



**Faculty Of Engineering
Telecommunication Department
Training AWS IT and Network**

Under Supervision

Dr	Mohamed Maher
Eng	Hazem Yehia
Eng	Mustafa El-Bahety

Prepared By

Student Name	Ahmed Mohamed Atef
ID	211070

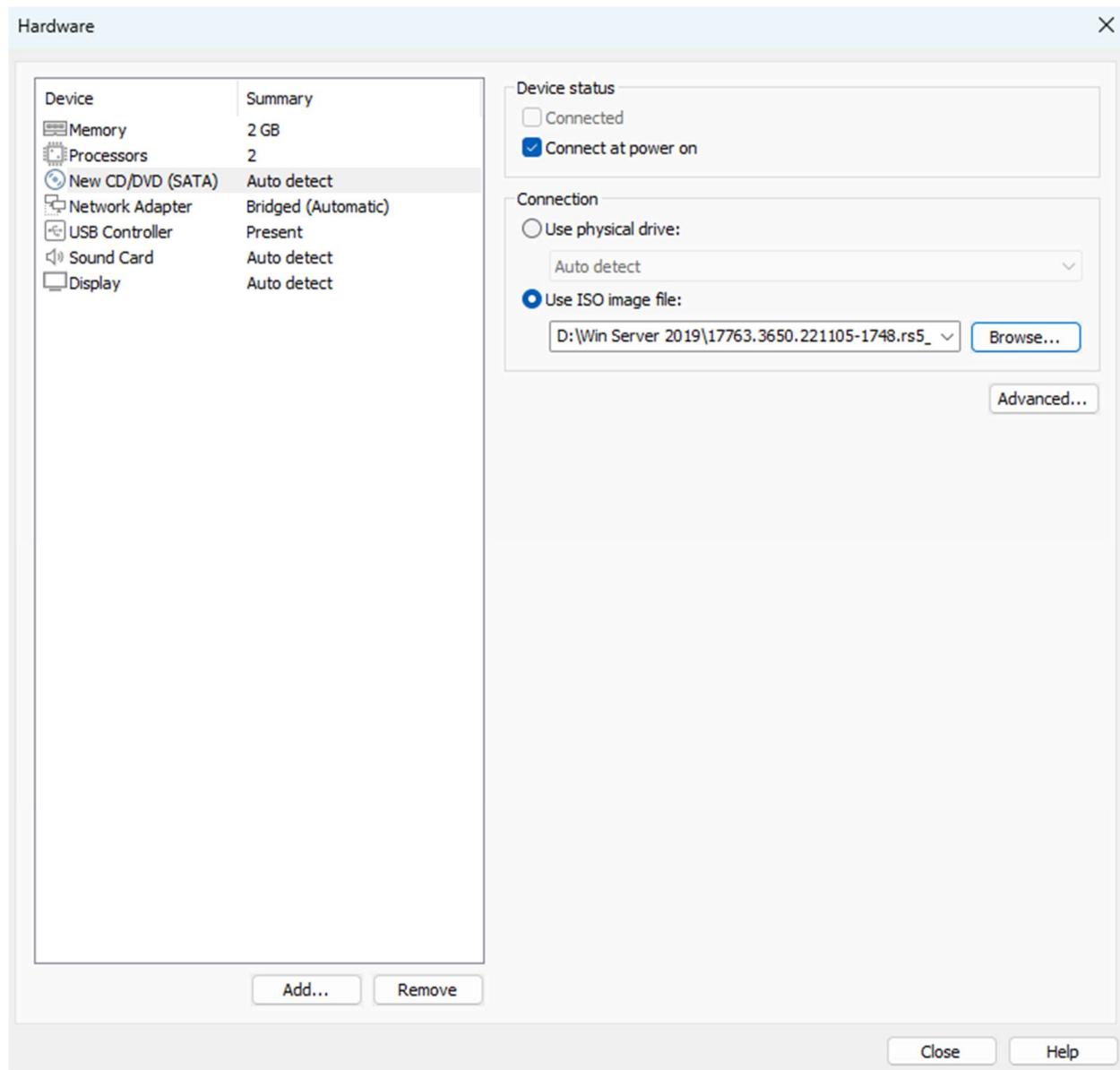
Content

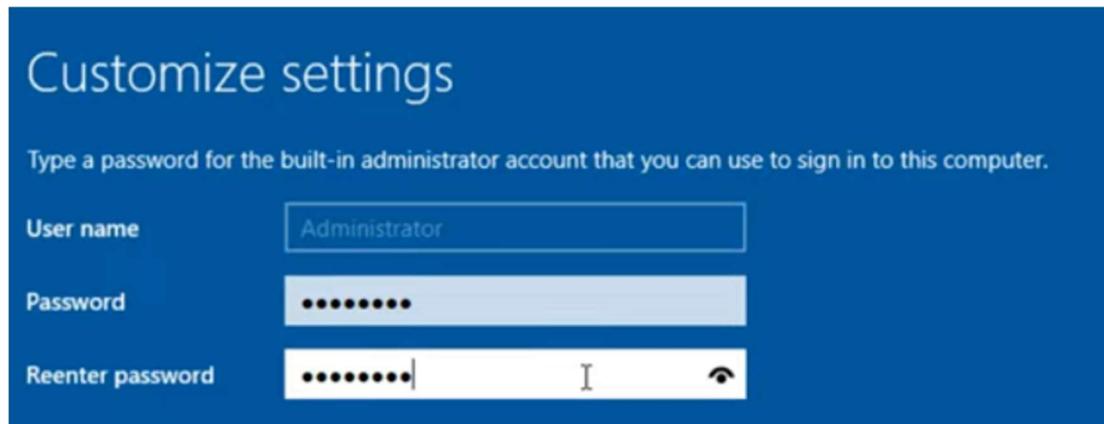
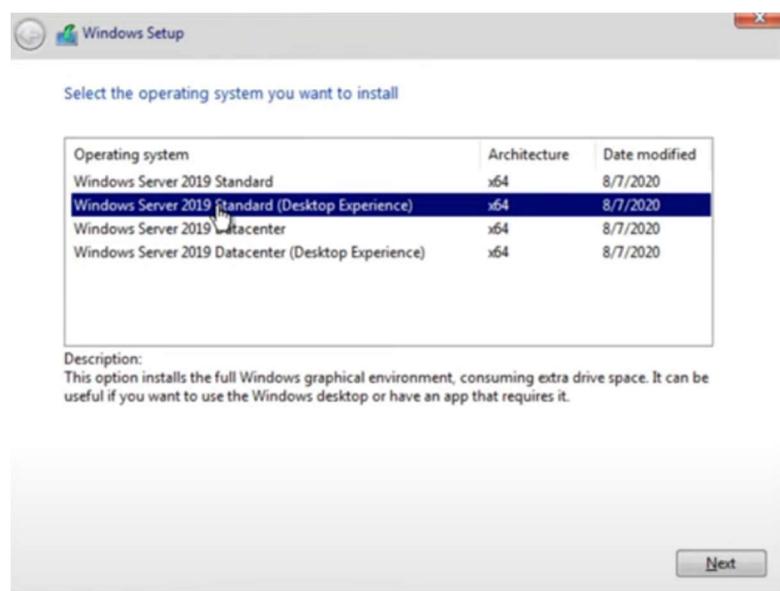
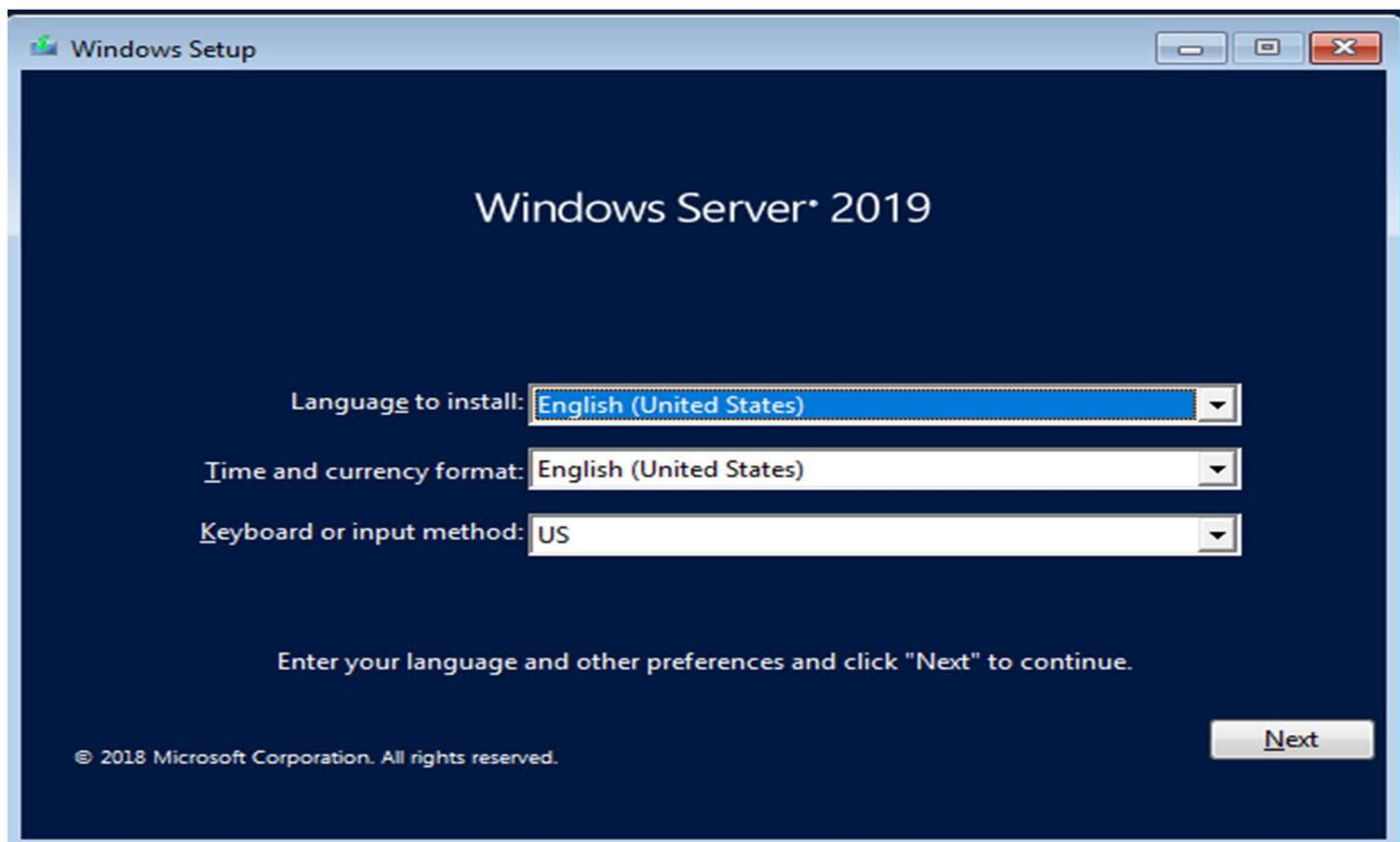
- (1) Install Win Sev and Win 10
- (2) Add rule active directory domain service
- (3) Add policy on users
- (4) Add DHCP
- (5) Share file
- (6) Create VHD
- (7) Create another Win Server for backup

Windows Server Domain Configuration

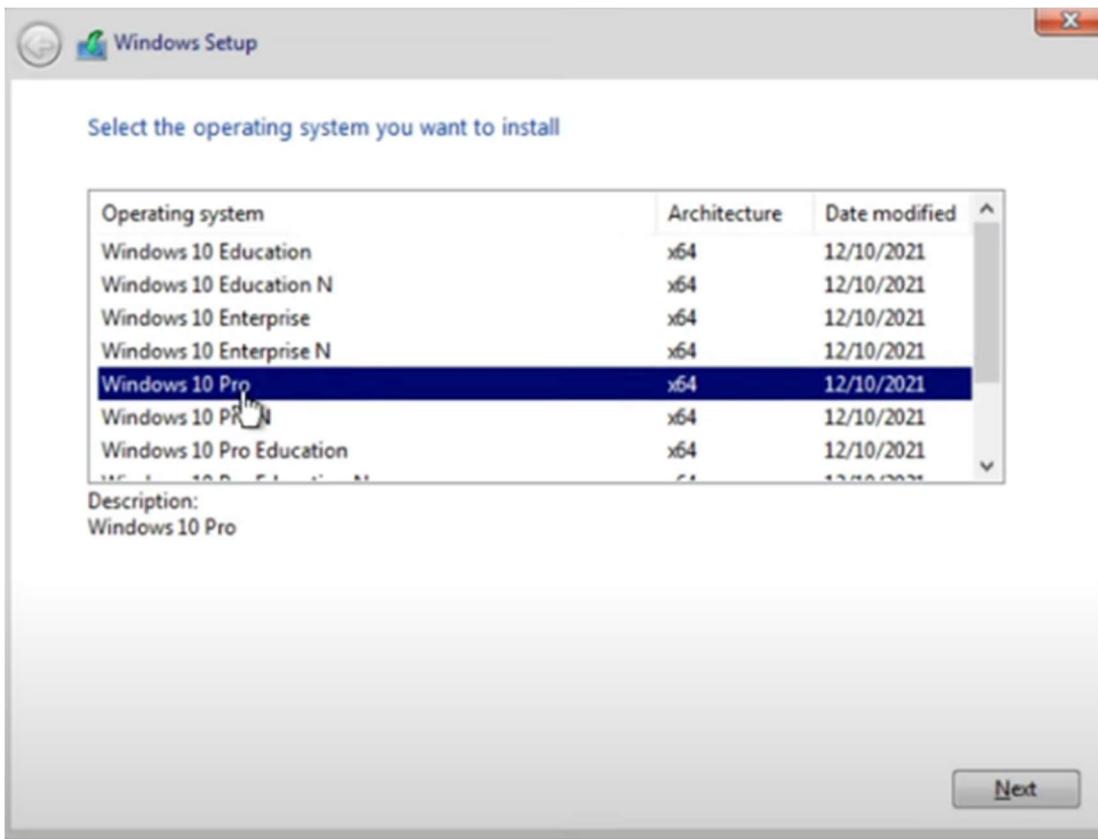
1-Install One VM for Win10 and Two VM for Win Server (Primary Domain and Additional) and Computer name will be your name like

