

Ontario Skills Competition – Practical Lab

Scenario: Data Center IT Infrastructure – Rogers-like Office / DC Environment

Scenario Overview

You are hired as a Junior IT Administrator at Evergreen Telecom, a company with a small office-connected data center.

The data center hosts critical services for internal and client-facing operations:

- Virtualized Servers: Windows Server VMs for Active Directory, file services, and internal apps.
- Linux Web Servers: Hosting company intranet and monitoring dashboards.
- Network Devices: Managed switches, firewall, and routers.
- Client Office: 10 staff PCs connected via VPN to the data center.

Current Situation:

The IT manager has received reports of:

- Some staff PCs cannot access shared drives.
- VPN clients sometimes cannot resolve internal hostnames.
- A monitoring dashboard shows intermittent connectivity issues between some VMs.

Your task is to investigate, troubleshoot, and implement solutions to ensure the network and services are fully operational.

Lab Objectives

Students must:

1. Analyze the network to identify misconfigurations.
2. Troubleshoot connectivity between office PCs, VPN clients, and data center servers.
3. Verify DNS and DHCP functionality for both physical and virtual networks.
4. Check virtualization host settings (VM IPs, virtual switches).
5. Document issues found and steps taken to resolve them.

6. Verify service accessibility (file sharing, web dashboard, intranet).
-

Tasks

Task 1 – Network Verification

- Check IP addresses, subnets, gateways, and DNS on:
 - Office PCs
 - VPN clients
 - VMs in the data center
- Identify any connectivity problems.

Deliverable: Table showing device name, IP, subnet, gateway, and DNS status.

Task 2 – DHCP & DNS Troubleshooting

- Verify that DHCP is assigning correct IPs for office clients.
- Verify that DNS resolves:
 - Internal hostnames (fileserver1.dc.evergreen.local)
 - Web dashboard hostnames (monitor.dc.evergreen.local)

Deliverable: Short report highlighting misconfigurations and corrective actions.

Task 3 – Virtualization Verification

- Check that VMs are connected to the correct virtual networks.
- Ensure no overlapping IPs between virtual and physical networks.
- Confirm that VMs can ping each other and the gateway.

Deliverable: Screenshot of VM network configuration and ping tests.

Task 4 – Firewall & Access

- Review firewall rules on the edge router and server VMs:

- Allow internal file sharing
- Allow internal web access
- Block unnecessary ports

Deliverable: Table or screenshot of firewall rules applied.

Task 5 – Verification & Documentation

- Ensure all office PCs and VPN clients can:
 - Access shared files on the file server
 - Reach internal web services
 - Resolve internal hostnames correctly

Deliverable: Final verification table and short troubleshooting report.

Skills Assessed

- IP addressing, subnetting, and DHCP verification
 - DNS troubleshooting
 - VM and virtual network verification
 - Firewall rule assessment and access control
 - Network troubleshooting using ping, tracert, nslookup
 - Documentation and reporting
-

Optional Extensions / Advanced Tasks

- Configure VPN routing for remote clients
- Implement role-based access control on file shares
- Configure basic monitoring alerts for VM or server downtime