Digital Egypt Pioneers Initiative

Track: Infrastructure and Security

Google IT Technical Support Specialist

Project: Network Setup & Configuration and Troubleshooting

2024

BY:

Ramzey Elsayed Mohammed

AbdulRhman AbdulGhaffar Ewais

Mustafa Abdullah Mohammed

A Project Graduation Document Submitted in Partial Fulfillment of the Requirements for Network Setup and Troubleshooting in Digital Egypt Pioneers Initiative Track (**Google Technical Support Specialist)**

Digital Egypt Pioneers Initiative

Tracker Infrastructure and Security

Google IT Technical Support Specialist

2024

Digital Egypt Pioneers Initiative

Track: Infrastructure and Security

Google IT Technical Support Specialist

Project: Network Setup and Troubleshooting

A Project Graduation Document Submitted in Partial Fulfillment of the Requirements for Network Setup and Troubleshooting in Digital Egypt Pioneers Initiative Track (Google Technical Support Specialist)

RAM Team:

- **Ramzey Elsayed Mohammed**
- **AbdulRhman AbdulGhaffar Ewais**
- **Mustafa Abdullah Mohammed**

Under The Supervision of:

DR. Mustafa Salah

Mustafa is an IT Support professional who provides technical support to end-users, dedicated to helping users with their computer problems, troubleshooting hardware and software issues, configuring systems, and delivering excellent customer experience.
He feels a sense of accomplishment to see users get their issues fixed.

This section outlines the roles and responsibilities of the team members:

- **Ramzey Elsayed Mohammed:**

  A graduate of the DEPI scholarship, which was provided by the Ministry of Communications. My role involved responsibility for network troubleshooting and testing. My role entailed the identification and resolution of network issues, with the objective of maintaining optimal performance and uptime. I conducted a series of tests to diagnose the root cause of the problem, evaluated the configuration of the network, and ensured that all systems were operating at optimal efficiency. I have experience in troubleshooting connectivity issues, analyzing network traffic, and performing routine maintenance to prevent potential disruptions. With acute attention to detail and a proactive methodology, I am committed to ensuring the stability and reliability of network operations.

- **AbdulRhman AbdulGhaffar Ewais:**

  A graduate of the DEPI scholarship provided by the Ministry of Communications. During my tenure, I was responsible for the configuration of network settings. During the scholarship period, I was engaged in the design and implementation of network infrastructure, in addition to the assurance of security settings and connection integrity. I acquired practical experience in the operation of network devices and the configuration of communication protocols, which enhanced the efficiency of the team and guaranteed the stability of the network.

- **Mustafa Abdullah Mohammed:**

  A graduate of the DEPI scholarship, which was provided by the Ministry of Communications. In this role, I was responsible for the design and planning of networks. My role entailed the design of network topologies, the determination of hardware and software requirements, and the assurance that the network infrastructure satisfied the organization's performance and security standards. I have practical experience in the creation of scalable network architectures, the effective management of bandwidth, and the implementation of strategies for network redundancy and fault tolerance. With a strong focus on optimizing network performance and security, I Endeavor to deliver reliable solutions that align with business needs and support future growth.

Project: Network Setup and Troubleshooting:

- Objective: Build and troubleshoot a basic network to understand networking concepts better.
- Description: Create a small local network using routers, switches, and a few computers or virtual machines. Configure the network with a range of IP addresses, set up DHCP, and ensure devices can communicate with each other. Introduce intentional errors (like IP conflicts or disabled services) and have students diagnose and resolve these issues
- Skills Covered: Networking, IP addressing, DHCP, troubleshooting, network configuration.

Week 1:

- Plan network layout: Develop a network design plan including IP addressing and DHCP configuration.
    - Deliverable: Network design plan.
- Set up network components: Configure routers, switches, and VMs or physical devices
    - Deliverable: Network setup documentation.
- Test network functionality: Ensure devices communicate and test basic connectivity.
    - Deliverable: Network test results.

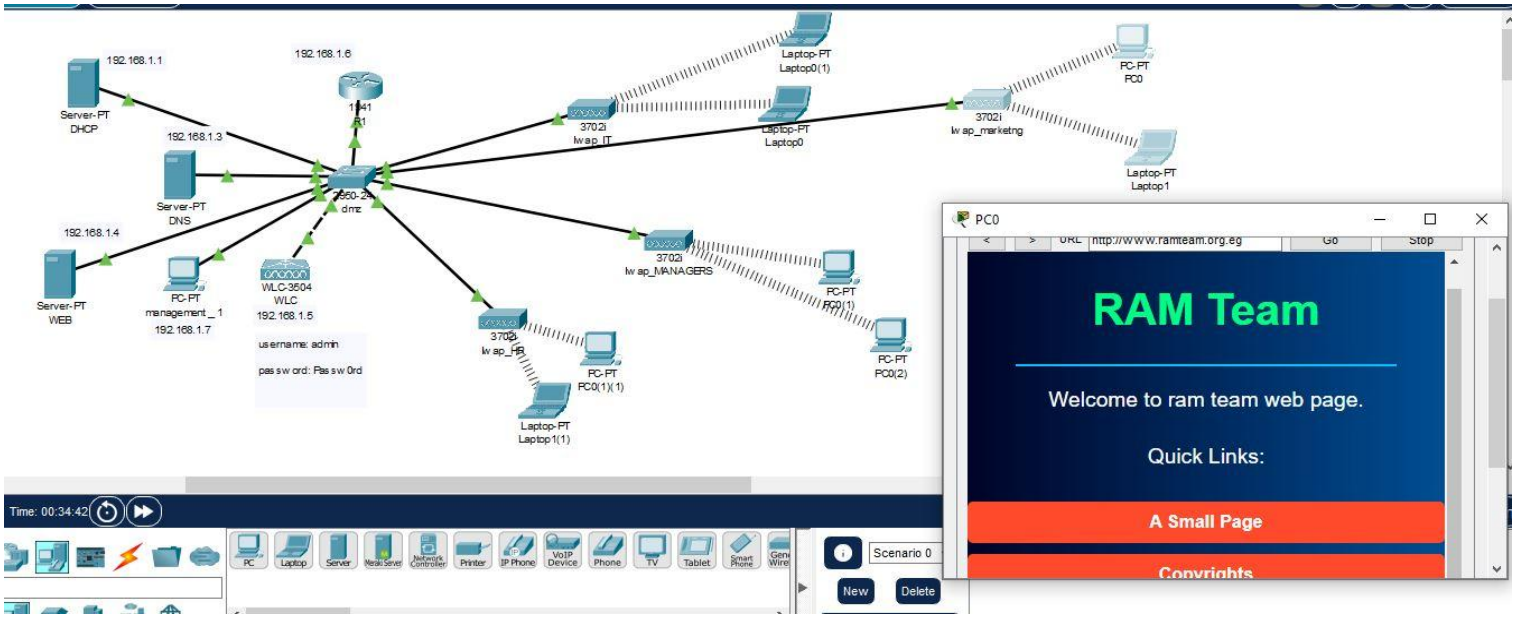
Week 2:

- Introduce and troubleshoot errors: Create intentional errors and document troubleshooting steps.
    - Deliverable: Error scenarios and troubleshooting guide.
- Compile all materials: Review and compile documentation into a complete guide.
    - Deliverable: Complete Network Setup and Troubleshooting Guide

Design and Planning of Networks:

The illustrated network topology demonstrates a structured and organized configuration, designed using Cisco Packet Tracer. The network comprises a variety of interconnected devices, including a central router, multiple servers (DHCP, DNS, and WEB), a switch, PCs, laptops, and several access points, which are managed by a Wireless LAN Controller (WLC). Each device is assigned a specific IP address and connected to a designated subnet, thus facilitating streamlined communication and efficient network management,The central router serves as the primary hub, facilitating connectivity between servers and client devices and ensuring the uninterrupted flow of data across the network. The switch is responsible for distributing this connectivity to different departments and access points, with each serving a particular group of users. The access points provide wireless connectivity to laptops and PCs, thus enabling flexible and mobile access to network resources. Overall, the topology reflects a well-designed infrastructure with clear segmentation and robust network services.

The image illustrates the comprehensive and definitive design of the project, showcasing the progression of design elements throughout the project's development.



Project Link: https://drive.google.com/file/d/1B_DEPuYSv7FYABG7J9TB13ulQaFx86Ij/view?usp=drive_link

The network topology provided was created using Cisco Packet Tracer and includes a variety of devices, including routers, switches, servers, personal computers, and access points. The following section provides a comprehensive account of each component, delineating its function and IP configuration.

1. **A network overview is provided below.**

The network diagram comprises a number of interconnected devices, which are organised in a well-structured network configuration. The devices included in the network are as follows:

The network comprises the following devices:

Router (1841 R1)

Switch (Cisco 2960)

Access Points (Cisco 3702i)

Wireless LAN Controller (WLC-3504)

Various Servers (DHCP, DNS, WEB)

PCs and Laptops

The IP addresses have been assigned in an appropriate manner to each device and subnet, facilitating efficient communication and management. The network appears to be divided into discrete segments or VLANs, with each segment serving a specific department or service.

---

2. Network Components and IP Configuration:

1. **Router:**
    - **Device Name:** 1841 R1
    - **IP Address:** 192.188.1.6
    - **Function:** Central routing device connecting multiple segments and managing network traffic.
2. **Servers:**
    - **DHCP Server:**
        - **Device Name:** Server-PT
        - **IP Address:** 192.188.1.1
        - **Role:** Provides dynamic IP address allocation to the devices in the network.

- **DNS Server:**
  - **Device Name:** Server-PT
  - **IP Address:** 192.188.1.3
  - **Role:** Resolves domain names to IP addresses for devices within the network.
- **WEB Server:**
  - **Device Name:** Server-PT
  - **IP Address:** 192.188.1.4
  - **Role:** Hosts web applications or websites for internal or external access.

3. **PCs and Laptops:**
   - Devices like PC-PT and Laptop-PT are spread across the network and connected to specific VLANs or departments.
   - **Example Devices:**
     - PC-PT (management_1) with IP: 192.188.1.7
     - PC-PT (FC0) with IP: (Configured via DHCP)
4. **Wireless Devices:**
   - **Access Points:**
     - lw ap_IT: Connected to IT devices (Laptops)
     - lw ap_MANAGERS: Serves manager-specific devices
     - lw ap_marketing: Connected to marketing PCs and laptops
     - All access points are centrally managed by the Wireless LAN Controller (WLC).
5. **Wireless LAN Controller (WLC-3504):**
   - **Device Name:** WLC-3504
   - **IP Address:** 192.188.1.5
   - **Username:** admin
   - **Password:** Passw0rd
   - **Role:** Manages wireless connections and configurations for all access points in the network.

3. Network Design Details:

- Central Routing and Switching:
    - The central router (R1) manages connections between the internal servers and various client devices.
    - A switch (Cisco 2960) acts as a distribution point for all connected devices, ensuring efficient packet delivery.
- IP Address Allocation:
    - Servers have static IP addresses assigned within the 192.188.1.X range.
    - End-user devices, such as PCs and laptops, are likely configured to obtain IP addresses dynamically from the DHCP server.
- Wireless Connectivity:
    - Three main wireless access points are dedicated to specific departments, each serving a group of devices.
    - The WLC is used for centralized management of these access points, providing seamless connectivity and monitoring capabilities.

---

4. Summary and Recommendations:

This network topology showcases a well-designed network for an organization with multiple departments. The use of a centralized router and switch for traffic management, along with dedicated servers and a wireless LAN controller, ensures a robust and scalable network infrastructure.

- Improvements:
    - Implementing VLANs on the switch can further segment traffic and improve security.
    - Enable security features like WPA3 for wireless networks to secure communications.
- Potential Issues:
    - Ensure that all servers and critical devices have backup configurations and redundant connections to prevent downtime.

---

5. Network Functionalities and Services:

The designed network provides several critical services to ensure smooth communication and efficient management across the organization. Below is a detailed explanation of each service and its implementation:

5.1 DHCP Service:

- The DHCP Server (IP: 192.188.1.1) is responsible for dynamically assigning IP addresses to devices within the network. This setup reduces manual configuration efforts and ensures that devices automatically receive IP addresses, DNS settings, and default gateway information.
- Configuration Details:
    - DHCP IP address pool: 192.188.1.10 - 192.188.1.50
    - Default Gateway: 192.188.1.6 (Router IP)
    - Lease Time: 24 hours

5.2 DNS Service:

- The DNS Server (IP: 192.188.1.3) translates domain names (e.g., www.company.local) into IP addresses, enabling easier access to internal and external websites. The DNS server can be configured with multiple domain zones, allowing efficient name resolution.
- Configuration Details:
    - Primary Zone: company.local
    - Example Domain to IP Mapping:
        - www.company.local -> 192.188.1.4 (WEB Server)

5.3 WEB Service:

- The WEB Server (IP: 192.188.1.4) hosts internal web applications, such as a company portal or intranet, that employees can access for information sharing and collaboration.
- Suggested Features:
    - Implement HTTPS for secure web communication.
    - Host employee portals, HR systems, and document management systems on this server.

5.4 Centralized Wireless Management:

- The Wireless LAN Controller (WLC-3504) is used to centrally manage all the wireless access points in the network. It allows the network administrator to configure, monitor, and optimize wireless networks without needing to manually configure each access point.
- Key Benefits:
    - Simplified wireless network management.
    - Improved security through centralized authentication and encryption policies.
    - Load balancing and automatic channel management for optimal performance.

5.5 Segmentation and Security:

- Network Segmentation:
    - Each department, such as IT, Managers, and Marketing, has its own dedicated access point and subnet. This segmentation isolates network traffic, enhancing security and minimizing broadcast domain sizes.
- Security Measures:
    - Strong passwords and user authentication are enforced on the WLC and access points.
    - Consider implementing ACLs (Access Control Lists) on the router to restrict unauthorized access between subnets.

