



Debian console

debian

Sommaire

Table des matières

LOOTEN Axel.....	1
Sommaire.....	2
1 Vérification du DNS commande.....	3
2 Désactiver l'ipv6.....	3
3 Configuration du réseau en mode static avec une adresse ip précise.....	4
4 Vérifier de l'installation du Network Manager.....	4
5 Commandes réseau utile.....	5
6 DHCP et DNS.....	5
7 TCP IP et MTU.....	5
8 ARP et analyse des échanges.....	6
9 Routage.....	6
10 NAT.....	6
11 Switchs et VLAN.....	6
12 VPN et certificats.....	7
13 LDAP.....	7
14 IPv6.....	7
15 Supervision.....	7
16 Méthode rapide quand le réseau ne marche pas.....	8
17 liste des commande basique a utiliser pour naviguer et modifier les document.....	8
18 Les différent Grep.....	9
19 Liens.....	9
20 mettre en œuvre une redirection.....	9
21 Chaînage de commandes.....	9
22 Utilisateurs, groupes.....	10
23 Droit.....	10

1 Vérification du DNS commande

- Pour accéder au DNS choisie sur Debian console il faut effectuer la commande « nano /etc/resolv.conf »

2 Désactiver l'ipv6

-Vérifier si l'ipv6 est activé avec « ip a » si (Inet6 scop host noprefixroute) s'affiche alors cela veut dire qu'il est actif

- Entrer les différentes commandes suivantes pour désactiver l'ipv6

crée nano /etc/sysctl.d/sysctl

- Ajoutez ce qui suit au bas du fichier :

```
net.ipv6.conf.all.disable_ipv6 = 1
```

```
net.ipv6.conf.default.disable_ipv6 = 1
```

```
net.ipv6.conf.lo.disable_ipv6 = 1
```

```
net.ipv6.conf.tun0.disable_ipv6 = 1
```

- Enregistrez et fermez le fichier.

- Redémarrez l'appareil. ou sysctl -p pour appliquer les changements

- Pour ré-activer IPv6, supprimez les lignes ci-dessus de /etc/sysctl.conf et redémarrez l'appareil.

3 Configuration du réseau en mode static avec une adresse ip précise

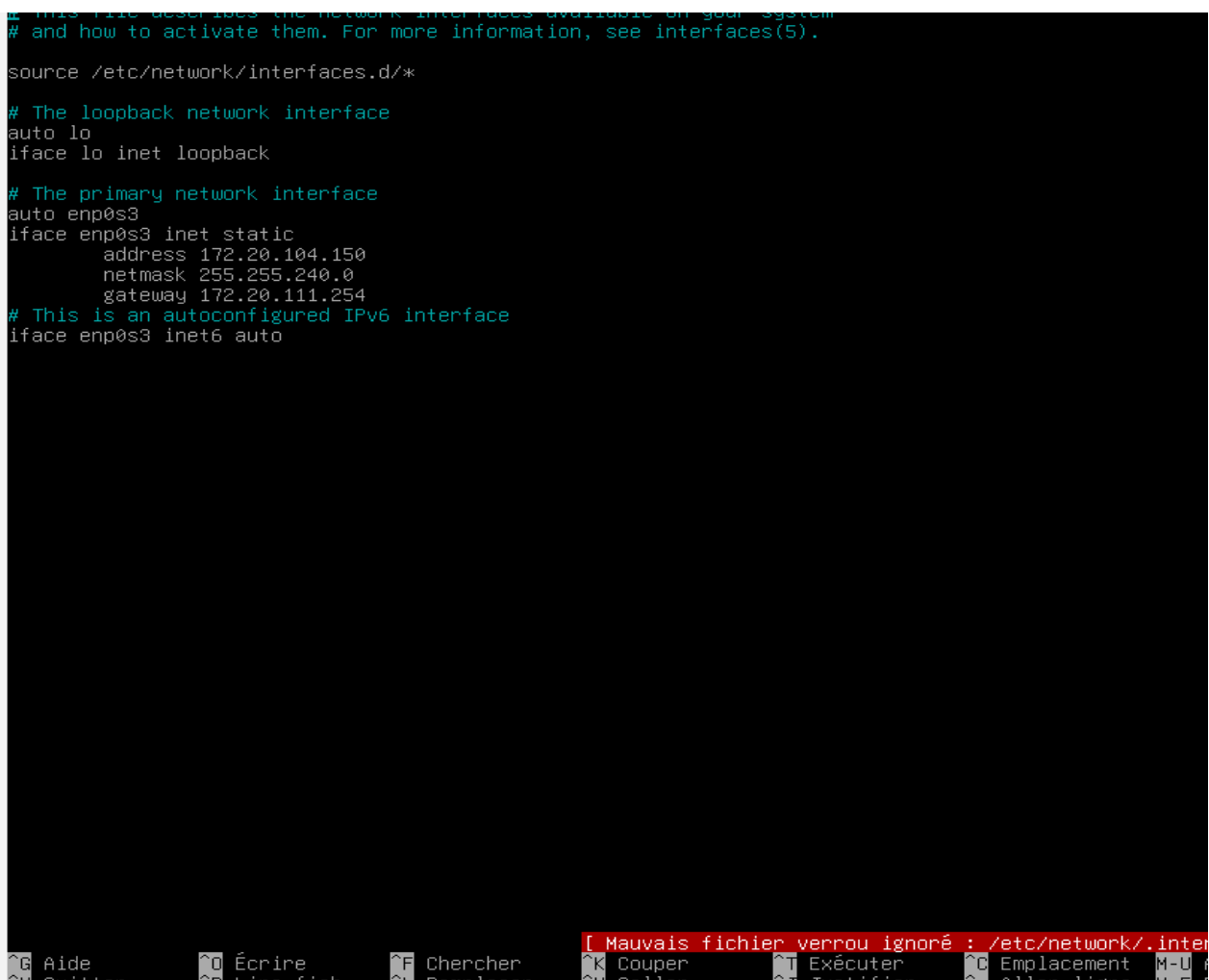
Effectuer la commande nano /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
    address 172.20.104.150
    netmask 255.255.240.0
    gateway 172.20.111.254
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```



Changer le document comme ci dessous en mettant l'adresse ip souhaiter

4 Vérifier de l'installation du Network Manager

Effectuer un « systemctl list units » pour afficher tout les service en cours d'exécution

effectuer « | grep manager » pour afficher une liste qui contiens ce motif

« man ... (par exemple grep) » permet d'avoir les commande de l'attribut (grep)

utiliser la touche « q » pour quitter le man

5 Commandes réseau utile

ip a → affiche les interface réseau avec les adresses ip

ip link → affiche si la carte est UP ou DOWN

ip link set eth0 up → active la carte réseau

ip route → affiche la passerelle et les routes

hostname -I → affiche rapidement l'adresse ip de la machine

ss -tulpn → montre les ports ouvert et les service qui écoute

A retenir : quand le réseau ne marche pas il faut regarder dans l'ordre ip, masque, passerelle, dns puis firewall.

6 DHCP et DNS

DHCP sert a donner automatiquement une ip, un masque, une passerelle et le DNS

dhclient -r → libère l'adresse actuelle

dhclient eth0 → redemande une adresse sur la carte eth0

cat /etc/resolv.conf → affiche le DNS utilisé

nslookup google.fr → vérifie si le DNS répond

dig google.fr → donne plus de détail sur la résolution DNS

Si ping 8.8.8.8 fonctionne mais ping google.fr fonctionne pas, souvent c'est le DNS qui est mal configuré.

7 TCP IP et MTU

ping adresse_ip → teste si la machine répond

ping -c 4 adresse_ip → fait seulement 4 ping

tracert adresse_ip → montre par ou passe le paquet

tracert -d adresse_ip → affiche aussi des infos sur la MTU

ping -M do -s 1472 8.8.8.8 → test de MTU sans fragmentation

La MTU correspond a la taille max d'un paquet. Si elle est trop grande le paquet peut être bloqué ou fragmenté.

