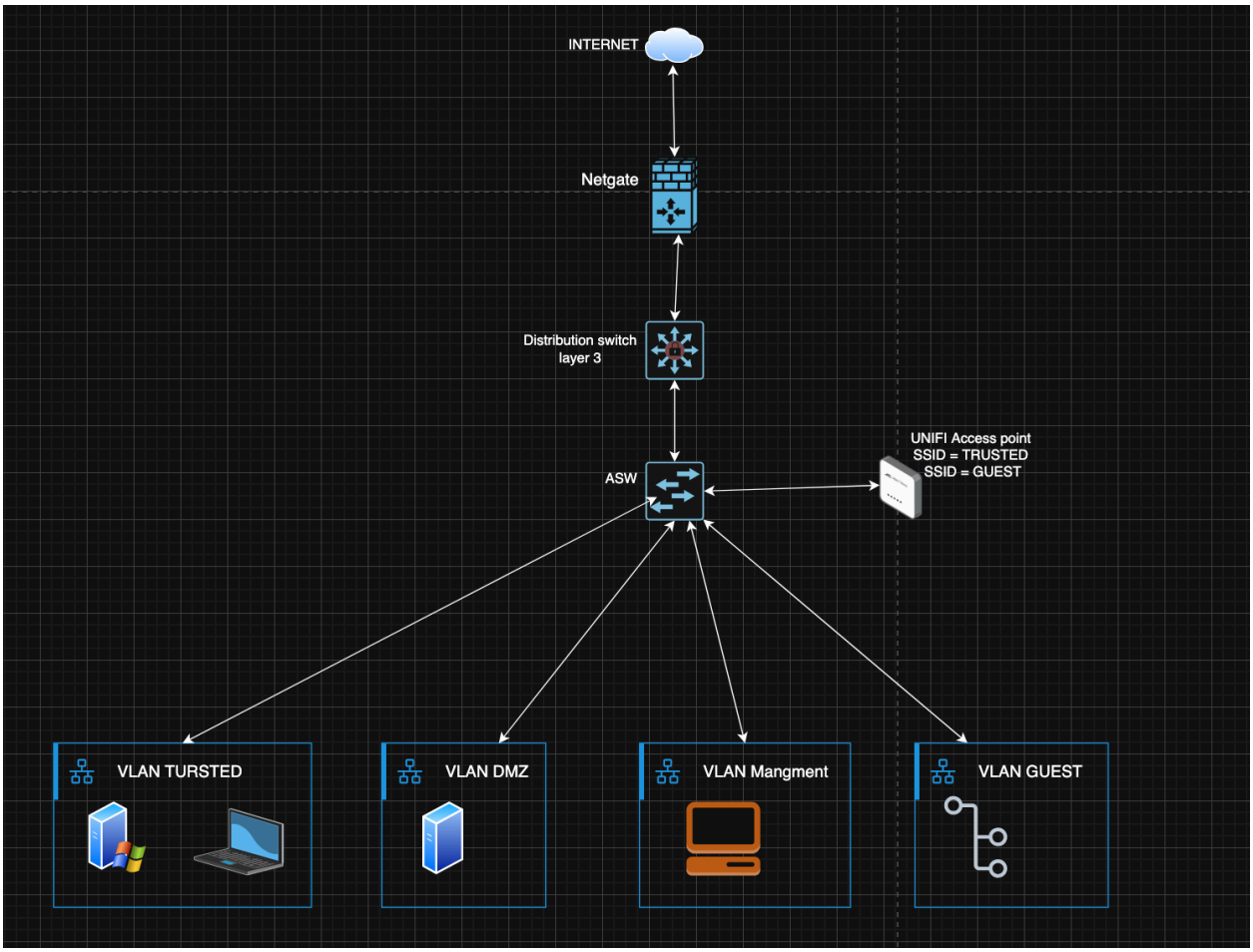
Mobile and Wireless Data Security - 2DV703, Report. Kinan Almasri, ka223mf



VLAN on DSW

VLANs are added on the DSW to separate the network into trusted, DMZ, guest and management areas. This allows traffic to be isolated and controlled with routing, ACLs and firewall rules.

```
vlan 10
 name Trusted
vlan 20
 name DMZ
vlan 30
 name Guest
vlan 99
 name Management
```

Define trunking ports and Native VLAN:

I configured the trunk ports between DSW and access switch ASW. The trunk allows all VLANs to pass through, and I set VLAN 99 as the native VLAN. I also disabled DTP for security so the port does not negotiate automatically. The same trunk configuration was also applied on the uplink ports of ASW to allow VLANs 10, 20, 30, and 99 to pass between switches.

```
interface fastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,99
 switchport trunk native vlan 99
 switchport nonegotiate
 no shutdo
```

DSW (VTP Server):

VTP was used so all switches have the same VLAN information automatically. The DSW works as the VTP server, and ASW are VTP client. This makes VLAN management easier and reduces manual configuration on each switch.

```
vtp mode server
vtp version 2
```

```
vtp domain Group6. "important that they are at same domain name"
vtp password cisco

OBS! Same command i used on ASW but instead of server, i wrote client
```

Enable routing on DSW & create SVIs:

To make the VLANs able to communicate with each other, I first enabled routing on the DSW so it works as a Layer 3 switch. This is necessary, because without it the switch can’t route between VLANs.

```
ip routing "important command on DSW"
```

SVI Configuration (for inter-VLAN routing):

```
interface vlan 10
ip address 10.0.10.1 255.255.255.0
no shutdown

interface vlan 20
ip address 10.0.20.1 255.255.255.0
no shutdown

interface vlan 30
ip address 10.0.30.1 255.255.255.0
no shutdown

interface vlan 99
ip address 10.0.99.1 255.255.255.0
no shutdown
```

DHCP on DSW (all VLANs)

DHCP is configured on the DSW so each VLAN gets IP addresses automatically. Each VLAN has its own DHCP pool with the correct network, gateway, and DNS. The gateway addresses and some IPs are excluded to avoid conflicts with servers or static devices.

```
ip dhcp excluded-address 10.0.10.1 10.0.10.10
ip dhcp excluded-address 10.0.10.245 10.0.10.254
ip dhcp excluded-address 10.0.20.1 10.0.20.10
ip dhcp excluded-address 10.0.20.245 10.0.20.254
ip dhcp excluded-address 10.0.30.1 10.0.30.10
ip dhcp excluded-address 10.0.30.245 10.0.30.254
ip dhcp excluded-address 10.0.99.1 10.0.99.10
ip dhcp excluded-address 10.0.99.245 10.0.99.254

ip dhcp pool VLAN10-POOL
 network 10.0.10.0 255.255.255.0
 default-router 10.0.10.1
 dns-server 8.8.8.8

ip dhcp pool VLAN20-POOL
 network 10.0.20.0 255.255.255.0
 default-router 10.0.20.1
 dns-server 8.8.8.8

ip dhcp pool VLAN30-POOL
 network 10.0.30.0 255.255.255.0
 default-router 10.0.30.1
 dns-server 8.8.8.8

ip dhcp pool VLAN99-POOL
 network 10.0.99.0 255.255.255.0
 default-router 10.0.99.1
 dns-server 8.8.8.8
```