---

6. VLAN Configuration and Traffic Segmentation:

To further improve the network's efficiency and security, VLANs (Virtual LANs) can be implemented on the switch (Cisco 2960). VLANs separate network traffic logically, even if devices are connected to the same physical switch.

VLAN Details:

- VLAN 10 – IT Department
    - Devices: PC-PT, Laptop-PT
    - IP Range: 192.188.1.50 - 192.188.1.60
- VLAN 20 – Management Department
    - Devices: PC-PT (management_1), PC-PT FC0
    - IP Range: 192.188.1.60 - 192.188.1.70
- VLAN 30 – Marketing Department

- Devices: Marketing laptops and PCs
- IP Range: 192.188.1.70 - 192.188.1.80

Benefits of VLAN Implementation:

- Isolates network traffic to enhance security.
- Reduces broadcast traffic, improving network performance.
- Allows better management and monitoring of each department's traffic.

---

7. Network Troubleshooting Recommendations:

Effective troubleshooting techniques are essential to maintain a healthy network. Below are some recommended practices to identify and resolve common issues:

7.1 Connectivity Issues:

- Symptom: Devices are unable to connect to the network or communicate with other devices.
- Troubleshooting Steps:
  1. Check device connectivity and IP address allocation using the command ping.
  2. Verify that devices are receiving IP addresses correctly from the DHCP server.
  3. Ensure that the default gateway (Router) is reachable from each device.

7.2 DNS Resolution Issues:

- Symptom: Devices can connect to IP addresses but cannot access domain names.
- Troubleshooting Steps:
  1. Test DNS resolution using the command nslookup <domain-name>.
  2. Verify DNS server configuration on the client device.
  3. Check DNS server logs for errors or misconfigurations.

7.3 Wireless Connectivity Problems:

- Symptom: Devices cannot connect to the wireless network or experience frequent disconnections.

- Troubleshooting Steps:
    1. Check access point configurations and signal strength.
    2. Ensure that the Wireless LAN Controller is properly managing the access points.
    3. Check for interference or overlapping channels and adjust AP placement or channel settings accordingly.

---

8. Conclusion and Future Enhancements:

The network setup demonstrated in this project provides a solid foundation for an organization's IT infrastructure. It incorporates various services like DHCP, DNS, and centralized wireless management, ensuring efficient and secure communication.

Future Enhancements:

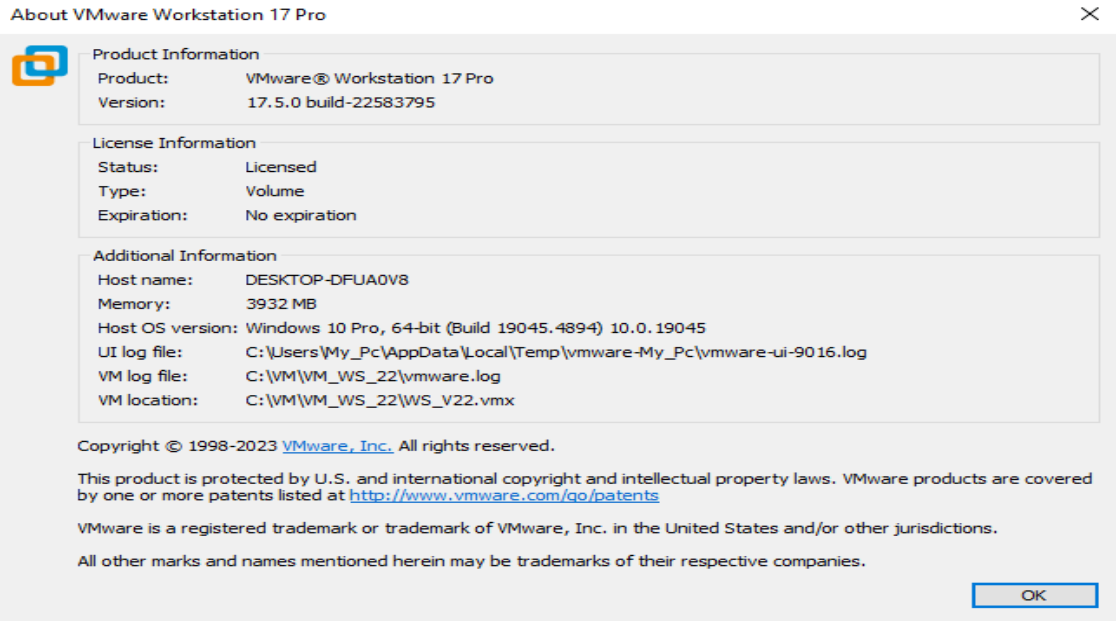
- Implement network redundancy through additional routers or switches.
- Upgrade security protocols (e.g., WPA3) on wireless networks to improve protection.
- Introduce network monitoring tools like SNMP (Simple Network Management Protocol) for real-time performance tracking and alerting.

This report covers the detailed description of your network setup and its configurations, along with recommendations for improvement. You can integrate this content into your final project documentation under relevant sections like "Network Design," "Implementation," and "Troubleshooting." Let me know if there are any more details you'd like to include!

Network Setup & Configuration:

We shall commence with the VMware environment setup program. The following steps will be taken in order to install Windows Server and Windows Private Client, as well as to set up the tools for the Setup Network, DHCP Server, DNS Server, Print Server, and Sharing Folder.

- **Install VMware, configure the environment, and add the activation key. This is the first step.**
  - **Download The VMWare Workstation version 17pro:**
    Link: https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html
  - **The Website License key:**
    Link: https://github.com/hegdepavankumar/VMware-Workstation-Pro-17-Licence-Keys
  - **License key used: MC60H-DWHD5-H80U9-6V85M-8280D**

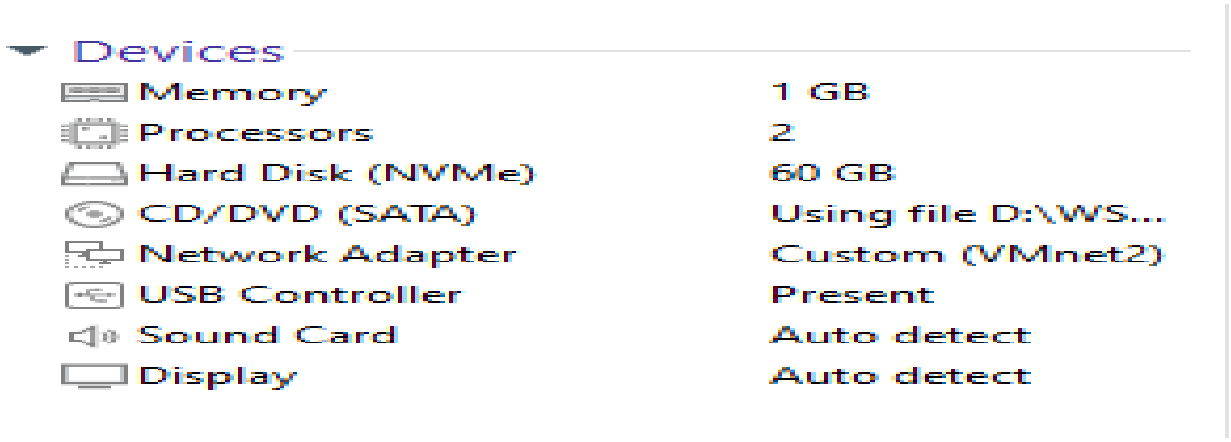


Upon completion of the download and activation process, the user will be presented with the following interface.

The subsequent step is to configure the virtual machine prerequisites for the installation of Windows Server.

Virtual Machine Requirements	
Processer	2 cores
RAM	1 GB
Hard Disk	60 GB
Network Adapter	Custom (VMnet2)

This image clearly shows all the requirements.



The subsequent step is to proceed to the official Microsoft website in order to download the ISO file, which is required for the boot process. The process will be completed in a relatively short period of time.

- **Download Windows Server version 2022 United States Ios (Data Center _GUI) now.**
- **Windows Server IOS Link:** https://go.microsoft.com/fwlink/p/?LinkID=2195280&clcid=0x409&culture=en-us&country=US
- **Activation key: Windows Active Valid For 180 Day**

A username and password will be requested in order to gain access to the local Windows Server. These should be employed to complete the remainder of the installation and proceed to the subsequent step, which is to convert the server to a domain controller.

Username and Password to Access the Local Windows Server v22	
User:	Administrator
Pass	P@ssw0rd

In order to effect a conversion of a server to Active Directory, it is necessary to complete the following steps.

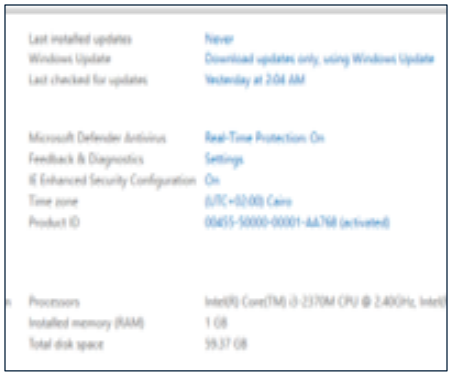
It is necessary to reboot the server once more in order to implement the new name following a change. Failure to comply with this instruction will result in complications. At this point, navigate to the Server Management page and complete the remaining configuration steps. It is imperative to ascertain the time zone in order to circumvent any potential complications when integrating the client's device into the domain. It is now necessary to activate the firewall and check for updates, including any that address vulnerabilities. It is now necessary to activate remote management and remote desktop, and to verify the Ethernet0 settings. Upon completion of the aforementioned steps, the download of AD on the server may then be initiated.

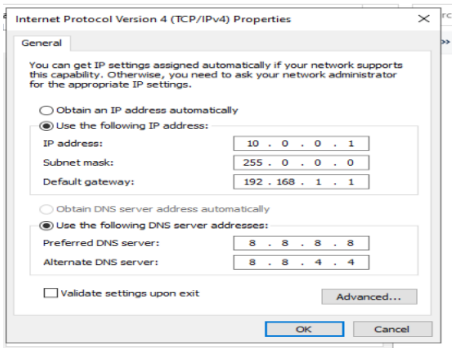
It is advisable to reboot the device after changing the server's name and activating all the aforementioned settings. This will ensure that everything is configured correctly and that the download of AD can be carried out without any issues.

- **properties of Local server:**
  - **Server Name: DC_RAM**
  - **Time Zone:(UTC+02:00) Cairo**
  - **Microsoft Defender Firewall: On**
  - **Remote Management: Enable**
  - **Remote Desktop: Enable**
  - **Ethernet0: Enable**

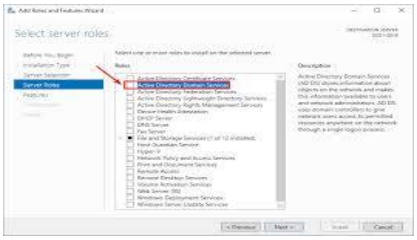
○ **Ipv4: 10.0.0.1/8**
○ **Subnet mask: 255.0.0.0**
○ **Gateway: 192.168.1.1**
○ **DNS1: 8.8.8.8**
○ **DNS2: 8.8.4.4**

The image in question serves to illustrate the point in question with great clarity.

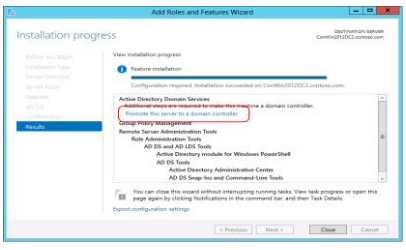




The AD is now available for download. To begin the process, navigate to the Dashboard and select the "Add Roles and Features" option. Select the option to download the Active Directory Domain Services. Once all components have been activated, the new forest should be created, and the server restarted in order to implement the requisite changes.

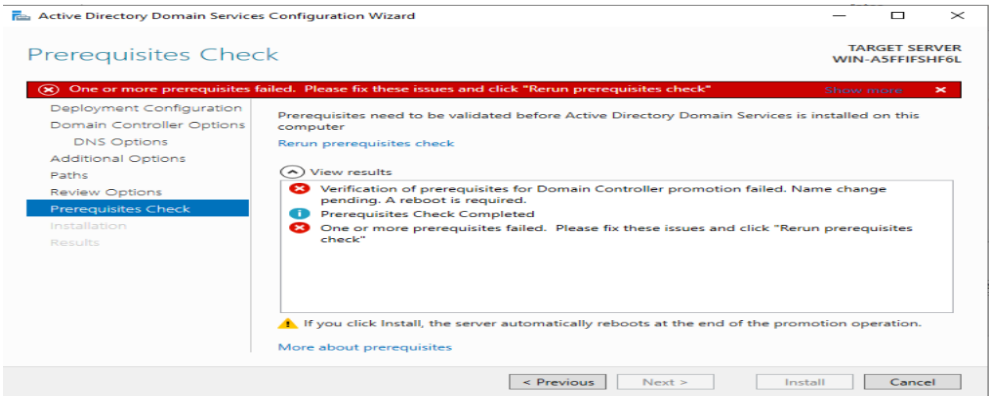


Active Directory Domain



Active Directory Domain Services Download Successfully

It is imperative to read the instructions with the utmost care in order to avoid any potential errors. Should you encounter the issue depicted in the accompanying screenshot, we invite you to follow along with us as we work to identify a solution.



