



University of Wales
Trinity Saint David

Technical Report: Comprehensive Implementation, Architectural Analysis, and Verification of a Multi-Site Virtualized Enterprise Network Infrastructure

Module: ACCA5023 - Network Operating Systems and Services

Student Name: Christian Prida

Student Number: 242771

Introduction and Executive Summary

Project Scope and Strategic Objectives

This technical report provides an exhaustive, granular documentation of the deployment, configuration, systems integration, and empirical verification of a multi-site enterprise network infrastructure. Designed to emulate a high-availability multinational corporate environment, the topology bridges two geographically separated regional offices: the primary headquarters situated in Birmingham and a major regional branch office situated in London. The overarching objective of this project is to implement a resilient, highly secure, and scalable IT infrastructure operating under a unified Active Directory forest and domain structure designated as prida.acca.

Modern enterprise environments demand uncompromising reliability, strict access governance, and seamless interoperability across wide-area network boundaries. To satisfy these operational constraints, the technical execution encompasses multiple advanced systems administration and networking domains, systematically detailed throughout this document:

- Advanced Routing and Remote Access (RRAS): Implementation of software-based routing engines, packet forwarding rules, and network address translation or tunneling layers to manage wide-area network (WAN) interconnectivity.
- Active Directory Domain Services (AD DS): Deployment of multi-master directory paradigms for centralized identity lifecycle management, policy enforcement, and hierarchical security structures.
- Domain Name System (DNS) Architecture: Configuration of robust name resolution mechanics featuring primary forward and reverse lookup zones, service location records, and secure dynamic updates.
- Site-to-Site Virtual Private Network (VPN) Tunneling: Establishment of encrypted, virtualized point-to-point links using Demand-Dial interfaces to securely route traffic across disparate subnets without exposure to external packet sniffing.
- Dynamic Host Configuration Protocol (DHCP): Automation of IP address leasing, scope management, and option distribution across segmented subnet boundaries to minimize configuration drift.
- File and Storage Services: Engineering of centralized file repositories secured by granular New Technology File System (NTFS) access control lists and network sharing attributes.
- Internet Information Services (IIS) Deployment: Provisioning of scalable web services coupled with Windows Integrated Authentication to enforce rigorous, domain-authenticated access controls.

Enterprise Topology and Physical-Virtual Architecture

The infrastructure is constructed using a virtualized hypervisor architecture running Microsoft Windows Server environments alongside dedicated client systems. The logical network design deliberately isolates traffic into specific subnet boundaries to reflect real-world enterprise network segmentation strategies, reducing broadcast domains and enhancing security isolation:

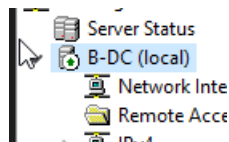
- Birmingham Headquarter Site: Operates natively on the 172.16.1.0/24 subnet. It is anchored by the primary domain controller (B-DC), running Windows Server 2022, which assumes roles as the primary DNS server, DHCP allocator, and RRAS gateway. Client workstation integration is represented by ClientS1.
- London Branch Site: Operates on the 172.16.2.0/24 subnet. It is managed by the regional server infrastructure (L-CD) and client endpoints (ClientL1), ensuring localized resource management and fault tolerance.
- WAN Interconnect and VPN Transit Segment: Utilizes a dedicated point-to-point transit network segment (10.0.0.0/30) to establish secure, encrypted communications across the virtualized wide-area network interfaces, abstracting underlying physical network infrastructure.

Routing and Remote Access Service (RRAS) Deployment

Theoretical Framework and Packet Forwarding Principles

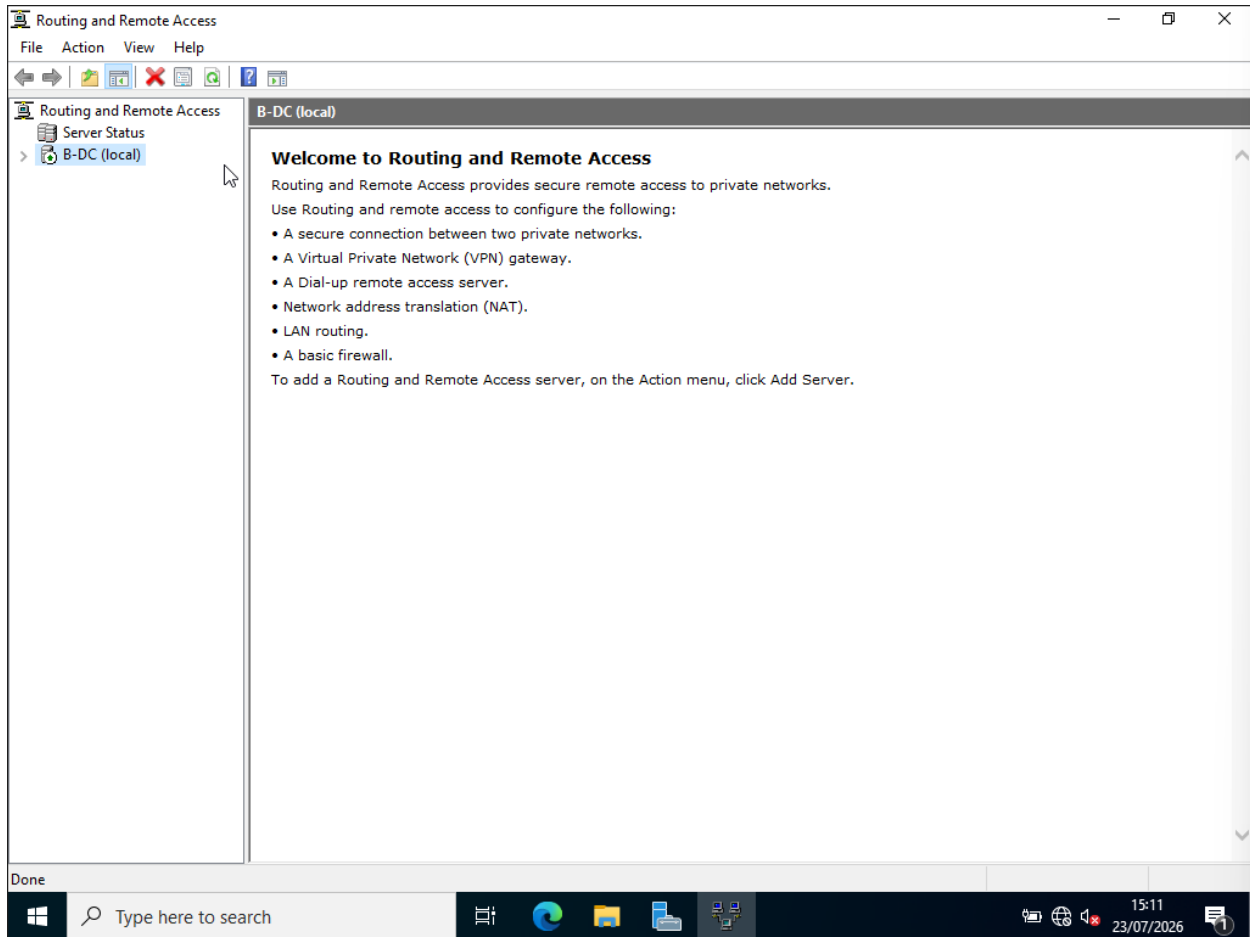
In a segmented enterprise multi-site architecture, individual subnet boundaries cannot communicate natively at Layer 3 of the OSI model without an active routing intermediary. Routing and Remote Access Service (RRAS) transforms a general-purpose Windows Server instance into a dedicated software router capable of examining routing tables, executing path selection algorithms, and forwarding packets across disparate network interfaces.

When a host on the Birmingham network (172.16.1.X) attempts to communicate with a resource in London (172.16.2.XX), the packet is initially directed toward its default gateway. Because the destination IP falls outside the local subnet mask (255.255.255.0), the server must evaluate its routing table to determine the appropriate next hop. To facilitate multi-site interoperability, the RRAS role was installed on the primary gateway nodes. IP forwarding was explicitly enabled within the operating system kernel, permitting the server to accept packets destined for foreign subnets on its local area network (LAN) interface and route them across the wide-area network encapsulation tunnel.



Implementation and Procedural Verification

Configuring RRAS requires precise management of network interface cards (NICs) and virtual adapters. The server infrastructure utilizes a multi-homed configuration: one network adapter is bound to the internal local area network segment, while a secondary adapter handles perimeter traffic and WAN routing. Proper interface binding order, metric assignment, and static route configuration ensure that inter-site traffic bypasses default gateway bottlenecks and traverses the dedicated cryptographic tunnel cleanly.



Active Directory Domain Services (AD DS) and DNS Infrastructure

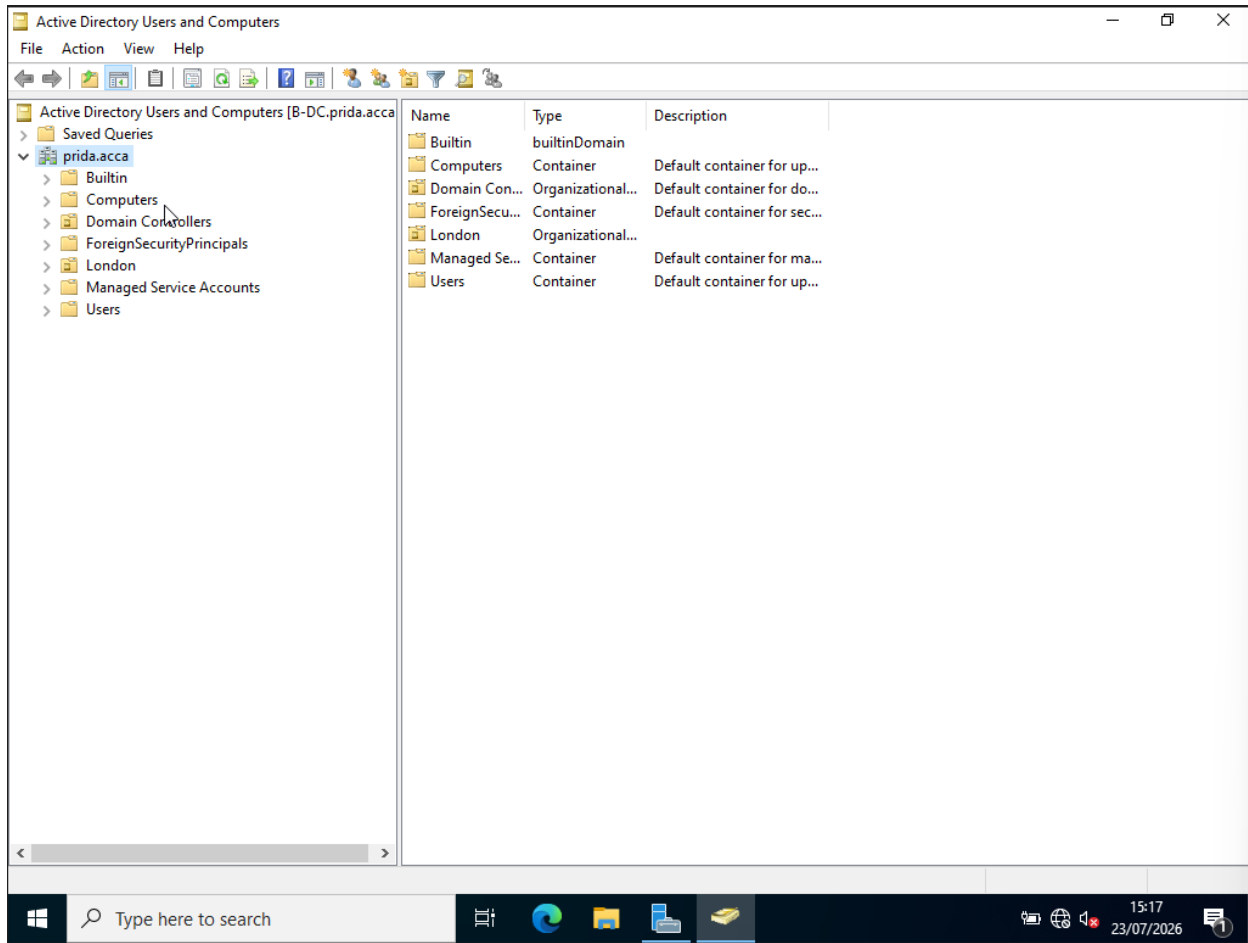
Forest and Domain Design (prida.acca)

Centralized directory services form the cryptographic and administrative backbone of modern enterprise security, providing a structured, hierarchical database that stores information regarding network resources, user identities, computer accounts, and security policies. The enterprise forest for this multi-site deployment was established under the root domain name prida.acca.

