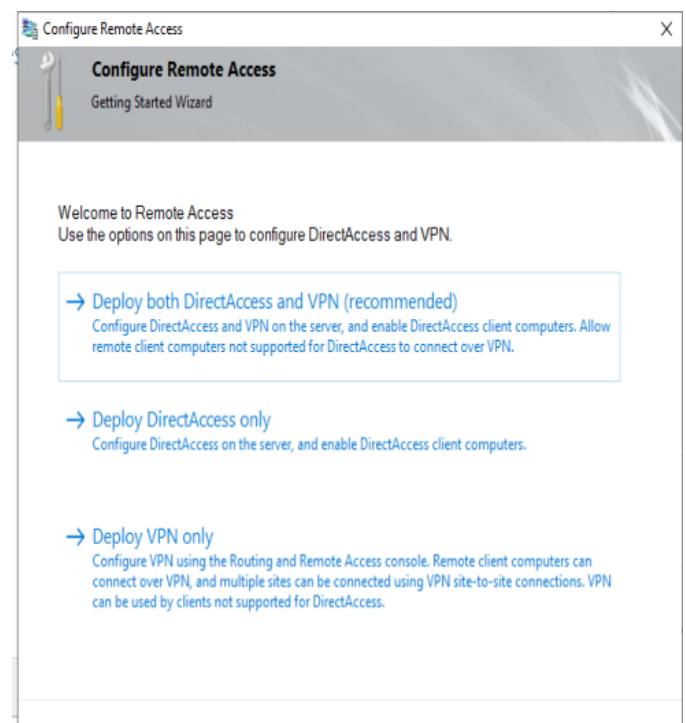


Fig. 15. Figure of Windows Server I - Setting up Remote Access Service

Selected **Custom configuration** radio button to select any combination of the features available in Routing and Remote Access.

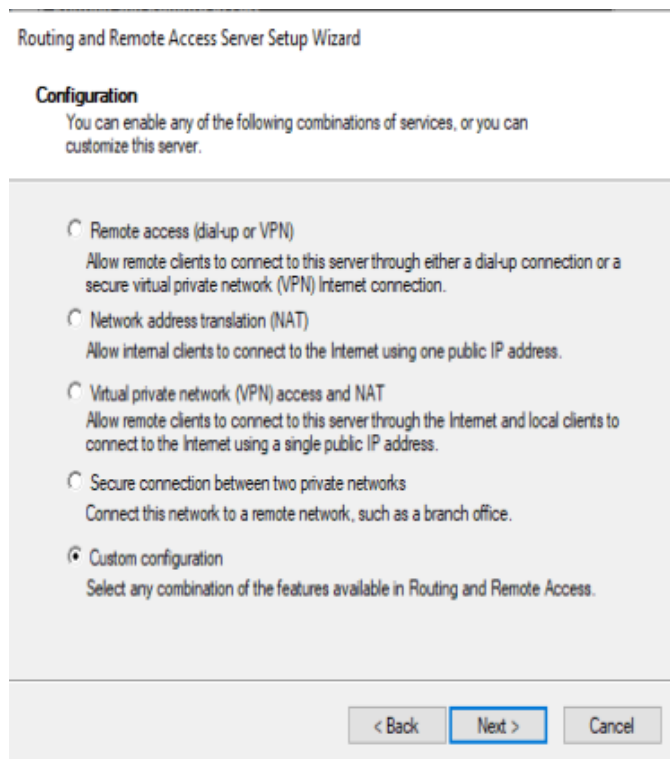


Fig. 16. Figure of Windows Server I - Setting up Remote Access Service

Selected **Local Area Network (LAN) routing** checkbox.