First solution:

- **Restart the server and reinstall AD. This will resolve the issue.**

Second solution:

- **To access the second solution, click on the YouTube link. This solution uses some of the first ones in the Terminal. (Verification of prerequisite for domain controller promotion failed | Active directory error).**
  Link: https://youtu.be/2N-_SDnTlFA

---

properties of Active Directory Domain Services:

- **Domain Name: DPEIRAM.net**

  - **Login: Administrator@DPEIRAM.net | DPEIARM\Administrator**
  - **Pass: P@ssw0rd**

- **Forest Functional Level: Windows Server 2012R2**
- **Forest Functional Level: Windows Server 2016**
- **Specify Domian Controller Capabilities**

○ DNS Server	✓
○ Global Catalog (GC)	✓
○ RODC	

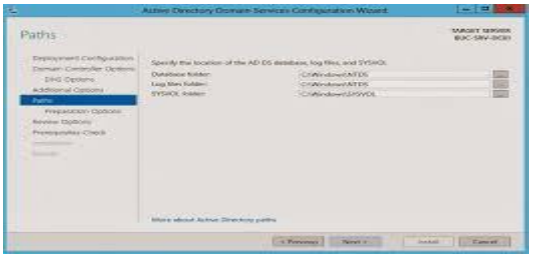
Type The Directory Services Restore Mode:

Password (DSRM): P@ssw0rd

Specify The Location of the (AD DN) Data bases log files, and SysVol:

Data Base: c:\windows\NTDS
Log: c:\windows\NTDS
Sys: c:\windows\SysVol

This image clearly demonstrates the point:



Specify The Location of the (AD DN) Data bases log files, and SysVol:

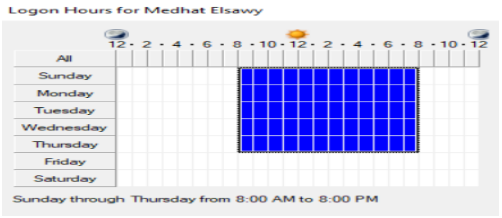
Type The Directory Services Restore Mode:

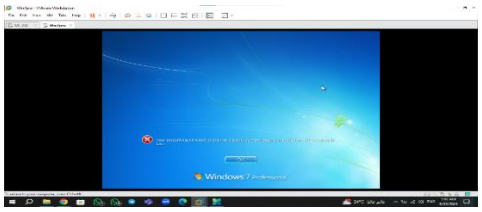
Now that the Active Directory (AD) server has been installed, the remaining setup can be completed. The next step is to create a new organizational unit (OU) that will contain the necessary groups, users, computers, and other equipment. Furthermore, user accounts and passwords will be created. Subsequently, a group will be created in order to implement the policy. Subsequently, the aforementioned table will serve as a repository for all pertinent information.

AD_Login : Administrator@DPEIRAM.net : DPEIARM\Administrator			
AD_Pass: P@ssw0rd			
OU: DEPIRAM			
	OU_User , OU_Goups , OU_Group_Police , OU_Compuoter		
	OU_User (Accounts)		
OU	1-OU_IT	User	Pass
Name	1-AbdulRhman AbdulGhaffar 2-Mustafa Mohammed 3-Ramzey Elsayed	1-DEPI_AB 2-DEPI_MU 3-DEPI_RA	P@ssw0rd
OU	2-O_HR	User	Pass
Name	1-Omnia Mansour 2-Esraa Soliman	1-DEPI_OMN 2-DEPI_ESO	P@ssw0rd
OU	3-OU_Marketing	User	Pass
Name	1-Mohammed Ashraf 2-Mohammed Ragab	1-DEPI_MSH 2-DEPI_MRA	P@ssw0rd
OU	4-OU_Sales	User	Pass
Name	1-Abdullah Khaled 2-Mohammed Nasser	1-DEPI_AK 2-DEPI_MN	P@ssw0rd
OU	5-OU_Graphic Design	User	Pass
Name	1-Medhat Elsawy 2-Ahmed Shaban	1-DEPI_MDH 2-DEPI_AHM	P@ssw0rd
OU	6-OU_Management	User	Pass
Name	1-Mustafa Salah 2- Global Knowledge	1-DEPI_MUS 2-DEPI_GKL	P@ssw0rd

Once all the requisite employee configurations have been established, the next step will be to define the applicable work hours. This is a security measure designed to prevent employees from using the device outside of work hours. It has been determined that the aforementioned measure will be in effect from 8 a.m. to 8 p.m. on all days of the week, with the exception of Friday and Saturday.

This image clearly demonstrates the point:





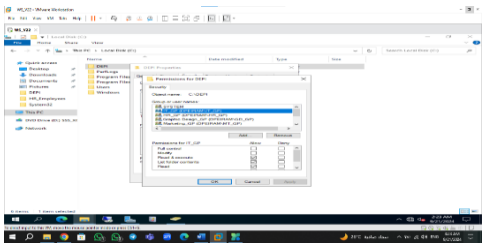
The next step is to create a sharing folder and grant permissions to employees. As can be observed, each department is afforded complete control over the files pertaining to its own operations. Additionally, some departments will have read-only access to other files, which will facilitate their work. The only individuals with the ability to view all departments are those in the information technology department and those in management.

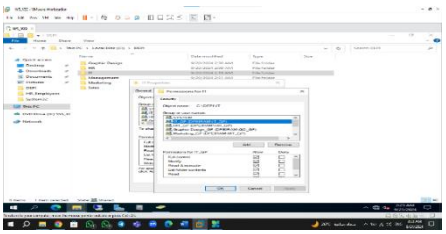
The following table shows all these details:

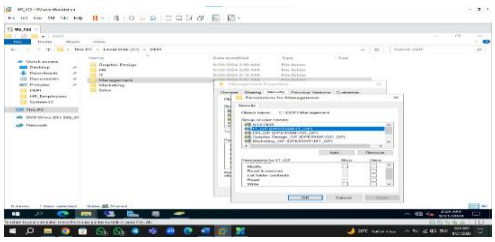
- **The cells with the letter F mean you have full access. The cells with the letter R mean you have read-only access. Empty cells mean there is no access.**
  F: Full Access, R: Read only , W: Write , M: Modify , R&E: Read & Execute

sharing folder permissions						
Permissions OU	**IT**	**HR**	**Sales**	**Marketing**	**Graphic Design**	Management
IT	**F**	**R**	**R**	**R**	**R**	R
HR		**F**				
Sales			**F**			
Marketing				**F**		
Graphic Design					**F**	
Management		R	R	R	R	F

This image clearly demonstrates the point:







Read-only	Permutations	Full Access

The subsequent phase of the process is the downloading and configuration of the DHCP Server. This will prepare it for operational readiness. Proceed with the remaining steps by selecting the "New Rules" tool and choosing "DHCP Server." The utility of this process will become apparent as you proceed.

• Automatic IP Assignment: The Dynamic Host Configuration Protocol (DHCP) automates the assignment of Internet Protocol (IP) addresses to devices on a network, thereby reducing the need for manual configuration.

• Conflict Prevention: The system thus prevents IP address conflicts by ensuring that each device is allocated a unique address.

• Simplified Management: It facilitates the administration of networks, particularly in those comprising a considerable number of nodes, by enabling centralized configuration alterations.

• Automatic Configuration: Additionally, it furnishes devices with other requisite settings, including gateway and DNS server information.

• The software offers support for mobile devices. It facilitates connectivity for mobile devices that connect to disparate networks by providing new settings in an expedient manner.

• Reduction of time and effort required for implementation: This process reduces the time and effort required for the manual configuration of each device.

• Dynamic Updates: It permits the implementation of dynamic updates to settings without the necessity of device restarting.

In summary, DHCP has the overall effect of enhancing network efficiency and simplifying network management.

The following table presents a comprehensive overview of the essential settings and configurations that must be adhered to.

Setting up a DHCP (Dynamic Host Configuration Protocol) Server allows you to automate the assignment of IP addresses and other network configuration parameters to devices on your network. Below are the steps to install and configure a DHCP Server on a Windows Server environment.

Steps to Install and Configure a DHCP Server

1. Open Server Manager
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager from the Start menu.
2. Add the DHCP Server Role
   - In the Server Manager, click on Manage in the upper right corner.
   - Select Add Roles and Features.
   - Click Next until you reach the Server Roles section.
   - Check the box for DHCP Server.
   - Click Next through the wizard, and then click Install.
   - Wait for the installation to complete and click Close.

3. Authorize the DHCP Server

- After installation, you need to authorize the DHCP server in Active Directory.
- Open the DHCP Management Console:
    - In Server Manager, go to Tools and select DHCP.
- Right-click on DHCP and select "Authorize".
- Wait a moment, then right-click again and select "Refresh" to verify that the server is authorized.

4. Create a DHCP Scope

A DHCP scope defines the range of IP addresses that the DHCP server can assign to clients.

- In the DHCP Management Console, expand the DHCP server node.
- Right-click on IPv4 and select "New Scope".
- Follow the New Scope Wizard:
    - Name: Give your scope a descriptive name (e.g., "Office Network").
    - Description: Optional description for the scope.
    - IP Address Range: Define the start and end IP addresses of the range.
    - Subnet Mask: This will typically auto-fill based on the IP range.
    - Add Exclusions: Specify any IP addresses that should not be assigned (e.g., static IPs).
    - Lease Duration: Set how long an IP address can be leased to a client.
    - Configure DHCP Options: You can set options like router (default gateway), DNS servers, and WINS servers. This can be configured later if needed.
    - Activate Scope: Choose to activate the scope immediately.

5. Configure DHCP Options

- Right-click on your newly created scope and select Properties.
- Go to the Advanced tab to configure lease duration and other settings.
- To set options such as DNS servers and default gateway:
    - Expand your scope in the DHCP Management Console.
    - Right-click on Scope Options and select Configure Options.
    - Check the relevant options and fill in the necessary information.

6. Test the DHCP Configuration

- Connect a client device to the network.
- Ensure that the device is set to obtain an IP address automatically.
- Check that the device receives an IP address from the DHCP server.

7. Monitor DHCP Server

- Regularly monitor the DHCP server to ensure it's functioning correctly.
- Check the DHCP logs and client lease status to troubleshoot any issues.

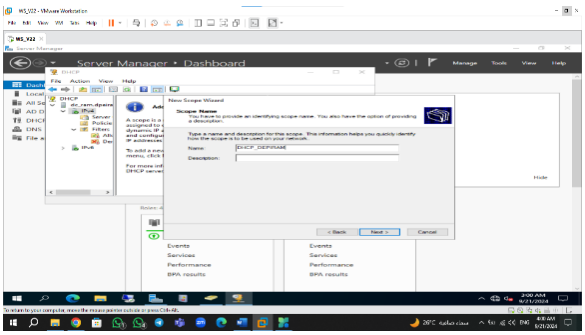
Important Notes

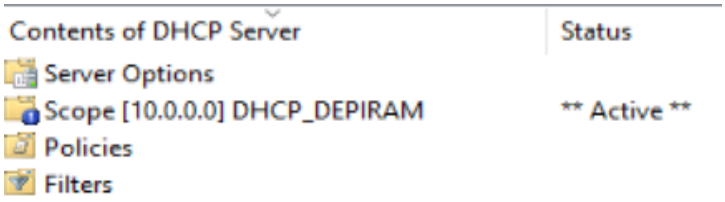
- Security: Ensure that only authorized devices can connect to the DHCP server, as unauthorized access can lead to network issues.
- Documentation: Keep records of your DHCP settings, including scopes, options, and exclusions, for troubleshooting and auditing.
- Backups: Regularly back up the DHCP server configuration to avoid loss of settings in case of server failure.

This table shows the settings for the DHCP settings of the server.

DHCP Server		
Scope Name	DHCP_DEPI_RAM	
IP_Server	10.0.0.1	
IP Range	**10.0.0.1**	10.0.0.254
Subnet Mask	255.255.255.0	
Length	24	
Gateway	192.168.1.1	
DNS	10.0.0.1	
	8.8.8.8	
	8.8.4.4	
Exclusions	**10.0.0.1**	10.0.0.20
Lease	30 Days	

This image clearly demonstrates the point:





The next step is to install Internet Information Services (IIS) and add Webserver Local. Let us now proceed to the remaining expressions of congratulation.

Open Server Manager:

Steps to Set Up Internet Information Services (IIS) on Windows Server:

- Click on the Start menu.
- Type Server Manager and select it.

  2. Add Roles and Features:
- In the Server Manager dashboard, click on "Manage" in the upper-right corner.
- Select "Add Roles and Features" from the dropdown menu.

  3. Start the Installation Wizard:
- In the "Add Roles and Features Wizard", click "Next" until you reach the Installation Type page.
- Select "Role-based or feature-based installation" and click "Next".

  4. Select Destination Server:
- Choose the server on which you want to install IIS. Usually, it’s the local server.
- Click "Next".

  5. Select Server Roles:
- In the "Select Server Roles" window, check the box for "Web Server (IIS)".
- A popup may appear to add required features. Click "Add Features".

  6. Add Required Features:
- Click "Next" to proceed through the Features window, as IIS will have the required features automatically selected.

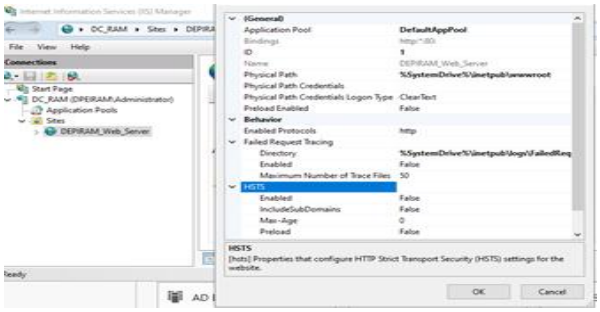
  7. Configure Web Server (IIS):
- Click "Next" on the Web Server Role (IIS) page to view the role services that are installed by default.
- Select additional role services as needed (e.g., Application Development, Security, or Management Tools).

  8. Confirm Installation Selections:
- Click "Next" and review your selections.
- If everything is correct, click "Install".