8 ARP et analyse des échanges

ARP permet de trouver l'adresse MAC qui correspond a une adresse IP sur le même réseau

`ip neigh` → affiche la table ARP

`arp -a` → autre commande pour voir la table ARP

`ip neigh flush all` → vide la table ARP

`tcpdump -i eth0 arp` → capture seulement les paquets ARP

`tcpdump -i eth0 icmp` → capture seulement les ping

Attention : l'ARP spoofing consiste a envoyer de fausse réponse ARP pour faire passer le trafic par une mauvaise machine.

9 Routage

Le routage permet de joindre un autre réseau, par exemple un autre LAN

`ip route add 192.168.20.0/24 via 192.168.10.254` → ajoute une route

`ip route del 192.168.20.0/24` → supprime une route

`ip route add default via 192.168.1.1` → ajoute une passerelle par défaut

`sysctl net.ipv4.ip_forward` → vérifie si le transfert de paquet est actif

`sysctl -w net.ipv4.ip_forward=1` → active le routage temporairement

En routage static on met les routes a la main. Avec RIP les routeurs peuvent apprendre les routes automatiquement.

10 NAT

Le NAT sert a traduire une adresse privée vers une autre adresse, souvent pour sortir sur internet

`iptables -t nat -L -n -v` → affiche les règles NAT

`iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE` → ajoute un NAT de sortie

`iptables -L -n -v` → affiche les règles firewall classique

`nft list ruleset` → affiche les règles si la machine utilise nftables

Si une machine ping sa passerelle mais pas internet, il faut vérifier le routage, le NAT et le DNS.

11 Switchs et VLAN

Un switch apprend les adresses MAC et les ports ou elles sont brancher

Un VLAN permet de séparer plusieurs réseaux sur le même switch

Un port access appartient a un seul VLAN

Un port trunk transporte plusieurs VLAN entre deux switchs ou vers un routeur

`bridge link` → peut aider a voir les interfaces dans un bridge sur Linux

Quand deux machines ne communiquent pas, il faut comparer VLAN, adresse IP, masque et passerelle.

12 VPN et certificats

Un VPN crée un tunnel chiffré entre deux réseaux ou entre un client et un serveur

`openssl version` → vérifie la version d'OpenSSL

`openssl x509 -in certificat.crt -text -noout` → lit le contenu d'un certificat

`systemctl status openvpn` → regarde si le service OpenVPN est lancé

`journalctl -u openvpn` → affiche les logs OpenVPN

Si le VPN ne monte pas il faut vérifier la date du certificat, la clé, le port, le firewall et les logs.

13 LDAP

LDAP sert à centraliser les comptes et les groupes dans un annuaire

`ldapsearch -x -H ldap://serveur -b dc=exemple,dc=local` → fait une recherche simple

`getent passwd nom_user` → vérifie si l'utilisateur est visible par le système

`getent group nom_groupe` → vérifie si le groupe est visible

`cat /etc/nsswitch.conf` → regarde si le système cherche aussi dans ldap

Si un compte LDAP existe mais ne se connecte pas, regarder NSS, PAM et les logs d'authentification.

14 IPv6

`ip -6 a` → affiche les adresses IPv6

`ip -6 route` → affiche les routes IPv6

`ping -6 ipv6.google.com` → test en IPv6

`sysctl net.ipv6.conf.all.disable_ipv6` → vérifie si IPv6 est désactivé

Une adresse link-local commence souvent par `fe80::` et marche seulement sur le réseau local

Pour IPv6 il faut bien regarder le préfixe, souvent `/64`, et la passerelle donnée.

15 Supervision

La supervision permet de surveiller les machines, les services et les équipements réseau

`systemctl status snmpd` → vérifie le service SNMP

`snmpwalk -v2c -c public adresse_ip` → interroge une machine en SNMP

`zabbix_agentd -t system.hostname` → test une clé Zabbix agent

`tail -f /var/log/syslog` → suit les logs en direct

La supervision sert à voir rapidement si un hôte tombe, si un disque est plein ou si un service ne répond plus.