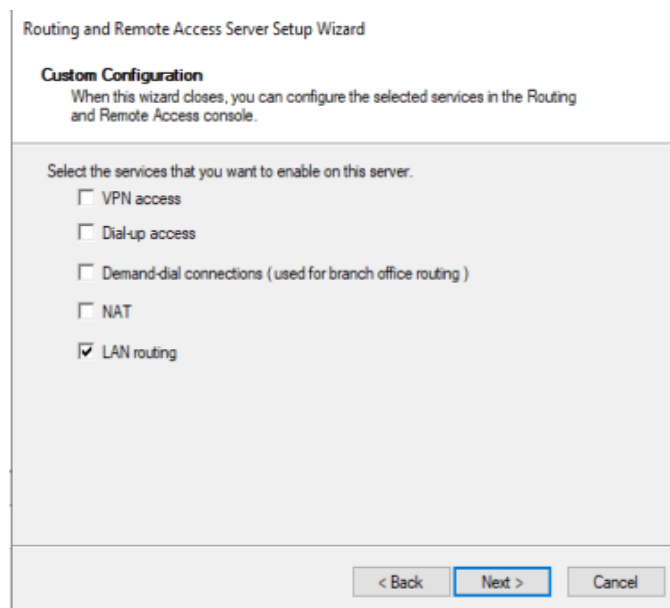


Fig. 17. Figure of Windows Server I - Setting up Remote Access Service

Created a New Routing Protocol and chose **Routing Information Protocol (RIP) Version 2 for Internet Protocol** for the routing protocol.

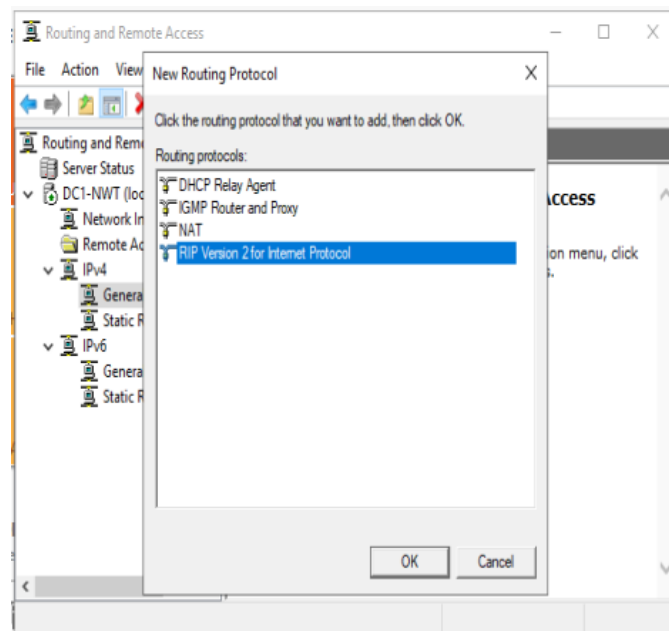


Fig. 18. Figure of Windows Server I - Setting up Remote Access Service

Evidence that RIP routing protocol exists. Repeated these steps for Windows Server II.

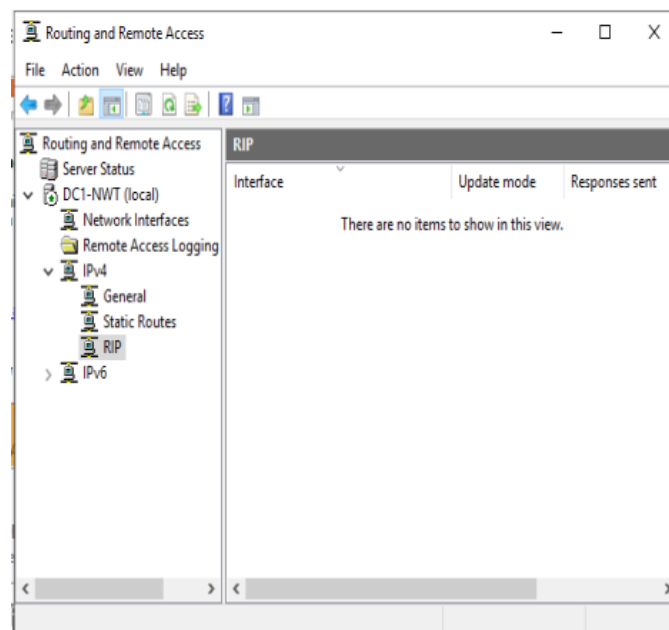


Fig. 19. Figure of Windows Server I - Setting up Remote Access Service

H. Windows Server I - Pings

Windows Server I pinging Windows Server II's public IP successfully.

