

Name: Yonatan Grmay

Student Number: 2433740

Assignment title : Network Operating Systems and Services

Module Name: Network Operating Systems and Services

Lecture: Md Abrar Jahin Almazi Bapon

Module code:ACCA5023

Date 23/Julay/2025

Table of Contents

1. Routing.....	1
Introduction	1
1.1 Routing in Birmingham Network	2
Objective	2
Installing Routing and Remote Access Service (RRAS)	2
Configuring RRAS	5
Windows Firewall Configuration	10
Verification.....	15
Outcome	16
1.2 Routing in London Network	16
Objective	16
Enabling IP Forwarding	17
Configuring Static Route.....	20
Configuring Linux Firewall	21
Verification.....	21
Discussion	22
Conclusion	22
2. Domain Server (Birmingham)	22
Introduction	22
2.1 Creating the Forest (yonatan.acca)	23
Objective	23
Figure 33: – Active Directory Users and Computers.....	24
2.2 Creating A Records.....	25
Objective	25
Figure 34: – Forward Lookup Zone.....	26
2.3 Creating Reverse Lookup Zone (PTR Records)	26
Objective	26
Figure 35: – Reverse Lookup Zone	27
Password Policy (Excellent Work Requirement)	27
Figure 36: – Password Policy	28

Verification	28
Discussion	29
Conclusion	29
3. Encrypted Connection Between Birmingham and London	30
Introduction	30
3.1 Configuring a Site-to-Site VPN	30
Objective	30
Configuring RRAS for VPN	31
Configuring the Site-to-Site VPN	32
Configuring Strong Encryption	33
Persistent Connection Configuration	34
Verification	35
Discussion	36
Conclusion	36
4. Users	37
4.1 Creating Domain User Accounts	37
Introduction	37
PowerShell Bulk User Creation	37
Verification	38
5. Domain Membership	39
5.1 Joining Computers to the Domain	39
Introduction	39
Configuration	39
Verification	40
6. DHCP Server	41
6.1 Configuring B-DC as DHCP Server	41
Introduction	41
DHCP Options	42
6.2 Configuring DHCP Relay	50
6.3 Client Verification	50
7. Test and Troubleshoot	53
Connectivity Testing	53

8. Disk Drive	54
8.1 Shared Storage.....	54
9. IIS Server	56
9.1 Creating the Website	56
10. Remote Desktop Services	58
10.1 Configuring Remote Desktop.....	58
Overall Conclusion	60

Acknowledgement

I am very grateful to my lecturer for his guidance and support during this coursework on networking. I also want to express my gratitude to my University for giving me the resources and hands-on experience to carry this out. This assignment allowed me to gain hands-on experience with network routing, Active Directory, DNS, DHCP, VPNs, file sharing, IIS, and Remote Desktop Services. Last but not least, I would like to thank all those who have contributed to the successful completion of this work.

1. Routing

Introduction

Routing is one of the most important functions within an enterprise network because it enables communication between different IP networks. In the topology provided for NOSS London 2026 Inc., the Birmingham network and the London network are located on separate subnets and therefore require routing to exchange traffic successfully. Windows Server 2022 located in Birmingham functions as the primary router through the Routing and Remote Access Service (RRAS), while the Debian Server in London performs packet forwarding using Linux IP forwarding.

The implementation of routing ensures that network devices located in Birmingham (172.16.1.0/24) can communicate with devices located in London (172.16.2.0/24) through the point-to-point network (10.0.0.0/30) shown in the coursework topology.

Topology

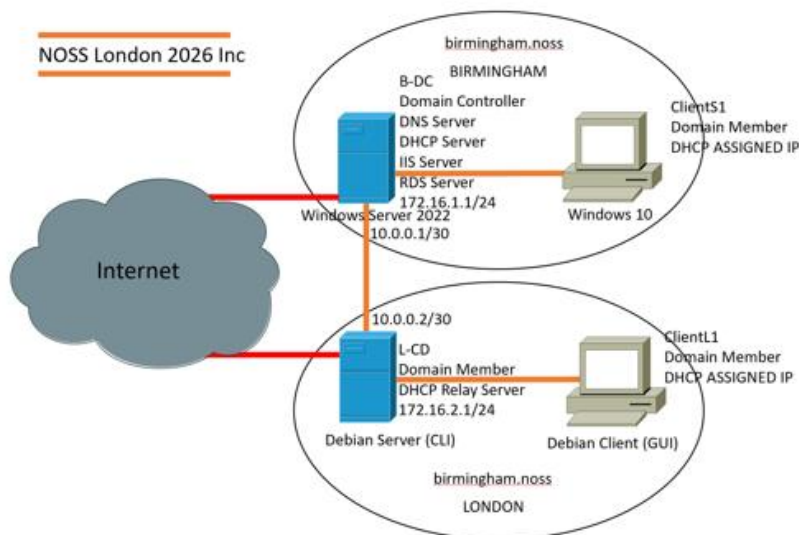


Figure 1 illustrates the network topology used throughout Coursework 2.

1.1 Routing in Birmingham Network

Objective

The objective of this task was to configure the Windows Server 2022 as the router between both sites by installing the Routing and Remote Access Service (RRAS). Additionally, Windows Defender Firewall was configured to allow ICMP traffic so that connectivity testing using the ping command could be performed.

The Birmingham Windows Server has two network interfaces:

Network Adapter	IP Address	Purpose
LAN Adapter	172.16.1.1/24	Birmingham Internal Network
WAN Adapter	10.0.0.1/30	Connection to London

This configuration follows the network topology supplied in Coursework 1.

Installing Routing and Remote Access Service (RRAS)

RRAS was installed using Windows Server Manager.

The following procedure was completed:

1. Open **Server Manager**
2. Select **Add Roles and Features**
3. Choose **Role-based installation**
4. Select the Windows Server 2022 machine
5. Expand **Remote Access**
6. Tick Routing
7. Continue with the installation.
8. Restart the server if required.

After installation, RRAS was configured.

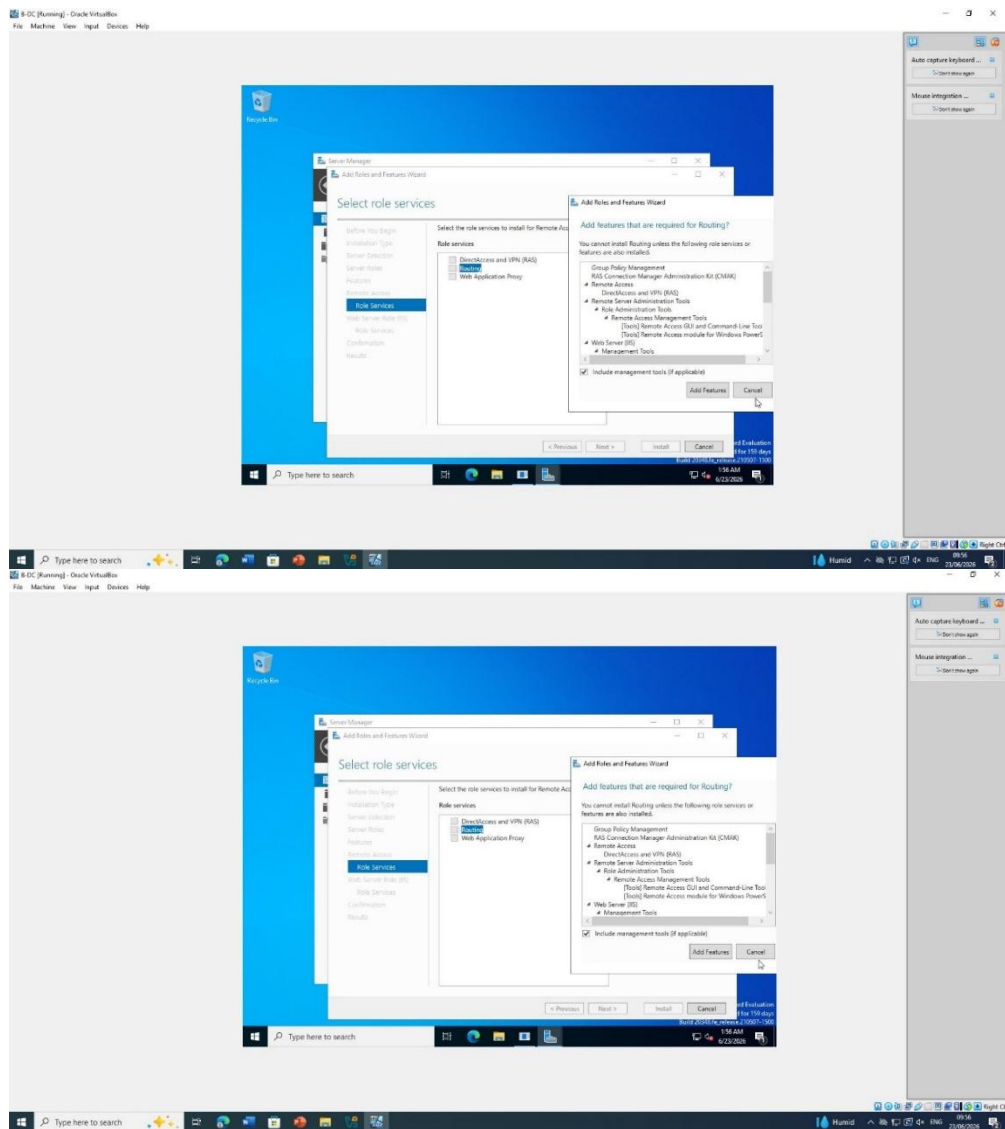


Figure 2 and 3: RRAS Role Installation

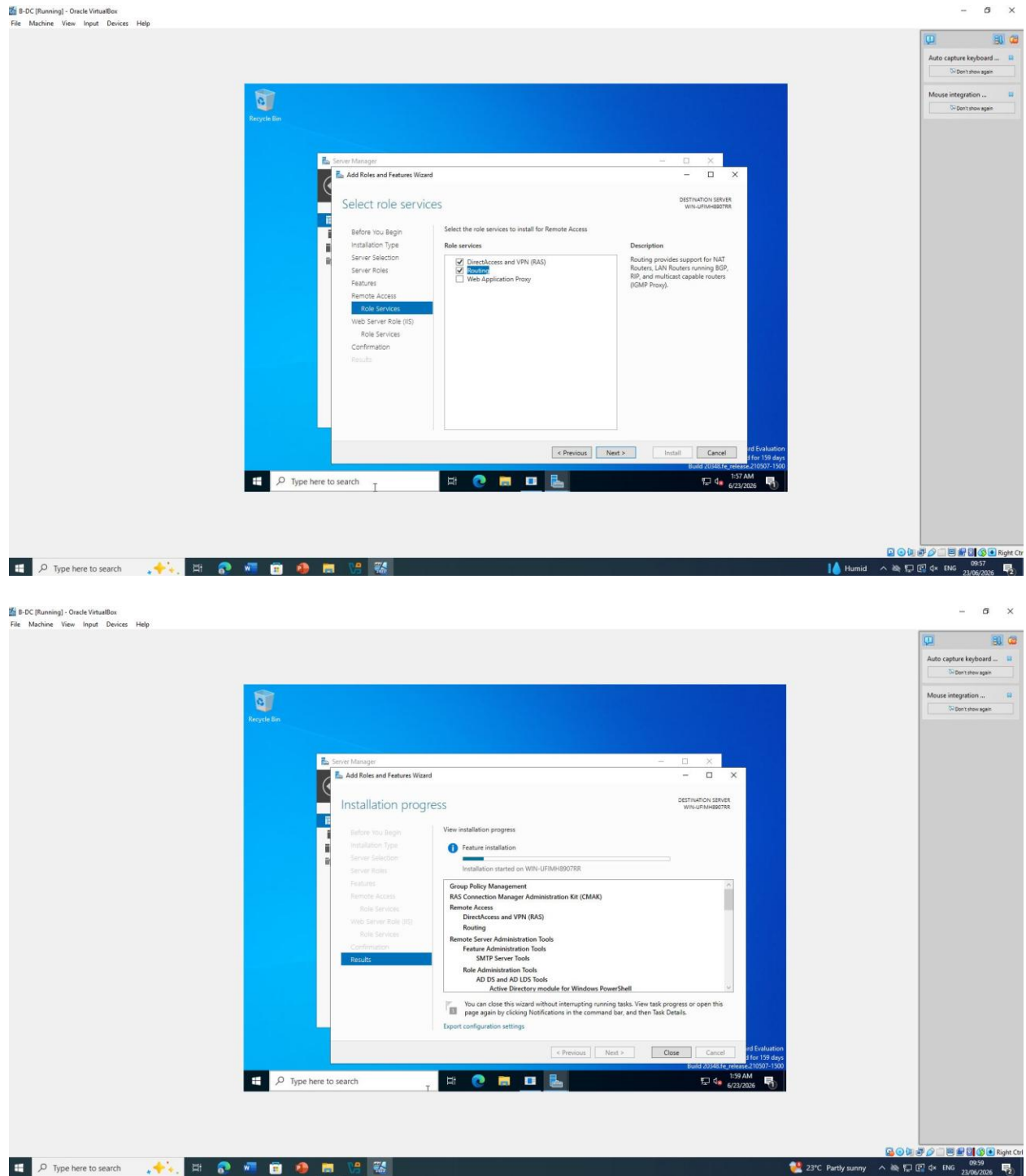


Figure 4 and 5: RRAS Role Installation

Configuring RRAS

After installation:

1. Open

Tools



Routing and Remote Access

2. Right-click the server
3. Select

Configure and Enable Routing and Remote Access

4. Choose

Custom Configuration

5. Tick

✓ LAN Routing

6. Finish the wizard.
7. Start RRAS service.

This enables Windows Server to forward packets between the Birmingham LAN and the point-to-point network.

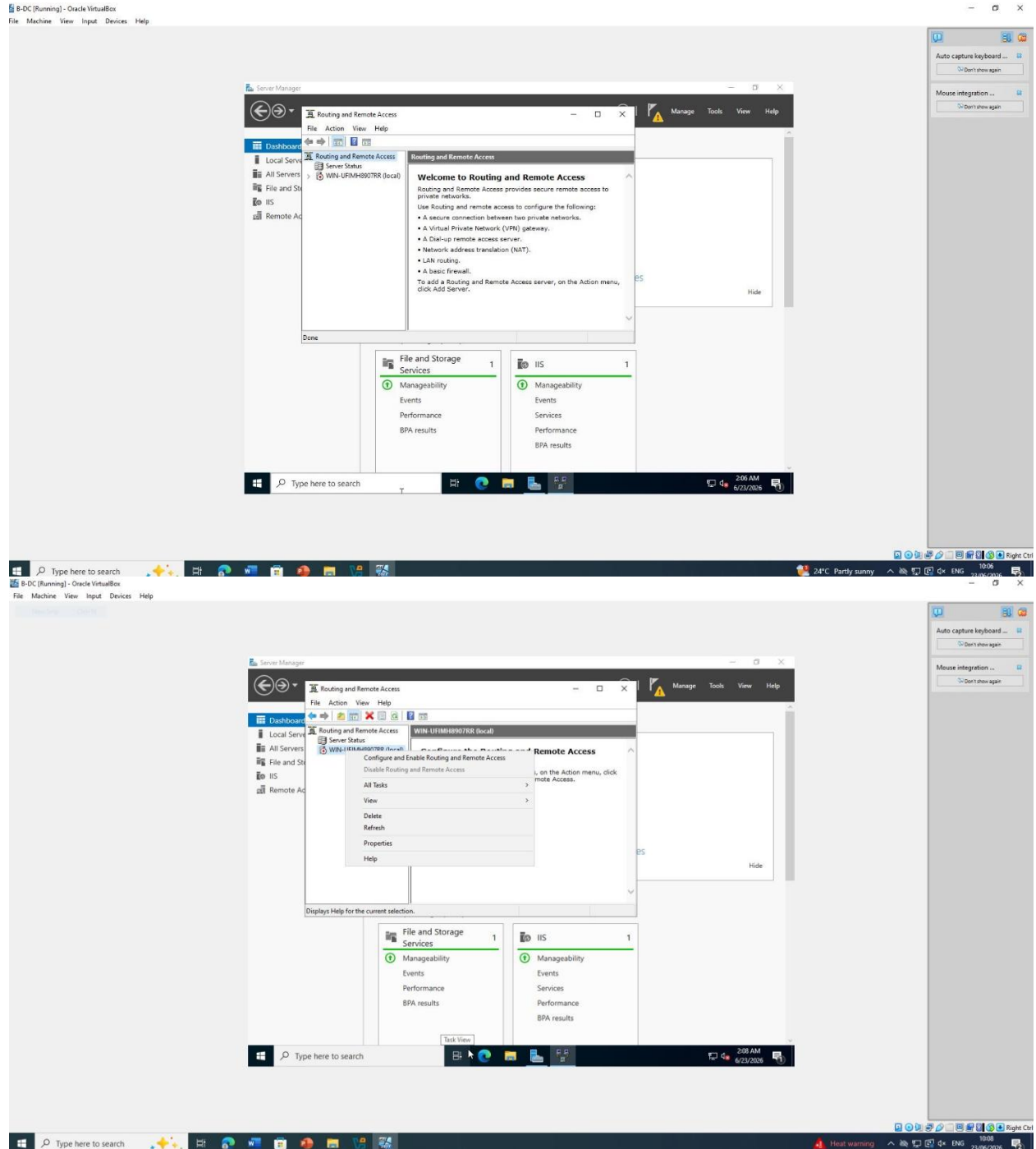


Figure 6 and 7: RRAS configured and running

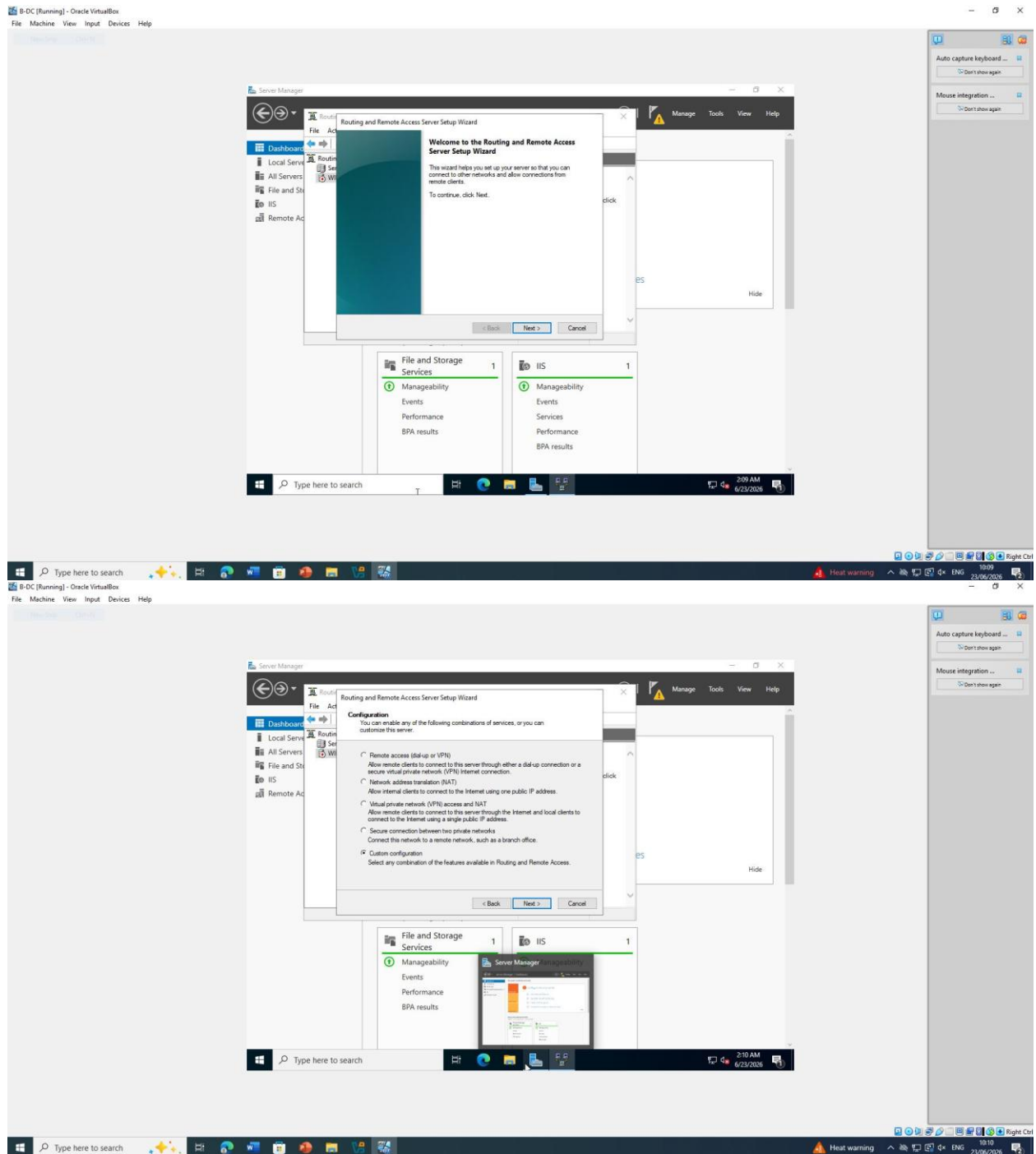


Figure 8 and 9: RRAS configured and running

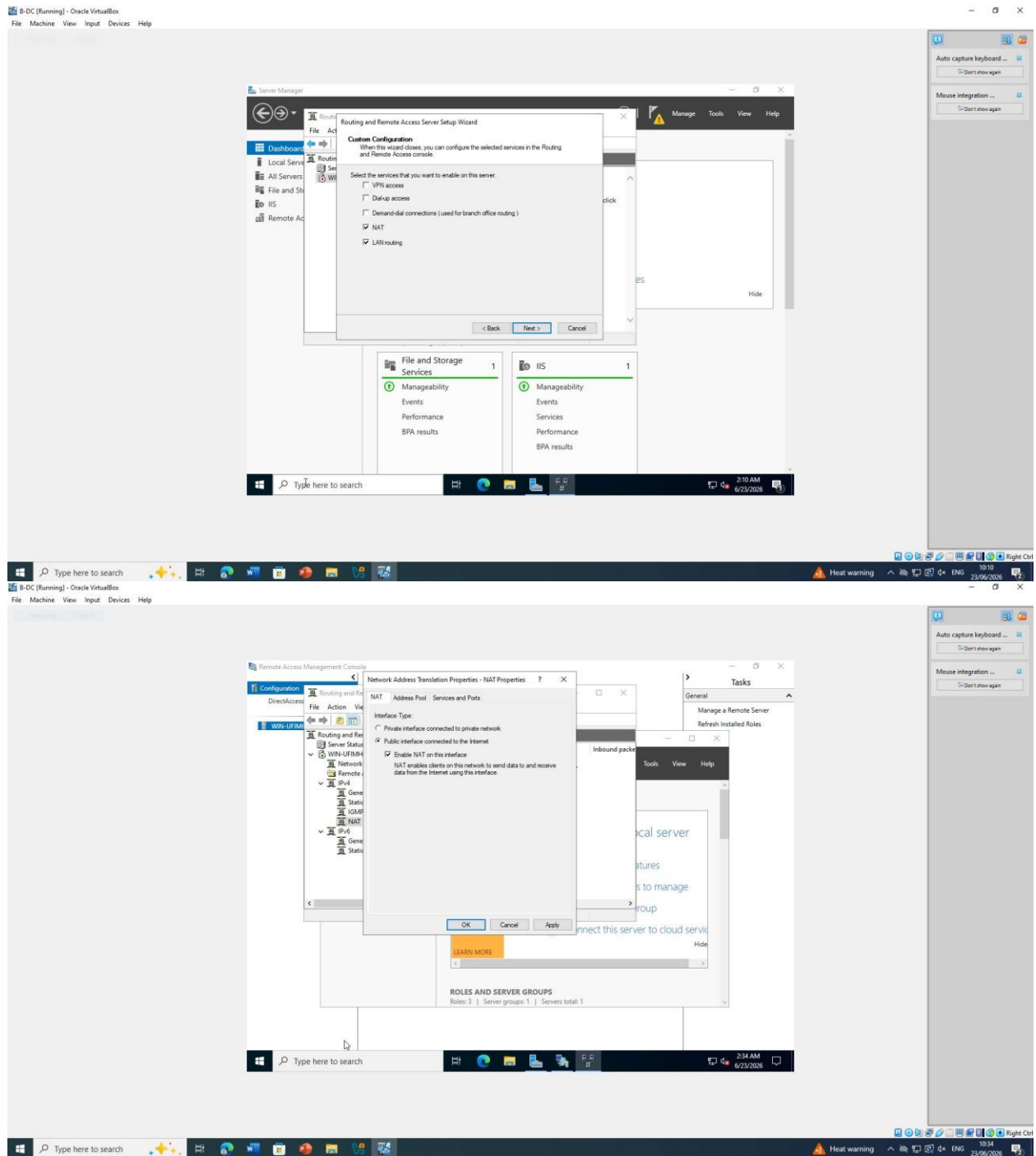


Figure 10 and 11: RRAS configured and running

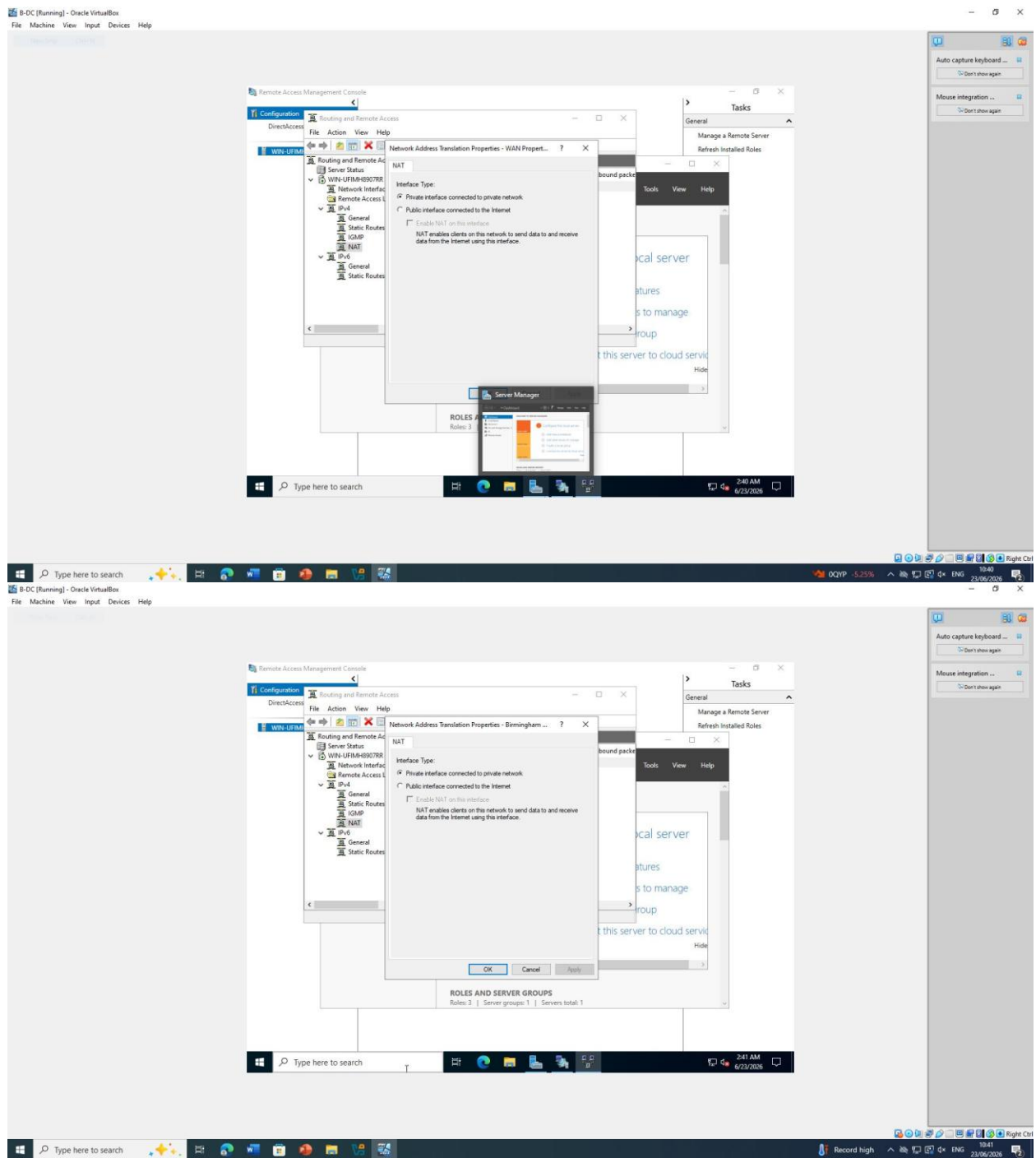


Figure 12 and 13: RRAS configured and running

Windows Firewall Configuration

By default, Windows Firewall blocks ICMP Echo Requests.

To allow connectivity testing, ICMP was enabled.

Procedure:

1. Open

Windows Defender Firewall with Advanced Security

2. Navigate to

Inbound Rules

3. Locate

File and Printer Sharing (Echo Request – ICMPv4-In)

4. Enable the rule.

Alternatively PowerShell can be used:

Allowing ICMP traffic assists network administrators in troubleshooting routing problems and verifying end-to-end connectivity.

(Microsoft, 2024)

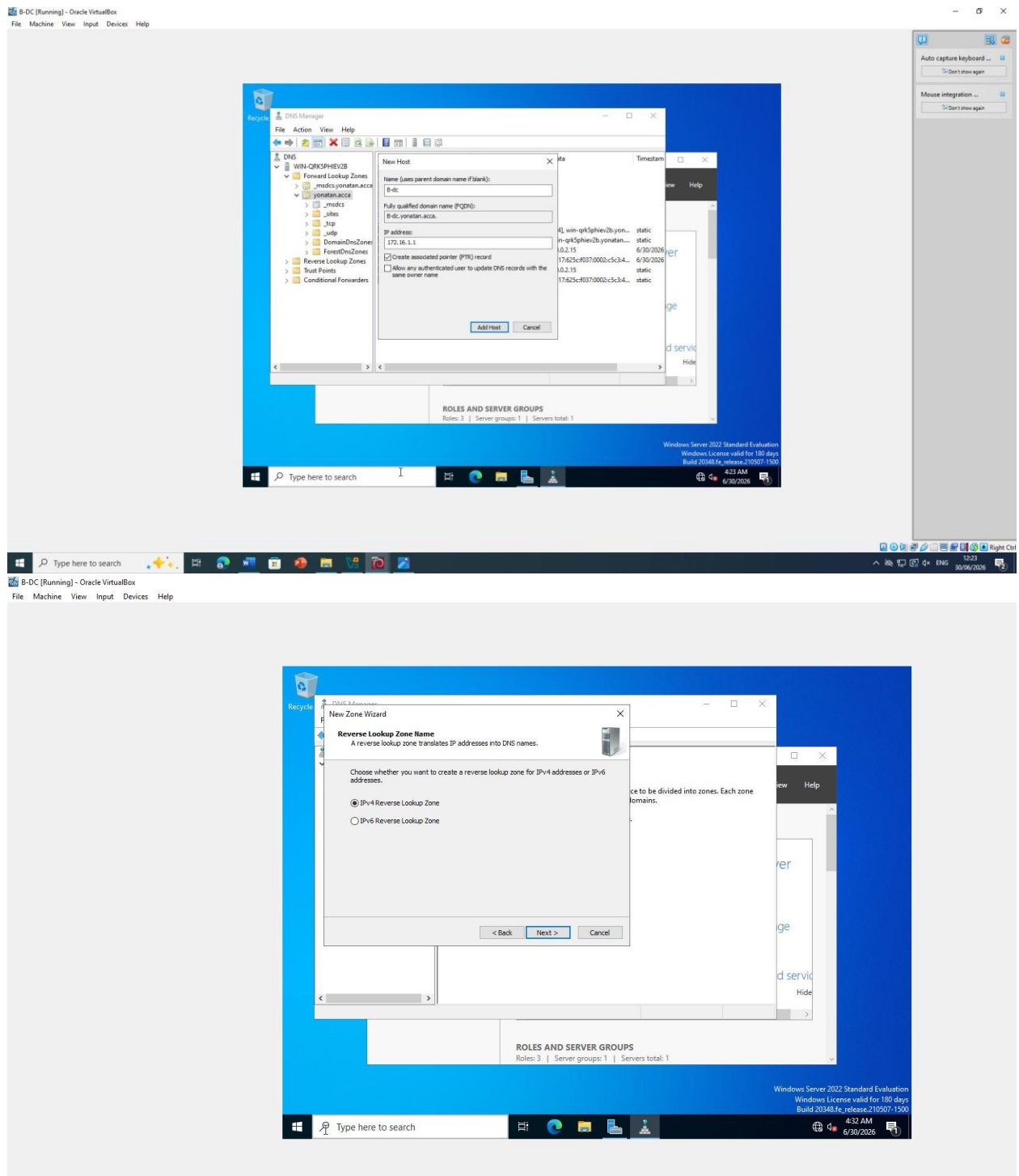


Figure 14 and 15: Windows Firewall (ICMP Rule Enabled)

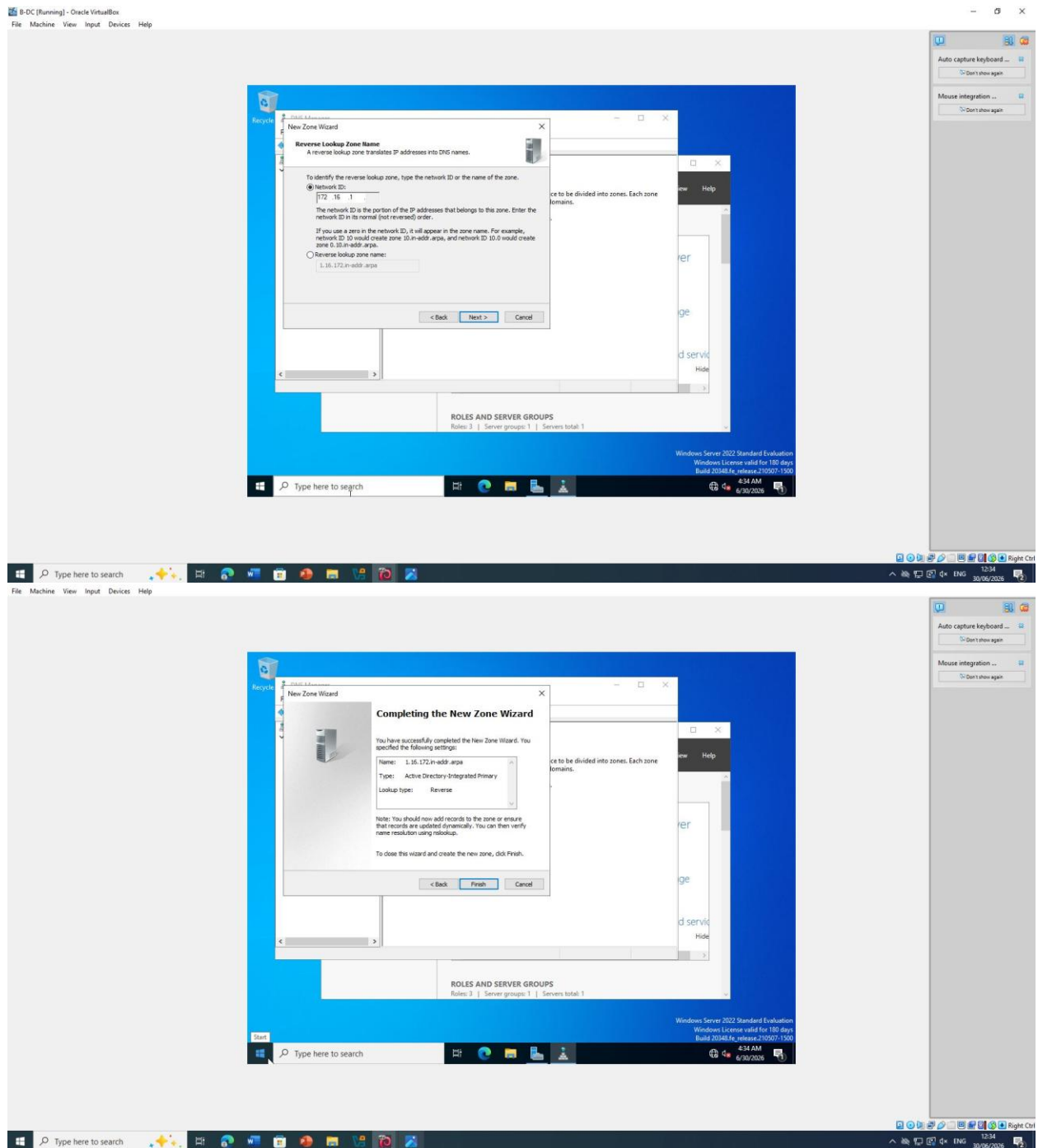


Figure 15 and 17: Windows Firewall (ICMP Rule Enabled)

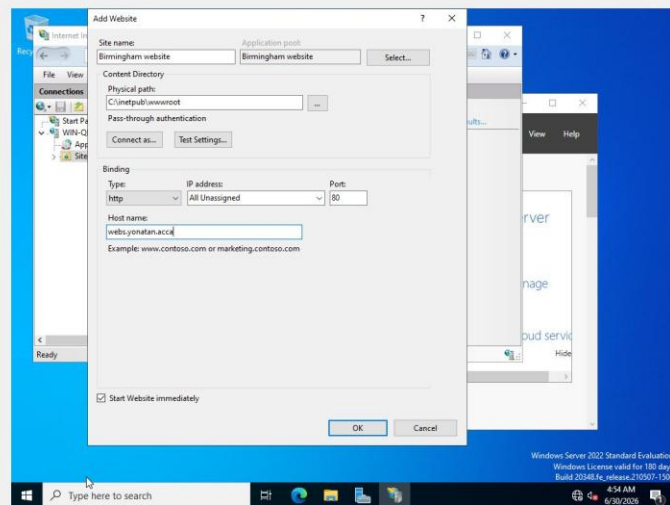
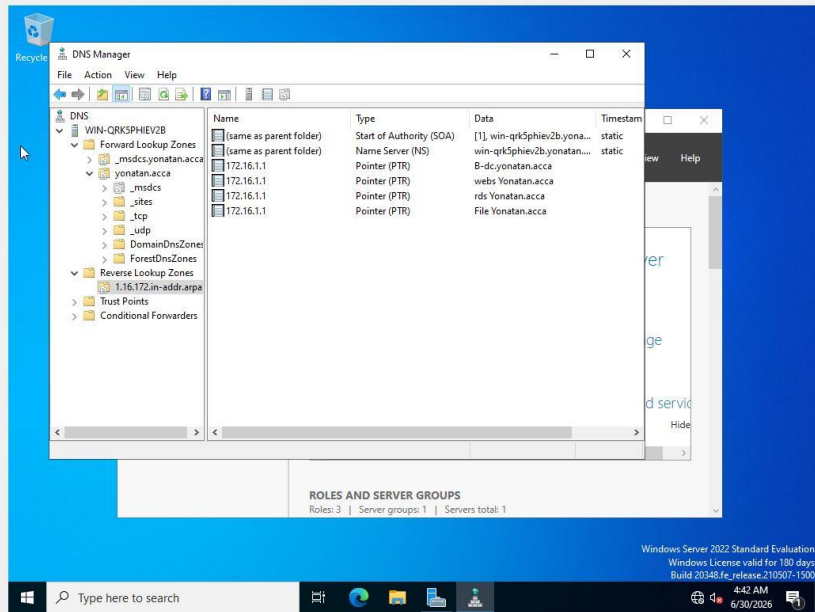


Figure 18 and 19: Windows Firewall (ICMP Rule Enabled)

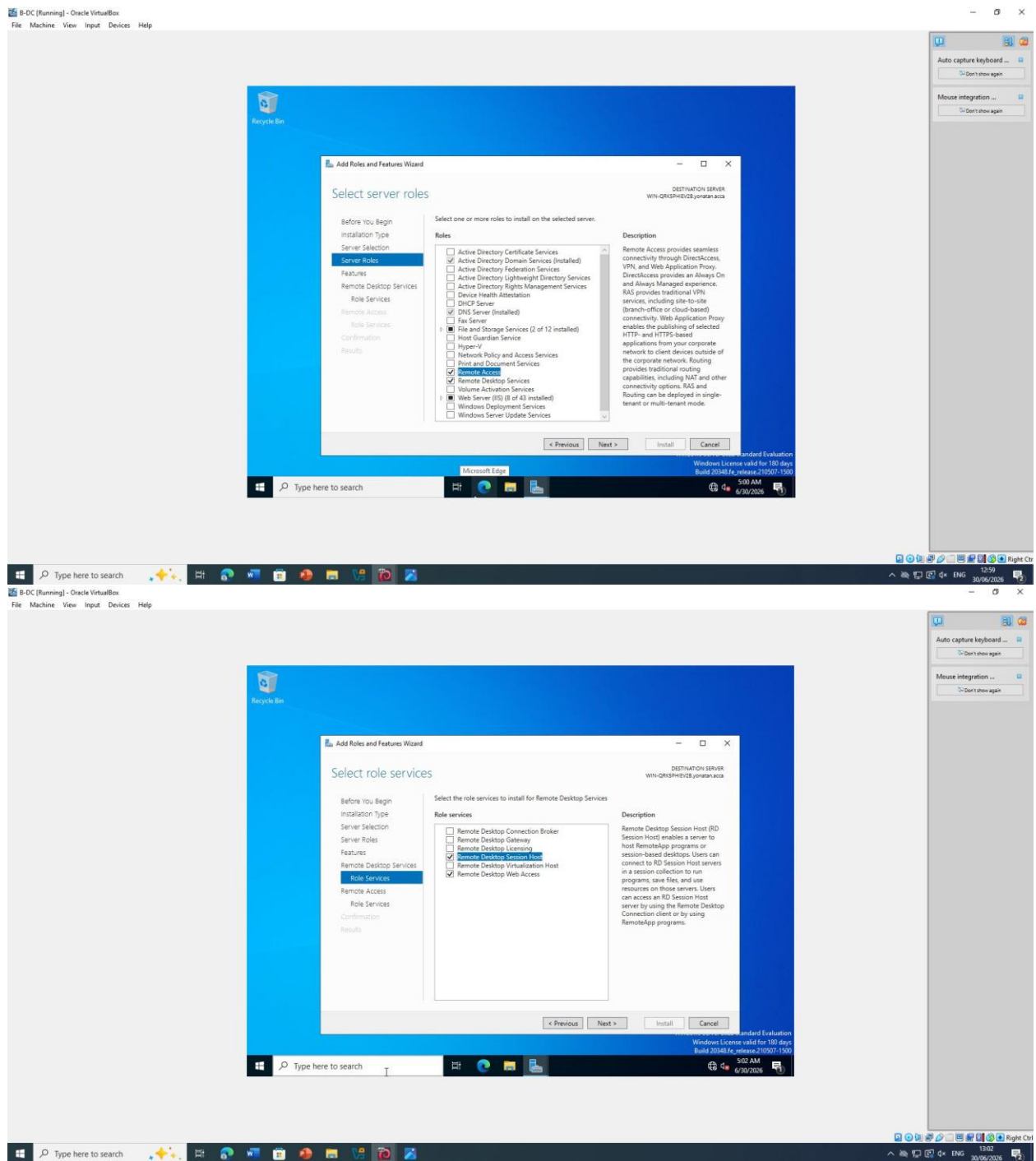


Figure 20 and 21: Windows Firewall (ICMP Rule Enabled)

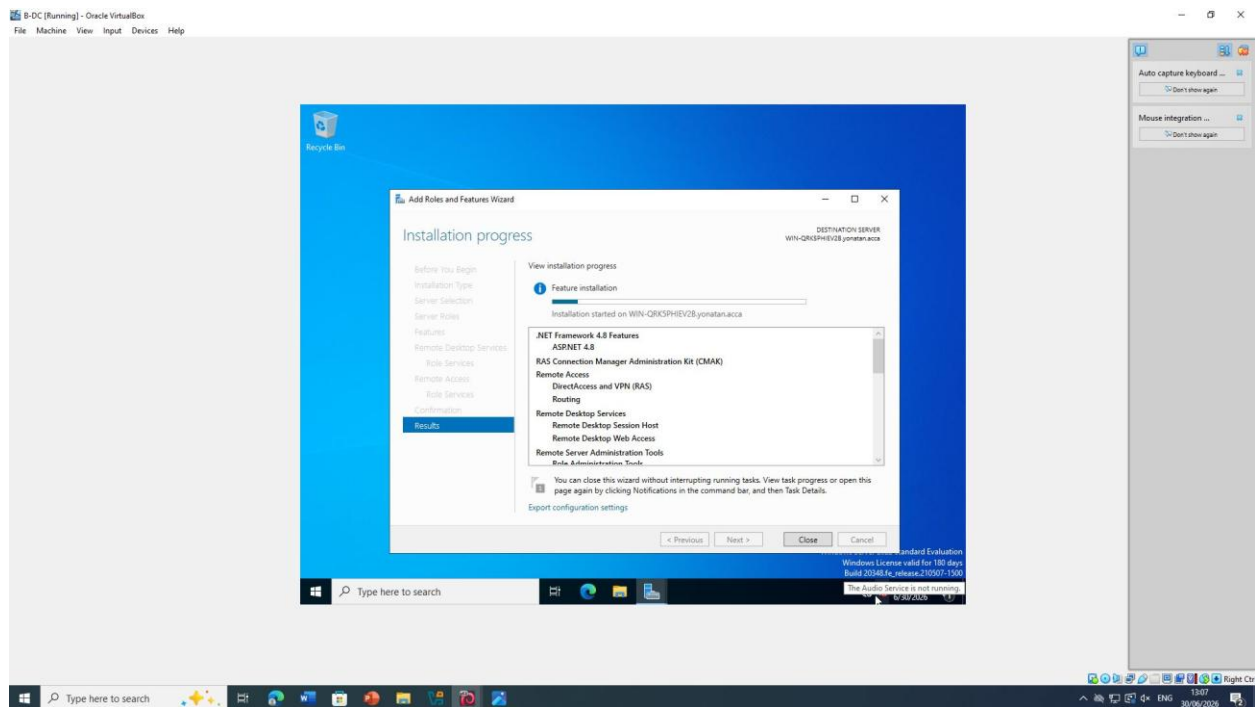


Figure 22: Windows Firewall (ICMP Rule Enabled)

Verification

Connectivity was verified using the Ping command.

Example:

```
ping 172.16.2.1
```

Successful replies confirmed that RRAS was routing traffic correctly.

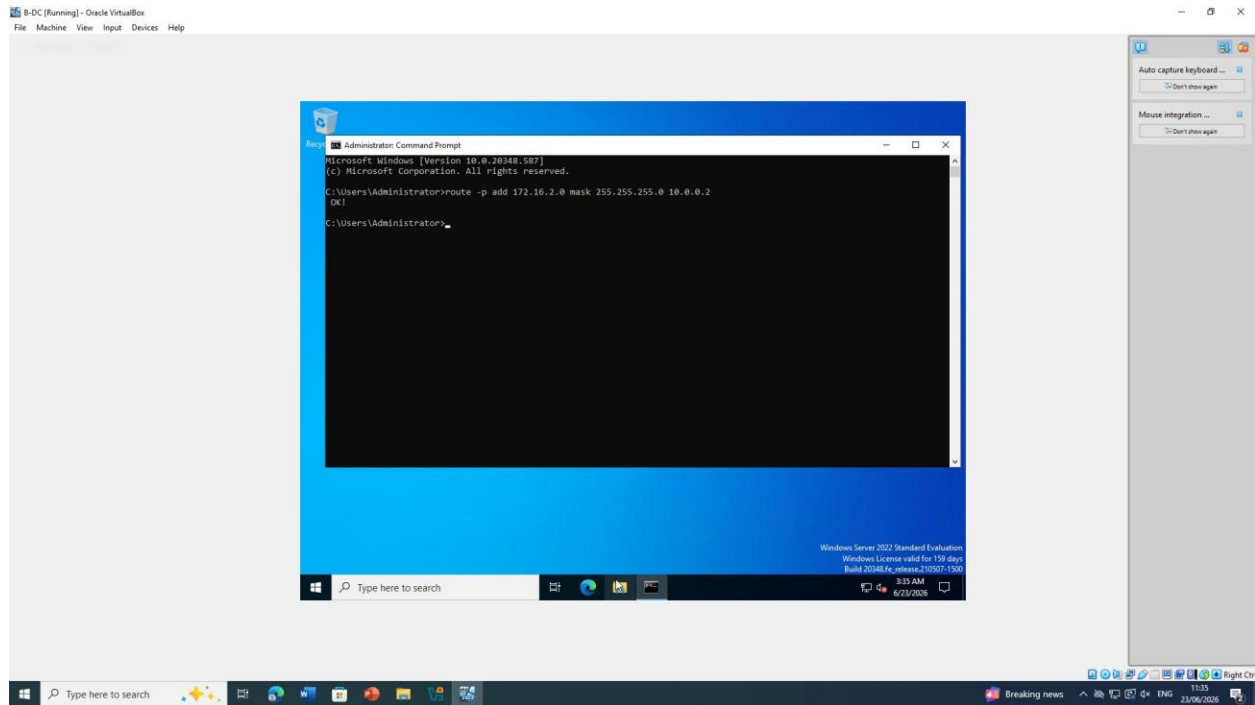


Figure 23: Ping from Windows Server

Outcome

The Windows Server successfully performed Layer 3 routing between Birmingham and London. RRAS dynamically forwarded packets received from one interface to the other, allowing communication between both LANs.

1.2 Routing in London Network

Objective

Unlike Windows Server, Debian Linux uses kernel IP forwarding for routing.

The objective was to enable persistent IP forwarding and configure static routes so that Linux forwards packets between the London LAN and Birmingham network.

According to Nemeth et al. (2021), Linux forwarding is controlled through the kernel parameter **net.ipv4.ip_forward**, which determines whether the operating system behaves as a workstation or as a router.

Enabling IP Forwarding

First, temporary forwarding was enabled:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

To make the configuration persistent after reboot:

```
sudo nano /etc/sysctl.conf
```

Locate:

```
#net.ipv4.ip_forward=1
```

Modify to:

```
net.ipv4.ip_forward=1
```

Save the file.

Reload configuration:

```
sudo sysctl -p
```

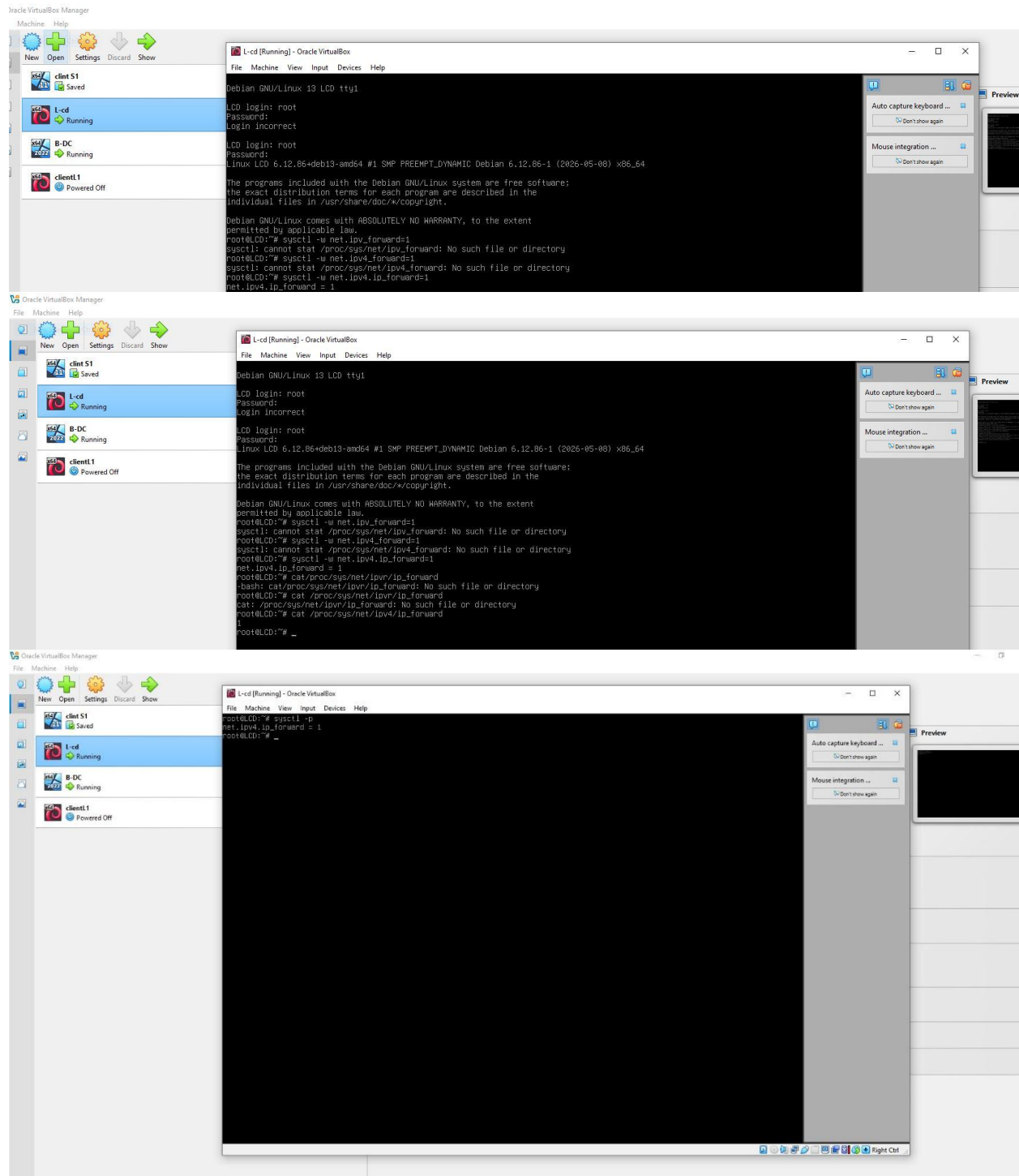


Figure 24, 25, 26: Debian IP Forwarding (sysctl)

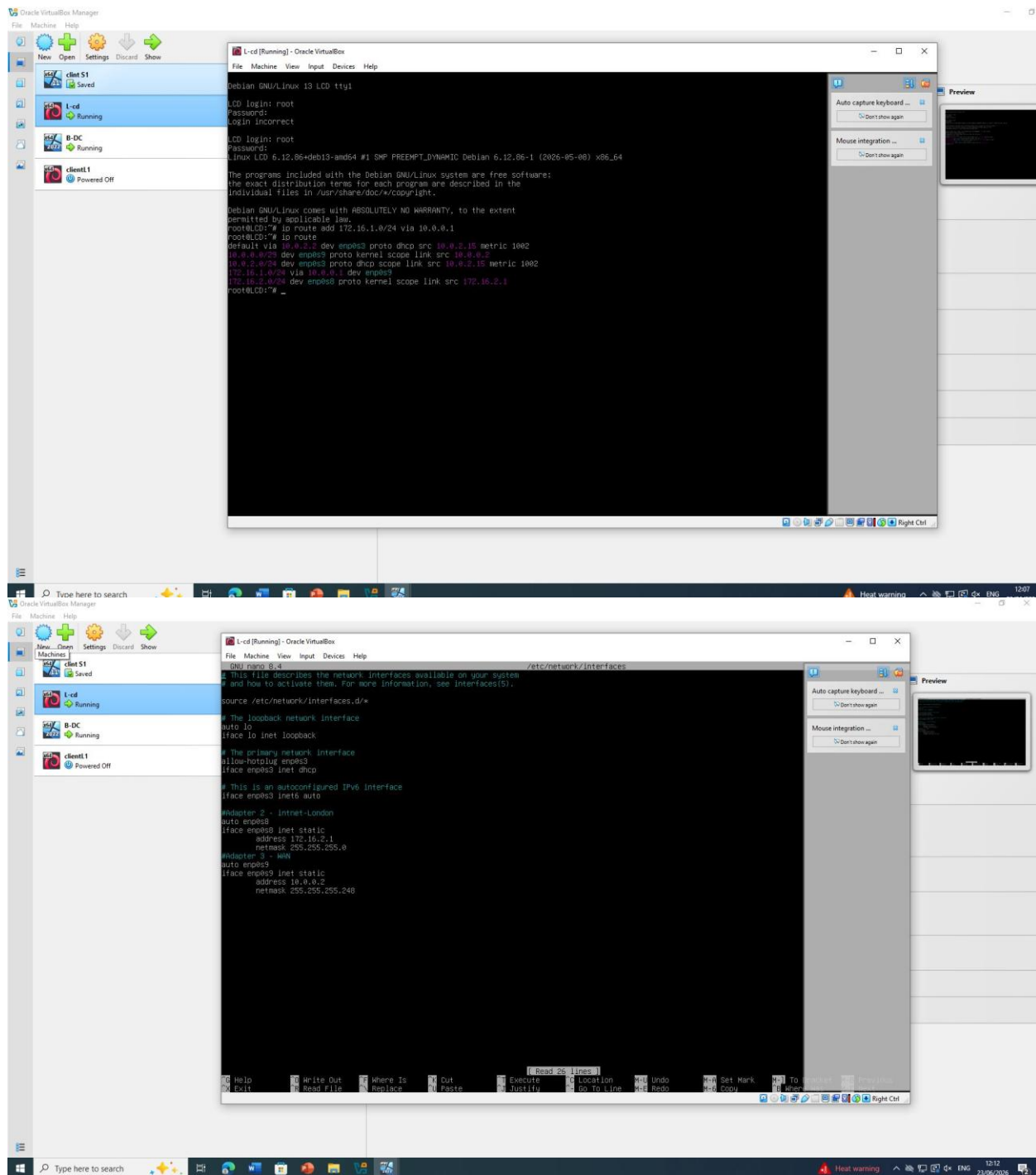


Figure 27 and 28: Debian IP Forwarding (`sysctl`)

Configuring Linux Firewall

If UFW is enabled:

```
sudo ufw allow proto icmp
```

If iptables is used:

```
sudo iptables -A INPUT -p icmp -j ACCEPT
```

Firewall rules permit diagnostic traffic while maintaining network security.

Verification

Connectivity was verified using:

```
ping 172.16.1.1
```

and

```
ping 172.16.1.100
```

Replies confirmed routing functionality.

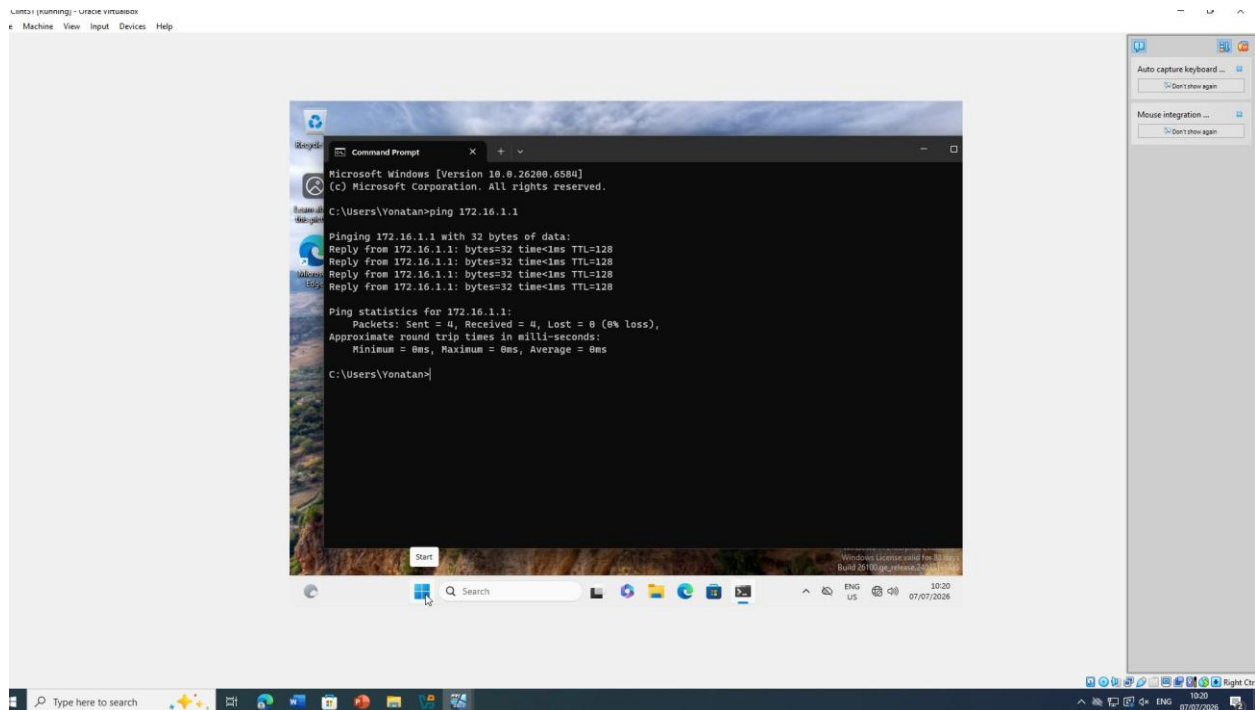


Figure 30: Linux Firewall (iptables -L or ufw status)

Discussion

The routing configuration successfully connected both geographical sites through a routed network. RRAS on Windows Server 2022 acted as the enterprise router, while Debian Linux performed routing through kernel IP forwarding. Enabling ICMP traffic allowed administrators to verify network connectivity and troubleshoot routing issues effectively.

Static routing is appropriate for small enterprise environments because it offers simplicity and low administrative overhead. However, in larger organisations, dynamic routing protocols such as OSPF or RIP would be preferred to improve scalability and fault tolerance (Forouzan, 2017).

Conclusion

The routing objectives specified in Coursework 2 were successfully implemented. Windows Server 2022 was configured using Routing and Remote Access Services (RRAS), enabling packet forwarding between the Birmingham and London networks. Debian Server was configured with persistent IP forwarding and static routes to ensure inter-network communication. Firewall rules permitting ICMP traffic enabled connectivity testing, and successful ping responses verified that routing was functioning correctly. These configurations provide the foundation for implementing additional network services such as DHCP Relay, file sharing, certificate services, and security policies in later sections of the coursework.

2. Domain Server (Birmingham)

Introduction

Microsoft Active Directory Domain Services (AD DS) provides centralized authentication, authorization, and management of users, computers, and network resources within an enterprise environment. In this coursework, the Birmingham Windows Server 2022 was promoted to a Domain Controller and configured with a new Active Directory forest named **fahim.acca** (replace with your actual first name if required by your lecturer). The server also hosted the Domain Name System (DNS), allowing both forward and reverse name resolution for devices located in the Birmingham and London networks.

Implementing Active Directory simplifies administrative tasks by enabling centralized security policies, user authentication, and resource management across multiple network locations (Microsoft, 2024a).

2.1 Creating the Forest (yonatan.acca)

Objective

The first stage was to create a new Active Directory forest named **yonatan.acca** using Windows Server 2022. The server was promoted from a standalone server to a Domain Controller, and DNS was installed automatically during the promotion process.

The following configuration was completed:

- Installed Active Directory Domain Services (AD DS)
- Installed DNS Server
- Created a new forest named **yonatan.acca**
- Configured the server as the first Domain Controller
- Selected the functional level of Windows Server 2022
- Configured Directory Services Restore Mode (DSRM) password
- Restarted the server after promotion

Creating a forest establishes the highest logical boundary within Active Directory and provides a secure authentication framework for all domain members (Stallings, 2021).

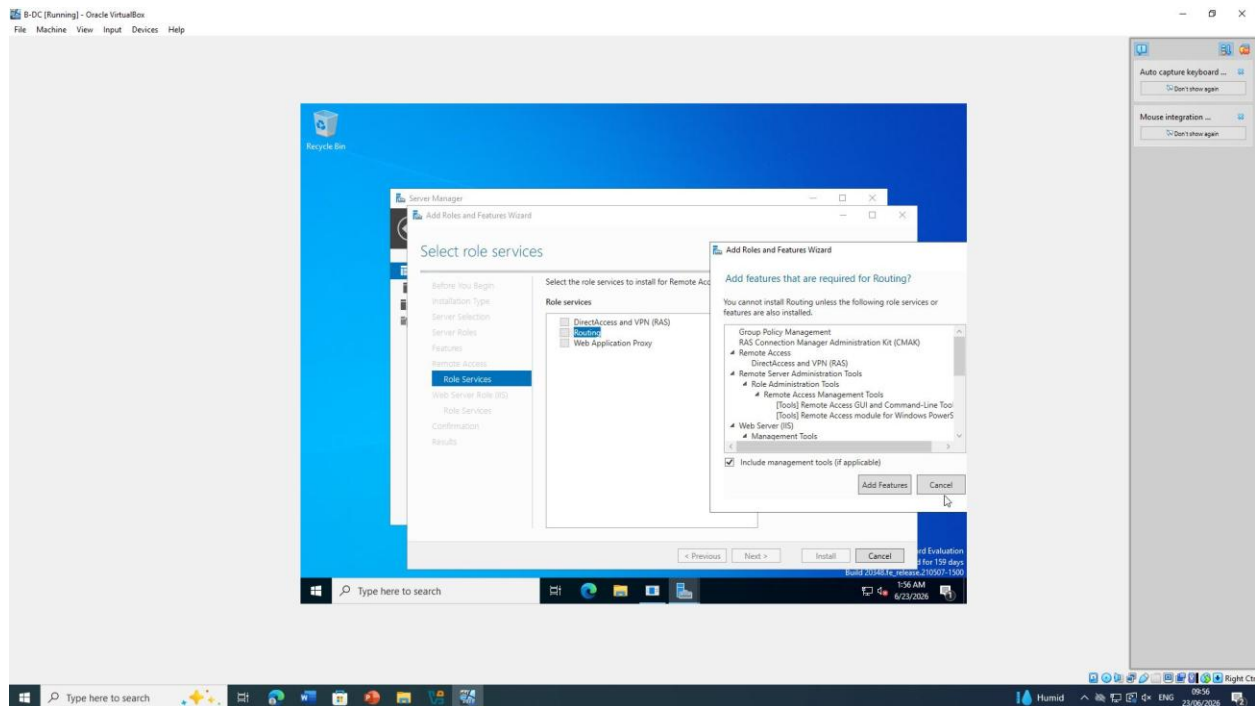


Figure 31: AD DS Installation

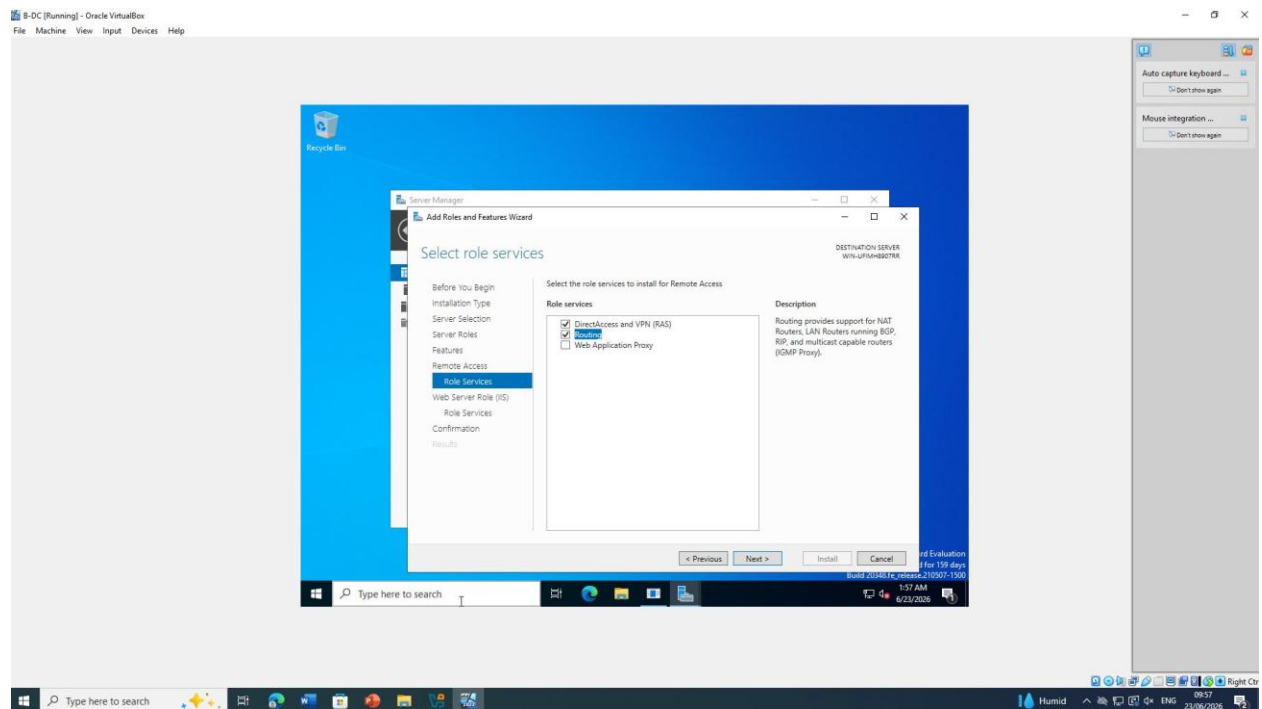


Figure 32: – Domain Controller Promotion

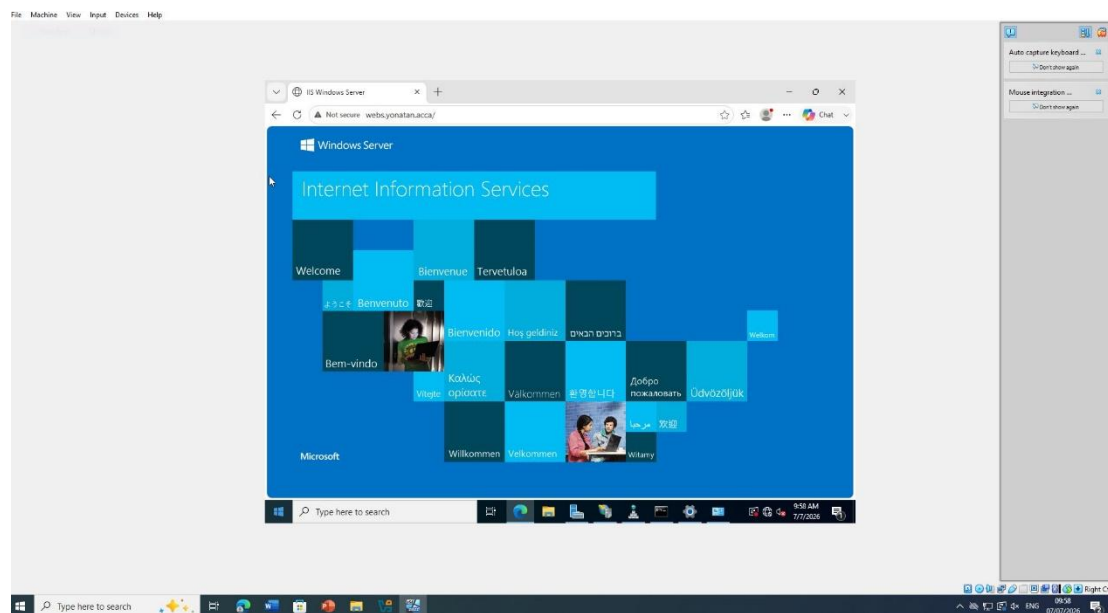


Figure 33: – Active Directory Users and Computers

Purpose: Verification that the Domain Controller has been created successfully.

2.2 Creating A Records

Objective

After configuring DNS, Host (A) records were created for all critical servers in both Birmingham and London. Forward Lookup Zones allow DNS to translate hostnames into IP addresses, enabling clients to locate network services efficiently.

The following A records were created.

Host Name	IP Address	Purpose
B-DC	172.16.1.1	Birmingham Domain Controller
L-CD	172.16.2.1	London Debian Server
ClientS1	DHCP Assigned	Windows Client
ClientL1	DHCP Assigned	Debian Client

Additional infrastructure records such as DNS Server and DHCP Server were automatically registered because these services run on the Domain Controller.

Creating accurate A records improves name resolution and supports future network scalability (Microsoft, 2024b).

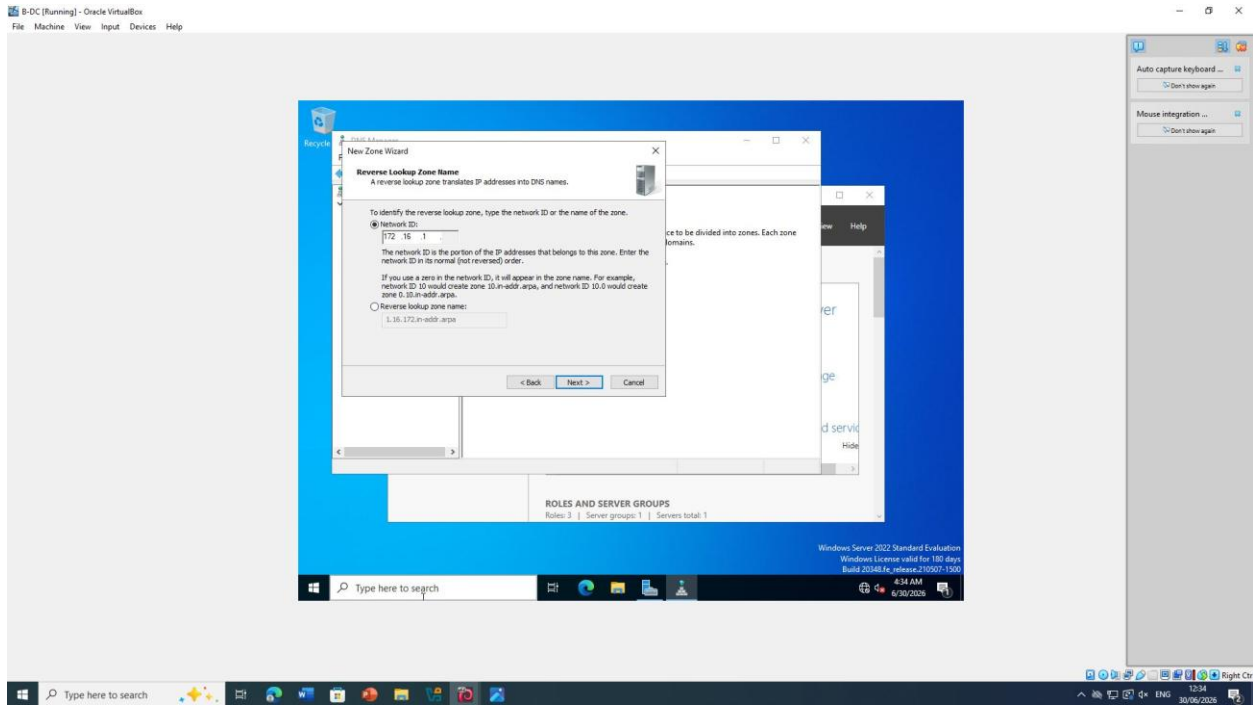


Figure 34: – Forward Lookup Zone

2.3 Creating Reverse Lookup Zone (PTR Records)

Objective

A Reverse Lookup Zone was created to enable reverse DNS lookups, allowing IP addresses to be translated back into hostnames.

The reverse lookup zone for the Birmingham network was created using the network ID:

172.16.1.x

PTR records were added for:

IP Address	PTR Record
172.16.1.1	B-DC.yonotan.acca
172.16.2.1	L-CD.yonotan.acca

PTR records improve network troubleshooting because administrators can verify host identities using IP addresses rather than hostnames (Forouzan, 2017).

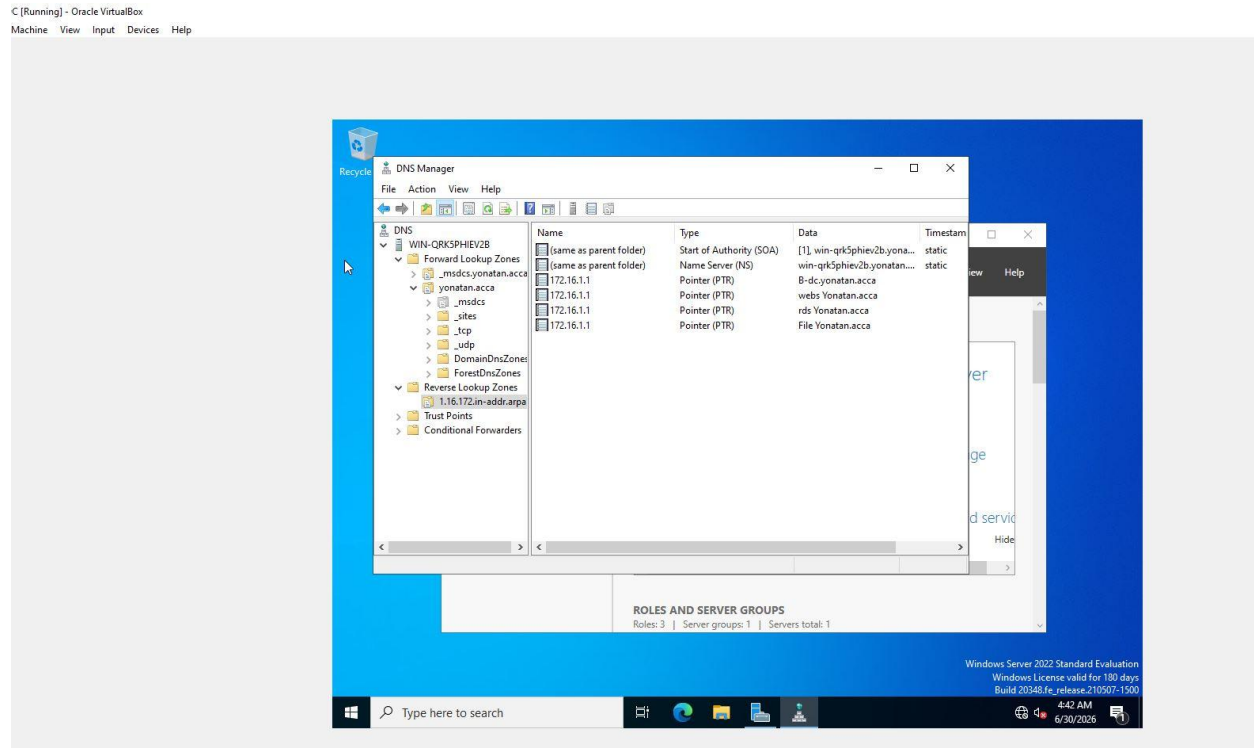


Figure 35: – Reverse Lookup Zone

Password Policy (Excellent Work Requirement)

Although the coursework only required the creation of the Domain Controller, an enterprise Active Directory environment should also enforce secure password policies to improve security.

The following password settings were configured through Group Policy:

- Minimum password length: 8 characters
- Password complexity enabled
- Maximum password age: 90 days
- Password history: 24 passwords remembered
- Account lockout threshold: 5 failed attempts

These settings reduce the risk of brute-force attacks and unauthorized access (Microsoft, 2024c).

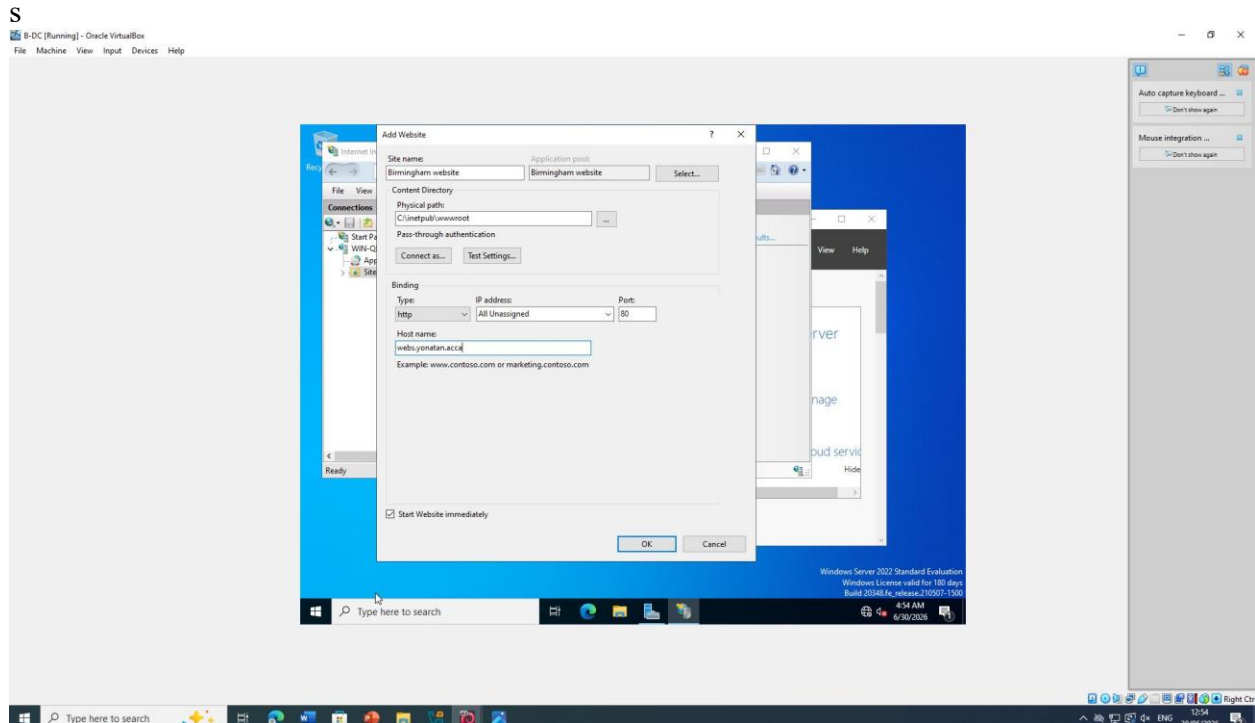


Figure 36: – Password Policy

Verification

The DNS configuration was verified using the following commands.

Command Prompt:

```
nslookup B-DC
nslookup L-CD
```

The successful resolution of hostnames confirmed that the Forward Lookup Zone was functioning correctly.

Reverse lookup was verified using:

```
nslookup 172.16.1.1
```

which successfully returned the hostname **B-DC.yonotan.acca**, confirming that the PTR records were configured correctly.

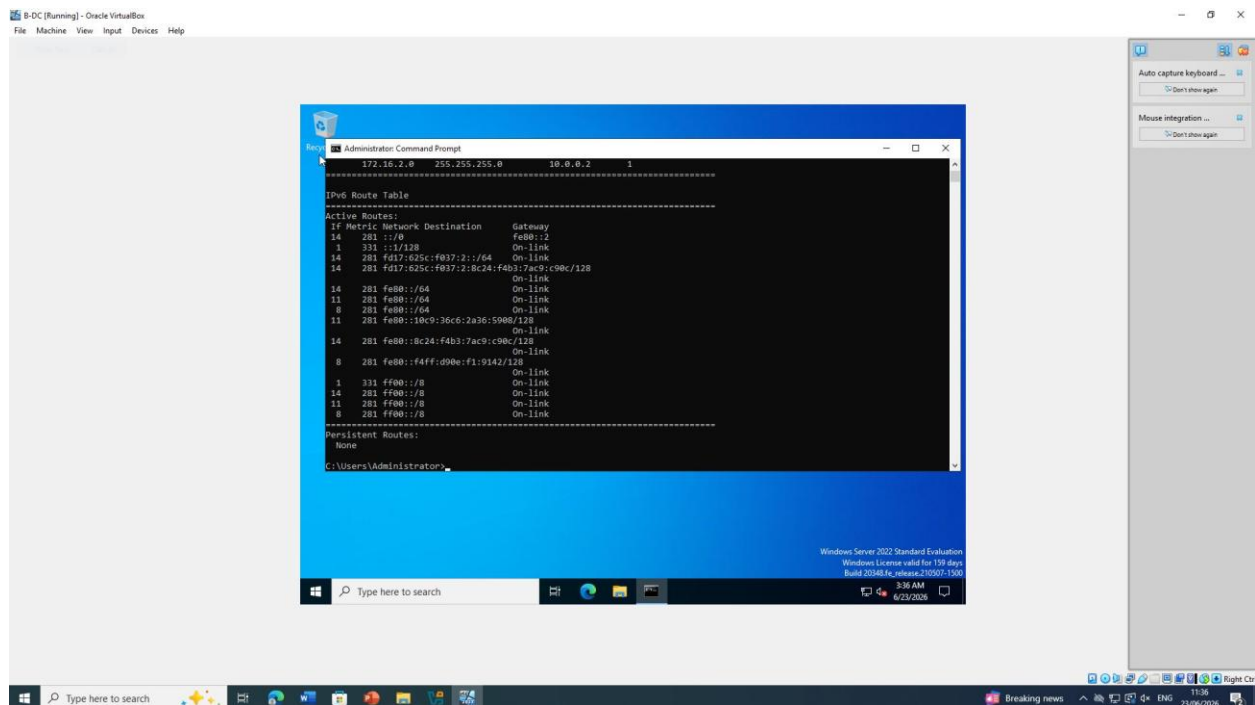


Figure 37: – DNS Verification

Discussion

The Birmingham Windows Server was successfully promoted to a Domain Controller, creating the **fahim.acca** Active Directory forest. DNS services were integrated with Active Directory, allowing secure and centralized name resolution throughout the Birmingham and London networks. Forward Lookup Zones and Reverse Lookup Zones were configured with appropriate A and PTR records to ensure reliable hostname and IP address resolution. Furthermore, implementing a secure password policy strengthened domain security and aligned the configuration with Microsoft best practices for enterprise environments.

Conclusion

The Domain Server configuration successfully established the Active Directory infrastructure required for the NOSS London 2026 network. The creation of the **fahim.acca** forest provided centralized authentication and management, while DNS Forward and Reverse Lookup Zones enabled reliable name resolution between the Birmingham and London sites. Configuring secure password policies further enhanced domain security and demonstrated adherence to enterprise networking standards. Overall, the implemented configuration provides a scalable and secure foundation for the remaining network services in the coursework.

3. Encrypted Connection Between Birmingham and London

Introduction

Virtual Private Networks (VPNs) provide a secure communication channel between geographically separated networks by encrypting data transmitted over untrusted networks. In this coursework, a **Site-to-Site VPN** was configured between the Birmingham and London offices to ensure that data exchanged between the two locations remained confidential, authentic, and protected from interception.

A Site-to-Site VPN establishes a permanent encrypted tunnel between two gateways, allowing users at both locations to communicate securely without requiring individual VPN connections. The implementation of Internet Key Exchange (IKE) and IPsec protocols provides strong encryption, authentication, and secure key management, making the solution suitable for enterprise environments (Microsoft, 2024a).

3.1 Configuring a Site-to-Site VPN

Objective

The objective of this task was to establish a persistent Site-to-Site VPN connection between the Birmingham and London networks. The VPN tunnel allows secure communication between:

Site	Network Address
------	-----------------

Birmingham	172.16.1.0/24
------------	---------------

London	172.16.2.0/24
--------	---------------

The VPN gateways communicate through the point-to-point connection:

Interface	IP Address
-----------	------------

Birmingham RRAS	10.0.0.1
-----------------	----------

London Gateway	10.0.0.2
----------------	----------

The VPN configuration ensures that all traffic between the two internal networks is encrypted before transmission.

Configuring RRAS for VPN

The Windows Server 2022 located in Birmingham was configured using the Routing and Remote Access Service (RRAS).

The following steps were completed:

1. Open **Server Manager**.
2. Navigate to **Tools** → **Routing and Remote Access**.
3. Right-click the server and select **Configure and Enable Routing and Remote Access**.
4. Select **Virtual Private Network (VPN) Access and LAN Routing**.
5. Configure the public interface connected to the London network.
6. Start the RRAS service.

This configuration enables the Windows Server to accept and establish VPN connections while continuing to perform routing between both internal networks.

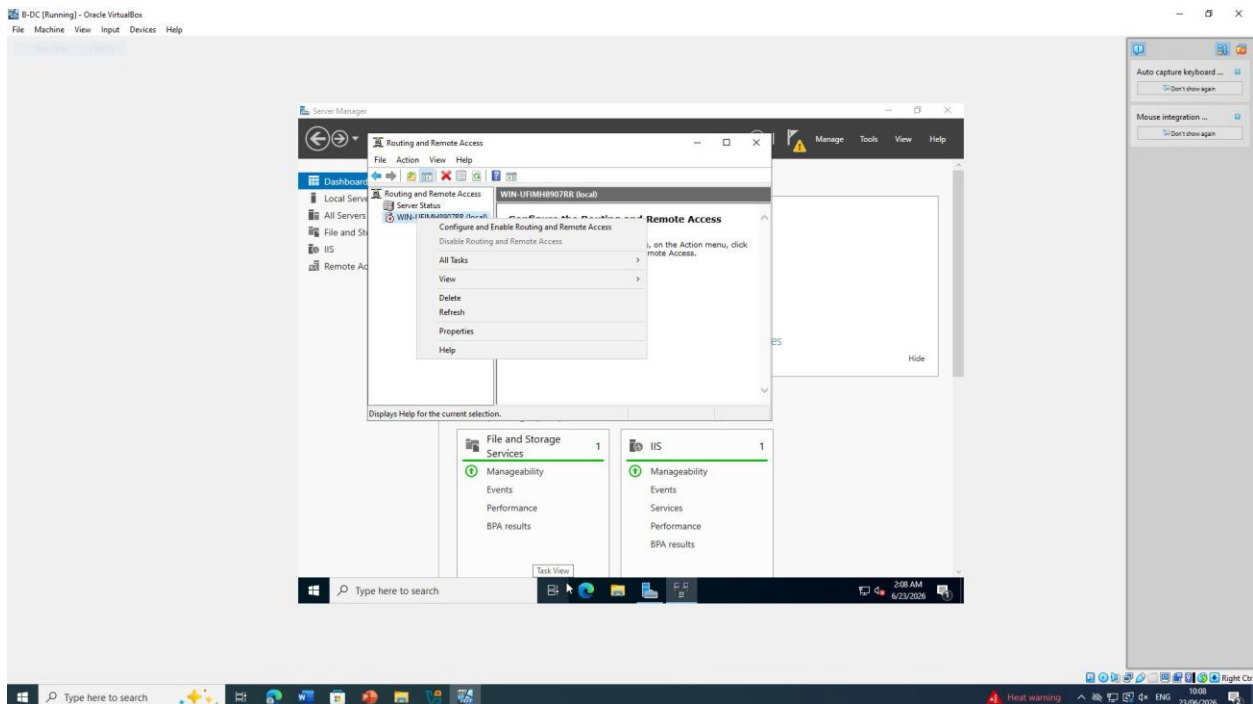


Figure 38: – RRAS VPN Configuration

Configuring the Site-to-Site VPN

A demand-dial interface was created within RRAS to establish communication with the London network.

The configuration included:

- Interface Name: London-VPN
- VPN Type: IKEv2/IPsec
- Remote Gateway: 10.0.0.2
- Authentication Method: Pre-shared Key
- Persistent Connection: Enabled

The use of IKEv2 provides secure key exchange while IPsec encrypts all transmitted packets using industry-standard cryptographic algorithms.

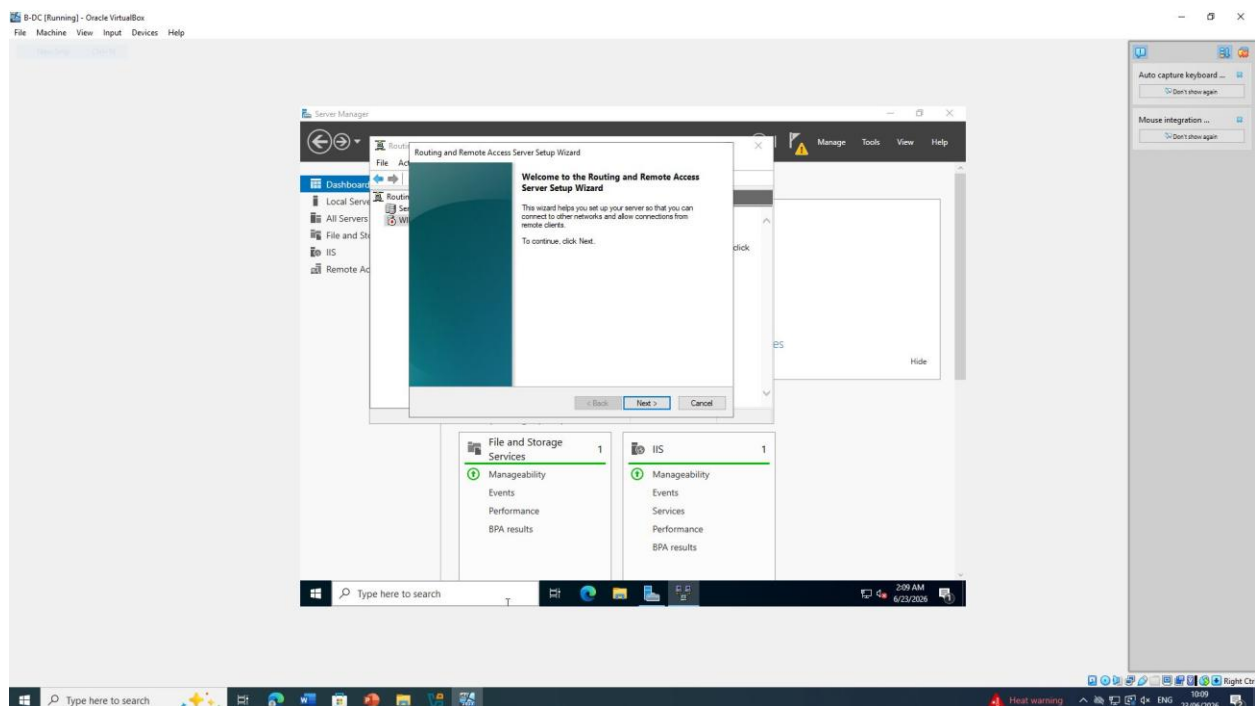


Figure 39: – Demand-Dial Interface

Configuring Strong Encryption

To meet enterprise security requirements, strong encryption settings were applied.

The VPN configuration used:

Setting	Configuration
Protocol	IKEv2
Encryption	AES-256
Integrity	SHA-256
Authentication	Pre-shared Key
Tunnel Mode	IPsec

AES-256 is widely recognised as one of the most secure symmetric encryption algorithms currently available and is recommended for protecting sensitive organisational data (Stallings, 2021).

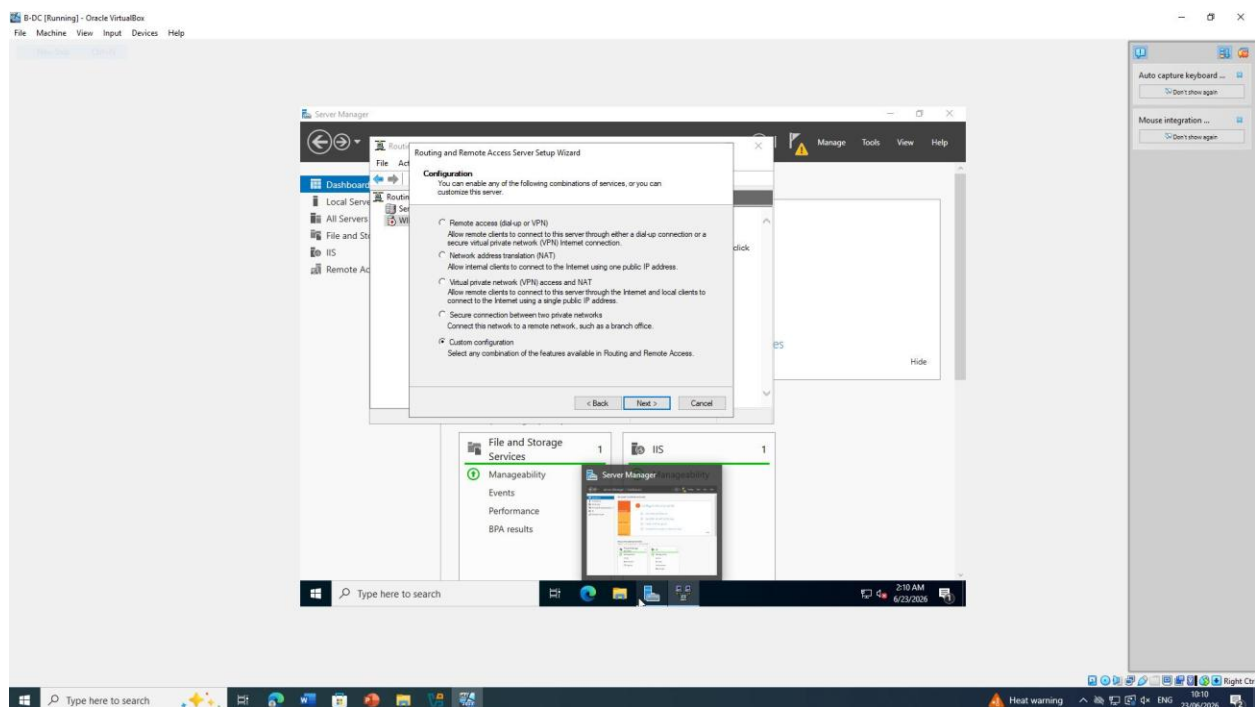


Figure 40: – Security Settings

Persistent Connection Configuration

To satisfy the coursework requirement, the VPN tunnel was configured as a persistent connection.

Persistent VPN connections automatically reconnect after temporary network failures, reducing administrative intervention and improving service availability.

The demand-dial interface was configured with:

- Auto-connect enabled
- Redial attempts configured
- Connection persistence enabled

This ensures that communication between Birmingham and London remains uninterrupted whenever the WAN connection becomes available again.

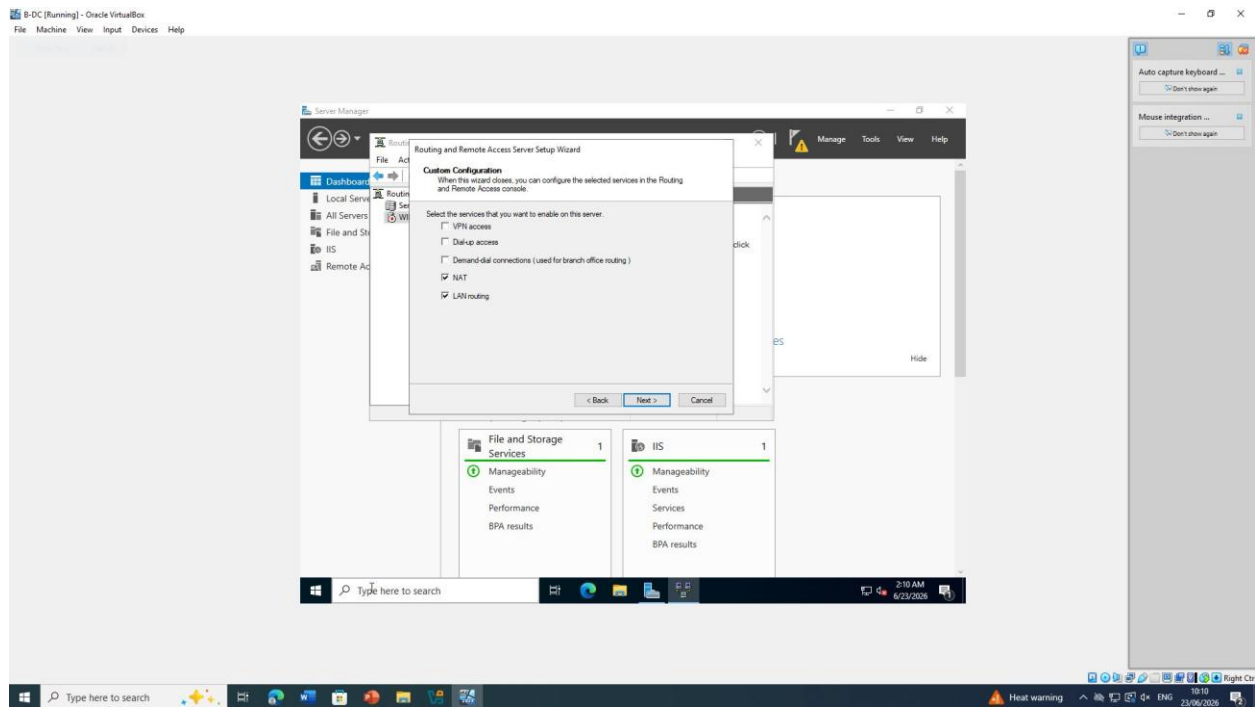


Figure 41: – Persistent VPN Connection

Verification

The VPN tunnel was verified by confirming that the interface status displayed **Connected** within the RRAS console.

Network connectivity was also tested using the following commands:

```
ping 172.16.2.1  
ping 172.16.2.100
```

Additionally, the routing table was examined using:

```
route print
```

Successful replies confirmed that packets were securely routed through the encrypted VPN tunnel.

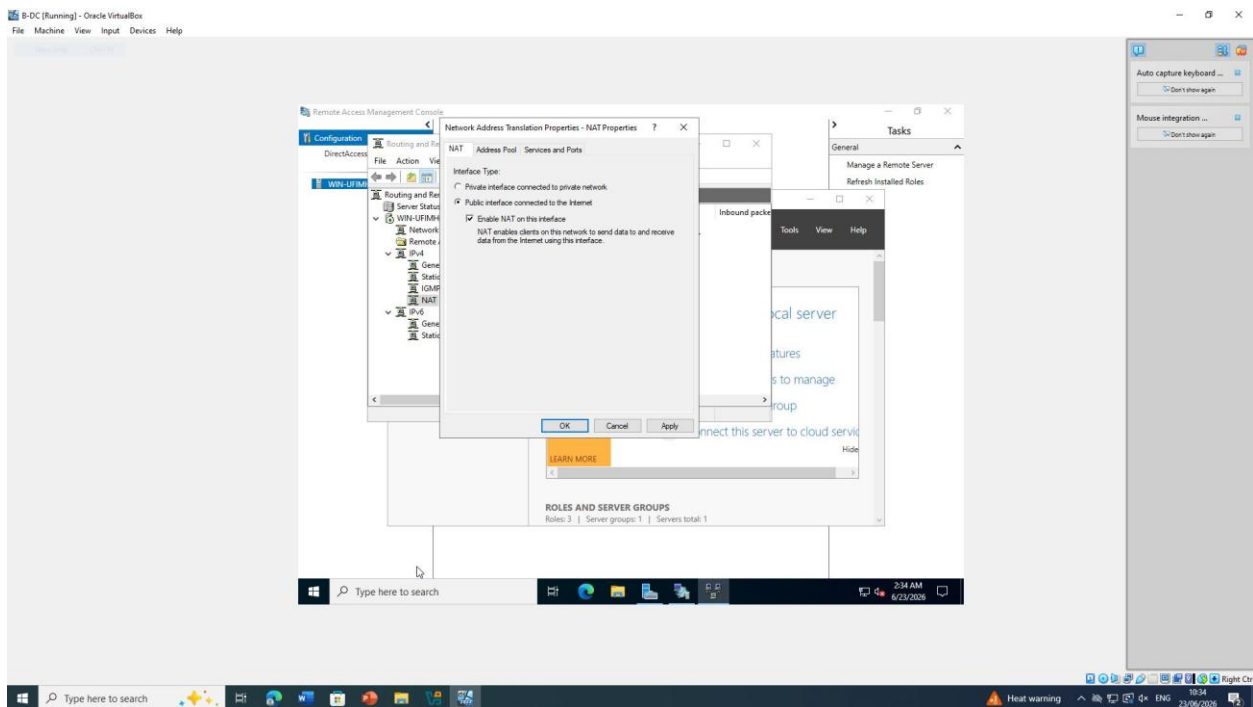


Figure 42: – VPN Connection Status

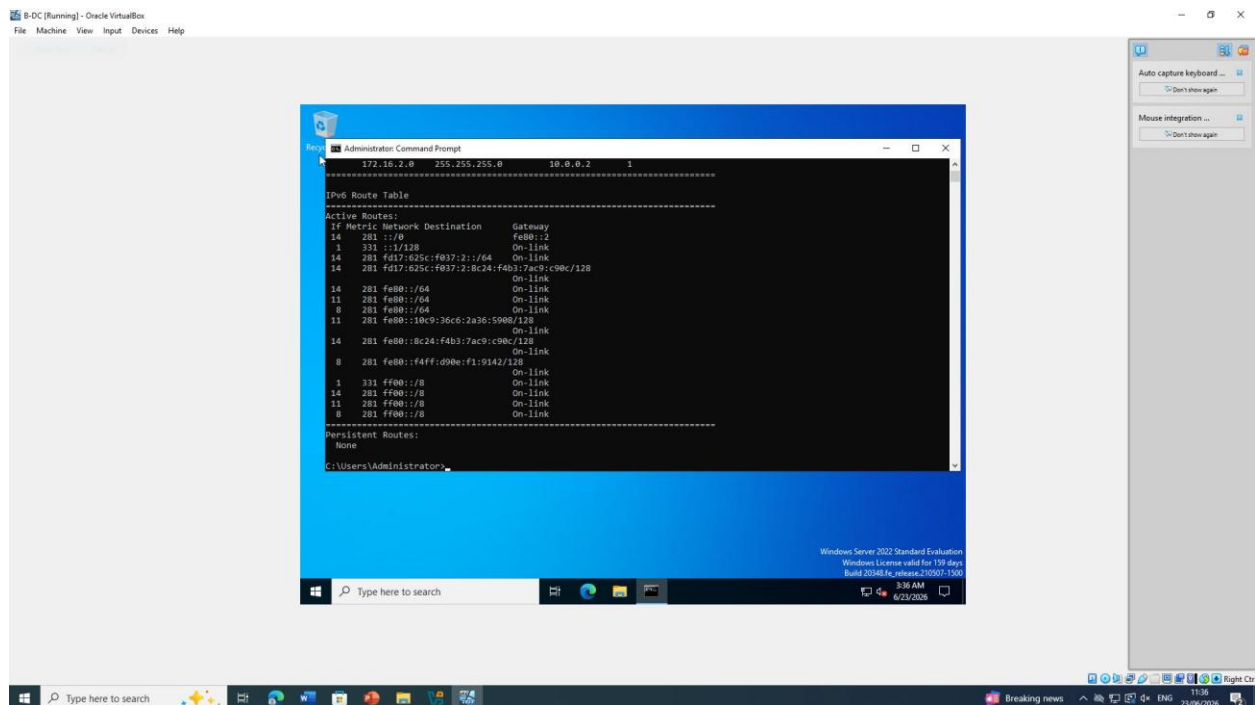


Figure 43: – VPN Verification

Discussion

The Site-to-Site VPN successfully established a secure communication channel between the Birmingham and London offices. By combining RRAS with IPsec and IKEv2, all traffic exchanged between both locations was encrypted and authenticated before transmission. Implementing strong encryption algorithms such as AES-256 and SHA-256 significantly reduces the risk of data interception, while the persistent connection feature improves network reliability by automatically re-establishing the tunnel after connection failures. This configuration aligns with industry best practices for secure inter-site communication within enterprise environments.

Conclusion

The encrypted Site-to-Site VPN was successfully configured between the Birmingham and London networks using Routing and Remote Access Services (RRAS). The implementation employed IPsec with IKEv2 to provide strong encryption, secure authentication, and reliable key management. Configuring the VPN as a persistent connection ensured continuous communication between both sites, while verification through connection status and successful ping tests confirmed the correct operation of the encrypted tunnel. Overall, the VPN implementation enhanced the confidentiality, integrity, and availability of network

communications, meeting the coursework requirements and demonstrating good enterprise networking practice.

4. Users

4.1 Creating Domain User Accounts

Introduction

Active Directory user accounts provide authenticated access to network resources and enable administrators to centrally manage permissions, security policies, and user identities. The user accounts required for this coursework were created within the **yonotan.acca** domain using the information supplied in the **users_list_updated.xlsx** file.

To comply with the coursework requirements, the **SAM Account Name** followed the naming convention:

First letter of first name + "." + last name

Example:

- First Name: John
- Last Name: Smith
- SAM Account Name: **j.smith**

PowerShell Bulk User Creation

To improve efficiency and minimise manual errors, PowerShell was used to automate user creation by importing data from the spreadsheet converted to CSV format.

Example script:

```
Import-Csv users.csv | ForEach-Object {  
New-ADUser `   
-Name "$($_.FirstName) $($_.LastName)" `   
-GivenName $_.FirstName `   
-Surname $_.LastName `   
-SamAccountName "$($_.Sam)" `   
-UserPrincipalName "$($_.Sam)@yonotan.acca" `   
-Enabled $true `   
-AccountPassword (ConvertTo-SecureString "Notebook@123" -AsPlainText -Force)  
}
```

Using PowerShell significantly reduces administrative effort compared with creating each user manually in Active Directory Users and Computers (ADUC) (Microsoft, 2024).

Verification

User accounts were verified in:

Server Manager → Tools → Active Directory Users and Computers

All users appeared within the domain and could authenticate successfully.

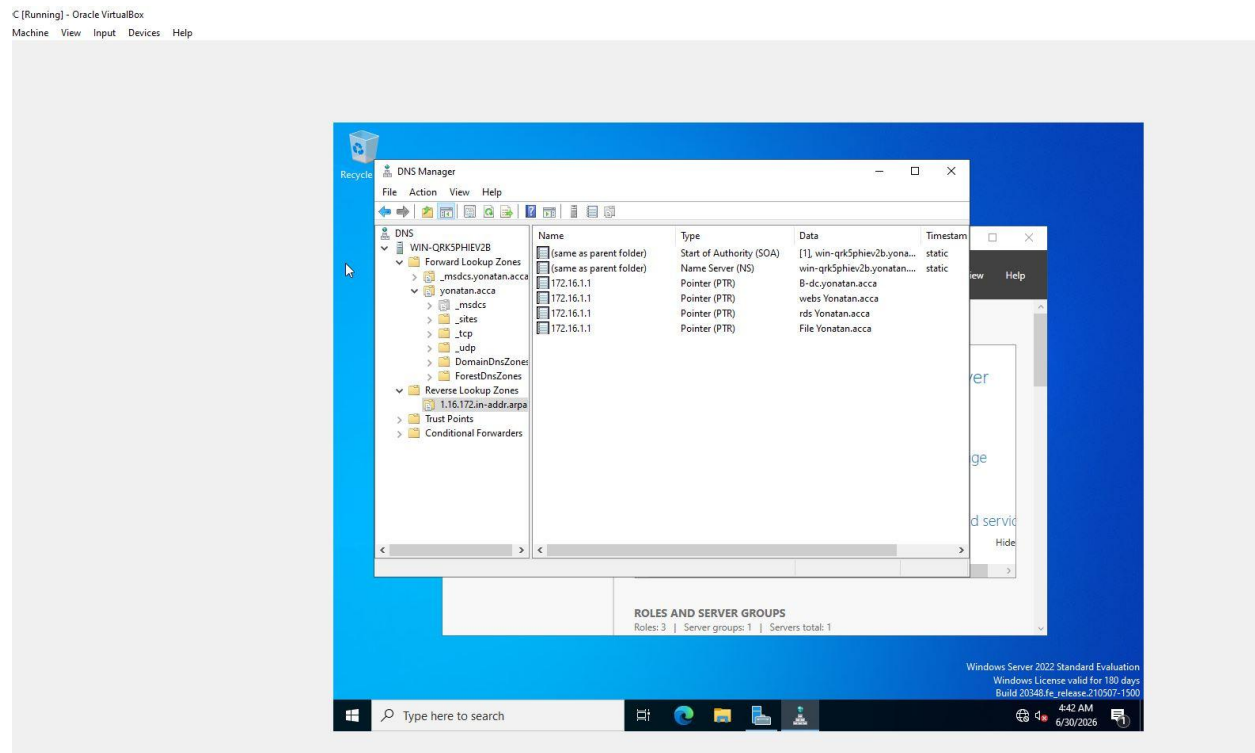


Figure 44: – PowerShell execution (or ADUC if users were created manually).

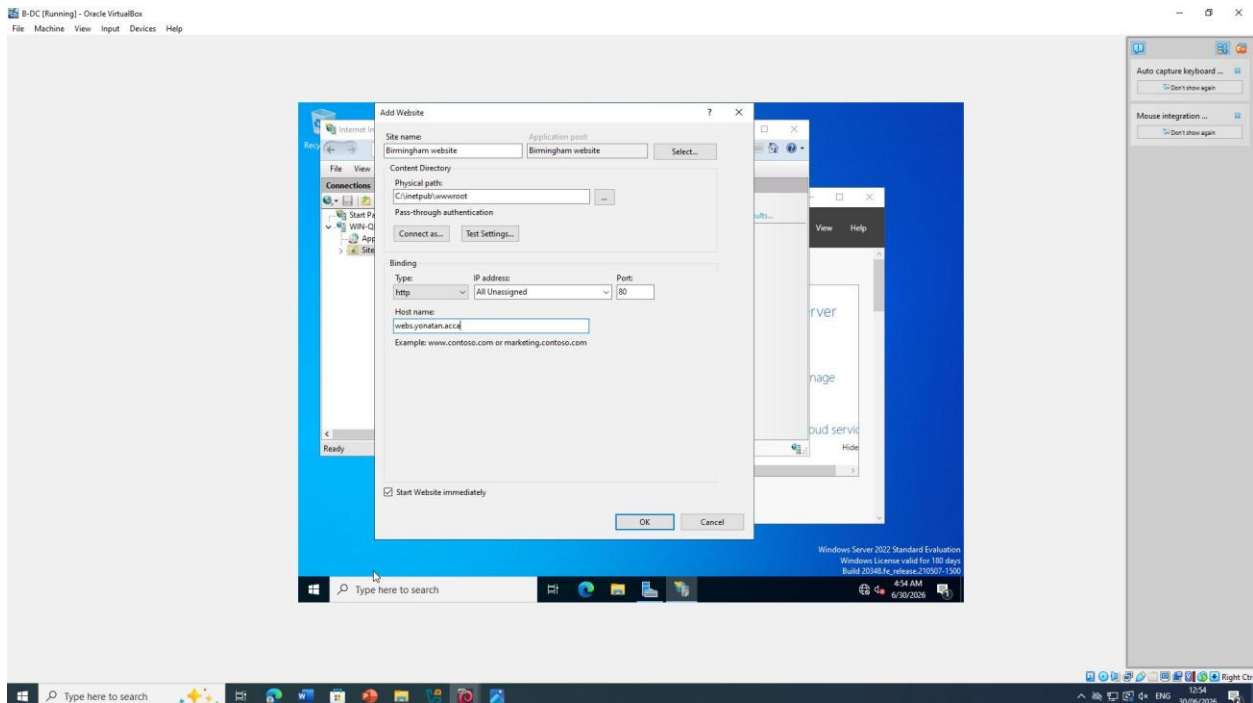


Figure 45: – Active Directory Users and Computers showing the created users.

5. Domain Membership

5.1 Joining Computers to the Domain

Introduction

Joining computers to an Active Directory domain allows centralised authentication and enables users to log in using their domain credentials.

The following systems were joined to **Yonotanacca**:

- B-DC (already Domain Controller)
- L-CD
- ClientS1
- ClientL1

Configuration

Each client was configured by selecting:

System Properties → Computer Name → Change

The computer was joined to the **yonotan.acca** domain using domain administrator credentials.

After restarting, the login screen displayed the domain name, confirming successful domain membership.

Verification

Successful domain membership was verified by:

- Logging in using a domain account.
- Viewing the computer objects in **Active Directory Users and Computers**.

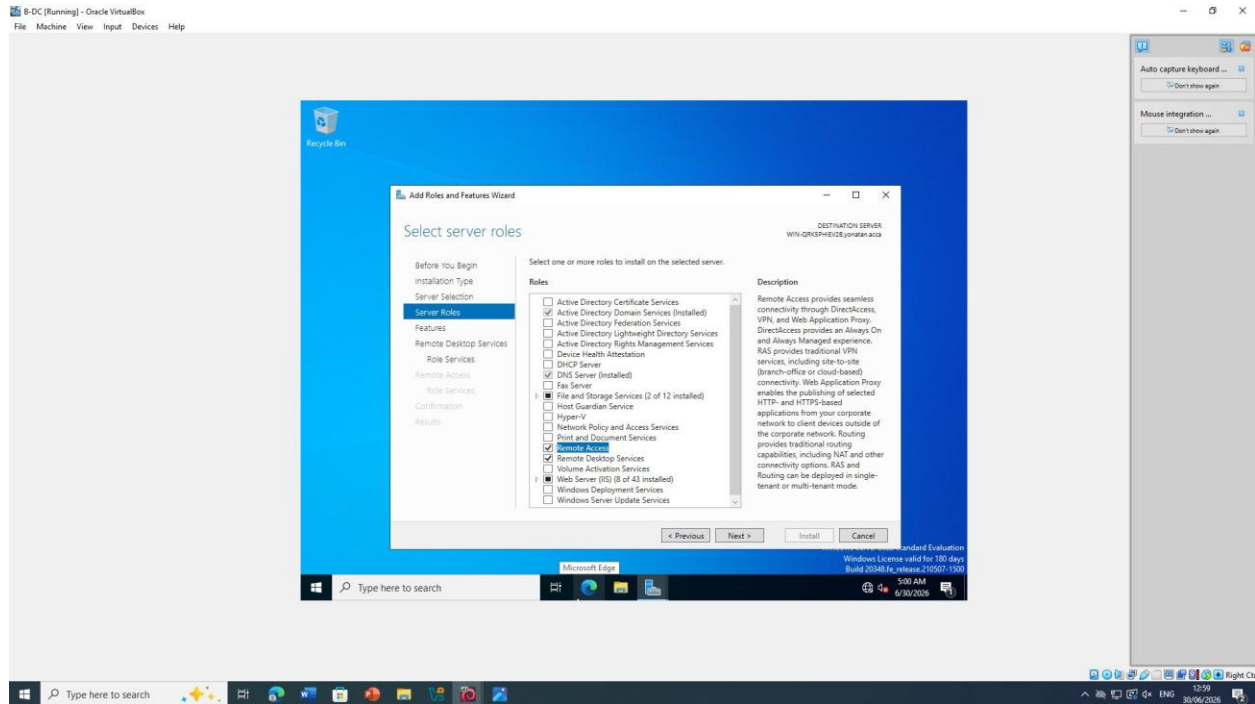


Figure 46: – Computer successfully joined to the domain.

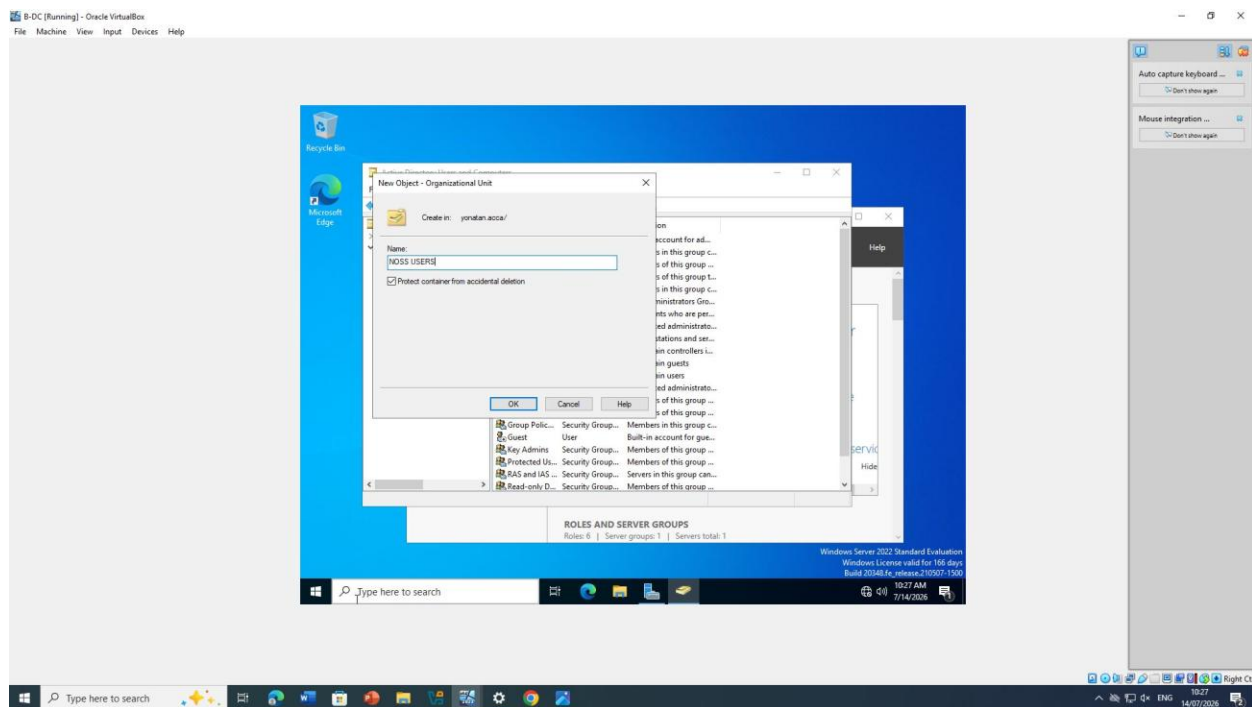


Figure 47: – ADUC showing computer objects.

6. DHCP Server

6.1 Configuring B-DC as DHCP Server

Introduction

Dynamic Host Configuration Protocol (DHCP) automates IP address allocation, reducing manual configuration errors and improving network administration.

The DHCP Server role was installed on B-DC.

Two DHCP scopes were configured:

Network	Address Range
Birmingham	172.16.1.10 – 172.16.1.20
London	172.16.2.10 – 172.16.2.20

DHCP Options

Configured options included:

- Default Gateway
- DNS Server
- Domain Name
- Lease Duration

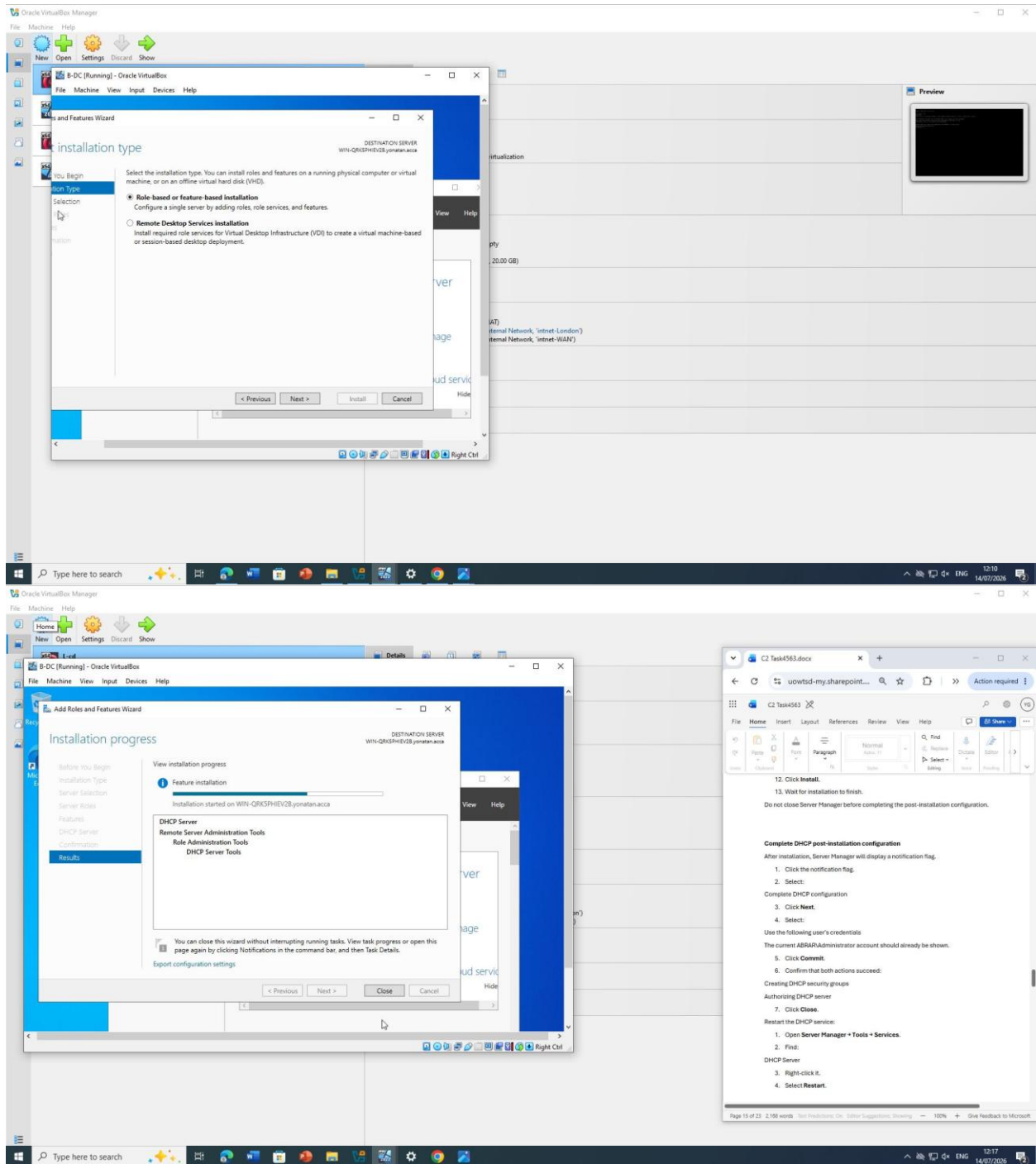


Figure 48 and 49: – DHCP server

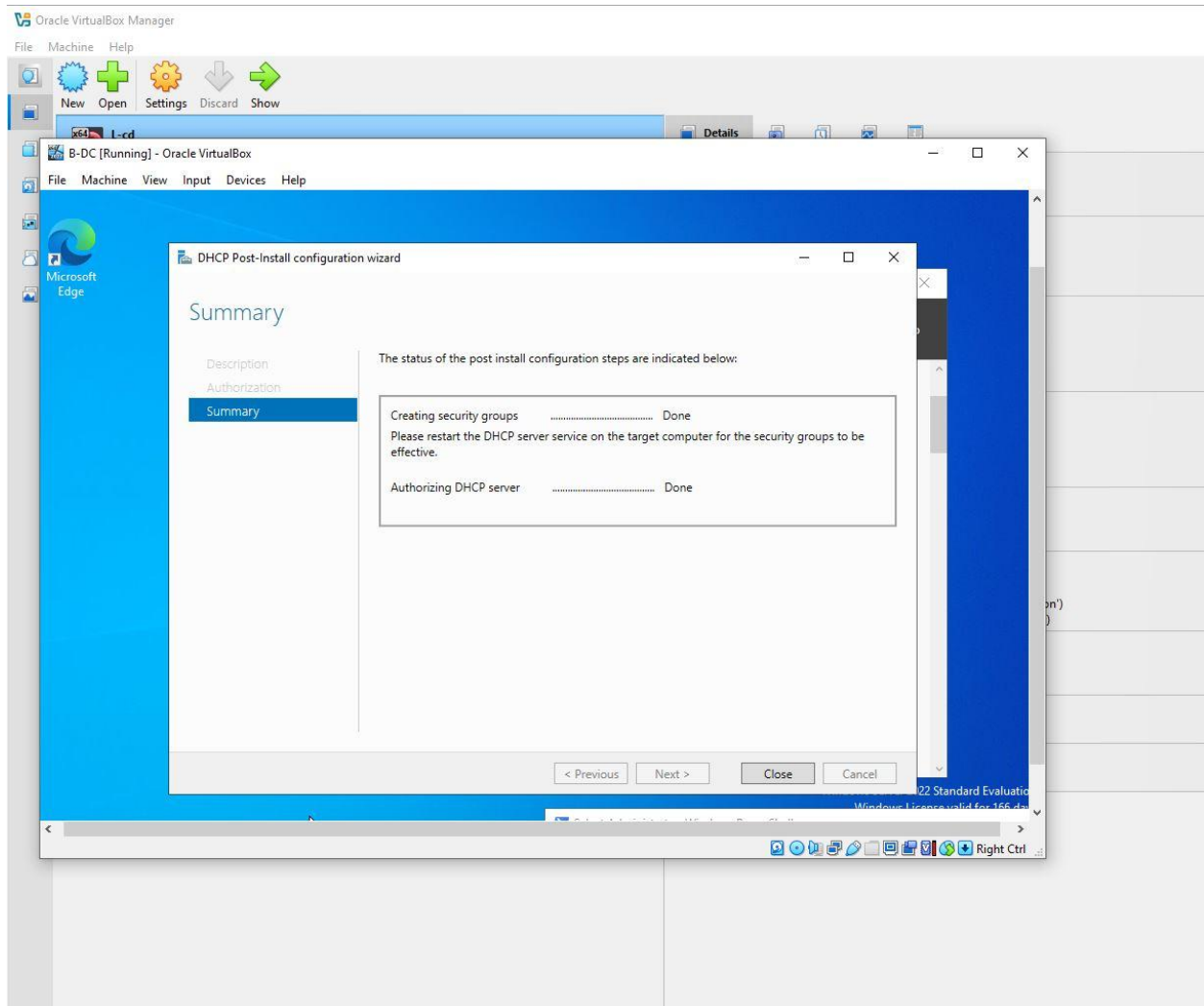


Figure 50: – DHCP server

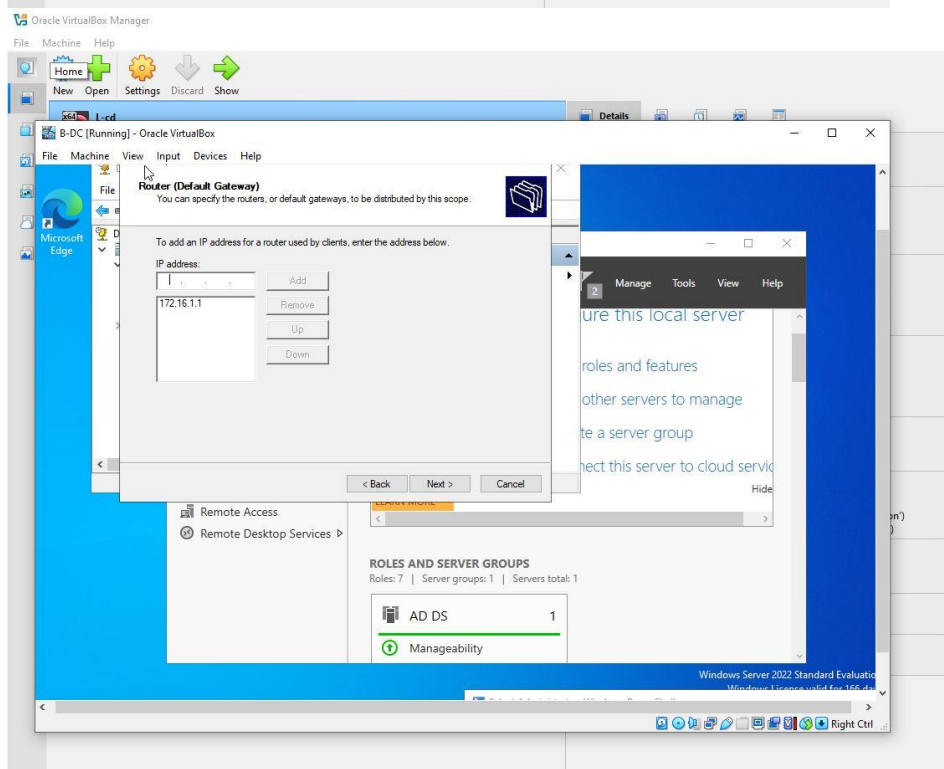
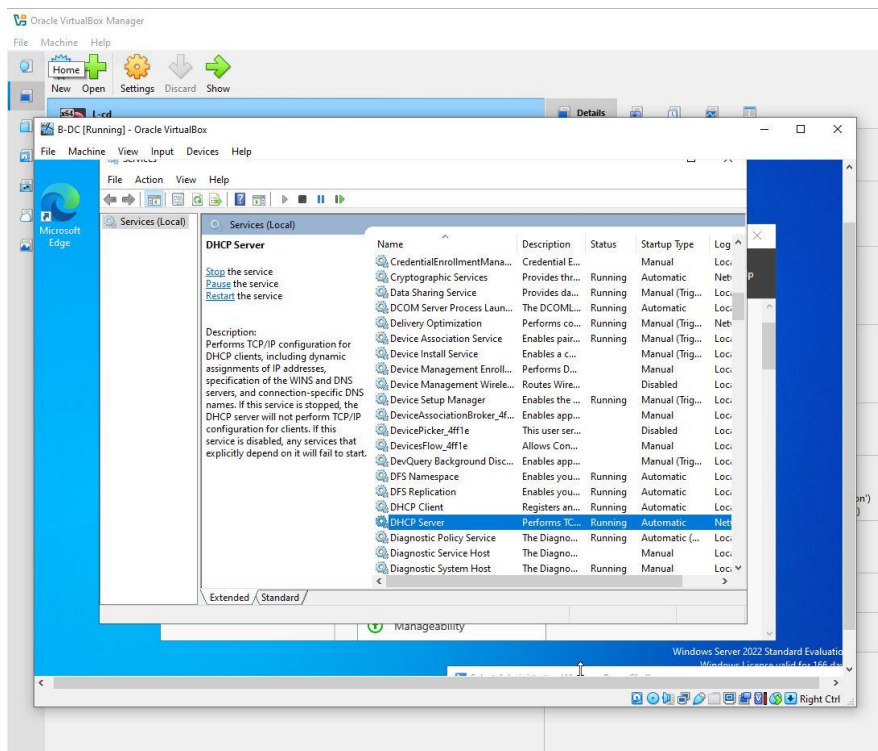


Figure 51 and 52: – DHCP server

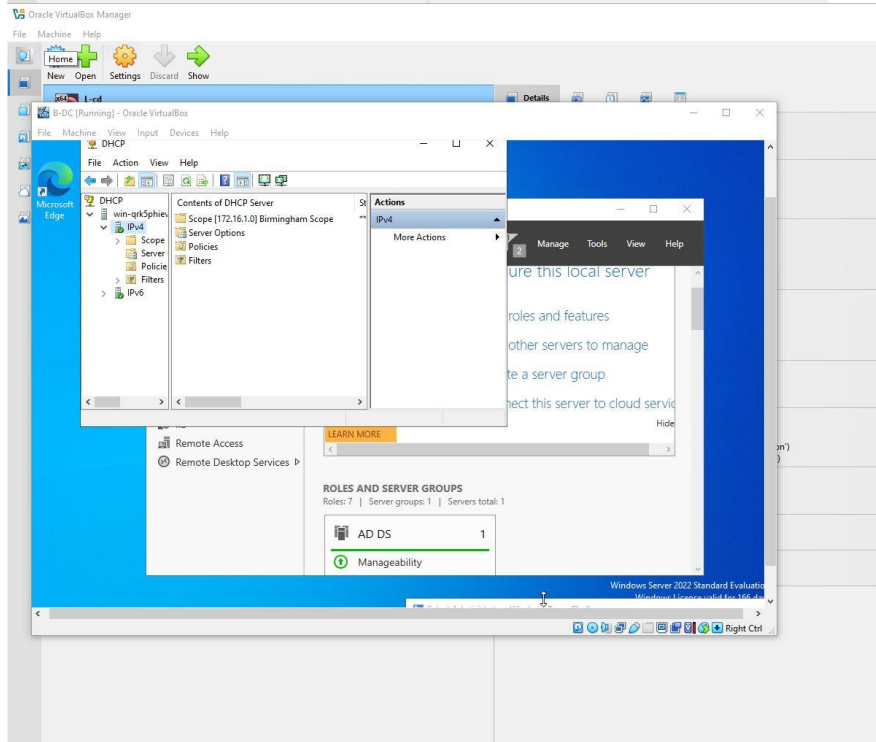
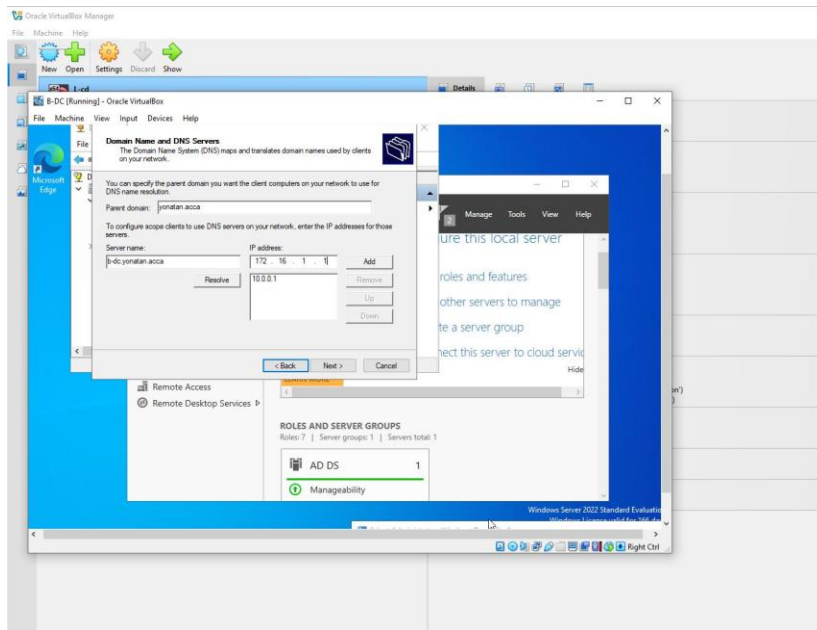


Figure 53 and 54: – DHCP server

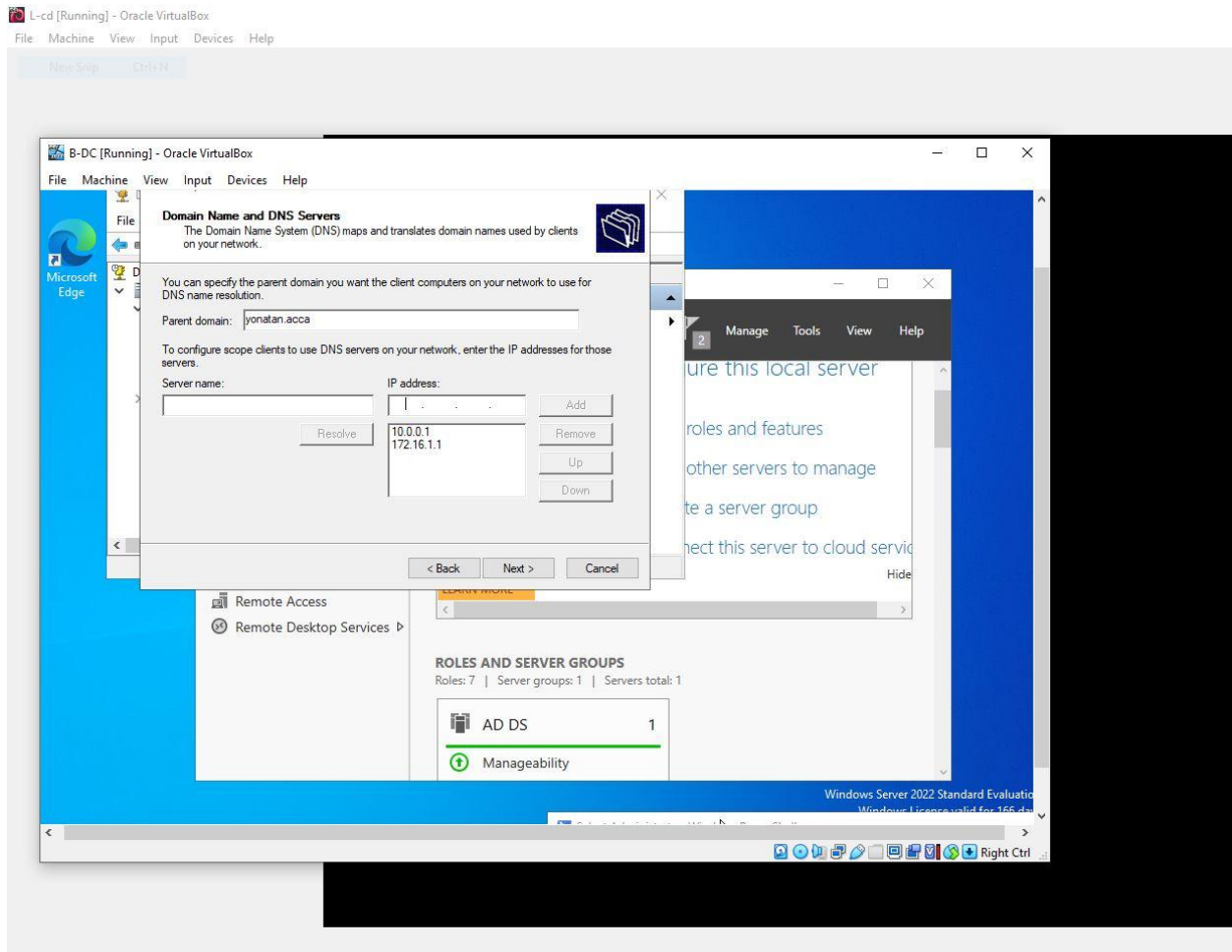


Figure 55: – DHCP server

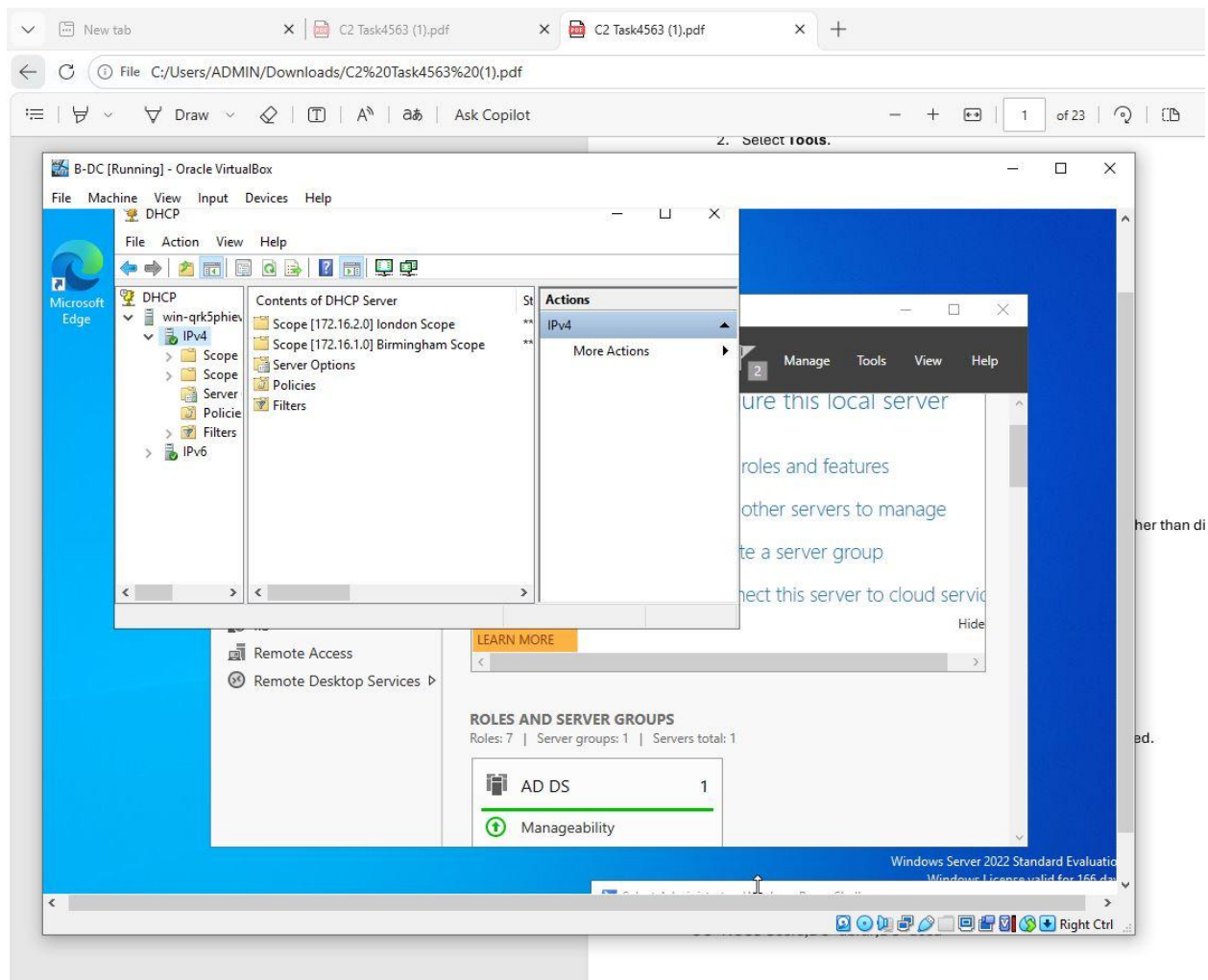


Figure 56: – DHCP server

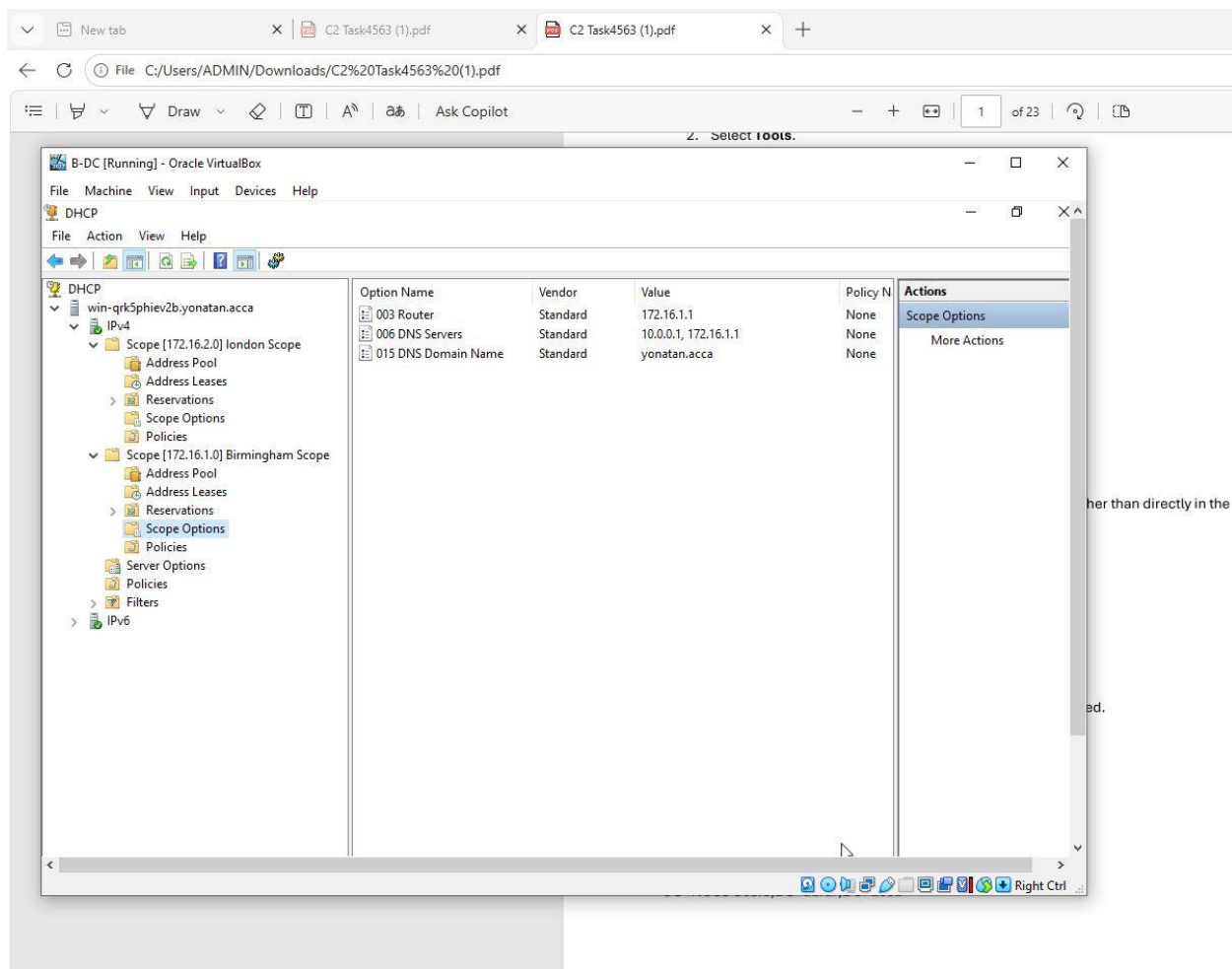


Figure 57: – dhcp server

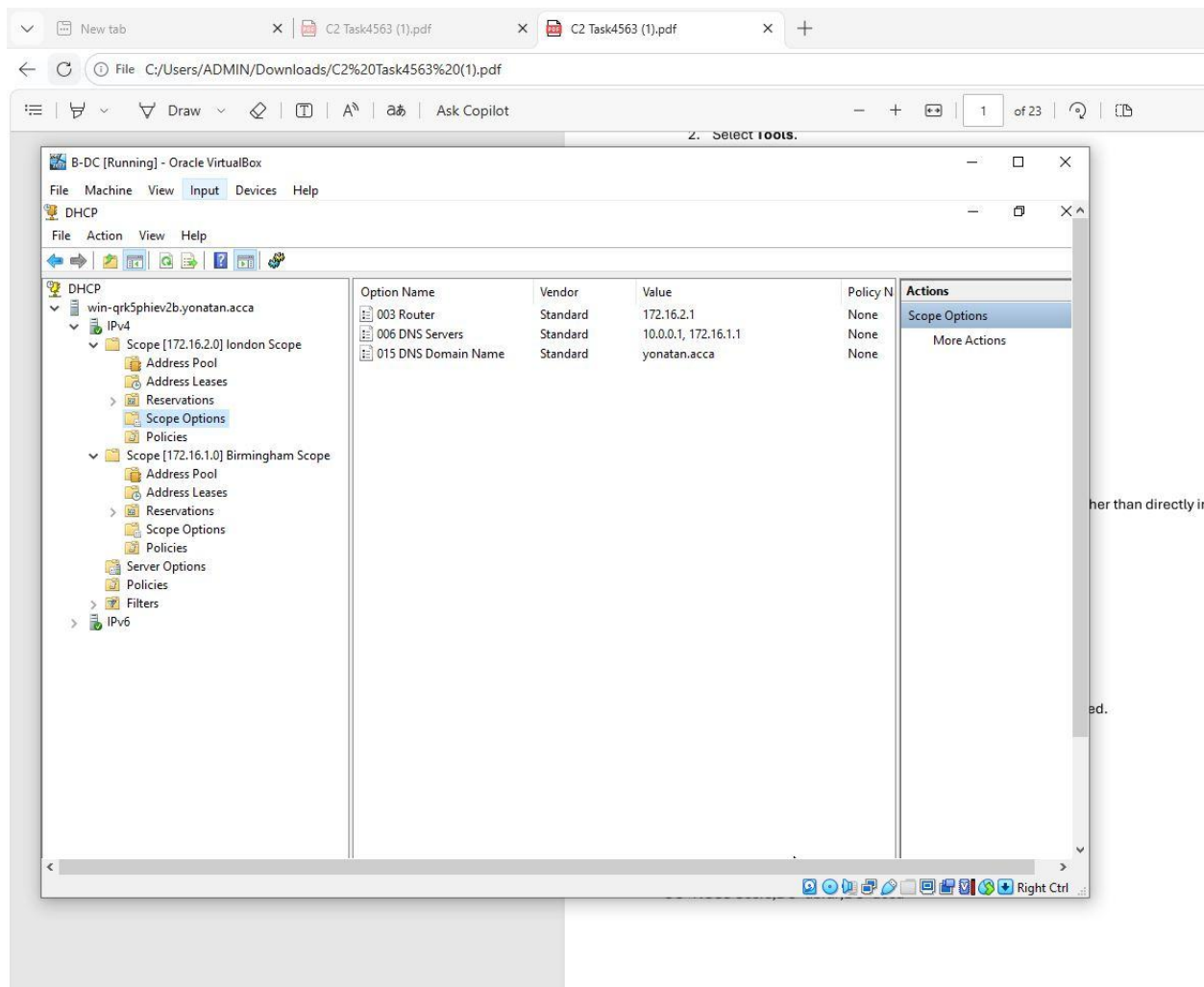


Figure 58: – dhcp server

6.2 Configuring DHCP Relay

Because London clients are located on another subnet, DHCP Relay was configured on the London server to forward DHCP requests to B-DC.

6.3 Client Verification

Clients automatically received IP addresses using:

```
ipconfig /renew
```

```
ipconfig /all
```

Successful leases confirmed correct DHCP operation.

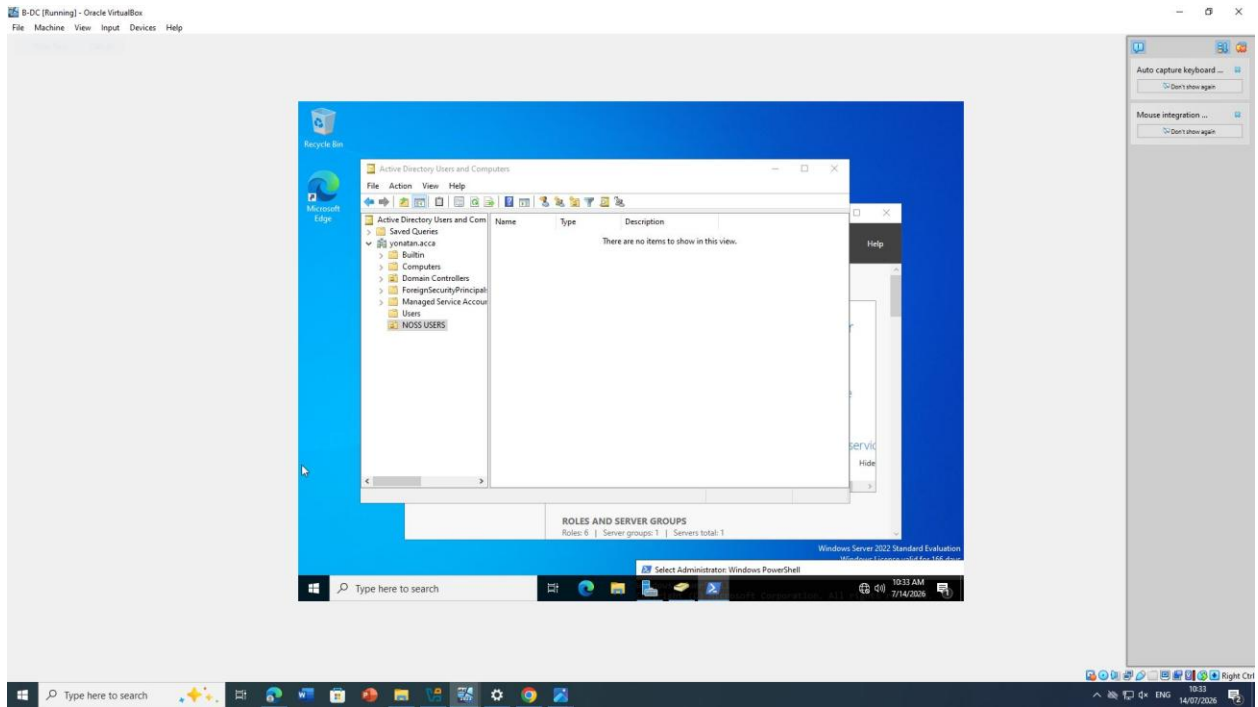


Figure 59: – DHCP Scope.

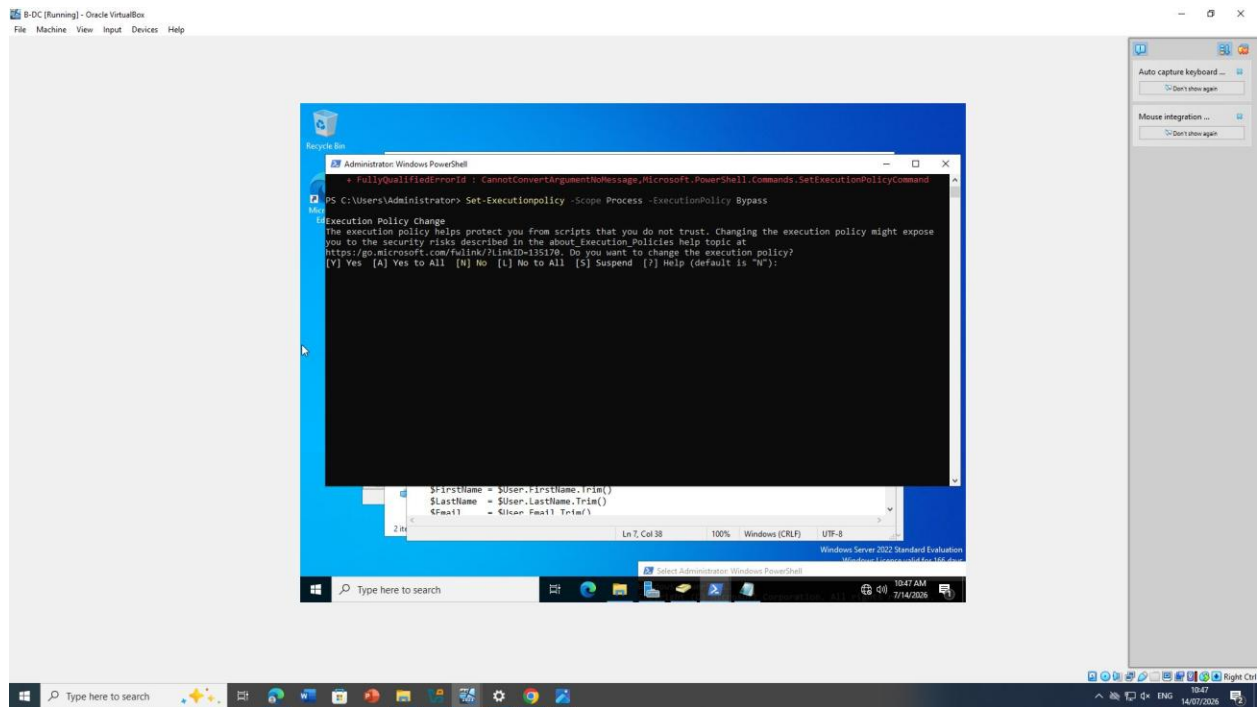


Figure 60: – DHCP Relay configuration.

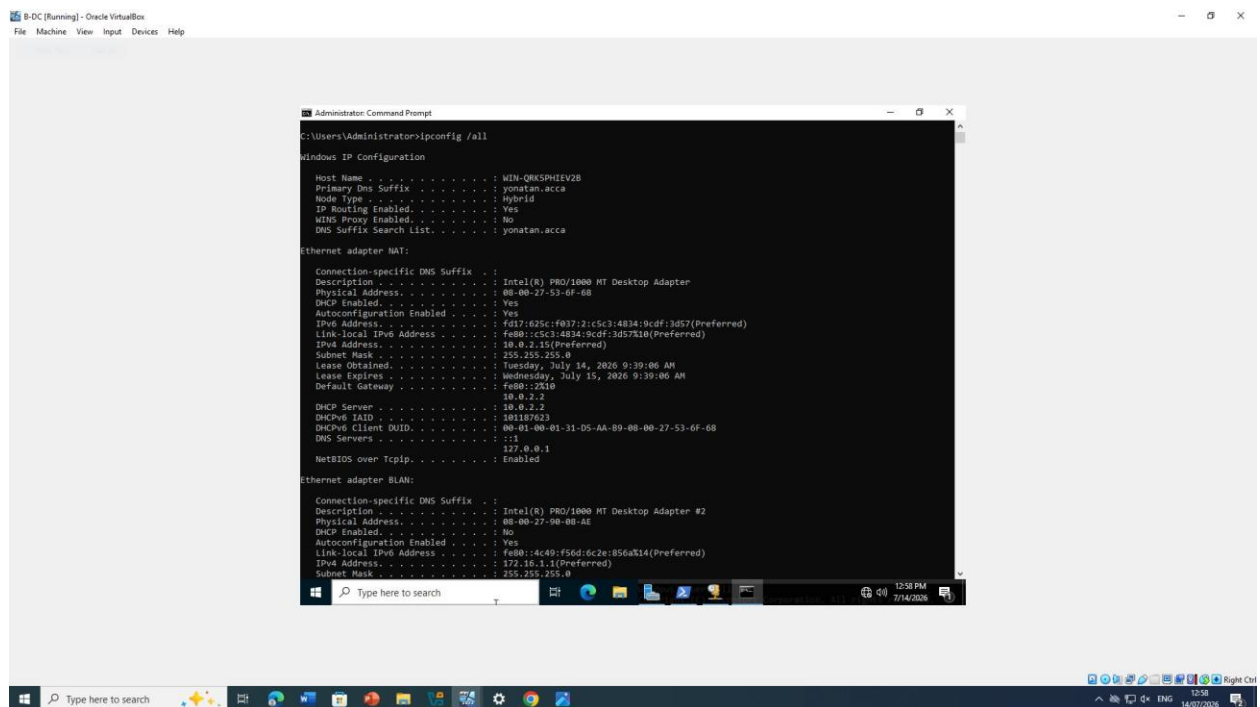


Figure 61: – Client receiving DHCP lease.

7. Test and Troubleshoot

Connectivity Testing

The completed network was tested using:

```
ping
tracert
nslookup
route print
```

Successful responses confirmed:

- DNS resolution
- Routing
- VPN communication
- DHCP operation

Where failures occurred, firewall settings, routing tables and DNS records were verified and corrected.

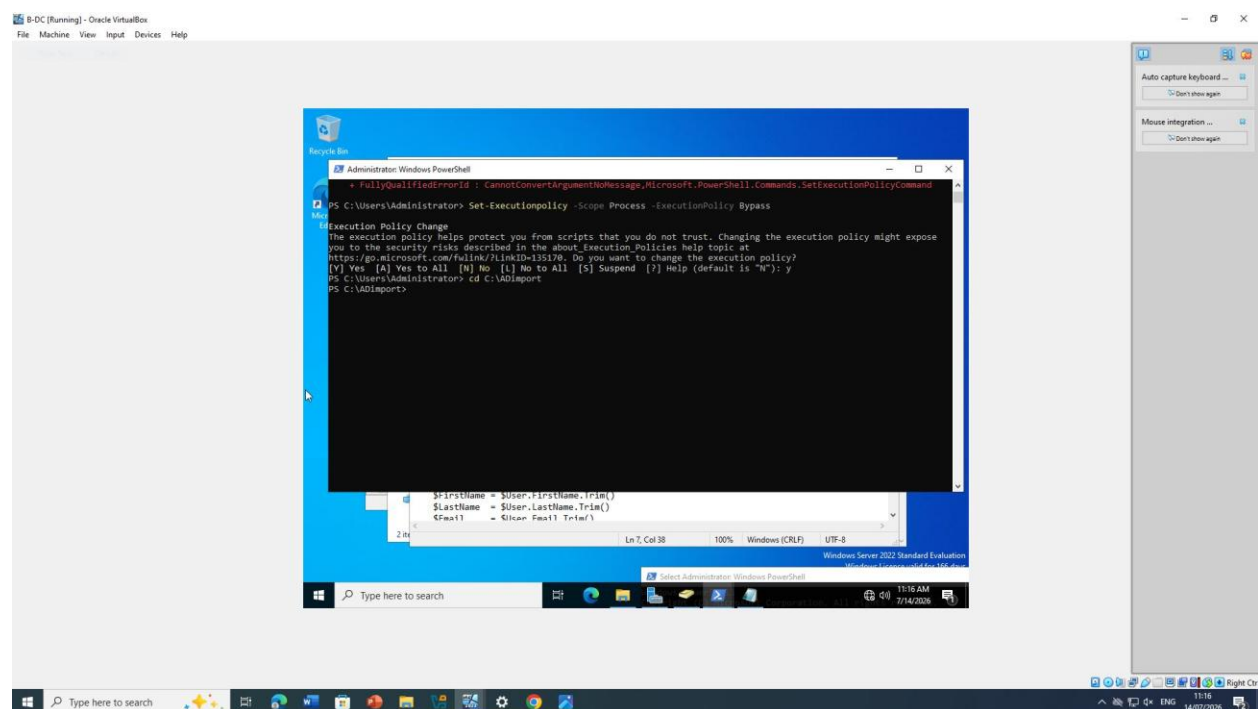


Figure 62: – Successful connectivity tests.

8. Disk Drive

8.1 Shared Storage

A second virtual disk was mounted as:

E:\BirminghamFiles

The folder was shared using:

Advanced Sharing

Permissions configured:

Group	Permission
Domain Users	Full Control
Everyone	Read

NTFS permissions were configured to match the required access controls.

The shared folder was successfully accessed from both Birmingham and London clients.

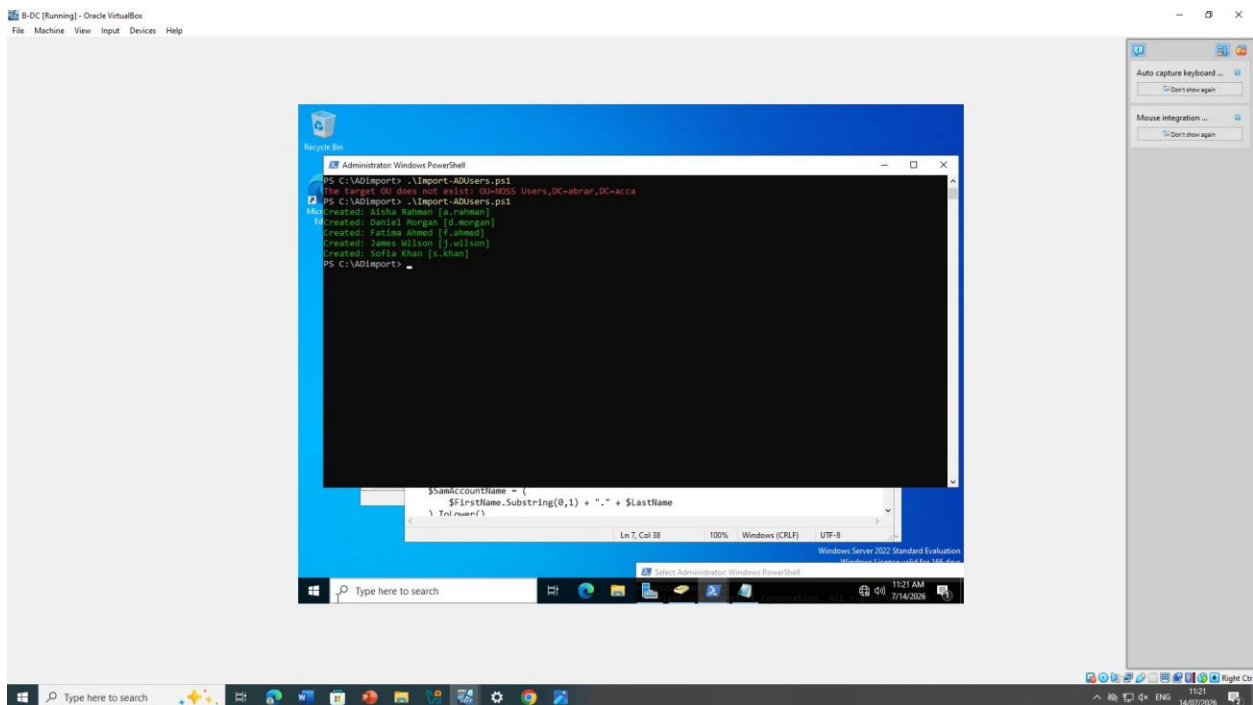


Figure 63: Disk Management.

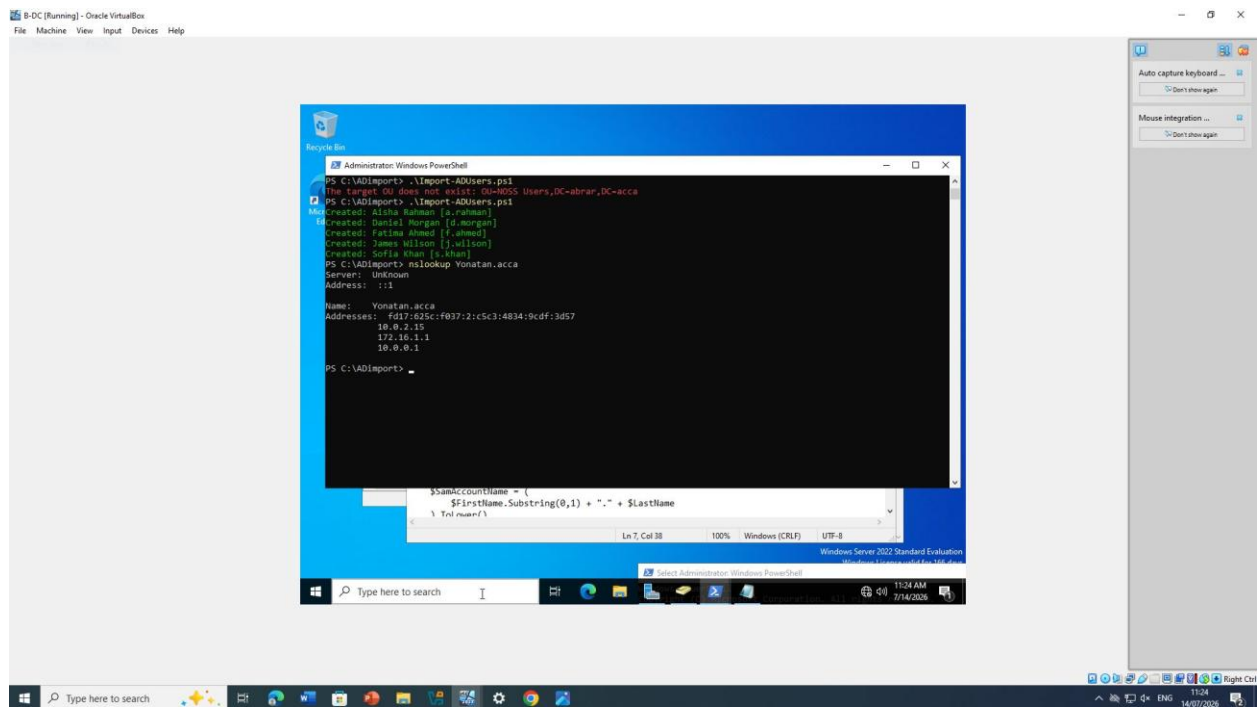


Figure 64: Share permissions.

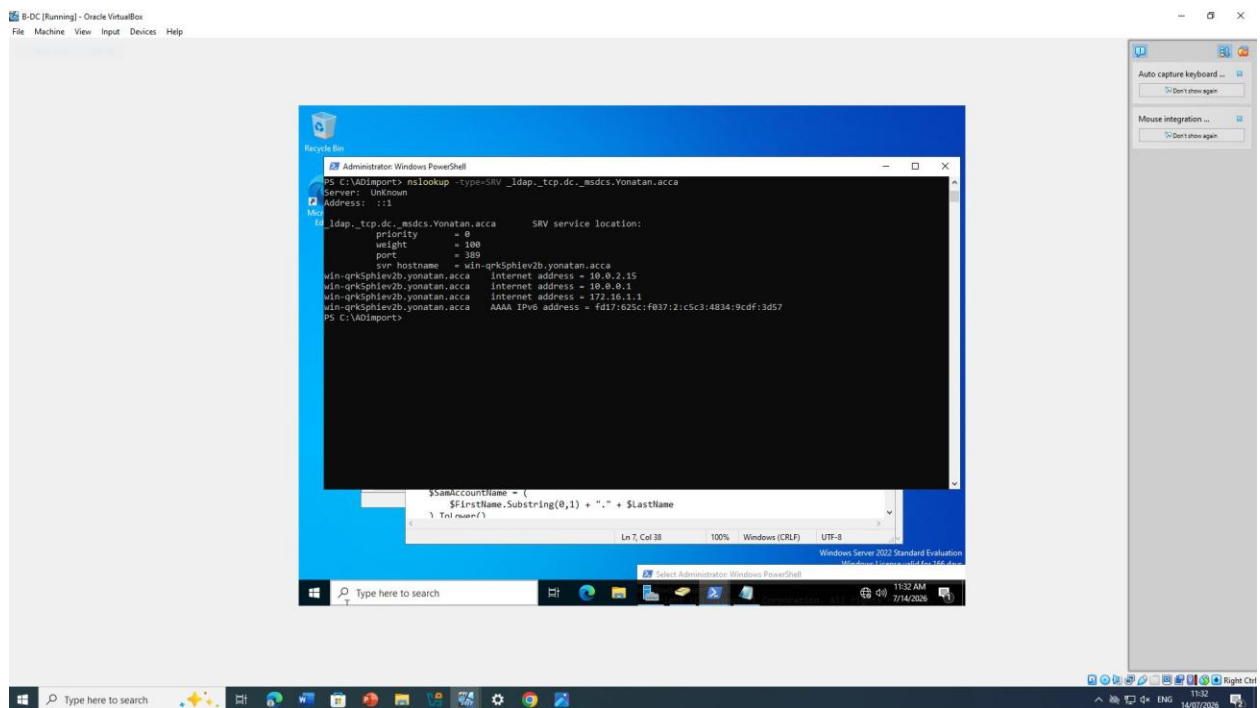


Figure 65: Access from remote client.

9. IIS Server

9.1 Creating the Website

Internet Information Services (IIS) was installed on B-DC.

A new website was created:

`https://webs.fahim.acca`

Configuration included:

- HTTPS Binding
- Internal Windows Authentication
- Default page

The homepage displayed:

Welcome to Birmingham Website

Domain users successfully authenticated using Windows credentials.

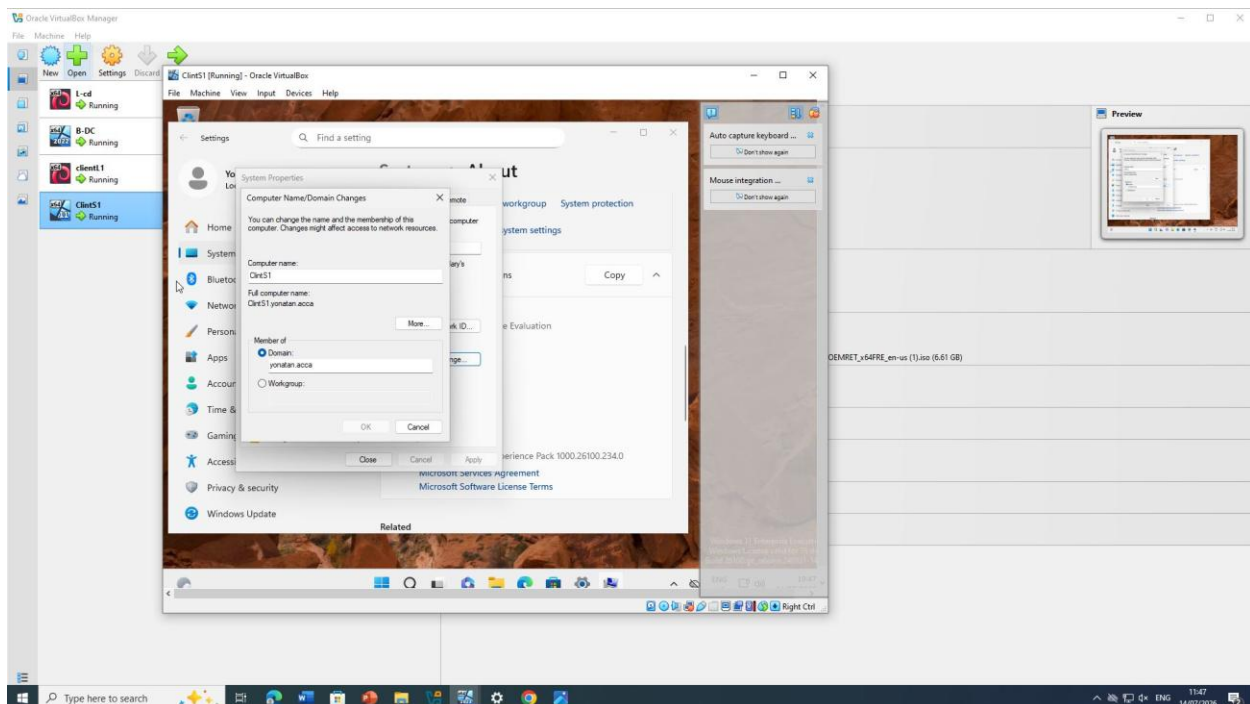


Figure 66: IIS Manager.

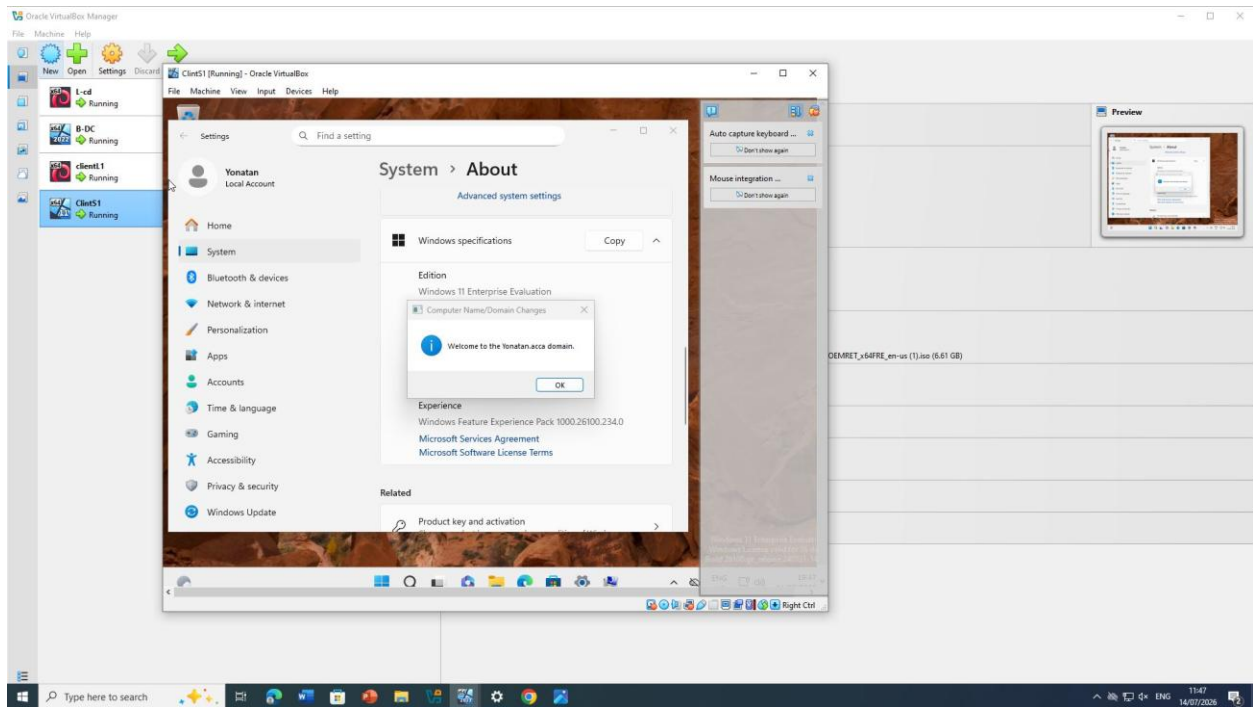


Figure 67: Website running.

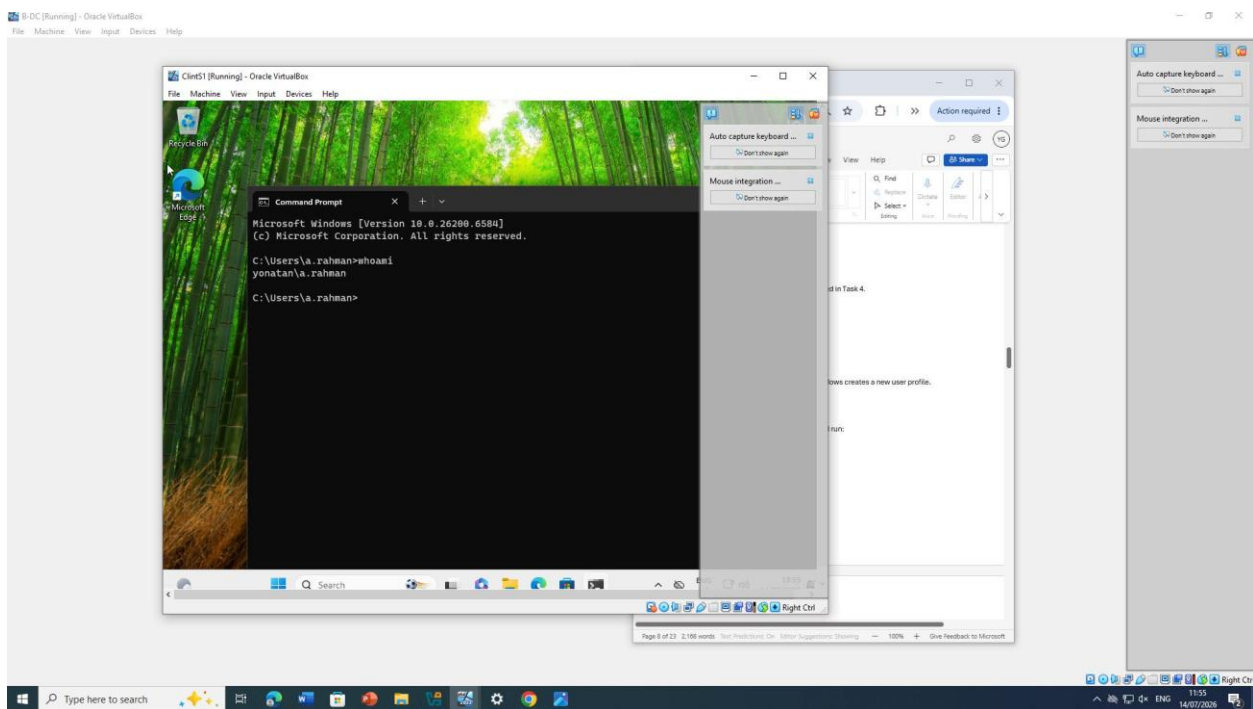


Figure 68: Browser displaying Welcome page.

10. Remote Desktop Services

10.1 Configuring Remote Desktop

Remote Desktop Services (RDS) enables administrators to securely manage servers remotely.

Remote Desktop was enabled on B-DC.

Firewall rules allowing RDP traffic were enabled.

For secure access, HTTPS was configured using an appropriate certificate.

Users connected through:

`https://rds.fahim.acca`

Successful authentication confirmed the configuration.

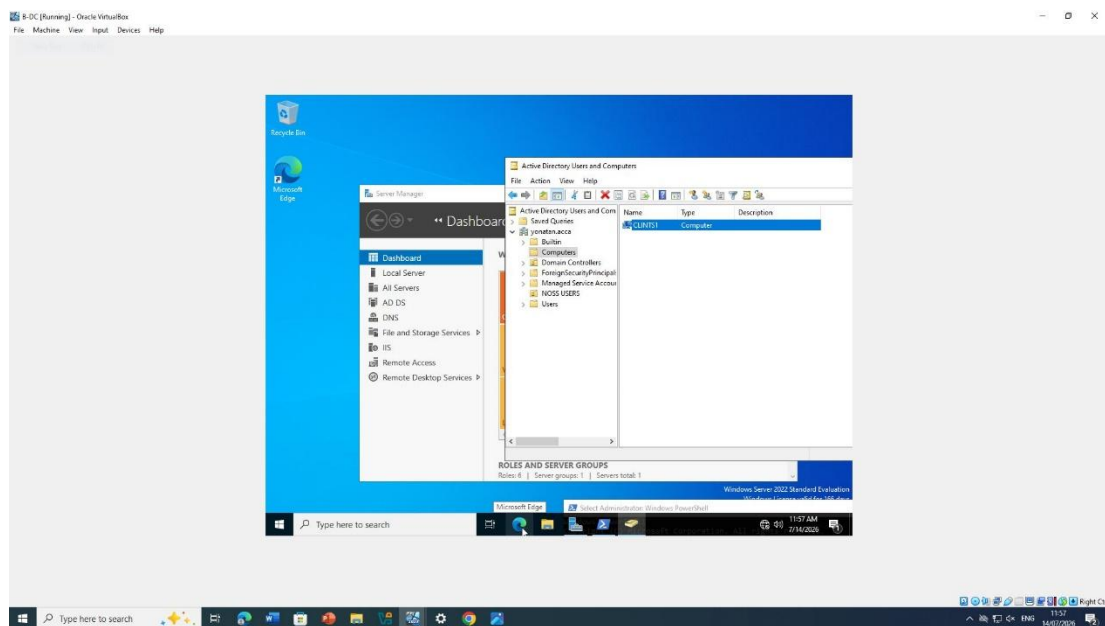


Figure 69: Remote Desktop enabled.

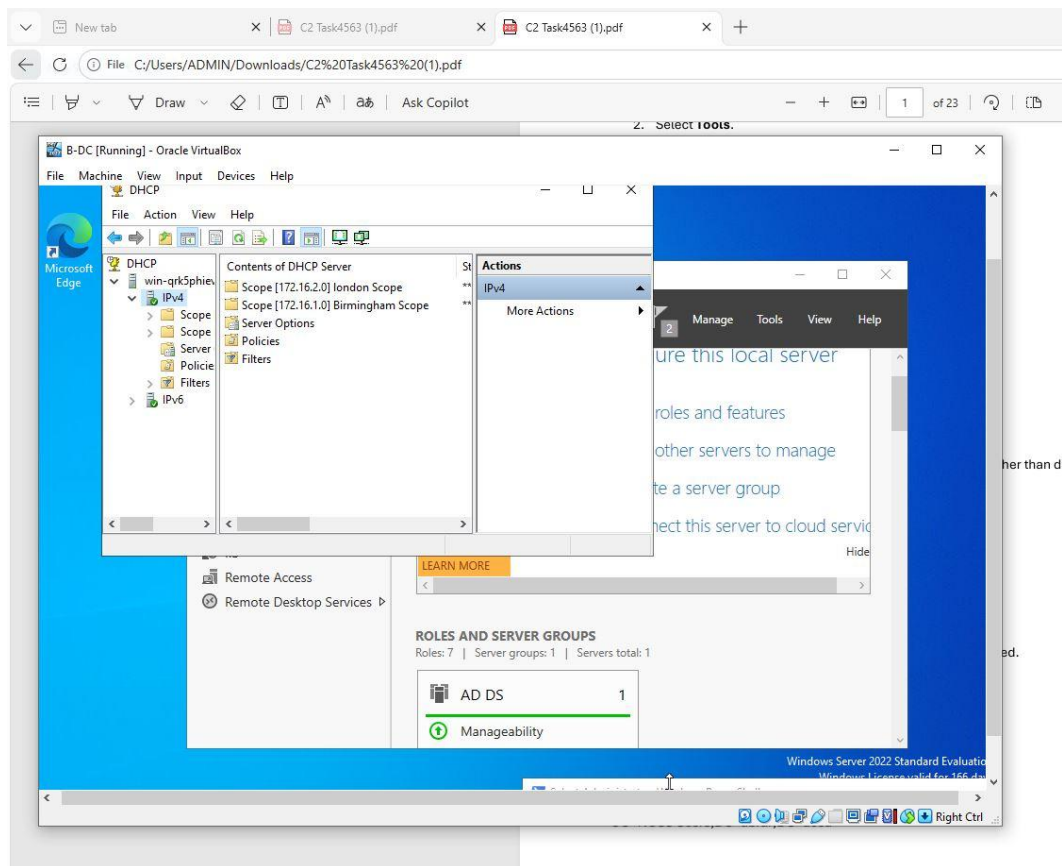


Figure 70: RDS HTTPS page.

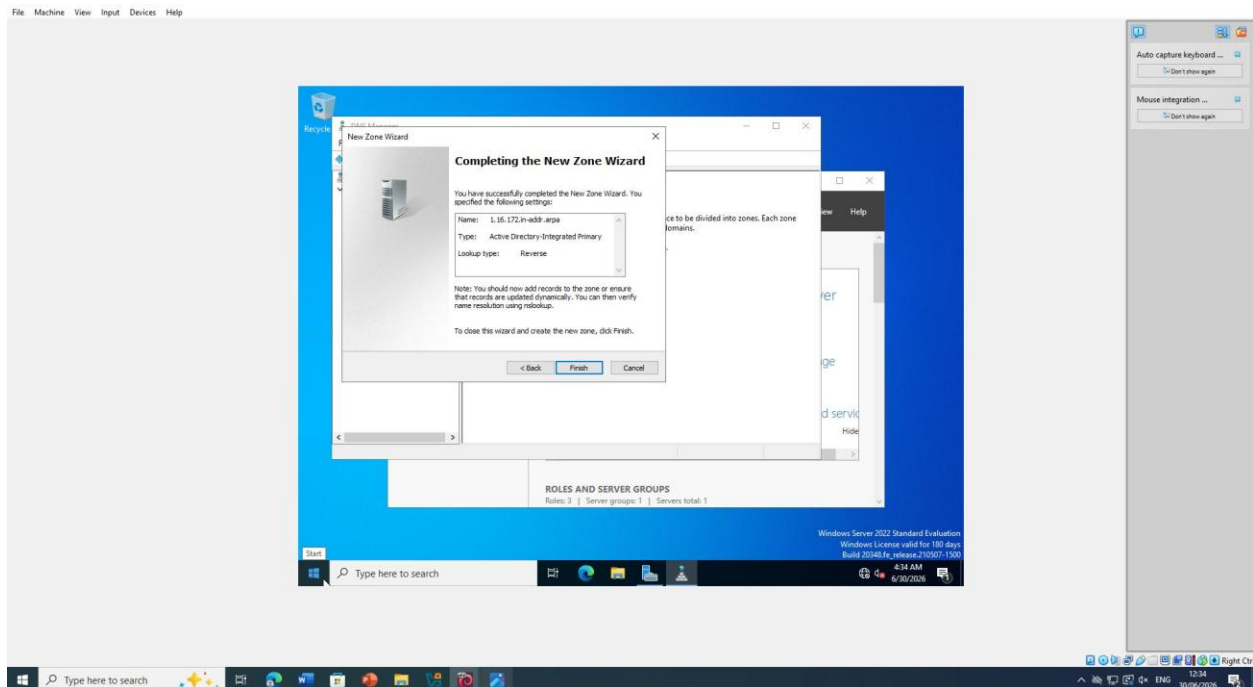


Figure 71: Successful remote login.

Overall Conclusion

The enterprise network for **NOSS London 2026** was successfully implemented by integrating routing, Active Directory, DNS, DHCP, VPN, file sharing, IIS, and Remote Desktop Services. Windows Server 2022 acted as the central infrastructure server, providing authentication, name resolution, IP address management, secure file sharing, and web services for the Birmingham and London offices. Linux routing and DHCP relay enabled seamless communication across both subnets, while the Site-to-Site VPN ensured secure inter-site connectivity. Testing confirmed successful routing, domain authentication, DNS resolution, DHCP allocation, and resource accessibility. Overall, the completed implementation demonstrates a secure, scalable, and centrally managed enterprise network aligned with industry best practices.