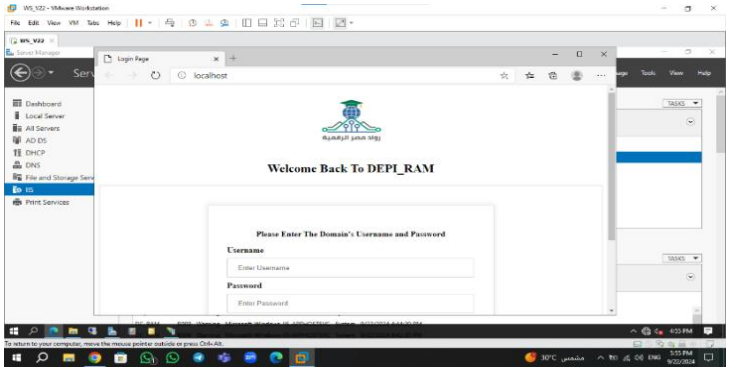
  9. Complete the Installation:
- Wait for the installation to be completed, and then click "Close".

  10. Verify the Installation:
- Open a web browser and type http://localhost.
- If IIS is installed successfully, you should see the IIS welcome page

This image clearly demonstrates the point:



Here's an image showing all the basic data



This image confirms that the server is running

This link will take you to the code for the web server.

Link: https://drive.google.com/file/d/1m8VKD_8WIKshx6aw9Ie_BJbGF_0-ZZbf/view

---

The subsequent step is to input the designation "Role New." This is a print server that oversees the printing process by implementing specific functions. To illustrate, the printer is accessible only between the hours of 8 a.m. and 8 p.m., and only employees are permitted to utilize it. All employees are now able to print white and black documents and indicate which items are of particular importance. The Graphic Design department is permitted to print in color, while the management department is authorized to print any other employee's documents that have been designated as of higher priority.

Steps to Set Up a Print Server on Windows Server:

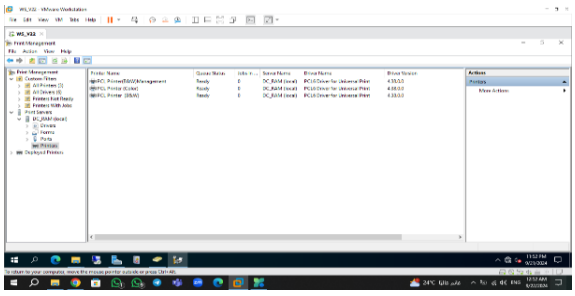
1. Open Server Manager
   - Log in to your Windows Server.
   - Click on Start, and open Server Manager.
2. Add Print and Document Services Role
   - In the Server Manager dashboard, click on "Manage" in the top-right corner.
   - Select "Add Roles and Features."
   - In the Add Roles and Features Wizard, click "Next" until you reach the Installation Type page.
   - Select "Role-based or feature-based installation" and click "Next."
   - Choose your server from the server pool and click "Next."
3. Select Server Roles
   - On the Select Server Roles page, check the box for "Print and Document Services."
   - A prompt may appear to add features required for this role. Click "Add Features."
   - Click "Next" until you reach the Role Services page.
   - Ensure "Print Server" is selected and click "Next."
4. Complete the Installation
   - Review the installation selections and click "Install."
   - Wait for the installation to be completed, then click "Close."
5. Add a printer

- In Server Manager, go to Tools and select "Print Management."
- In the Print Management window, expand your server's name.
- Right-click on "Printers" and select "Add Printer."
- Choose "Add a TCP/IP or Web Services Printer by IP Address or Hostname" and click "Next."

6. Configure Printer Settings
   - Enter the printer's IP address or hostname, then click "Next."
   - Choose the appropriate driver for the printer. If it is not listed, you may need to install the driver from the manufacturer's website.
   - Follow the attempts to complete the printer installation.
7. Share the Printer
   - After adding the printer, right-click on the printer in Print Management.
   - Select "Printer Properties."
   - Go to the Sharing tab.
   - Check the box for "Share this printer."
   - Give the printer a share name, which users will use to connect to the printer.
8. Configure Additional Settings (Optional)
   - You can set additional options such as printer security, advanced settings, and printing preferences as needed.
9. Connect Client Computers to the Print Server
   - On client machines, open "Devices and Printers."
   - Click on "Add a printer."
   - Choose "The printer that I want isn't listed."
   - Select "Select a shared printer by name" and enter the printer path (e.g., \\YourPrintServerName\PrinterShareName).
   - Follow the prompts to complete the installation.
10. Test the Printer
    - Print a test page from both the print server and client machines to ensure everything is functioning correctly.

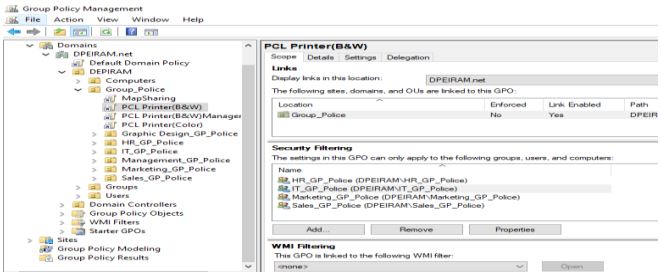
Notes:

- Ensure that the printer is connected to the network and powered on.
- Make sure to configure firewall settings to allow for print sharing.
- In a domain environment, consider using Group Policy to manage printers centrally



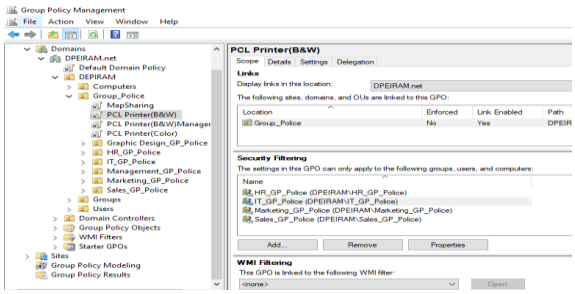
Print Management Server

This image clearly demonstrates the point

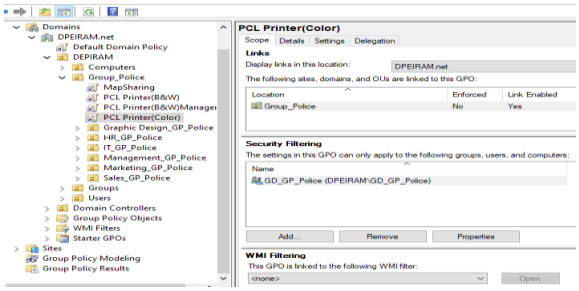


This is the department's printing permissions image.

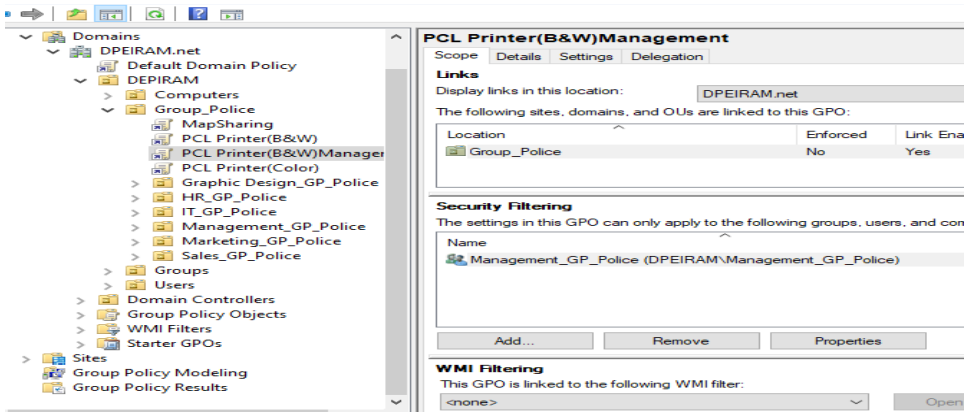
This image clearly demonstrates the point PCL printer (B&W) Group Police:



PCL printer (B&W) Group Police



PCL printer (Color) Group Police



PCL printer (Color) Group Police

It is of the utmost importance that the information presented be reviewed in its entirety during the installation of the print server.

1-Drive: download driver Ricoh Network printer model H for windows server 22

Link: https://support.ricoh.com/bb/html/dr_ut_e/rc3/model/p_i/p_i.htm?lang=en

2-IP printer: 10.0.0.5 /24 **3-periorty :99 for Management | 80 for Graphic Design | 1 for (IT/HR/Sales/Marketing**

We will now install some Group Police to ensure the security of the organization :

Steps to Install and Configure Group Policy

1. Open Group Policy Management

- Log in to your Windows Server with administrative privileges.
- Open Server Manager from the Start menu.
- Click on Tools in the top right corner and select "Group Policy Management."

2. Create a New Group Policy Object (GPO)

- In the Group Policy Management window, expand the forest and domain tree.
- Right-click on the Organizational Unit (OU) where you want to apply the policy.
- Select "Create a GPO in this domain, and Link it here."

- Name your new GPO (e.g., “Security Policy”) and click "OK."

3. Edit the Group Policy Object
   - Right-click on the newly created GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Configure Security Settings
   - In the Group Policy Management Editor, navigate to the following path:
     - Computer Configuration > Policies > Windows Settings > Security Settings.
   - Here, you can configure various security settings:
     - Account Policies: Set password policies, account lockout policies, and Kerberos policies.
     - Local Policies: Configure audit policies, user rights assignments, and security options.
     - Event Log: Configure security event log settings.
     - Restricted Groups: Define group memberships for users.
5. Configure Additional Security Settings
   - You can also navigate to:
     - User Configuration > Policies > Administrative Templates: Set restrictions on user behavior, such as disabling Control Panel access.
     - Computer Configuration > Policies > Administrative Templates: Set system policies for all computers in the OU.
6. Enable Security Auditing
   - To enable auditing, navigate to:
     - Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.
   - Configure auditing for logon events, object access, and other critical security events.
7. Enforce the GPO
   - Once you have configured the settings, close the Group Policy Management Editor.
   - Ensure the GPO is linked to the correct OU, and it will apply to all users and computers within that OU.
8. Force Group Policy Update
   - To apply the new policies immediately, you can force a Group Policy update.
   - Open Command Prompt on client machines and run the following command:

```
bash
gpupdate /force
```

9. Monitor Group Policy Application
   - To verify that the Group Policies have been applied successfully, use the Resultant Set of Policy (RSoP) tool.
   - Open Command Prompt and run:

```
bash
rsop.msc
```

   - This will show the effective policies for the user or computer.

Best Practices for Group Policy Security

- Regularly review and update Group Policies to meet changing security needs.
- Backup Group Policy Objects before making significant changes.
- Document all changes to Group Policies for future reference.
- Limit the number of users with permissions to modify Group Policies

1- Map Sharing police (GP):

To create a Group Policy (GP) that enforces map sharing policies in a Windows environment, follow these steps. This guide will help you configure shared folders and network drives using Group Policy Management.

Steps to Create a Group Policy for Map Sharing

1. Open Group Policy Management
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager and navigate to Tools > Group Policy Management.
2. Create a New Group Policy Object (GPO)
   - In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., a specific department).
   - Select "Create a GPO in this domain, and Link it here."
   - Name your GPO (e.g., “Map Network Drives”) and click "OK."
3. Edit the GPO
   - Right-click on the newly created GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Configure Drive Mapping
   - In the Group Policy Management Editor, navigate to:
     - User Configuration > Preferences > Windows Settings > Drive Maps.
   - Right-click on Drive Maps, select New, and choose Mapped Drive.
5. Set Drive Mapping Properties
   - In the New Mapped Drive Properties window, configure the following:
     - Action: Select Create to create a new mapped drive.
     - Location: Enter the path of the shared folder (e.g., \\ServerName\SharedFolder).
     - Drive Letter: Choose the letter you want to assign to the mapped drive (e.g., Z:).
     - Reconnect: Check this box if you want the drive to reconnect at logon.
     - Label as: Optionally, provide a name for the drive that will appear to users.
6. Configure Additional Options (Optional)
   - You can set additional options, such as:
     - User Configuration: Specify which users or groups should receive the mapped drive.
     - Common: You can set common options like Hide/Show this item, Run in logged-on user’s security context, etc.
7. Apply the GPO
   - Click OK to save your mapped drive settings.
   - Close the Group Policy Management Editor.
8. Force Group Policy Update
   - To apply the new Group Policy immediately, open Command Prompt on client machines and run:

```bash
gpupdate /force
```

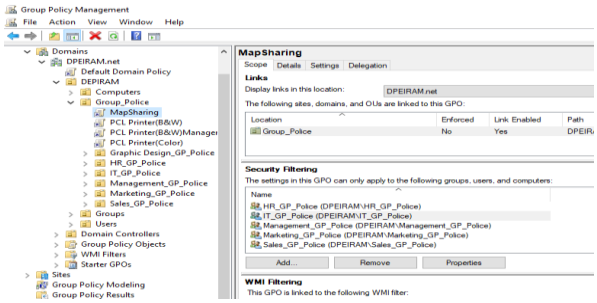
9. Verify the Mapped Drives
   - Log in to a client machine that is part of the OU where the GPO is applied.
   - Open File Explorer and check under This PC to see if the network drive is mapped correctly.

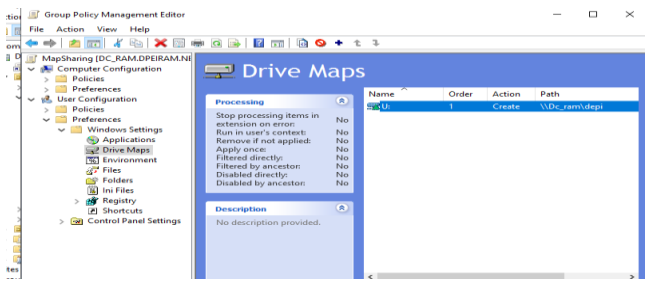
Additional Notes

- Permissions: Ensure that the users have the necessary permissions to access the shared folder.
- Testing: It is advisable to test the GPO on a small group of users before applying it organization-wide.
- Troubleshooting: If the mapped drive does not appear, ensure that Group Policy is applied correctly, and check network connectivity.