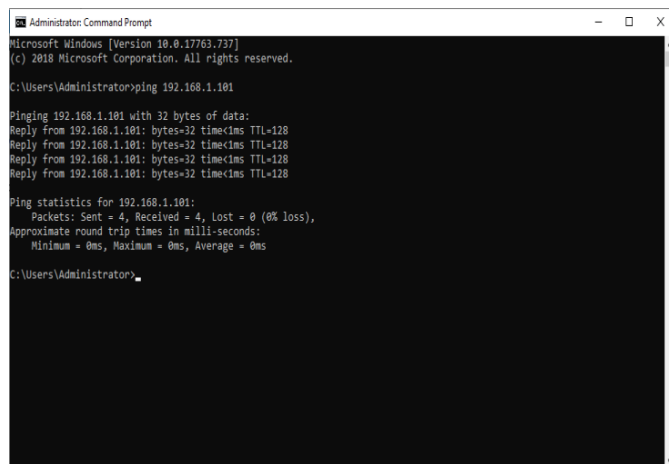


Fig. 20. Figure of Windows Server I - Pinging Windows Server II Public IP

I. Windows Server II - Pings

Windows Client I pinging Windows Client II.

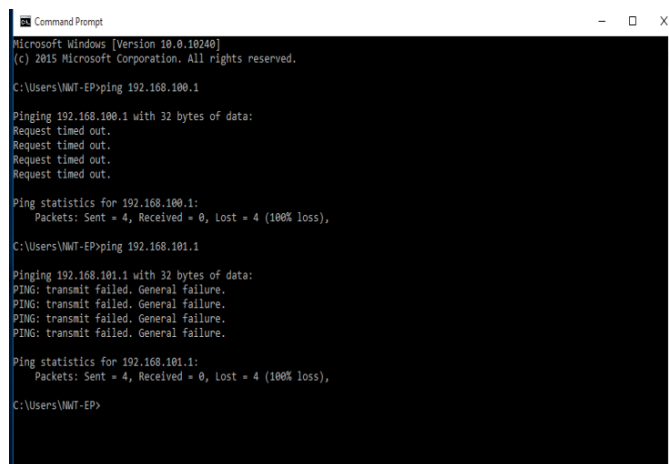


Fig. 21. Figure of Windows Client I - Pinging Windows Client II

III. WORKSHEET FOUR - OBSERVATIONAL

A. Failover Clustering

Based on Microsoft's [2], Failover Clustering in Windows Server article, a failover supplies the ability to increase the availability and scalability of the clustered roles. These clustered servers, also known as nodes, are connected by physical cables and software to communicate within the network.

Cluster Shared Volume (CSV) comes with Failover clusters, a consistent and distributed namespace containing clustered roles. These CSV's are helpful when it comes to accessing shared storage from all nodes within the network.

From the article mentioned, Microsoft [2] suggests that "Failover Clustering has many practical applications, including:

- Highly available or continuously available file share storage for applications such as Microsoft Structured Query Language (SQL) Server and Hyper-V virtual machines.
- Highly available clustered roles that run on physical servers or on virtual machines that are installed on servers running Hyper-V."

Methods to Deploy a Failover Cluster

Tutorial sourced from PaperCut's [3], Microsoft Failover Cluster Manager (MSFCM) on Windows server 2012/2016.

Steps briefly covered off PaperCut's [3] Failover Cluster tutorial.

- Step 1: Configure roles/features on the node for high availability.
- Step 2: Connecting to Internet Small Computer Systems Interface (iSCSI) network drives.
- Step 3: Create the failover cluster.

Requirements to set up a Failover Cluster:-

- 2+ Physical Servers.
- MS Server 2012/2016 with Hyper-V capabilities.
- iSCSI Storage Area Network (SAN) Protocol with two drives configured.
- Drive 1: 5GB (to be used for the Quorum if using only two nodes).
- Drive 2: Virtual Machine (VM) server storage.

