# PROJET PROFESSIONNEL ENCADRE

## Mise en place d'un serveur DHCP et DNS

avec Failover et Filtrage MAC sous Debian 12

| | |
|---|---|
| **Candidat** | Fossey Florent |
| **Formation** | BTS SIO — Option SISR (2eme annee) |
| **Etablissement** | IRIS Mediaschool Rouen |
| **Annee scolaire** | 2025 / 2026 |
| **Domaine utilise** | florent.local |
| **Environnement** | VMware Workstation Pro — Debian 12 Bookworm |

# Sommaire

# 1. Introduction

## Contexte du projet

Dans le cadre de ma deuxieme annee de BTS SIO option SISR, j'ai realise ce Projet Professionnel Encadre portant sur le deploiement de services reseau essentiels en entreprise. L'objectif etait de mettre en place une infrastructure reseau complete dans un environnement virtualise, en simulant des conditions proches de la realite professionnelle.

Ce projet m'a permis d'aborder concretement des notions fondamentales : administration d'un serveur Linux sans interface graphique, configuration de services reseau, haute disponibilite et securisation des acces reseau par filtrage d'adresses MAC.

## Objectifs

### Objectifs techniques

- Installer et configurer Debian 12 en environnement serveur (sans interface graphique)
- Deployer un serveur DNS avec Bind9 pour la resolution de noms locale
- Mettre en place un serveur DHCP avec attribution automatique des adresses IP
- Configurer un mecanisme de failover DHCP pour garantir la haute disponibilite
- Securiser le reseau par filtrage des adresses MAC (directive deny unknown-clients)
- Valider l'ensemble par des tests sur un poste client Windows 11

### Objectifs pedagogiques

- Approfondir mes connaissances en administration systeme Linux
- Comprendre en profondeur les protocoles TCP/IP, DNS et DHCP
- Developper mes competences en documentation technique professionnelle
- Mettre en pratique une methodologie de projet informatique structuree

## Environnement technique

| Composant | Outil / Version | Role |
|---|---|---|
| Hyperviseur | VMware Workstation Pro | Virtualisation de l'infrastructure |
| Reseau virtuel | VMnet19 (Host-only) | Isolation du reseau de test |
| OS Serveurs | Debian 12 Bookworm | Systeme d'exploitation serveur |
| Serveur DNS | Bind9 — ISC | Resolution de noms de domaine |
| Serveur DHCP | isc-dhcp-server 4.4.3 | Attribution automatique des IP |
| Outils reseau | dnsutils, net-tools, curl | Diagnostic et tests reseau |
| Acces distant | OpenSSH | Administration a distance via SSH |
| Client test | Windows 11 (VM) | Validation des services DHCP/DNS |

## Identifiants du projet

L'ensemble des acces utilises dans ce projet sont recapitules ci-dessous.