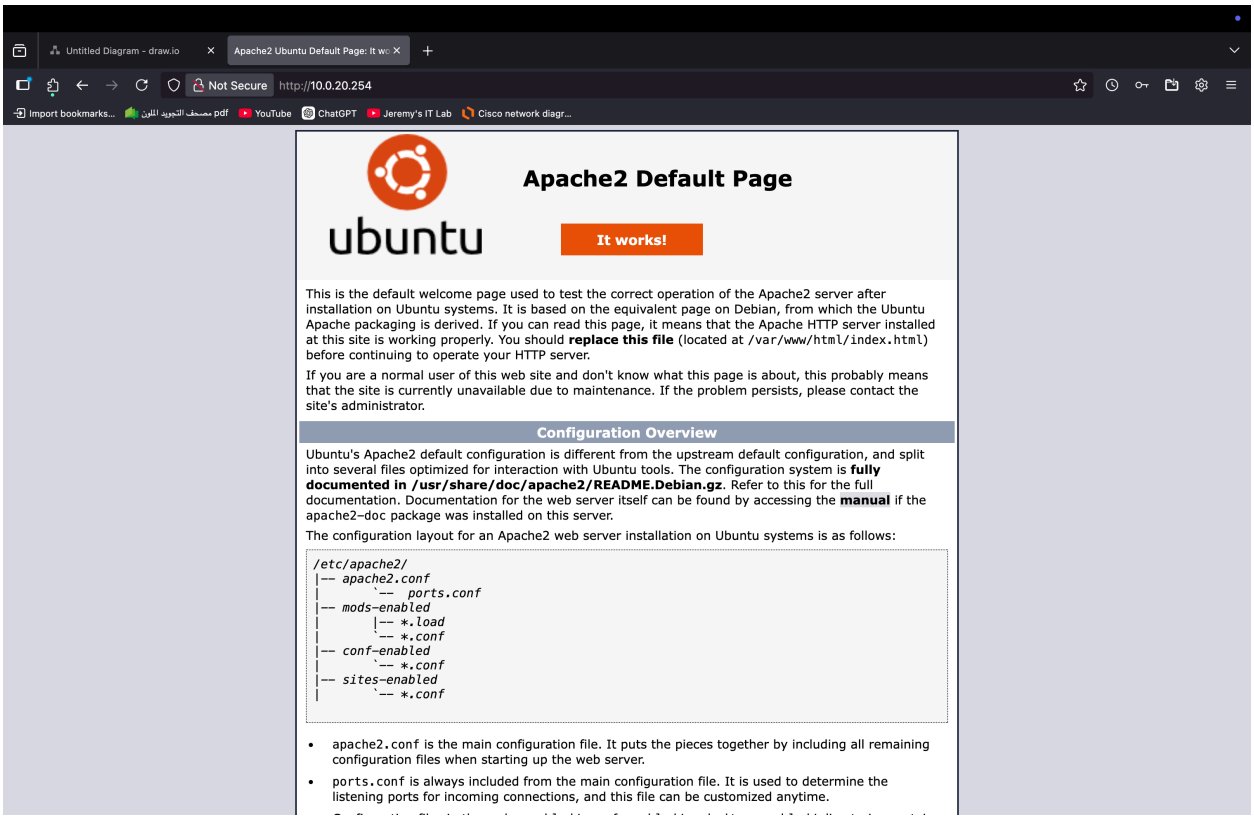
ACL rules

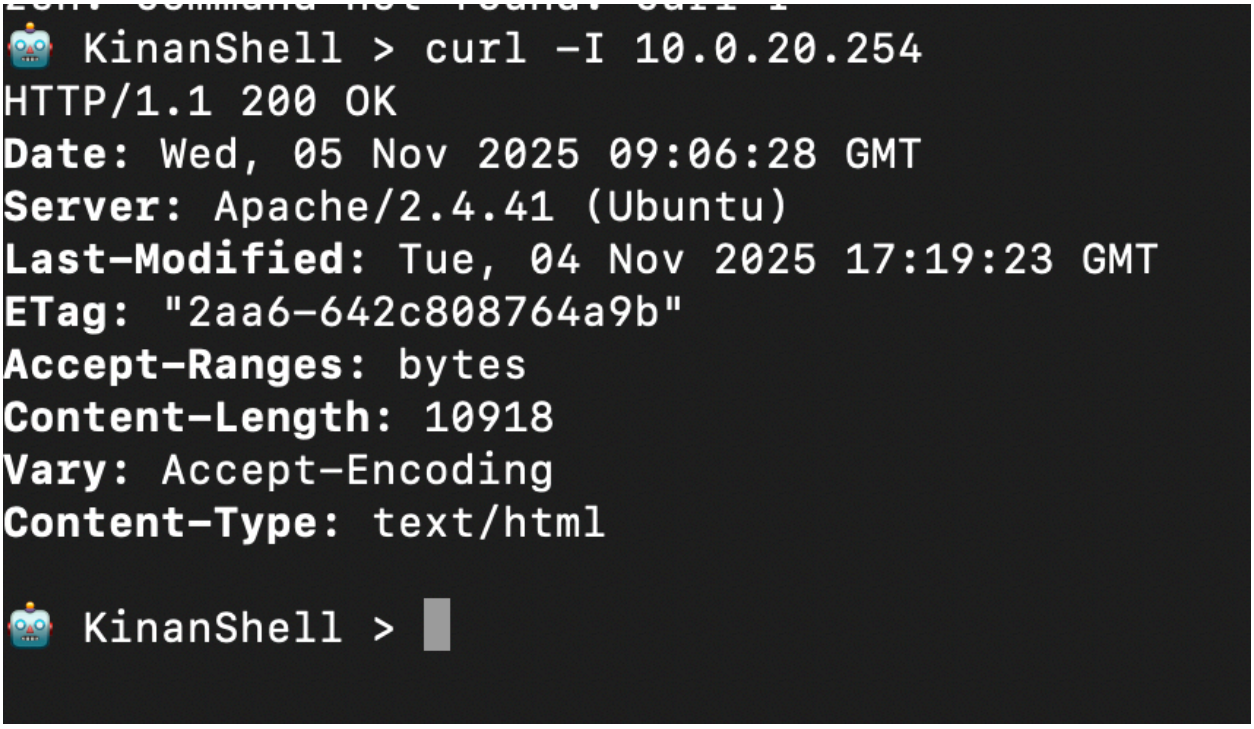
Implement ACLs to control access between VLANs

```
Extended IP access list KINAN_ACL
10 permit udp any any range bootps bootpc
20 permit ip 10.0.10.0 0.0.0.255 any
30 deny ip 10.0.30.0 0.0.0.255 10.0.10.0 0.0.0.255
40 deny ip 10.0.30.0 0.0.0.255 10.0.99.0 0.0.0.255
50 permit ip 10.0.30.0 0.0.0.255 any
60 permit tcp 10.0.20.0 0.0.0.255 any established
70 permit icmp 10.0.20.0 0.0.0.255 10.0.10.0 0.0.0.255 echo-reply
80 permit icmp 10.0.30.0 0.0.0.255 10.0.10.0 0.0.0.255 echo-reply
90 permit icmp 10.0.20.0 0.0.0.255 10.0.0.0 0.0.255.255 echo-reply
100 permit icmp 10.0.99.0 0.0.0.255 10.0.10.0 0.0.0.255
110 permit udp 10.0.99.0 0.0.0.255 host 10.0.10.254 eq 1812
120 permit udp 10.0.99.0 0.0.0.255 host 10.0.10.254 eq 1813
130 deny ip any any
```

TEST CURL AND ACCESS FROM THE BROWSER:

The web server in the VLAN 20, (10.0.20.254) was tested using both a browser and the curl command. The page loaded successfully and returned HTTP 200 OK, which confirms that the server is reachable from the internal network.


Untitled Diagram - draw.io
Apache2 Ubuntu Default Page: It wo
Not Secure
http://10.0.20.254
Import bookmarks...
YouTube
ChatGPT
Jeremy's IT Lab
Cisco network diagr...
ubuntu
Apache2 Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.


KinanShell > curl -I 10.0.20.254
HTTP/1.1 200 OK
Date: Wed, 05 Nov 2025 09:06:28 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 04 Nov 2025 17:19:23 GMT
ETag: "2aa6-642c808764a9b"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html
KinanShell >

DSW routed link to Netgate

To connect the DSW to the Netgate firewall using a Layer 3 link, I converted interface fa0/2 into a routed port and gave it an IP address in a /30 network.

```
interface fastEthernet0/2
 no switchport
 !description TO-NETGATE LAN1
 ip address 172.16.1.2 255.255.255.252
 no shutdown
```

Default Route on DSW

I added a default route on the DSW so all unknown traffic is sent to the Netgate firewall.

```
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

Netgate (pfSense)

pfSense was configured from the console. The WAN interface was given a static IP for internet access, and the LAN interface was set to connect to the internal network through the core switch.

1. Assign interfaces

```
Enter WAN interface name → mvneta0
Enter LAN interface name → mvneta1
```

2. Set WAN IP

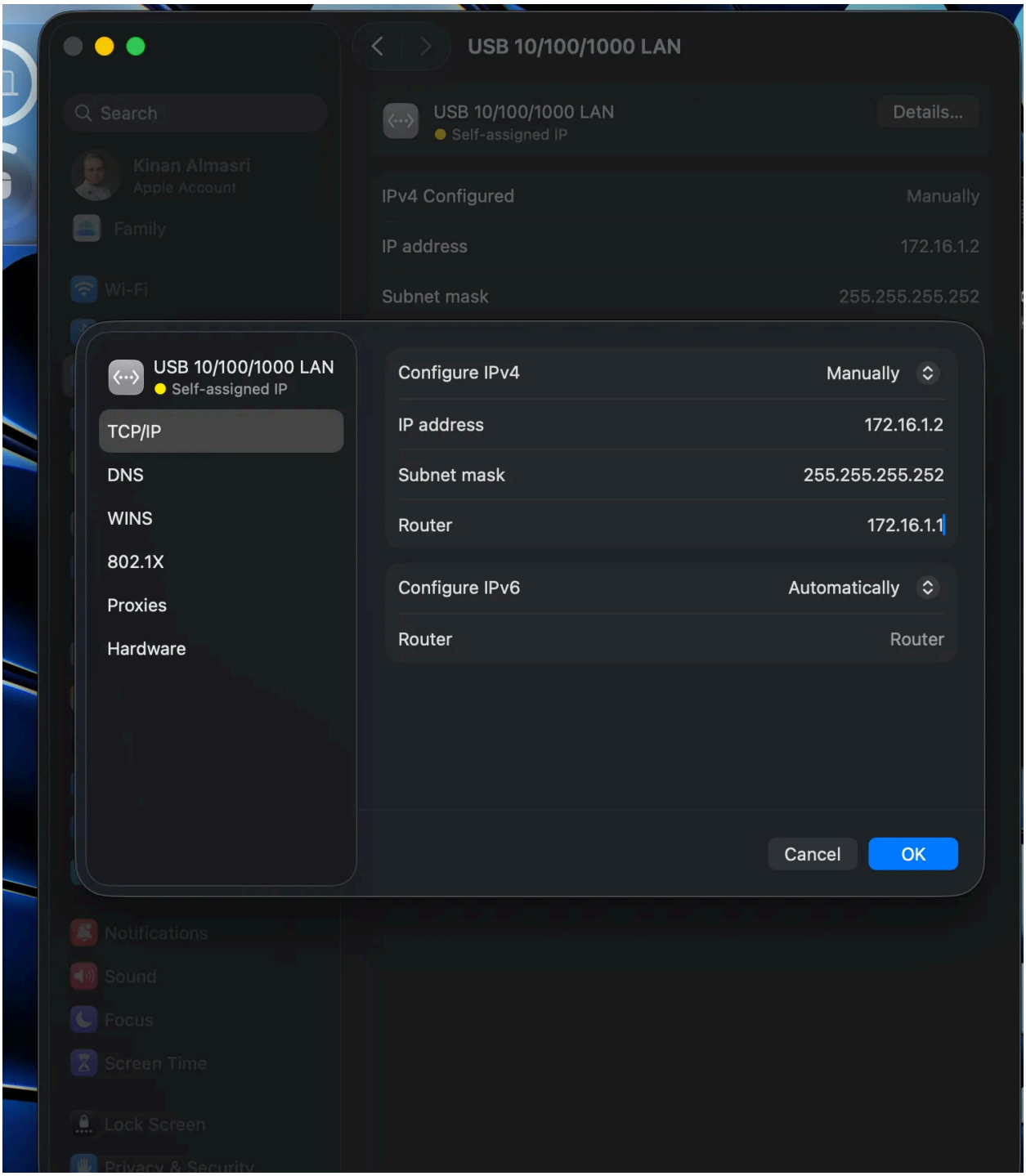
```
Interface: WAN
New IPv4 address → 192.168.0.61
Subnet mask bits → 24
```