The systems set up within the network we've created have the minimum requirements, except for iSCSI Storage Area Network (are not with the current build). Read any other requirements within the article supplied above.

After analysing the first step, it asks to install MS Server 2012 or 2016 (Windows Server 2019 in this particular case). Within the Add Roles and Features window within the Server Role selection, the role of Hyper-V needs to be selected (demonstrated in the figure 22). Within the Features selection, the feature Failover Clustering is required (shown in the figure 23). The network adapter that inherits Failover Clustering is PrivateNet1.

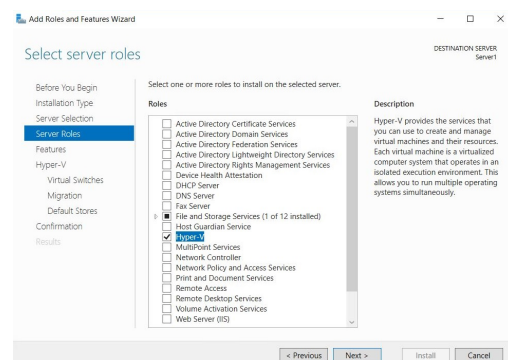


Fig. 22. Figure of Failover Cluster Theory

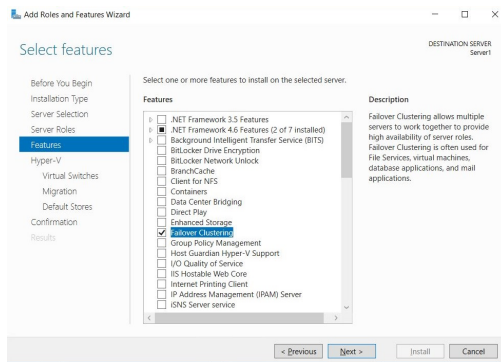


Fig. 23. Figure of Failover Cluster Theory

The iSCSI drives would need to be set up within the virtual network to complete the second step. Follow the second step closely within PaperCut's [3] to complete this step. This enables users to store information similar to our NTFS File Sharing method for clients to move files to and from the Windows Server I node.

The creation of the Failover Cluster happens in step three. This is done by launching the Failover Cluster Manager window by the Administrative Tools window (demonstrated by figure 24). Create Cluster option is available within this window. After clicking the option, a new window will display. This window offers Failover Cluster configuration, which includes the Server Name that the cluster belongs to. This can be done manually or using the browse feature.

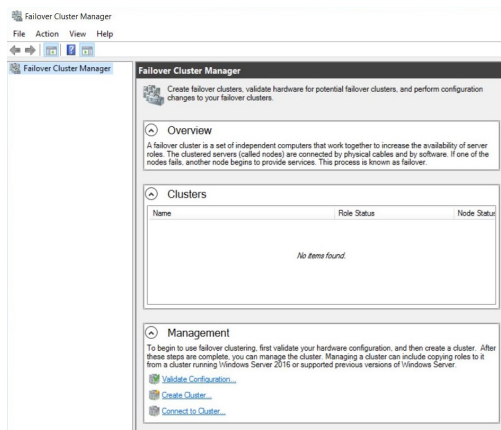


Fig. 24. Figure of Failover Cluster Theory

It is crucial to verify the cluster services to ensure the cluster is set up and runs correctly. It is also important to validate any options and run tests given. This is to make sure that there are no errors and notifies the user of any problems in detail. If the user was experienced and could figure out the process in given cases, then in some cases, the user will not touch the feature. Make sure to read PowerCut's [3] to configure the Failover Cluster correctly.

IV. HEAD NETWORK ADMISTRATOR SUGGESTIONS

A. Network Architecture

The network architecture is as followed.

- **Head Network Administrator** - This role can suggest and implement the network architecture, topology, design, and policies within the network.
- **Network Administrator** - This role can test, and review is capable of testing and reviewing to test and review
- **Administrator** - Administrative role makes sure that users issues with connectivity, logging on, and software that the user requires users within guidelines of the policies set for the network are met to keep staff workflow and positivities high. Any vulnerabilities that are detected reports to the Network Administrator or Head Network Administrator.
- **User** - User role may use the network with restrictions. These restrictions are mentioned within the Network Policy IV-B Network Policy, page 7.
- **FTPUser** - The FTP access role may give the user permissions to edit, create and delete file contents depending on the location where the user account can access. FTP User groups are guidelines and can be overridden depending on the user account that is set up.

