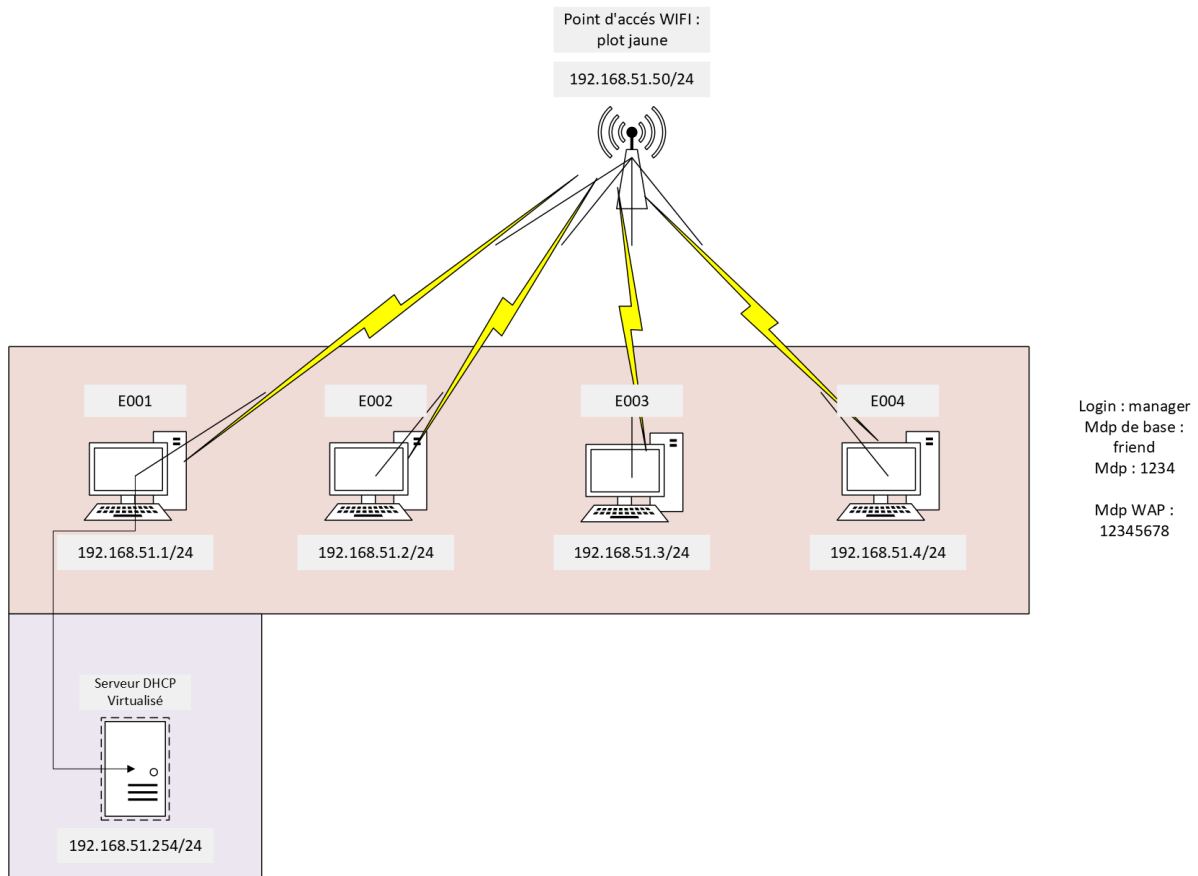


Mode opératoire
Mission KIWI

Pour nous:IP de base point accès wifi:192.168.1.230

Plan première étape:



CONTEXTE :

Vous attribuez l'adresse IP au point d'accès WIFI en vous référant au plan d'adressage fourni en annexe.

Vous vous assurez de la bonne communication au sein de l'infrastructure sans fil, pour cela vous désactivez les cartes filaires.

L'accès au point d'accès devra être sécurisé. Proposez une solution.

Changer IP pc pour qu'il soit dans le même réseau que le point d'accès

IP point d'accès WIFI : 192.168.1.230

I. Première étape:

A. Configuration du point accès wifi

Changer de mot de passe si nécessaire de l'interface admin changer le nom du wifi si besoin

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password	
New Password	
Confirm new password	
Network Name (SSID)	Radio Interface 1 plot jaune
	Radio Interface 2 plot jaune

*

Onglet : sécurité

Et changer le mode passe du wifi si nécessaire et mettre le mode:WPA Personnel

WPA personnel : Pour que ce soit sécurisé

☒ Broadcast SSID	☐ Station Isolation	☐ Deny communication between Radio 1 and Radio 2
Mode: WPA Personal		
WPA Versions: ☒ WPA		☒ WPA2
Cipher Suites: ☒ TKIP		☐ CCMP (AES)
Key: 12345678		

Dans l'onglet : Manage (juste cliquer dessus)

Dans l'idéal,il faudrait changer le paramétrage ip du point accès wifi en 192.168.51.50.Or ici on a laissé l'adresse de base.

Connection Type	Static IP ▼
Static IP Address	192 . 168 . 1 . 230
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 254
DNS Settings via DHCP	☐ On ☒ Off
DNS Nameservers	. . .
	. . .
DNS Domain	example.com

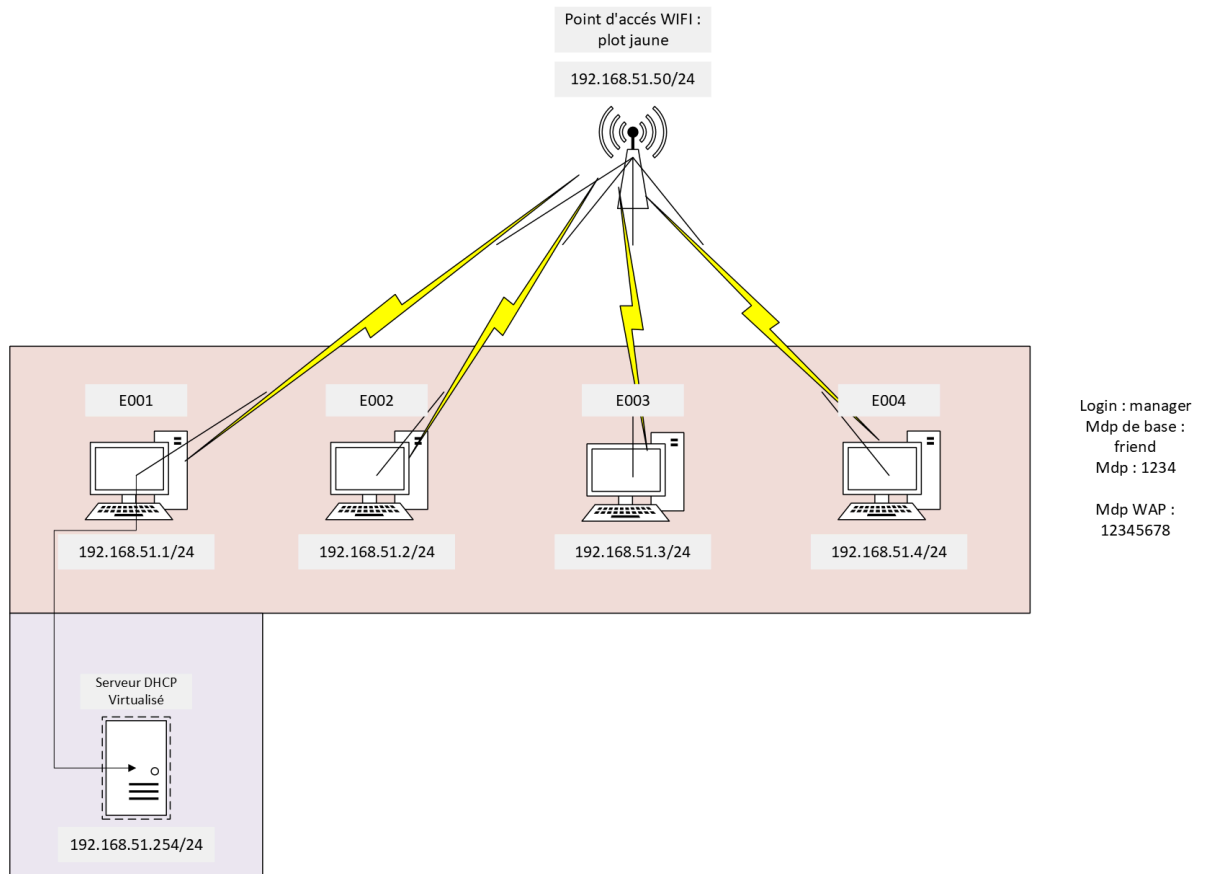
On peut maintenant brancher le point d'accès wifi sur le switch avec les autres ordinateurs !

Dans la logique après avoir fait cela **VOUS POUVEZ PLUS VOUS CONNECTER !**

Il faut se remettre dans le réseau : 192.168.51.0

Après toutes les étapes connecter tous les pc au point d'accès, une fois tous connectés faite des ping pour voir si cela fonctionne.

Plan deuxième étape:



Deuxième partie:

Partie 1.A:

identifiant vm dhcp:romaind

mot de passe: Password1

il va falloir ajouter sur un des postes du plot une machine virtuelle sous Ubuntu Server 20.04 LTS qui fera office de serveur DHCP. Il faut donc créer un serveur dhcp sur ubuntu

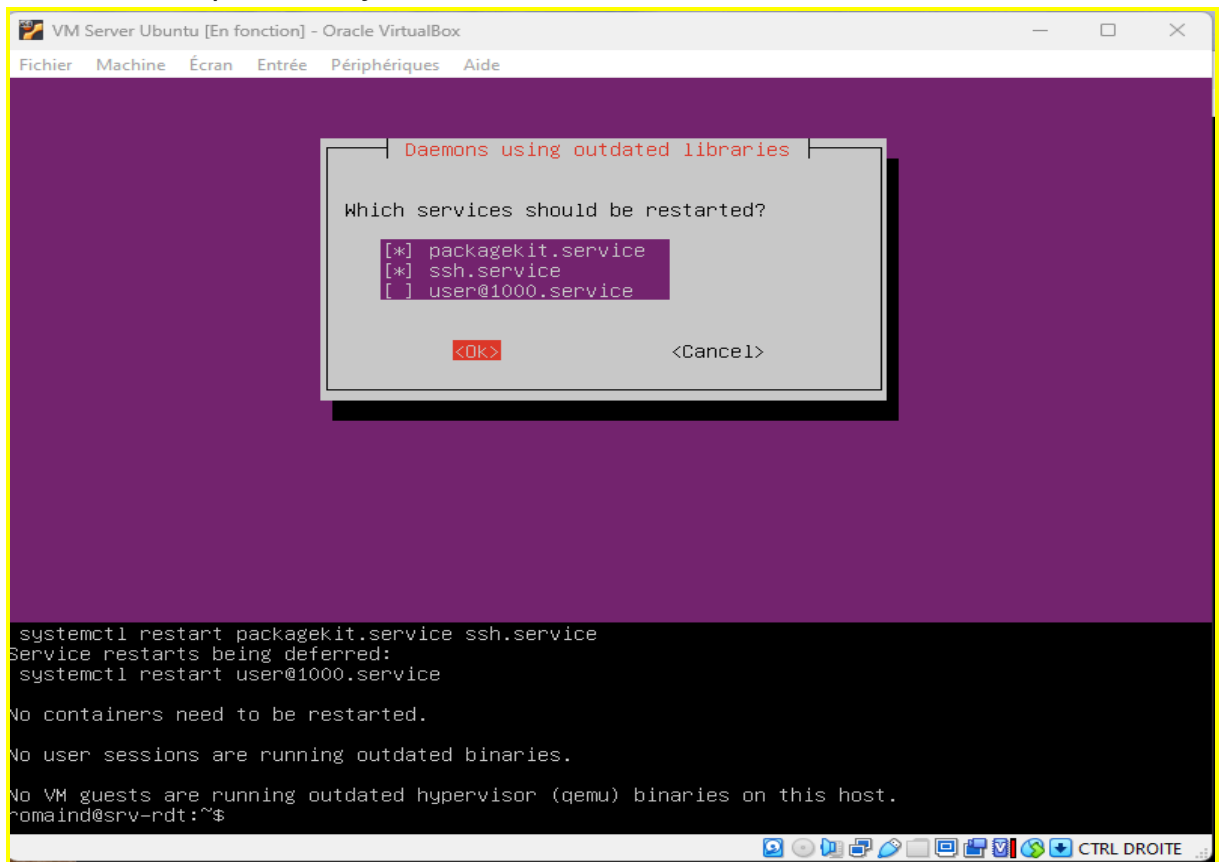
A. Préalable

Pour les besoins de la mission, nous allons avoir besoin de la VM Linux Server afin que cette dernière fasse des requêtes DHCP sur le serveur. Pour cela, nous allons créer un réseau virtuel sur lequel est connecté notre VM.

Sur virtualbox, il faut aller dans configuration de la VM Linux serveur

A. Configuration du serveur

1. Maintenant il faut installer le serveur DHCP via la commande : `sudo apt install isc-dhcp-server -y`



2. Maintenant il faut configurer le serveur DHCP pour lui indiquer quelles informations transmettre aux clients. Pour cela, il faut modifier le fichier `/etc/dhcp/dhcpd.conf`. On commencera par commenter les options DNS et décommenter "authoritative"

```
# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
```

3. Il faut aussi déclarer dans ce fichier la zone étendue

```
# Etendue LAN intnet
subnet 172.16.1.0 netmask 255.255.255.0 {
range 172.16.1.50 172.16.1.100;
}
```

en ajoutant en fin de fichier la zone étendu correspondant au réseau local avec une plage d'adresse allant de .20 à .50

4. Un fois le fichier sauvegardé, il faut relancer le service DHCP via la commande : *sudo systemctl restart isc-dhcp-server*

```
romaind@srv-rdt:~$ sudo systemctl restart isc-dhcp-server
romaind@srv-rdt:~$
```

`sudo systemctl restart isc-dhcp-server`: Pour redémarrer le serveur DHCP
`sudo systemctl status isc-dhcp-server`: donne le statut du serveur DHCP
c'est-à-dire si il est fonctionnel ou non.

Partie 1.B:

Accès par pont (Bridged Adapter)

La machine virtuelle se connecte directement au réseau local, comme s'il s'agissait d'un ordinateur physique.

Elle reçoit une adresse IP du réseau, comme ton PC hôte.

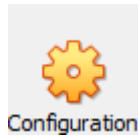
Elle peut accéder à Internet, communiquer avec le PC hôte, et échanger avec d'autres appareils (box, imprimantes, autres PC). Utilisé quand la VM doit être visible et accessible sur le réseau local.

Accès interne (Internal Network)

La VM est isolée du réseau physique et du PC hôte.

Elle ne peut pas accéder à Internet ni aux autres appareils du réseau.

Elle peut uniquement communiquer avec d'autres VM configurées sur le même nom de réseau interne. Utilisé pour créer un réseau privé entre VM, sans contact avec l'extérieur.



et il faut choisir la partie Réseau, ajouter activer la première interface(adapter 1) si pas déjà activé et choisir le mode d'accès réseau "accès pour pont"

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

☒ Activer l'interface réseau

Mode d'accès réseau : Accès par pont

Name: Realtek PCIe 2.5GbE Family Controller

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 080027D0C5F1

☒ Câble branché

désactiver la deuxième interface(adapter2) réseau

server DHCP - Settings

Basic Expert

Général
System
Affichage
Stockage
Audio
Réseau
Ports séries
USB
Shared Folders
Interface utilisateur

Search settings

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

☐ Activer l'interface réseau

Mode d'accès réseau : Réseau interne

Name: intnet

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 080027C6AB2E

☒ Câble branché

Ports séries

Port 1 Port 2 Port 3 Port 4

☐ Activer le port série

OK Annuler Aide

Ensuite lancer le serveur DHCP et vérifier les adresses ip associées aux interfaces avec la commande `ip a` normalement il devrait pas avoir d'adresse pour l'interface or ici c'est le résultat après la configuration du dhcp

```
Last login: Tue Apr  1 12:09:16 UTC 2025 on tty1
romaind@srv-rdt:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d0:c5:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.51/24 brd 192.168.51.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed0:c5f1/64 scope link
        valid_lft forever preferred_lft forever
romaind@srv-rdt:~$ _
```

Toujours dans l'hypothèse où la configuration du dhcp n'a pas été changé, il faut attribuer une adresse ip à l'interface pour l'accès par pont en faisant la commande `sudo nano /etc/netplan/00-installer-config.yaml`

Il faut donc lister tous les fichiers dans `/etc/netplan/` via la commande :
`ls /etc/netplan`

```
link/ether 08:00:27:e1:0f:e3 brd ff:ff:ff:ff:ff:ff
romaind@srv-rdt:~$ ls /etc/netplan
00-installer-config.yaml
romaind@srv-rdt:~$
```

Editer le fichier yaml avec nano

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: false
      dhcp6: false
      addresses: [192.168.51.51/24]
  version: 2
```

et affecter à l'interface l'adresse ip 192.168.51.51/24 (voir exemple ci-dessus, attention à bien mettre le nom des interfaces correspondant à votre VM)

Maintenant, il faut appliquer les changements avec la commande : *sudo netplan apply* et vérifier que les changements ont bien été pris en compte avec la commande *ip a*.

5. Pour vérifier que le DHCP fonctionne correctement, se connecter en filaire sur un autre PC windows, ouvrir le cmd :

