

Euromed University of Fes
School of Digital Engineering and Artificial Intelligence



Rapport des travaux pratiques
Architecture Des Réseaux

Mentagui Adam

Superviseur :

Pr. Amamou Ahmed

Date de soumission : 31/10/2024

1 Introduction

L'architecture du réseau est essentiellement la manière dont il a été conçu et assemblé pour permettre à différents appareils de communiquer entre eux. Cela repose sur des modèles qui expliquent comment les données sont envoyées et reçues. Les éléments majeurs d'un réseau comprennent les routeurs, qui dirigent le trafic, les switches qui connectent les appareils, et les serveurs, qui fournissent divers services.

2 Le routage

1. Les adresses IP - Différentes classes :

Une adresse IP est l'abréviation de Internet Protocol, c'est un numéro d'identification donné à chaque appareil qui se connecte à un réseau. Elles permettent essentiellement aux appareils de communiquer entre eux sur Internet. Le format de l'IPv4 est de 32 bits, et elles sont exprimées sous la forme de quatre octets séparés par des points, par exemple : 192.168.1.1.

La classe A comprend des adresses allant de 1.0.0.0 à 126.255.255.255. Elles sont utilisées pour des réseaux très grands. La classe B se situe entre 128.0.0.0 et 191.255.255.255, et elle est destinée aux réseaux de taille moyenne. De plus, la plage des réseaux de classe C se situe entre l'adresse 192.0.0.0 et 223.255.255.255, et elle est utilisée pour des réseaux plus petits.

Les adresses de classe D sont utilisées pour le multicast et vont de 224.0.0.0 à 239.255.255.255, tandis que les adresses de classe E vont de 240.0.0.0 à 255.255.255.255 et sont réservées pour des recherches expérimentales.

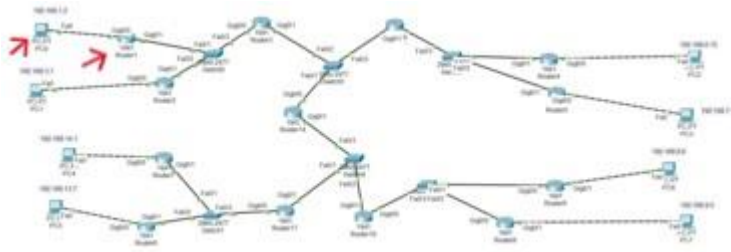
2. L'objectif des adresses IP :

Les adresses IP sont utilisées pour catégoriser et gérer les réseaux. Cette classification en catégories permettra ensuite d'optimiser en fonction de la taille des réseaux ainsi que de leurs besoins. Elles jouent aussi un rôle majeur dans l'administration de la sécurité sur les réseaux, car elles sont capables d'identifier et de suivre un appareil connecté afin de mettre en place des mesures de sécurité.

3 Les types de routage :

• Routage Statique :

L'image ci-dessous représente l'architecture de 4 bâtiments similaires, dont chaque bâtiment contient deux routeurs et deux ordinateurs connectés respectivement. Les deux routeurs sont connectés à un autre routeur grâce à un switch, afin d'assurer la communication entre les 4 bâtiments.



Les commandes :

L'exemple montre les commandes utilisées pour la configuration de l'ordinateur 0 connecté avec le routeur R0 : (ils sont désignés par une flèche rouge ci-dessus)

On affecte l'IP 192.168.1.2 avec le masque 255.255.255.0 et comme passerelle (gateway) 192.168.1.1 à PC0 sur son panneau de configuration.

PC0

Physical Config Desktop Programming Attributes

GLOBAL	Global Settings
Settings	
Algorithm Settings	
INTERFACE	
FastEthernet0	
Bluetooth	

Display Name PC0

Interfaces FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 192.168.1.1

DNS Server

Physical Config Desktop Programming Attributes

GLOBAL	FastEthernet0
Settings	
Algorithm Settings	
INTERFACE	
FastEthernet0	
Bluetooth	

Port Status

Bandwidth

Duplex

MAC Address 0001.C7A9.896E

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Pour le routeur ; on sélectionne sa fenêtre CLI et on tape les commandes suivantes : enable config t interface Gig0/1 ip address 192.168.1.1 255.255.255.0 no shutdown
exit interface Gig0/0 ip address 192.168.2.1 255.255.255.0 no shutdown
exit **configuration des routes du R0 :**

ip route 192.168.3.0 255.255.255.0 192.168.2.2
(il faut ajouter tout les routes disponibles sur l'architecture (voir tableau routage ci-dessous))

Pour s'assurer, apr`es avoir entrer les commandes ci-dessus, vous devriez obtenir les resultats suivants :

Physical

Config

CLI

Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/0

Port Status

Bandwidth

Duplex

MAC Address

IP Configuration

IPv4 Address

Subnet Mask

Tx Ring Limit

1000 Mbps

0001.9791.3C01

192.168.1.1

255.255.255.0

10

Physical

Config

CLI

Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Network

Mask

Next Hop

Network Address

192.168.3.0/24 via 192.168.2.4

192.168.4.0/24 via 192.168.2.3

192.168.5.0/24 via 192.168.2.3

192.168.6.0/24 via 192.168.2.3

192.168.7.0/24 via 192.168.2.3

192.168.11.0/24 via 192.168.2.3

192.168.12.0/24 via 192.168.2.3

Table de routage du routeur 0:

Destination	Net mask	Gateway	Interface
192.168.3.0	255.255.255.0	192.168.2.4	192.168.2.2
192.168.4.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.5.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.6.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.7.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.11.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.12.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.14.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.13.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.10.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.8.0	255.255.255.0	192.168.2.3	192.168.2.2
192.168.9.0	255.255.255.0	192.168.2.3	192.168.2.2

Avantage du routage statique :

Le routage statique permet une configuration simple et prévisible, il permet un contrôle total sur le chemin des données dans un réseau.

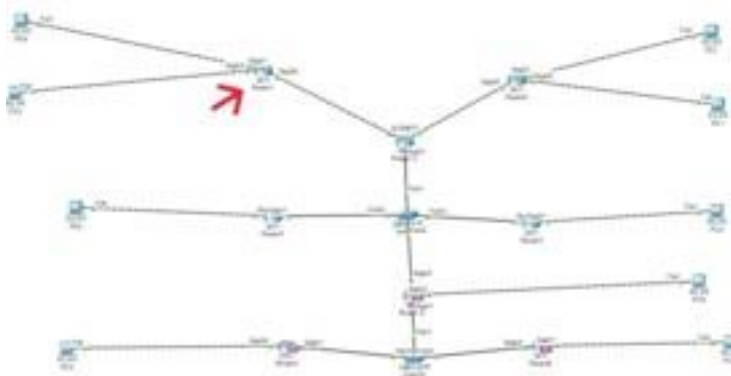
Inconvénient du routage statique :

Le routage statique nécessite une configuration manuelle, ce qui le rend peu flexible et difficile à maintenir dans des environnements réseau dynamiques.

• Routage dynamique:

1. Le protocole RIP :

l'image ci-dessous représente une architecture qui utilise le protocole RIP, afin d'assurer la communication entre ses ordinateurs.



Les commandes :

L'exemple montre les commandes utilisées pour la configuration du routeur R0 désigné par une flèche rouge ci-dessus. (On garde la même adresse IP et le gateway de l'ordinateur qu'auparavant)

Pour le routeur ; on sélectionne sa fenetre CLI et on tape les commandes suivantes : enable config t interface Gig0/1 ip address 192.168.1.1 255.255.255.0 no shutdown
exit interface Gig0/0 ip address 192.168.2.1 255.255.255.0 no shutdown

exit **configuration des routes du R0**

:

R0(config)router rip

R0(config-router)version 2

R0(config-router)no auto-summary

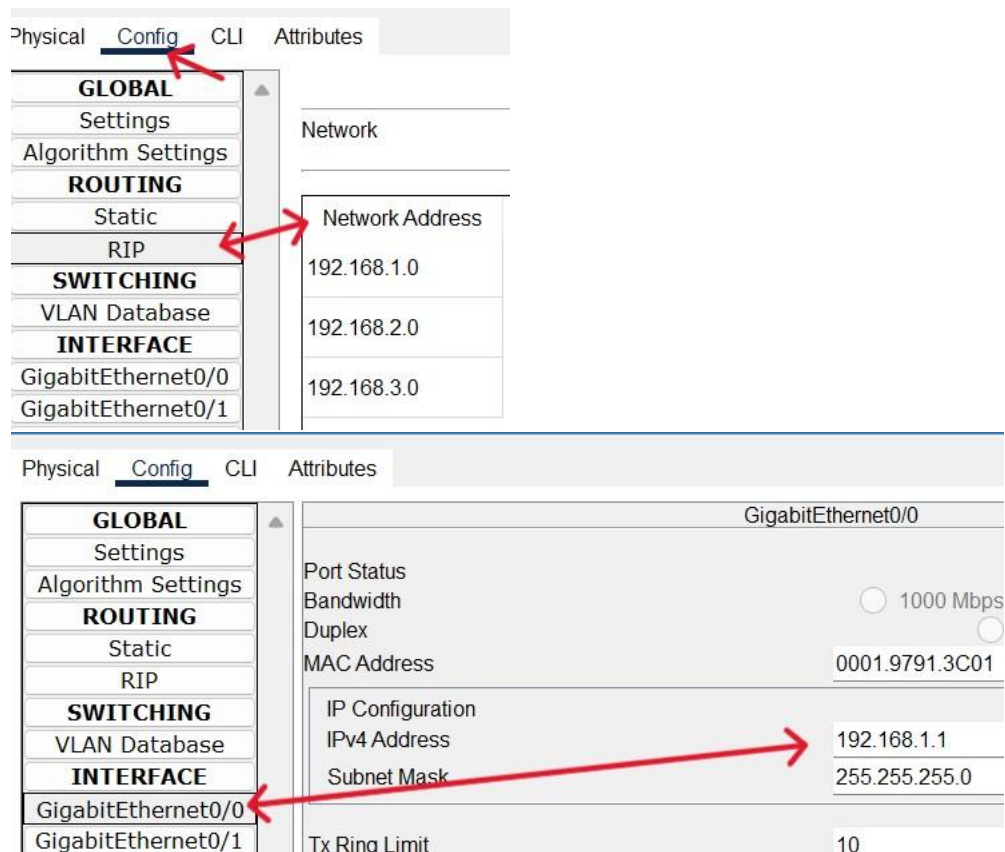
R0(config-router)network 10.0.0.0

R0(config-router)network 192.168.1.0

R0(config-router)network 192.168.2.0

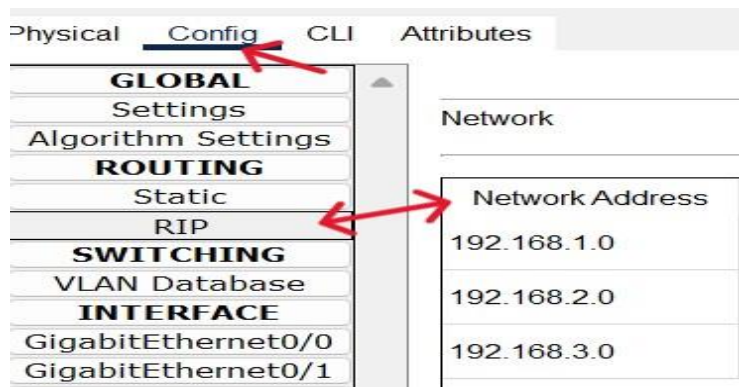
(il faut ajouter toutes les routes disponibles qui sont conec'tées directement avec le routeur sur l'architecture)

Pour s'assurer, apr`es avoir entrer les commandes ci-dessus, vous devriez obtenir les resultats suivants :



2. Le protocol OSPF :

L'image ci-dessous représente une architecture qui utilise le Protocol OSPF, afin d'assurer la communication entre ses ordinateurs.