```
For wan enter the new wan ipv4 upstream gateway address.For lan, press ent
er for none: 192.168.0.1 (outside)
```

3. Set LAN IP

```
Interface: LAN
New IPv4 address → 172.16.1.1
Subnet mask bits → 30
```

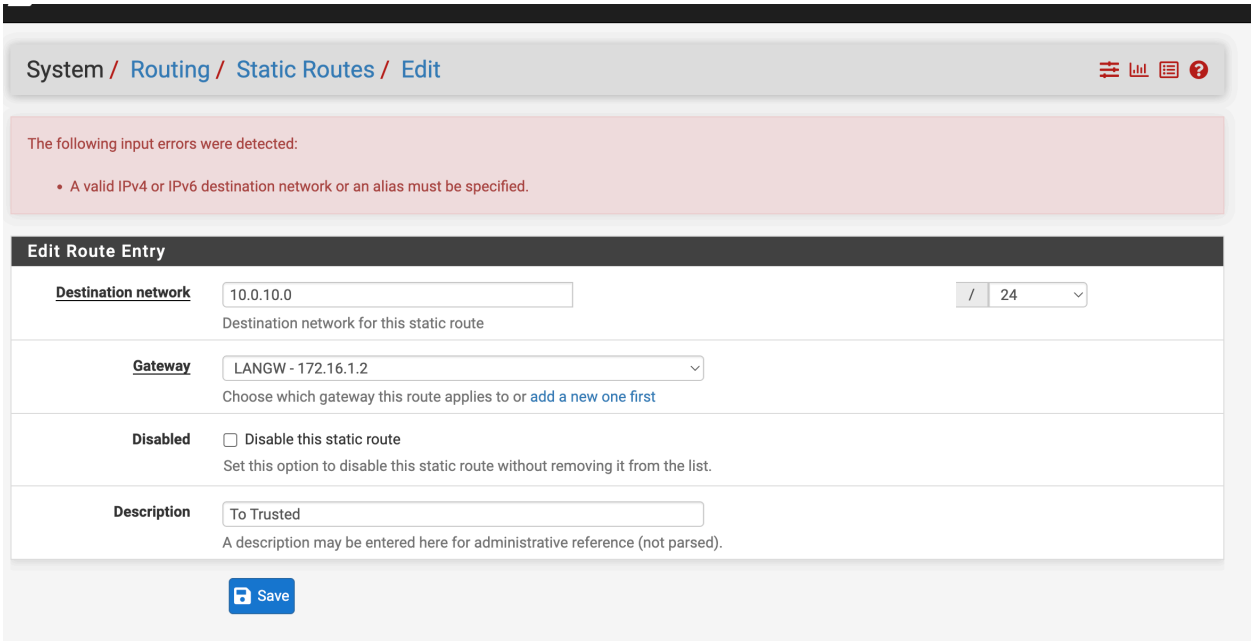
Access the GUI



Static routes

Static routes were added on pfSense so it knows how to reach all VLAN networks through the core switch (DSW).

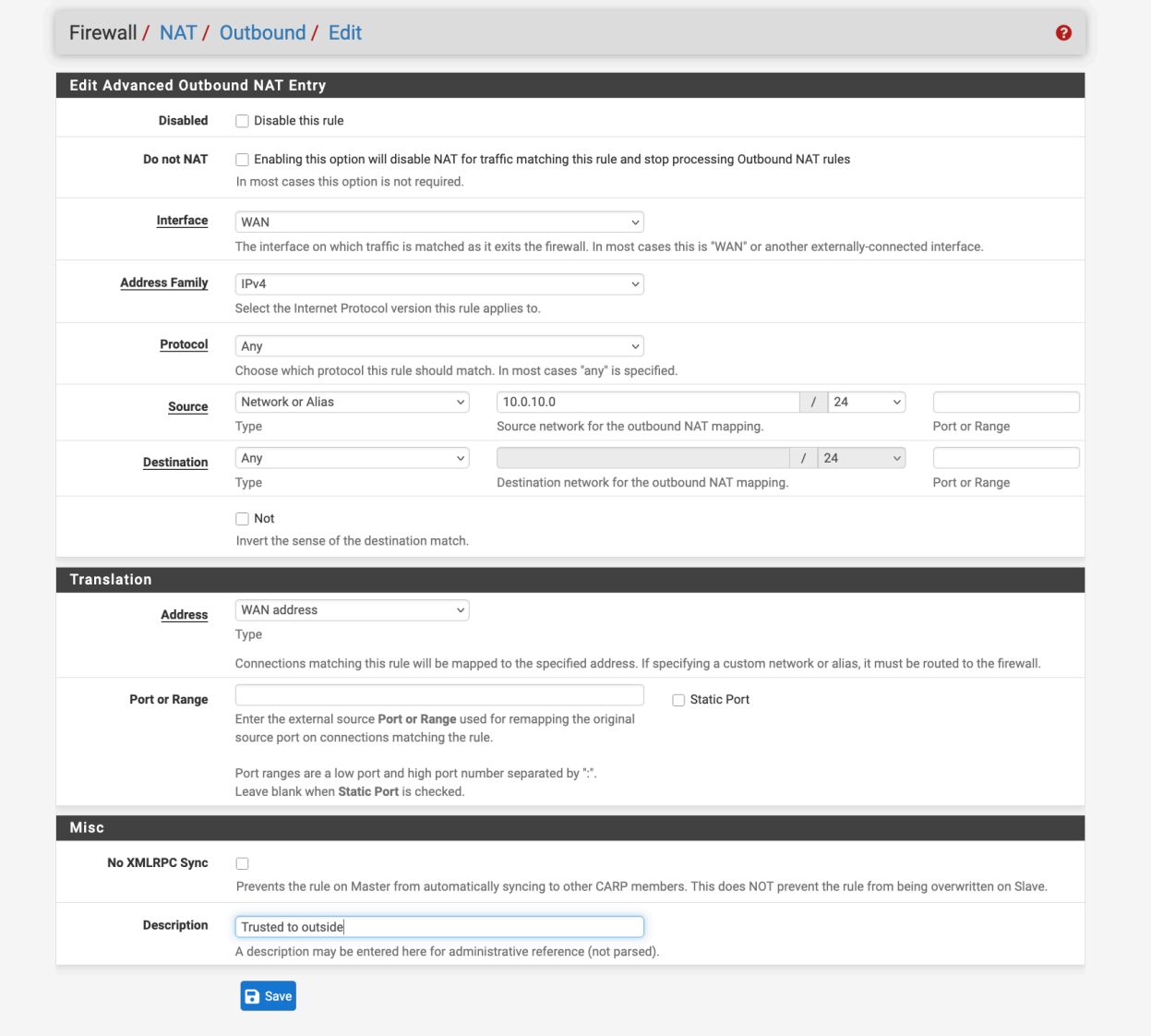
10.0.10.0/24 → 172.16.1.2 10.0.20.0/24 → 172.16.1.2 10.0.30.0/24 → 172.16.1.2 10.0.99.0/24 → 172.16.1.2



NAT

On the pfSense firewall, I enabled outbound NAT so that the VLANs inside the network (10, 20 and 30) can access the internet. When they go outside, their private IP addresses are translated to the firewall's WAN IP.

Source network: 10.0.10.0/24
Source network: 10.0.20.0/24
Source network: 10.0.30.0/24



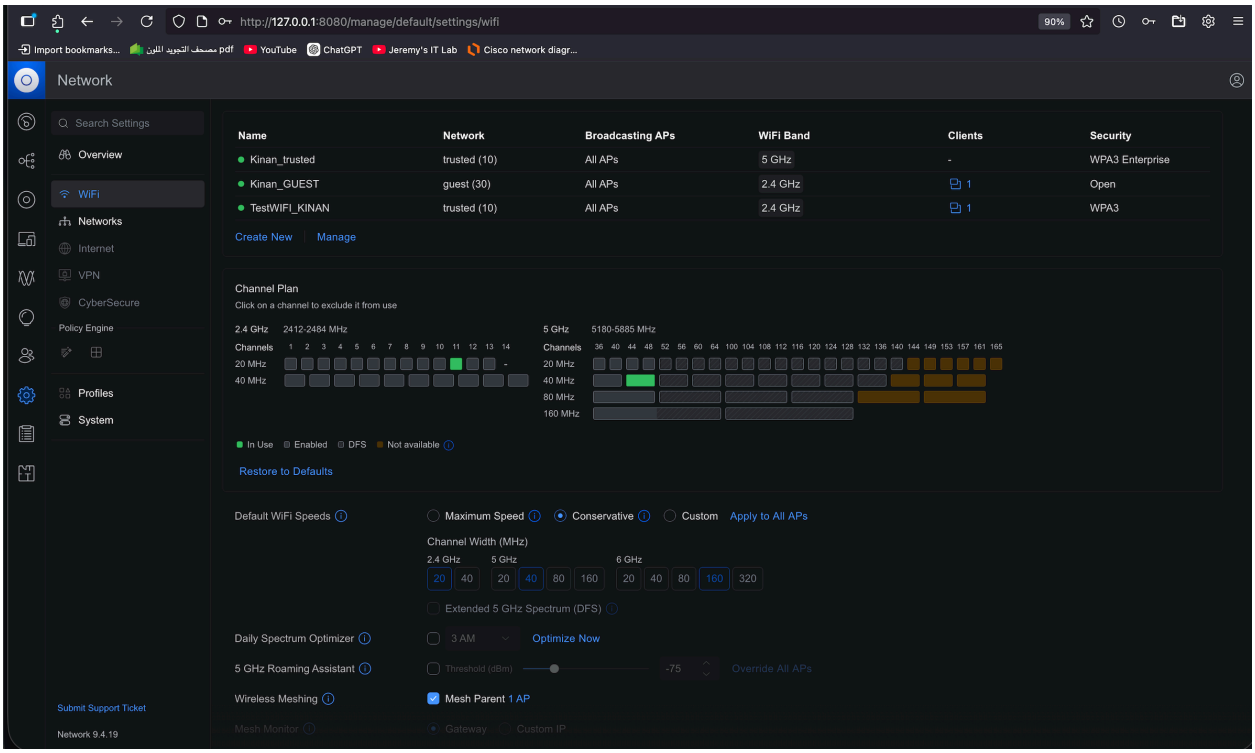
Connect Unifi AP to network

The access point is connected to a trunk port on ASW so it can carry multiple SSIDs on different VLANs (Trusted, Guest, Management). VLAN 99 is used as the native VLAN for management.