The image shows the image of the department's Map Drive permissions:

Path: \\Dc_ram\depi





2-Disable (USB&DVD) _Group Police:

Steps to Disable USB and DVD Drives Using Group Policy

1. Open Group Policy Management
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager and go to Tools > Group Policy Management.
2. Create or Edit a Group Policy Object (GPO)
   - In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., a specific department).
   - Select "Create a GPO in this domain, and Link it here." (If you already have a GPO for security settings, you can edit that instead.)
   - Name your GPO (e.g., “Disable USB and DVD Drives”) and click "OK."
3. Edit the GPO
   - Right-click on the newly created or existing GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Disable USB Drives
   - In the Group Policy Management Editor, navigate to:
     - Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access.
   - Locate the following policies:
     - "All Removable Storage classes: Deny all access"
   - Double-click on this policy and set it to Enabled.
   - Click OK to save the settings.
5. Disable DVD Drives
   - Still in the Removable Storage Access section, locate:
     - "CD and DVD: Deny read access"
     - "CD and DVD: Deny write access"
   - Double-click on each policy and set them to Enabled.
   - Click OK to save the settings.

6. Apply the GPO

- Close the Group Policy Management Editor.
- Ensure the GPO is linked to the correct OU, and it will apply to all computers within that OU.

7. Force Group Policy Update

- To apply the new Group Policy immediately, you can run the following command on the client machines:

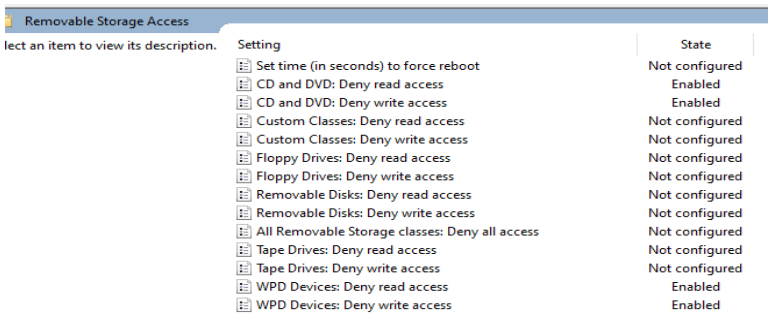
```
bash
gpupdate /force
```

8. Verify the Policy

- Log in to a client machine that is part of the OU where the GPO is applied.
- Try to access a USB drive or DVD drive. The system should deny access.

Important Notes

- Testing: It is advisable to test the GPO on a small group of users or a test OU before applying it organization-wide to avoid disruption.
- Permissions: Ensure that users have necessary permissions for other resources while denying access to removable drives.
- Undoing the Policy: If you need to revert these settings, simply set the policies to Not Configured or Disabled.



3-Disable (ALT+CTRL+DEL) _Group Police:

Steps to Disable Ctrl+Alt+Del Using Group Policy

1. Open Group Policy Management

- Log in to your Windows Server with administrative privileges.
- Open Server Manager and go to Tools > Group Policy Management.

2. Create or Edit a Group Policy Object (GPO)

- In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., a specific department).
- Select "Create a GPO in this domain, and Link it here." (If you already have a GPO for security settings, you can edit that instead.)
- Name your GPO (e.g., “Disable Ctrl+Alt+Del”) and click "OK."

3. Edit the GPO

- Right-click on the newly created or existing GPO and select "Edit."
- This opens the Group Policy Management Editor.

4. Disable the Ctrl+Alt+Del Options

- In the Group Policy Management Editor, navigate to:
    - User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options.
- In this section, you will find several options related to the Ctrl+Alt+Del screen.

5. Configure the Policy Settings

- Double-click on the following policies to configure them:
    - "Remove Task Manager": Set this to Enabled if you want to prevent users from accessing Task Manager.
    - "Remove Change Password": Set this to Enabled if you want to remove the option to change passwords from the security screen.
    - "Remove Lock Computer": Set this to Enabled to prevent users from locking their computers.
    - "Remove Logoff": Set this to Enabled to remove the logoff option.

6. Apply the GPO

- Close the Group Policy Management Editor.
- Ensure the GPO is linked to the correct OU, and it will apply to all users within that OU.

7. Force Group Policy Update

- To apply the new Group Policy immediately, you can run the following command on the client machines:

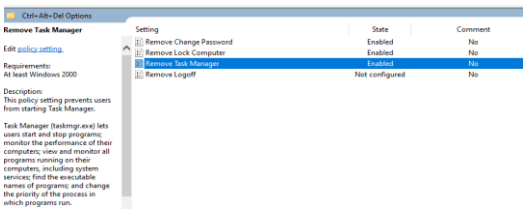
```
bash

gpupdate /force
```

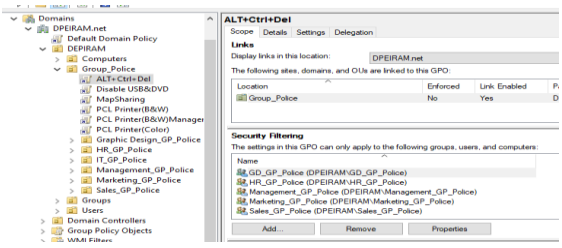
8. Verify the Policy

- Log in to a client machine that is part of the OU where the GPO is applied.
- Press Ctrl+Alt+Del and check the options available. The configured options should be disabled or removed.

Important Notes

- Testing: Always test the GPO on a small group of users or in a test environment before applying it organization-wide to prevent disruption.
- User Experience: Consider the user experience, as removing these options may limit functionality and convenience for users.





4-Disable (Account & Pass) _Group Police:

Steps to Disable Account and Password Settings Using Group Policy

1. Open Group Policy Management
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager and navigate to Tools > Group Policy Management.
2. Create or Edit a Group Policy Object (GPO)
   - In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., specific department or user group).
   - Select "Create a GPO in this domain, and Link it here." (If you already have a GPO for security settings, you can edit that instead.)
   - Name your GPO (e.g., “Disable Account and Password Settings”) and click "OK."
3. Edit the GPO
   - Right-click on the newly created or existing GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Configure Password Policies
   - In the Group Policy Management Editor, navigate to:
     - Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.
   - Here you can modify the following settings:
     - Enforce password history: Set this to 0 to disable password history requirements.
     - Maximum password age: Set this to 0 to effectively disable password expiration.
     - Minimum password age: Set this to 0 to disable minimum age requirements.
     - Minimum password length: Set this to 0 to disable minimum length requirements.
     - Password must meet complexity requirements: Set this to Disabled to remove complexity requirements.
5. Configure Account Lockout Policies
   - Still in the Security Settings section, navigate to:
     - Account Policies > Account Lockout Policy.
   - Here you can configure:
     - Account lockout duration: Set this to 0 to disable account lockout.
     - Account lockout threshold: Set this to 0 to disable account lockouts.
     - Reset account lockout counter after: This can be left as is if lockout is disabled.
6. Apply the GPO
   - Close the Group Policy Management Editor.
   - Ensure the GPO is linked to the correct OU, so it applies to the desired user accounts.
7. Force Group Policy Update
   - To apply the new Group Policy immediately, you can run the following command on the client machines:

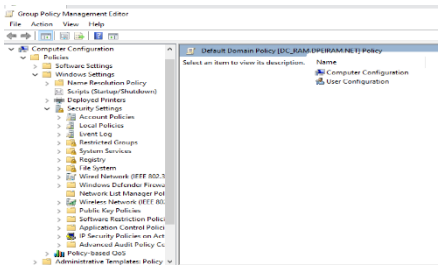
```
bash
gpupdate /force
```

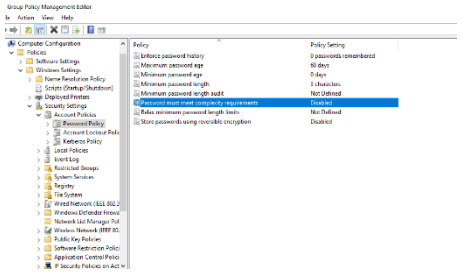
8. Verify the Policy
   - Log in to a client machine that is part of the OU where the GPO is applied.
   - Check the password and account settings by attempting to change passwords or observing account lockout behavior.

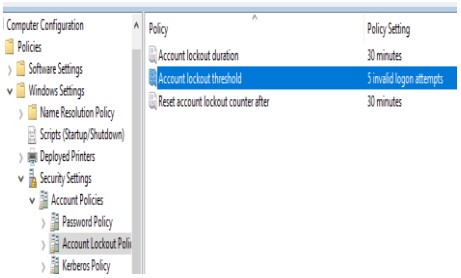
Important Notes

- Testing: It is highly recommended to test the GPO on a small group of users before applying it organization-wide.

- User Security: Disabling these settings can pose security risks. Ensure you have other security measures in place, such as strong authentication methods or monitoring systems.
- Documentation: Document any changes made to Group Policy for future reference and auditing purposes.







5- Disable (Folder Option) _Group police:

Steps to Disable Folder Options Using Group Policy

1. Open Group Policy Management
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager and navigate to Tools > Group Policy Management.
2. Create or Edit a Group Policy Object (GPO)
   - In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., specific department or user group).
   - Select "Create a GPO in this domain, and Link it here." (If you already have a GPO for user settings, you can edit that instead.)
   - Name your GPO (e.g., “Disable Folder Options”) and click "OK."
3. Edit the GPO
   - Right-click on the newly created or existing GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Navigate to User Configuration Settings
   - In the Group Policy Management Editor, navigate to:
     - User Configuration > Administrative Templates > Windows Components > File Explorer (or Windows Explorer, depending on your version).
5. Disable Folder Options
   - Locate the policy named "Remove Folder Options menu from the View menu".
   - Double-click on this policy and set it to Enabled.
   - Click OK to save the settings.
6. Additional Settings (Optional)
   - You may also want to disable the ability to change other settings in File Explorer by configuring the following policies:
     - "Do not allow the use of the search-based method when resolving shell shortcuts": Set this to Enabled.
     - "Prevent the use of the control panel": This will restrict access to the Control Panel, further limiting users' ability to change settings.
7. Apply the GPO
   - Close the Group Policy Management Editor.
   - Ensure the GPO is linked to the correct OU so that it applies to the desired user accounts.

8. Force Group Policy Update

- To apply the new Group Policy immediately, run the following command on the client machines:

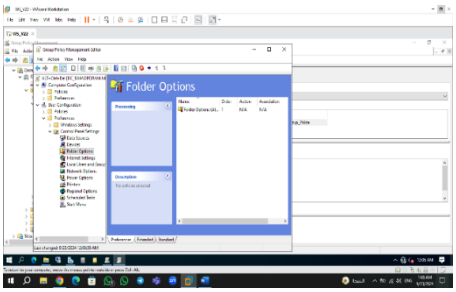
```
bash
gpupdate /force
```

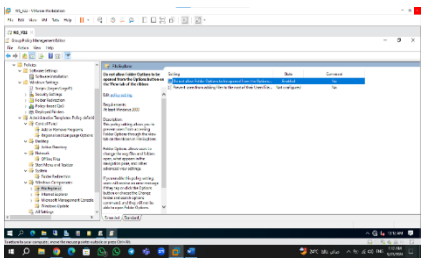
9. Verify the Policy

- Log in to a client machine that is part of the OU where the GPO is applied.
- Open File Explorer and check the View menu. The Folder Options option should be disabled or removed.

Important Notes

- Testing: It is advisable to test the GPO on a small group of users or a test environment before applying it organization-wide to prevent disruption.
- User Experience: Consider the impact on user experience, as disabling Folder Options may limit users' ability to customize their file browsing experience





6-create Shortcuts (URL)_Group police:

Steps to Create URL Shortcuts Using Group Policy

1. Open Group Policy Management

- Log in to your Windows Server with administrative privileges.
- Open Server Manager and navigate to Tools > Group Policy Management.

2. Create or Edit a Group Policy Object (GPO)

- In the Group Policy Management console, right-click on the Organizational Unit (OU) where you want to apply the policy (e.g., a specific department).
- Select "Create a GPO in this domain, and Link it here." (If you already have a GPO for user settings, you can edit that instead.)
- Name your GPO (e.g., “Create URL Shortcuts”) and click "OK."

3. Edit the GPO

- Right-click on the newly created or existing GPO and select "Edit."
- This opens the Group Policy Management Editor.

4. Navigate to User Configuration Settings

- In the Group Policy Management Editor, navigate to:

    - User Configuration > Preferences > Windows Settings > Shortcuts.

5. Create a New Shortcut

- Right-click on Shortcuts, then select New > Shortcut.

6. Configure the Shortcut Properties

In the New Shortcut Properties window, configure the following settings:

- Action: Select Create to create a new shortcut.
- Name: Enter a name for the shortcut (e.g., "Company Intranet").
- Target type: Select URL from the dropdown menu.
- Location: Choose where to place the shortcut:
    - Desktop: To place it on the user's desktop.
    - Start Menu: To place it in the Start Menu.
    - Quick Launch: To place it in the Quick Launch bar (if applicable).
- Target URL: Enter the URL of the website you want to link to (e.g., https://www.example.com).
- Icon file: Optionally, you can specify a custom icon for the shortcut by browsing to an icon file (e.g., .ico).

7. Additional Settings (Optional)

- You can set additional options such as:
    - Comment: Add a description that will be displayed when the user hovers over the shortcut.
    - Common: You can set common options like Hide/Show this item, Run in logged-on user's security context, etc.

8. Apply the GPO

- Click OK to save your shortcut settings.
- Close the Group Policy Management Editor.

9. Force Group Policy Update

- To apply the new Group Policy immediately, you can run the following command on the client machines:

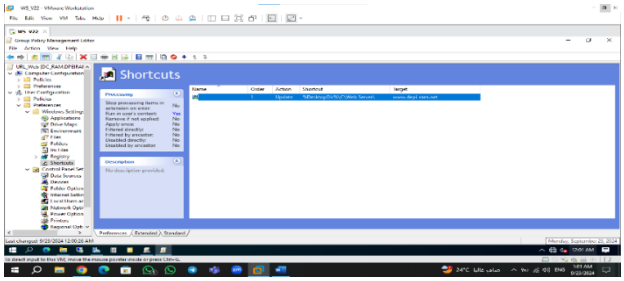
```
bash

gpupdate /force
```

10. Verify the Shortcut

- Log in to a client machine that is part of the OU where the GPO is applied.
- Check the desktop or Start Menu to see if the URL shortcut has been created successfully.