Les commandes :

L'exemple montre les commandes utilisées pour la configuration du routeur R0 désigné par une flèche rouge ci-dessus. (On garde la même adresse IP et le gateway de l'ordinateur qu'auparavant)

Pour le routeur ; on sélectionne sa fenêtre CLI et on tape les commandes suivantes : enable config t interface Gig0/1 ip address 192.168.1.1 255.255.255.0 no shutdown

exit interface Gig0/0 ip address
192.168.2.1 255.255.255.0
no shutdown

exit **configuration des routes du R0 et sa zone :**

R0(config)#router ospf 100
R0(config-router)#network 192.168.2.1 0.0.0.255 area 0

(il faut ajouter toutes les routes disponibles qui sont connectées directement avec le routeur sur l'architecture)

Avantage du routage dynamique :

Le routage dynamique s'adapte automatiquement aux changements du réseau, et simplifie la gestion et l'amélioration de la réactivité aux pannes.

Inconvénient du routage dynamique :

Le routage dynamique peut consommer plus de ressources réseau et introduire une latence en raison du calcul des routes.

4. Configuration de réseau à travers Linux (Ubuntu)

Dans ce moment-là, on a découvert juste la méthode de DHCP, une entre client et serveur et l'autre avec relais en suivant ces étapes :

DHCP SERVEUR

Installation des packages :

On utilise la commande : « sudo apt install isc-dhcp-server ».

```
~$ sudo apt install isc-dhcp-server
```

Note : L'image ne correspond pas les autres images, just un exemple de l'exécution car j'ai perdu l'image.

On installe le fichier « net-tools » pour utiliser quelques commandes :

```
adam4@ubuntu:~$ sudo apt install net-tools
```

Editer le fichier /etc/default/isc-dhcp-server :

Après, on remarque que l'interface ens33 a été créée après l'utilisation la commande « ifconfig ».

```
.
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
adam4@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.170.154 netmask 255.255.255.0 broadcast 192.168.170.255
    inet6 fe80::915d:5889:160e:40a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:59:5c:31 txqueuelen 1000 (Ethernet)
    RX packets 2935 bytes 3428876 (3.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 651 bytes 71630 (71.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 231 bytes 23092 (23.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 231 bytes 23092 (23.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

On doit entrer le fichier de dhcp et mettre cette interface « ens33 » comme l'interface de V4 pour dhcp.

La commande : `sudo nano /etc/default/isc-dhcp-server` (si tu n'es pas le root).

```
root@ubuntu:/home/adam1/Desktop# nano /etc/default/isc-dhcp-server
root@ubuntu:/home/adam1/Desktop#
```

Vous devez voir le fichier, donc écrivez le nom de l'interface (ens33) dans la section « INTERFACEV4 ».

INTERFACEV4 = "ens33"

```
GNU nano 4.8 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDV4_CONF=/etc/dhcp/dhcpd.conf
DHCPDV6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPDV4_PID=/var/run/dhcpd.pid
DHCPDV6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACEV4="ens33"
INTERFACEV6=""
```

Ctrl+X pour sauvegarder, après la confirmation tapez sur Entrée dans votre clavier.

Addition des subnets :

Après la modification vous devez retourner au terminal et tapez la commande suivante :

`Sudo nano /etc/dhcp/dhcpd.conf` (si tu n'es pas le root).