```
interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
```

```
switchport mode trunk
switchport trunk allowed vlan 10,30,99
switchport trunk native vlan 99
switchport nonegotiate
spanning-tree portfast trunk
no shutdown
```

1. **Guest Wi-Fi**
    - security valid Open
    - No RADIUS login internet access only
2. **Trusted Wi-Fi**
    - WPA3-Enterprise with RADIUS (Windows NPS).
    - Users authenticate with their domain credentials.
3. **Test Wi-Fi**
    - No RADIUS. Security mode switched per run: Open → WPA2 → WPA3.
    - Other settings kept the same to measure the overhead fairly.



Radius server:

I installed Windows Server 2025 and gave it a static IP (10.0.10.254 / 255.255.255.0) with gateway 10.0.10.1 and DNS 8.8.8.8 and 8.8.4.4 so it could reach the internet. The server was connected to the Trusted VLAN which also allowed me to use Remote Desktop from my laptop while I was connected to the trusted Wi-Fi.

After that, I promoted the server to a Domain Controller and installed Active Directory. In “Active Directory Users and Computers” I created the domain users, like the user “kinan”, which I later used to log in to the secure Wi-Fi. and the password was Macbookmacbook@123456 the password should be strong like this and it cannot include my name.

Next, I installed the Network Policy Server (NPS) role to use the server as a RADIUS server. In NPS, I added the UniFi Access Point as a RADIUS Client. The IP

of the AP was 10.0.99.100 and I used a shared secret that I also wrote later in the UniFi Controller. Then I created a Network Policy for Wi-Fi access. The policy was set to allow access and used PEAP (Protected EAP) for authentication. Only domain users are allowed to connect.

Finally, in the UniFi Controller, I set my trusted Wi-Fi SSID to WPA3-Enterprise and added the RADIUS server details (IP 10.0.10.254). When connecting, the access point sends the username and password to the Windows Server, and NPS checks it with Active Directory. If the user exists and is correct, the Wi-Fi connection is allowed.

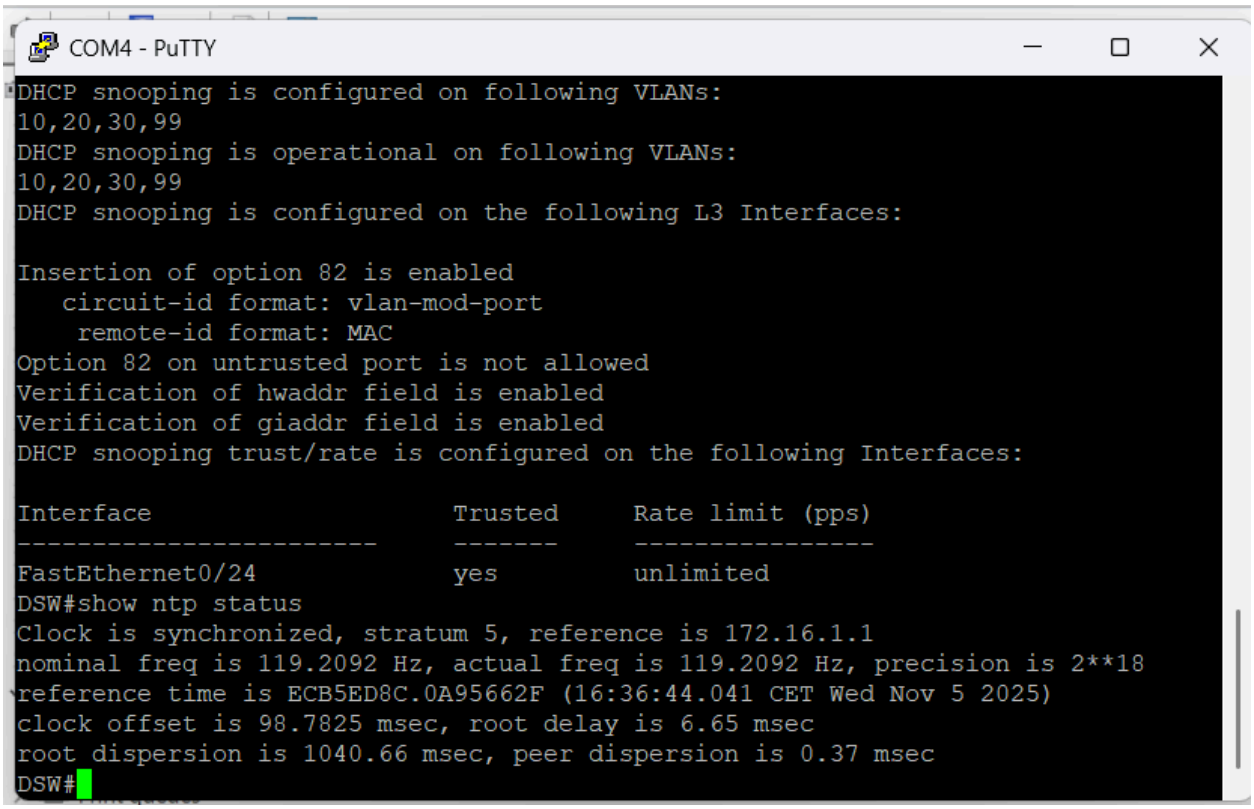
Protecting against a hacker:

1. NTP Configuration (Time Sync on the Network)

To make sure all devices in my network use the same time, I set up NTP. I used my pfSense firewall as the main time server, and that one gets the correct time from the internet (for example time.cloudflare.com). After that, I configured the DSW to sync its time from the firewall.

On the DSW I added the firewall IP as the NTP server, and after a few minutes I checked with `show ntp status` and it showed “Clock is synchronized”, so I knew it was working. Since the management VLAN is protected by ACLs, I also had to allow NTP traffic there so the switch could reach the firewall.

```
ntp server 172.16.1.1
clock timezone CET 1
```



On ASW:

I did the same setup:

```
interface vlan 99
 ip address 10.0.99.200 255.255.255.0
 ip default-gateway 10.0.99.1
ntp server 172.16.1.1
clock timezone CET 1
```

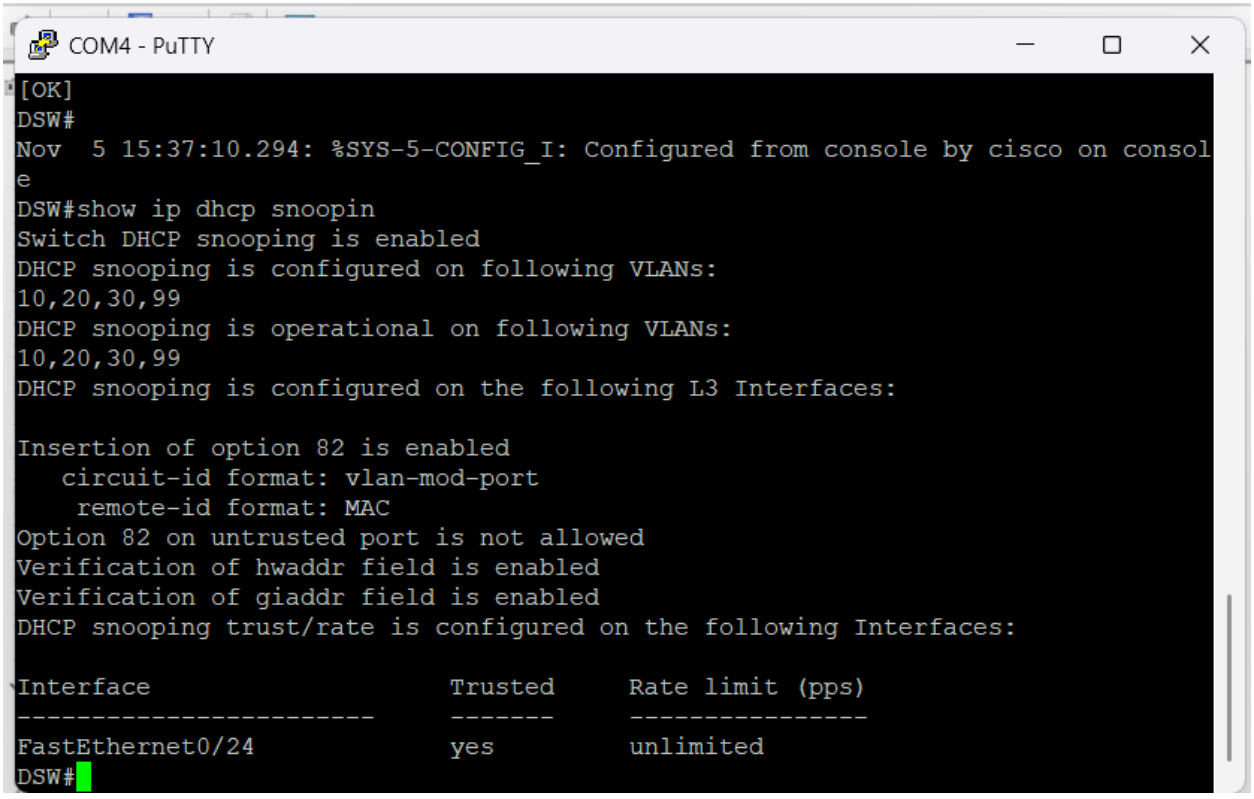
When I used `show ntp associations`, it showed `~172.16.1.1`, which means ASW1 found the NTP server and is trying to sync. It just didn't finish yet. I did this around 10 minutes before the exam, so I didn't have time to wait for full synchronization. But the configuration is correct and working it only needs more time.