1.1-Install Win Server

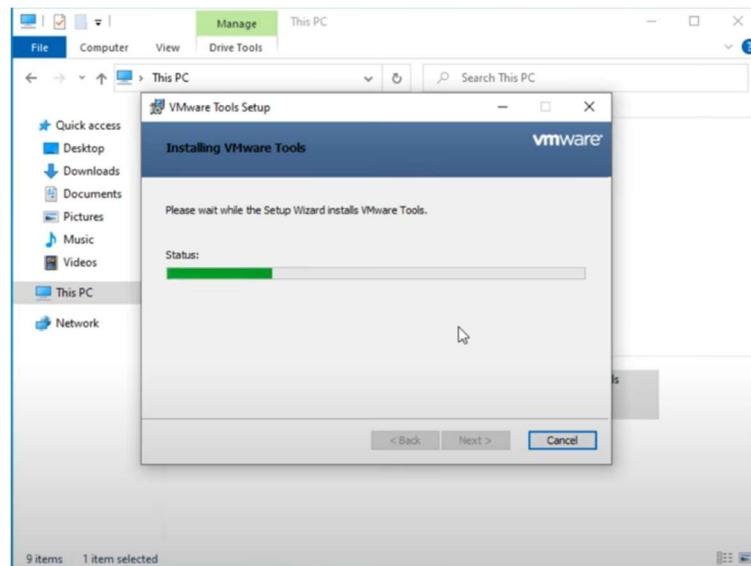




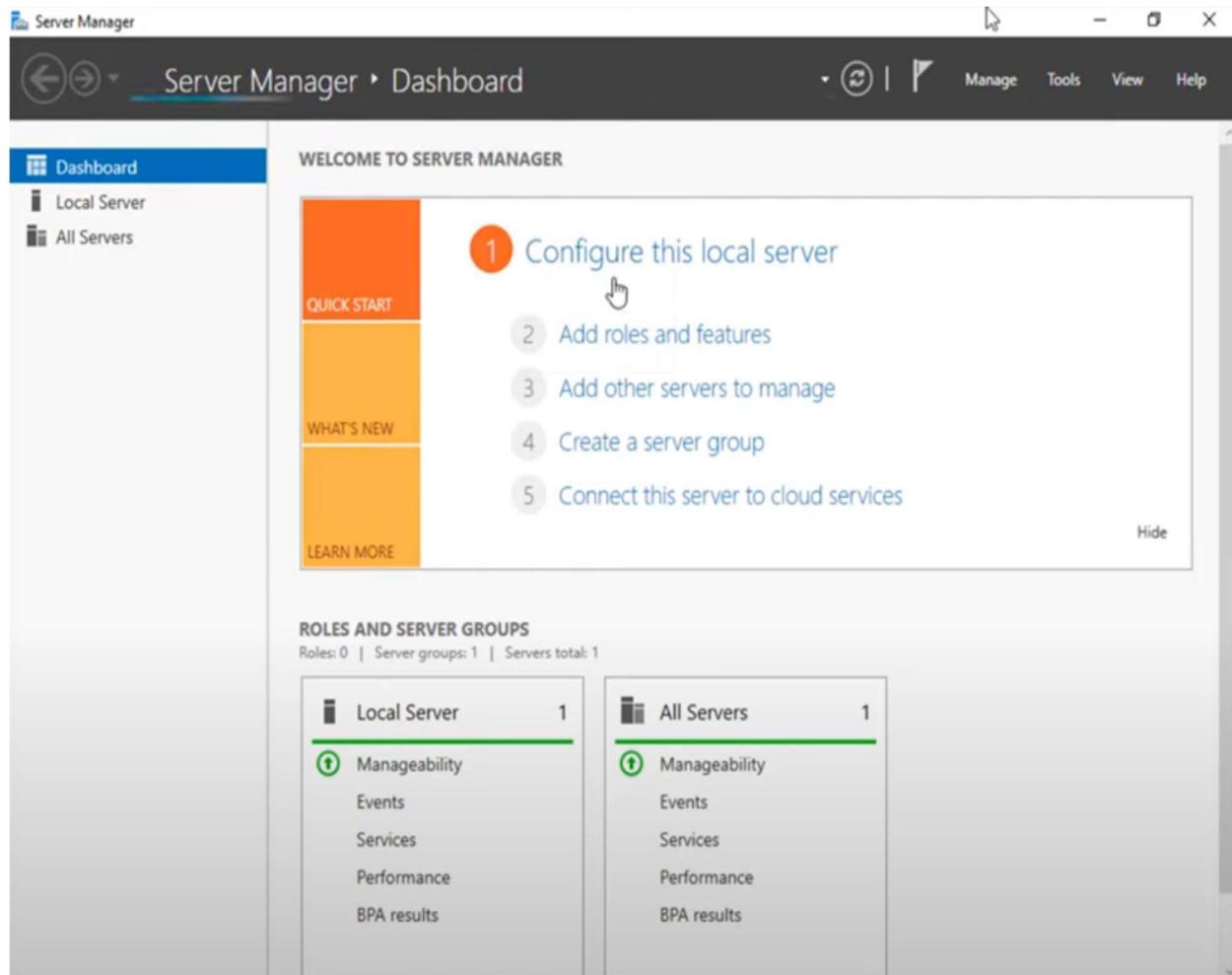
1.2-Install Win 10 as User

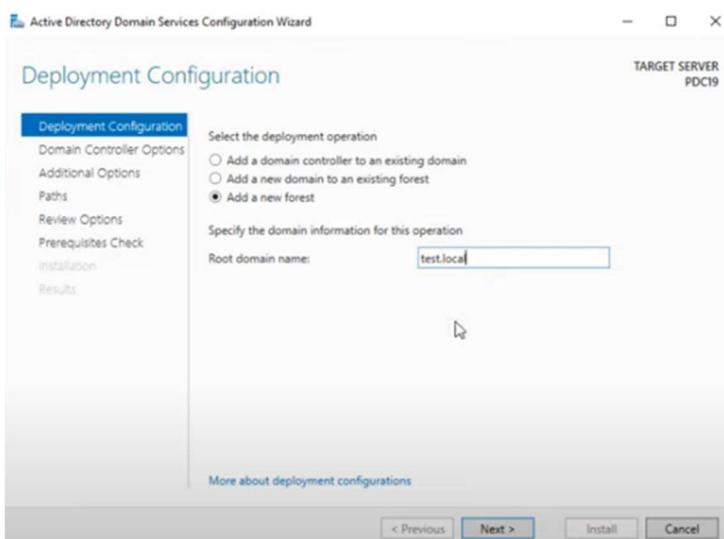
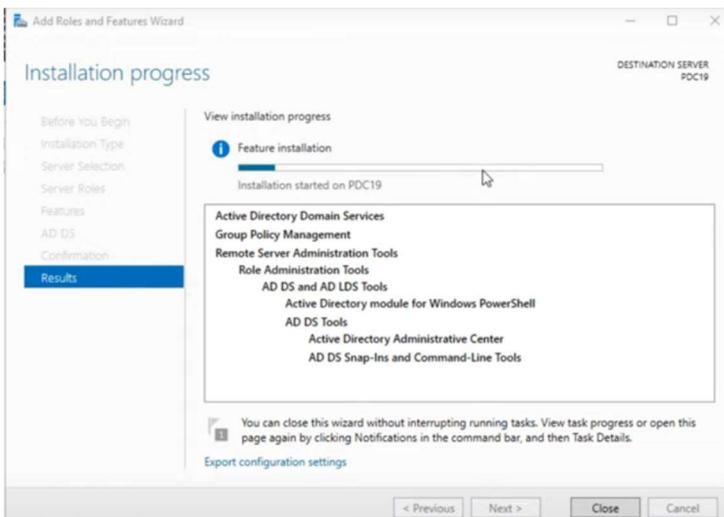
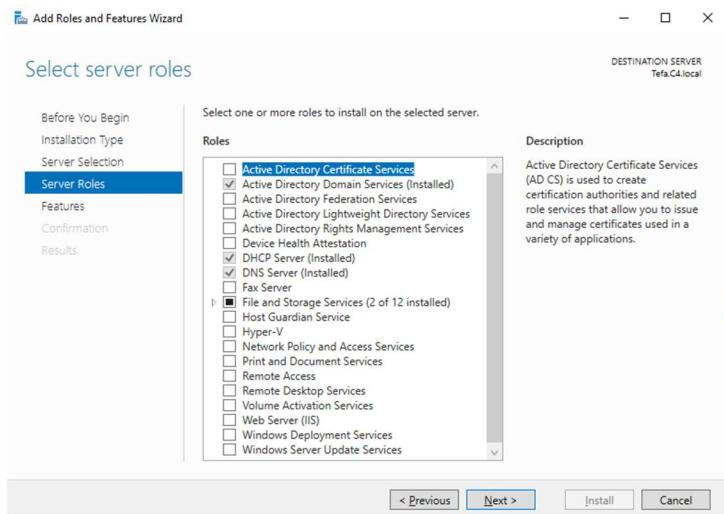


1.3-Then install VM tools



2-Add role active directory domain service





2.1-After installation add some OU and add users,computers

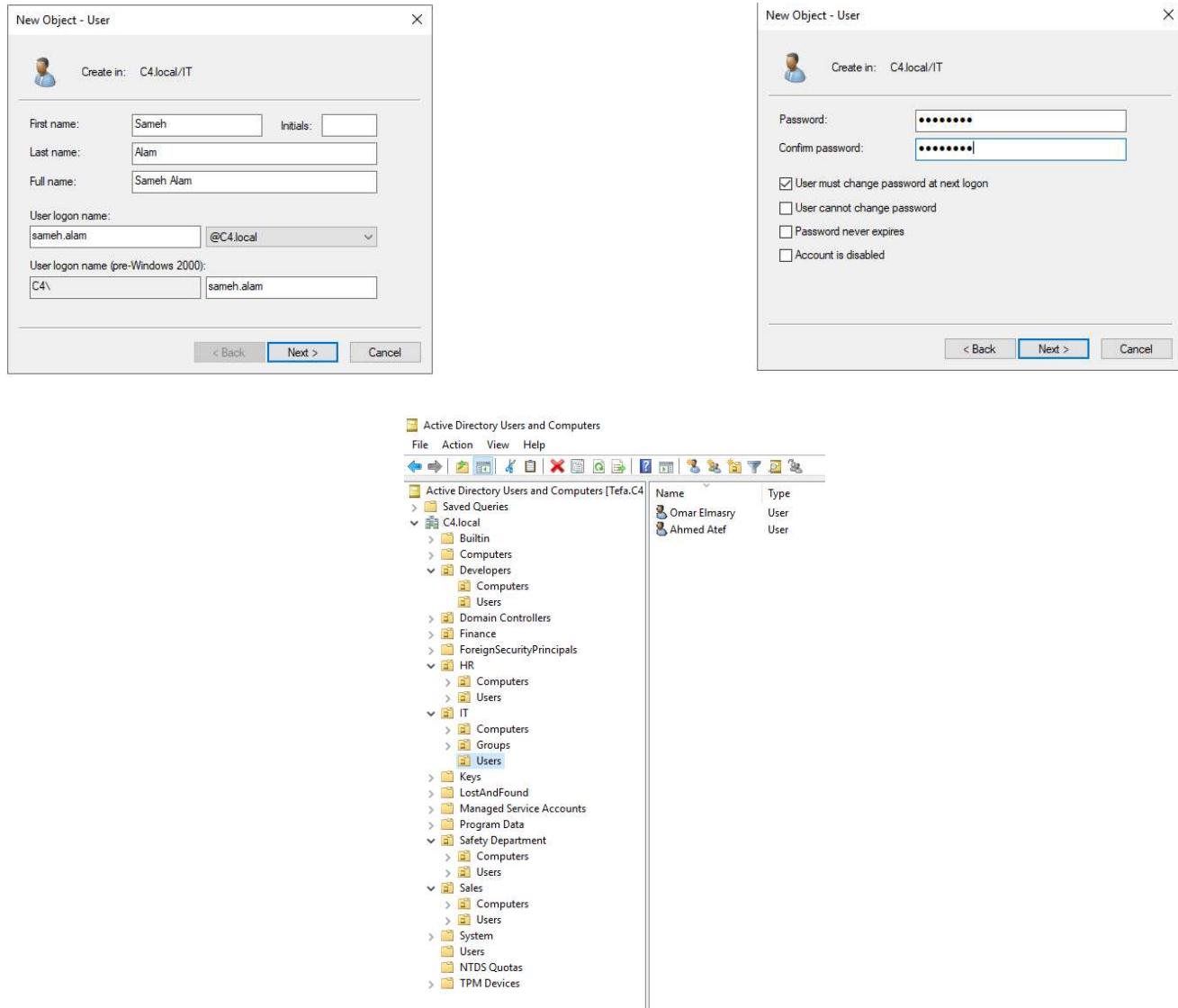
-This is a design for C4 company, and here the sections will be explained:

“IT,HR,Developers,Finance,Safety,Sales” Each department contains users and computers.

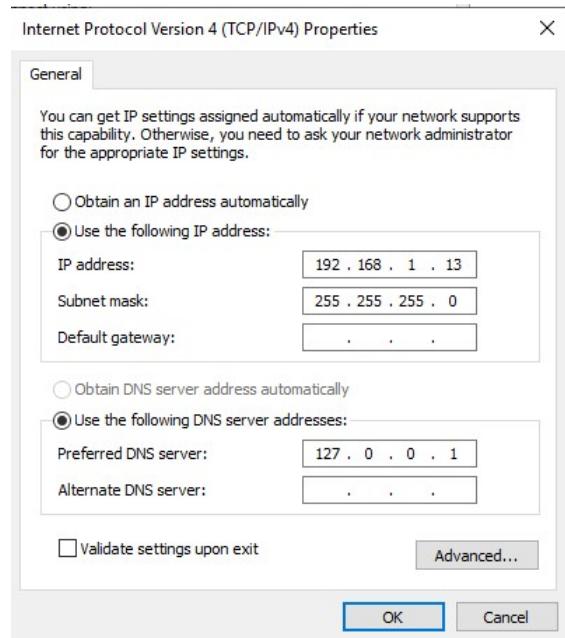
-Each department has permissions on the company's domain

Such as the IT department, which has permissions to access user devices and solve problems.

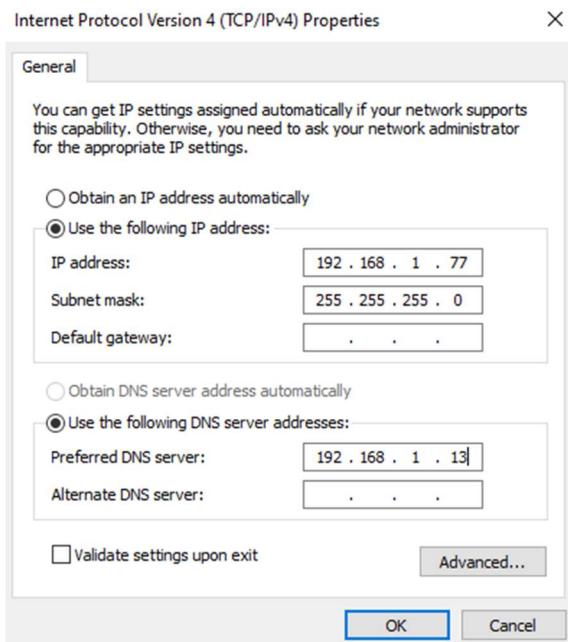
-The HR department deals with applications for jobs within the company, the Sales department deals with accounts, and so on with other departments



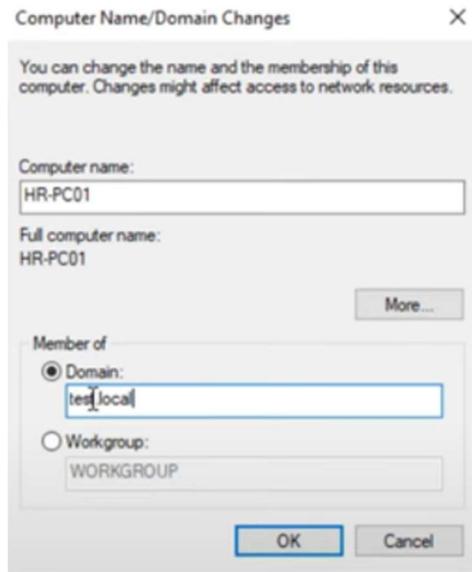
2.2-Before add active directory, you must edit time and add IP for win server and DNS 127.0.0.1 to see himself



2.3-In Win 10 you must edit time and add IP also but in different form

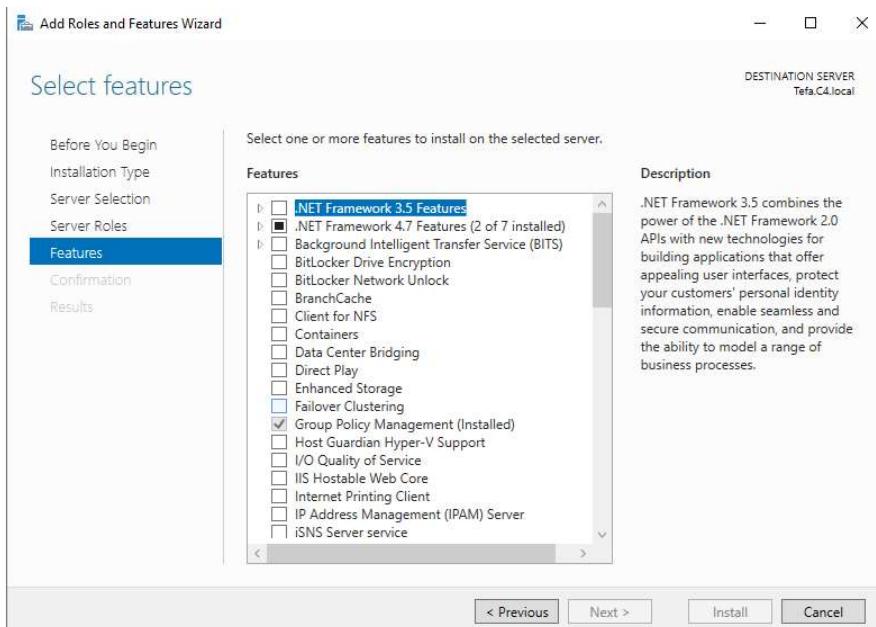


2.4-After this step , we will join to domain



Then add Username,Password “Administrator”

3-Install Group policy



3.1-Add Policy on user in HR department

The screenshot shows the Group Policy Management console interface. The left pane displays a tree view of Group Policy Objects (GPOs) under the domain C4.local. The right pane shows a list of GPOs in the C4.local domain.

