

# RAPPORT

**Le dns c'est quoi** (domaine name systèmes ) Domaine name systèmes Le DNS agit comme un traducteur entre les humains et les ordinateurs lorsque tape exemple www.mata.com le DNS va nous permettre d'obtenir l'adresse IP associé au nom de domaine enfin de contacter le serveur qui héberge le site en question le DNS le traduit en adresse ip et la donne au navigateur web notions de hiérarchie le (.) il correspond au top level domain (TLD) les domaine de pré minier niveau ( org , com , Fr ) deuxième niveau ( it-Connect ) et les sous domaine (www)

dns utilise le port 53 avec comme protocole udp (user data gramme protocole)

dnssec (domaine name systeme security extension) c'est la version sécurisée de dns. elle utilise le port 53 avec comme protocole

tcp (transmission control protocole) se retrouve dans la couche transport dans le modèle osi

le udp est plus rapide que le tcp parce que le tcp fait des vérifications

Mais avant avant ca je vais mettre a jour le systeme avec la commande (apt update)

On va rendre le serveur dns local accessible sur le navigateur web et pour cela on va télécharger apache qui est le serveur web le plus utiliser permet des servir des sites je vais utiliser la commande apt apche2 pour telecharger apache

Après avoir télécharger apache je vérifie si la connexion a été établie en écrivant dans mon navigateur <http://192.168.248.150> qui est mon adresse ip et normalement me ramener sur une page qui confirme que apache2 a ete installer

je vais telecharger le dns et faire sa configuration et pour cela je vais utiliser bind9 ( Berkley internet name domain ) implémentation open source du DNS

En utilisant la commande Apt Install bind9 bind9utils bind9-doc -y je téléchargé bind9 et ses outils

Apres installation je vais taper cette commande sudo nano /etc/bind/named.conf.local qui est le fichier de configuration de Bind9

Et je vais inserer ceci dedans

```
(declaration d'une zone dns direct )zone "rr" {  
    (signifie que ce serveur et le serveur principal )type master;  
    (chemin du fichier zone )  file "/etc/bind/db rr";  
};
```

```
(zone inverse) zone "248.168.192.in-addr.arpa" {  
    type master;  
    (fichier qui contient les enregistrement PTR) file "/etc/bind/db.192";  
};
```

Ensuite nous allons créer le fichier de zone les fichiers de zones sont utiliser pour stocker les enregistrement DNS d'une zone particulière

En utilisant cette commande cp /etc/bind/db.local /etc/bind/db.ra qui permet de copier le contenu du fichier db.local et le mettre dans le fichier db.ra

Le fichier db.local c est le fichier DNS fournit par Bind Il contient les enregistrements DNS qui définissent comment un domaine particulier doit être résolu

On va ajouter ceci dans le fichier

```
$TTL 604800  
@ IN SOA serveur.ra. root.serveur.ra. (  
        2 ; Serial  
        604800 ; Refresh  
        86400 ; Retry
```

```
2419200      ; date d expiration
604800 )      ; Negative Cache TTL
;
@    IN    NS    serveur.ra.
@    IN    A     192.168.248.150
serveur.ra.   IN    A     192.168.248.150
```

@ represente le nom de domaine lui meme

**TTL :** Durée en secondes (604800s = 7 jours) pendant laquelle les résolveurs DNS peuvent mettre en cache les informations avant de devoir les rafraîchi

Ensuite je vais creer le fichier de zone inverse en faisant cette commande pour copier le contenu  
cp /etc/bind/db.127 /etc/bind/db.192

Et cette commande pour modifier le contenu du fichier

```
nano /etc/bind/db.192
```

```
@    IN    NS    serveur.ra.
```

```
150   IN    PTR   serveur.ra.
```

Je modifie en mettant cette partie la

Ensuite on va verifier si tout fonctionne en utilisant les commande suivante :

```
named-checkzone ra /etc/bind/db.ra
```

```
named-checkzone 248.168.192.in-addr.arpa /etc/bind/db.192
```

```
named-checkconf
```

Si on effectue ses commandes ci ca fonctionne il va répondre OK ce qui veut dire que les configurations sont bonne

Ensuite nous allons redemarer le sytème en utilisant cette commande systemctl restart bind9

Mais pour que ca puisse fonctionner nous allons chercher a modifier le fichier host

En allant dans windows >> system32>>driver>>etc>>host

Et nous allons ajouter cette ligne a la fin

```
192.168.248.150 serveur.ra
```

Et enregistrer

Normalement si tu tapes sur ton navigateur <http://mata.ra> tu devrais te retrouver sur la page d'acceuille d'apache

La résolution inverse DNS est le processus qui permet de retrouver un nom de domaine à partir d'une adresse IP

## Passons a FTP

Qui signifie Filer Transfer Protocole c'est un protocole de communication qui permet de transferer des fichier entre un ordinateur local et un serveur distant