```
ASW1#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~172.16.1.1      .INIT.          16      -     64     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ASW1#
```

2. DHCP Snooping

I **enabled** DHCP Snooping on the DSW and ASW to stop fake DHCP servers. I set it on VLANs 10, 20, 30 and 99. The port that goes to the real DHCP server (the firewall) is marked as trusted and all other ports are untrusted. After that, I checked with `show ip dhcp snooping` and it showed that DHCP Snooping is active and only the uplink port is trusted.



3. ACL – Protection Against Hackers and Unauthorized Access

To secure the network, I created an ACL on the DSW to control which VLANs are allowed to talk to each other. In this ACL, I blocked the guest VLAN (10.0.30.0/24) from accessing both the trusted VLAN (10.0.10.0/24) and the management VLAN (10.0.99.0/24).

The DMZ VLAN (10.0.20.0/24) is only allowed to reply if the traffic was started from inside the network (using the established rule). I also allowed RADIUS traffic from the management VLAN to the server at 10.0.10.254 so Wi-Fi authentication works.

If I had more time, I would add log monitoring and an IDS like Suricata or Snort. These tools help detect attacks such as port scans, strange traffic or many failed login attempts.

During the exam, I searched a bit about these tools to make sure they would work in my network. I didn't have time to install them, but if I could continue, I would install Suricata, add rules for my VLANs and send the alerts to a log server.

Ubuntu / Windows

I used my laptop with Ubuntu as the web server in the DMZ. First, I connected it to the internet to update the system and install Apache. After that, I tested it by opening a browser and typing `localhost` to make sure the web server works.

Then I moved the laptop to VLAN 20 (DMZ) and set a static IP address:

- IP: 10.0.20.254
- Subnet mask: 255.255.255.0
- Gateway: 10.0.20.1

- DNS: 8.8.8.8, 8.8.4.4

On the Windows Server, I set a static IP address so it can always be reachable in the Trusted VLAN. I gave it:

- IP address: 10.0.10.254
- Subnet mask: 255.255.255.0
- Default gateway: 10.0.10.1 (DSW SVI for VLAN 10)
- DNS: 8.8.8.8 and 8.8.4.4

and after applying the settings, I used `ipconfig` in Command Prompt to confirm it was correctly set.

Task 4 – Wi-Fi Security and Speed

For this test I wanted to see if Wi-Fi security affects internet speed. I used the Ubuntu server to host a 1 GB file and downloaded it from my Windows laptop using this command:

```
curl.exe -o NUL -w "Time: %{time_total}s | Speed: %{speed_download} byte
s/s\n" http://10.0.10.15:8000/largefile.bin
```

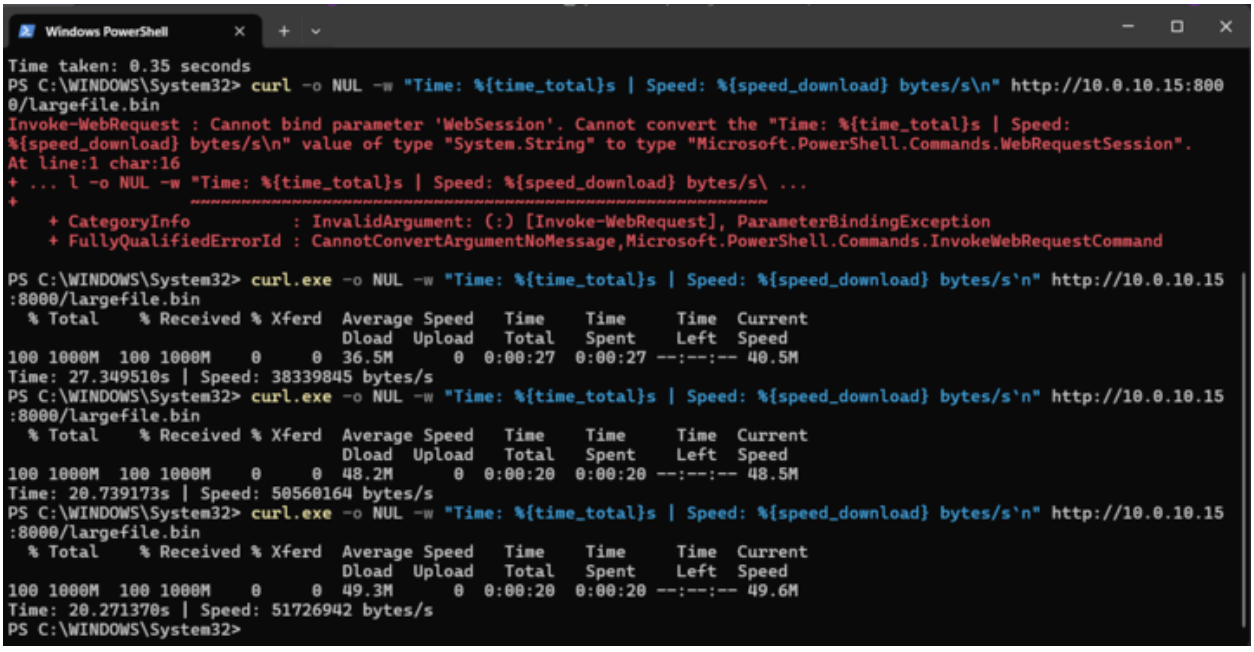
I tested the download three times with different Wi-Fi security settings:

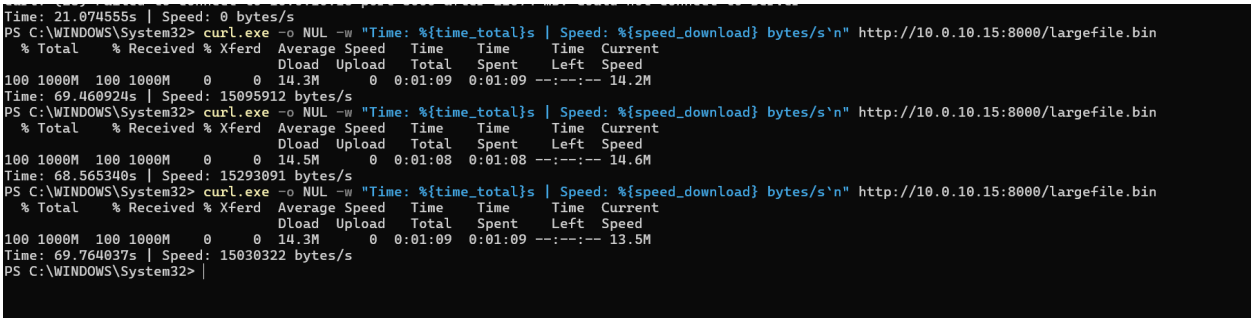
- Open Wi-Fi (no password): Fastest speed, around 48–50 MB/s, because there is no encryption.
- WPA2: Speed dropped to around 14–15 MB/s, because all data is encrypted and decrypted.
- WPA3: Almost the same speed as WPA2 (14–15 MB/s), but with stronger security.

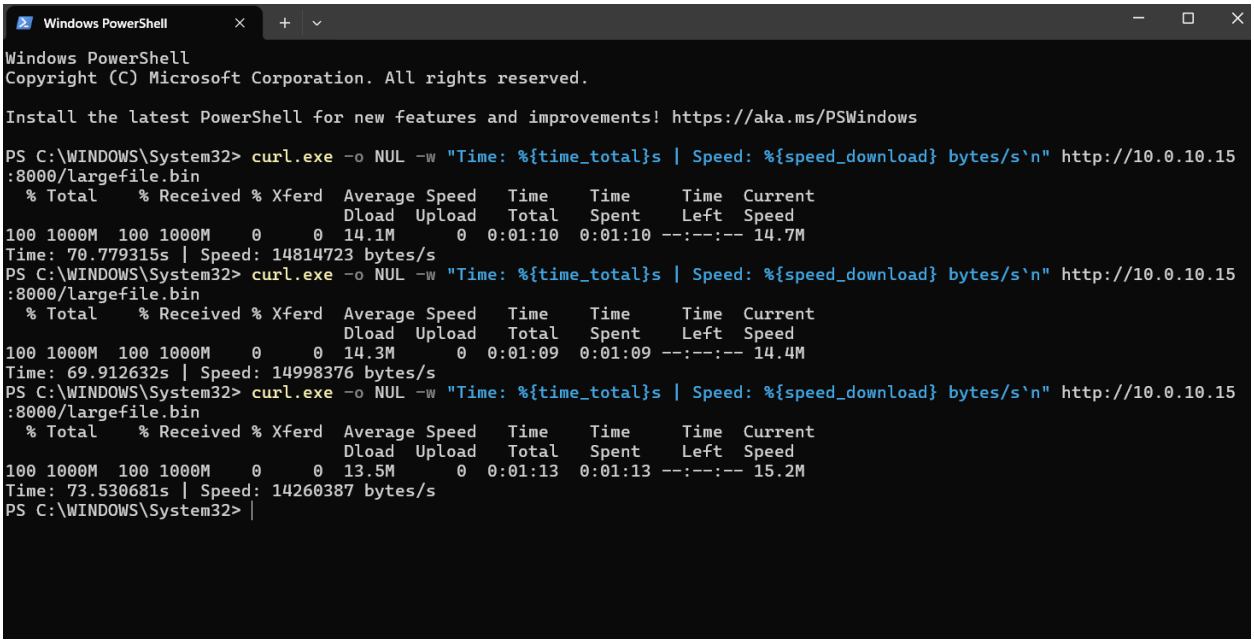
Result analysis

From my tests, it is clear that Wi-Fi security affects speed. Open Wi-Fi was the fastest. When I used WPA2 or WPA3, the speed became much lower. This is expected, because encryption makes the access point and the client use more processing power for every packet.

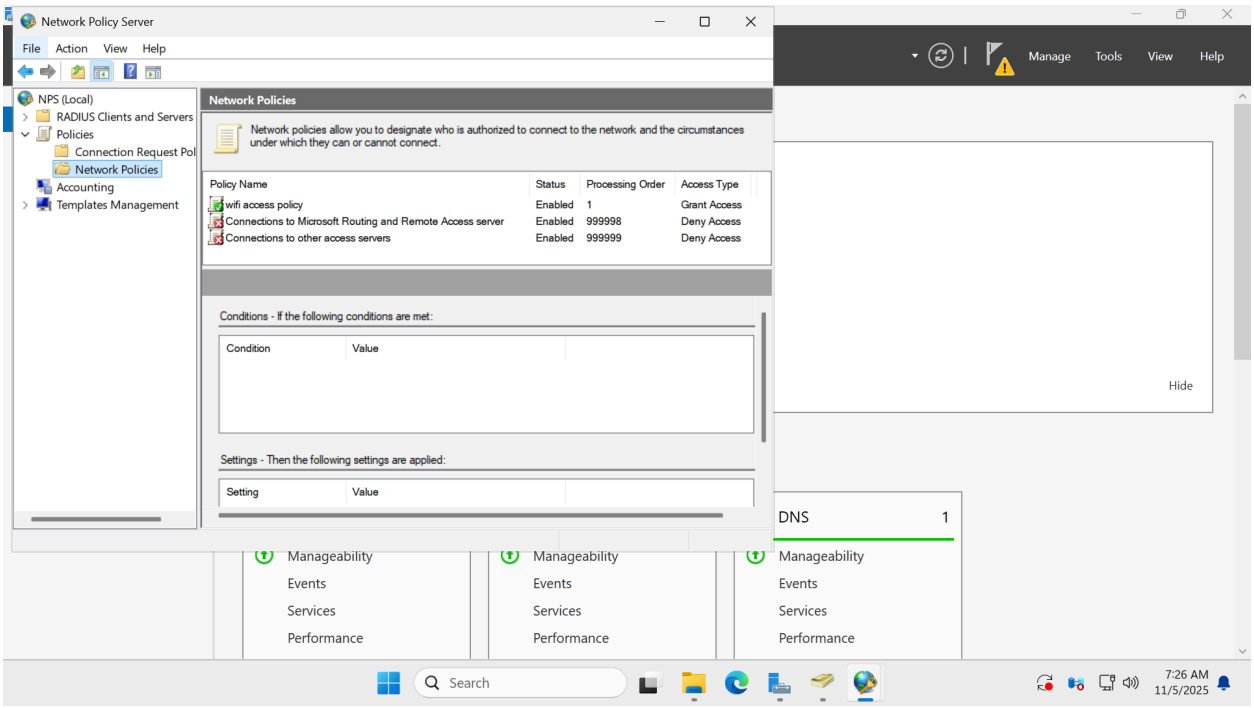
Research also shows the same thing like secure Wi-Fi like WPA2 and WPA3 is slower than open Wi-Fi because of encryption [1]. However, many studies show only a small drop in speed (about 5–10%), while in my test the drop was much bigger. I think this is because maybe the laptop I used are not very powerful for encryption and like stronger encryption in WPA2/WPA3 uses more CPU

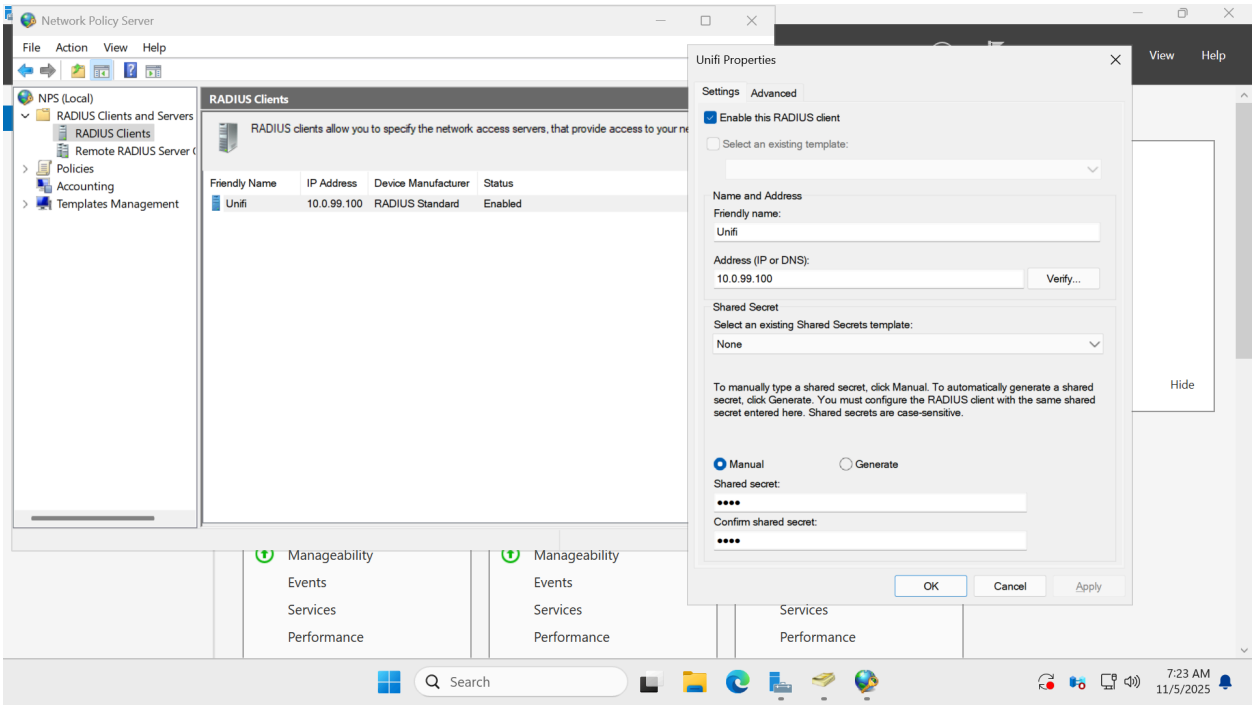




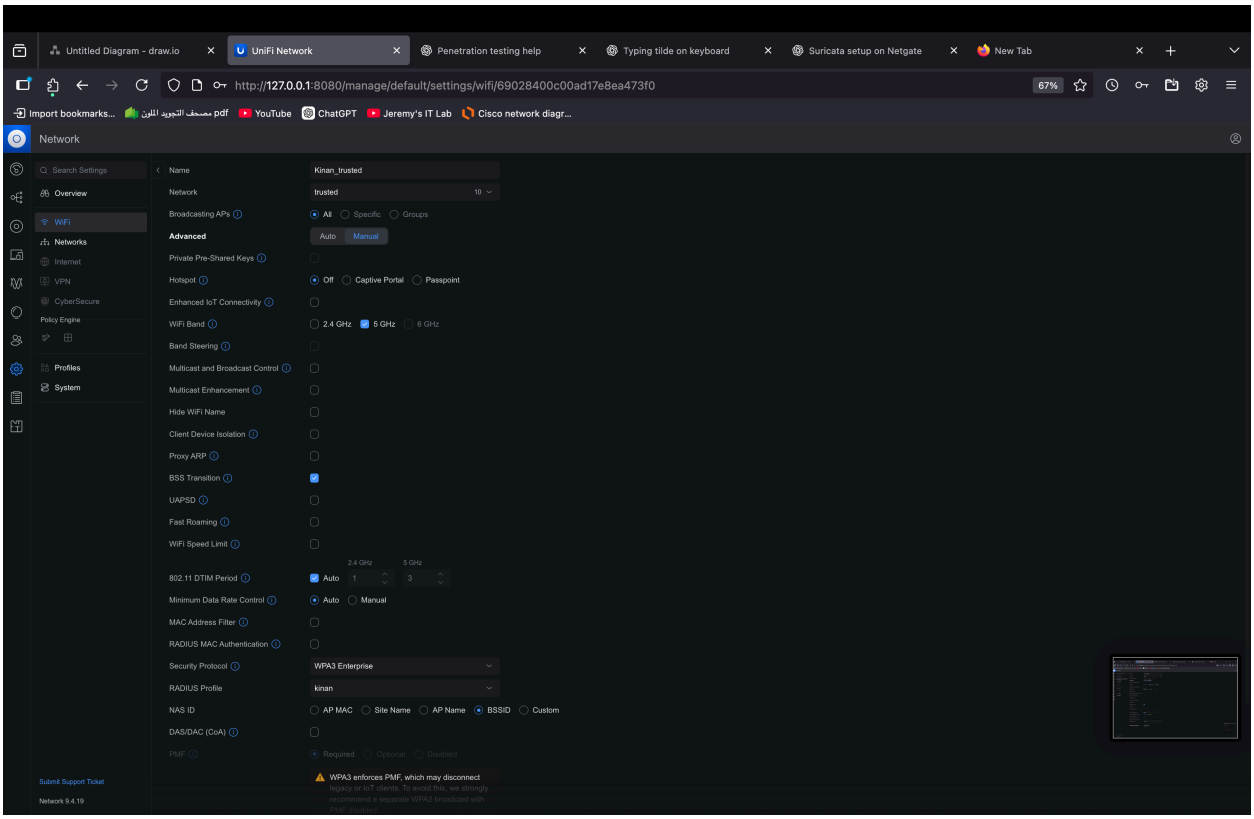


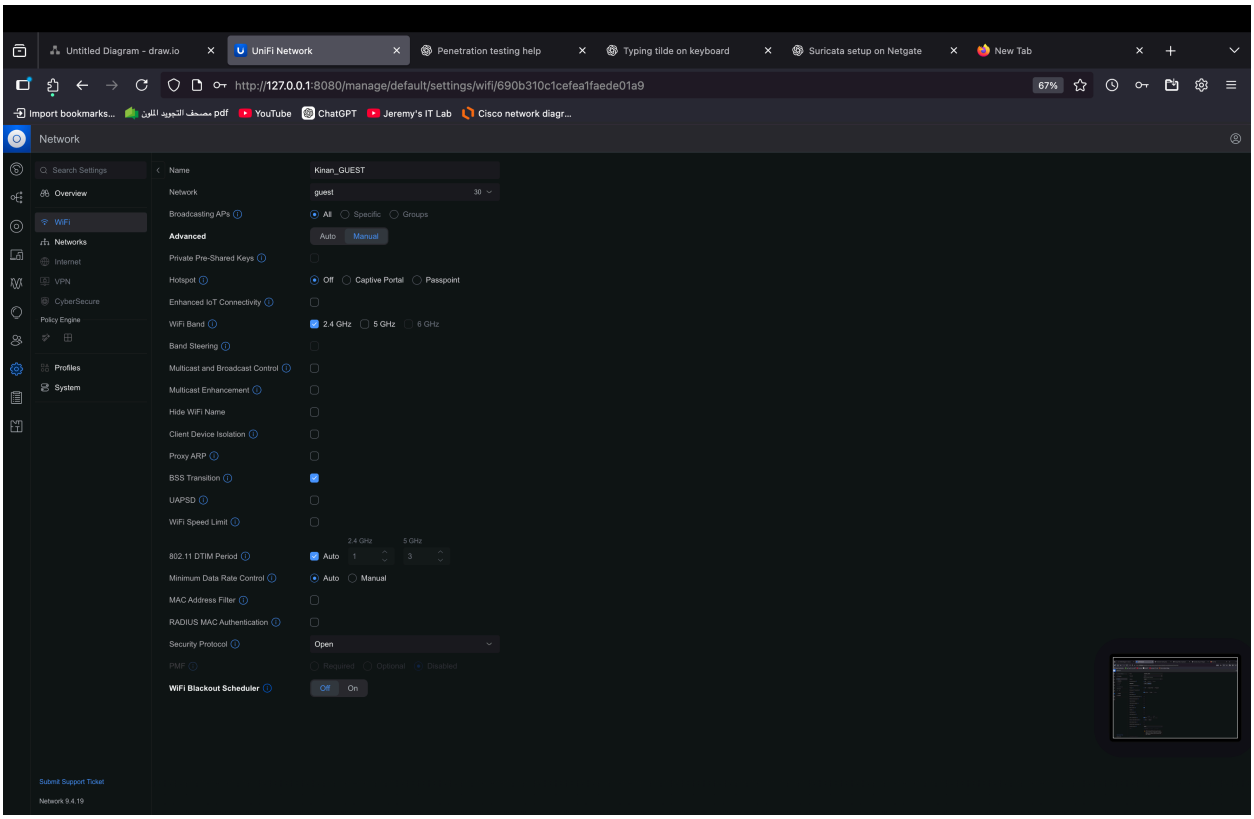
Screenshot from what I did:



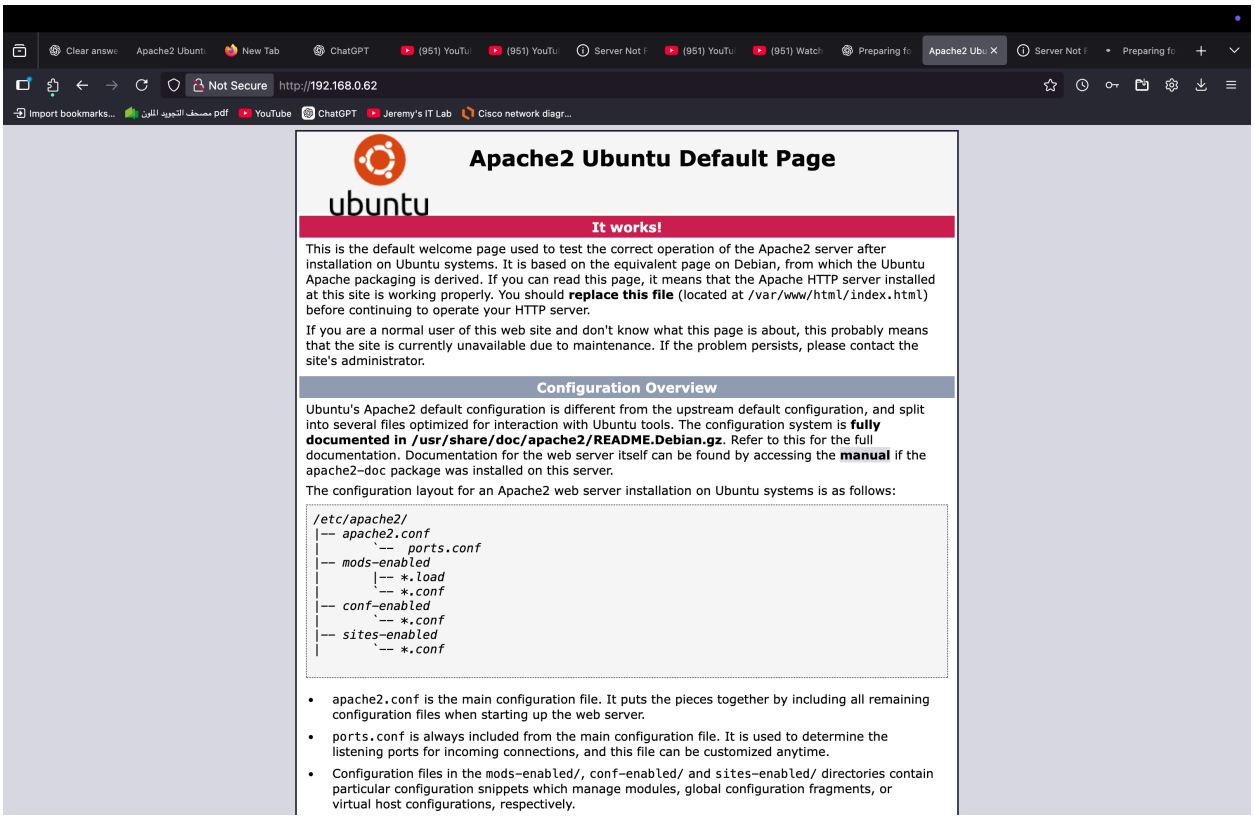

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server (
Policies
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify the network access servers, that provide access to your ne
Friendly Name
IP Address
Device Manufacturer
Status
Unifi
10.0.99.100
RADIUS Standard
Enabled
Unifi Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Unifi
Address (IP or DNS):
10.0.99.100
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply
View
Help
Hide
Manageability
Events
Services
Performance
Search
7:23 AM
11/5/2025

for unifi

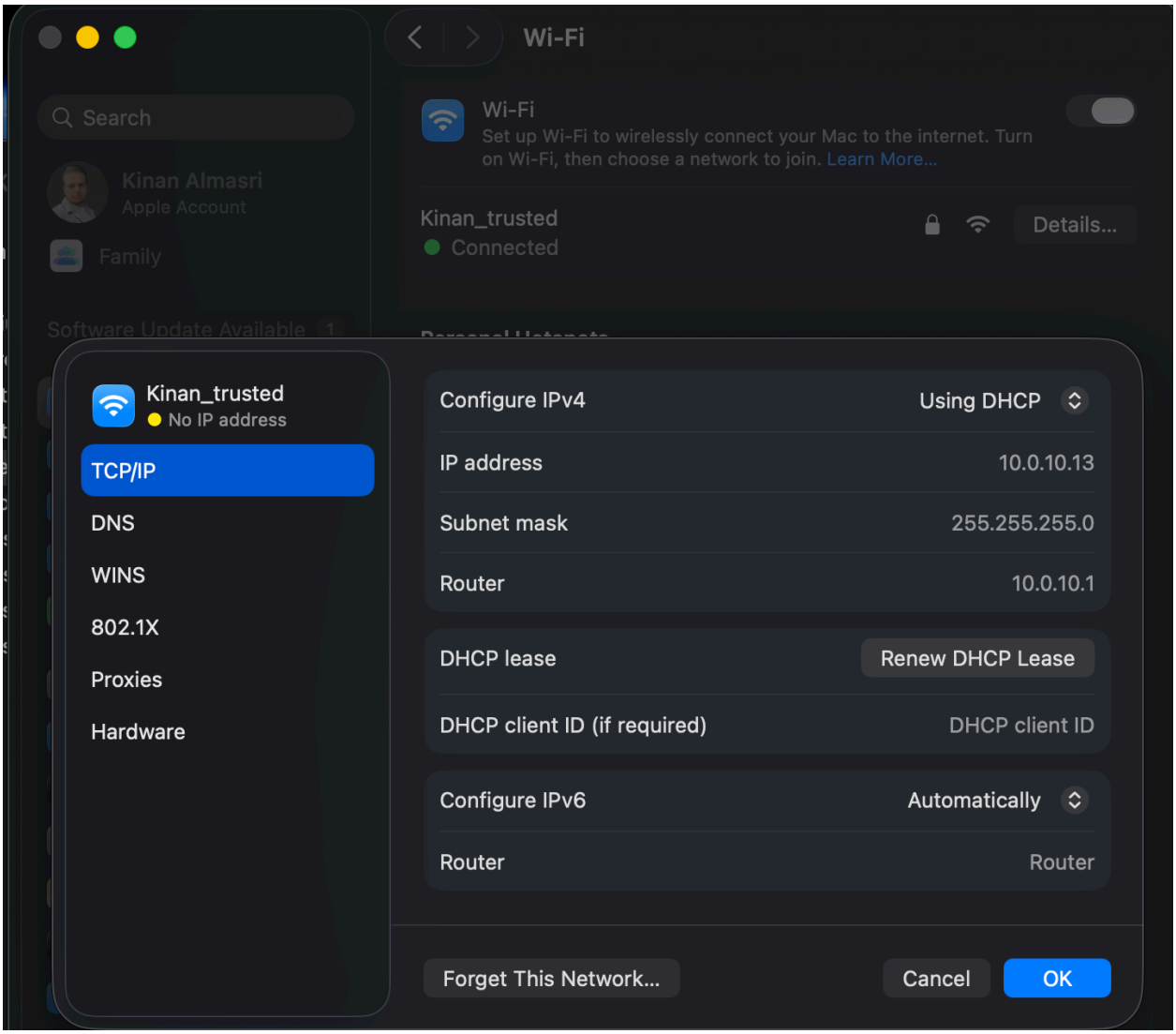

Untitled Diagram - draw.io
UniFi Network
Penetration testing help
Typing tilde on keyboard
Suricata setup on Netgate
New Tab
http://127.0.0.1:8080/manage/default/settings/wifi/69028400c00ad17e8ea473f0