Group Policy Objects in C4.local

Name	GPO Status
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled
RemoveProperties	Enabled
RemoveTaskManger/lock	Enabled
Remove-USB	Enabled

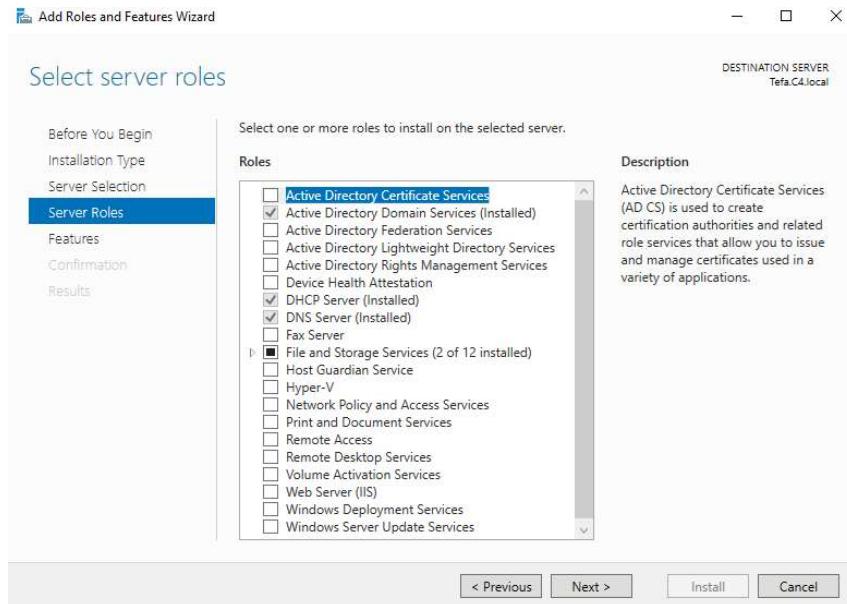
A policy has been applied to block a user's USB drive in the department because a virus could be transmitted from the user's flash drive, affecting the domain

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the forest 'C4.local' and various OUs like Developers, Domain Controllers, Finance, HR, IT, Safety Department, Sales, Group Policy Objects, WMI Filters, Starter GPOs, Sites, Group Policy Modeling, and Group Policy Results. A specific GPO named 'Remove-USB' is selected under the HR OU. On the right, the details pane is titled 'Remove-USB' and shows the 'Scope' tab selected. It displays the linked OUs: 'C4.local'. Below that, it lists the locations where the GPO is applied: 'HR' with 'Enforced' set to 'No' and 'Link Enabled' set to 'Yes'.

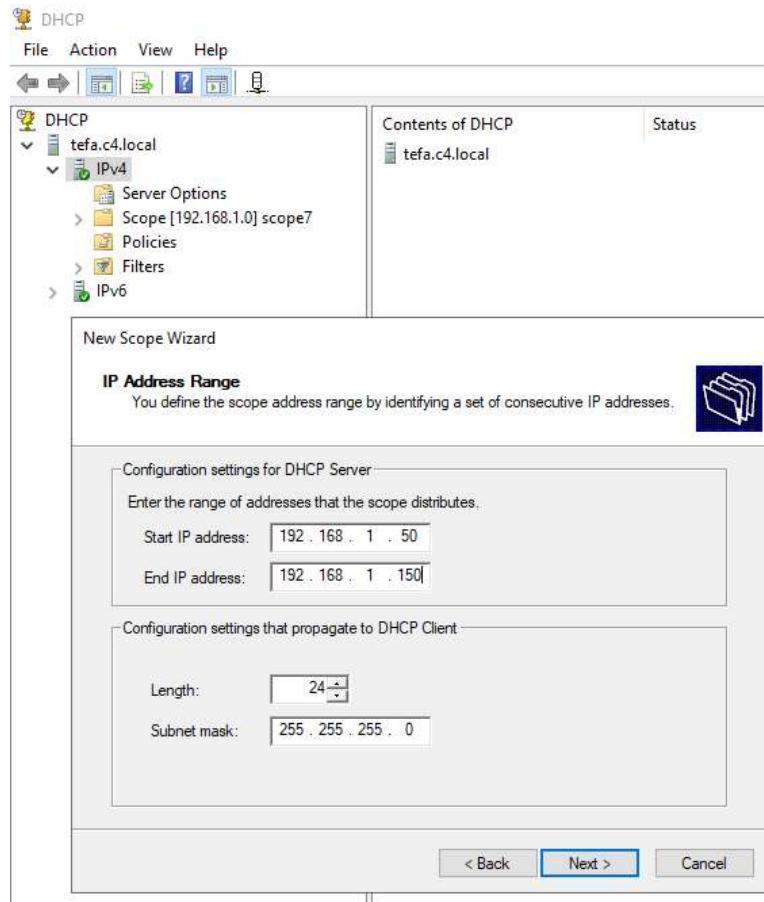
The screenshot shows the Group Policy Management Editor. The left navigation pane shows the structure of policy settings, including Windows Settings, Administrative Templates, System, and Removable Storage Access. The 'Removable Storage Access' node is expanded, showing the 'Tape Drives: Deny read access' policy. The right pane displays the configuration for this setting, listing various options like 'Set time (in seconds) to force reboot', 'CD and DVD: Deny read access', etc. The 'Tape Drives: Deny read access' option is highlighted. At the bottom, it shows 14 setting(s) and tabs for Extended and Standard.

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny read access	Enabled	No
CD and DVD: Deny write access	Enabled	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny read access	Enabled	No
Floppy Drives: Deny write access	Enabled	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Enabled	No
WPD Devices: Deny write access	Enabled	No

4-Add DHCP



4.1-Configuration DHCP



4.2-Active users on DHCP

The screenshot shows the Microsoft DHCP Management console. The left pane displays a tree view of DHCP configurations for the domain 'tefa.c4.local'. Under 'IPv4', the 'Scope [192.168.1.0] scope7' is selected, revealing its 'Address Pool' which includes 'Address Leases'. The right pane lists active leases:

Client IP Address	Name	Lease Expiration
192.168.1.14	C4-ADC.C4.local	Reservation (active)
192.168.1.77	Ahmed-Atef.C4.local	Reservation (active)

5-Share file

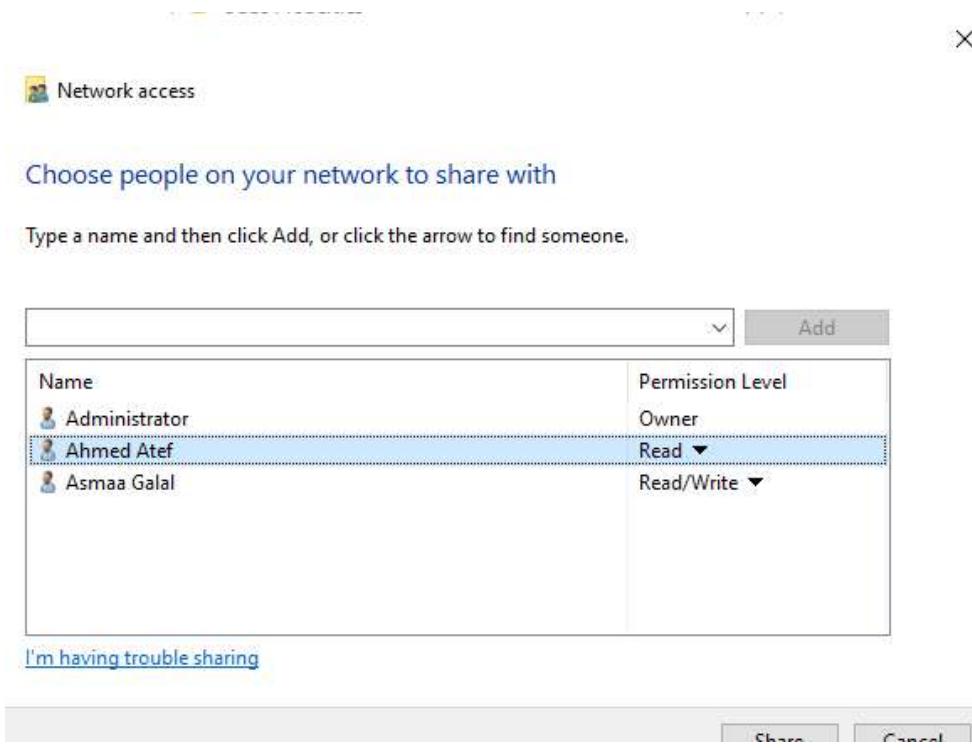
5.1-Share file from “Administrator” to other users

“TEFA” name of the server

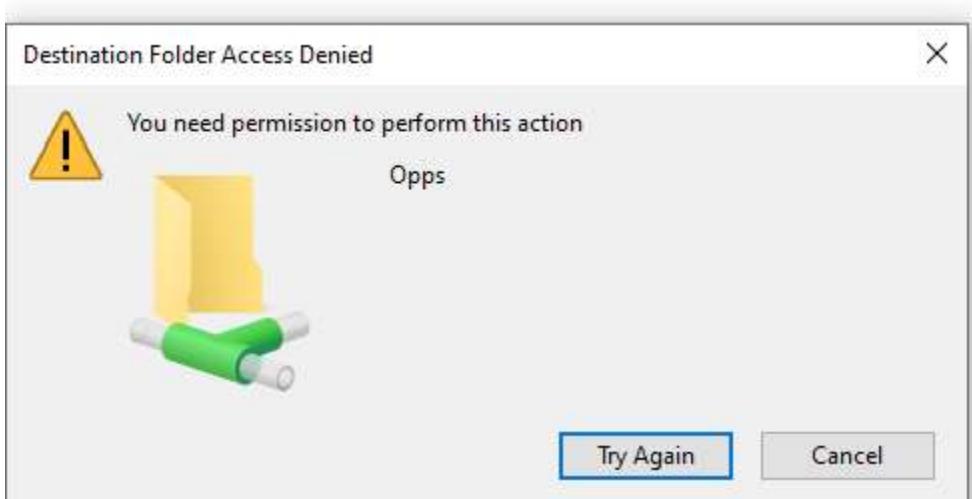
The image contains two side-by-side windows. The left window is titled 'Opps Properties' and shows the 'Sharing' tab. It displays a single share named 'Opps' under 'Network File and Folder Sharing' and the network path '\\\TEFA\\Opps'. The 'Share...' button is visible. The right window is titled 'Permissions for Opps' and shows the 'Share Permissions' tab. It lists two users with 'Allow' permissions: 'Ahmed Atef (ahmed.atef@c4.local)' and 'Asmaa Galal (asmaa.galal@c4.local)'. Below this, a detailed permission table is shown for 'Asmaa Galal':

Permissions for Asmaa Galal	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Change	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

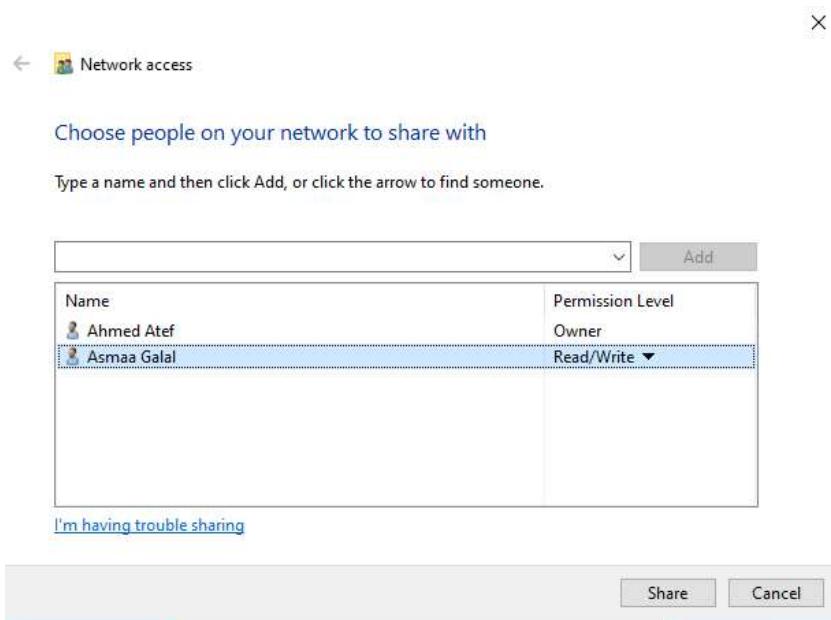
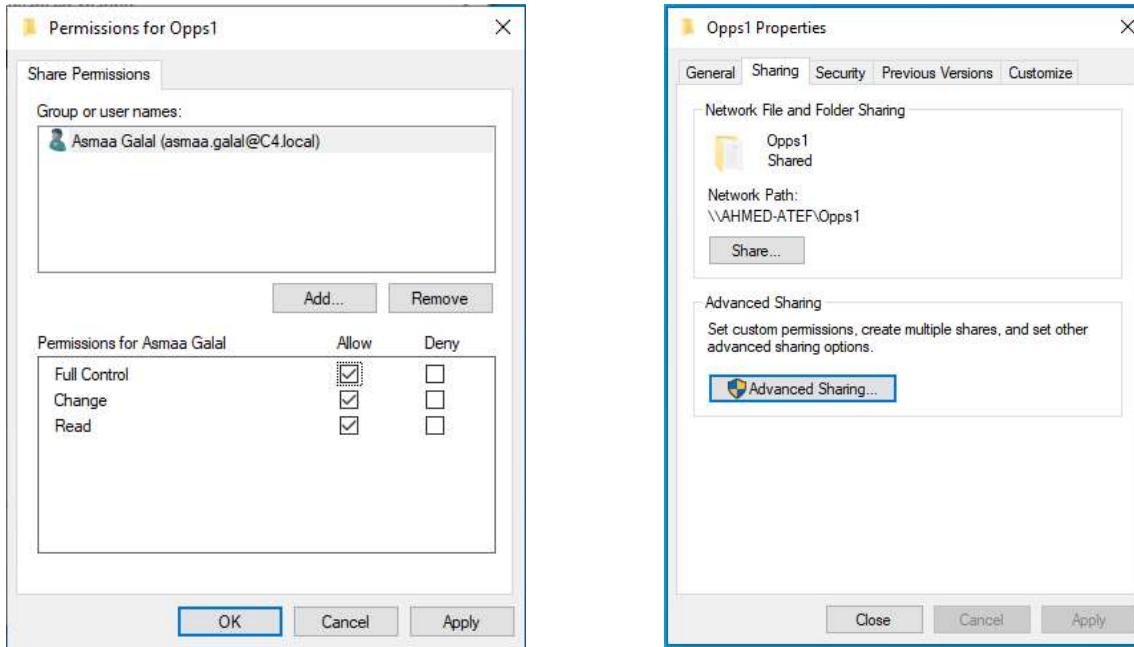
When give user “Ahmed” permission Read only