Important Notes

- Testing: Always test the GPO on a small group of users before applying it organization-wide to ensure everything works as expected.
- User Experience: Providing shortcuts can enhance user experience by facilitating quick access to essential resources.



Here’s how to apply Group Policy to restrict internet access for all devices except specific groups (like Graphic Design, IT, and Marketing and Sales):

Steps to Apply Group Policy

1. Open Group Policy Management
   - Log in to your Windows Server with administrative privileges.
   - Open Server Manager and go to Tools > Group Policy Management.
2. Create a New GPO
   - In Group Policy Management, right-click on the Domain or OU containing the devices you want to apply the policy to.
   - Select "Create a GPO in this domain, and Link it here."
   - Name the GPO (e.g., "Restrict Internet Access") and click OK.
3. Edit the GPO
   - Right-click on the newly created GPO and select "Edit."
   - This opens the Group Policy Management Editor.
4. Configure the Restriction Settings
   - Navigate to:
     - User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Connection.
   - Right-click on Connection and select "Configure Proxy Settings."
   - Enter proxy settings that will prevent unauthorized devices from accessing the internet (like an incorrect IP address).
5. Specify Allowed Groups
   - In the Group Policy Management Editor, go to:
     - User Configuration > Preferences > Control Panel Settings > Network Options.

- Right-click and select "New" > "Network Connection."
- Enter the network settings for the allowed groups.

6. Apply the GPO

- Close the Group Policy Management Editor.
- Ensure the GPO is linked to the correct OU or Domain containing the devices.

7. Cut Internet Access for Other Devices

- If you're using a router or firewall, you can restrict internet access for unauthorized devices through the router or firewall settings.
- Create a rule to block the IP addresses of unauthorized devices from accessing the internet.
- You can also disable DHCP for unauthorized devices.

8. Update Group Policy

- To apply the new policy on devices, you can run the following command on each device:

```
bash

gpupdate /force
```

9. Test Connectivity

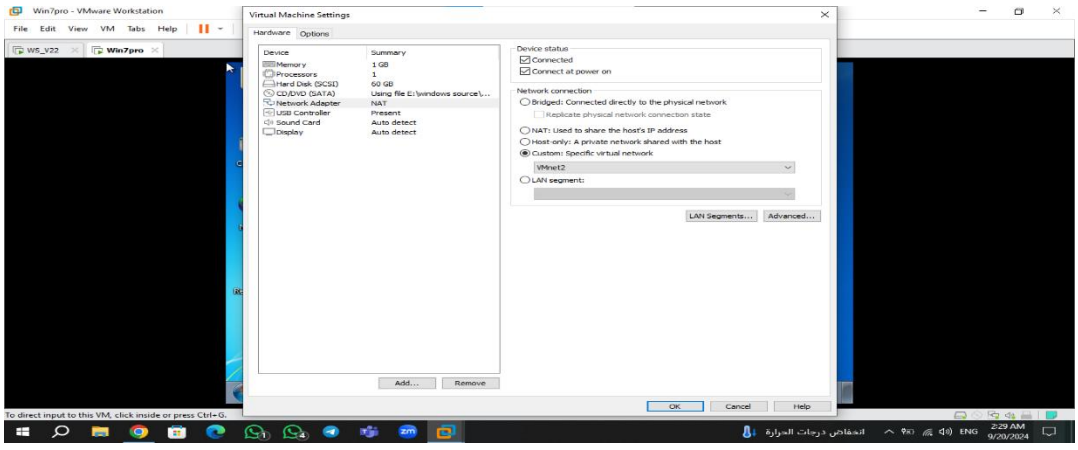
- Verify that the devices that are restricted cannot access the internet, while the allowed groups maintain access.

Important Notes

- Policy Testing: It's advisable to test the policy on a small group of devices before applying it across the entire domain.
- User Sign-In: Ensure that all devices are connected to the network and logging in with the appropriate user accounts.

The final phase is the testing phase. The initial domain machine will be configured to verify the efficacy of the completed work.

Firstly, the device and server will be placed on the same network. A basic procedure will then be performed to confirm the connection. Clint will be able to view the server and access the images.



Subsequently, a test will be conducted on the client machine to ascertain the efficacy of the operations performed on the server.

A Join Domain computer will then be created, comprising the Windows 10 Pro operating system.

OS: Windows 10 Pro 64bit 2022 Update | Version 22H2

Link: https://www.microsoft.com/en-us/software-download/windows10

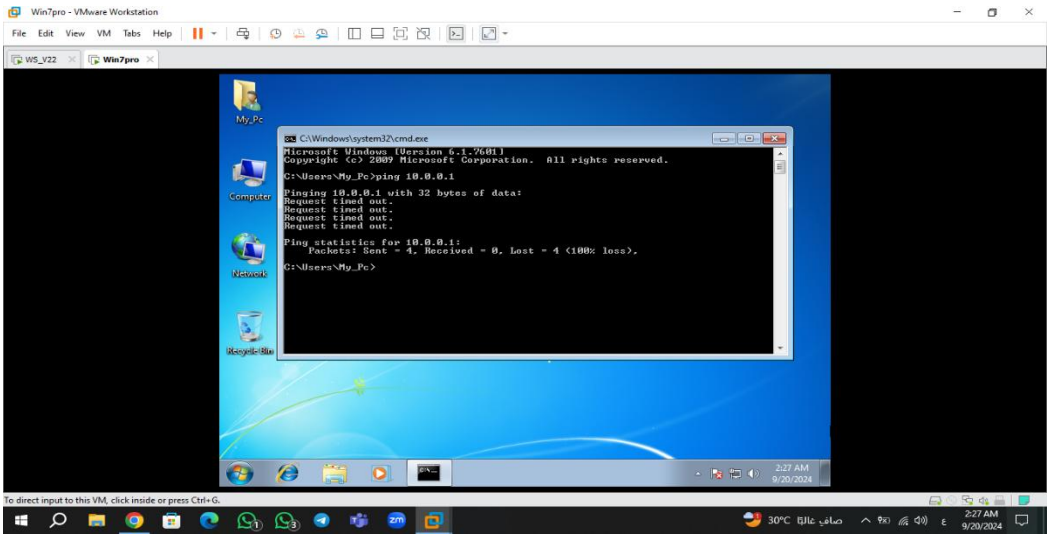
License key used: W269N-WFGWX-YVC9B-4J6C9-T83GX

Link File Use to Active: https://drive.google.com/file/d/1eiKyXA-Eavmo4aT4M73O5V41hTSXirwD/view?usp=drive_link

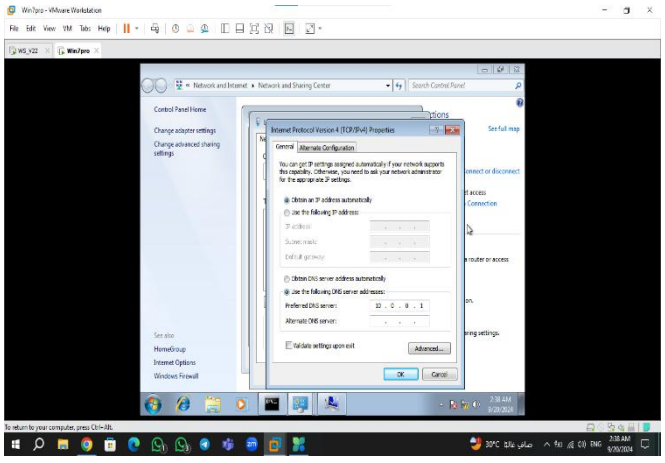
Pc name : Win10

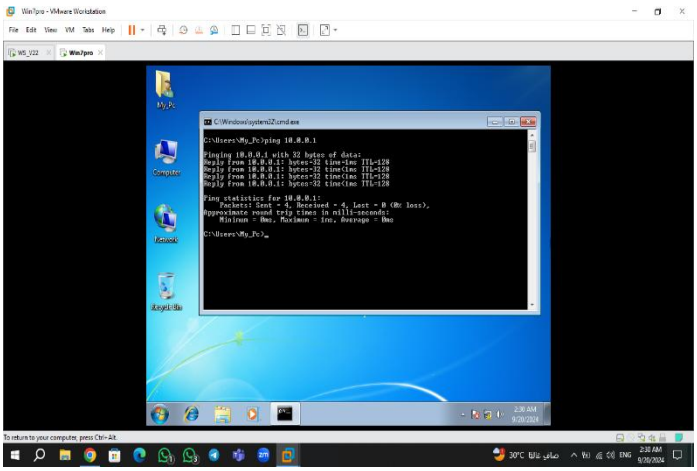
Pass:P@ssw0rd

We shall proceed to the command prompt and enter the requisite command to ascertain the operational status of the server. As illustrated in the accompanying screenshot, the next step is to ping 10.0.0.1.

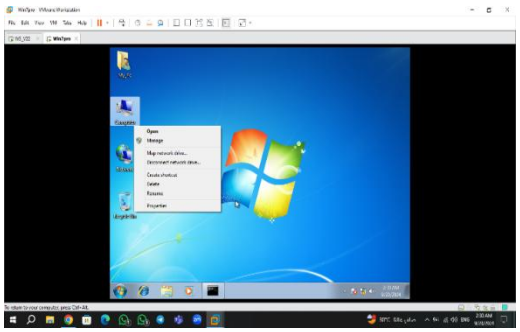


In the event of encountering this issue, it is imperative to ascertain the time zone of both the server and the client. Furthermore, it is essential to confirm the functionality of the DHCP server and ensure that it is operating within the same network range. Should this issue persist, it is recommended that the DNS be added to the network adapter, which should then function as intended.

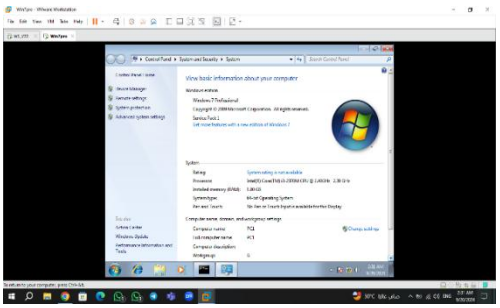




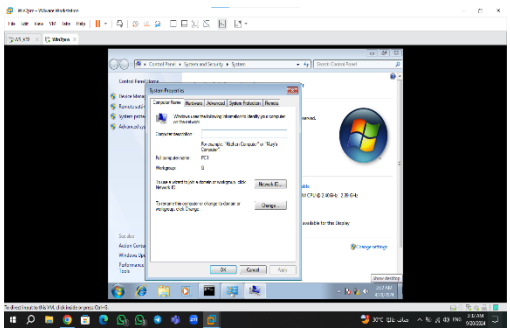
Let us now proceed to the Settings menu and modify the device name. Subsequently, the device will be restarted. It should be noted that the alteration of the device name and the completion of join domain phases are two distinct steps. Consequently, these processes must be carried out in sequence.



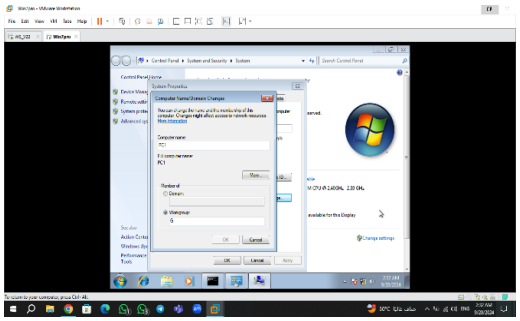
Click Manage



Change Settings

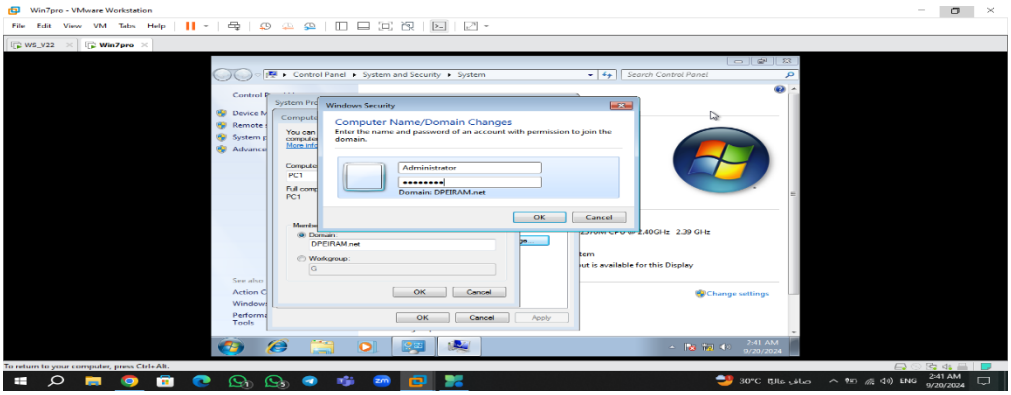


Change pc name



Go ahead and click on the Domain tab. Type in our domain and click Enter.