Ftp utilise le port20 et le port 21

Avec FTP nous allons utiliser vsftpd (very secure ftp daemon)

```
sudo apt install vsftpd -y pour pouvoir telecharger vstpd
```

Ensuite nous allons ajouter un utilisateur ftpd en utilisant la commande

```
adduser ftpuser
```

```
mkdir -p /home/ftpuser/ftp/upload cette commande permet de creer un dossier special pour les utilisateur ftpd
```

Ensuite nous allons definir les permissions des utilisateurs

```
sudo chown nobody:nogroup /home/ftpuser/ftp cette commande en gros elle permet d empêcher que n'importe quel utilisateur puisse modifier le repertoire racine du serveur FTP
```

```
chmod a-w /home/ftpuser/ftp elle empêche quiconque meme les utilisateurs de modifier supprimer des fichiers directement dans le repertoire de base
```

```
chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

Ensuite nous allons copier le contenu de vstftpd.conf et le mettre dans vstftpd.conf.bak

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

Pourquoi faire une copie ? C'est une question de securiter si l'ont fait une erreur on pourrait tjs restaurer le fichier

Ensuite nous ouvrons le fichier

```
Nano /etc/vstpd.conf.bak
```

Et on doit le configurer ainsi

```
listen=YES (permet a ftp d ecouter les connexion entrante)
```

Listen\_ipv6=NO (n'accepte que les connexions via IPV4)

anonymous\_enable=NO ne permet pas les connexions anonymes

local\_enable=YES active la connexion des utilisateurs locaux

write\_enable=YES sans cette option les utilisateurs ne peuvent que lire et télécharger

chroot\_local\_user=YES isole les utilisateurs locaux

allow\_writeable\_chroot=YES permet aux utilisateurs de téléverser les fichiers dans leur répertoire d'accueil

Ensuite nous allons redémarrer le serveur

sudo systemctl restart vsftpd

**DHCP** ( dynamic Host Configuration Protocol ) est un protocole informatique qui permet d'attribuer des adresses IP automatique et de faire la configuration d'un réseau il écoute les requêtes du client sur le port 68 et envoie les requêtes au serveur sur le port 67

La communication DHCP se passe en 4 étapes

Discovery : un client DHCP envoie un message de diffusion afin de trouver un serveur DHCP la requête se fait du port 68 qui va envoyer vers le port 68

Offer : lorsque le DHCP répond il lui offre une adresse IP disponible .cette offre ce fait du port 67 vers 68

Request : le client choisit une des offres et envoie une demande pour informer le serveur qu'il a accepté une offre

Acknowledgment : le serveur qui a fait l'offre envoie un message à l'accuse de réception> ce message confirme au client qu'il peut utiliser l'adresse IP

Maintenant je vais expliquer comment mettre en place un serveur DHCP

apt install isc-dhcp-server on commence par installer le serveur DHCP avec la commande ci-dessous qui représente l'entreprise qui fournit ce paquet

Ensuite on tape cette commande :

nano /etc/default/isc-dhcp-server elle représente le fichier de configuration de DHCP pour son activation et on va modifier la ligne INTERFACESv4="e" qui est vide et mettre ça

INTERFACESv4="ens33" elle permet de spécifier l'interface réseau sur laquelle DHCP va écouter pour écouter les adresses IP

Ensuite nous allons passer à la configuration de DHCP en tapant cette commande nano /etc/dhcp/dhcpd.conf

subnet 192.168.248.0 netmask 255.255.255.0 {

range 192.168.248.100 192.168.248.100; (la plage d'adresse IP que le serveur peut attribuer au client)

option domain-name-servers 192.168.248.150; (l'adresse IP du serveur DNS)

option domain-name "ra"; (le nom de domaine)

option subnet-mask 255.255.255.0; (le masque du sous-réseau)

option routers 192.168.248.1; (la passerelle du réseau)

option broadcast-address 192.168.248.255; (l'adresse de diffusion)

default-lease-time 600; (le temps de bail pour une adresse IP)

```
max-lease-time 7200;(le temps de bail maximal en seconde)
```

```
}
```

Apres avoir effectuer les différentes modification on redémarre le système pour établir les modification en tapant cette commande

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

On vérifie le statut du serveur DHCP qui doit etre en active au cas contraire il y a des erreurs

On verifie le statut avec cette commande :

```
sudo systemctl status isc-dhcp-server
```

Pour vérifier si cela fonctionne nous allons effectuer un test sur un client mais avant tout nous devons télécharger le paquet dhcp\_client

```
sudo apt install isc-dhcp-client
```

Donc apre installation on tape cette commande afin de créer un client

```
sudo dhclient
```

Le client creer si on fait IP A normalement nous allons retrouver l'adresse du client d2