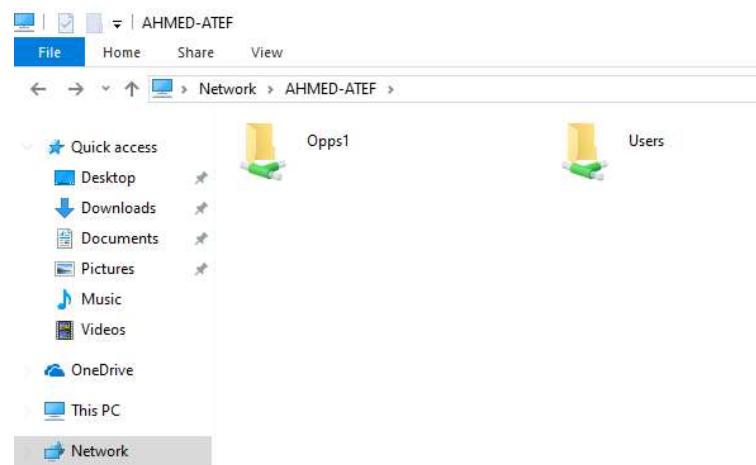
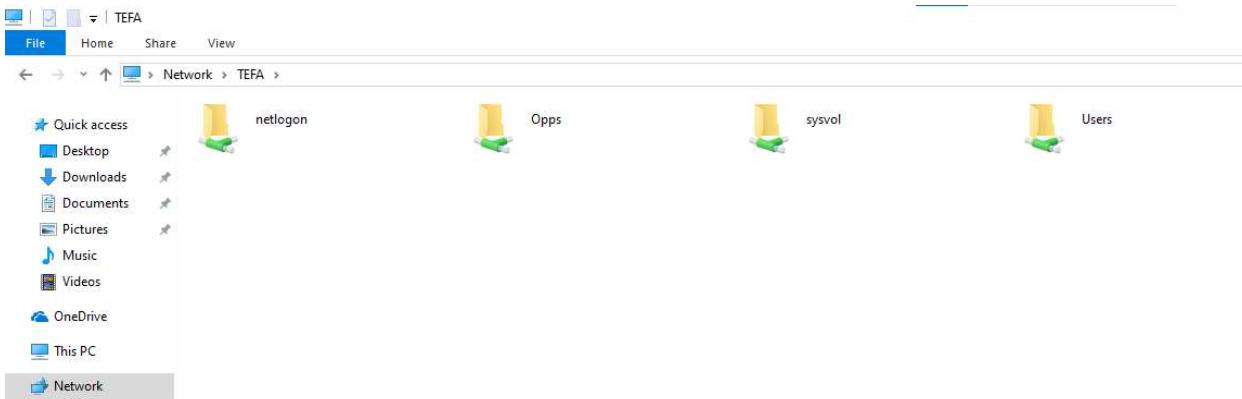


If Ahmed cannot add or modify anything inside the file

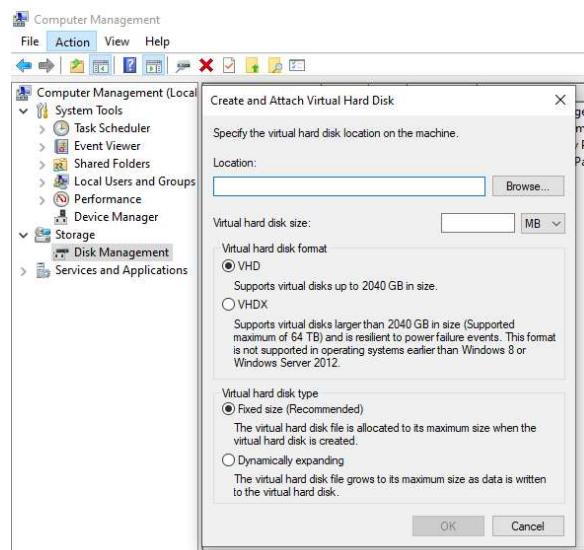


5.2-Share file from user to another user





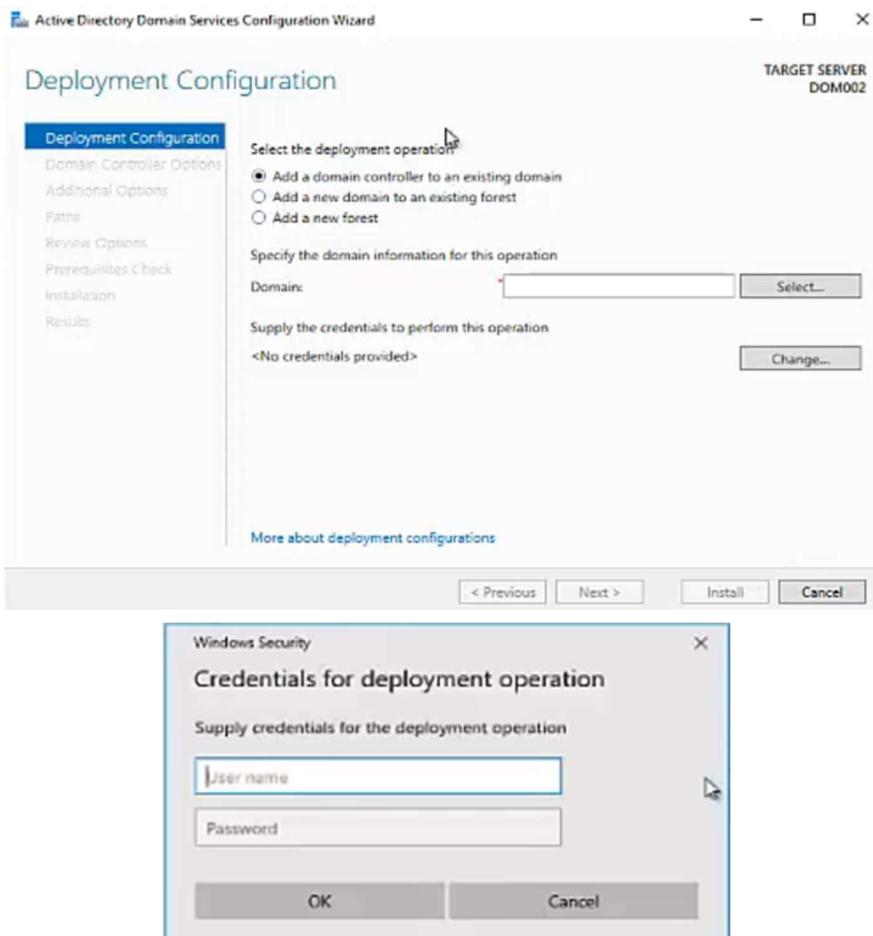
6-Create VHD



Then install VHD and give it a letter

7-Create another Win Server for backup

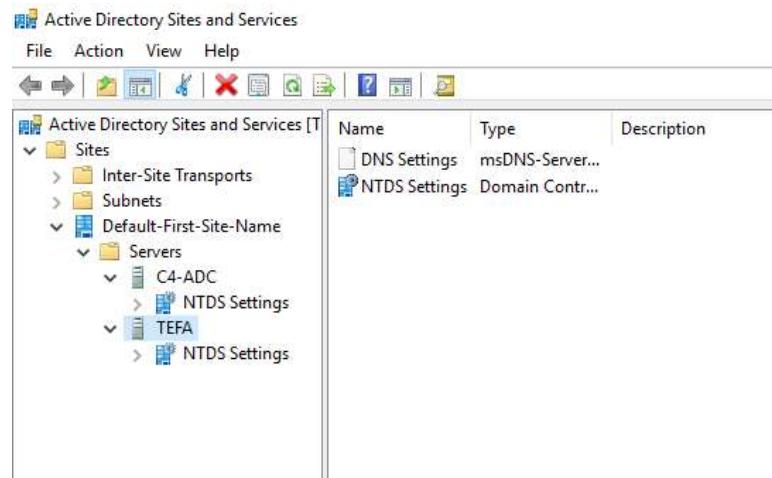
Then install active directory domain service on it, not choose new forest but add domain controller



After these steps a new server will be copy from old server

The screenshot shows the 'Active Directory Users and Computers' snap-in. The title bar says 'Active Directory Users and Computers'. The left pane shows a tree structure with 'Saved Queries', 'C4.local' (which is expanded to show 'Builtin', 'Computers', 'Developers', 'Domain Controllers', and 'Finance'), and 'Active Directory Users and Computers [Tefa.C4.local]'. The right pane displays a table of objects:

Name	Type	DC Type	Site	Description
C4-ADC	Computer	GC	Default-First-Site	Default-First-Site
TEFA	Computer	GC	Default-First-Site	Default-First-Site



Content

(1) Install SOPHOS Firewall VMware

(2) Add rule and policy on users

(3) Add policy on users

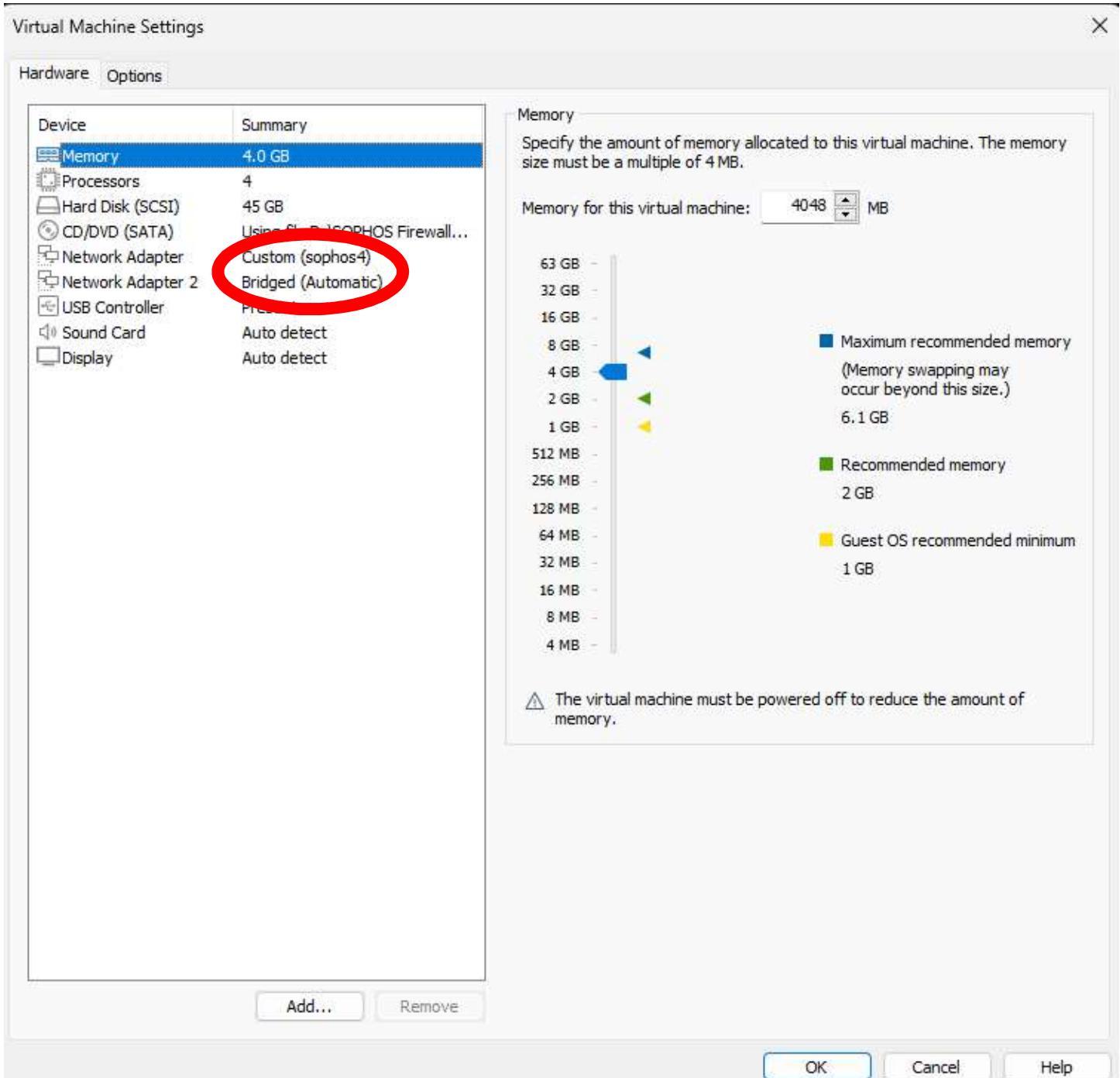
(4) Web filter and applications filter

(5) Configure DNS and DHCP

(6) Create user as viewer

1- Install SOPHOS Firewall VMWare

After choosing the ISO version of the firewall, there must be 2 network adapters in the VM, the first to be host and the second to be bridge, must be install this version on LINUX



NB: network called custom is host

After the installation window of Sophos will be in this form



Choose 1 then 1, you will seen port 1 is LAN , port 2 is WAN ,if you want to change IP address for port 1 LAN do it , for me it became **192.168.1.15**

Open the browser write <https://IP address:4444>

Default password in SOPHOS is :admin ,after write <https://IP address:4444>

Will show that ,if you want to create new password

A screenshot of the Sophos Basic Configuration interface. On the left is a blue shield icon with a white letter 'S'. The main title is "Basic Configuration". A note below says: "You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below." To the right is a link "Restore Backup or Connect as HA Spare".

Create New Admin Account

New Admin Password:

Reenter the Password:

Install the latest firmware automatically during setup (recommended).

Serial number will send to you in mail after register in SOPHOS

Register Your Firewall

Every firewall must have a serial number. We can get one for you automatically. Alternatively, if you have an unused serial number, you can specify it here.

- I have an existing serial number
- I don't have a serial number [Start a Trial]. You will automatically receive a serial number and a 30-day trial period. During this period, you can test the full functionality of Sophos XG Firewall. Do not use this option for Home use.
- I would like to migrate my UTM 9 license now
- I do not want to register now You can skip registration for now. A reminder to register will appear during your next login. You can continue without registration for another 30 days.

You will receive a serial number automatically. Your equivalent UTM 9 license will be converted and applied to the XG Firewall.

This is not reversible. If you are not sure about migrating now, click Start a Trial. You can migrate the license after you test XG Firewall.