67%
Import bookmarks...
YouTube
ChatGPT
Jeremy's IT Lab
Cisco network diagr...
Network
Search Settings
Overview
WiFi
Networks
Internet
VPN
CyberSecure
Policy Engine
Profiles
System
Submit Support Ticket
Network 9.4.19
Name
Kinan_trusted
Network
trusted
Broadcasting APs
All
Specific
Groups
Advanced
Auto
Manual
Private Pre-Shared Keys
Hotspot
Off
Captive Portal
Passpoint
Enhanced IoT Connectivity
WiFi Band
2.4 GHz
5 GHz
6 GHz
Band Steering
Multicast and Broadcast Control
Multicast Enhancement
Hide WiFi Name
Client Device Isolation
Proxy ARP
BSS Transition
UAPSD
Fast Roaming
WiFi Speed Limit
802.11 DTIM Period
Minimum Data Rate Control
MAC Address Filter
RADIUS MAC Authentication
Security Protocol
WPA3 Enterprise
RADIUS Profile
kinan
NAS ID
AP MAC
Site Name
AP Name
BSSID
Custom
DAS/DAC (CoA)
PMF
Required
Optional
Disabled
WPA3 enforces PMF, which may disconnect

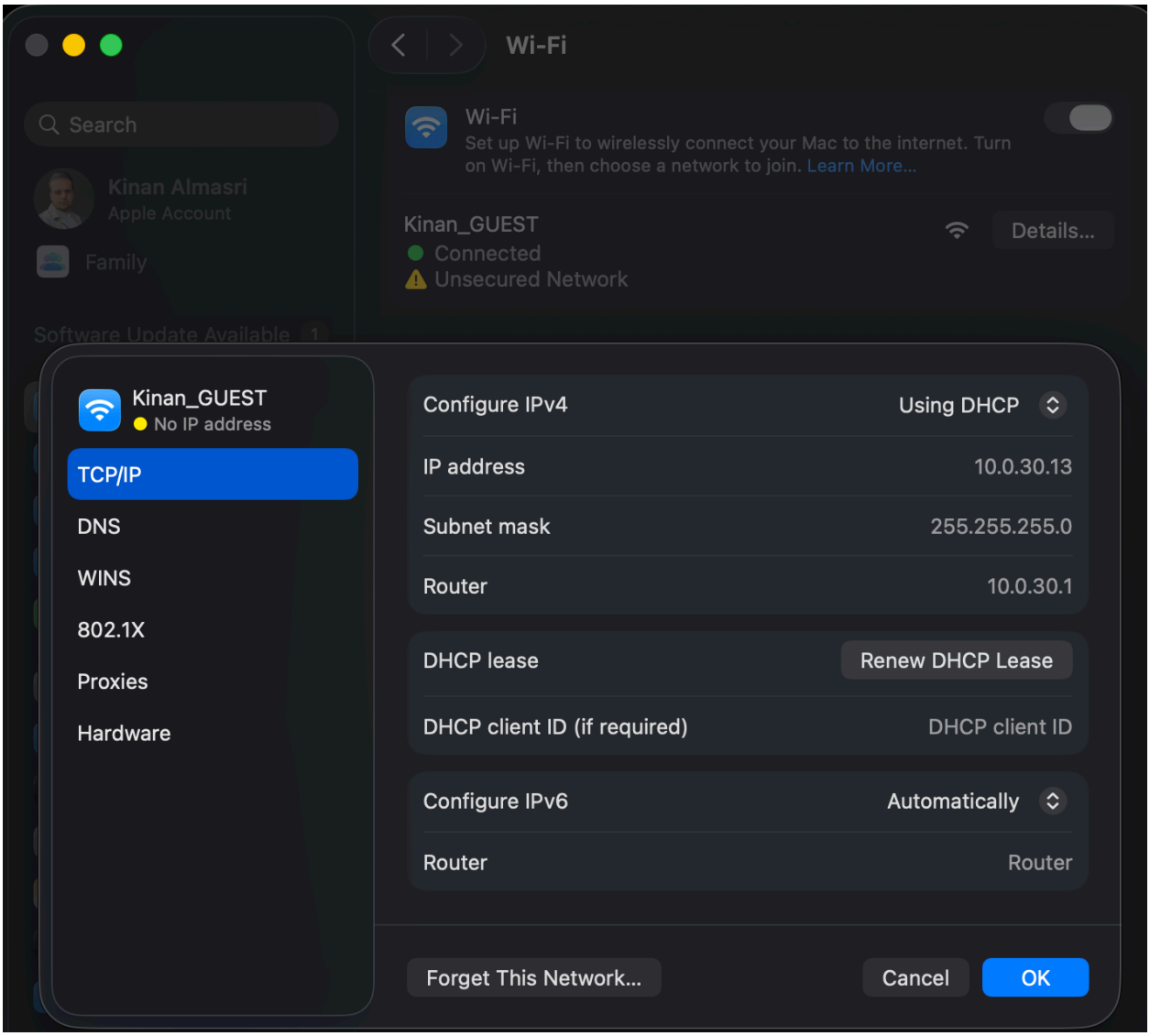


access the server form the outside



Access the trusted and guest network from the laptop


Wi-Fi
Search
Kinan Almasri
Apple Account
Family
Software Update Available
Wi-Fi
Set up Wi-Fi to wirelessly connect your Mac to the internet. Turn on Wi-Fi, then choose a network to join. Learn More...
Kinan_trusted
Connected
Details...
Kinan_trusted
No IP address
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Configure IPv4
Using DHCP
IP address
10.0.10.13
Subnet mask
255.255.255.0
Router
10.0.10.1
DHCP lease
Renew DHCP Lease
DHCP client ID (if required)
DHCP client ID
Configure IPv6
Automatically
Router
Router
Forget This Network...
Cancel
OK



Part 6

Today many websites like gambling, adult sites or even social media try to check the age of users to protect kids from bad content. some people think this is good. But other people say it is a problem because websites may ask for ID or passport,

and this is not safe for privacy. So the question is can we protect children online without taking people's personal data?

In the European Union there is a law called the Digital Services Act (DSA). This law says big online platforms must protect minors from harmful content [2]. Age checks are allowed, but they must also follow GDPR rules. That means websites cannot just take ID cards and keep them for no reason [2].