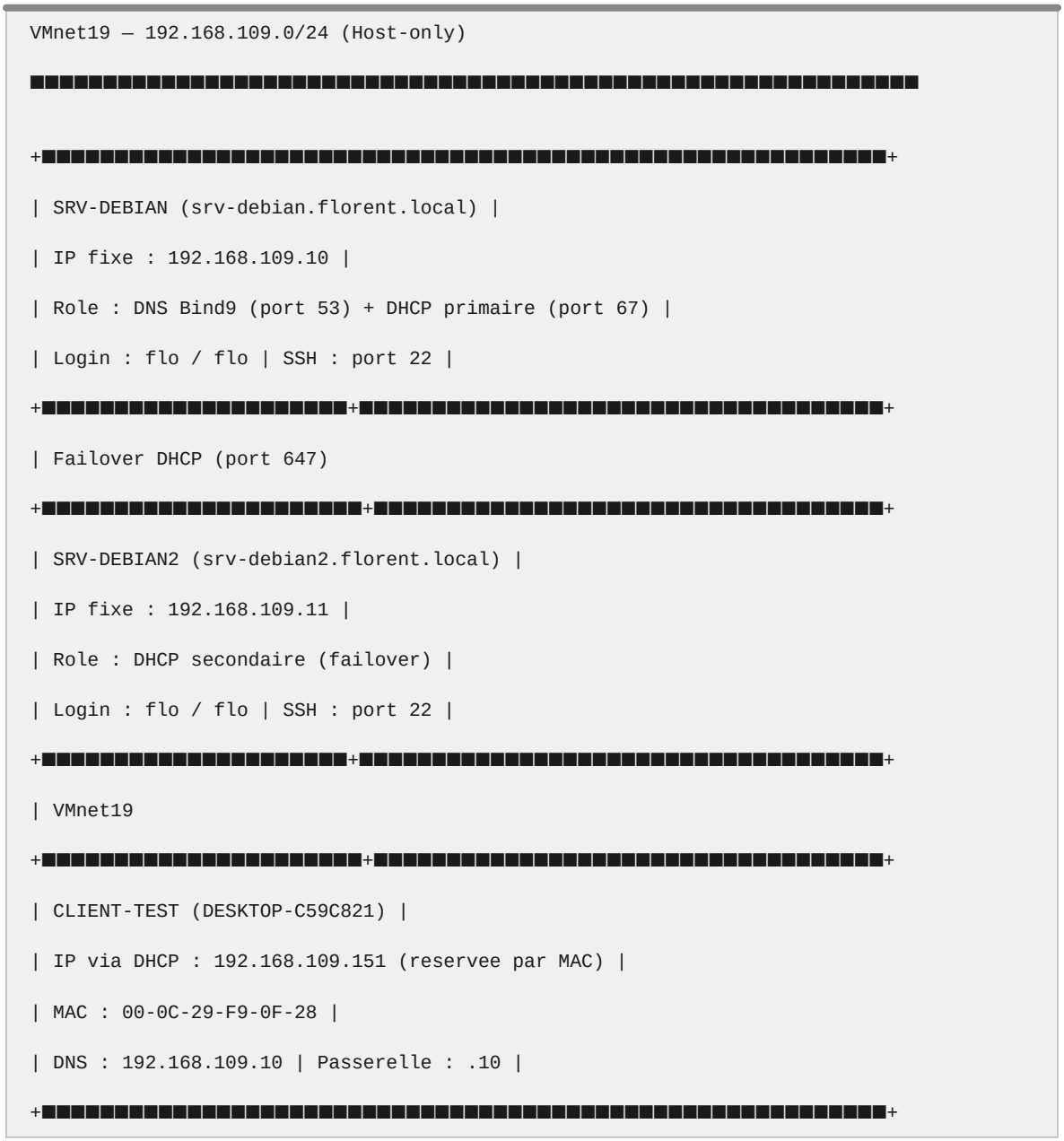
| Machine | Nom d'hote | Adresse IP | Login | Mot de passe | Connexion SSH |
|---|---|---|---|---|---|
| Serveur primaire | srv-debian | 192.168.109.10 | flo / root | flo | ssh flo@192.168.109.10 |
| Serveur secondaire | srv-debian2 | 192.168.109.11 | flo / root | flo | ssh flo@192.168.109.11 |
| Client test | DESKTOP-C59C821 | 192.168.109.151 | — | — | Windows 11 |

*Note : Les mots de passe sont volontairement simples car il s'agit d'un environnement de test isole (reseau VMnet19 sans acces Internet). En production, des mots de passe complexes et une authentification par cle SSH publique seraient utilises.*

# 2. Architecture reseau

## Schema de l'architecture

L'infrastructure repose sur un reseau prive virtuel VMnet19, en mode Host-only, isole du reseau physique. Les trois machines communiquent uniquement entre elles sans acces Internet depuis ce reseau.




## Plan d'adressage IP

| Plage d'adresses | Utilisation | Description |
|---|---|---|
| 192.168.109.1 – 99 | Adresses statiques | Serveurs et equipements reseau |
| 192.168.109.10 | Serveur DNS/DHCP primaire | srv-debian — IP fixe |
| 192.168.109.11 | Serveur DHCP secondaire | srv-debian2 — IP fixe (failover) |
| 192.168.109.100 – 200 | Pool DHCP dynamique | Attribution automatique aux clients |

| | | |
|---|---|---|
| 192.168.109.151 | CLIENT-TEST | Reserve par adresse MAC |
| 192.168.109.201 – 254 | Reserve | Extension future |
| 192.168.109.255 | Broadcast | Adresse de diffusion |

# 3. Installation de l'environnement

## Configuration VMware

Avant de creer les machines virtuelles, il faut configurer un reseau virtuel dedie dans VMware Workstation Pro pour isoler l'environnement de test.