SOPHOS License Schedule

Serial Number: C160703HBRQMRCE

After all that will show the main window

Control center

SFVH [SFOS 20.0.2 MR-2-Build378] V010012RTJD84FD

System

- Performance: 0/0 RED
- Interfaces: 0/0 Wireless APs
- Connected remote users: 0
- Live users: 0
- CPU: 3% (490B/s Bandwidth)
- Memory: 66% (0 Sessions)
- Decryption capacity: 0%

High availability: Not configured

Running for 0 day(s), 0 hour(s), 58 minute(s)

Traffic insight

Web activity: 137 max | 64 avg

Cloud applications: 2 Apps, 258 KB In, 82 KB Out

Allowed app categories: Streaming Media (76.77M), Social Networking (40.89M), Software Update (17.32M), General Internet (13.24M), Infrastructure (4.6M)

Network attacks: N/A 0

Allowed web categories: Social Networking (464), Information Tec... (431), Search Engines (252), Video hosting (113), Portal Sites (83)

Blocked app categories: Streaming Media (32)

User & device insights

Security Heartbeat*: 0 At risk (Monitor endpoint health and systems at risk) Click here

Synchronized Application Control™: 0 Apps (Identify unknown apps on your network) Click here

Zero-day protection: 0 Recent, 0 Incidents, 0 Scanned

Active threat response: 0 MDR, 0 Sophos X-Ops, 0 Accounts at risk (Configure)

SSL/TLS connections: 100% Of traffic, 0% Decrypted, 0 Failed

Active firewall rules

Type	Count
WAF	0
User	2
Network	4
Scanned	6

Unused: 6, Disabled: 3, Changed: 1, New: 1

Reports

- Risky apps seen: 0 Yesterday (Alert: All the VPN functionality has moved from the user port...) 4m ago
- Objectionable websites seen: 0 Yesterday
- Used by top 10 web users: 518 MB Yesterday (Warning: IPS protection is turned off. To enforce the intrusion pr...) 15:31
- Intrusion attacks: 0 Yesterday

Messages

Click on widgets to open details

2- Add rule and policy on users

2.1-first create host ,there are types of ways to add host, for me MAC host better because MAC not changed

The screenshot shows the 'Hosts and services' section of the Sophos interface. The 'MAC host' tab is selected. A table lists a single host entry: 'Win-10' with address '00:0C:29:96:01:D4'. The interface includes search, type, address detail, usage, and manage buttons.

2.2-second we will add policy to block facebook

Will add URL first

The screenshot shows the 'Web' section of the Sophos interface, specifically the 'URL groups' tab. It lists three URL groups: 'Blocked URLs for Default Policy' (containing 'www.example.com'), 'Facebook' (containing 'www.facebook.com'), and an unnamed group ('Domain'). The 'Facebook' group is selected, showing its configuration details: 'URL group name * Facebook', 'Description' (empty), and 'Domain names to match' containing 'www.facebook.com'. There is also a note: 'Edit this URL Group to specify sites that should be blocked by your default policy'.

2.3-Then add policy, add in which URL and blocked

The screenshot shows the Sophos Firewall's Policy test interface. At the top, there are tabs for Policies, Policy Quota Status, User activities, Categories, URL groups, Exceptions, General settings, File types, Surfing quotas, and a three-dot menu. Below the tabs, a section titled "Policy test" contains a table with columns for Name, Description, In use, Manage, and three icons. Two policies are listed: "Default Policy" and "Block Facebook". The "Block Facebook" policy has a description: "A typical starter policy with options suitable for many organizations". It shows "In use" status and manage icons. A blue oval highlights the "Actions" column for the "Block Facebook" policy, which contains a red shield icon and a lock icon. Below this, there are sections for Users, Activities, Constraints, Manage, and Status. Under "Activities", it shows "Anybody" and "Facebook". Under "Constraints", there is a green checkmark icon. At the bottom right, there is a link to "Edit additional settings".

2.4 add rule

The screenshot shows the Sophos Firewall's Rules and policies interface. At the top, there are tabs for Firewall rules, NAT rules, and SSL/TLS inspection rules. The Firewall rules tab is selected. Below the tabs, there are buttons for IPv4, IPv6, Disable filter, Add firewall rule, and Delete. A search bar and a "Reset filter" button are also present. The main area displays a table of firewall rules with columns for Rule type, #, Name, Source, Destination, What, ID, Action, Feature and service, and three-dot actions. Seven rules are listed:

#	Name	Source	Destination	What	ID	Action	Feature and service
1	Block Facebook-Block Some YouTube Features	LAN, Win-10	WAN, Any host	Any service	#7	Accept	[IPS AV WEB APP QoS LB LinkedNAT PRX LOG]
	Traffic to Internal Zones	To LAN, WiFi, VPN, DMZ.	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...				
	Traffic to WAN	Outbound traffic to WAN.	Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...				
	Traffic to DMZ	Inbound traffic to DMZ.	Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...				
5	Auto added firewall policy for MTA	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	[IPS AV WEB APP QoS LB LinkedNAT PRX LOG]
6	#Default_Network_Policy	LAN, Any host	WAN, Any host	Any service	#5	Accept	[IPS AV WEB APP QoS LB LinkedNAT PRX LOG]
7	Drop all	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	[IPS AV WEB APP QoS LB LOG]

At the bottom left, it says "Showing 7 of 7. Selected 0".

Edit firewall rule

[How-to guides](#) [Log viewer](#)

Rule status

Rule name *

Description

Enter Description

Rule group

None

Action

Accept

Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source

Select the source zones, networks, and devices.

The rule applies to traffic from these sources during the scheduled time period.

Source zones *

LAN	
Add new item	

Source networks and devices *

Win-10	 
Add new item	

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week

Destination and services

Select the destination zones, networks, devices, and services.

The rule applies to traffic to these destinations.

Destination zones *

WAN	
Add new item	

Destination networks *

Any	
Add new item	

Services *

Any	
Add new item	

Services are traffic types based on a combination of protocols and ports.

Security features

Web filtering

Web policy

Block Facebook	
----------------	---

Apply web category-based traffic shaping

Block QUIC protocol

Malware and content scanning

Scan HTTP and decrypted HTTPS

Use zero-day protection

Scan FTP for malware

Filtering common web ports

Use web proxy instead of DPI engine

 [DPI engine or web proxy?](#)

Web proxy options

Decrypt HTTPS during web proxy filtering

In these screens we must determine (source zone – source network-destination zone-destination networks) then add web policy then save

4- Web filter and applications filter

We will close some features on a specific site, for example (YOUTUBE)

We will do all the steps that happened in #3, But we won't block it

Users	Activities	Action	Constraints	Manage	Status
Anybody	YouTube				
Default action					

[Edit additional settings](#)

Then will do block for some features in youtube , move to applications

Application filter			Synchronized Application Control	Cloud applications	Application list	Traffic shaping default	Application object
<input type="checkbox"/>	Name	Default action	Description				
<input type="checkbox"/>	Allow All	Allow	Allow All Policy.				
<input checked="" type="checkbox"/>	<u>Block Some YouTube Features</u>	Allow					
<input type="checkbox"/>	<u>Block filter avoidance apps</u>	Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.				
<input type="checkbox"/>	<u>Block generally unwanted apps</u>	Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.				
<input type="checkbox"/>	<u>Block high risk (Risk Level 4 and 5) apps</u>	Allow	Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).				
<input type="checkbox"/>	<u>Block peer to peer (P2P) networking apps</u>	Allow	Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.				
<input type="checkbox"/>	<u>Block very high risk (Risk Level 5) apps</u>	Allow	Drops traffic that are classified under very high risk apps (Risk Level- 5).				
<input type="checkbox"/>	Deny All	Deny	Deny All Policy.				

We will add some features and don't forget to deny them as (Video playback)

Applications

How-to guides Log viewer Help admin@C4 • Sophos

Application filter Synchronized Application Control Cloud applications Application list Traffic shaping default Application object

Add application filter policy rules

Category Risk Characteristics Technology Classification Smart filter Clear filter

Smart filter: youtube video x

Select all Select individual application

Name	Description	Category	Risk	Technology	Characteristics	Classification
Youtube Video Search	Youtube Video Search	General Internet	3 - Medium	Browser Based	Excessive Band...	
Youtube Video Streaming	Youtube Video Streaming	Streaming Media	3 - Medium	Browser Based	Excessive Band...	
Youtube Video Upload	Youtube Video Upload	Streaming Media	3 - Medium	Browser Based	Excessive Band...	

List of matching applications (1 - 3 of 3)

Action * Allow Deny

Schedule * All the Time

Add Delete

Application	Application filter criteria	Schedule	Action	Manage
YouTube Subscribe, YouTube Video Streaming, YouTube Like/Plus, YouTube Video Search, YouTube Video Upload, YouTube Comment	Smart filter = youtube comm, youtube like, youtube subscribe, youtube video	All the Time	Deny	 

Then move to rules and policies to add it

Other security features

Identify and control applications (App control)

Block Some YouTube Features

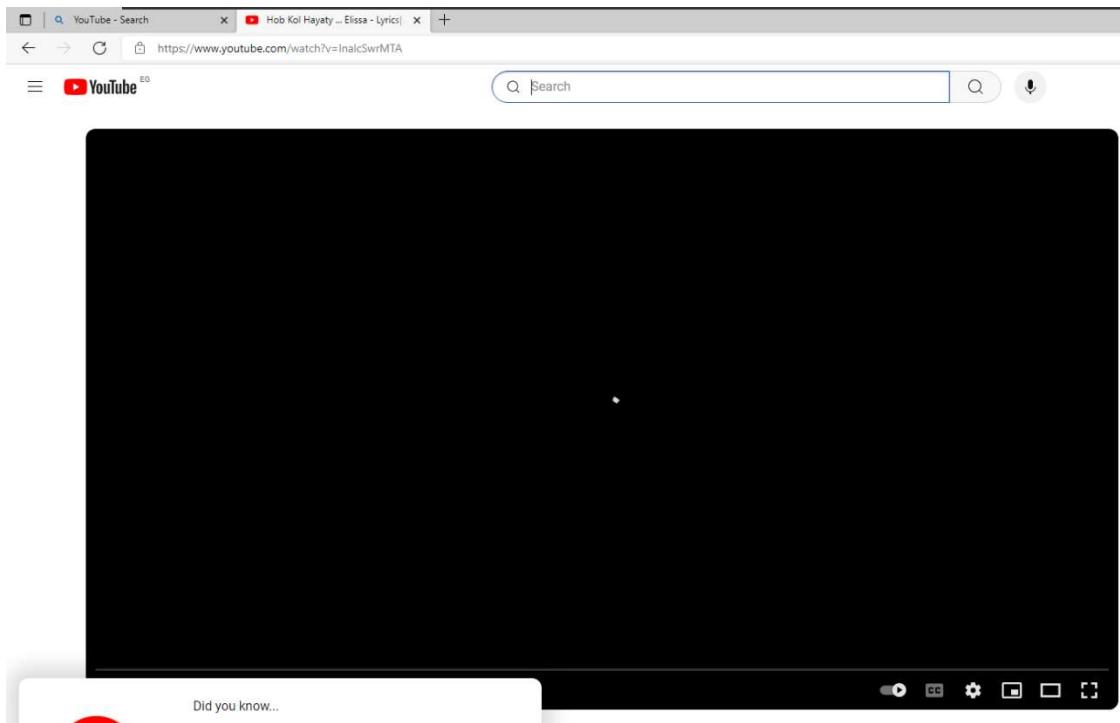
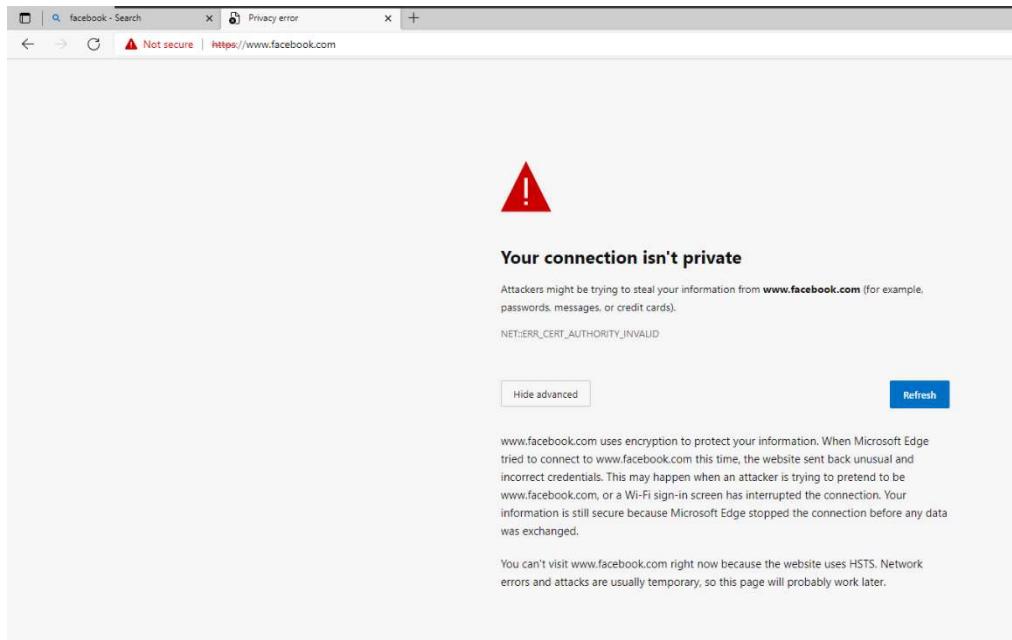
Apply application-based traffic shaping policy

Detect and prevent exploits (IPS) ⚠

None

Scan email content

Then move to user lets try this



In this way it was applied rules and polices

4- Configure DNS and DHCP

In the previous steps, I set the IP address as static, not dynamic, and also the gateway

Now let's Configure DNS and DHCP

The screenshot shows the Sophos Firewall interface under the 'Network' tab. On the left sidebar, 'Network' is selected. The main content area is titled 'DNS configuration'. It has two sections: 'IPv4' and 'IPv6'. In the 'IPv4' section, 'Static DNS' is selected. The 'DNS 1' field contains '192.168.1.13', 'DNS 2' contains '8.8.8.8', and 'DNS 3' contains '127.0.0.1'. The 'IPv6' section is currently empty.

In this screen DNS-1 special for WIN Server IP, DNS-2 for Global , DNS-2 for loopback

DHCP

Network

Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels

Interface: Port1 - 192.168.1.15
 Accept client request via relay

Dynamic IP lease: Start IP 192.168.1.20, End IP 192.168.1.100
* Press Tab to add a new row

Static IP MAC mapping: Hostname, MAC address, IP address
* Press Tab to add a new row

Subnet mask * /24 [255.255.255.0]

Domain name C4.local

Gateway * Use interface IP as gateway
192.168.1.15

Default lease time * 1440 1-43200 minutes (30 days)

Max lease time * 2880 1-43200 minutes (30 days)

Conflict detection Enable

DNS server

Use device's DNS settings
Primary DNS 192.168.1.15
Secondary DNS 192.168.1.13

Save Cancel Sophos Assistant

DNS server

Use device's DNS settings
Primary DNS 192.168.1.15
Secondary DNS 192.168.1.13

WINS server

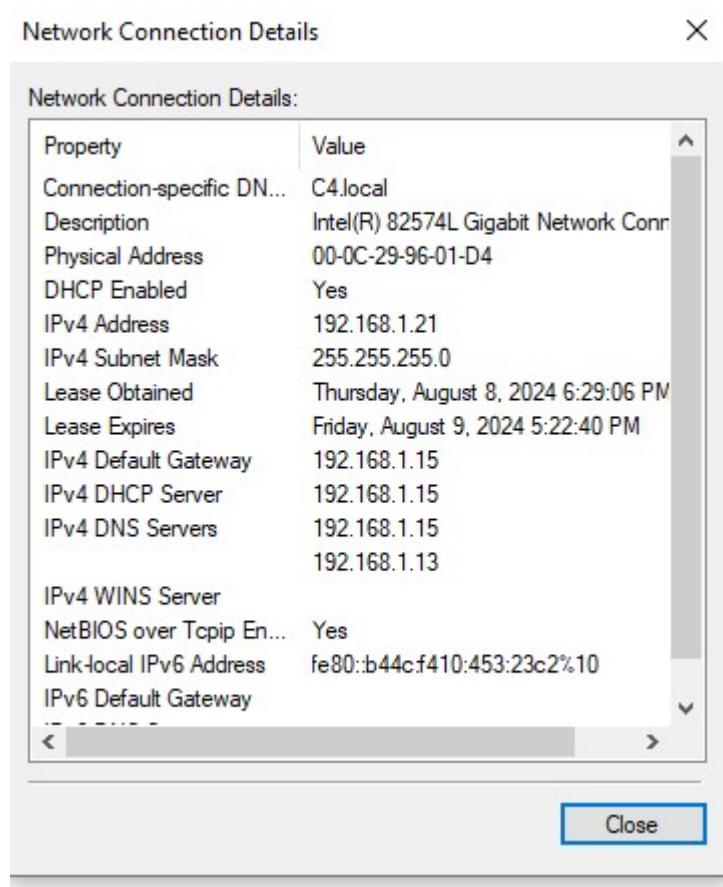
Primary WINS server
Secondary WINS server

Boot options
Enter the next-server and boot file details to provision thin clients and diskless workstations. Alternatively, specify the corresponding options under DHCP options.