```
root@ubuntu:/home/adam1/Desktop# nano /etc/dhcp/dhcpd.conf
root@ubuntu:/home/adam1/Desktop#
```

Modifier le domaine et supprimer la phrase qui est près le nom de domaine :

Option `domain-name` "example.org"

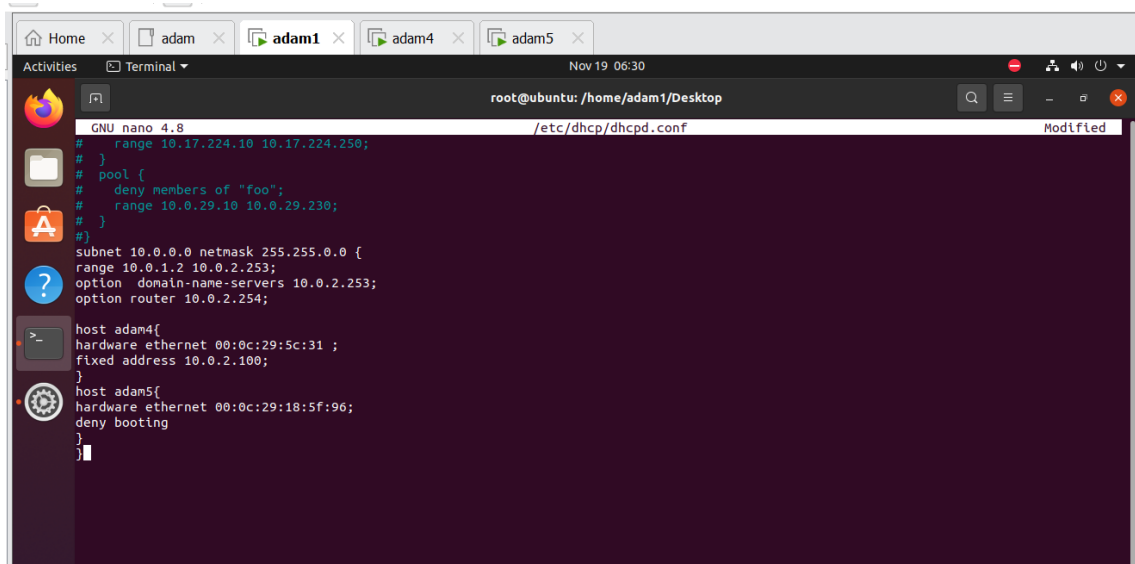
Supprimer la ligne qui est après la commande.

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



Note: J'ai oublié de prendre une capture de la modification.

Dans cette manipulation, nous allons ajouter deux clients : adam5 et adam4. Le premier sera le client banni de ce serveur et l'autre non. Le subnet qu'on a choisi est 10.0.0.0, DNS 10.0.2.253, gateway 10.0.2.254 et la destination 10.0.2.100.



The screenshot shows a terminal window with the nano text editor open, editing the file /etc/dhcp/dhcpd.conf. The configuration includes a pool, a subnet 10.0.0.0 with netmask 255.255.0.0, and two hosts: adam4 and adam5. Host adam4 is configured with a fixed address 10.0.2.100 and is not denied booting. Host adam5 is configured with a fixed address 10.0.2.100 and is denied booting. The terminal window has tabs for 'adam1', 'adam4', and 'adam5'.

```
GNU nano 4.8 /etc/dhcp/dhcpd.conf Modified
# range 10.17.224.10 10.17.224.250;
# }
# pool {
#   deny members of "foo";
#   range 10.0.29.10 10.0.29.230;
# }
#
subnet 10.0.0.0 netmask 255.255.0.0 {
  range 10.0.1.2 10.0.2.253;
  option domain-name-servers 10.0.2.253;
  option router 10.0.2.254;
}

