Technicien Système et Réseau et Assistance Informatique

TAI-TSSR

20/04/24

Table des matières

Objectifs

Découvrir des systèmes et réseaux

Appréhender et pratiquer GNU-Linux

Comprendre les principes des réseaux IP et les appliquer

Introduction

La production ou exploitation informatique exige des compétences pour gérer les systèmes et réseaux pour :

- déployer et mettre en production les solutions
- maintenir en fonctionnement opérationnel

I Les réseaux IP

1. Découvrir les réseaux IP

==> Module "Introduction Réseau Déploiement Administration" (IRDA)

2. La carte réseau et l'adressage MAC.

2.1. *Carte réseau physique*

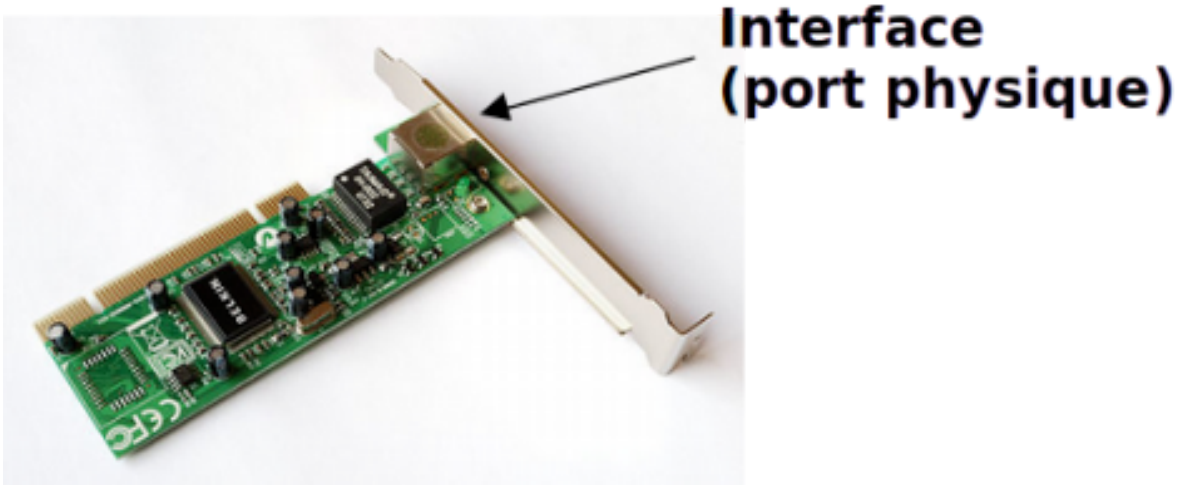


Image 1

2.2. Liaison

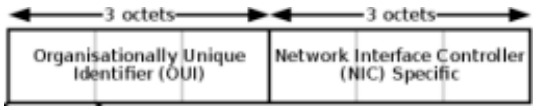
Adresse *MAC* (Media Access Control)

Attribué par IEEE

Format : 6 octets

Couche 2 : liaison

6octets = 48 bits = 2^48 adresses → 2,8 X 10^14



3. La translation d'adresses et de ports (NAT/PAT)

- Le réseau fait transiter des numéros de port normalisés
- Sur présentation d'une requête externe sur un N° de port, le routeur adresse le paquet au serveur qui lui a été désigné pour ce port
- Le network address translation (NAT) associe dynamiquement IP et port TCP/UDP publics à une IP et port TCP/USP privés
- Le Port Address Translation (PAT) associe de manière statique un port TCP/UDP à un hôte interne

4. GNU-Linux : commandes et outils réseau

4.1. Les couches réseau

On peut agir aux différents niveaux du réseau selon le modèle OSI mais les principaux sont :

- le niveau physique (interface)
- le niveau réseau (IP)
- le niveau application (services)

a) Niveau physique

Exemple

arrêt d'une interface : sudo ifdown <interface>

démarrage d'une interface : sudo ifup <interface>

Le redémarrage de l'interface est nécessaire dès qu'on change sa configuration (adresse IP,..)

b) niveau réseau IP

vérifier joignabilité d'un réseau et mesure de la latence

ping <@IP>

pour l'internet : utilisser une adresse IP fixe publique

Exemple **ping 8.8.8.8** ou **ping 1.1.1.1**

```
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=56.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=86.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=138 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=23.4 ms
```

i) identifier la route des paquets IP

la table de routage

```
$ route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         192.168.99.254  0.0.0.0         UG    600    0        0 wlp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp2s0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.99.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp2s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0

```

indic(ateur) = état de la route

U = Up

G = Gateway

ii) identifier la route des paquets IP

la table de routage

```
$ route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         192.168.99.254  0.0.0.0         UG    600    0        0 wlp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp2s0
```

```
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.99.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp2s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0

```

indic(ateur) = état de la route

U = Up

G = Gateway

4.2. Netstat

Cette commande permet de connaître :

- les ports en écoute sur la machine
- sur quelles interfaces
- avec quels protocoles de transport (TCP ou UDP)
- les connexions actives
- connaître les routes

Elle a un grand nombre d'options sont disponibles.

a) connaître les ports d'écoute de transmission

```
sudo netstat -utape
tcp        0      0 tilleul.lan:46686   scenari-community:https ESTABLISHED eric
106556     5822/brave --type=u
udp        0      0 0.0.0.0:4520            0.0.0.0:*
asterisk   46166      2167/asterisk
```

4.3. Parefeu GNU-Linux

- Le noyau GNU-Linux intègre un parefeu géré par l'outil UFW
- utilisation en ligne de commande
- par défaut, il est installé mais désactivé
- des outils graphiques complémentaires permettant de le gérer, par exemple : gfuw

a) usage général

Statut

$ sudo ufw status

activer / désactiver

```
$ sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
$ sudo ufw disable
Le pare-feu est arrêté et désactivé lors du démarrage du système

```

i) règles de gestion de sécurité

Si le FW est actif, pour visualiser les règles :

```
$ sudo ufw status
Vers                       Action      De
----                       ------      --
5060                       ALLOW       Anywhere
```

ouverture d'un port

exemple : port 3080

sudo ufw allow 3080

II GNU-Linux

1. Découvrir GNU-Linux

==> module « Linux Exploité : GO ! »

III Sécurité

1. hygiène informatique recommandées par l'ANSSI

Lire et analyse le guide suivant et appliquer les règles dans la mesure du possible

https://cyber.gouv.fr/publications/guide-dhygiene-informatique