Next-server
Boot file

Save Cancel

Move to user lets try that



5- Create user as viewer

We must create user in SOPHOS

The screenshot shows the Sophos Authentication interface. The top navigation bar includes links for How-to guides, Log viewer, Help, admin@C4, and Sophos. Below the navigation is a horizontal menu with tabs: Servers, Services, Groups, **Users**, Multi-factor authentication, Web authentication, Guest users, Clientless users, STAS, and a three-dot menu. The 'Users' tab is active. On the left, there's a 'Show additional properties' link. The main area has a header with columns: UserID, Name, Username, Type, Profile, Group, Other group memberships, Status, and Manage. At the bottom right of this header are buttons for Add, Delete, Change status, and Purge AD users. A message at the top right says 'Active users: 1 out of 1'.

Edit user

Username *	user
Name *	Ahmed Atef
Description	Description
User type *	<input checked="" type="radio"/> User <input type="radio"/> Administrator
Profile *	Profile
Password *	***** Change Password
Email *	ahmed1hazo@gmail.com
Internet usage time	00:00 (HH:MM)

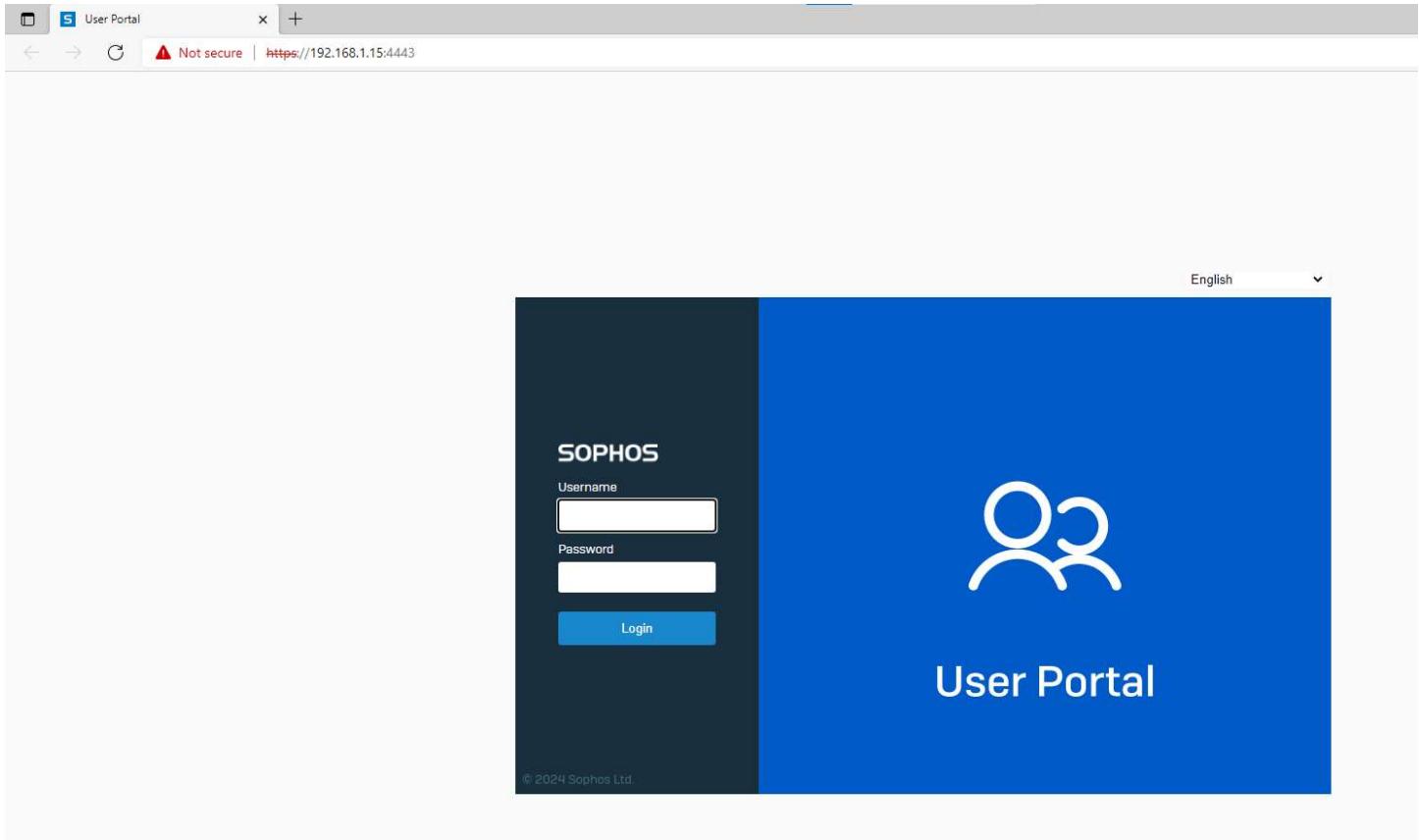
Policies

Group *	Open Group
Surfing quota *	Unlimited Internet Access i
Access time *	Allowed all the time i
Network traffic	None i
Traffic shaping	None i

VPN

[Save](#)[Reset user accounting](#)[View usage](#)[Cancel](#)

To try open SOPHOS as user must not use portal 4444 but 4443



The screenshot shows a web browser window titled "User portal". The address bar indicates a "Not secure" connection at <https://192.168.1.15:4443/userportal/webpages/myaccount/index.jsp#87470>. On the left is a dark sidebar with the "SOPHOS" logo and links for "Home", "Personal", "Download client", "Internet usage" (which is highlighted in blue), "Email", and "Logout". The main content area is titled "User portal for user". It contains two sections: "Policy information" and "Usage information".

Policy information:

Username	user
Group	Open Group
Time allotted to user (HH)	Unlimited
Surfing quota expiry date	N.A.
Data transfer cycle renewal	N.A.
Internet usage time (HH:MM)	00:00

Usage information:

Resource	Allotted	Usage	
		Up to last session	Current session
Upload network traffic	N.A.	0 MB	0 MB
Download network traffic	N.A.	0 MB	0 MB
Total network traffic	N.A.	0 MB	0 MB

At the bottom, there is a search bar for "View usage for:" with "August-2024" selected, and filters for "IP address", "Start time", "Stop time", "Used time (in minutes)", and "Download network traffic". A message "No records found" is displayed.

Content

- (1) Create WIN Server at Microsoft Azure
- (2) Configure the cloud server as Domain
- (3) Complete Azure or AWS one certification
- (4) Create (DHCP,VLAN,OSPF,AAA,ACL) with eNSP
- (5) Wireshark Report

1- Create WIN Server at Microsoft Azure

Microsoft Azure Search resources, services, and docs (G)

Home > All resources > Create a resource >

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more ↗](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Concierge Subscription ▼

Resource group * ⓘ learn-54746f96-5350-4e4f-8f5f-1e200abace6c ▼

[Create new](#)

Instance details

Virtual machine name * ⓘ PDC ✓

Region * ⓘ (US) West US ▼

Availability options ⓘ No infrastructure redundancy required ▼

Security type ⓘ Trusted launch virtual machines ▼

[Configure security features](#)

Image * ⓘ Windows Server 2019 Datacenter - x64 Gen2 ▼

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64 x64

ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount ○

< Previous Next : Disks > Review + create

[Home](#) > All resources > Create a resource >

Create a virtual machine

i Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

Administrator account

Username *

Ahmed

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *

- None
 Allow selected ports

Select inbound ports *

RDP (3389)

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing Windows Server license?

[Review Azure hybrid benefit compliance](#)

[< Previous](#)[Next : Disks >](#)[Review + create](#)

PDC

Virtual machine

Search

Connect ▾ Start ▾ Stop ▾ Hibernate ▾ Capture ▾ Delete ▾ Refresh ▾ Open in mobile ▾ Feedback ▾ CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Settings

Availability & scale

Resource group (move) : learn-54746f96-5350-4e4f-8f5f-1e200abace6c

Status : Creating

Location : West US

Subscription (move) : Concierge Subscription

Subscription ID : 16982123-2d3c-44ce-ab2d-0c419f4ce699

Operating system : Windows

Size : Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address : 13.88.41.105

Virtual network/subnet : PDC-vnet/default

DNS name : Not configured

Health state : -

Time created : 8/16/2024, 1:28 PM UTC

Tags (edit) : Add tags

This Public IP to remote this VM



2- Configure the cloud server as Domain

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS 1	DNS 1	File and Storage Services 1	Local Server 1	All Servers 1
Manageability	Manageability	Manageability	Manageability	Manageability
Events	Events	Events	Events	Events
Services	Services	Services	Services	Services
Performance	Performance	Performance	Performance	Performance
BPA results	BPA results	BPA results	BPA results	BPA results

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

Saved Queries

C5.local

Name	Type	Description
Saved Queries	Domain	Folder to store your favo...
C5.local	Domain	

3-Azure certification

Modules Learning Paths Courses Plans Other

BADGE
Configure Azure Files and Azure File Sync
Completed on 8/16/2024

BADGE
Implement access management for Azure resources
Completed on 8/16/2024

BADGE
Manage virtual machines with the Azure CLI
Completed on 8/16/2024

BADGE
Provisioning a Linux virtual machine in Microsoft Azure
Completed on 8/16/2024

BADGE
Plan your Linux environment in Azure
Completed on 8/16/2024

BADGE
Introduction to Linux on Azure
Completed on 8/16/2024

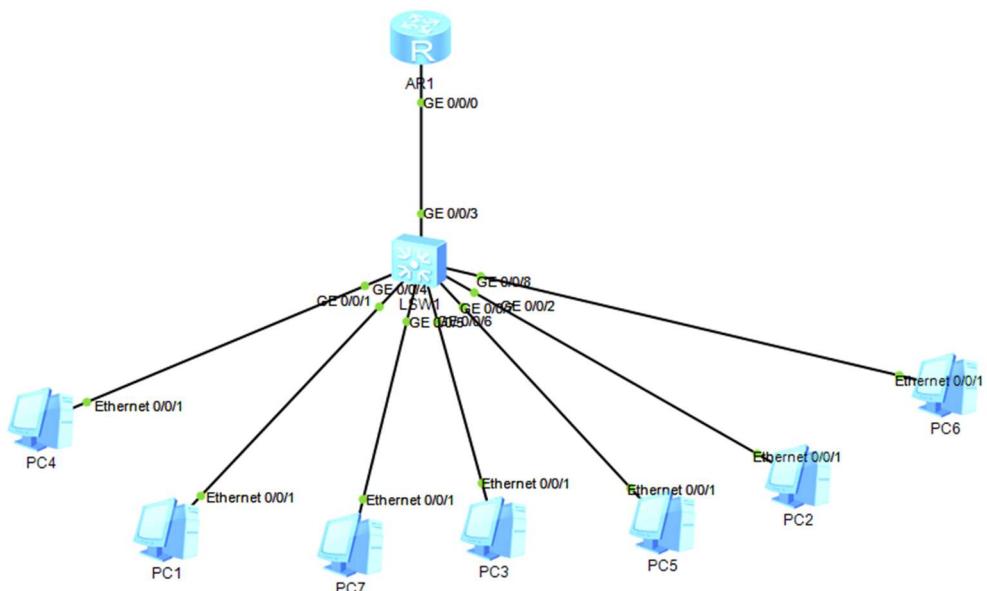
BADGE
Build and run a web application with the MEAN stack on an Azure Linux virtual machine
Completed on 8/16/2024

BADGE
Create a Windows virtual machine in Azure
Completed on 8/16/2024

BADGE
Introduction to Azure virtual machines
Completed on 8/13/2024

4- Create (DHCP,VLAN,OSPF,ACL,AAA) with eNSP

4.1-DHCP



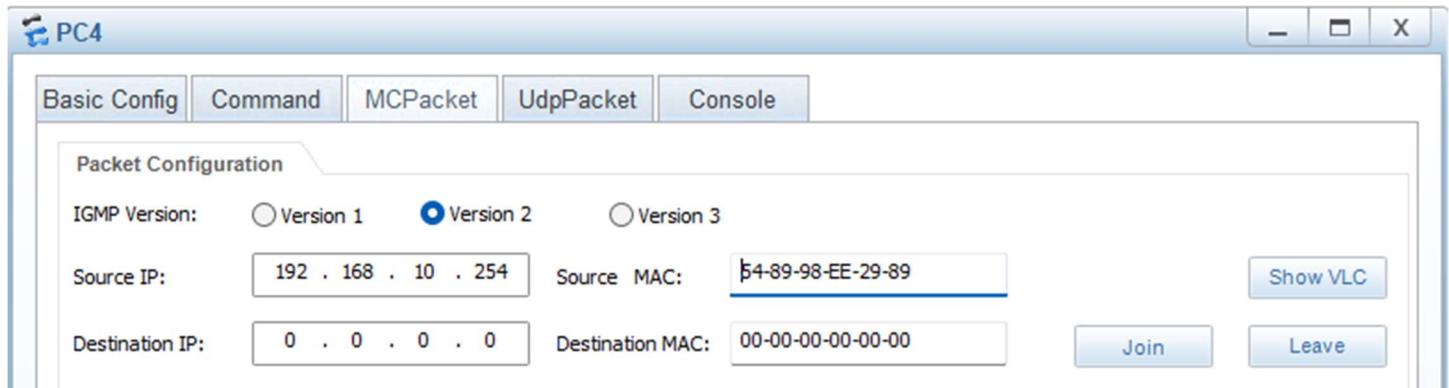
To active DHCP in Router ,there are some steps