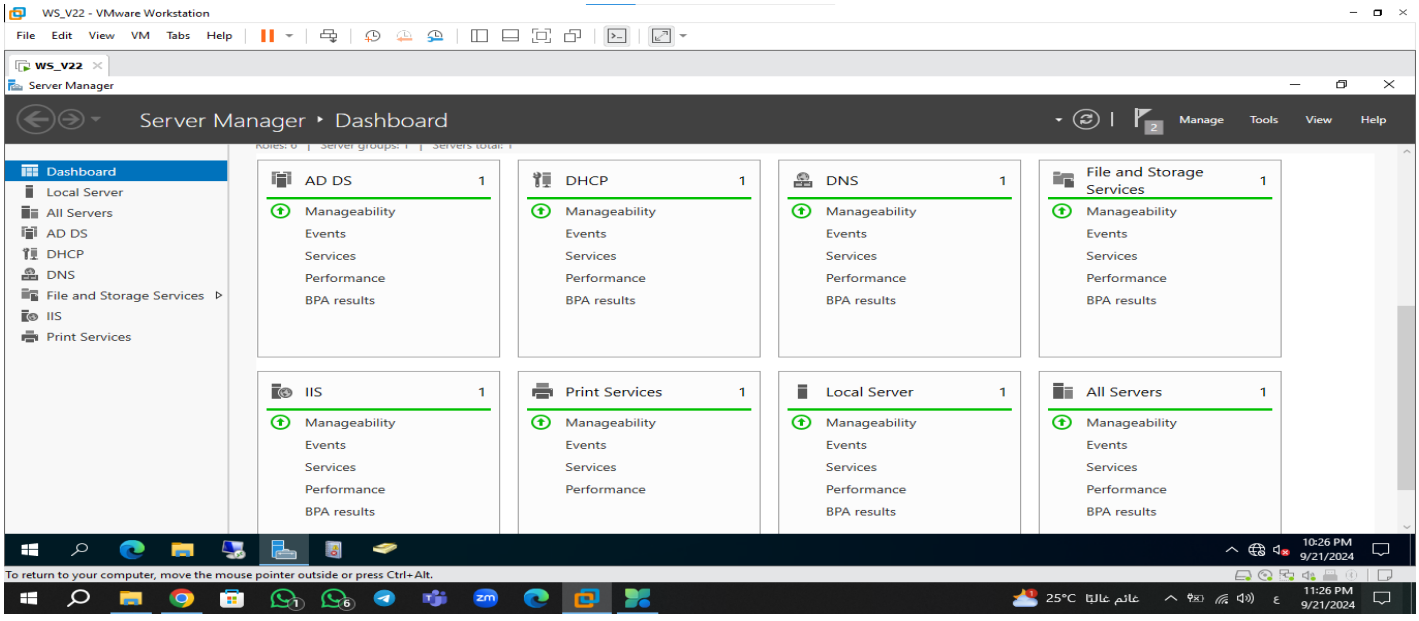
Enter the employee's username and password from any department or the administrator's username and password as shown in the image



User: Administrator
Pass: P@ssw0rd

Upon selecting the "OK" option, Damien will be successfully joined, and the process will be concluded.

The task has been completed and the final stage before delivery has been reached. This is the preliminary stage of the delivery process, during which all outstanding issues are reviewed and resolved.



I can confirm that the server is operational.

Network Troubleshooting:

1. Unable to Access the Internet

Problem: The user cannot access the internet.

Steps to Solve the Problem:

1. Check Physical Connections:
    - Ensure the computer is properly connected to the Wi-Fi or wired network.
    - Check the router's lights to ensure it's functioning correctly.
2. Test Connectivity:
    - Open Command Prompt and use the command:

```
bash
ping 8.8.8.8
```

    - If you receive replies, the local network is working. If not, check the cables or network settings.
3. Check IP Configuration:
    - Open Command Prompt and use the command:

```
bash
ipconfig
```

    - Ensure you have a valid IP address.
4. Restart Devices:
    - Restart the router and the computer.
5. Check DNS Settings:
    - Ensure DNS settings are correct. You can use a public DNS like:
        - 8.8.8.8 (Google)
        - 1.1.1.1 (Cloudflare)

---

2. Device Not Joining the Network

Problem: A computer is unable to join the network.

Steps to Solve the Problem:

1. Check Network Adapter Status:
    - Go to Device Manager and check the network adapter's status. Ensure there are no warning signs.
2. Verify Network Settings:
    - Check that the IP settings match those in the network. Use the command:

```
bash
ipconfig /all
```

3. Reset Network Settings:
    - Use the command:

```
bash
netsh int ip reset
netsh winsock reset
```

4. Update Network Drivers:
    - Ensure the drivers are up to date. Visit the manufacturer's website for the latest drivers.
5. Restart the Device:
    - Restart the device and attempt to join the network again.

---

3. DHCP Issues

Problem: Devices are not receiving IP addresses from the DHCP server.

Steps to Solve the Problem:

1. Check DHCP Server Status:
    - Open DHCP Management Console and ensure the service is running and scopes are available.
2. Verify Scope Settings:
    - Make sure the DHCP scope has available IP addresses for distribution.
3. Restart DHCP Service:
    - Restart the DHCP service from Services.
4. Check for IP Conflicts:
    - Ensure that no devices are using the same IP address.
5. Restart Devices:
    - Restart the affected devices to try obtaining a new IP address.

---

4. Connectivity Issues Between Devices

Problem: Devices are unable to communicate with each other.

Steps to Solve the Problem:

1. Check Firewall Settings:
    - Ensure that the firewall on each device is not blocking communications.
2. Use Ping Command:
    - Try using the ping command from one device to another to check connectivity:

```
bash
ping [IP Address of another device]
```

3. Verify Workgroup Settings:
    - Ensure all devices are in the same workgroup or domain.
4. Update Network Settings:
    - If using static IP addresses, ensure the addresses being used do not conflict with others.
5. Restart Devices:
    - Restart all involved devices.

---

5. Slow Internet Browsing

Problem: Internet speed is unusually slow.

Steps to Solve the Problem:

1. Test Internet Speed:
    - Use a site like speedtest.net to check your connection speed.
2. Check Connected Devices:
    - Ensure that no other devices are using bandwidth excessively (e.g., large downloads).
3. Restart the Router:
    - Restart the router.
4. Check for Malware:
    - Ensure no malware is affecting network performance. Use antivirus software to scan the system.
5. Update Software:
    - Ensure all software is updated to the latest version.
    -

---

6. Wireless Connection Drops Frequently

Problem: The wireless connection keeps disconnecting.

Steps to Solve the Problem:

1. Check Signal Strength:
    - Ensure the device is within range of the Wi-Fi router. Weak signals can cause drops.
2. Change Wi-Fi Channel:
    - Log into the router's settings and change the Wi-Fi channel to reduce interference from nearby networks.
3. Update Wireless Drivers:

- Ensure the device's wireless network adapter drivers are up to date. Check the manufacturer's website for updates.

4. Disable Power-Saving Features:
    - Go to Device Manager, find the wireless adapter, and disable any power-saving features that may be causing the disconnection.
5. Reset Network Settings:
    - On Windows, go to Settings > Network & Internet > Status > Network Reset.

---

7. Cannot Connect to Specific Websites

Problem: The device can access some websites but not others.

Steps to Solve the Problem:

1. Clear Browser Cache:
    - Clear the browser cache and cookies to resolve potential loading issues.
2. Check Firewall/Antivirus:
    - Ensure that the firewall or antivirus software is not blocking access to specific websites.
3. Check Hosts File:
    - Open the hosts file located at C:\Windows\System32\drivers\etc\hosts and check if the website is listed there. Remove any unwanted entries.
4. Use Different Browser:
    - Try accessing the website using a different browser to rule out browser-specific issues.
5. Check DNS Settings:
    - Change the DNS settings to a public DNS server like Google (8.8.8.8) or Cloudflare (1.1.1.1).

---

8. Network Printer Not Detected

Problem: The network printer is not detected by devices on the network.

Steps to Solve the Problem:

1. Check Printer Connections:
    - Ensure the printer is turned on and connected to the same network as the devices.
2. Restart Printer:
    - Power cycle the printer by turning it off, waiting a few seconds, and turning it back on.
3. Update Printer Drivers:

- Make sure that the printer drivers are up to date on the devices trying to access the printer.

4. Check Network Settings on Printer:
   - Print a network configuration page from the printer to ensure it has a valid IP address.
5. Re-add the Printer:
   - Go to Devices and Printers on Windows and remove the printer. Then, add it again using the Add a printer wizard.

---

9. IP Address Conflict

Problem: Two devices on the network have the same IP address.

Steps to Solve the Problem:

1. Identify Conflicting Devices:
   - Use the command:

```
bash
arp -a
```

   - Look for duplicate IP addresses in the list.
2. Change IP Address:
   - Manually change the IP address of one of the conflicting devices or set the DHCP server to assign dynamic addresses.
3. Release and Renew IP Address:
   - On the affected devices, use the following commands:

```
bash
ipconfig /release
ipconfig /renew
```

4. Check DHCP Settings:
   - Ensure the DHCP server has a proper scope and is not running out of IP addresses.

---

10. VPN Connection Issues

Problem: The VPN connection fails to establish.

Steps to Solve the Problem:

1. Check Internet Connectivity:
   - Ensure that the device has a stable internet connection before connecting to the VPN.

2. Verify VPN Credentials:
    - Double-check the VPN username and password for accuracy.
3. Restart VPN Client:
    - Close and restart the VPN client application.
4. Update VPN Client:
    - Ensure the VPN client software is up to date. Check the vendor's website for updates.
5. Firewall Settings:
    - Check that the firewall is not blocking the VPN connection. You may need to create an exception for the VPN application.

---

11. Slow Network Performance

Problem: The network is running slowly, affecting file transfers and streaming.
Steps to Solve the Problem:

1. Check for Bandwidth Usage:
    - Use tools to monitor network usage and identify if any applications are consuming excessive bandwidth (e.g., downloads, backups, streaming services).
2. Limit Background Applications:
    - Close unnecessary applications and background processes that may be using the network.
3. Upgrade Internet Plan:
    - If multiple users are consistently experiencing slow speeds, consider upgrading to a higher bandwidth plan with your ISP.
4. Optimize Wi-Fi Settings:
    - Change the Wi-Fi channel to a less congested one, especially in dense residential areas.
    - Enable Quality of Service (QoS) settings on the router to prioritize certain types of traffic.
5. Check for Interference:
    - Ensure that the router is placed away from electronic devices that may cause interference (like microwaves, cordless phones).

---

12. Frequent Disconnections from Wi-Fi

Problem: The device frequently disconnects from the Wi-Fi network.
Steps to Solve the Problem:

1. Forget and Reconnect:
    - On the device, forget the Wi-Fi network and reconnect by entering the password again.
2. Check Router Placement:
    - Ensure the router is in a central location in the home or office to provide better coverage.
3. Update Firmware:
    - Log into the router's settings and check for firmware updates. Update if necessary.
4. Change Security Settings:
    - Change the security settings on the router (e.g., from WPA2 to WPA3, or vice versa) to see if it improves stability.
5. Adjust Wi-Fi Frequency:
    - If the router supports both 2.4 GHz and 5 GHz, try switching to the 5 GHz band for better performance in close proximity.

13. Email Connection Issues

Problem: Unable to send or receive emails.
Steps to Solve the Problem:

1. Check Internet Connection:
    - Ensure the device is connected to the internet.
2. Verify Email Settings:
    - Confirm the incoming and outgoing server settings in the email client match the recommended settings from the email provider.
3. Check for Email Quota:
    - Ensure that the email account is not exceeding its storage limit, which can prevent new emails from being received.
4. Disable Antivirus/Firewall Temporarily:
    - Temporarily disable antivirus or firewall software to see if it's blocking email traffic.
5. Recreate Email Account:
    - If issues persist, remove the email account from the email client and add it again.

---

14. Network Device Not Found

Problem: A network device (like a printer or file share) cannot be found.
Steps to Solve the Problem:

1. Check Network Visibility:
    - Ensure that network discovery is enabled on the device. For Windows, go to Control Panel > Network and Sharing Center > Change advanced sharing settings.
2. Ping the Device:
    - Use the ping command to check if the device is reachable:

bash
Copy code
ping [IP address of the device]

3. Verify Network Connection:
    - Make sure the device is connected to the network and powered on.
4. Check Firewall Settings:
    - Ensure that the firewall on the device is not blocking incoming connections.
5. Update Network Drivers:
    - Ensure that network drivers are up to date on both the device trying to access and the device being accessed.

---

15. Router Not Responding

Problem: The router is unresponsive and cannot be accessed.
Steps to Solve the Problem:

1. Power Cycle the Router:
    - Unplug the router, wait for 30 seconds, and plug it back in to reboot.
2. Check for Overheating:
    - Ensure the router is not overheating. If it is, relocate it to a cooler area.
3. Factory Reset:
    - If all else fails, perform a factory reset on the router. Note that this will erase all configurations:
        - Press and hold the reset button (usually located at the back) for about 10 seconds.

4. Check for Firmware Issues:
    - If accessible, check for firmware updates that may resolve bugs or stability issues.
5. Contact ISP:
    - If the router still does not respond, contact your Internet Service Provider for assistance.

---

16. Security Breaches or Suspicious Activity

Problem: Unusual activity or security breaches on the network.
Steps to Solve the Problem:

1. Change Passwords:
    - Immediately change passwords for the router and all devices connected to the network.
2. Update Security Protocols:
    - Ensure that the router is using strong security protocols (WPA2 or WPA3).
3. Check Connected Devices:
    - Log into the router and check for any unauthorized devices connected to the network.
4. Install Security Software:
    - Install and regularly update antivirus and anti-malware software on all devices.
5. Monitor Network Traffic:
    - Use network monitoring tools to keep an eye on traffic and detect any anomalies.

---

17. VoIP Call Quality Issues

Problem: VoIP calls are dropping or have poor audio quality.
Steps to Solve the Problem:

1. Check Bandwidth:
    - Ensure there's enough bandwidth available for VoIP calls. A minimum of 100 kbps is typically needed per call.
2. Prioritize VoIP Traffic:
    - Enable Quality of Service (QoS) settings on the router to prioritize VoIP traffic over other types of traffic.
3. Inspect Network Configuration:
    - Ensure the firewall is configured to allow VoIP traffic. Check SIP and RTP ports.
4. Check for Latency:
    - Use the ping command to test latency to the VoIP server:

```
bash
ping [VoIP server address]
```

    - If latency is high (over 150 ms), investigate further.
5. Test Different Devices:
    - If possible, test calls on different devices to rule out device-specific issues.