```
ip /renew  
ipconfig /all
```

Si ça fonctionne, une IP dans la plage indiquée sera attribuée automatiquement.

6. Il faut ensuite configurer le serveur DHCP en lui indiquant depuis quelle interface réseau seront prises en compte les requêtes DHCP. Pour cela, il faut éditer le fichier `isc-dhcp-server`

```
# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?  
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".  
INTERFACESv4="enp0s8 "  
#INTERFACESv6=""
```

via la commande *sudo nano /etc/default/isc-dhcp-server* et indiquer pour l'interface v4(enp0s3) le nom de l'interface et en mettant en commentaire (#) l'interface v6.

METTRE L'INTERFACE SUR LAQUELLE ON A CONFIG @IP

Partie 2:

CONTEXTE :

Vous devez ajouter sur un des postes du plot une machine virtuelle sous Ubuntu Server 20.04 LTS qui fera office de serveur DHCP et qui attribuera les adresses comme précédemment expliqué.

L'adresse IP du serveur est définie dans le plan d'adressage fourni en annexe. Attention la machine virtuelle sera sur le poste physique dans la partition Données.

Les sauvegardes pourront être réalisées sur les disques durs externes.

Pour chaque poste il faut définir deux réservations :

- une réservation en liant l'adresse IP et l'adresse MAC de la carte réseau filaire et
- une réservation en liant l'adresse IP et l'adresse MAC de la carte réseau WIFI.

Vous vérifierez que lors du passage en adressage dynamique, la configuration obtenue est correcte.

Chaque poste doit être testé sur sa partie filaire et WIFI.

Pour recup @MAC : `ipconfig /all`

Attribuer adresse physique a une @IP via le DHCP :

Adresse physique = @MAC

Dans un premier temps établir un tableau des carte réseau de notre réseau :

Ordinateur	Carte réseau concerné	IP Attribué	Adresse MAC
PC 1	Ethernet 01 (E001)	192.168.51.20	D8-BB-C1-05-1A-B0
PC 2	Ethernet 01 (E002)	192.168.51.21	D8-BB-C1-15-91-62
PC 3	Ethernet 01 (E003)	192.168.51.22	D8-BB-C1-15-89-0A
PC 4	Ethernet 01 (E004)	192.168.51.23	D8-BB-C1-15-8F-39
PC 1	Wi-Fi	192.168.51.24	70-9C-D1-3F-16-91
PC 2	Wi-Fi	192.168.51.25	B4-0E-DE-71-F1-38
PC 3	Wi-Fi	192.168.51.26	84-1B-77-FF-7C-60
PC 4	Wi-Fi	192.168.51.27	B4-0E-DE-FD-CD-C5
@ Libre		192.168.51.28	
@ Libre		192.168.51.29	

Une fois fait allez sur le linux server, puis allez sur ce fichier de configuration
/etc/dhcp/dhcpd.conf :

Entrer chaque ligne pour chaque PC et carte réseau :

```
host pc_nom_que_l'on-souhaite {
    hardware ethernet 08:00:27:12:34:56;
    fixed-address 192.168.1.50;
}
```

Ensuite redémarrer le DHCP :

```
sudo systemctl restart isc-dhcp-server
```

Si des clients (host) sont connectés au réseau reset toutes les IP attribuée (renouvellement de bail) :

```
sudo dhclient
```

Schéma à respecter :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.150;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8;
```

Pour Partie Filaire:

```
host pc1-ETH {
    hardware ethernet 08:00:27:aa:bb:cc;
    fixed-address 192.168.1.10;
}
```

Pour partie wifi:

```
host PC1-WIFI {
    hardware ethernet b8:27:eb:11:22:33;
    fixed-address 192.168.1.11;
}
}
```

Faire les tests en **DÉSACTIVANT TOUTE INTERFACES** non utilisées (seulement Ethernet 1 ou Ethernet Ethernet et Wifi) dans le panneau de configuration.

Vérifier en faisant : `ipconfig /renew`

Puis : `ipconfig`

Une fois fais cela fais vérifier que l'ip attribuer et bien celle qui a été entrer dans la configuration pour cette @MAC

Vérifier la syntax en cas d'erreur:`sudo dhcpcd -t`

`sudo dhcpcd -t -cf /etc/dhcp/dhcpcd.conf`