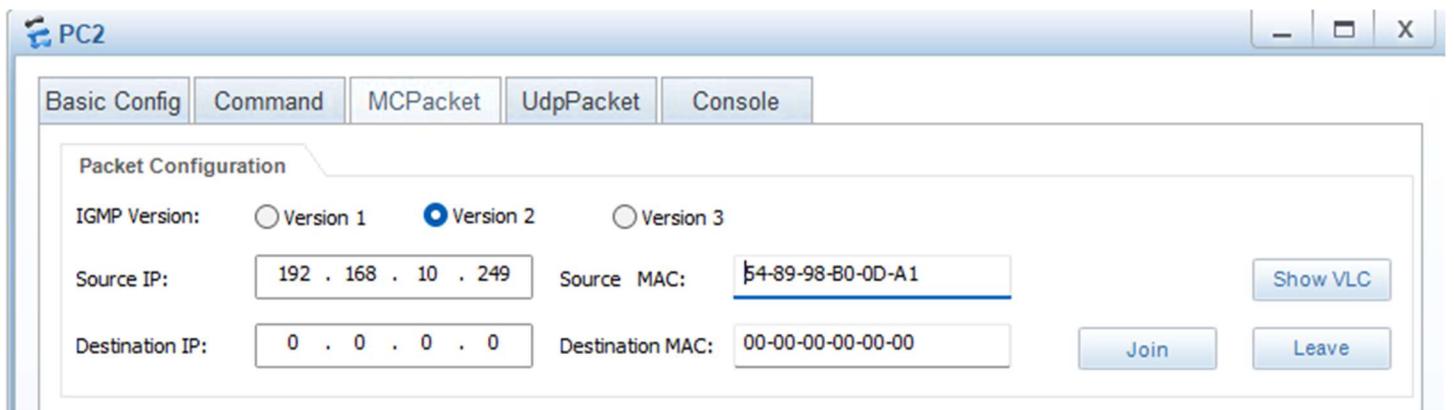
```
<Huawei>
<Huawei>
<Huawei>
<Huawei>sy
Aug 18 2024 02:42:41-08:00 Huawei %%01IFPDT/4/IF_STATE(1)[0]:Interface GigabitEthernet0/0/0 has turned into UP state.
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname C4
[C4]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[C4]int g0/0/0
[C4-GigabitEthernet0/0/0]dhcp selec
      ^
Error: Unrecognized command found at '^' position.
[C4-GigabitEthernet0/0/0]dhcp se
      ^
Error:Ambiguous command found at '^' position.
[C4-GigabitEthernet0/0/0]dhcp select interface
Error: Failed to create interface IP pool, because no IP address has been configured on the interface.
[C4-GigabitEthernet0/0/0]ip address 192.168.10.1 255.255.255.0
Aug 18 2024 02:44:44-08:00 C4 %%01IFNET/4/LINK_STATE(1)[1]:The line protocol IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[C4-GigabitEthernet0/0/0]dhcp select interface
[C4-GigabitEthernet0/0/0]dhcp server dns-list 8.8.8.8 8.8.4.4
[C4-GigabitEthernet0/0/0]dhcp server lease day 10
[C4-GigabitEthernet0/0/0]q
[C4]q
<C4>save
The current configuration will be written to the device.
Are you sure to continue? (y/n) [n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
<C4>

Please check whether system data has been changed, and save data in time

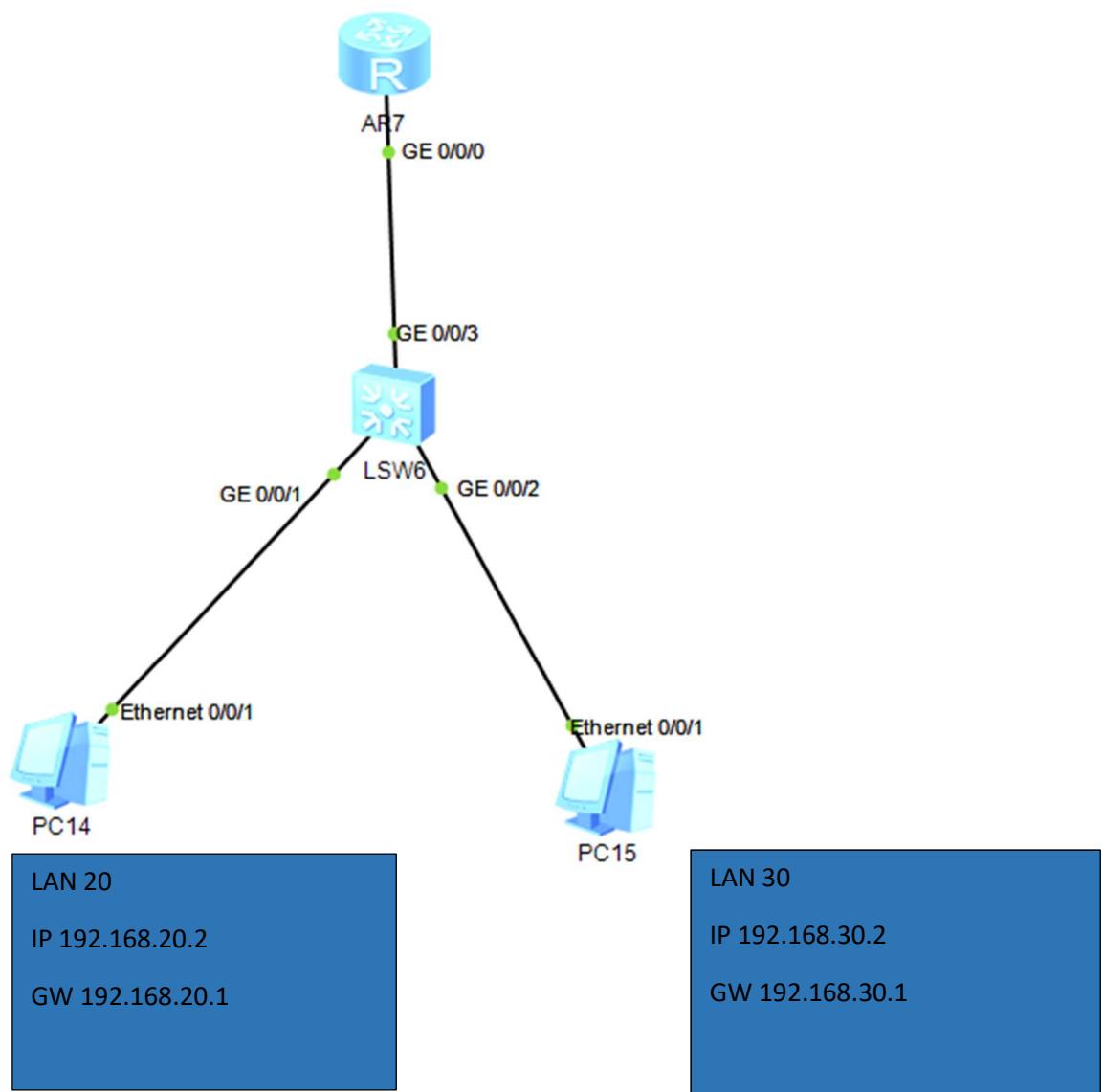
Configuration console time out, please press any key to log on
```

This Router taken IP Address 192.168.10.1 then ips start form 10.2 to 10.254





4.2-VLAN



```
The device is running!

<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]v
[Huawei>vlan b
[Huawei]vlan 20
[Huawei>vlan20]
Aug 17 2024 23:36:28-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 4, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-vlan20]de
[Huawei-vlan20]description IT
[Huawei-vlan20]
Aug 17 2024 23:36:58-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 5, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-vlan20]v
[Huawei-vlan20]vlan 30
[Huawei-vlan30]
Aug 17 2024 23:37:08-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 6, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-vlan30]de
[Huawei-vlan30]description HR
[Huawei-vlan30]
Aug 17 2024 23:37:38-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 7, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-vlan30]
[Huawei-vlan30]q
[Huawei]
[Huawei]in
[Huawei]int
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]po
[Huawei-GigabitEthernet0/0/1]port 1
[Huawei-GigabitEthernet0/0/1]port link-t
[Huawei-GigabitEthernet0/0/1]port link-type ac
[Huawei-GigabitEthernet0/0/1]port link-type access
[Huawei-GigabitEthernet0/0/1]
Aug 17 2024 23:39:18-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 8, th
e change loop count is 0, and the maximum number of records is 4095.
```

```
[Huawei-GigabitEthernet0/0/2]port default v
[Huawei-GigabitEthernet0/0/2]port default vlan 30
[Huawei-GigabitEthernet0/0/2]
Aug 17 2024 23:40:18-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 11, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-GigabitEthernet0/0/2]
[Huawei-GigabitEthernet0/0/2]q
[Huawei]
[Huawei]
[Huawei]dis
[Huawei]display cu
[Huawei]display current-configuration int
[Huawei]display current-configuration interface g0/0/1
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 20
#
return
[Huawei]int
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/0
[Huawei]interface GigabitEthernet 0/0/0
^
Error: Wrong parameter found at '^' position.
[Huawei]int
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/3
[Huawei-GigabitEthernet0/0/3]po
[Huawei-GigabitEthernet0/0/3]port 1
[Huawei-GigabitEthernet0/0/3]port link-t
[Huawei-GigabitEthernet0/0/3]port link-type tr
[Huawei-GigabitEthernet0/0/3]port link-type trunk
[Huawei-GigabitEthernet0/0/3]
Aug 17 2024 23:42:48-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 12, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-GigabitEthernet0/0/3]po
[Huawei-GigabitEthernet0/0/3]port tr
[Huawei-GigabitEthernet0/0/3]port trunk v
[Huawei-GigabitEthernet0/0/3]port trunk al
[Huawei-GigabitEthernet0/0/3]port trunk allow v
[Huawei-GigabitEthernet0/0/3]port trunk allow vlan 20 30
[Huawei-GigabitEthernet0/0/3]
Aug 17 2024 23:43:38-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
```

Basic Config Command MCPacket UdpPacket Console

```
From 192.168.20.1: bytes=32 seq=4 ttl=255 time=31 ms
From 192.168.20.1: bytes=32 seq=5 ttl=255 time=47 ms
```

```
--- 192.168.20.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/40/47 ms
```

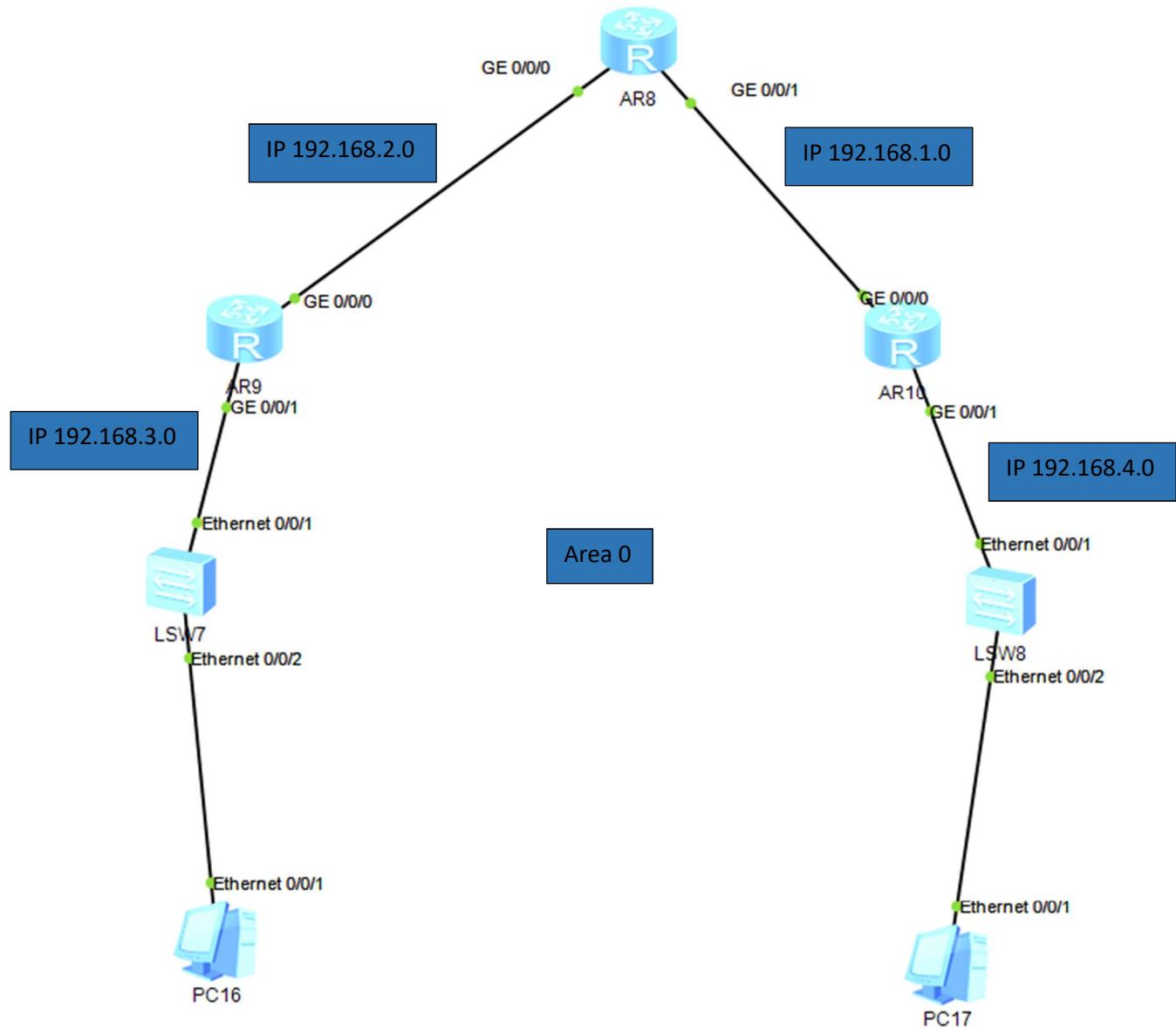
```
PC>ping 192.168.30.1 -t
```

```
Ping 192.168.30.1: 32 data bytes, Press Ctrl_C to break
From 192.168.30.1: bytes=32 seq=1 ttl=255 time=31 ms
From 192.168.30.1: bytes=32 seq=2 ttl=255 time=31 ms
From 192.168.30.1: bytes=32 seq=3 ttl=255 time=32 ms
From 192.168.30.1: bytes=32 seq=4 ttl=255 time=31 ms
From 192.168.30.1: bytes=32 seq=5 ttl=255 time=31 ms
From 192.168.30.1: bytes=32 seq=6 ttl=255 time=31 ms
```

```
--- 192.168.30.1 ping statistics ---
6 packet(s) transmitted
6 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/31/32 ms
```

```
PC>
```

4.3-OSPF



To configure OSPF first configure each router with another

```
AR9
The device is running!

<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]int g0/0/0
[Huawei-GigabitEthernet0/0/0]ip ad
[Huawei-GigabitEthernet0/0/0]ip address 192.168.2.2 24
Aug 18 2024 05:25:15-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[0]:The line protocol
IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]int g0/0/1
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]ip ad
[Huawei-GigabitEthernet0/0/1]ip address 192.168.3.2 ^

Error:Incomplete command found at '^' position.
[Huawei-GigabitEthernet0/0/1]ip address 192.168.3.2 24
Aug 18 2024 05:25:50-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[1]:The line protocol
IP on the interface GigabitEthernet0/0/1 has entered the UP state.
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
<Huawei>
<Huawei>ospf ?
      ^
Error: Unrecognized command found at '^' position.
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]int
[Huawei]interface g ^
      ^
Error:Incomplete command found at '^' position.
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/0
[Huawei-GigabitEthernet0/0/0]ip a
[Huawei-GigabitEthernet0/0/0]ip ad
[Huawei-GigabitEthernet0/0/0]ip address 192.168.2.1 24
Aug 18 2024 05:24:22-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[0]:The line protocol
IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]int g0/0/1
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]ip ad
[Huawei-GigabitEthernet0/0/1]ip address 192.168.1.1 24
[Huawei-GigabitEthernet0/0/1]
Aug 18 2024 05:24:49-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[1]:The line protocol
IP on the interface GigabitEthernet0/0/1 has entered the UP state.
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]ospf 1
[Huawei-ospf-1]a
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]net
```