host adam4{
  hardware ethernet 00:0c:29:5c:31 ;
  fixed address 10.0.2.100;
}

host adam5{
  hardware ethernet 00:0c:29:18:5f:96;
  deny booting
}
```

Ctrl+X pour sauvegarder, après la confirmation tapez sur Entrée dans votre clavier.

Configuration de le connexion et le type de réseau :

Premièrement, on part au paramètre de la machine et on ajoute les mêmes adresses qu'on a dans le subnet .

Cancel **Wired** Apply

Details Identity **IPv4** IPv6 Security

IPv4 Method

☐ Automatic (DHCP) ☐ Link-Local Only

☒ Manual ☐ Disable

☐ Shared to other computers

Addresses

Address	Netmask	Gateway	
10.0.2.100	255.255.0.0	10.0.2.254	

DNS Automatic ☒

10.0.2.253

Separate IP addresses with commas

On clique sur « apply » pour sauvegarder la modification et on met le type de machine en custom (VMnet0 ou n'importe).

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD 2 (SATA)	Using file C:\Users\cyber\Dow...
CD/DVD (SATA)	Using file autoinst.iso
Floppy	Using file autoinst.flp
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☒ Connected

☒ Connect at power on

Network connection

☐ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

☐ NAT: Used to share the host's IP address

☐ Host-only: A private network shared with the host

☒ Custom: Specific virtual network

VMnet0

☐ LAN segment:

LAN Segments... Advanced...

On clique sur Ok pour sauvegarder les modifications.

Vérification :

Après la terminaison de toutes les étapes, on va
Utiliser ces deux commandes :

```
root@ubuntu:/home/adam1/Desktop# systemctl restart isc-dhcp-server
root@ubuntu:/home/adam1/Desktop# systemctl status isc-dhcp-server
```

- « `systemctl restart isc-dhcp-server` » : Pour
redémarrer et mise à jour le serveur dhcp.
- “`systemctl status isc-dhcp-server`” : Pour voir le
statue de serveur DHCP .

Voilà le bon résultat que si le serveur dhcp marche :

```
root@ubuntu:/home/adam1/Desktop# nano /etc/dhcp/dhcpd.conf
root@ubuntu:/home/adam1/Desktop# systemctl restart isc-dhcp-server
root@ubuntu:/home/adam1/Desktop# systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-11-19 06:51:55 PST; 3s ago
     Docs: man:dhcpd(8)
  Main PID: 108753 (dhcpd)
    Tasks: 4 (limit: 4541)
   Memory: 4.8M
   CGroup: /system.slice/isc-dhcp-server.service
           └─108753 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf ens33

Nov 19 06:51:55 ubuntu sh[108753]: Wrote 0 leases to leases file.
Nov 19 06:51:55 ubuntu dhcpd[108753]: Wrote 0 new dynamic host decls to leases file.
Nov 19 06:51:55 ubuntu dhcpd[108753]: Wrote 0 leases to leases file.
Nov 19 06:51:55 ubuntu dhcpd[108753]: Listening on LPF/ens33/00:0c:29:ac:9b:37/10.0.0.0/16
Nov 19 06:51:55 ubuntu sh[108753]: Listening on LPF/ens33/00:0c:29:ac:9b:37/10.0.0.0/16
Nov 19 06:51:55 ubuntu dhcpd[108753]: Sending on LPF/ens33/00:0c:29:ac:9b:37/10.0.0.0/16
Nov 19 06:51:55 ubuntu sh[108753]: Sending on LPF/ens33/00:0c:29:ac:9b:37/10.0.0.0/16
Nov 19 06:51:55 ubuntu dhcpd[108753]: Sending on Socket/fallback/fallback-net
Nov 19 06:51:55 ubuntu sh[108753]: Sending on Socket/fallback/fallback-net
Nov 19 06:51:55 ubuntu dhcpd[108753]: Server starting service.
root@ubuntu:/home/adam1/Desktop#
```

Le cas de deux subnet :

Si on a deux subnets dans le fichier
/etc/dhcp/dhcpd.conf, donc il sera compliqué de
configurer le serveur dhcp .Alors on n'est obligé de
faire une route entre le premier subnet et le
deuxième , voici la commande qu'on doit le faire :

- **Route add -net @adresse 2ème
subnet/classe gw @adresse gateway de
1^{er} subnet**

Note : J'ai perdu la capture de cette commande.

Pour la vérification on fait route -n.