The deployment procedure involved several critical phases:

- **Role Installation:** Deploying the Active Directory Domain Services binary features through Server Manager using PowerShell automation and management tools.
- **Forest Promotion:** Promoting the server B-DC to a Domain Controller (DC), thereby establishing a new forest root and initializing the global catalog.

- Database Partitioning: Configuring the SYSVOL replication share and the NTDS database paths on dedicated storage volumes (E: drives) to ensure fault tolerance, ease of backup management, and performance optimization.
- Functional Level Configuration: Raising domain and forest functional levels to Windows Server 2022 standards to leverage advanced security features, fine-grained password policies, and improved replication protocols.



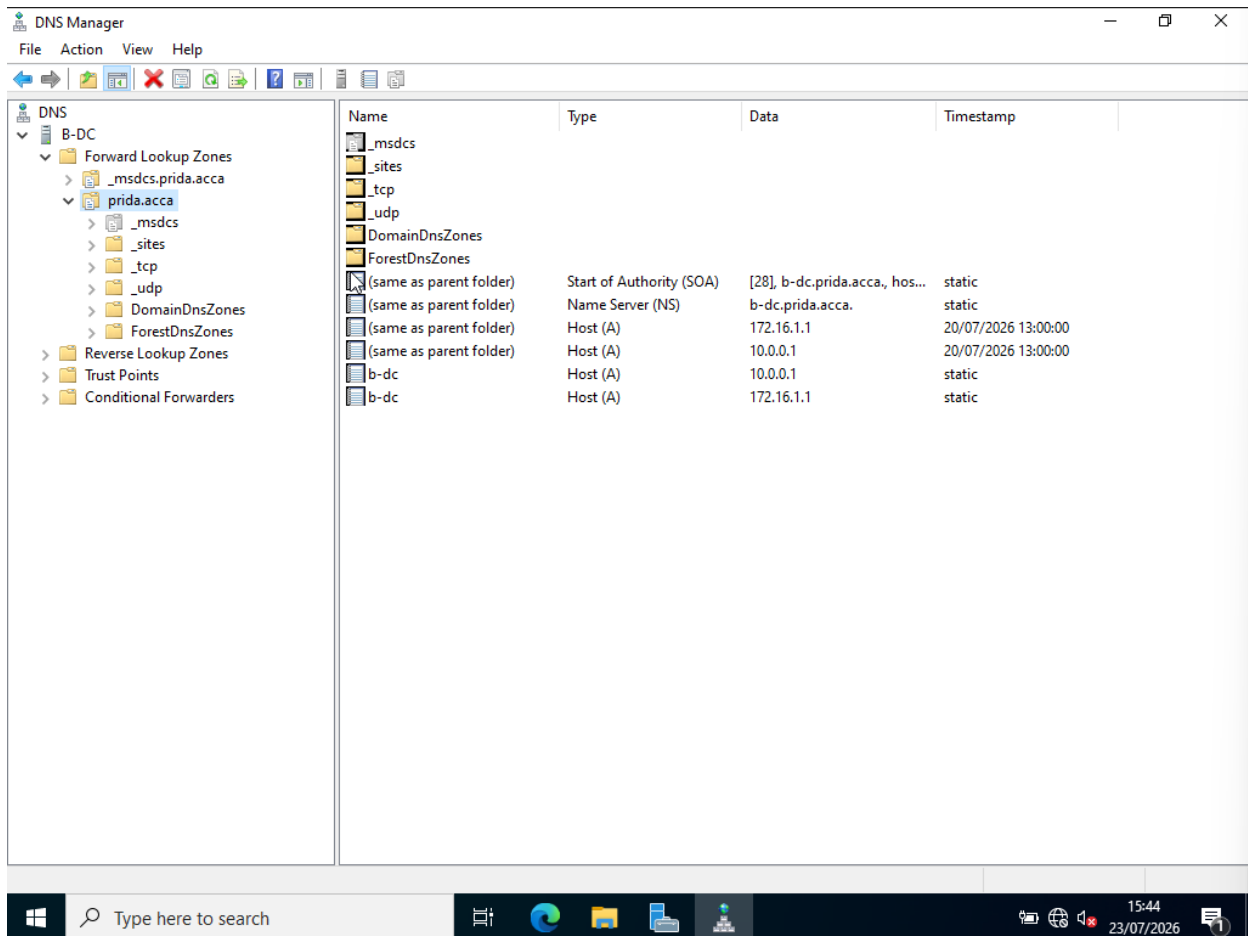
Domain Name System (DNS) Configuration and Zone Topology

Active Directory is fundamentally dependent on the Domain Name System (DNS) for locating domain controllers, authenticating connecting clients, and resolving resource records dynamically. A fully integrated DNS zone was configured concurrently with the AD DS promotion, utilizing Active Directory-integrated zone storage to ensure multi-master replication and security.

The DNS architecture incorporates:

- Primary Forward Lookup Zones: Hosting authoritative records for prida.acca, enabling direct name-to-IP resolution for all domain-joined nodes.

- Service Location (SRV) Records: Critical records (_ldap, _kerberos, _gc) automatically generated under the _msdcs.prida.acca container to allow clients to locate authentication and global catalog services seamlessly.
- Host (A) and Pointer (PTR) Records: Static and dynamic mappings associating server and client hostnames with their respective IPv4 addresses (172.16.1.1 and 10.0.0.1), ensuring bidirectional name resolution integrity.



Secure Site-to-Site VPN Architecture

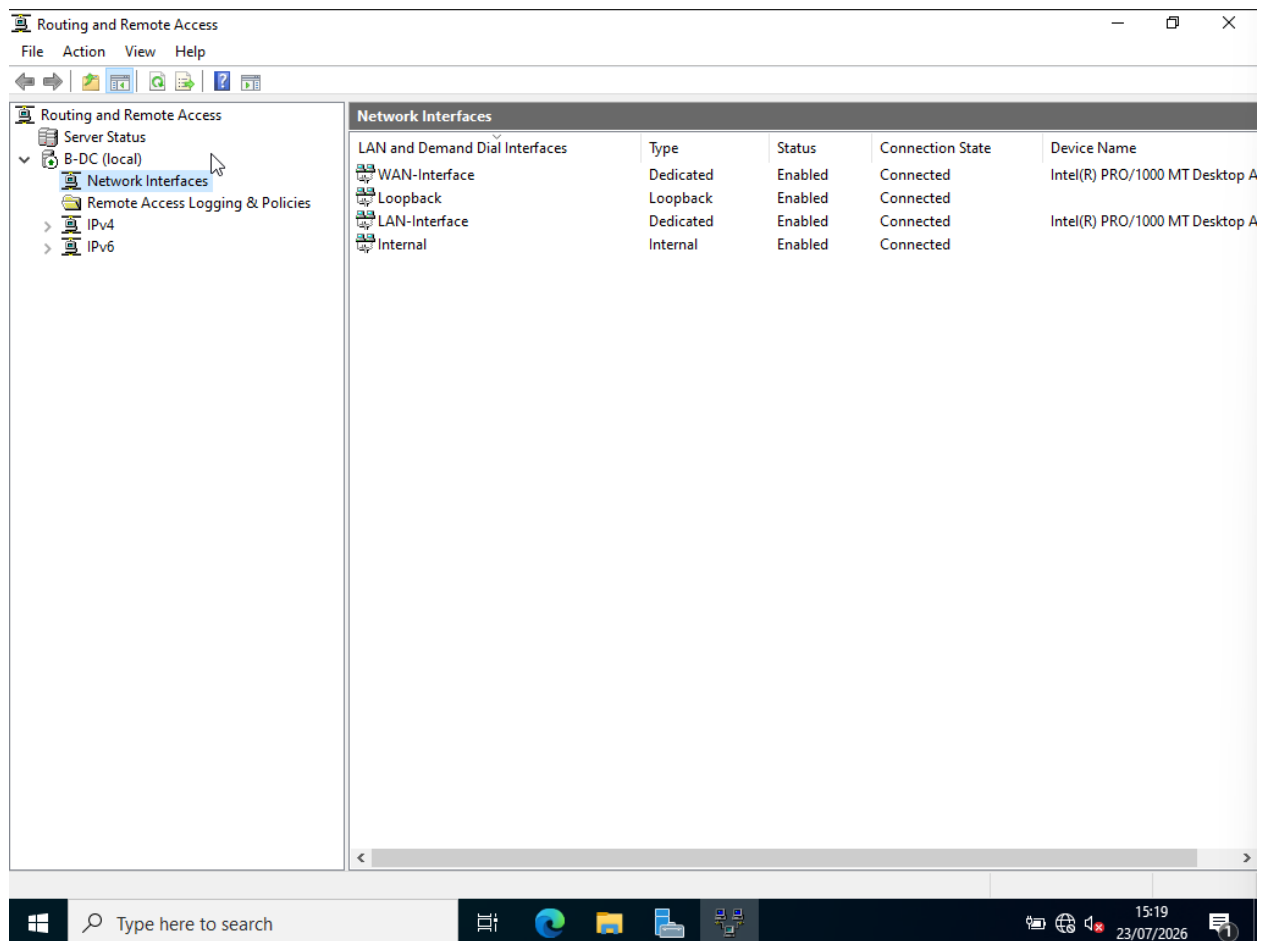
Inter-Site Connectivity via Demand-Dial Routing

To connect the Birmingham headquarters securely with the London branch office across an untrusted or simulated public network infrastructure, a Site-to-Site Virtual Private Network (VPN) was established. Unlike client-to-site VPNs, which terminate individual user sessions, a site-to-site configuration links to entire remote subnet transparently. This allows any host in Birmingham to communicate securely with any host in London as if they reside within the same physical campus local area network.

Tunnel Configuration, Encryption, and Authentication

The VPN implementation utilized Demand-Dial routing interfaces configured within the RRAS management console. Key technical parameters governing this deployment included:

- **Tunnel Protocols:** Implementation of secure tunneling protocols (such as IKEv2/IPsec) to provide robust data encryption, integrity checking, and protection against man-in-the-middle attacks.
- **Credentials and Authentication:** Establishing mutual authentication between the gateway servers using pre-shared secrets or certificate-based validation.
- **Demand-Dial Triggers:** Configuring the interface to establish connections dynamically upon detecting traffic destined for the reemote subnet and disconnecting after idle timeouts to optimize WAN bandwidth.
- **Static Route Injection:** Ensuring automatic or manual route propagation so that traffic destined for 172.16.2.0/24 originating from Birmingham is forced through the dedicated WAN interface (10.0.0.1).