B. Network Policy

The network should meet the following criteria.

- **Password Policy** - Use of:-
 - randomised characters (12 - 32 character length.)
 - uppercase and lowercase characters.
 - numerical characters.
 - symbols.
 - a secure password generator - Refer to Daniel Blechynden [4] Best password generators in 2021 to decide on the best one. (Author's recommendation: NordPass — Author's Reason: The service offers a secure password generator and password encryption. However, it can cost the user a small fee per month. The password generator that Nord's [5] NordPass offers is free, store this password in a safe place and if the password is compromised, change the password as soon as possible.)

• User Group Policies

- *Head Network Administrator* - Password Policy Restriction - Any user groups with extra access abilities must remain protected to protect the network.
Audit logs must be kept to track the latest changes or history of the user. This stops data leakage or provides clues of any problems that crop up in the network.
- *Network Administrator* - Password Policy Restriction - Any user groups with extra access abilities must remain protected to protect the network.
Audit logs must be kept to track the latest changes or history of the user. This stops data leakage or provides clues of any problems that crop up in the network.
- *Administrator* - Password Policy Restriction - Any user groups with extra access abilities must remain protected to protect the network.
Audit logs must be kept to track the latest changes or history of the user. This stops data leakage or provides clues of any problems that crop up in the network.
The role should have no access to the BIOS configuration on the server-side. However, Administrative roles need to have BIOS configuration on workstations. This helps configure workstations when configuring new or existing stations to work within the network.
- *User* - Password Policy Restriction.
Audit logs help prevent hackers or any tampering from using User groups. For example, if a user tried to use PowerShell instead of Command Prompt to gain extra privileges or used a USB attack. Refer to Catalin Cimpanu [6] Here's a List of 29 Different Types of USB Attacks article to read more on the dangers of external USB's and how to safeguard the issues.
The user group should be restricted to administrative tools such as control panel, command prompt, PowerShell and scripts. It is mindful that Java scripts that run in a Java Virtual Machine (JVM), which can be executed just by running the file, C++, Python or other scripts, can be a potential issue. These applications are not always the standard Windows execution programmes and can provide the user with weak network points.
Backdoors within the network, such as access points, can have the same detrimental effect on the network. With the capabilities of brute-forcing and sniffing. Refer to Ahmed mohammed [7] Password Cracking Using Cain & Abel article to understand the problems with password bruteforcing and sniffing.
- *FTPUser* - Password Policy Restriction - It is required for this in place for FTP user's as it provides a remote connection to the network.

Audit logs are required as malware could be uploaded and executed via FTP access. This helps prevent any outside attack. It is essential to focus anti-virus or malware detection programmes directly on any weak areas known for remote access or storage area networks that computer users use to protect both staff and consumers who use the internal network.

The FTP User should have a timeout and other policies in place to prevent password cracking. FTP has the functionality to disallow IPs that make too many attempts at logging in or uploading invalid file formats. Refer to [8] Filename Filters understand about Filezilla Server - File Name Filters to prevent any unknown file types.

C. Network Topology

After observing the Study Tonight [9] Types of Network Topology article, the Mesh topology sounds reasonable for the network. The method chosen is to make sure there is a minimal fault within the network. Any defect that arises within a Mesh topology is accessible to detect. The features of the topology are fully connected, robust and not flexible. The advantages of the topology are that data transfers can be initiated or sent anywhere during the network, and it provides security and privacy between nodes. However, the installation and configuration are complex, the cabling cost is higher, and bulk wiring is required.

The author has chosen this technique over another topology like Ring topology, similar to the Mesh topology. However, troubleshooting within a Ring topology is more complicated, which may sound cheap to create the setup but could prove costly further down the line. When adding workstations or other network nodes to the topology disrupts the network, the Mesh topology enables new devices to be added or removed with no network disruption.