---

18. DNS Issues

Problem: Websites are not resolving, or there are frequent DNS errors.
Steps to Solve the Problem:

1. Flush DNS Cache:
    - Open Command Prompt and use the command:

```
bash
ipconfig /flushdns
```

2. Change DNS Server:
    - Change to a public DNS server (like Google DNS 8.8.8.8) in the network settings.
3. Check Host File:
    - Inspect the hosts file for incorrect entries that might be causing DNS resolution issues:
        - Location: C:\Windows\System32\drivers\etc\hosts
4. Restart DNS Client Service:
    - Open Services and restart the DNS Client service.
5. Test Connectivity:
    - Use the nslookup command to test DNS resolution for a specific website:

```
bash
nslookup [website]
```

---

19. Network Switch Issues

Problem: Devices connected to a switch cannot communicate with each other.
Steps to Solve the Problem:

1. Check Physical Connections:
    - Ensure all cables are securely connected to the switch and devices.
2. Restart the Switch:
    - Power cycle the switch to clear any temporary issues.
3. Inspect Switch Configuration:
    - Log into the switch management interface to check for VLAN configurations or port security settings that may be blocking communication.
4. Update Firmware:
    - Check for firmware updates for the switch and apply them if necessary.
5. Use Diagnostic Tools:
    - Use network diagnostic tools (like tracert) to identify where communication is failing.

---

20. IP Address Assignment Issues

Problem: Devices are unable to obtain IP addresses from the DHCP server.
Steps to Solve the Problem:

1. Restart DHCP Service:
    - Restart the DHCP service on the server to refresh IP assignment.
2. Check DHCP Scope:
    - Verify that the DHCP scope has enough IP addresses available for assignment.
3. Check for IP Conflicts:
    - Use arp -a to check for duplicate IP addresses on the network.
4. Release/Renew IP Address:
    - On the affected device, use the commands:

```
bash
ipconfig /release
ipconfig /renew
```

5. Verify DHCP Client Settings:
    - Ensure that the affected devices are set to obtain an IP address automatically.

21. Network Authentication Issues

Problem: Users are unable to authenticate to the network.
Steps to Solve the Problem:

1. Verify Credentials:
    - Ensure users are entering the correct username and password.
2. Check Domain Controller Status:
    - If using Active Directory, ensure the domain controller is online and functioning.
3. Review Network Policies:
    - Check for any Group Policies that may affect user authentication.
4. Inspect Network Time:
    - Ensure the device's clock is synchronized with the domain controller. Time discrepancies can cause authentication failures.
5. Reset User Passwords:
    - If necessary, reset user passwords to resolve authentication issues.

---

22. File Sharing Issues

Problem: Unable to access shared files or folders on the network.
Steps to Solve the Problem:

1. Check Sharing Permissions:
    - Ensure that the folder is shared and that users have appropriate permissions to access it.
2. Verify Network Discovery:
    - Ensure network discovery is enabled on the devices trying to access shared resources.
3. Use the UNC Path:
    - Try accessing the shared folder using the UNC path:

```bash
\\[ComputerName]\[SharedFolder]
```

4. Check Firewall Settings:
    - Ensure that the firewall on both the host and accessing devices is not blocking file sharing ports.
5. Restart File and Print Sharing Service:
    - Restart the File and Print Sharing service on the host machine.

---

23. Network Time Protocol (NTP) Issues

Problem: Devices are not synchronizing time correctly.
Steps to Solve the Problem:

1. Verify NTP Configuration:
    - Check the NTP server settings on the devices. Ensure they point to a reliable NTP server.
2. Restart Time Services:
    - Restart the Windows Time service using:

```bash
net stop w32time
net start w32time
```

3. Manually Sync Time:
    - Use the command:

```bash
w32tm /resync
```

4. Check Firewall Rules:
    - Ensure that the firewall allows NTP traffic (UDP port 123).

5. Test Connectivity:
    - Use the command:

```
bash
w32tm /query /status
```

    - This can provide insights into the time synchronization status.

---

24. Remote Desktop Connection Issues

Problem: Unable to connect to a remote desktop.
Steps to Solve the Problem:

1. Check Remote Desktop Settings:
    - Ensure that remote desktop is enabled on the target machine.
2. Verify Network Connectivity:
    - Ensure the device attempting to connect is on the same network or has the necessary routing in place.
3. Inspect Firewall Settings:
    - Make sure that the firewall on the remote machine allows Remote Desktop connections (default port is 3389).
4. Test with IP Address:
    - Instead of using the hostname, try connecting using the IP address of the remote machine.
5. Review Group Policies:
    - Ensure that there are no Group Policies preventing remote desktop connections

---

25. Limited or No Connectivity

Problem: A device shows a status of "Limited" or "No Connectivity."
Steps to Solve the Problem:

1. Restart the Device:
    - Restart the device that is having connectivity issues to reset its network settings.
2. Check Physical Connections:
    - Ensure that Ethernet cables are properly connected and that there are no loose connections.
3. Forget and Reconnect:
    - On wireless devices, forget the Wi-Fi network and reconnect by entering the password again.
4. Release and Renew IP Address:
    - Use the following commands in Command Prompt:

```
bash
ipconfig /release
ipconfig /renew
```

5. Run Network Troubleshooter:
    - Use the built-in network troubleshooter in Windows by navigating to Settings > Network & Internet > Status > Network troubleshooter.

---

26. Packet Loss

Problem: Data packets are being lost during transmission, leading to poor performance.
Steps to Solve the Problem:

1. Check Network Cable Connections:
    - Ensure all cables are securely connected and not damaged.
2. Ping Test:
    - Use the command:

```
bash
ping [destination IP] -t
```

    - Look for packet loss percentage in the results.
3. Inspect Network Devices:
    - Restart routers, switches, and modems to clear temporary issues.
4. Update Network Drivers:
    - Ensure that the network adapter drivers on the devices are up to date.
5. Check for Interference:
    - Identify and eliminate any sources of interference (e.g., microwaves, cordless phones) if using wireless connections.

---

27. VPN Connection Drops

Problem: The VPN connection is unstable and drops frequently.
Steps to Solve the Problem:

1. Check Internet Stability:
    - Ensure that the primary internet connection is stable and has sufficient bandwidth.
2. Change VPN Protocol:
    - Switch between different VPN protocols (e.g., from OpenVPN to L2TP or IKEv2) within the VPN client settings.
3. Adjust MTU Settings:
    - Lower the MTU (Maximum Transmission Unit) settings in the VPN client to see if it stabilizes the connection.
4. Disable IPv6:
    - In some cases, disabling IPv6 on the VPN client can resolve connection drops.
5. Reinstall VPN Client:
    - Uninstall and then reinstall the VPN client software to ensure all settings are reset.

---

28. No Internet Access After Changing Router Settings

Problem: Users lose internet access after modifying router settings.
Steps to Solve the Problem:

1. Reset Router to Factory Settings:
    - If critical settings were changed, reset the router to factory defaults and reconfigure it.
2. Verify WAN Settings:
    - Ensure that the WAN (Wide Area Network) settings are correctly configured, including IP addressing (static or DHCP) from the ISP.
3. Check for IP Address Conflicts:
    - Confirm that there are no IP conflicts within the network by checking connected devices.
4. Power Cycle the Router:
    - Restart the router to apply changes effectively.
5. Consult ISP:
    - If issues persist, contact the ISP for assistance regarding internet connectivity.

29. File Transfer Issues Over the Network

Problem: Slow or failed file transfers between networked devices.
Steps to Solve the Problem:

1. Check Network Speed:
    - Use speed test tools to check the local network speed. Identify if the transfer speed is consistent.
2. Inspect Network Configuration:
    - Ensure that there are no configurations limiting bandwidth for file transfers.
3. Disable Antivirus Temporarily:
    - Some antivirus programs may interfere with file transfers. Temporarily disable them to see if performance improves.
4. Use Wired Connection:
    - If transferring files over Wi-Fi, switch to a wired Ethernet connection for faster speeds.
5. Limit Background Processes:
    - Close any unnecessary applications that may be using network resources during file transfers.

---

30. Router Overheating

Problem: The router becomes unresponsive due to overheating.
Steps to Solve the Problem:

1. Check Router Placement:
    - Ensure the router is placed in a well-ventilated area, away from direct sunlight or heat sources.
2. Clean Dust and Debris:
    - Regularly clean dust from the router's vents to prevent airflow blockage.
3. Power Cycle the Router:
    - Restart the router to cool down and clear temporary issues.
4. Upgrade Firmware:
    - Check for firmware updates that may optimize the router’s performance and heat management.
5. Consider Cooling Solutions:
    - If overheating persists, consider adding a fan or using a cooling pad for the router.

---

31. Network Configuration Errors

Problem: Incorrect network configurations prevent devices from connecting.
Steps to Solve the Problem:

1. Review IP Configuration:
    - Use the command:

```
bash
ipconfig /all
```

    - Check for incorrect IP addresses, subnet masks, and gateway settings.
2. Check DNS Settings:
    - Ensure that DNS settings are correctly configured, either for automatic assignment or pointing to the right DNS server.
3. Verify Network Adapter Settings:
    - Ensure that the network adapter is enabled and configured properly in Device Manager.
4. Run Network Reset:
    - On Windows, go to Settings > Network & Internet > Status > Network Reset to reset all network configurations.
5. Consult Documentation:

- Refer to device manuals for proper configuration steps or consult IT support if available.

---

32. Malware or Virus Infections Affecting Network Performance

Problem: Network performance is compromised due to malware or viruses.
Steps to Solve the Problem:

1. Run Full System Scans:
   - Use reliable antivirus software to perform full scans on affected devices.
2. Update Security Software:
   - Ensure all security software is up to date with the latest virus definitions.
3. Disconnect Infected Devices:
   - Temporarily disconnect infected devices from the network to prevent further spread.
4. Review Network Traffic:
   - Use network monitoring tools to identify suspicious traffic patterns indicative of malware activity.
5. Restore Systems:
   - If infections are severe, consider restoring systems from clean backups or reinstalling the operating system.

---

33. Inconsistent Connectivity Across Devices

Problem: Some devices connect to the network while others do not.
Steps to Solve the Problem:

1. Check Compatibility:
   - Ensure that all devices are compatible with the network (e.g., Wi-Fi standards, supported frequencies).
2. Inspect Device Settings:
   - Verify that network settings on the problematic devices are configured correctly (e.g., IP configuration, Wi-Fi credentials).
3. Reset Network Settings:
   - On devices with connectivity issues, reset network settings to default and reconnect.
4. Update Device Drivers:
   - Ensure that network drivers on all devices are updated to the latest versions.
5. Check for Device Limits:
   - Some routers have a limit on the number of devices that can connect. Check the router's settings to see if this limit has been reached.

---

34. Outdated Network Hardware

Problem: Older hardware may not support newer network standards.
Steps to Solve the Problem:

1. Upgrade Hardware:
   - Consider upgrading to newer routers, switches, or network cards that support the latest standards (like Wi-Fi 6).
2. Check Compatibility:
   - Ensure that all network devices (routers, switches, and adapters) are compatible with each other.
3. Review Performance Reports:
   - Analyze performance reports and logs to determine if hardware upgrades are necessary for efficiency.
4. Consult IT Support:
   - If unsure about hardware specifications, consult with IT support for recommendations based on current and future needs.
5. Test Alternative Solutions:

- Before upgrading, test different configurations or setups to see if existing hardware can meet the requirements with tweaks.

Conclusion:

In conclusion, the successful configuration and troubleshooting of network systems are critical components for ensuring seamless communication and data exchange within any organization. This project has sought to elucidate the essential steps involved in establishing a robust network infrastructure, from the initial design phase to the practical implementation stage.

I would like to express my sincerest gratitude to Dr. Mustafa Salah for the invaluable experience and insights gained during this project.

The necessity of comprehensive planning and implementation in network configuration has been emphasised, including the selection of suitable hardware, the configuration of IP addresses and the establishment of secure connections. Furthermore, our emphasis on troubleshooting has highlighted the importance of promptly identifying and resolving common network issues, thereby ensuring minimal downtime and optimal performance.

The implementation of systematic approaches and best practices in network management enables organizations to enhance their operational efficiency and maintain a secure and reliable networking environment. The insights gained from this project not only equip us with the necessary skills to address current network challenges but also prepare us for future advancements in technology.

His guidance and expertise have significantly enhanced our learning experience, and we have gained invaluable knowledge under his mentorship

Contact Information:

For further information or inquiries regarding our project on Network Setup, Configuration, and Troubleshooting, please feel free to reach out to any of us:

Team Members:

1. **AbdulRhman AbdulGhaffar**

- **Role**: Network Setup & Configuration, and Documentation Project
- **Email**: abdulrhman.abdulghaffar001@gmail.com
- **Phone**: +201093981406
- **LinkedIn**: https://www.linkedin.com/in/abdulrhmanabdulghaffar

2. **Ramzey Elsayed**

- **Role**: **Network Troubleshooting**
- **Email**: zpx15266@gmail.com
- **Phone**: +201024975563
- **LinkedIn**: https://www.linkedin.com/in/ramzey-elsayed-mohamed-1a2126246?utm_source=share&utm_campaign=share_via&utm_content=profile&utm_medium=android_app

3. **Mustafa Abdullah**

- **Role**: **Design and Planning of Networks**
- **Email**: sasaelsaedy08@gmail.com
- **Phone**: +201114572543
- **LinkedIn**: https://www.linkedin.com/in/mustafa-abdullah-032205274/

We are delighted to connect with you and welcome any questions, feedback, or discussions related to our project and its application in network management. Thank you for your interest and support

I welcome any feedback, questions, or discussions related to the project and am eager to connect with fellow professionals and enthusiasts in the field of network management and cybersecurity.