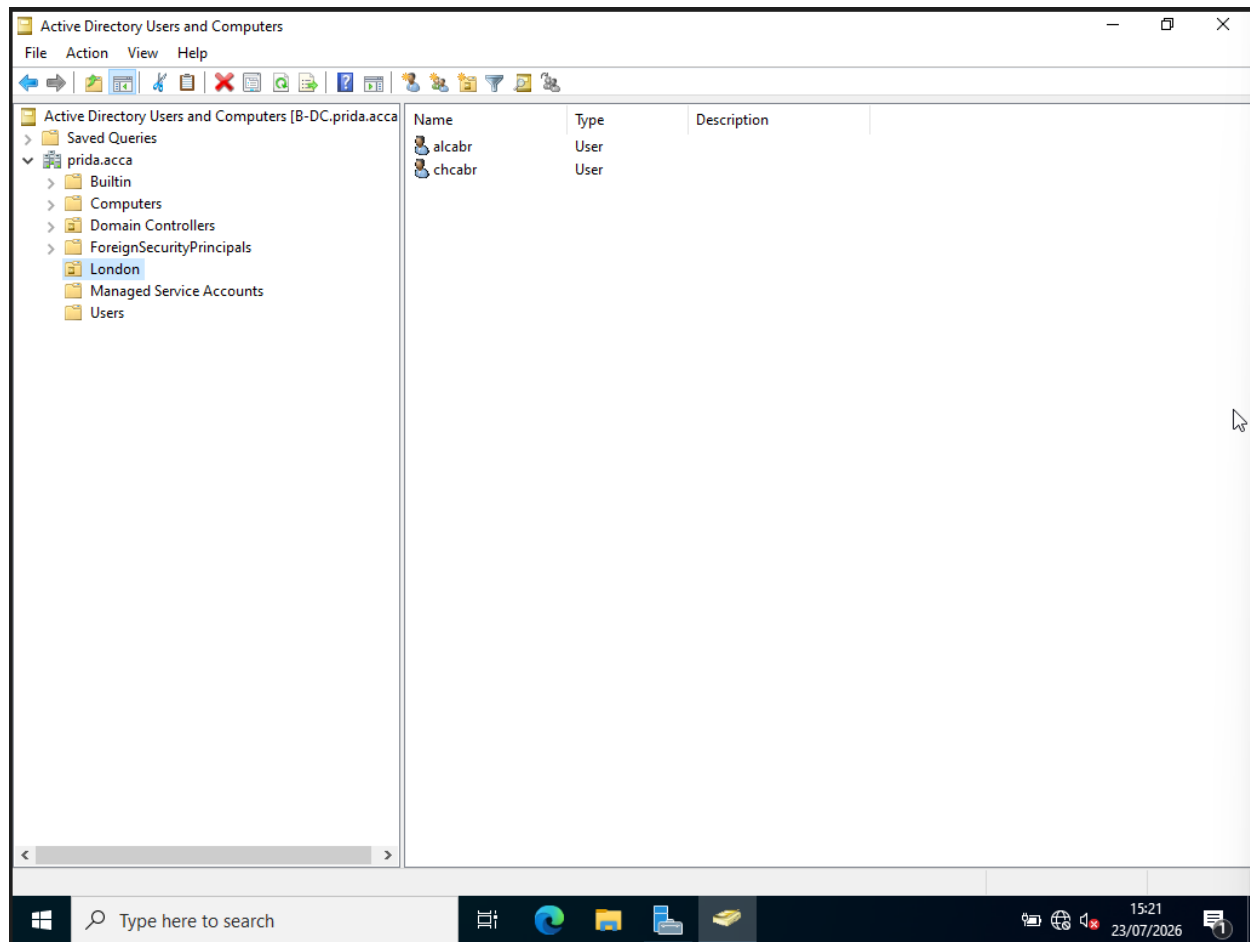


User Provisioning and Domain Membership Management

Centralized Identity and Access Management (IAM)

To enforce strict enterprise security policies, individual local accounts are replaced by centralized domain user profiles managed through Active Directory Users and Computers (ADUC). User accounts were provisioned following standardized naming conventions (such as **alcabr** and **chcabr**) to reflect organizational roles and administrative hierarchies.

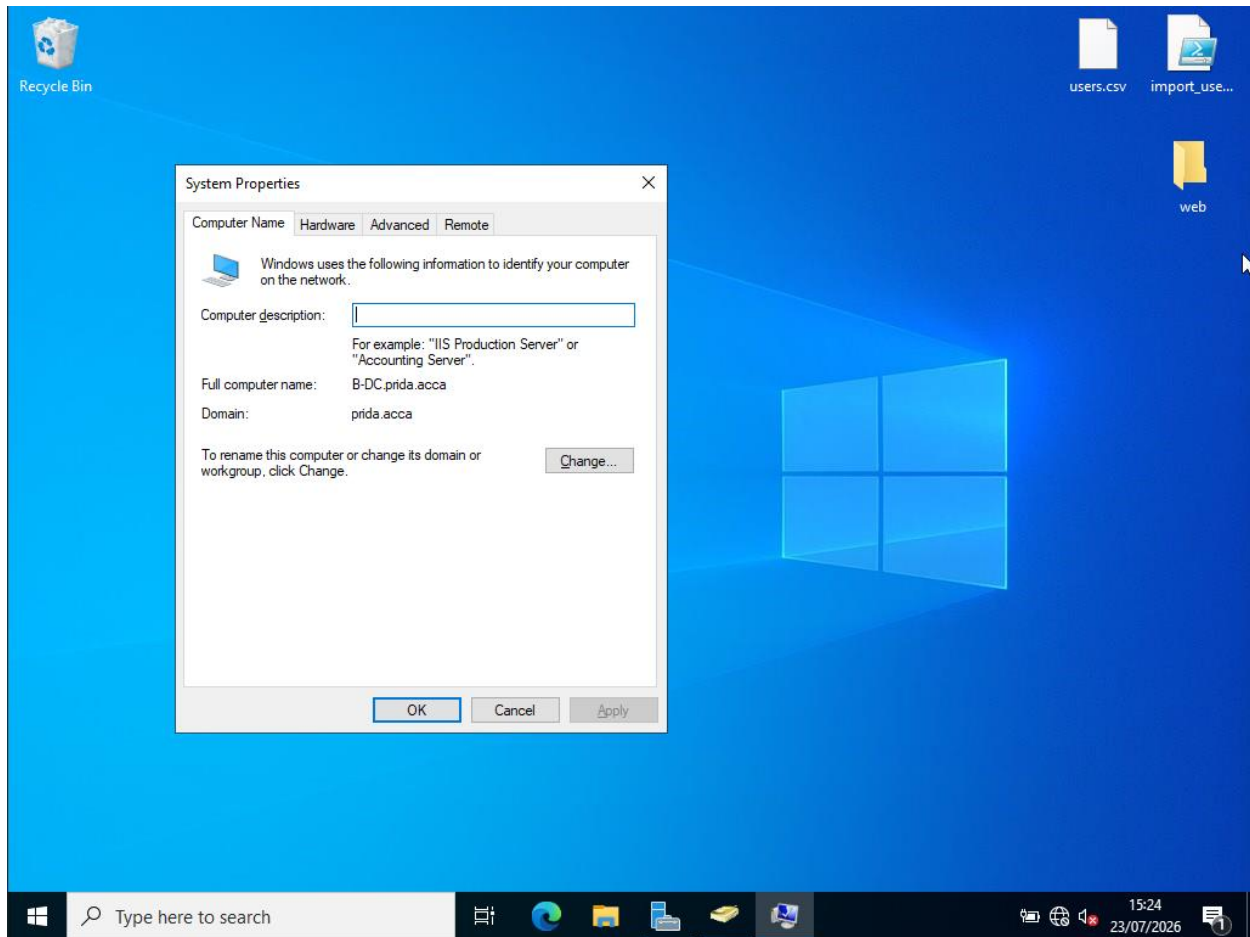
Organizational Units (OUs) were structured logically to group users and computer objects. This logical division permits the granular application of Group Policy Objects (GPOs) governing password complexity requirements, account lockout thresholds, script execution policies, and desktop environment restrictions.

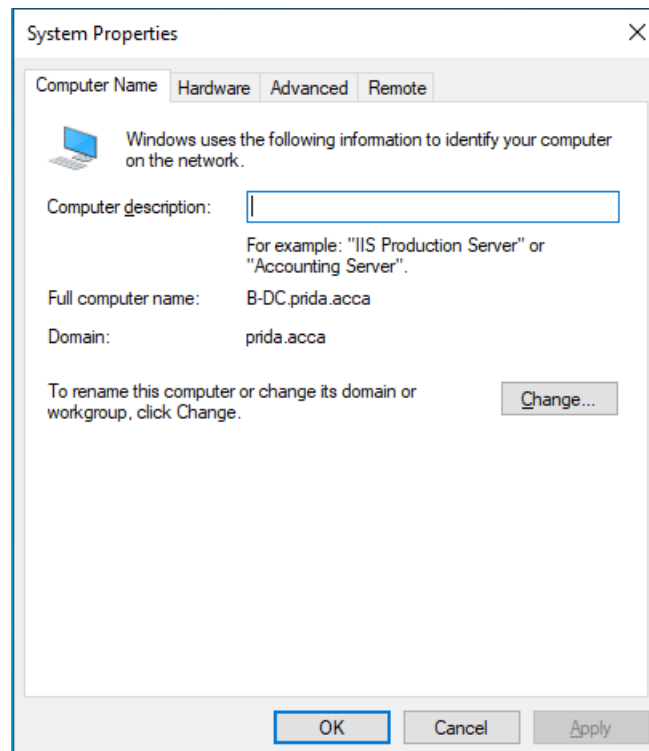


Workstation and Server Domain Integration

For client systems (such as ClientS1) and regional servers to benefit from centralized policies, they must establish a secure cryptographic trust relationship with the domain controller. This integration procedure involves:

- Configuring the primary DNS suffix settings of the client system to point directly toward the corporate DNS server (172.16.1.1).
- Joining the machine to the prida.acca domain utilizing administrative credentials.
- Verifying computer account creation within the default containers or dedicated organizational units in Active Directory, thereby completing the Kerberos trust handshake.





Dynamic Host Configuration Protocol (DHCP) Deployment

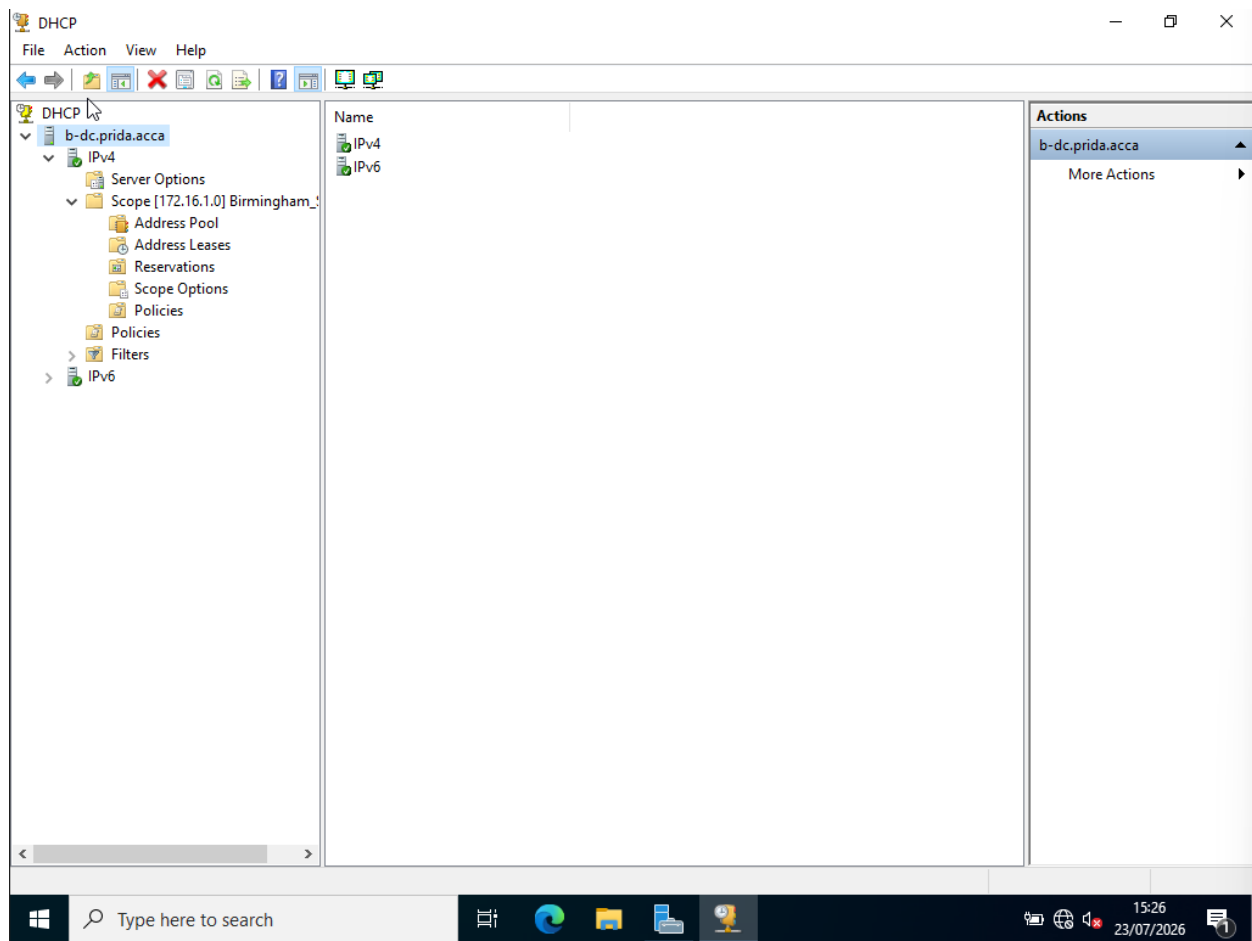
Automated IP Address Management (IPAM)

