5 - Configuration réseau

M1 RÉSEAUX & TÉLÉCOMS

RT0701 : ADMINISTRATION SYSTÈME 1

OLIVIER FLAUZAC

Configuration

Que configurer ?

Configuration des interfaces

- Adresse
- Masque
- Broadcast

Routage

- Route par défaut
- Routage statique

Résolution

- Statique
- DNS

Gestion de la configuration

Dans des fichiers de configuration

- Dépendant des distributions

Eléments de définition

- Gestion des interfaces (IP, DHCP ...)
  `/etc/network/interfaces`
- Résolution des noms
  `/etc/resolv.conf`
  `/etc/hosts`

En ligne de commande

- Ifconfig + route
- iproute2

Fichier debian

Exploitation de `/etc/network/interfaces`

Définition des propriétés des interfaces

- allow-hotplug : configuration événementielle
- auto : interfaces configurée au boot

Définition des interfaces

- `iface` : définition
- `address` : adresse
- `netmask` : masque de sous réseau
- `gateway` : passerelle
- `dns-nameservers` : dns

Fichier de résolution (Debian)

```
auto lo eth1

iface lo inet loopback

iface eth0 inet dhcp

iface eth1 inet static
    address 192.168.0.42
    netmask 255.255.255.0
    gateway 192.195.0.1

iface eth1 inet6 static
    address 2001:db8::6726
    netmask 32
    gateway 2001:db8::1
```

Configuration en ligne `ifconfig`

`ifconfig` : commande de contrôle et de configuration

`ifconfig interface adresse [paramètres]`

- `interface` : logique ou physique
- `ip / down` : activation désactivation
- `netmask` : masque de sous-réseau
- `broadcast` : adresse de broadcast

```
ifconfig eth0 10.0.2.16 netmask 255.255.255.0 broadcast 10.0.2.255
```

`Ifconfig` (Ubuntu)

```
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:73:6c:c7
          inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe73:6cc7/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:1 erreurs:0 :0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:590 (590.0 B) Octets transmis:990 (990.0 B)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:21:2d:40
          inet adr:192.168.59.99  Bcast:192.168.59.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe21:2d40/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:60 erreurs:0 :0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:8156 (8.1 KB) Octets transmis:7264 (7.2 KB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          Packets reçus:160 erreurs:0 :0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1
          Octets reçus:11840 (11.8 KB) Octets transmis:11840 (11.8 KB)
```

Routage
`route`

`route`: commande de contrôle et de configuration

Définition du routage

- passerelle par défaut
- routage statique

```
route add [net|host] addr [gw passerelle][default][dev interface]
```

- `net / host` : destination de la route
- `addr` : adresse de destination
- `default` : route par défaut
- `interface` associée à la route

```
route add default gw 192.168.0.1 dev eth0
```

Définition du DNS

Fichiers

- `/etc/resolv.conf`
- `/ets/hosts`

Résolution statique et dynamique

```
nameserver 8.8.8.8
```

Iproute2
commande `ip`

Ensemble d'outils de gestion

- Des protocoles TCP,UDP,IP
- Du réseau IPv4 , IPv6

Remplacement de `net-tools`

Unification des éléments

- De configuration
- D'activation / désactivation
- De test & configuration

Equivalence

Utilité	Net-tools	iproute2
Adressage	ifconfig	ip addr, ip link
Routage	route	ip route
Résolution des adresses	arp	ip neigh
Vlan	iptunnels	ip link
Tunnels	vconfig	ip tunnel
statistiques	netstat	ss

Gestion des adresses

Affichage des informations

```
ip addr [interface] show
```

Configuration d'une adresse sur une interface

```
ip addr add address/prefix brd dev interface
```

Destruction d'une adresse sur une interface

```
ip addr del address/prefix brd dev interface
```

Gestion des interfaces

Affichage des interfaces

```
ip link [interface] show
```

Activation / désactivation d'une interface

```
ip link set interface up / down
```

Gestion des routes

Affichage des informations

```
ip route show
```

Ajout d'une route

```
ip route add default via addr dev interface
ip route add –net add/prefix via addr dev interface
```

Remplacement d'une route

```
ip route replace default via address via dev
```

Suppression d'un route

```
ip route delete –net addr/prefix
```

Commandes du réseau

tcpdump

Analyseur de paquets en ligne de commande

Nécessite les droits administrateur

Comparable avec *Wireshark* mais en ligne de commande

Permet de voir le trafic

- d'une interface
- d'un protocole

Options

`-i` choix de l'interface écoutée

`src` choix de la source

`dst` choix de la destination

`port` choix du port de communication

`-w` sortie dans un fichier de log

`-c count` : sortie après count fichiers

`-n` pas de coversion des adresses

`-XX` affichage des contenus des paquets au format hexa

`-s` taille des paquets

- `-s 0` : quelle que soit la taille des paquets

tcpdump

```
sudo tcpdump -n -i eth0 src 192.168.1.17
sudo tcpdump -n -i eth0 src net 10.22.1
sudo tcpdump -n -i eth0 src 192.168.1.17 and port http


sudo tcpdump -XX -s 0 -i eth0 port http | grep -A2 GET
sudo tcpdump -XX -s 0 -i eth0 tcp and port 21 | grep -A1 PASS
sudo tcpdump -XX -s 0 -i eth0 port 1863 | grep -A10 "text/plain"
```

nmap

Scanner réseau

Assure la détection des ports ouverts / machines présentes

Scan possible

- machine
- réseau
- plage d’adresse

Utilisations classiques

Les machines

`nmap –sP <cible>`

```
nmap -sP 192.168.1.1
nmap -sP 192.168.0.0/24
nmap -sP 192.168.0.55-100
```

Les ports

`nmap –p / -sS / -sU`

```
nmap 192.168.1.1
nmap -p 22 192.168.0.0/24
nmap -sS 192.168.0.55-100
nmap -sU 192.168.0.55-100
```

Nmap autres utilisation

Scan agressif

```
--osscan-guess
```

Détection du système scanné

```
-A
```

Scan rapide

```
-F
```

Détection de services

```
-sV
```

Usurpation

```
-spoof-mac mac
-S IP
```

netstat

Etat des connexions TCP actives

Liste des ports TCP et UDP ouverts

Gestion de statistiques

- ethernet IP
- TCP
- UDP
- ICMP

Netstat : états des connexions

```
ESTABLISHED
SYN_SENT
SYN_RECV
FIN_WAIT1
FIN_WAIT2
TIME_WAIT
CLOSED
CLOSE_WAIT
LAST_ACK
LISTEN
CLOSING
UNKNOWN
```

Informations sur les connexions

Informations sur les connexions

- Etat de toutes les connexions
  `-a`
- Utilisation numérique des adresses
  `-n`
- Association processus / connexion
  `-o`

Statistiques

- Etat des interfaces *autoconf*
  `-i`
- Filtre & tri sur le protocole
  `-p proto`
  `-s`
- Tables de routages associées
  `-r`

Exploitation des Commandes

Utilisation locale

- ligne de commande «directe»
- ligne de commande puis redirection dans un fichier
- scripts locaux

Utilisation distante

- connexion ssh et commandes / scripts interactifs
- exécution ssh de commandes / scripts à distances