- Ouvrir VMware -> Edit -> Virtual Network Editor
- Cliquer sur Change Settings (droits administrateur requis)
- Ajouter un reseau : Add Network -> VMnet19
- Configurer en mode Host-only, Subnet IP : 192.168.109.0, Mask : 255.255.255.0
- Decocher imperativement Use local DHCP service — sinon conflit avec notre serveur DHCP
- Valider : Apply -> OK

## Creation des machines virtuelles

| Parametre | SRV-DEBIAN | SRV-DEBIAN2 | CLIENT-TEST |
|---|---|---|---|
| Systeme | Debian 12 x64 | Debian 12 x64 | Windows 11 x64 |
| RAM | 2 048 MB | 2 048 MB | 4 096 MB |
| CPU | 2 coeurs | 2 coeurs | 2 coeurs |
| Disque | 20 GB | 20 GB | 64 GB |
| Reseau install. | NAT (temporaire) | NAT (temporaire) | VMnet19 direct |
| Reseau prod. | VMnet19 | VMnet19 | VMnet19 |
| IP | 192.168.109.10 | 192.168.109.11 | 192.168.109.151 (DHCP) |

*Strategie reseau lors de l'installation : les serveurs demarrent en NAT pour permettre le telechargement des paquets depuis les depots Debian. Une fois les paquets installes, la carte reseau est basculee sur VMnet19 et l'IP fixe est configuree manuellement.*

## Installation de Debian 12

La procedure est identique pour les deux serveurs. Choix effectues lors de l'installation :

| Etape | srv-debian | srv-debian2 |
|---|---|---|
| Mode d'install. | Graphical install | Graphical install |
| Langue / Clavier | Francais | Francais |
| Nom de machine | srv-debian | srv-debian2 |
| Nom de domaine | florent.local | florent.local |
| Utilisateur | flo | flo |
| Mot de passe root | flo | flo |
| Mot de passe flo | flo | flo |
| Partitionnement | Tout dans une seule partition | Tout dans une seule partition |

| | | |
|---|---|---|
| Logiciels | Serveur SSH + Utilitaires | Serveur SSH + Utilitaires |
| Interface graphique | Aucune | Aucune |

*Justification du choix sans interface graphique : un serveur n'en a pas besoin. Cela reduit la consommation de RAM et de CPU, diminue la surface d'attaque et correspond aux pratiques professionnelles en production.*

## Installation des paquets

Une fois connecte en root sur chaque serveur (su -), on met a jour le systeme et on installe les paquets necessaires :

```
# Mise a jour du systeme

apt update && apt upgrade -y


# Installation des services DNS et DHCP + outils reseau

apt install bind9 bind9utils bind9-doc dnsutils isc-dhcp-server net-tools vim curl
-y
```

| Paquet | Role |
|---|---|
| bind9 | Serveur DNS Berkeley Internet Name Domain |
| bind9utils / bind9-doc | Utilitaires de verification et documentation Bind9 |
| dnsutils | Outils de diagnostic DNS (nslookup, dig) |
| isc-dhcp-server | Serveur DHCP de l'Internet Systems Consortium |
| net-tools | Outils reseau classiques (ifconfig, netstat) |
| vim, curl | Editeur de texte et outil de transfert HTTP |

*Comportement normal : lors de l'installation, isc-dhcp-server echoue au demarrage car il n'est pas encore configure. C'est attendu et se resout a l'etape suivante.*

## Configuration de l'IP fixe

Apres basculement de la carte reseau sur VMnet19, on edite /etc/network/interfaces pour attribuer une adresse statique :

```
nano /etc/network/interfaces


# Loopback

auto lo

iface lo inet loopback


# Interface principale — IP statique
```

```
auto ens33

iface ens33 inet static

address 192.168.109.10 # 192.168.109.11 pour srv-debian2

netmask 255.255.255.0

network 192.168.109.0

broadcast 192.168.109.255
```

```
# Application de la configuration

systemctl restart networking


# Verification

ip a

-> ens33: inet 192.168.109.10/24 scope global ens33
```

# 4. Configuration du DNS (Bind9)

Bind9 est le serveur DNS open-source le plus repandu. Il permet la resolution de noms de domaine en adresses IP (resolution directe) et l'operation inverse (resolution inverse). Il est developpe et maintenu par l'ISC (Internet Systems Consortium).

## Options globales — /etc/bind/named.conf.options

```
nano /etc/bind/named.conf.options


options {

directory "/var/cache/bind";


forwarders {

8.8.8.8; # DNS Google

8.8.4.4;

};


dnssec-validation auto;

listen-on-v6 { any; };

allow-query { localhost; 192.168.109.0/24; };

};
```

| Directive | Role |
|---|---|
| directory | Dossier de travail pour les fichiers temporaires de Bind9 |
| forwarders | Redirige les requetes inconnues vers les DNS Google (8.8.8.8 / 8.8.4.4) |
| dnssec-validation | Verifie les signatures DNSSEC pour eviter les donnees falsifiees |
| allow-query | Restreint les requetes DNS au reseau local 192.168.109.0/24 |