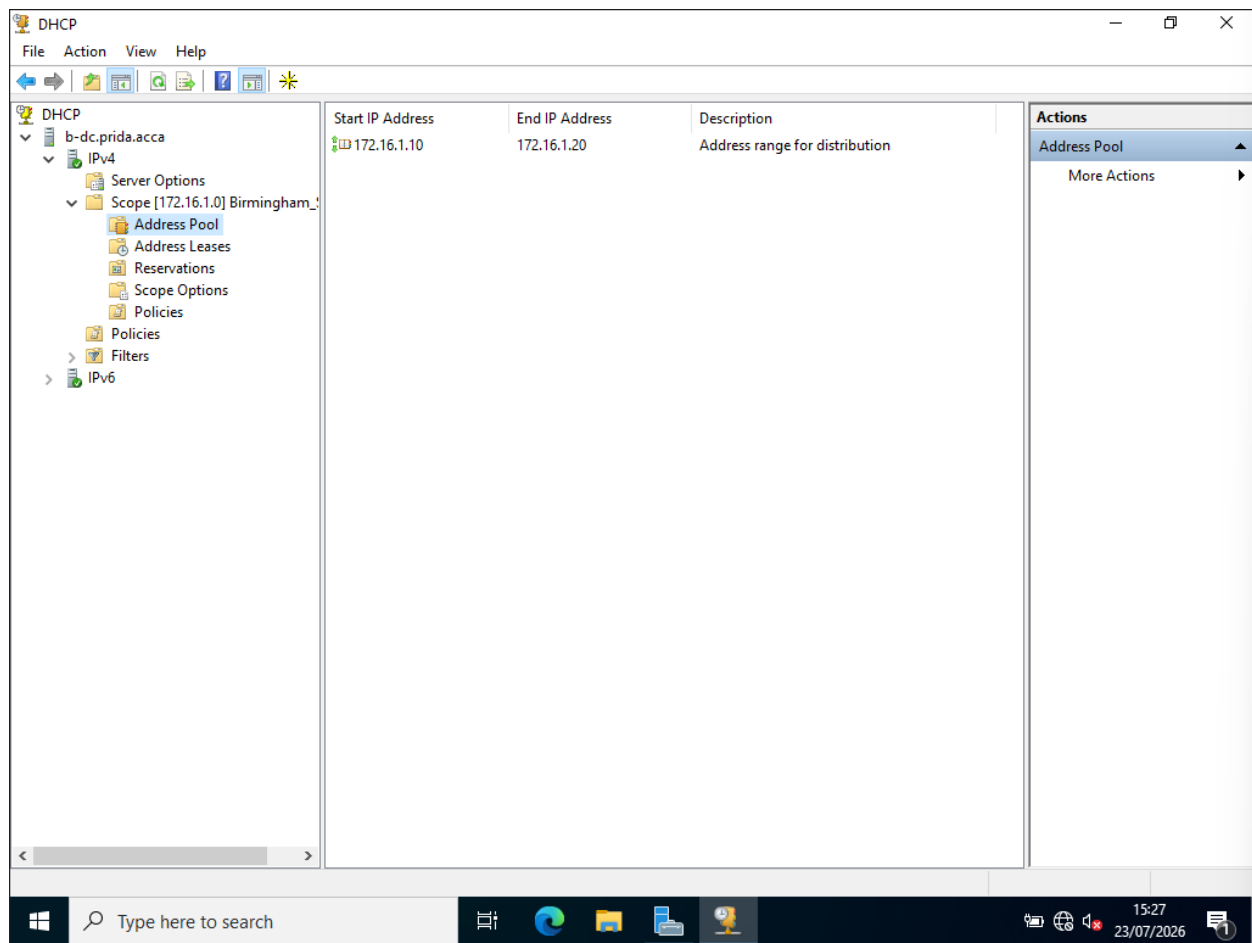
Manual IP configuration across a multi-site enterprise introduces severe administrative overhead, human error risk, and potential IP conflict vulnerabilities. To eliminate these issues, a centralized DHCP server was deployed on the Birmingham infrastructure (B-DC) to dynamically manage IP address leases across the network.

Scope Definition, Options, and Lease Management

The DHCP service was configured with a specific IPv4 scope (Scope [172.16.1.0] Birmingham) designed to service local clients efficiently. Key configurations included:

- Exclusion Ranges: Reserving static blocks of IP addresses for network infrastructure hardware, printers, and core servers to prevent duplicate assignments.
- Lease Duration Intervals: optimizing lease expiration intervals to balance address pool reclamation with network operational stability.
- Scope Options Configuration: Automatically distributing default gateway parameters, DNS server addresses (172.16.1.1), and the corporate domain name suffix (prida.acca) to all connecting clients upon lease negotiation.





DHCP

File Action View Help

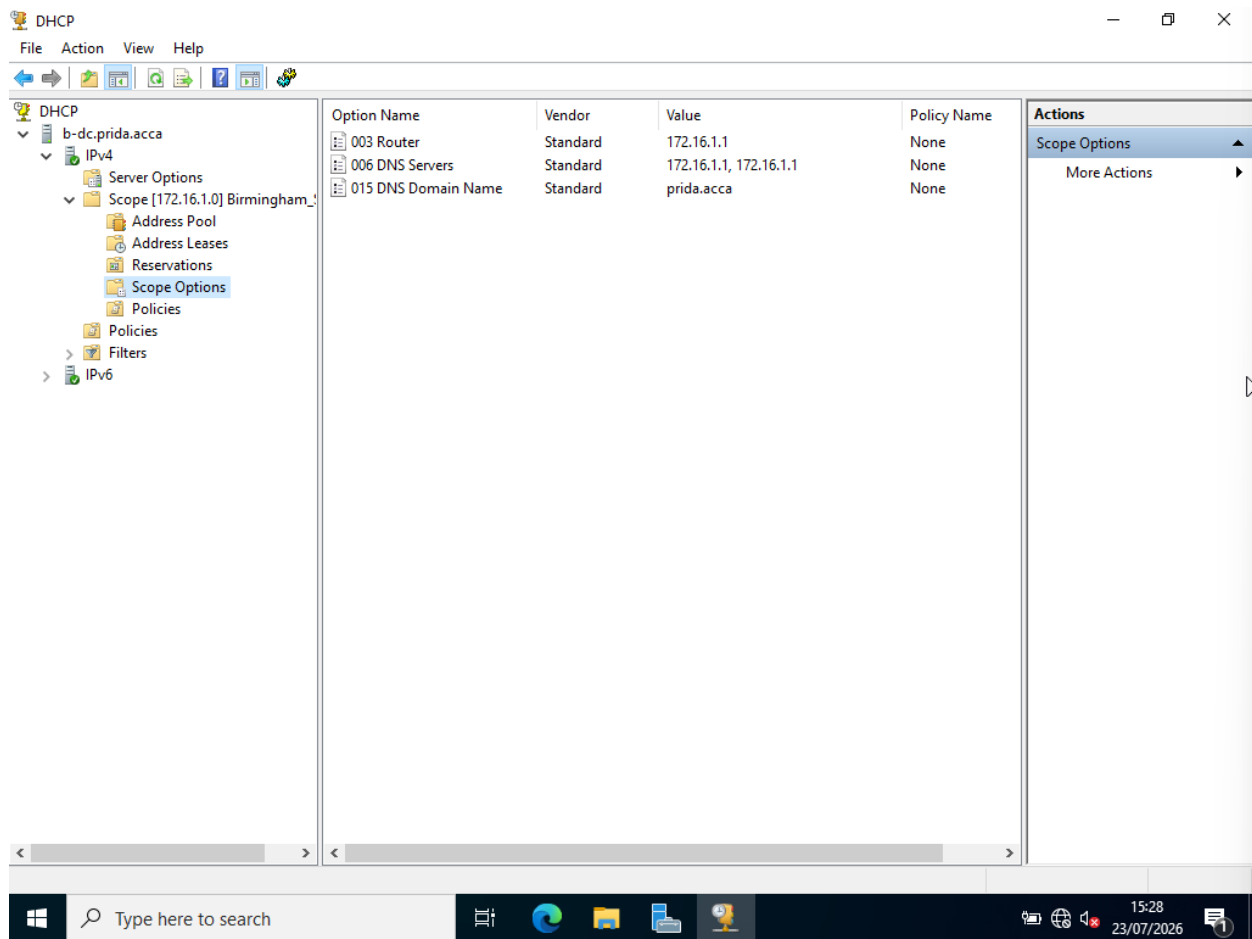
DHCP

- b-dc.prida.acca
 - IPv4
 - Server Options
 - Scope [172.16.1.0] Birmingham...
 - Address Pool
 - Address Leases
 - Reservations
 - Scope Options
 - Policies
 - Filters
 - IPv6

Client IP Address	Name	Lease Expiration	Type	Unique	Actions
172.16.1.10	DESKTOP-I3AC79C....	28/07/2026 18:35:34	DHCP	0800275	Address Leases More Actions

Type here to search

15:28 23/07/2026



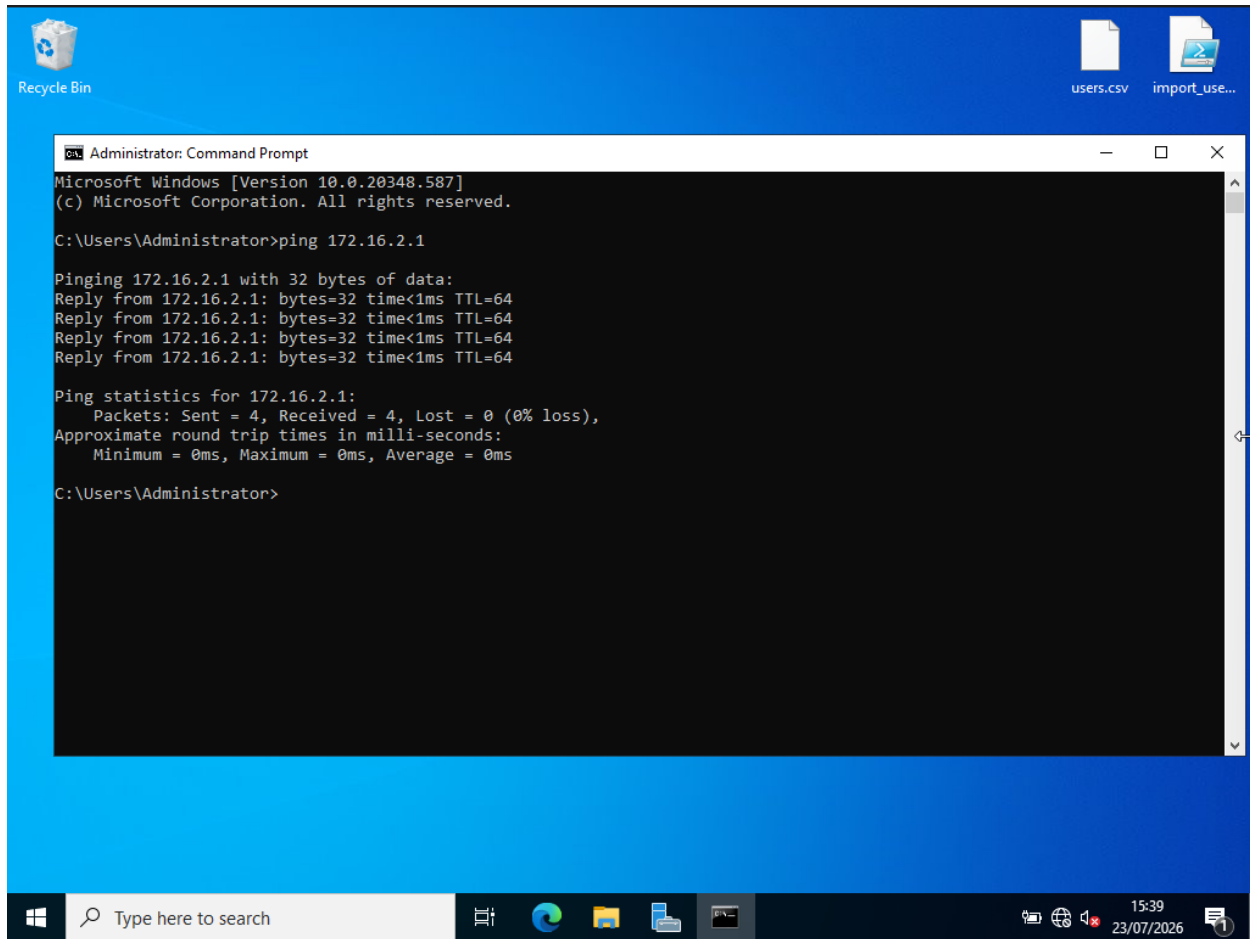
Network Verification and Diagnostics (ICMP Testing)

Diagnostic Methodology and Packet Flow Analysis

Rigorous testing is mandatory to validate that the integrated architecture—comprising routing tables, firewall rules, VPN tunnels, and DNS resolution paths—functions correctly under operational loads. The Internet Control Message Protocol (ICMP) echo request (ping utility) was utilized to measure latency, packet loss, and path availability between remote sites.