16 Méthode rapide quand le réseau ne marche pas

- 1 - ip a pour vérifier l'adresse et l'interface
- 2 - ip route pour vérifier la passerelle
- 3 - ping la passerelle
- 4 - ping une ip externe comme 8.8.8.8
- 5 - nslookup google.fr pour vérifier le DNS
- 6 - systemctl status nom_du_service pour vérifier le service
- 7 - journalctl -xe pour regarder les erreurs plus précise

17 liste des commande basique a utiliser pour naviguer et modifier les document

Commandes de manipulations de dossiers

- pwd → affiche le chemin complet du répertoire actuel
- ls → afficher tout les document et dossier présent dans le répertoire actuel
- cd → permet de changer de répertoire
- mkdir → pour crée un document dans un répertoire (ajouter le nom après la commande)
- rmdir → pour supprimer le document présent dans le répertoire (ajouter le nom après la commande)

Commandes de manipulations de fichiers

- cat → Elle permet de lire, concaténer et manipuler des fichiers.
more ou less
- file →
- cp → copie les fichier
- mv → déplace les fichier
- rm → remove les fichier
- type → affiche des informations sur le **type** de commande
- whoami → nous informe sur quelle utilisateur nous sommes actuellement
- who → pour savoir quelle utilisateur est connecter
- find ./ -name « ?? »

18 Les différent Grep

« `ls -l | grep -i *i` » → ici tout les fichier qui finisse par la lettre « i » vont s'afficher car « * » correspond à une infinité de caractère présent

« `ls -l | grep -i ??` » ici cela va afficher tout les dossiers qui possède seulement de caractère car «??» correspond a un caractère unique

« `ls -l | grep -i « ? [aeiou]*` » ici cela va afficher tout les dossiers **qui comprenne une voyelle** en deuxième position

« `ls -l | grep -i « ? [!aeiou]*` » ici cela va afficher tout les dossiers qui comprenne **aucune** en deuxième position car le « ! » va signifier exclure les recherche présente dans la liste

19 Liens

Un lien physique d'un objet **sont tous reliev entre eux** si un seul est modif alors tout les autre le sont aussi et pour supprimer l'objet **il faut supprimer l'ensemble des lien physique crée pour celui ci**

`ln` → Crée un lien physique

`ln -s` → Crée un lien symbolique (comme un raccourcie)

`ls -li` → affiche l'Inode des liens

20 mettre en œuvre une redirection

Plusieurs redirection possible :

`>` : Redirige la sortie standard vers un fichier. Si le fichier existe déjà, son contenu sera remplacé.

`>>` : Utilisé pour ajouter la sortie à la fin d'un fichier existant.

`2>` : Redirige la sortie d'erreur vers un fichier.

`&>` : Redirige à la fois la sortie standard et la sortie d'erreur vers un même fichier

21 Chaînage de commandes

Ici grâce au pipe on peut additionner des commande comme `xargs`

22 Utilisateurs, groupes

Voici les différents fichiers relatifs

group = liste des différents groupes

shadow = les mots de passe hashés et salés

passwd = toutes les infos sur les utilisateurs

getent passwd etu2 → va afficher les informations sur l'utilisateur comme ci-dessous

```
etu2:x:1001:1001:~/home/etu2:/bin/bash
```

anciennes emplacement du mdp

id user

id groupe

bash

Useradd -d /home/etu2 -m -s /bin/bash → pour créer un utilisateur

groupadd = créer un groupe

chmod = changer les droits du fichier

23 Droit

Position Binaire	Valeur octale	Droits	Signification
000	0	- - -	Aucun droit
001	1	- - x	Exécutable
010	2	- w -	Ecriture
011	3	- w x	Ecrire et exécuter
100	4	r - -	Lire
101	5	r - x	Lire et exécuter
110	6	r w -	Lire et écrire
111	7	r w x	Lire écrire et exécuter