## Declaration des zones — /etc/bind/named.conf.local

```
nano /etc/bind/named.conf.local


// Zone directe (nom -> IP)

zone "florent.local" {

type master;

file "/etc/bind/db.florent.local";
```

```
};

// Zone inverse (IP -> nom)
zone "109.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.192.168.109";
};
```

## Zone directe — /etc/bind/db.florent.local

```
nano /etc/bind/db.florent.local

$TTL 604800
@ IN SOA srv-debian.florent.local. admin.florent.local. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS srv-debian.florent.local.
@ IN A 192.168.109.10
srv-debian IN A 192.168.109.10
www IN A 192.168.109.10
```

| Enregistrement | Description |
|---|---|
| SOA (Start of Authority) | Definit le serveur de noms principal et les parametres de la zone |
| NS (Name Server) | Indique le serveur DNS autoritaire pour la zone florent.local |
| A (Address) | Associe un nom d'hote a une adresse IPv4 |
| Serial | Numero de version — doit etre incremente a chaque modification de zone |

## Zone inverse — /etc/bind/db.192.168.109

```
nano /etc/bind/db.192.168.109
```

```
$TTL 604800

@ IN SOA srv-debian.florent.local. admin.florent.local. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS srv-debian.florent.local.

10 IN PTR srv-debian.florent.local.
```

L'enregistrement PTR (Pointer) realise la resolution inverse : l'adresse .10 du reseau 192.168.109.0/24 est associee au nom complet srv-debian.florent.local.

## Verification et demarrage

```
# Verification syntaxique des fichiers de configuration

named-checkconf

named-checkzone florent.local /etc/bind/db.florent.local

-> zone florent.local/IN: loaded serial 2

-> OK


named-checkzone 109.168.192.in-addr.arpa /etc/bind/db.192.168.109

-> zone 109.168.192.in-addr.arpa/IN: loaded serial 1

-> OK


# Redemarrage et verification du statut

systemctl restart bind9

systemctl status bind9

-> Active: active (running)


# Test de resolution

nslookup srv-debian.florent.local 127.0.0.1

-> Name: srv-debian.florent.local

-> Address: 192.168.109.10
```

# 5. Configuration du DHCP avec Failover

Le protocole DHCP automatise l'attribution des parametres reseau aux postes clients (adresse IP, masque, passerelle, DNS). Le mecanisme de failover permet a deux serveurs DHCP de se synchroniser : si le primaire tombe, le secondaire prend le relais automatiquement sans interruption de service.

## Interface d'ecoute (les deux serveurs)

```
nano /etc/default/isc-dhcp-server


INTERFACESv4="ens33"

INTERFACESv6=""
```

## Configuration du serveur primaire (192.168.109.10)

```
nano /etc/dhcp/dhcpd.conf


# Parametres globaux

option domain-name "florent.local";

option domain-name-servers 192.168.109.10;

default-lease-time 600;

max-lease-time 7200;

authoritative;

deny unknown-clients; # Filtrage MAC : machines inconnues rejetees


# Configuration du failover – role primary

failover peer "dhcp-failover" {

primary;

address 192.168.109.10;

port 647;

peer address 192.168.109.11;

peer port 647;

max-response-delay 30;

max-unacked-updates 10;

mclt 3600;

split 128;
```

```
load balance max seconds 3;
}

# Pool DHCP
subnet 192.168.109.0 netmask 255.255.255.0 {
pool {
failover peer "dhcp-failover";
range 192.168.109.100 192.168.109.200;
}
option routers 192.168.109.10;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.109.255;
option domain-name-servers 192.168.109.10;
}

# Reservation MAC — CLIENT-TEST autorise
host client-test {
hardware ethernet 00:0c:29:f9:0f:28;
fixed-address 192.168.109.151;
}
```

| Parametre | Valeur | Role |
|---|---|---|
| domain-name | florent.local | Nom de domaine transmis aux clients |
| domain-name-servers | 192.168.109.10 | Serveur DNS communique aux clients |
| default-lease-time | 600 s (10 min) | Duree par defaut du bail IP |
| max-lease-time | 7 200 s (2 h) | Duree maximale du bail IP |
| authoritative | — | Ce serveur fait autorite sur le reseau |
| deny unknown-clients | — | Rejette toute machine non declaree |
| range | .100 a .200 | 101 adresses IP distribuables |
| split 128 | — | Repartition equitable entre primaire et secondaire |

## Configuration du serveur secondaire (192.168.109.11)

Le fichier dhcpd.conf du serveur secondaire est presque identique, avec deux differences : le role passe a secondary et les adresses sont inversees. Les directives mclt et split sont absentes (reservees au primaire).

```
# Differences dans le bloc failover peer "dhcp-failover" {

secondary; # Role secondaire

address 192.168.109.11; # Son propre IP

peer address 192.168.109.10; # IP du primaire

# mclt et split absents

}
```

## Demarrage et validation du failover

```
# Verification syntaxique

dhcpd -t -cf /etc/dhcp/dhcpd.conf

-> Pas d'erreur = syntaxe valide


# Demarrage sur les deux serveurs

systemctl restart isc-dhcp-server

systemctl status isc-dhcp-server

-> Active: active (running)


# Verification du failover dans les journaux

journalctl -u isc-dhcp-server | grep failover

-> failover peer dhcp-failover: Both servers normal
```

*Le message Both servers normal confirme que les deux serveurs DHCP sont synchronises et operationnels. En cas de panne du primaire, le secondaire prend le relais automatiquement.*

# 6. Securisation — Filtrage par adresse MAC

Le filtrage par adresse MAC est une mesure de securite qui permet de controler quelles machines peuvent obtenir une adresse IP du serveur DHCP. Combine a la directive deny unknown-clients, seules les machines explicitement declarees avec leur adresse MAC recoivent une configuration reseau.

| Directive | Effet |
|---|---|
| deny unknown-clients | Rejette toutes les machines dont l'adresse MAC n'est pas connue |
| host nom { hardware ethernet MAC; fixed-address IP; } | Autorise une machine et lui reserve une IP fixe |

Configuration appliquee dans /etc/dhcp/dhcpd.conf :

```
deny unknown-clients; # Bloquer toutes les machines inconnues


# CLIENT-TEST — seule machine autorisee sur ce reseau

host client-test {

hardware ethernet 00:0c:29:f9:0f:28;

fixed-address 192.168.109.151;

}
```

*Pour ajouter une nouvelle machine : recuperer son adresse MAC (ipconfig /all sous Windows ou ip a sous Linux), ajouter un bloc host dans dhcpd.conf sur les deux serveurs, puis redemarrer le service isc-dhcp-server.*

Comportement observe dans les journaux du serveur DHCP :

```
# Machine inconnue -> rejet

DHCPDISCOVER from 00:xx:xx:xx:xx:xx via ens33: unknown client


# CLIENT-TEST -> accepte

DHCPDISCOVER from 00:0c:29:f9:0f:28 via ens33

DHCPOFFER on 192.168.109.151 to 00:0c:29:f9:0f:28 (DESKTOP-C59C821)

DHCPACK on 192.168.109.151 to 00:0c:29:f9:0f:28
```

# 7. Tests et validation

## Mise en place du client test

Pour valider l'ensemble de l'infrastructure, une VM Windows 11 (CLIENT-TEST) a ete creee et connectee sur VMnet19 avec la carte reseau configuree en DHCP automatique. Specifications : 4 Go RAM, 64 Go disque, carte reseau Custom VMnet19.

## Test 1 — Attribution IP automatique (DHCP)

Apres demarrage du client Windows 11, on ouvre l'invite de commandes et on execute :

```
C:\Users\flo> ipconfig /release

C:\Users\flo> ipconfig /renew

C:\Users\flo> ipconfig /all
```

Resultat obtenu :

```
Carte Ethernet Ethernet0 :

Suffixe DNS propre a la connexion . . . : florent.local

Adresse physique . . . . . . . . . . . : 00-0C-29-F9-0F-28

DHCP active . . . . . . . . . . . . . . : Oui

Configuration automatique activee . . . : Oui

Adresse IPv4 . . . . . . . . . . . . . . : 192.168.109.151 (prefere)

Masque de sous-reseau . . . . . . . . . : 255.255.255.0

Bail obtenu . . . . . . . . . . . . . . : jeudi 7 mai 2026 10:12:20

Bail expirant . . . . . . . . . . . . . . : jeudi 7 mai 2026 10:22:20

Passerelle par defaut . . . . . . . . . : 192.168.109.10

Serveur DHCP . . . . . . . . . . . . . . : 192.168.109.10

Serveurs DNS . . . . . . . . . . . . . . : 192.168.109.10

NetBIOS sur Tcpip . . . . . . . . . . . : Active
```

| Parametre verifie | Valeur attendue | Valeur obtenue | Resultat |
|---|---|---|---|
| Adresse IPv4 | 192.168.109.100–200 | 192.168.109.151 | OK |
| Masque | 255.255.255.0 | 255.255.255.0 | OK |
| Passerelle | 192.168.109.10 | 192.168.109.10 | OK |
| Serveur DHCP | 192.168.109.10 | 192.168.109.10 | OK |
| Serveur DNS | 192.168.109.10 | 192.168.109.10 | OK |
| Suffixe DNS | florent.local | florent.local | OK |

## Test 2 — Resolution DNS

```
C:\Users\flo> nslookup srv-debian.florent.local

Serveur : srv-debian.florent.local
Address: 192.168.109.10

Nom : srv-debian.florent.local
Address: 192.168.109.10
```

Le client interroge bien notre serveur DNS (192.168.109.10) qui lui retourne correctement l'adresse IP associee au nom srv-debian.florent.local.

## Test 3 — Connectivite reseau par nom (ping)

```
C:\Users\flo> ping srv-debian.florent.local

Envoi d'une requete ping sur srv-debian.florent.local [192.168.109.10]
avec 32 octets de donnees :
Reponse de 192.168.109.10 : octets=32 temps<1ms TTL=64
Reponse de 192.168.109.10 : octets=32 temps=1ms TTL=64
Reponse de 192.168.109.10 : octets=32 temps<1ms TTL=64
Reponse de 192.168.109.10 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.109.10 :
Paquets : envoyes=4, recus=4, perdus=0 (perte 0 %)
Duree approximative des boucles en millisecondes :
Minimum=0ms, Maximum=1ms, Moyenne=0ms
```

Windows resout le nom FQDN en adresse IP avant d'envoyer les paquets ICMP. Les 4 paquets sont recus sans perte, confirmant la connectivite complete.

## Test 4 — Failover DHCP

Procedure de test du basculement automatique :

- Le serveur primaire (srv-debian) est eteint depuis VMware (Power -> Shut Down Guest)
- Sur le client Windows, on force le renouvellement du bail : ipconfig /release puis ipconfig /renew
- On verifie que le client obtient toujours son IP via le serveur secondaire

Resultat observe :

```
Carte Ethernet Ethernet0 :

Adresse IPv4 . . . . . . . . . . . . . : 192.168.109.151 (prefere)
Bail obtenu . . . . . . . . . . . . . . : jeudi 7 mai 2026 10:00:45
Bail expirant . . . . . . . . . . . . . : jeudi 7 mai 2026 10:08:18
Passerelle par defaut . . . . . . . . . : 192.168.109.10
Serveur DHCP . . . . . . . . . . . . . . : 192.168.109.11 <- secondaire actif
Serveurs DNS . . . . . . . . . . . . . . : 192.168.109.10
```

Le serveur DHCP indique est desormais 192.168.109.11 (srv-debian2). Le failover fonctionne : le client a conserve son IP et continue de recevoir une configuration reseau valide malgre la panne du serveur primaire.

## Test 5 — Filtrage MAC

Le filtrage MAC est valide par le fait que le client autorise (MAC 00-0C-29-F9-0F-28) obtient systematiquement son IP reservee. Toute machine inconnue est rejetee et ne recoit pas de bail DHCP.

## Synthese des tests

| Test | Objectif | Commande / Methode | Resultat |
|---|---|---|---|
| Attribution IP | Client obtient une IP du pool | ipconfig /all | 192.168.109.151 — OK |
| Suffixe DNS | Client recoit florent.local | ipconfig /all | florent.local — OK |
| Serveur DHCP | Pointeur vers .10 | ipconfig /all | 192.168.109.10 — OK |
| Serveur DNS | Pointeur vers .10 | ipconfig /all | 192.168.109.10 — OK |
| Resolution DNS | srv-debian.florent.local -> IP | nslookup | 192.168.109.10 — OK |
| Connectivite nom | Ping par nom reussi | ping srv-debian.florent.local | 4/4 paquets — 0% perte |
| Failover DHCP | Secondaire actif apres panne | ipconfig /all | Serveur DHCP : .11 — OK |
| Filtrage MAC | Machine autorisee seule servie | Journaux dhcpd | DHCPACK sur .151 — OK |

# 8. Difficultes rencontrees

### 1. Acces aux miroirs Debian impossible lors de l'installation

| | |
|---|---|
| Probleme | Durant l'installation, une erreur Miroir de l'archive Debian corrompu s'affichait. La VM etait configuree sur VMnet19 (Host-only) sans acces Internet, ce qui empechait le telechargement des paquets. |
| Solution | Basculement temporaire de la carte reseau en NAT pendant l'installation pour acceder aux depots Debian, puis retour sur VMnet19 une fois les paquets installes. |

### 2. Echec du service DHCP au premier demarrage

| | |
|---|---|
| Probleme | Apres l'installation, isc-dhcp-server refusait de demarrer avec le message control process exited with error code. Le service essayait de se lancer sans fichier de configuration valide. |
| Solution | Ce comportement est normal et attendu. Il se resout des la configuration du fichier dhcpd.conf avec un bloc subnet valide et la definition de l'interface dans /etc/default/isc-dhcp-server. |

### 3. Perte de session SSH lors du changement d'adaptateur reseau

| | |
|---|---|
| Probleme | En basculant la carte reseau de NAT vers VMnet19, la session SSH se coupait car l'adresse IP changeait completement (192.168.17.x -> 192.168.109.x). |
| Solution | Modifier le fichier /etc/network/interfaces avec l'IP statique AVANT de changer l'adaptateur dans VMware. Ainsi, des le basculement, le serveur repond sur sa nouvelle IP fixe et la reconnexion SSH fonctionne immediatement. |

### 4. Avertissement SSH — Remote Host Identification Changed

| | |
|---|---|
| Probleme | A la reconnexion SSH apres reinstallation, un avertissement de securite bloquait la connexion car l'IP 192.168.109.10 etait deja enregistree avec une cle SSH differente. |
| Solution | Supprimer l'ancienne cle avec ssh-keygen -R 192.168.109.10 sur la machine hote, puis relancer la connexion. Ce mecanisme de securite protege contre les attaques man-in-the-middle. |

### 5. Doublon dans dhcpd.conf lors de l'ajout du filtrage MAC

| | |
|---|---|
| Probleme | Lors de l'ajout du filtrage MAC, le collage dans nano s'est ajoute a la suite du contenu existant au lieu de le remplacer, causant des erreurs de declaration en double. |
| Solution | Utiliser cat /dev/null > /etc/dhcp/dhcpd.conf pour vider le fichier avant d'y coller le nouveau contenu. Toujours verifier avec dhcpd -t avant de redemarrer le service. |

# 9. Competences mobilisees

## Referentiel BTS SIO option SISR

| Competence | Actions realisees dans ce PPE |
|---|---|
| A1.3.2 — Deployer un service | Installation et configuration de Debian 12 sans interface graphique, deploiement de Bind9 (DNS) et isc-dhcp-server (DHCP), configuration des zones DNS et du pool DHCP |
| A1.3.3 — Automatiser les taches | Le service DHCP attribue automatiquement les parametres reseau a chaque client (IP, masque, passerelle, DNS) sans aucune intervention manuelle |
| A1.3.4 — Haute disponibilite | Mise en place du failover DHCP entre deux serveurs : continuite de service garantie meme en cas de panne du serveur primaire (valide par test) |
| A2.3.2 — Securiser les acces | Filtrage par adresse MAC (deny unknown-clients) : seules les machines explicitement autorisees obtiennent une configuration reseau |
| A4.1.10 — Concevoir un reseau | Definition d'un plan d'adressage IP coherent en /24 avec segmentation fonctionnelle, integration DNS/DHCP pour une gestion unifiee du reseau local |
| A5.1 — Mettre en oeuvre les procedures | Tests DNS (nslookup, dig), tests DHCP (ipconfig /all), test de failover (arret serveur primaire), verification par journaux systeme (journalctl) |
| A5.2 — Rediger la documentation | Redaction de ce rapport technique structure avec procedures detaillees, configurations commentees et resultats de tests |

## Competences transversales

| Competence | Mise en pratique |
|---|---|
| Resolution de problemes | 5 difficultes rencontrees et resolues par analyse methodique des journaux systeme et recherche de solutions alternatives |
| Administration Linux | Maitrise de la ligne de commande, edition de fichiers de configuration, gestion des services systemd (start, restart, status, journalctl) |
| Documentation technique | Redaction d'un dossier structure et professionnel avec procedures reproductibles et fichiers de configuration commentes |
| Gestion de projet | Planification des etapes (VMware -> Installation -> DNS -> DHCP -> Failover -> Tests), adaptation face aux difficultes rencontrees |

# 10. Conclusion

## Bilan du projet

Ce projet de mise en place d'un serveur DHCP et DNS sous Debian 12 avec failover et filtrage MAC a ete mene a bien dans sa totalite. L'infrastructure deployee repond a l'ensemble des objectifs fixes et constitue une base representative d'un environnement professionnel reel.

| Objectif | Statut |
|---|---|
| Installation et configuration de Debian 12 (x2) | Realise |
| Serveur DNS Bind9 — zones directe et inverse operationnelles | Realise |
| Serveur DHCP primaire avec pool d'adresses | Realise |
| Failover DHCP — Both servers normal | Realise |
| Filtrage MAC — deny unknown-clients | Realise |
| Reservation IP fixe par adresse MAC | Realise |
| Tests complets depuis client Windows 11 | Realise |
| Documentation technique | Realise |

## Perspectives d'evolution

L'infrastructure mise en place pourrait etre enrichie par plusieurs evolutions :

- Serveur DNS secondaire (esclave Bind9 sur srv-debian2) pour la haute disponibilite DNS
- Configuration d'un pare-feu (iptables/nftables) pour restreindre les acces aux services
- Supervision avec Zabbix pour surveiller les services et generer des alertes
- Integration Active Directory via Samba 4 pour la gestion centralisee des utilisateurs
- Scripts de sauvegarde automatique des fichiers de configuration

## Bilan personnel

Ce projet m'a apporte une experience concrete de l'administration systeme Linux en conditions proches du reel. J'ai particulierement progresse dans la comprehension des protocoles DNS et DHCP, dans la gestion des services systemd et dans la methodologie de diagnostic face aux erreurs.

Les difficultes rencontrees, notamment sur la gestion du reseau lors des changements d'adaptateur et la configuration du failover, ont ete de veritables opportunites d'apprentissage. Ce PPE me servira de reference pour mes futurs projets d'infrastructure.

# 11. Annexes

## A. Fichier /etc/network/interfaces — srv-debian

```
auto lo

iface lo inet loopback


auto ens33

iface ens33 inet static

address 192.168.109.10

netmask 255.255.255.0

network 192.168.109.0

broadcast 192.168.109.255
```

## B. Fichier /etc/bind/named.conf.options

```
options {

directory "/var/cache/bind";

forwarders {

8.8.8.8;

8.8.4.4;

};

dnssec-validation auto;

listen-on-v6 { any; };

allow-query { localhost; 192.168.109.0/24; };

};
```

## C. Fichier /etc/bind/named.conf.local

```
// Zone directe

zone "florent.local" {

type master;

file "/etc/bind/db.florent.local";

};
```

```
// Zone inverse

zone "109.168.192.in-addr.arpa" {

type master;

file "/etc/bind/db.192.168.109";

};
```

## D. Recapitulatif des commandes cles

| Commande | Description |
|---|---|
| apt install bind9 isc-dhcp-server -y | Installer DNS et DHCP |
| named-checkconf | Verifier la syntaxe globale de Bind9 |
| named-checkzone zone fichier | Verifier un fichier de zone DNS |
| systemctl restart bind9 | Redemarrer le service DNS |
| systemctl restart isc-dhcp-server | Redemarrer le service DHCP |
| dhcpd -t -cf /etc/dhcp/dhcpd.conf | Tester la syntaxe de la configuration DHCP |
| journalctl -u isc-dhcp-server \| grep failover | Verifier l'etat du failover |
| cat /var/lib/dhcp/dhcpd.leases | Consulter les baux DHCP accordes |
| nslookup nom.domaine | Tester la resolution DNS |
| ipconfig /release && ipconfig /renew | Renouveler le bail DHCP (Windows) |
| ssh-keygen -R IP | Supprimer une cle SSH enregistree |
| cat /dev/null > fichier | Vider un fichier avant reecriture |

## E. Glossaire

| Terme | Definition |
|---|---|
| DHCP | Dynamic Host Configuration Protocol — attribution automatique des parametres reseau |
| DNS | Domain Name System — resolution des noms de domaine en adresses IP |
| Bind9 | Berkeley Internet Name Domain v9 — serveur DNS open-source le plus repandu |
| Failover | Basculement automatique vers un systeme de secours en cas de panne |
| Bail (Lease) | Duree pendant laquelle une IP est attribuee a un client DHCP |
| Filtrage MAC | Controle d'acces base sur l'adresse physique de la carte reseau |
| deny unknown-clients | Directive DHCP rejetant toute machine non declaree |
| Zone DNS | Portion de l'espace de noms DNS geree par un serveur autoritaire |

| | |
|---|---|
| Enregistrement A | Associe un nom d'hote a une adresse IPv4 |
| Enregistrement PTR | Associe une adresse IP a un nom d'hote (resolution inverse) |
| Host-only | Reseau VMware isole — VMs communiquent entre elles et avec l'hote uniquement |
| APIPA | Adresse auto-configuree (169.254.x.x) quand aucun serveur DHCP ne repond |

## F. Bibliographie


- Documentation officielle Debian : https://www.debian.org/doc/
- ISC Bind9 : https://bind9.readthedocs.io/
- ISC DHCP : https://www.isc.org/dhcp/
- Debian Wiki : https://wiki.debian.org/
- DigitalOcean Tutorials : https://www.digitalocean.com/community/tutorials