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]int g0/0/0
[Huawei-GigabitEthernet0/0/0]ip ad
[Huawei-GigabitEthernet0/0/0]ip address 192.168.1.2 24
Aug 18 2024 05:26:14-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[0]:The line protocol
IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]int g0/0/1
[Huawei-GigabitEthernet0/0/1]op ad
[Huawei-GigabitEthernet0/0/1]op ad
[Huawei-GigabitEthernet0/0/1]ip ad
[Huawei-GigabitEthernet0/0/1]ip address 192.168.4.2 24
Aug 18 2024 05:27:04-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[1]:The line protocol
IP on the interface GigabitEthernet0/0/1 has entered the UP state.
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]ospf 1
[Huawei-ospf-1]a
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]n
[Huawei-ospf-1-area-0.0.0.0]net
[Huawei-ospf-1-area-0.0.0.0]network 192.168.1.2 0.0.0.0
[Huawei-ospf-1-area-0.0.0.0]net
[Huawei-ospf-1-area-0.0.0.0]network 192.168.4.0
Aug 18 2024 05:20:24-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[0]:Neighbor changes
```

To test the connection between them do ping

```
From 192.168.3.2: bytes=32 seq=3 ttl=255 time=31 ms
From 192.168.3.2: bytes=32 seq=4 ttl=255 time=32 ms
From 192.168.3.2: bytes=32 seq=5 ttl=255 time=31 ms

--- 192.168.3.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/37/47 ms

PC>ping 192.168.2.2

Ping 192.168.2.2: 32 data bytes, Press Ctrl_C to break
From 192.168.2.2: bytes=32 seq=1 ttl=255 time=31 ms
From 192.168.2.2: bytes=32 seq=2 ttl=255 time=47 ms
From 192.168.2.2: bytes=32 seq=3 ttl=255 time=47 ms
From 192.168.2.2: bytes=32 seq=4 ttl=255 time=47 ms
From 192.168.2.2: bytes=32 seq=5 ttl=255 time=47 ms

--- 192.168.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/43/47 ms

PC>
```

PC17

Basic Config Command MCPacket UdpPacket Console

Welcome to use PC Simulator!

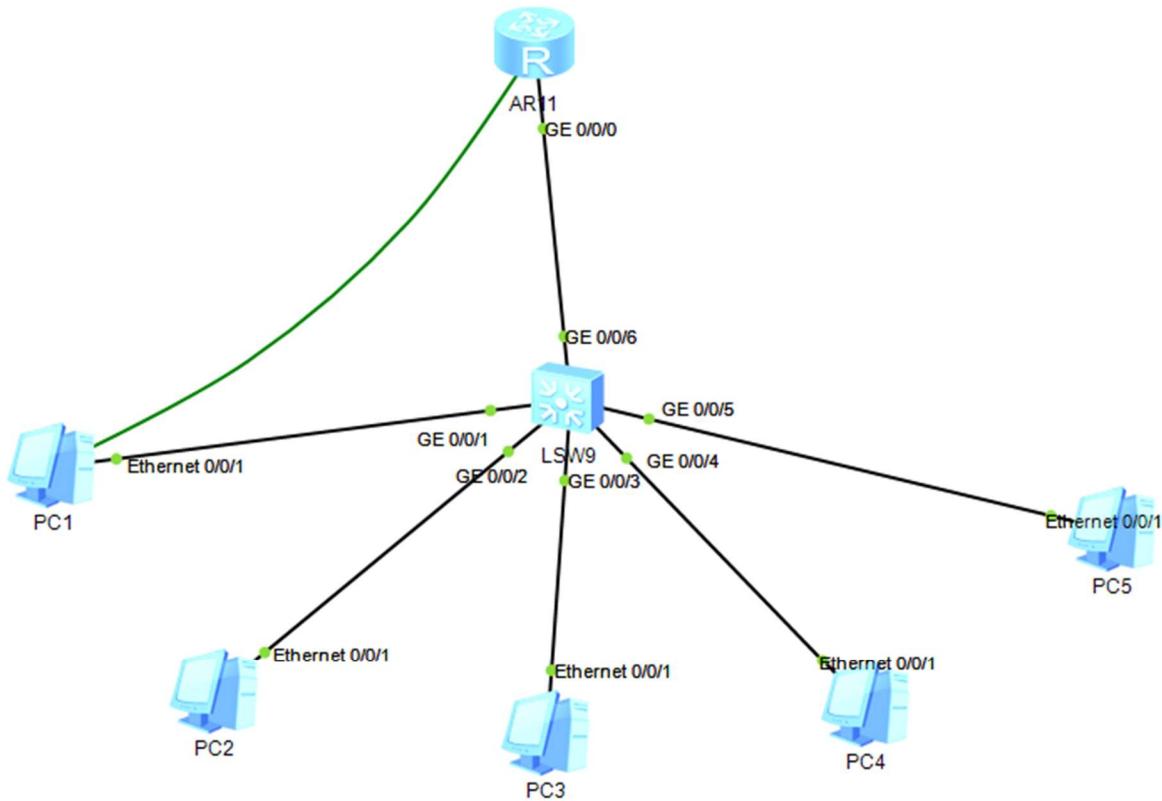
```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=255 time=47 ms
From 192.168.1.2: bytes=32 seq=2 ttl=255 time=46 ms
From 192.168.1.2: bytes=32 seq=3 ttl=255 time=32 ms
From 192.168.1.2: bytes=32 seq=4 ttl=255 time=47 ms
From 192.168.1.2: bytes=32 seq=5 ttl=255 time=46 ms

--- 192.168.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 32/43/47 ms

PC>
```

4.4-AAA



After activation DHCP from the router , if want to remote on the router from any PC connect console between router and PC then configure it from the router

```
[C4]us
[C4]user-int
[C4]user-interface c
[C4]user-interface console 0
[C4-ui-console0]au
[C4-ui-console0]auth
[C4-ui-console0]authentication-mode aaa
[C4-ui-console0]q
[C4]aaa
[C4-aaa]local
[C4-aaa]local-user admin pas
[C4-aaa]local-user admin password ci
[C4-aaa]local-user admin password cipher 123
[C4-aaa]
[C4-aaa]loca
[C4-aaa]local-user admin pr
[C4-aaa]local-user admin privilege 1
[C4-aaa]local-user admin privilege level 15
[C4-aaa]
[C4-aaa]loc
[C4-aaa]local-user admin ter
[C4-aaa]local-user admin se
[C4-aaa]local-user admin service-type ter
[C4-aaa]local-user admin service-type terminal
[C4-aaa]
[C4-aaa]q
[C4]z
```

PC1

Basic Config Command MCPacket UdpPacket Console

CmdLine

```
Login authentication

Username:admin
Password:
<C4>sys
Enter system view, return user view with Ctrl+Z.
[C4]

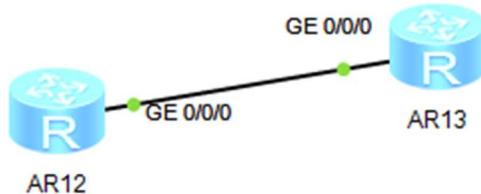
Please check whether system data has been changed, and
save data in time

Configuration console time out, please press any key to
log on
```

Settings

Bit Per Second: 9600
Data Bits: 8
Parity: None
Stop Bit: 1
Follow Control: None

Another connection



We will remote on AR13 from AR12 from terminal

First give everyone ip address AR12:192.168.1.1 AR13:192.168.1.2

```
[R1-aaa]auth
[R1-aaa]authentication-scheme C4
Info: Create a new authentication scheme.
[R1-aaa-authen-C4]ath
[R1-aaa-authen-C4]auth
[R1-aaa-authen-C4]authentication-m
[R1-aaa-authen-C4]authentication-mode ?
    hwtacacs  HWTACACS
    local      Local
    none       None
    radius     RADIUS
[R1-aaa-authen-C4]authentication-mode local
[R1-aaa-authen-C4]q
```

```
AR13
AR13

[R2-aaa]auth
[R2-aaa]authentication-scheme C4
Info: Create a new authentication scheme.
[R2-aaa-authen-C4]
[R2-aaa-authen-C4]
[R2-aaa-authen-C4]auth
[R2-aaa-authen-C4]authentication-m
[R2-aaa-authen-C4]authentication-mode local
[R2-aaa-authen-C4]
[R2-aaa-authen-C4]q
[R2-aaa]
[R2-aaa]do
[R2-aaa]domain C5
Info: Success to create a new domain.
[R2-aaa-domain-c5]auth
[R2-aaa-domain-c5]authorization-scheme C
[R2-aaa-domain-c5]authorization-scheme C4
Error: The authorization scheme does not exist.
[R2-aaa-domain-c5]auth
[R2-aaa-domain-c5]authentication-scheme C4
[R2-aaa-domain-c5]q
[R2-aaa]
[R2-aaa]lo
[R2-aaa]local-user admin pas
[R2-aaa]local-user admin password ci
[R2-aaa]local-user admin password cipher 123
[R2-aaa]lo
[R2-aaa]local-user admin pr
[R2-aaa]local-user admin privilege 1
[R2-aaa]local-user admin privilege level 15
[R2-aaa]local-user admin privilege level 15
```

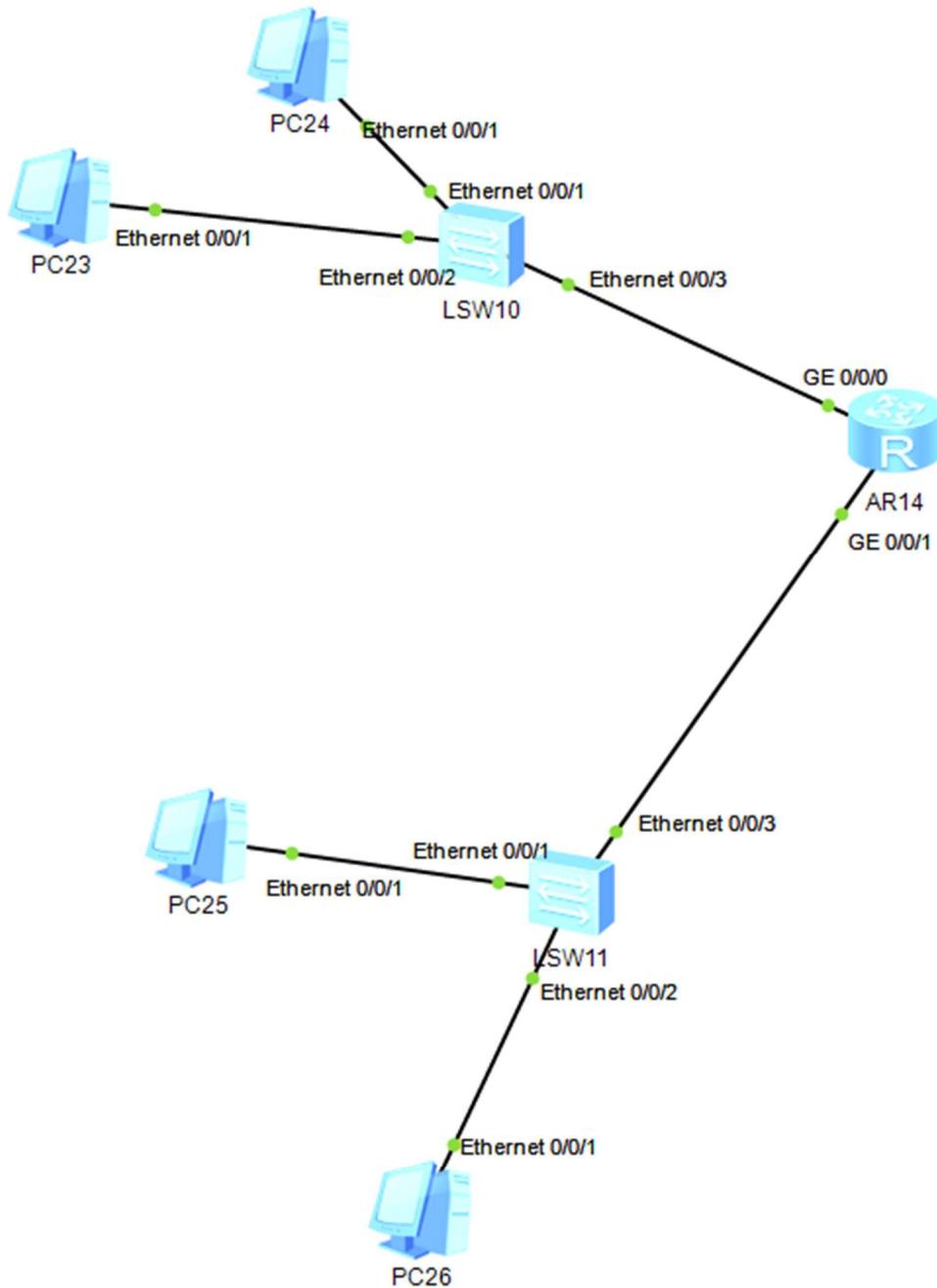
```
<R1>
<R1>te
<R1>telnet 192.168.1.2
      Press CTRL_] to quit telnet mode
      Trying 192.168.1.2 ...
      Connected to 192.168.1.2 ...

Login authentication

Username:admin
Password:
<R2>
<R1>
<R1>
```

4.5-ACL

We have two system as two area and in area one there is PC unwanted to reach PCs in area 1 so called that ACL



The device is running!

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]int
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/0
[Huawei-GigabitEthernet0/0/0]ipad
[Huawei-GigabitEthernet0/0/0]ip ad
[Huawei-GigabitEthernet0/0/0]ip address 192.168.10.1 24
Aug 18 2024 07:03:09-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[0]:The line protocol
IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]int g 0/0/1
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]ip ad
[Huawei-GigabitEthernet0/0/1]ip address 192.168.20.1 24
Aug 18 2024 07:03:34-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[1]:The line protocol
IP on the interface GigabitEthernet0/0/1 has entered the UP state.
[Huawei-GigabitEthernet0/0/1]
[Huawei-GigabitEthernet0/0/1]
<Huawei>
<Huawei>
<Huawei>
<Huawei>
<Huawei>ac
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]ac
[Huawei]access-user
```

After giving every interface ip address , must give every PC ip address

```
AR14
step      Specify step of ACL sub rule is
test-aaa   Accounts test
tracert    <Group> tracert command group
undo      Negate a command or set its defaults
[Huawei-acl-basic-2000]r
[Huawei-acl-basic-2000]ru
[Huawei-acl-basic-2000]rule ?
  INTEGER<0-4294967294> ID of ACL rule
  deny          Specify matched packet deny
  permit        Specify matched packet permit
[Huawei-acl-basic-2000]rule de
[Huawei-acl-basic-2000]rule deny s
[Huawei-acl-basic-2000]rule deny source 192.168.10.2 0.0.0.0
[Huawei-acl-basic-2000]q
[Huawei]
[Huawei]
[Huawei]int
[Huawei]interface g
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]tr
[Huawei-GigabitEthernet0/0/1]traf
[Huawei-GigabitEthernet0/0/1]traffic-fi
[Huawei-GigabitEthernet0/0/1]traffic-filter ou
[Huawei-GigabitEthernet0/0/1]traffic-filter outbound a
[Huawei-GigabitEthernet0/0/1]traffic-filter outbound acl 2000
[Huawei-GigabitEthernet0/0/1]

Please check whether system data has been changed, and save data in time
Configuration console time out, please press any key to log on
```

To test that from PC it has ip 192.168.10.2

```
PC>ping 192.168.20.2

Ping 192.168.20.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.20.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss

PC>
```

5- Wireshark Report