Any databases within the network should not be connected to the Mesh topology. Ensure that the database is connected to one or two nodes within the network, and connecting to the database connection can only be made via one or the other node with the appropriate identification. This is important; otherwise, users can connect directly to the database node from the workstation and start penetration methods to gather information. A couple of nodes as a gateway prevent connection based on user groups or login requests.

D. Security Methods

To summarise the policies to avoid data breaches and other security issues, it is essential to mention the methods to report suspicious activity. Systems should be put in place to scan audit logs to keep both the work environment safe from tampering or malicious activity. Having virus protection in a place like Malwarebytes [10] to monitor NAS, FTP or NTFS file sharing areas that have the risk of user accounts moving malicious files across (perhaps unintentionally).

Any security flaws found as a staff member or other roles, report any security flaws to either an Administrator, Network Administrator or Head Network Administrator. Any users with USB or remote access, make sure the device has appropriate security measures like Malwarebytes [10] or other virus protection programmes to make sure the device is virus-free. This means scanning a USB drive on a device not connected to the network. The network must have virus protection and malware protection to keep the network safe as much as possible.

Also, it is essential to mention that all database communications must be encrypted as user accounts or other sensitive data could be compromised within the network.

V. LIST OF ABBREVIATIONS

- *NTFS* - New Technology File System.
- *FTP* - File Transfer Protocol.
- *IIS* - Internet Information Services.
- *ARP* - Address Resolution Protocol.
- *NIC* - Network Interface Card.
- *MAC* - Media Access Control.
- *SSL* - Secure Sockets Layer.
- *IP* - Internet Protocol.
- *VPN* - Virtual Point Network.
- *NAS* - Network Attached Service.
- *LAN* - Local Area Network.
- *RIP* - Routing Information Protocol.
- *SQL* - Structured Query Language.
- *MSFCM* - Microsoft Failover Cluster Manager.
- *CSV* - Cluster Shared Volume.
- *iSCSI* - Internet Small Computer Systems Interface.
- *SAN* - Storage Area Network.
- *VM* - Virtual Machine.

VI. CONCLUSION

The report covers the different file services like the local NTFS file sharing vs the remote FTP file sharing, demonstrating the various connections and setting up the benefits and evidence of how the client workstations interact with one another.

VII. REFERENCES

- [1] SSLShopper, "Why SSL? The Purpose of using SSL Certificates." [Online]. Available: <https://www.sslshopper.com/why-ssl-the-purpose-of-using-ssl-certificates.html>
- [2] Microsoft, v-kents, MightyPen, DCtheGeek, eross-msft, and JasonGerend, "Failover Clustering," Jun. 2019. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview>
- [3] PaperCut, "Microsoft Failover Cluster Manager (MS-FCM) on Windows server 2012/2016." [Online]. Available: <https://www.papercut.com/support/resources/manuals/ng-mf/common/topics/cluster-server-2012-2016.html>
- [4] D. Blechynden, "Best password generators in 2021," Apr. 2021. [Online]. Available: <https://www.techradar.com/uk/best/password-generator>
- [5] Nord, "Password Generator: Strong & Random Passwords." [Online]. Available: <https://nordpass.com/password-generator/>
- [6] C. Cimpanu, "Here's a List of 29 Different Types of USB Attacks," Mar. 2018. [Online].

Available: <https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/>

- [7] A. Mohammed, "Password Cracking Using Cain & Abel," Jan. 2018. [Online]. Available: <https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/>
- [8] FileZilla, "Filename Filters - FileZilla Wiki," Apr. 2021. [Online]. Available: https://wiki.filezilla-project.org/Filename_Filters
- [9] Study tonight, "Types of Network Topology in Computer Networks | Studytonight." [Online]. Available: <https://www.studytonight.com/computer-networks/network-topology-types>
- [10] MalwareBytes, "Malwarebytes Premium | Anti-Malware Protection." [Online]. Available: <https://www.malwarebytes.com/lp/sem/uk/?gclid=Cj0KCQjwsqmEBhDiARIsANV8H3Z8jrTE04g-UNzrJHPaDVvg2QHUhXZJwcB>