```
root@ubuntu:/home/a# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.1.254  0.0.0.0         UG    20100 0      0 ens33
169.254.0.0    0.0.0.0        255.255.0.0     U     1000 0      0 ens33
192.168.1.0    0.0.0.0        255.255.255.0   U     100 0      0 ens33
192.168.2.0    192.168.1.254 255.255.255.0   UG    0 0      0 ens33
```

Le deuxième subnet que j'ai posé est 192.168.2.0, et
le premier est 192.168.1.0.

RELAIS

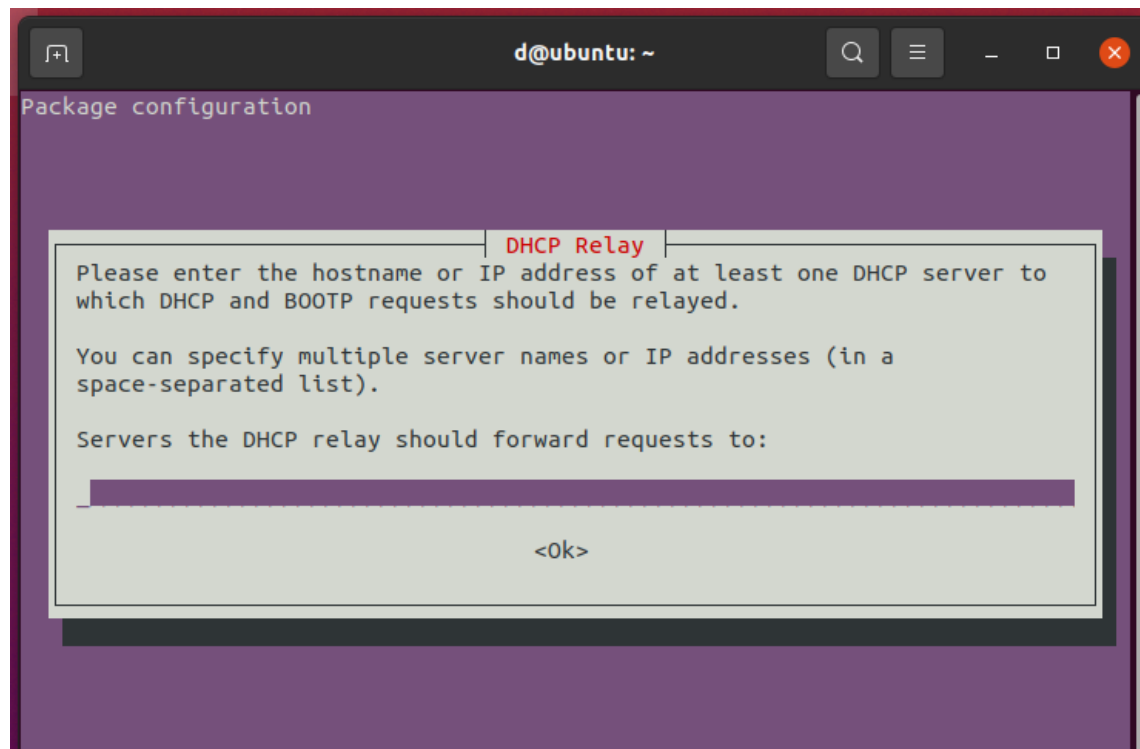
Le relais est l'intermédiaire entre le serveur client et le serveur DHCP, il est le responsable pour gérer la communication entre ces deux entités, maintenant on explique les étapes pour manipuler le relais.

Installation de package :

On utilise la commande : « sudo apt install isc-dhcp-relay ».

```
~$ sudo apt install isc-dhcp-relay
```

Après vous allez avoir cette fenêtre :



Vous allez entrer le gateway de serveur DHCP , pour l'écouter les deux interfaces et ne mettez rien dans les options .

On installe le fichier « net-tools » pour utiliser quelques commandes :

```
adam4@ubuntu:~$ sudo apt install net-tools
```

Editer le fichier /etc/default/isc-dhcp-relay :

Donc on doit créer deux network adapters (paramètre de la machine -> Add -> Network adapter) Une doit avoir le même interface que client et l'autre que serveur DHCP . Sachant que le réseau des deux interfaces sont mêmes réseaux qui relient avec eux.

Vous devez avoir ça en utilisant « ifconfig » commande :

```
d@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.40 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::e4f4:cc0b:da36:d58f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:39:4f:00 txqueuelen 1000 (Ethernet)
    RX packets 1779639 bytes 516252803 (516.2 MB)
    RX errors 0 dropped 7414 overruns 0 frame 0
    TX packets 38765 bytes 10540738 (10.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::84a5:eef9:d97c:28a5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:39:4f:0a txqueuelen 1000 (Ethernet)
    RX packets 187 bytes 23017 (23.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3541 bytes 301723 (301.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Malheureusement puisqu'on n'a pas les captures à cause du temps, ens33 est connecté avec serveur dhcp et l'autre avec client.

Vous allez après entrer cette commande : sudo nano /etc/default/isc-dhcp-relay

```
$ sudo nano /etc/default/isc-dhc-relay
```

Ajoute les deux interfaces :

```
INTERFACES="ens33 ens37 "
```

Et après ajoute le serveur de dhcp « dans mon est 192.168.1.0 »

```
SERVERS="192.168.1.0"
```

Ctrl+X pour sauvegarder, après la confirmation tapez sur Entrée dans votre clavier.

Configuration :

Pour configurer relay il faut entrer cette commande :
« sudo nano /etc/sysctl.conf »

```
~$ sudo nano /etc/sysctl.conf
```

Après avoir le fichier, vous devez sélectionner
« net.ipv4.ip_forward=1 » par supprimer le « # ».

Ctrl+X pour sauvegarder, après la confirmation tapez
sur Entrée dans votre clavier.

Utilise la commande « sysctl -p /etc/.conf » dans le
terminal pour afficher la ligne qui est décommenté.

Vérification :

Après la terminaison de toutes les étapes, vous devez
entrer ces deux commandes :

```
d@ubuntu:~$ systemctl restart isc-dhcp-relay
d@ubuntu:~$ systemctl status isc-dhcp-relay
```

- « systemctl restart isc-dhcp-relay » : Pour redémarrer et mise à jour le relay.
- « systemctl status isc-dhcp-relay » : Pour voir le statue de relay .

Voilà le bon résultat que si le relay marche :

```
d@ubuntu:~$ systemctl restart isc-dhcp-relay
d@ubuntu:~$ systemctl status isc-dhcp-relay
● isc-dhcp-relay.service - ISC DHCP IPv4 relay
   Loaded: loaded (/lib/systemd/system/isc-dhcp-relay.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-11-21 03:23:18 PST; 3s ago
     Docs: man:dhcrelay(8)
    Main PID: 7114 (dhcrelay)
      Tasks: 4 (limit: 4541)
    Memory: 1.5M
    CGroup: /system.slice/isc-dhcp-relay.service
            └─7114 /usr/sbin/dhcrelay -d -4 -i ens33 -i ens37 192.168.1.1
```

Connections entre serveur et client :

Il faut maintenant assurer que l'interface ens37 qui est relié avec client par exemple ont les mêmes les type de VMnet (VMnet2 pour mon cas) et que les toutes machines sont custom. Après assurer ça vous va entrer cette commande (par exemple on fait pour le client).

- Route add -net @réseau de dhcp server / classe gw @adresse de l'interface de relay

- qui appartient le même réseau que le client.
(Faire la route de client vers serveur dhcp).
- Route add -net @adresse de l'interface de relay qui appartient le même réseau que le client / classe gw 0.0.0.0. (Faire la route de client vers l'interface de relay).

Même chose avec serveur DHCP .

5 Conclusion

Ce rapport a exploré les principes fondamentaux du routage et de la gestion des réseaux, notamment en configurant un serveur DHCP sous Linux. Nous avons abordé les types de routage, comme le routage statique et dynamique, et leur impact sur la gestion des réseaux. L'installation et la configuration d'un serveur DHCP ont permis d'automatiser l'attribution d'adresses IP, tandis que la mise en place d'un relais DHCP a facilité la communication entre différents subnets. Ces travaux ont démontré l'importance de maîtriser ces outils pour optimiser la gestion des réseaux et garantir leur bon fonctionnement.