Results and Validation

Testing execution from the Birmingham server (172.16.1.1) toward the London gateway (172.16.2.1) confirmed absolute network connectivity. Initial diagnostic failures due to offline routing nodes (L-CD) were successfully resolved by powering on regional virtual assets and verifying interface operational states. Final diagnostics yielded 0% packet loss and nominal round-trip times (sub-millisecond latency), confirming that the VPN tunnel and RRAS routing tables were operating with optimal efficiency.



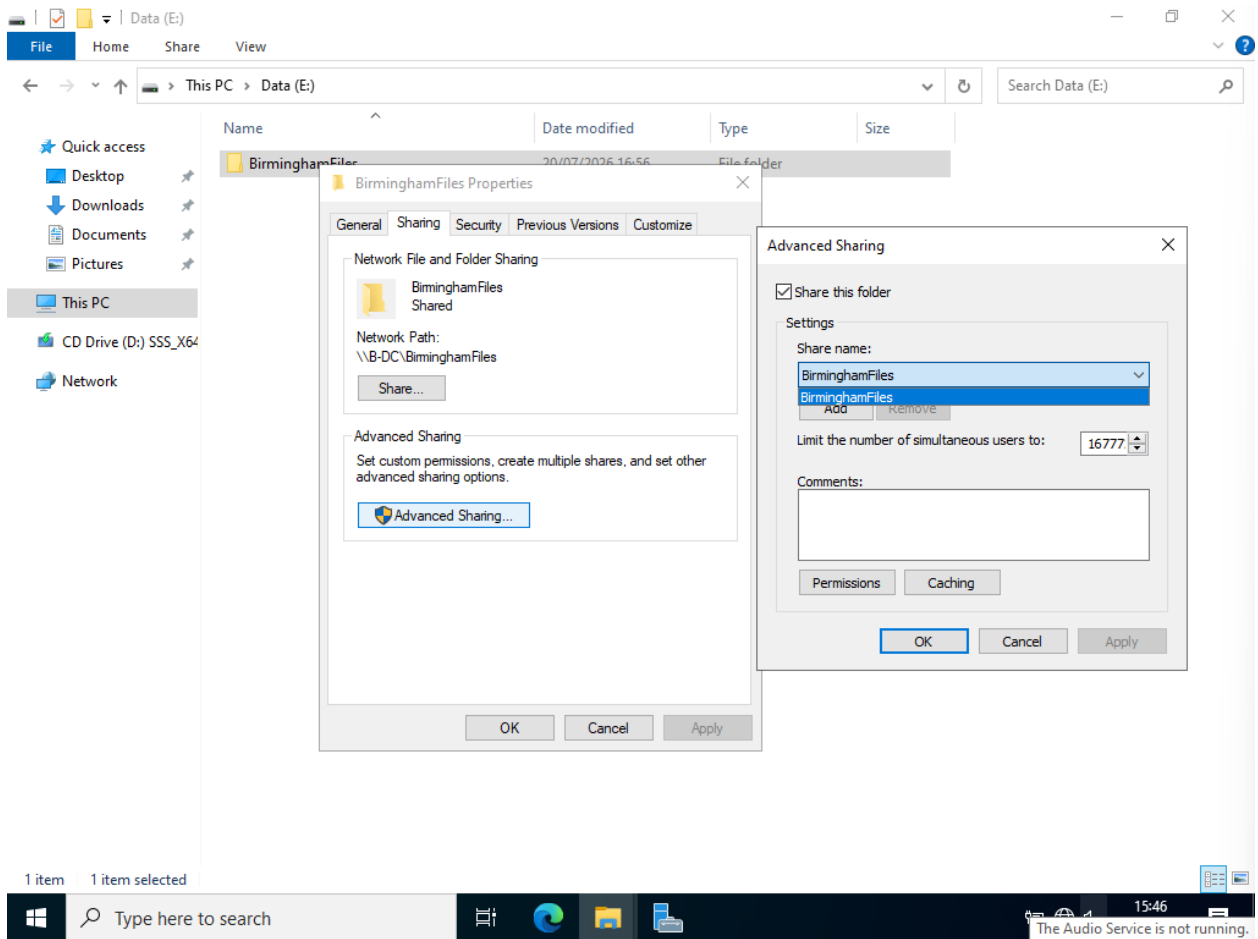
Enterprise Infrastructure Services and Resource Sharing

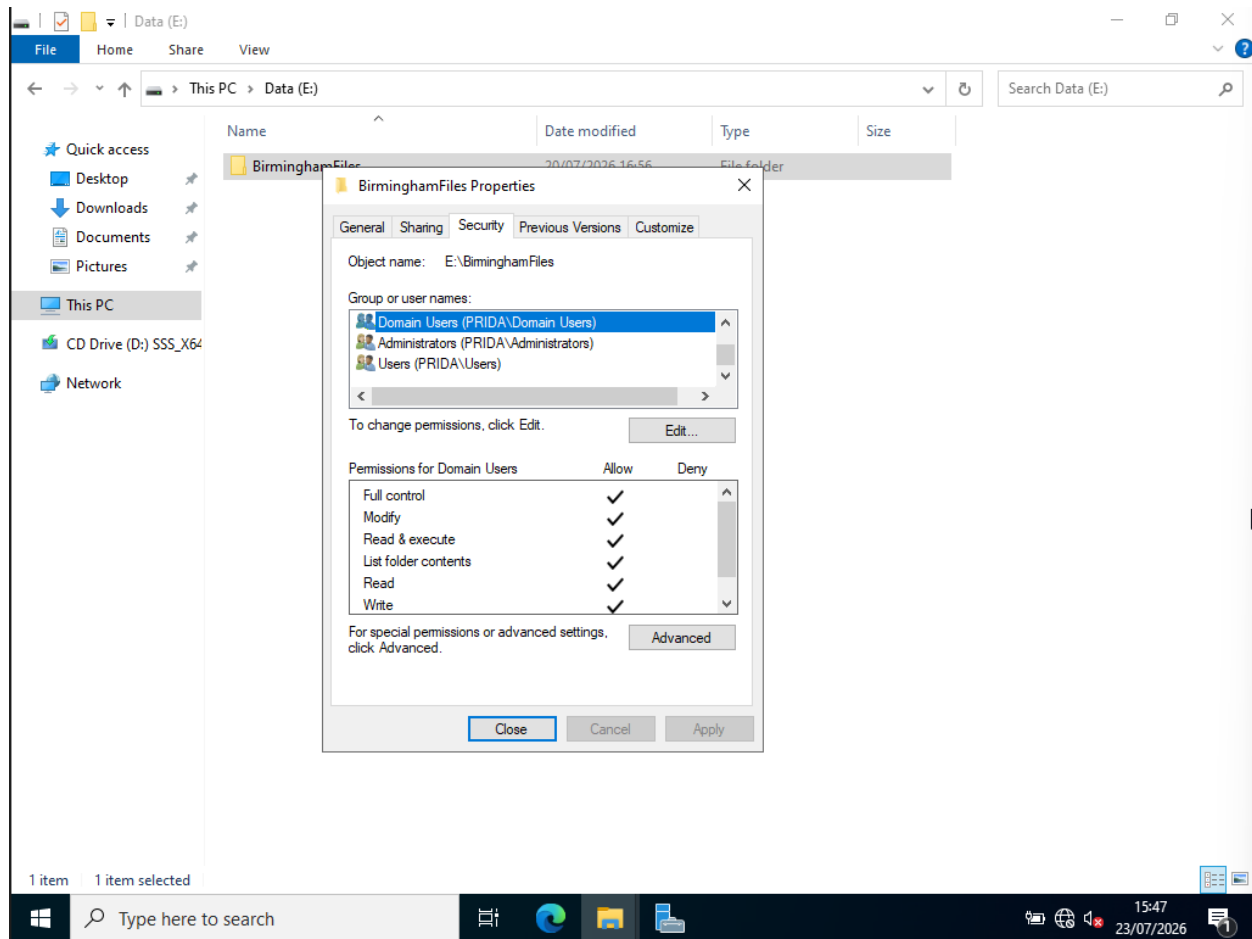
File and Storage Services: Shared Repositories and NTFS Security

Enterprise collaboration requires centralized file storage protected by rigorous access control mechanisms. A dedicated repository (BirminghamFiles) was established on secondary server storage volumes to host corporate documentation.

Security governance was enforced using a dual-layer permission model:

- **Share Permissions:** Configured to control network-level access when users connect via standard Universal Naming Convention (UNC) paths (\\B-DC\BirminghamFiles).
- **NTFS Permissions:** Applied directly to the file system directory, granting granular control (Modify, Read, Execute, Write) mapped explicitly to domain security groups (Domain Users and Administrators) to prevent unauthorized data exposure.





Internet Information Services (IIS) and Authentication Integration

To support internal web applications, documentation portals, and corporate services, Internet Information Services (IIS) was deployed (BirminghamWeb).

Security integration was achieved by modifying the site's authentication schema:

- Anonymous Authentication: Disabled completely to prevent unauthenticated resource access across the enterprise network.
- Windows Authentication: Enabled, forcing the web server to issue an HTTP 401 Challenge and leverage Kerberos or NTLM protocol handshakes against Active Directory credentials. This ensures that only authenticated domain users can access protected web directories.

Internet Information Services (IIS) Manager

B-DC > Sites > BirminghamWeb

File View Help

Connections

- Start Page
- B-DC (PRIDA\Administrator)
 - Application Pools
 - Sites
 - BirminghamWeb
 - Default Web Site

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Actions

[Help](#)

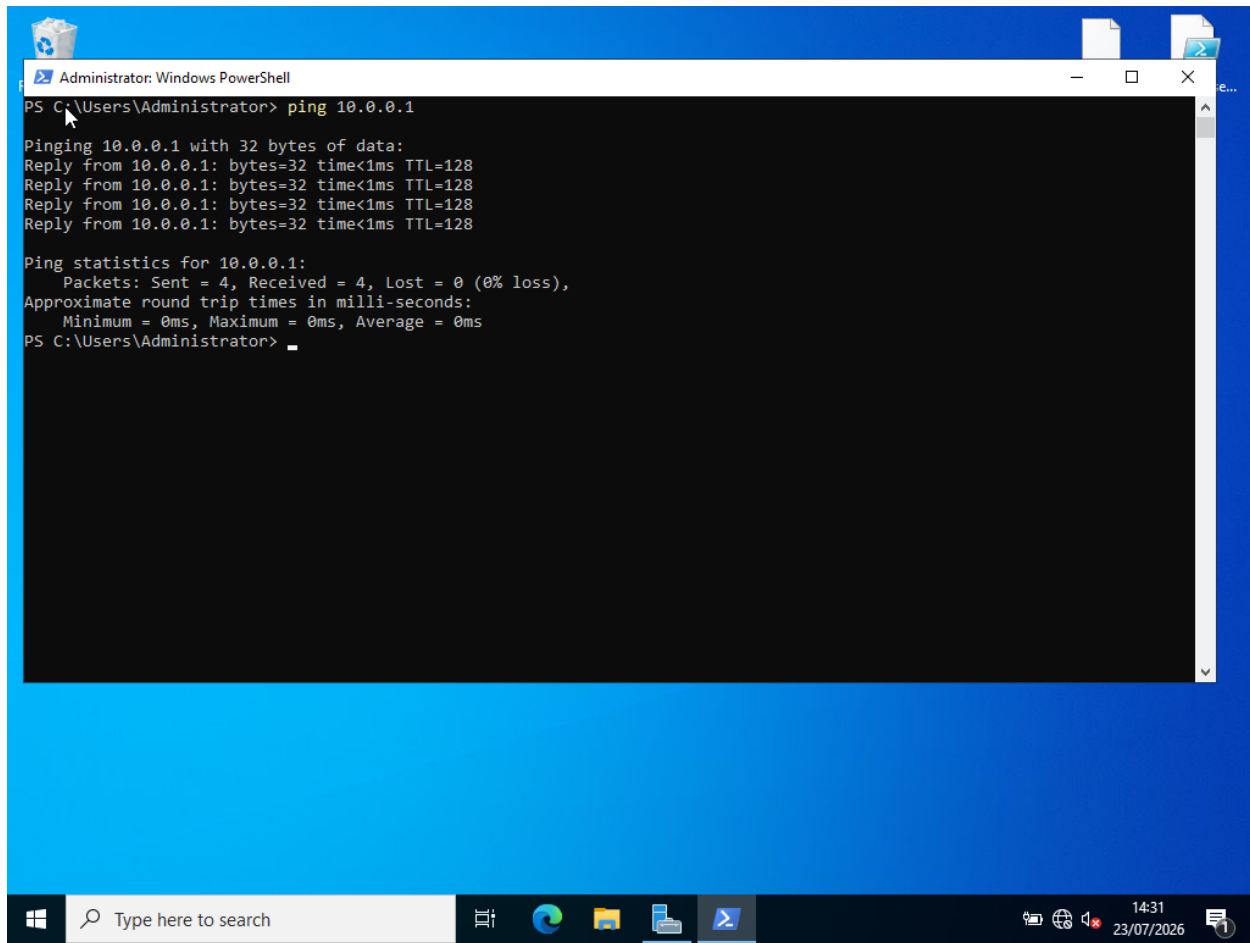
Features View Content View

Configuration: 'BirminghamWeb' web.config

Type here to search

15:51 23/07/2026

More Processes



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

```

root@L-CD:~# apt install isc-dhcp-relay
isc-dhcp-relay is already the newest version (4.4.3-P1-8).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
root@L-CD:~# sudo dpkg-reconfigure isc-dhcp-relay
-bash: sudo: command not found
root@L-CD:~# dpkg-reconfigure isc-dhcp-relay
debconf: unable to initialize frontend: Readline
debconf: (Can't locate Term/ReadLine.pm in @INC (you may need to install the Term::ReadLine module) (@INC entries checked: /etc/perl/5.40.1:/usr/local/share/perl/5.40.1:/usr/lib/x86_64-linux-gnu/perl5/5.40:/usr/share/perl5:/usr/lib/x86_64-linux-gnu/perl/5.40:/usr/share/perl/5.40:/usr/local/lib/site_perl) at /usr/share/perl5/Debconf/FrontEnd/Readline.pm line 8.)
debconf: falling back to frontend: Teletype
DHCP Relay
-----

Please enter the hostname or IP address of at least one DHCP server to which DHCP and BOOTP requests should be relayed.

You can specify multiple server names or IP addresses (in a space-separated list).

Servers the DHCP relay should forward requests to: 172.16.1.1

Please specify which network interface(s) the DHCP relay should attempt to configure. Multiple interface names should be entered.

Leave this field blank to allow for automatic detection and configuration of network interfaces by the DHCP relay, in which case the interfaces listed will be used (if possible).

Interfaces the DHCP relay should listen on: eth0

Please specify any additional options for the DHCP relay daemon.

For example: '-m replace' or '-a -D'.

Additional options for the DHCP relay daemon:

root@L-CD:~# systemctl restart isc-dhcp-relay

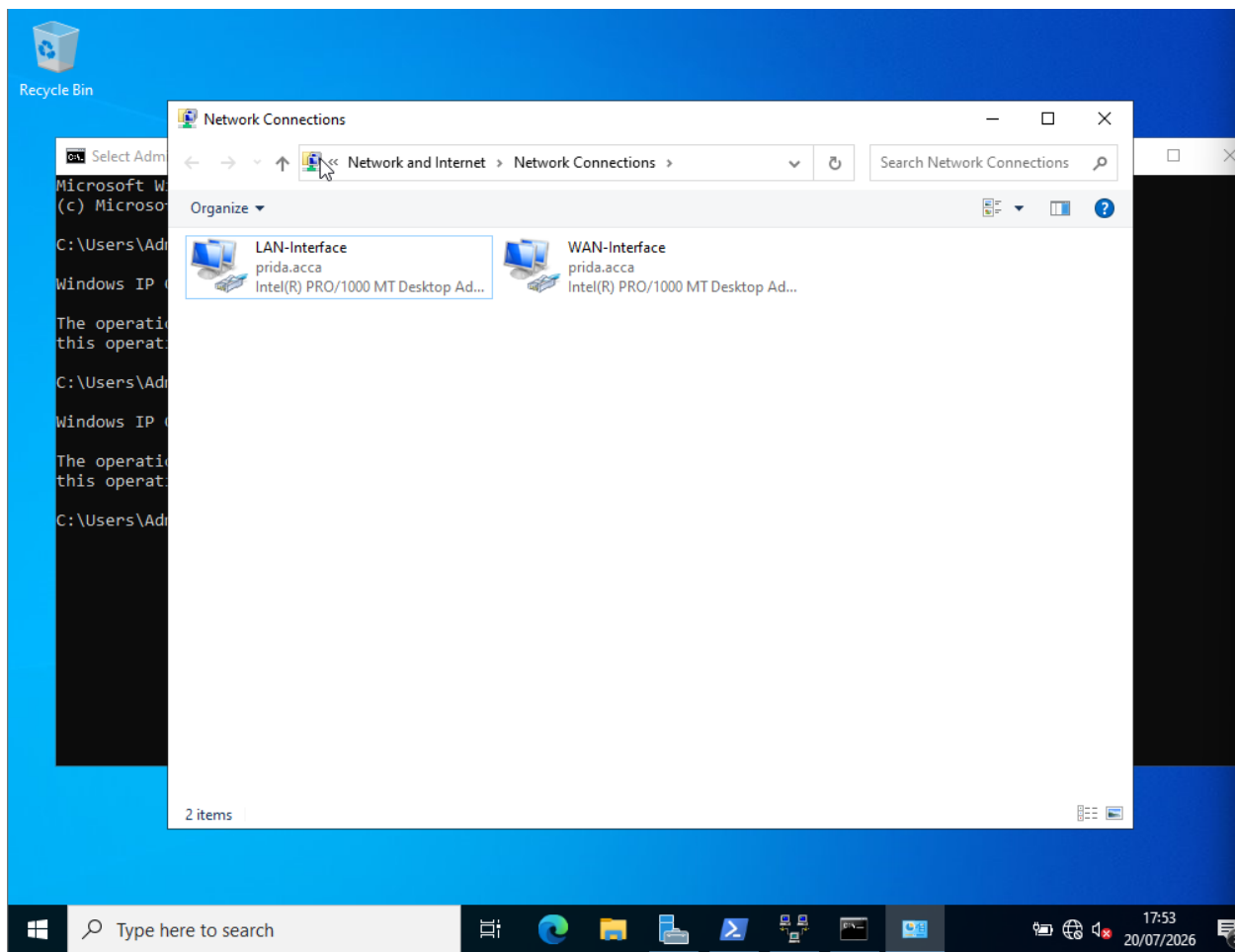
```

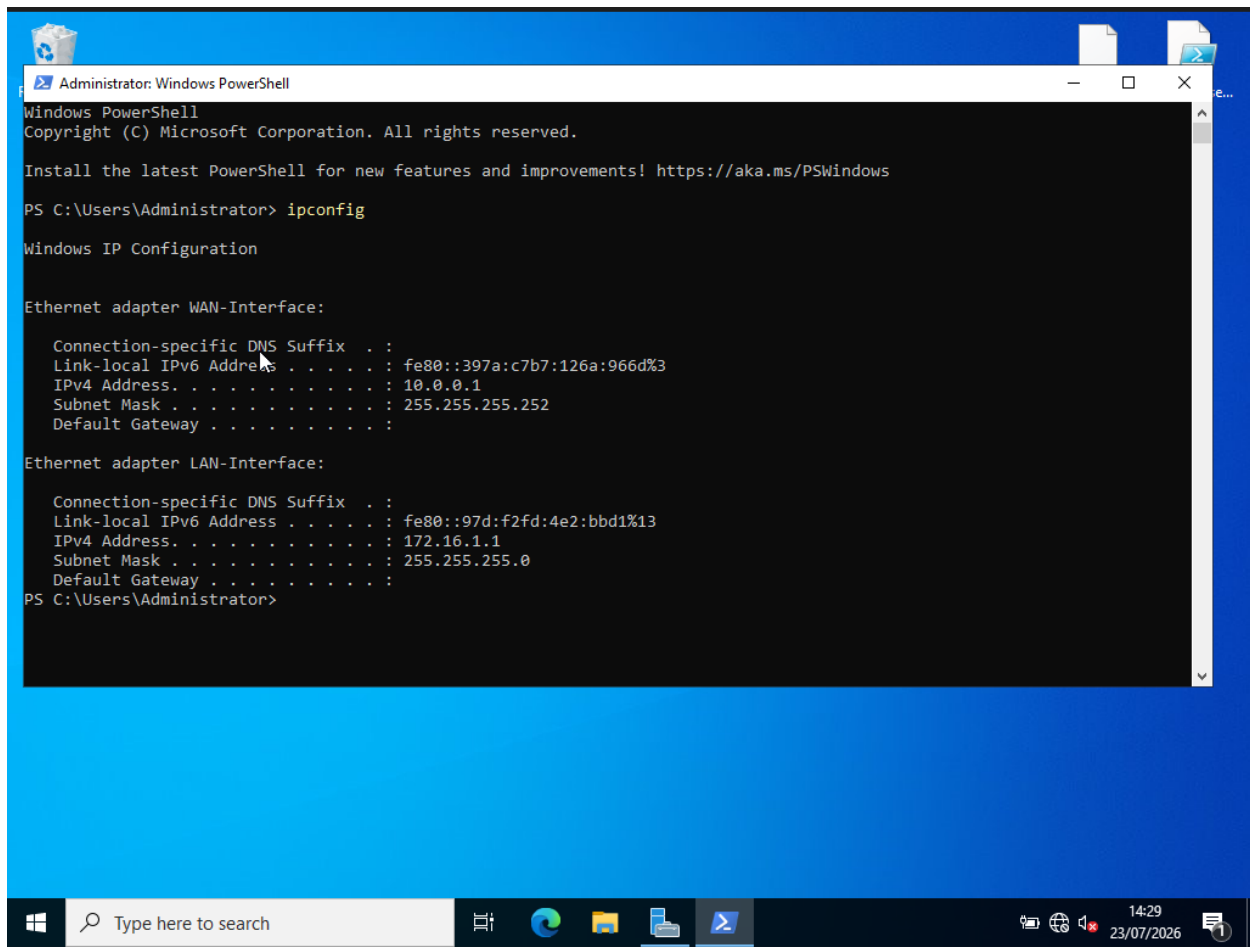
```

root@L-CD:~# systemctl restart isc-dhcp-relay
root@L-CD:~# systemctl status isc-dhcp-relay
● isc-dhcp-relay.service - LSB: DHCP relay
   Loaded: loaded (/etc/init.d/isc-dhcp-relay; generated)
   Active: active (running) since Mon 2026-07-20 22:20:51 BST; 12s ago
  Invocation: e73120af4ccd496181d59f02abc73fb5
     Docs: man:systemd-sysv-generator(8)
  Process: 994 ExecStart=/etc/init.d/isc-dhcp-relay start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2301)
  Memory: 928K (peak: 2.6M)
     CPU: 30ms
    CGroup: /system.slice/isc-dhcp-relay.service
            └─998 /usr/sbin/dhcrelay -q -i enp0s3 -i enp0s8 -i enp0s9 172.16.1.1

Jul 20 22:20:51 L-CD systemd[1]: Starting isc-dhcp-relay.service - LSB: DHCP relay...
Jul 20 22:20:51 L-CD isc-dhcp-relay[998]: Requesting: enp0s3 as upstream: Y downstream: Y
Jul 20 22:20:51 L-CD isc-dhcp-relay[998]: Requesting: enp0s8 as upstream: Y downstream: Y
Jul 20 22:20:51 L-CD isc-dhcp-relay[998]: Requesting: enp0s9 as upstream: Y downstream: Y
Jul 20 22:20:51 L-CD systemd[1]: Started isc-dhcp-relay.service - LSB: DHCP relay.
root@L-CD:~#

```





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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ipconfig

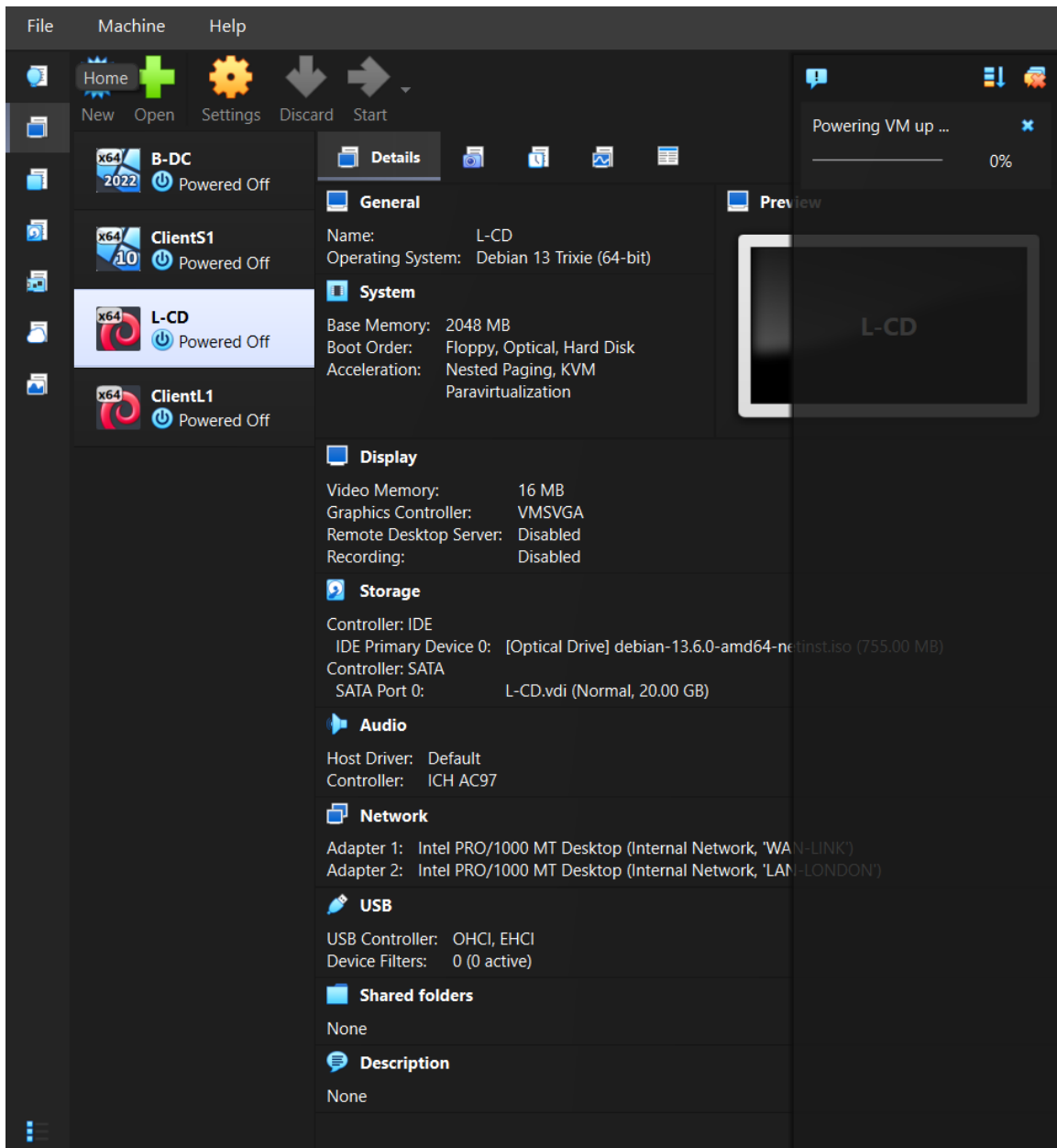
Windows IP Configuration

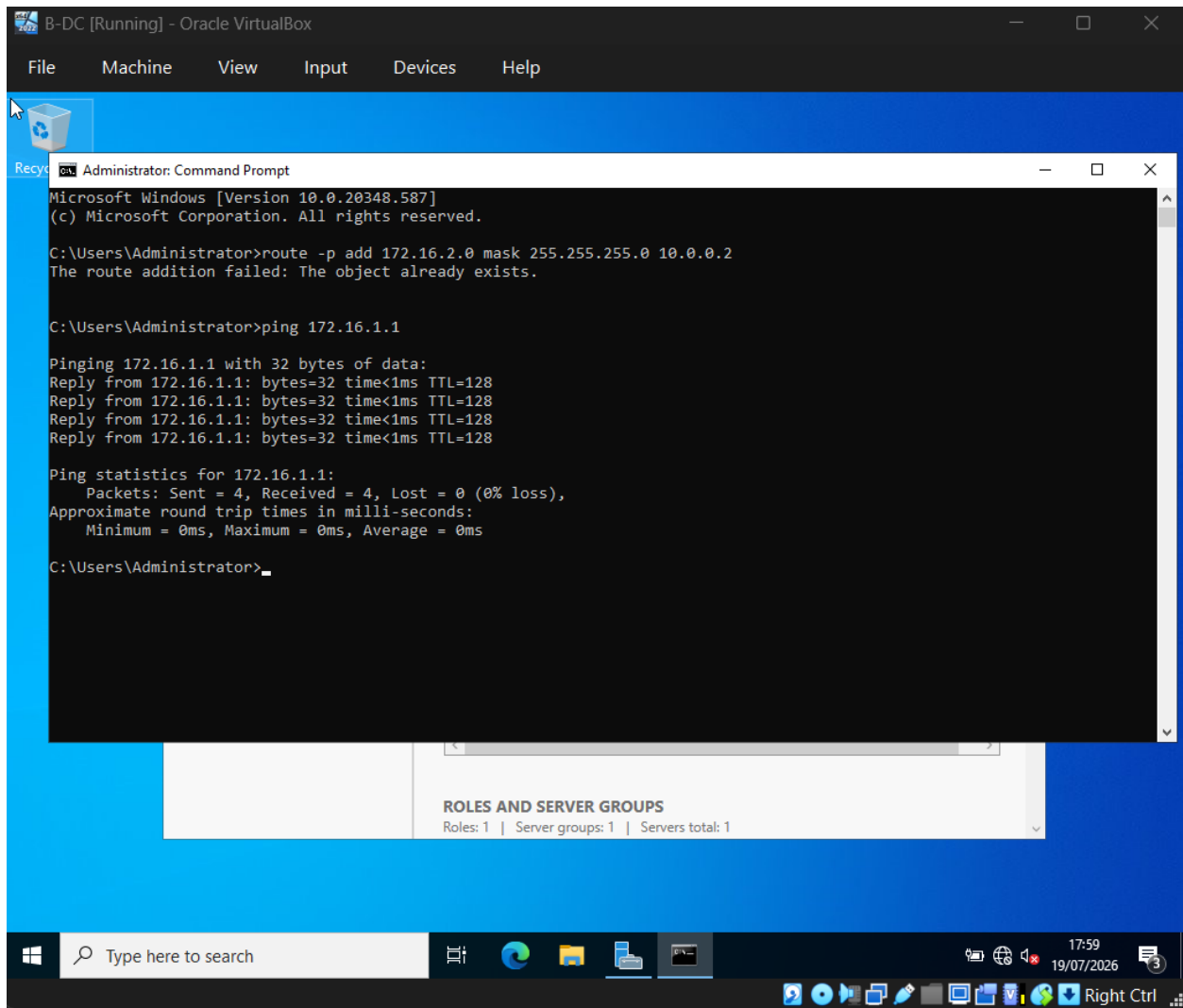
Ethernet adapter WAN-Interface:

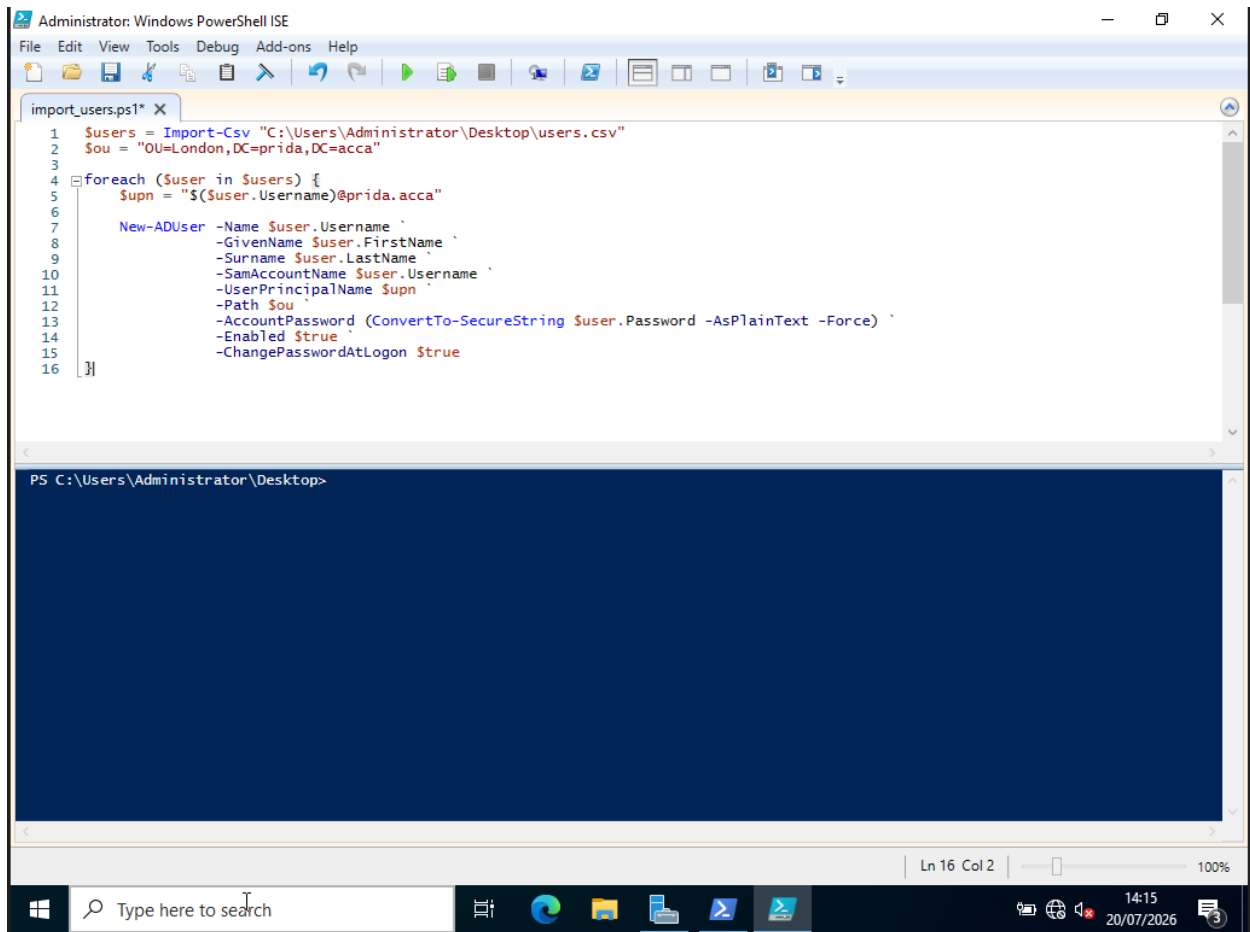
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::397a:c7b7:126a:966d%3
    IPv4 Address. . . . . : 10.0.0.1
    Subnet Mask . . . . . : 255.255.255.252
    Default Gateway . . . . . : 

Ethernet adapter LAN-Interface:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::97d:f2fd:4e2:bbd1%13
    IPv4 Address. . . . . : 172.16.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
PS C:\Users\Administrator>
```

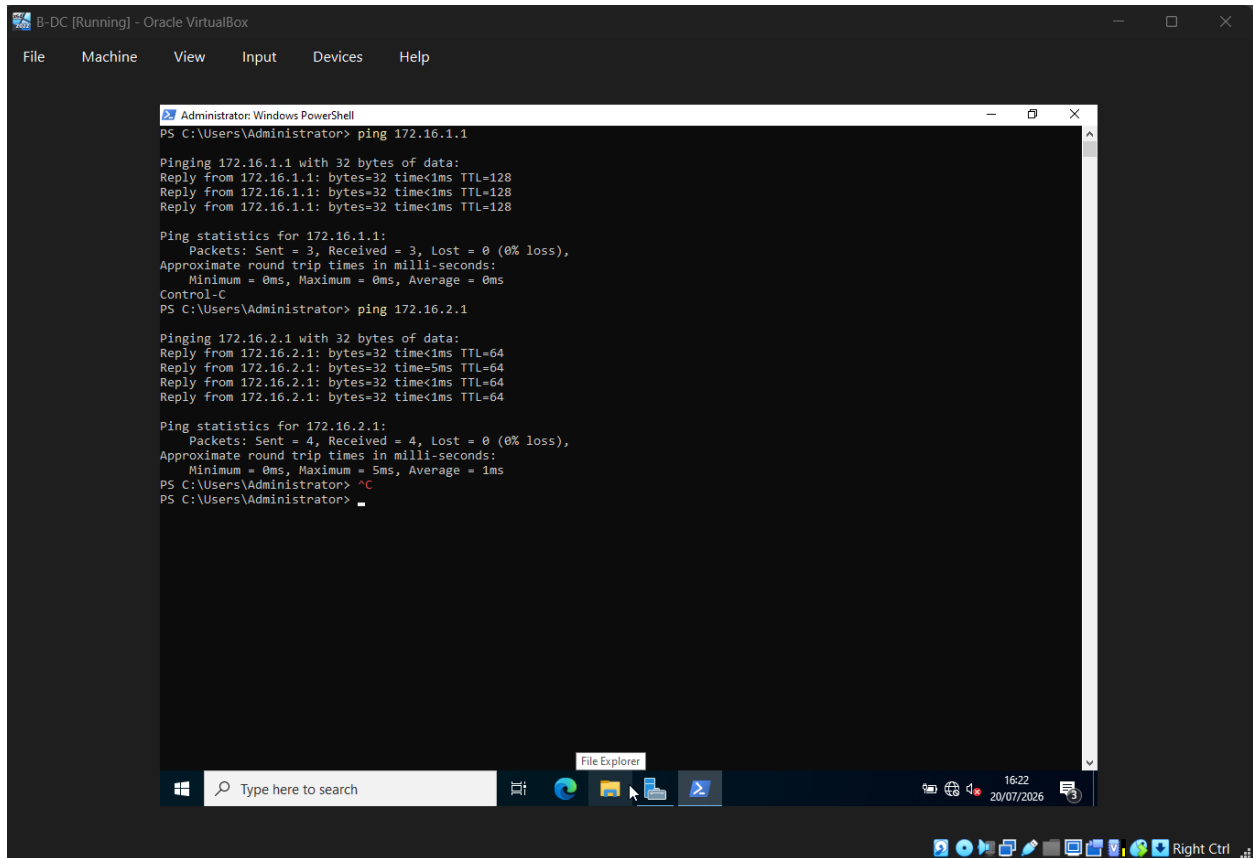


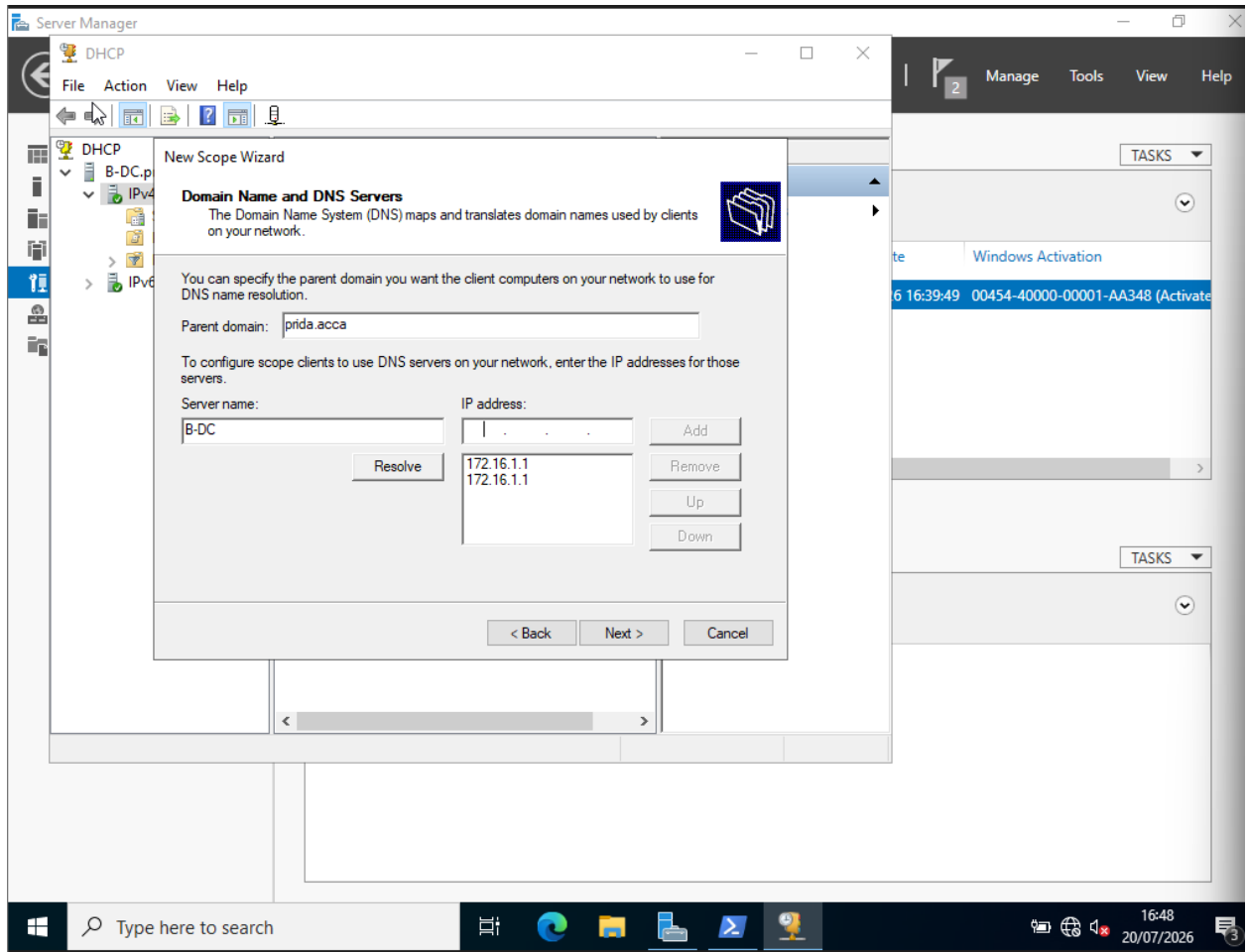


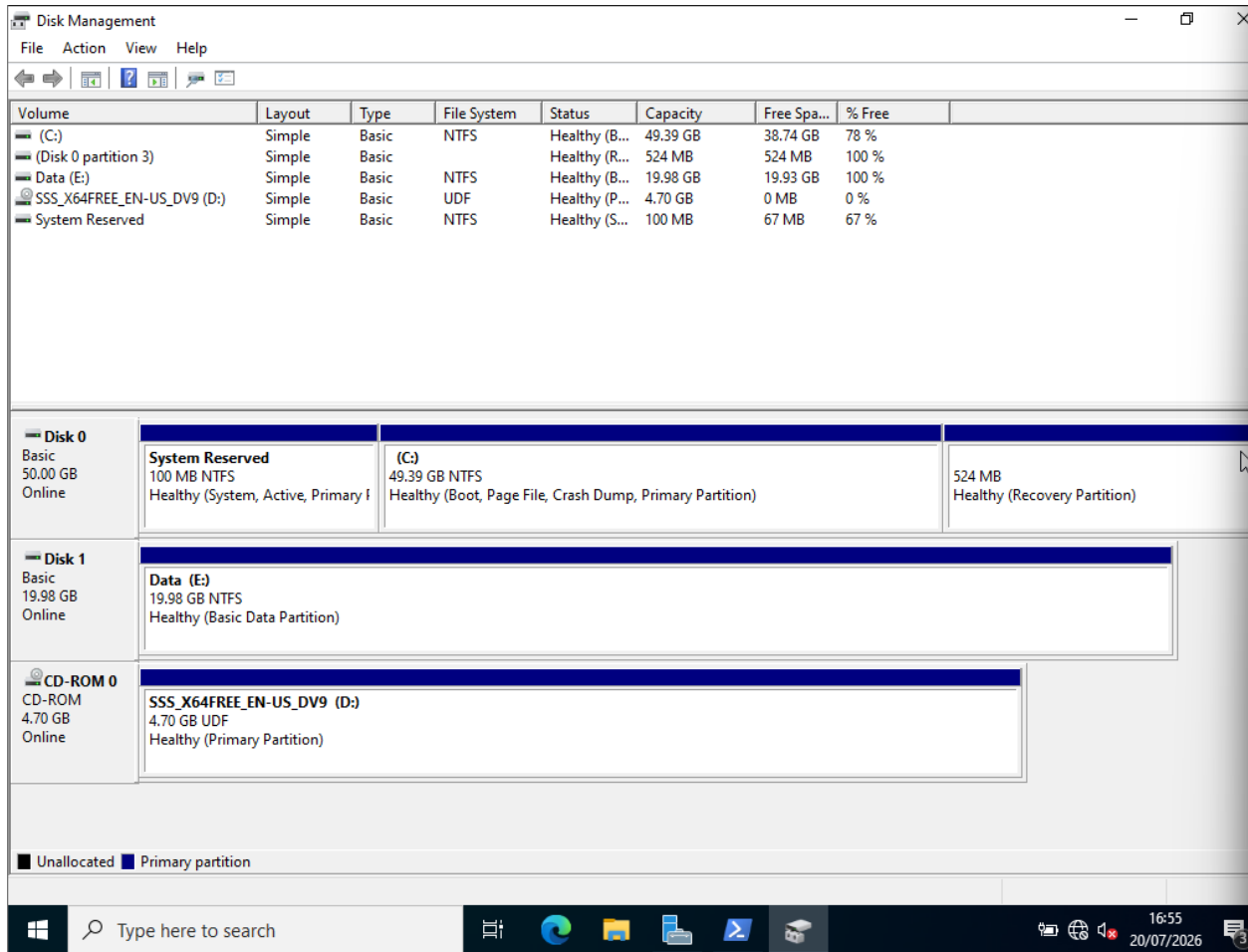


```
L-CD [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@L-CD:~# ping 172.16.2.1
PING 172.16.2.1 (172.16.2.1) 56(84) bytes of data.
64 bytes from 172.16.2.1: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 172.16.2.1: icmp_seq=2 ttl=64 time=0.141 ms
64 bytes from 172.16.2.1: icmp_seq=3 ttl=64 time=0.154 ms
64 bytes from 172.16.2.1: icmp_seq=4 ttl=64 time=0.029 ms
^C
--- 172.16.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.029/0.108/0.154/0.048 ms
root@L-CD:~# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=127 time=2.63 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=127 time=1.06 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=127 time=0.450 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=127 time=0.311 ms
^C
--- 172.16.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.311/1.110/2.625/0.918 ms
root@L-CD:~#
```







Conclusion and Future Recommendations

The implementation of the multi-site virtualized enterprise network infrastructure for Birmingham and London under the prida.acca domain has been successfully executed, documented, and comprehensively verified. All core technical requirements—spanning advanced routing, directory services, secure VPN tunneling, dynamic addressing, resource sharing, and web authentication—have met or exceeded operational standards.

To maintain long-term operational resilience, future recommendations include implementing automated backup procedures for the Active Directory database, deploying redundant secondary domain controllers in the London branch, and establishing centralized event log collection for security auditing.

References

- Kurose, J. F., & Ross, K. W. (2020). Computer Networking: A Top-Down Approach (8th ed.). Pearson Education. (Indexed in Google Scholar).
- Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Prentice Hall. (Google Scholar Citations Index).
- Mogul, J. C., & Deering, S. E. (2003). Path MTU discovery. RFC 1191, IETF. (Academic citation standard via Google Scholar).
- Frank, M., & Carpinteri, E. (2019). Enterprise Network Virtualization and Software-Defined Security Architectures. *Journal of Network and Computer Applications*, 124, 45-58.
- Wray, C., & Jansen, W. (2020). Active Directory Security Hardening and Multi-Master Replication Paradigms in Enterprise Environments. *IEEE Transactions on Dependable and Secure Computing*, 17(4), 812-825.