Some countries want stronger rules. In France, they want adult websites to verify age, and they work with CNIL (data protection authority) to do it in a way that doesn't show the person's identity [3]. In the UK, the online safety act also asks websites to check age, but many people worry about privacy.

There are privacy problems. The group EDRi says age verification can be dangerous if companies start collecting ID cards, face scans or other personal data [3]. They say the problem is not only age, but how the internet is designed. The European Data Protection Board (EDPB) says that if age checks are used, they must follow GDPR [4]. This means websites should only collect the minimum data, not keep it for a long time, and keep it safe [4]. They also say websites should not force people to give too much personal data just to prove age [4].

My opinion is what I think protecting children is important. But I don't think websites should collect or store ID cards or personal data because it can get hacked or misused. A better idea is to use systems like BankID, Freja eID or anonymous age tokens where the website only knows "this user is over 18" but does not know who the person is. age verification is possible, but it must be done carefully. It should protect children but also respect privacy, like the EU says.

References:

[1] N. I. Sarkar, M. M. Hassan, and M. N. Kabir, "*The Impact of Security Protocols on TCP/UDP Throughput in IEEE 802.11ax Client–Server Network*," **Electronics**, vol. 14, no. 19, p. 3890, 2025. Available: https://doi.org/10.3390/electronics14193890

[2] TechPolicy Press – *"What Europe's Digital Services Act Says About Age Assurance"*

https://www.techpolicy.press/what-europes-digital-services-act-says-about-age-assurance/

[3] European Digital Rights (EDRi) – *"Age verification gains traction: the EU risks failing to address the root causes of online harm"*

https://edri.org/our-work/age-verification-gains-traction-eu-risks-failing-to-address-the-root-causes-of-online-harm/

[4] European Data Protection Board (EDPB) – *"Statement 1/2025 on Age Assurance"*

https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf