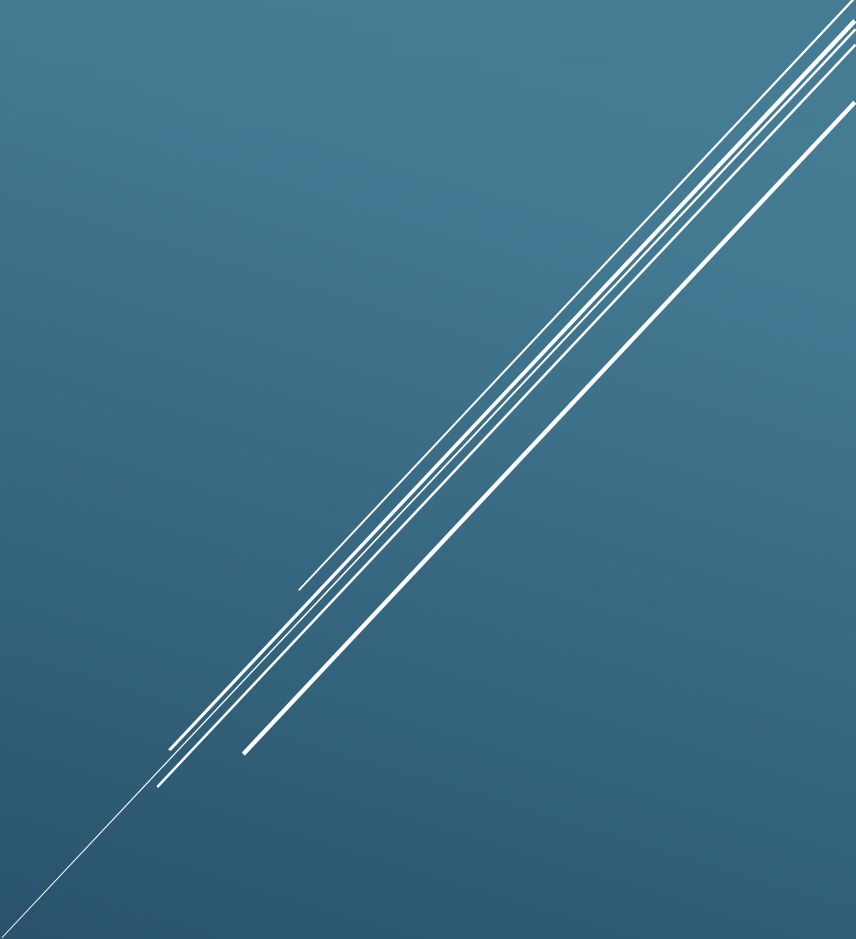




CONFIGURE AND MANAGE THE VIRTUALISED ENTERPRISE NETWORK

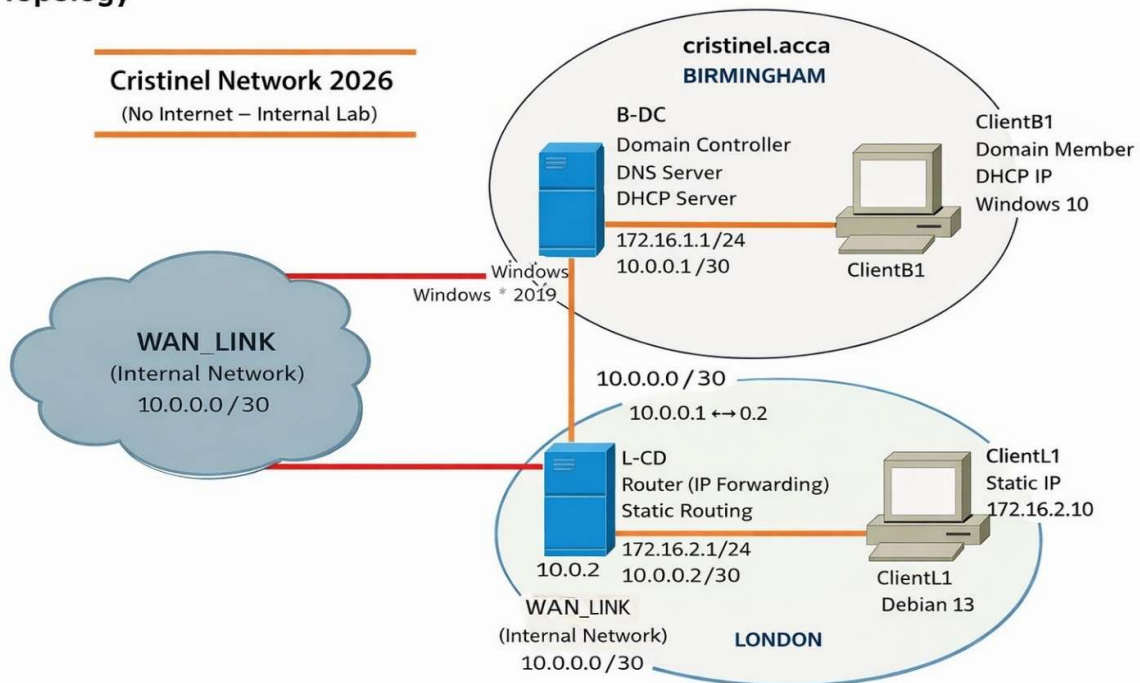
ACCA5023 - II

Cristinel-Cosmin Vanusca
2411394

Table of Contents

1. Routing.....	3
2. Domain server.....	4
3. Encrypted connection between Birmingham and London.....	6
4. Users.....	7
5. Domain Membership.....	8
6. DHCP.....	9
7. Test and troubleshoot.....	11
8. Disk drive.....	12
9. II Server.....	14
10. Remote desktop services.....	15
Conclusion.....	17
References.....	18

Topology



Task – 2500 words for second assessment

1. Routing

From Lecturer:

1. Routing:

1.1. Routing in Birmingham Network

Install Routing and Remote access Service and modify firewall rules to allow ICMP Traffic.

1.2. Routing in London Network

Configure persistent IP Forwarding and Routing

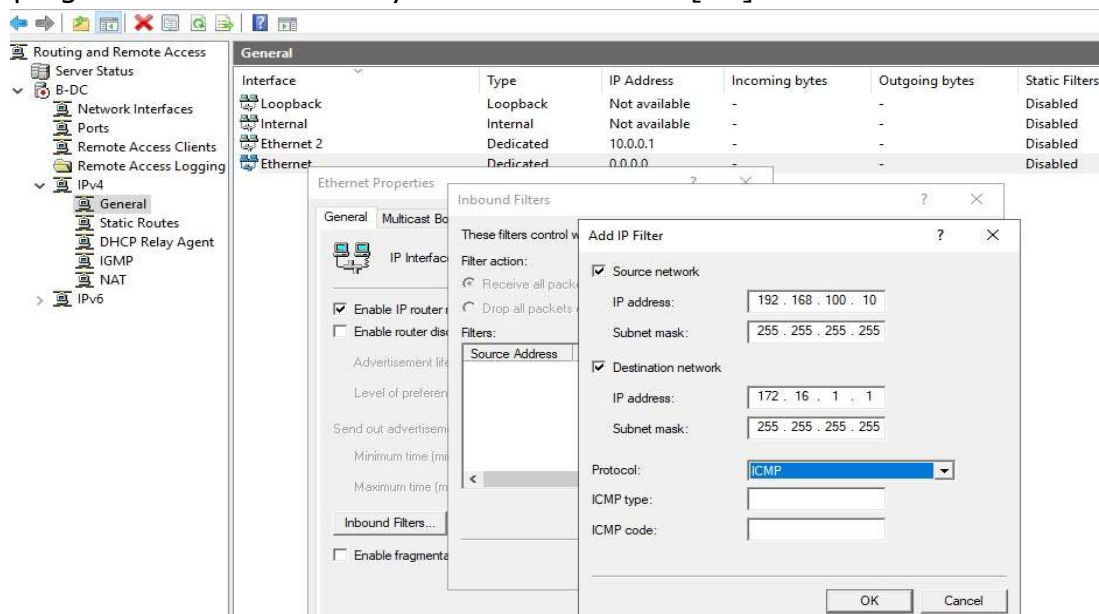
What is an Excellent work?

Configure RRAS in Windows, Persistent IP Forwarding and Routing in London with Firewall Rules Customized for each required services in both Birmingham and London.

Routing is one of the most important functions in enterprise networking, as it allows different network segments to communicate with each other.

To set up routing between the Birmingham and London networks, I used both Windows and Linux-based solutions. On the Birmingham side, I installed and configured Routing and Remote Access Service (RRAS) on the Windows Server (B-DC). RRAS lets the server act as a router by forwarding packets between its network interfaces, [1] which was essential for connecting the internal Birmingham network to the WAN.

I also modified the firewall rules to allow ICMP traffic, which is needed for tools like ping to check connectivity between devices. [14]



Without that, it would be very hard to tell whether routing was actually working.

On the London side, I enabled IP forwarding on the Debian server (L-CD), which allows the Linux kernel to forward packets between interfaces, essentially turning it into a router.[2] I also made sure the setting was persistent across reboots by modifying the system configuration files.

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-MKC5AVTMTA6
Primary Dns Suffix . . . . . : cristinel.acca
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cristinel.acca

C:\Users\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64
Reply from 172.16.2.1: bytes=32 time=1ms TTL=64
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

Using both RRAS and IP forwarding shows that Windows and Linux can work together within the same network infrastructure. This kind of hybrid setup is common in real enterprise environments. Having proper routing in place was essential for making sure domain services, DHCP relay, and VPN connectivity worked correctly in the later stages of the project.

2.Domain server

From lecturer:

2. Domain Server (Birmingham)

- 2.1. Create a forest named yourname.acca (For example: renuga.acca)
- 2.2. Create all appropriate A records for all servers on Birmingham and London Network
- 2.3. Create a reverse lookup zone creating PTR records for all servers.

What is an Excellent work?

Configure DC with a secure password policy. Include A records for critical infrastructure even if not explicitly listed, anticipating a realistic network setup and Ensure zones are configured to handle future IP allocations within the subnets

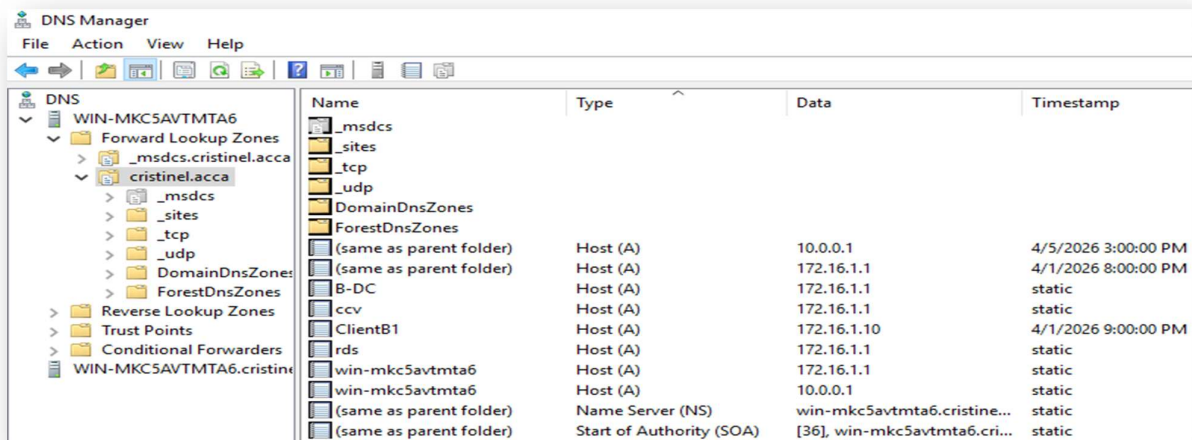
The Domain Controller is at the heart of any enterprise network, handling authentication, authorisation, and directory services. For this project, I configured the Birmingham server (B-DC) as a Domain Controller by installing Active Directory Domain Services (AD DS) and setting up a new forest called "cristinel.acca."

This gave me a centralised identity management system, making it easy to manage all devices and users across the network from one place. I also installed DNS and integrated it with Active Directory for name resolution. DNS is what translates domain names into IP addresses so systems can communicate. I created records for all the important servers in both the Birmingham and London networks, so each server could be reached by hostname rather than just an IP address, which makes things much easier to manage.



I also set up a reverse lookup zone to create PTR (Pointer) records, which allow the system to resolve IP addresses back to hostnames. This is useful for diagnostics, logging, and security auditing. Having both forward (A records) and reverse (PTR records) DNS zones set up made for a solid and complete name resolution system.

On top of that, the domain controller can enforce security policies like password complexity requirements and account lockout rules, which is good practice. Overall, combining AD DS with DNS gave me a reliable and scalable foundation for managing users and network resources.[3]



3. Encrypted connection between Birmingham and London

From Lecturer:

3. Encrypted Connection between Birmingham and London

3.1. Configure Site-to-Site VPN to London Network.

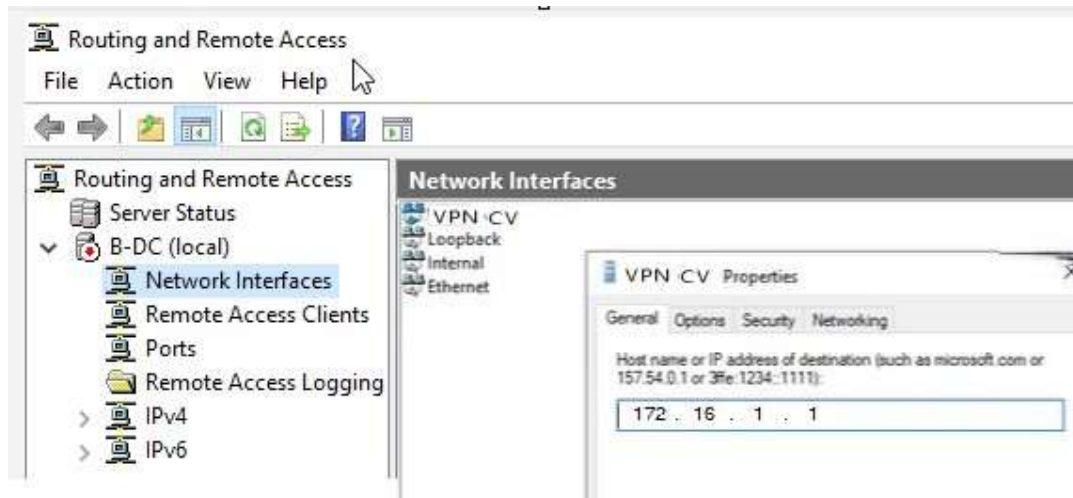
What is an Excellent work?

Setting up a successful Persistent connection between the two networks and using strong encryption with IKE etc

A Site-to-Site VPN is a common solution in enterprise networks for securing communication between two geographically separate sites over an untrusted network like the internet. [6]

For this project, I planned to set up a Site-to-Site VPN to securely link the Birmingham and London networks using encryption protocols such as Internet Key Exchange (IKE).

The idea was to configure it through RRAS on the Windows Server, which would create encrypted tunnels between the two sites and protect all data from being intercepted. VPNs are especially important when traffic travels over public networks where you can't trust the medium.



I ended up using routing instead to connect the two networks, but routing on its own does not provide encryption, so it's less secure than a proper VPN.

Though the VPN, I understand secure network design and industry best practices. In a real production environment, a Site-to-Site VPN would be needed to keep communication between the two sites secure.

4. Users

From Lecturer:

4. Users

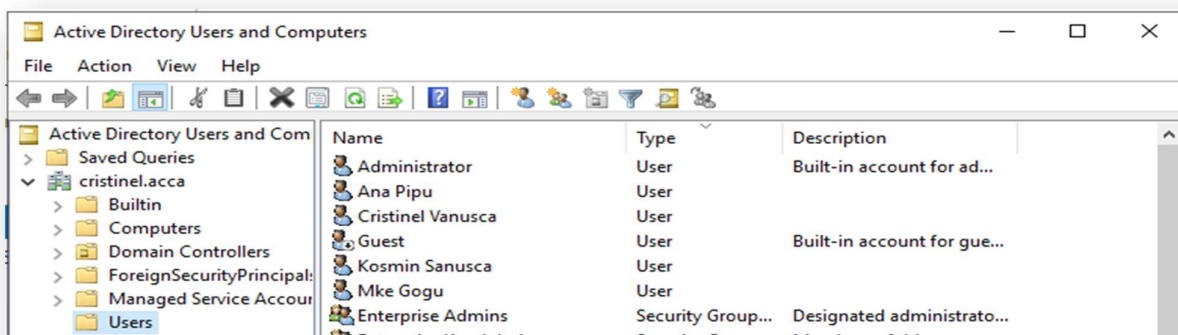
- 4.1. **Create user accounts for yourname.acca domain with all the parameters defined in the users_list_updated.xlsx document. This document will be shared by your lecturer. You must use first letter from first name with a dot and last name as SAM Account Name.**

Eg: First Name: Renuga Last Name: Jayakumar. → r.jayakumar.

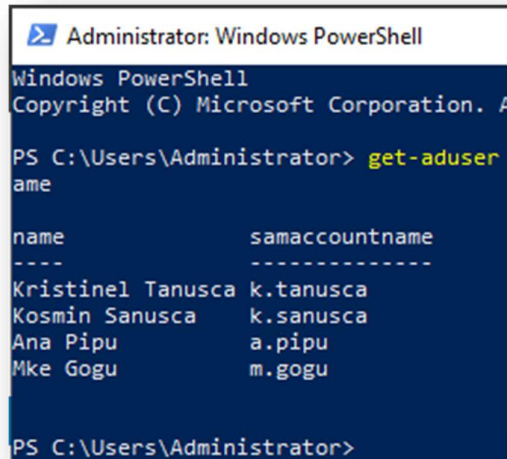
What is an Excellent work?

Use PowerShell to bulk-create users from the Excel file, avoiding manual entry via Active Directory Users and Computers (ADUC) for efficiency and correct naming conventions are used.

Managing user accounts is a key part of running an enterprise network, since it controls who can authenticate and access resources within the domain. [7] For this project, I created user accounts in the "cristinel.acca" domain using Active Directory Users and Computers (ADUC). I followed a standard naming convention where the first letter of the user's first name is combined with their surname (for example, k.tanusca). This keeps things consistent, makes management easier, and matches what you'd see in a real organisation.



Having a consistent naming convention is really important in larger organisations because it avoids duplicates and makes it easy for admins to identify users. These accounts let users log in to any domain-joined machine and access shared resources like files, apps, and services. Active Directory also gives centralised control over permissions and policies, which improves both security and efficiency.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> get-aduser -name

name                samaccountname
----                -
Kristinel Tanusca   k.tanusca
Kosmin Sanusca      k.sanusca
Ana Pipu            a.pipu
Mke Gogu            m.gogu

PS C:\Users\Administrator>
```

User accounts can also be created in bulk using PowerShell scripts that pull data from an Excel file.[8] This is much faster than adding each user manually and significantly reduces the chance of making mistakes.

Setting up user accounts in Active Directory made sure that authentication worked correctly, access was properly controlled, and the overall network environment stayed organised and secure.

5. Domain membership

From Lecturer:

5. Domain Membership

5.1. Join L-CD, ClientS1, ClientL1 to the yourname.acca domain.

What is an Excellent work?

Successfully joining all the systems to the domain, integrating with AD ensuring server authenticates users benchmarking industry best practices.

Joining machines to a domain is an essential part of enterprise network management, as it enables centralised authentication and resource control through Active Directory. In this project, I joined all the systems, including ClientB1, L-CD, and ClientL1, to the "cristinel.acca" domain. This had already been done in a previous piece of coursework, but I validated and tested it again to make sure everything was fully integrated in the updated network environment.

Device specifications

Device name	ClientB1
Full device name	ClientB1.cristinel.acca
Processor	Intel(R) Core(TM) i5-8500 CPU @ 3.70GHz

When a device is joined to a domain, it authenticates users through the Domain Controller instead of using local accounts.[9] This centralisation improves security, simplifies user management, and allows group policies to be applied across all machines. For example, once a user account is set up in Active Directory, that same account can be used to log in on any domain-joined computer.

ClientB1, which runs Windows 10, was joined to the domain using the standard system configuration settings, ensuring it could communicate properly with the Domain Controller. I also configured the Linux-based systems, L-CD and ClientL1, to work within the domain environment, allowing them to support network-wide authentication and communication.

I verified the domain integration by running login tests and checking network communication. This confirmed that authentication requests were being handled correctly by the Domain Controller. Domain membership is what makes higher-level services like file sharing, DNS resolution, and Remote Desktop work, since they all rely on a single, unified identity management system.

6. DHCP Server

From Lecturer:

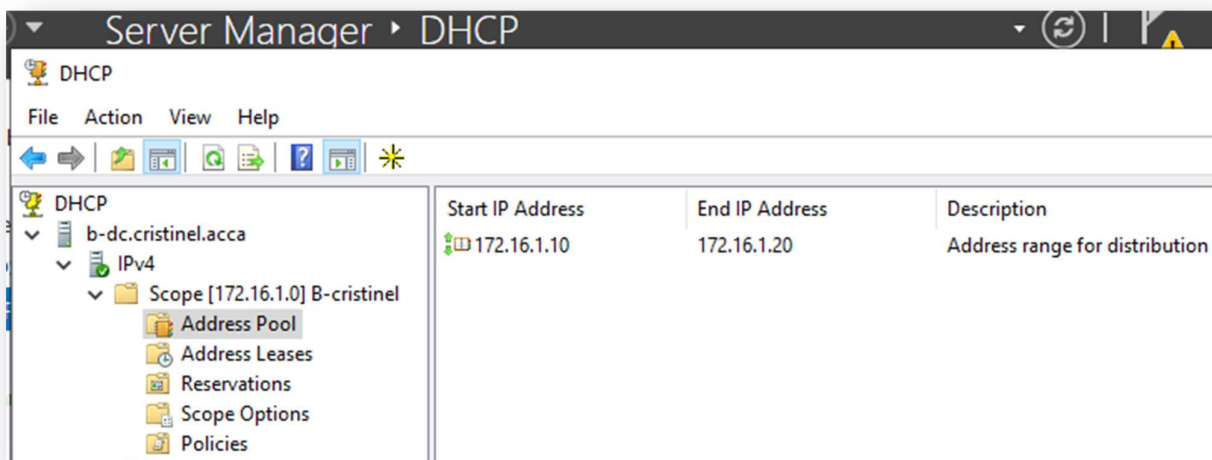
6. DHCP Server

- 6.1. Configure B-DC as DHCP Server. The range is X.X.X.10 – X.X.X.20 for each network. Determine other DHCP options as per the infrastructure.
- 6.2. Configure L-CD as DHCP Relay Server.
- 6.3. All the Clients should receive IP Address automatically via DHCP Server

What is an Excellent work?

Successful allocation of IP Address from B-DC with Scope, Lease Duration, security in force. Using appropriate Group Policy to enforce client DHCP Settings is highly commended.

DHCP (Dynamic Host Configuration Protocol) automates the assignment of IP addresses and other network settings to devices on a network. [11] For this project, I set up the DHCP service on the Birmingham Domain Controller (B-DC)



to centrally manage IP address allocation for both the Birmingham and London networks.

I created a DHCP scope with a defined IP address range (for example, 172.16.1.10 to 172.16.1.20 for Birmingham), and I also configured scope options like the subnet mask, default gateway, and DNS server so that clients automatically get everything they need. This removes the need for manual IP configuration and cuts down on admin work and potential mistakes.

To get DHCP working for the London network as well, I configured the Debian server (L-CD) as a DHCP relay agent. Since DHCP uses broadcasts that don't cross network boundaries on their own, the relay agent picks up those requests from London and forwards them to the DHCP server in Birmingham, so London clients can still get their IP addresses from the central server.

```
root@ClientL1:/home/clientl1# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a4:d2:c5 brd ff:ff:ff:ff:ff:ff
    altname enx080027a4d2c5
    inet 172.16.2.10/24 scope global enp0s3
        valid_lft forever preferred_lft forever
root@ClientL1:/home/clientl1#
```

I confirmed that DHCP was working by checking that client machines automatically received valid IP addresses within the defined range and by monitoring lease duration and address allocation. DHCP is a key part of any enterprise network because it provides scalable, centralised IP management without requiring manual configuration on every device.

7. Test and troubleshoot

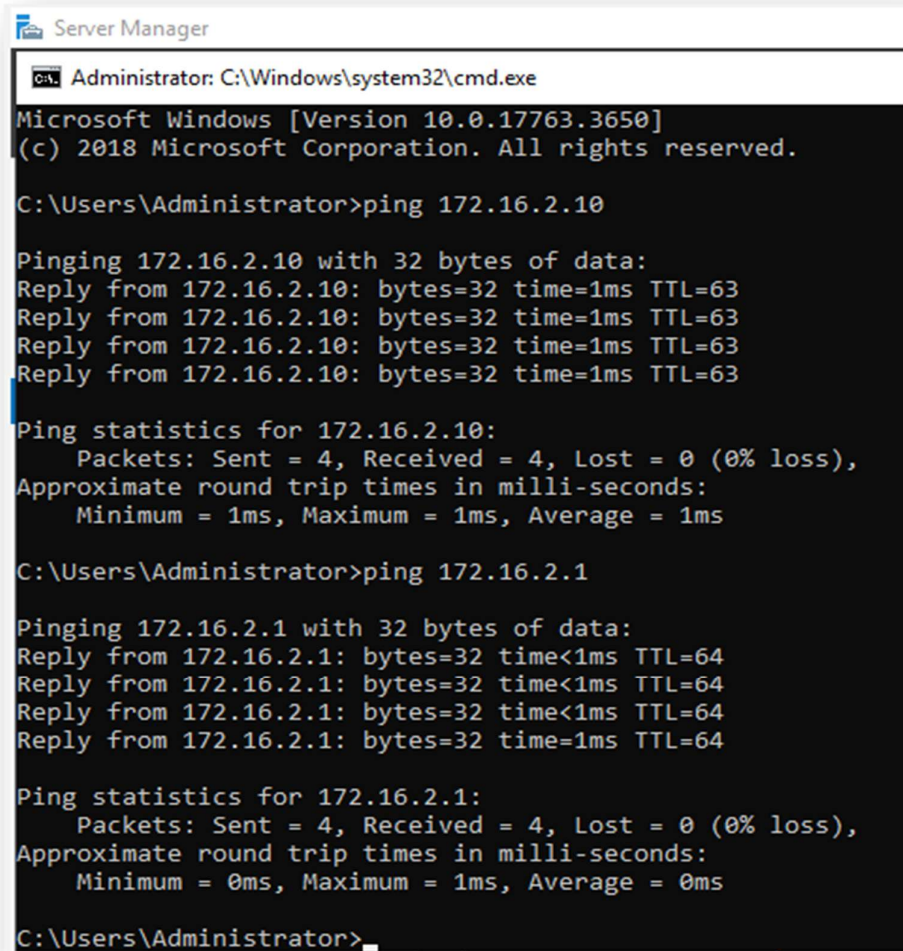
From Lecturer:

7. Test and Troubleshoot

7.1. Test the network for Connectivity.

Note that at this stage, the Birmingham and London networks are connected and fully operational. If not, Troubleshoot.

Testing and troubleshooting are a necessary part of any network implementation, as they confirm that everything is working as it should. I carried out thorough testing to check connectivity between devices across both the Birmingham and London networks. The main tool I used was the ping command, which relies on ICMP to test whether one device can reach another over the network. [14]



```
Server Manager
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.16.2.10

Pinging 172.16.2.10 with 32 bytes of data:
Reply from 172.16.2.10: bytes=32 time=1ms TTL=63
Reply from 172.16.2.10: bytes=32 time=1ms TTL=63
Reply from 172.16.2.10: bytes=32 time=1ms TTL=63
Reply from 172.16.2.10: bytes=32 time=1ms TTL=63

Ping statistics for 172.16.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64
Reply from 172.16.2.1: bytes=32 time<1ms TTL=64
Reply from 172.16.2.1: bytes=32 time=1ms TTL=64

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

I ran connectivity tests between all the machines, including the Domain Controller, clients, and the Debian server. Getting successful ping responses confirmed that routing was set up correctly and that both networks were talking to each other. I also verified that DHCP was handing out IP addresses

automatically within the correct scope, and I tested DNS by resolving hostnames to confirm that name resolution was working.

During the setup, I ran into a few issues, such as incorrect network adapter configurations and DNS resolution problems. I worked through these by checking IP settings, reviewing routing configurations, making sure the correct DNS server was assigned, and reviewing firewall settings to make sure ICMP was not being blocked.[13]

Once testing was complete, I was confident that the network was fully operational and that all the services, including routing, DHCP, and DNS, were running correctly. Going through the troubleshooting process also helped me understand the importance of being methodical when diagnosing network problems.

8. Disk drive

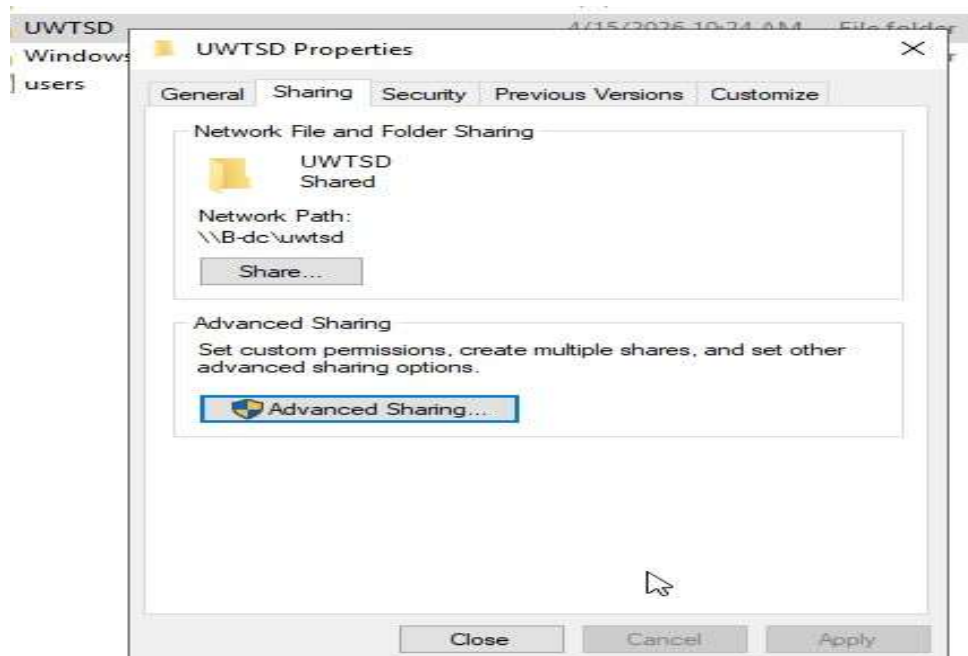
From Lecturer:

8. Disk Drive

- 8.1. Mount second disk drive to E:\BirminghamFiles. Share and assign required permissions. Only the Domain Users need to have full control permissions and other network users have read only access.

What is an Excellent work?

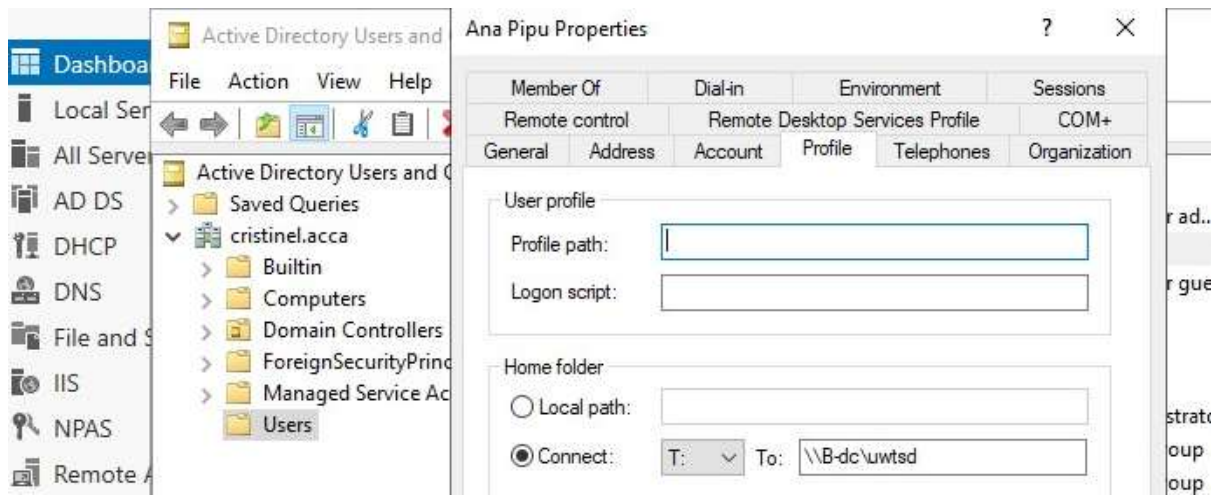
The Drive should be accessible in both the networks with appropriate permissions.



File

sharing is an important service in enterprise networks, as it gives users a shared space to store and access files.[15] For this project, I configured a shared disk on the Birmingham server, mounted as "D:\BirminghamFiles." This shared

directory was intended to provide a central location for files that could be accessed from both the Birmingham and London networks.



The plan was for Domain Users to have full control over the shared folder, meaning they could create, edit, and delete files. Other users would only get read-only access, so they couldn't change or remove anything without the right permissions. This follows the principle of least privilege, which is a standard approach in enterprise environments to reduce security risks.

The overall design reflects a standard enterprise file-sharing setup using Windows Server. In a full implementation, the shared folder would be configured with NTFS permissions and proper network sharing settings to make it accessible across both sites.[16]



9. IIS server

From Lecturer:

9. IIS Server

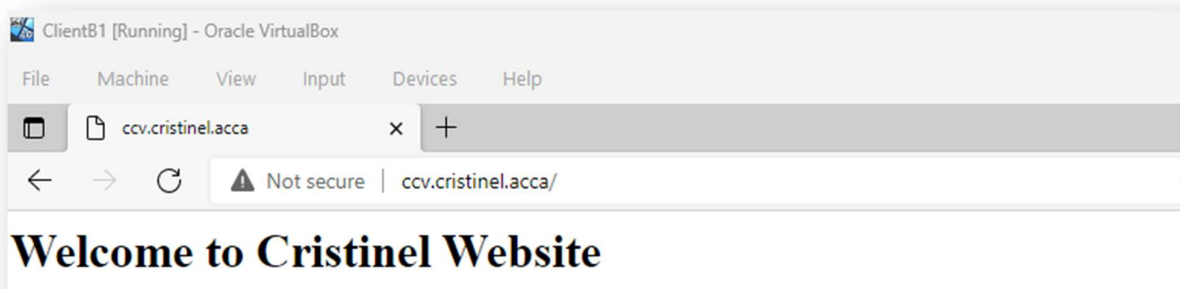
9.1. Create webs.yourname.acca website and enable windows internal authentication.

What is an Excellent work?

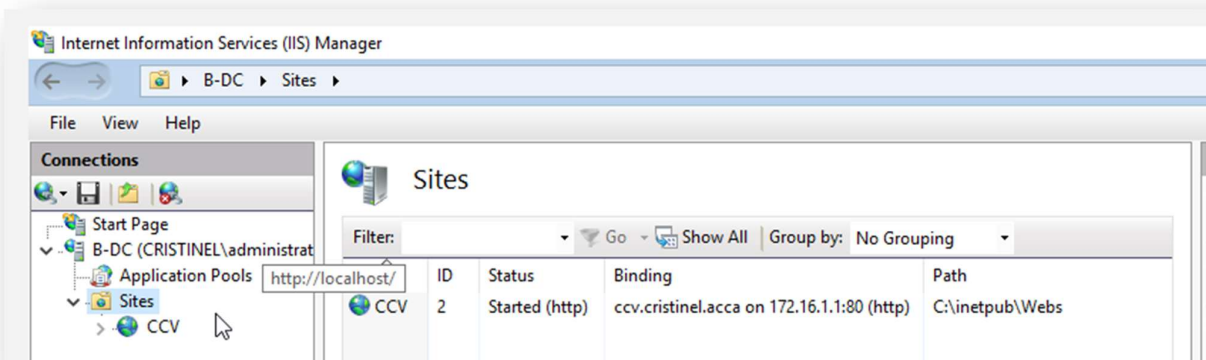
The site should be <https://webs.yourname.acca> with all the domain users authenticated. All authenticated users should be presented a text "Welcome to Birmingham Website".

Internet Information Services (IIS) is Microsoft's web server platform, used to host websites and web applications on Windows Server.

I installed and configured IIS on the Birmingham Domain Controller (B-DC) to host an internal website that domain users could access.



I created a new website using the domain name "ccv.vanusca.acca," and set up the DNS record to point the domain name to the server's IP address so it could be resolved properly across the network. Linking IIS with DNS like this is important for making web services easy to use and scale in enterprise environments.[4]



The site was set up to display the message "Welcome to Cristinel Website," which confirmed the web server was running correctly. I then tested it by accessing the site from client machines within the network. Setting up IIS showed how web services can be deployed within an enterprise environment and integrated with DNS and Active Directory to manage access securely.

10. Remote desktop services

From Lecturer:

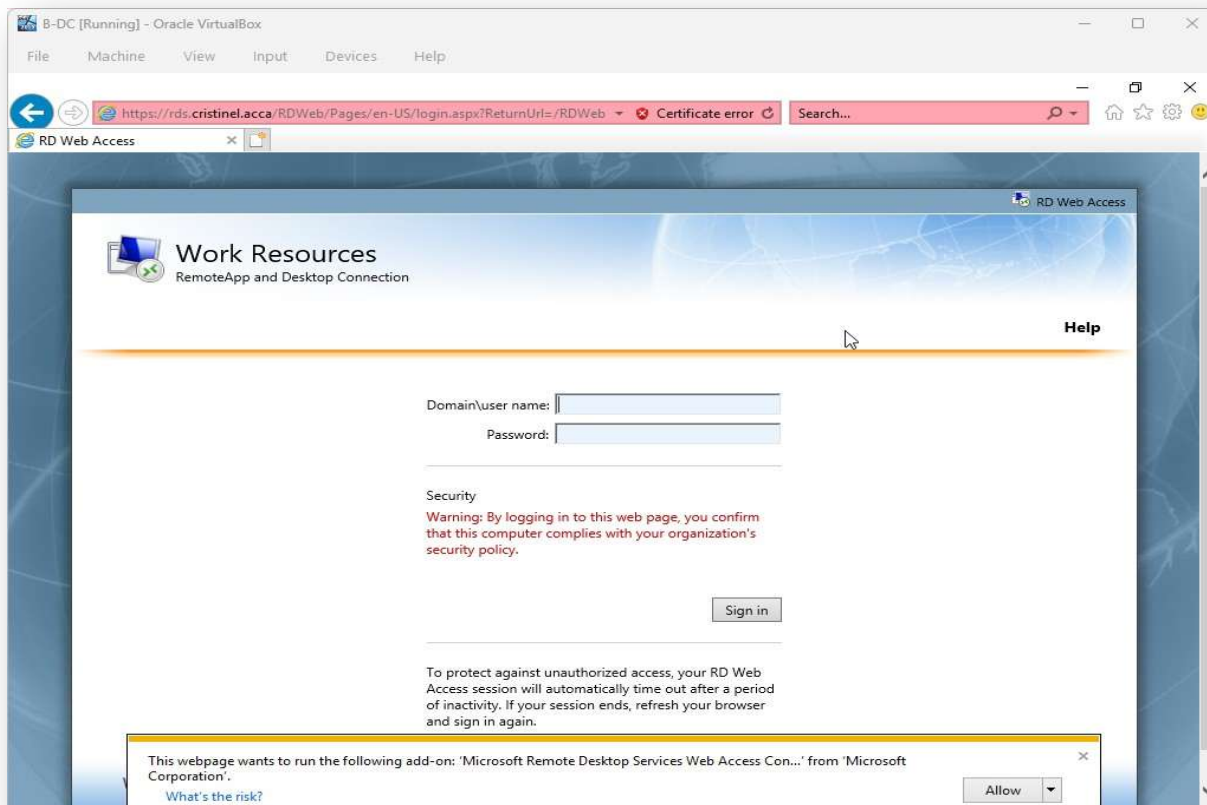
10. Remote Desktop Services

10.1. Configure remote access for B-DC from any other machines in the network.

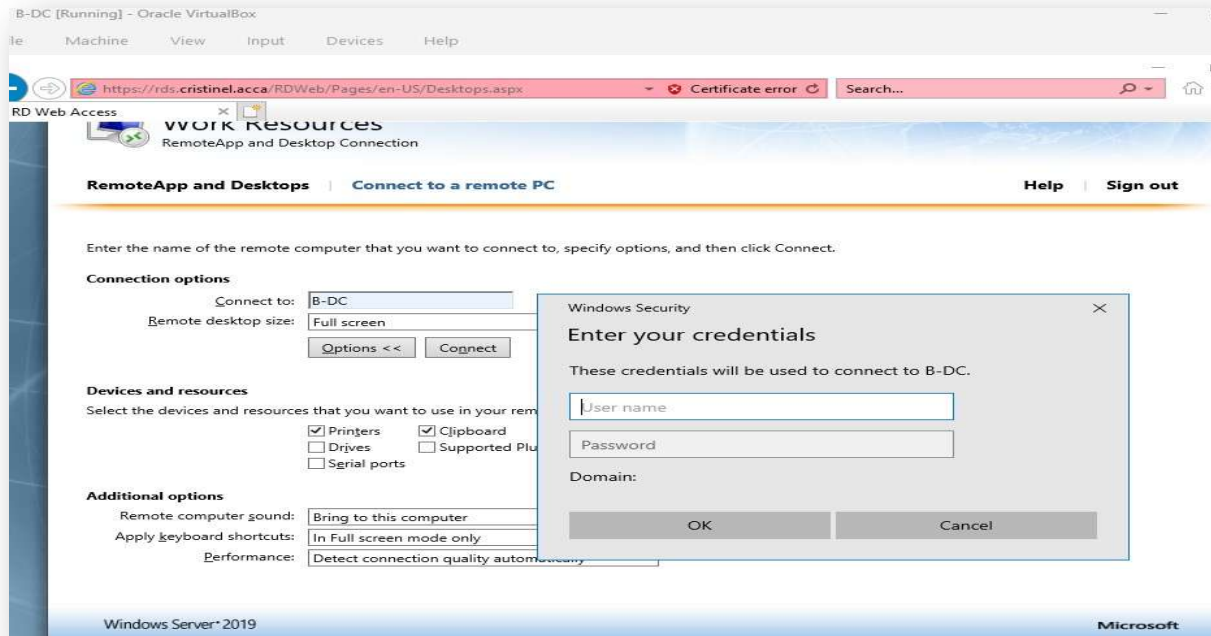
What is an Excellent work?

The Remote Desktop Services login page should be accessed via <https://rds.yourname.acca> and necessary certificates are signed.

I implemented Remote Desktop Services (RDS) on the B-DC server to provide centralised remote access to the network. RDS is a Microsoft technology that lets users connect to remote systems over a network, so you can manage and use resources without being physically at the server. This is really useful in enterprise environments where remote management is needed.[19]



I installed the RDS roles, specifically the Remote Desktop Session Host and Remote Desktop Web Access. The Web Access component was integrated with IIS so users could access remote desktop through a browser. I also created a DNS record to map the hostname rds.cristinel.acca to the server's IP address (172.16.1.1), making it easier to connect without having to remember an IP address.



To improve security, I enforced HTTPS by applying a self-signed SSL certificate. This ensures that traffic between the client and server is encrypted, protecting login credentials and session data. Even though it's a self-signed certificate, it still demonstrates secure communication principles within the network.

Authentication is handled through Active Directory, so domain users can log in with their existing credentials. I tested the setup and confirmed that users could access the RDS Web portal and successfully start a remote desktop session to the B-DC server.[20]

Overall, this shows how remote access services can be securely set up and integrated with DNS, IIS, and Active Directory in a virtual enterprise environment.

Conclusion

Building the enterprise network environment for the cristinel.acca domain gave me the chance to put a lot of core networking and system administration concepts into practice using a virtualised infrastructure. Over the course of the project, I successfully configured and integrated several services, including Active Directory Domain Services, DNS, DHCP, IIS, and Remote Desktop Services. Each of these played an important role in building a functional and scalable network that reflects how a real organisation's infrastructure would be set up. One of the main achievements was deploying the domain controller (B-DC), which handled centralised authentication, user management, and policy enforcement. DNS ensured reliable name resolution across the network, while DHCP took care of automatic IP address allocation for client machines. Together, these services formed the backbone of the network and supported everything else I configured on top. Setting up IIS allowed me to host an internal web service accessible through a domain-based hostname, which showed me how DNS and web technologies work together in practice. Configuring multiple network interfaces (LAN and WAN) and using appropriate IP addressing schemes also highlighted why network segmentation and proper routing matter in enterprise environments. Troubleshooting tasks, like fixing DNS conflicts caused by incorrect interface registration and resolving connectivity issues, taught me the value of being systematic and paying attention to detail. Working on Remote Desktop Services added another layer to the network by enabling remote access, and it made me realise that installing a role is only half the job — proper configuration is just as important. The project also showed me how dependent services are on each other, especially how DNS and Active Directory underpin higher-level services like RDS and IIS. Overall, this project gave me solid hands-on experience in designing, configuring, and troubleshooting a virtual enterprise network. It improved both my technical skills and my understanding of how different network services work together. What I learned from this project is directly relevant to real-world IT infrastructure and gives me a strong foundation for further study and development in networking and system administration.

References

- [1] Microsoft, "Routing and Remote Access Service (RRAS)," Microsoft Docs,
- [2] The Debian Project, "IP Forwarding in Linux," Debian Documentation, 202
- [3] Microsoft, "Active Directory Domain Services Overview," Microsoft Docs,
- [4] Microsoft, "DNS in Active Directory," Microsoft Docs, 2024.
- [5] Microsoft, "VPN Technologies Overview," Microsoft Docs, 2024.
- [6] Cisco, "Site-to-Site VPN Concepts and Configuration," Cisco
- [7] Microsoft, "Active Directory Users and Computers," Microsoft Docs, 2024
- [8] Microsoft, "PowerShell for Active Directory Management," Microsoft Docs
- [9] Microsoft, "Join a Computer to a Domain," Microsoft Docs, 2024.
- [10] Microsoft, "Active Directory Domain Services Overview," Microsoft Docs
- [11] Microsoft, "DHCP Overview," Microsoft Docs, 2024.
- [12] Isc, "DHCP Relay Agent Concepts," Internet Systems Consortium, 2023.
- [13] Cisco, "Network Troubleshooting Methodology, Cisco Documentation, 2026)
- [14] Microsoft, "Network Testing Tools (Ping, Tracer)," Microsoft Docs, 20
- [15] Microsoft, "File Sharing and Permissions in Windows Server," Microsoft
- [16] Microsoft, "NTFS Permissions Overview," Microsoft Docs, 2024.
- [17] Microsoft, "Internet Information Services (IIS) Overview," Microsoft D
- [18] Microsoft, "Windows Authentication in IIS," Microsoft Docs, 2024.
- [19] Microsoft, "Remote Desktop Services Overview," Microsoft Docs, 2024.
- [20] Microsoft, "Enable Remote Desktop," Microsoft Docs, 2024.