Administration Réseaux et Systèmes

Gestion réseau - routage et parfeu

Cas : OS Debian

Sommaire

Rappel TCP/IP

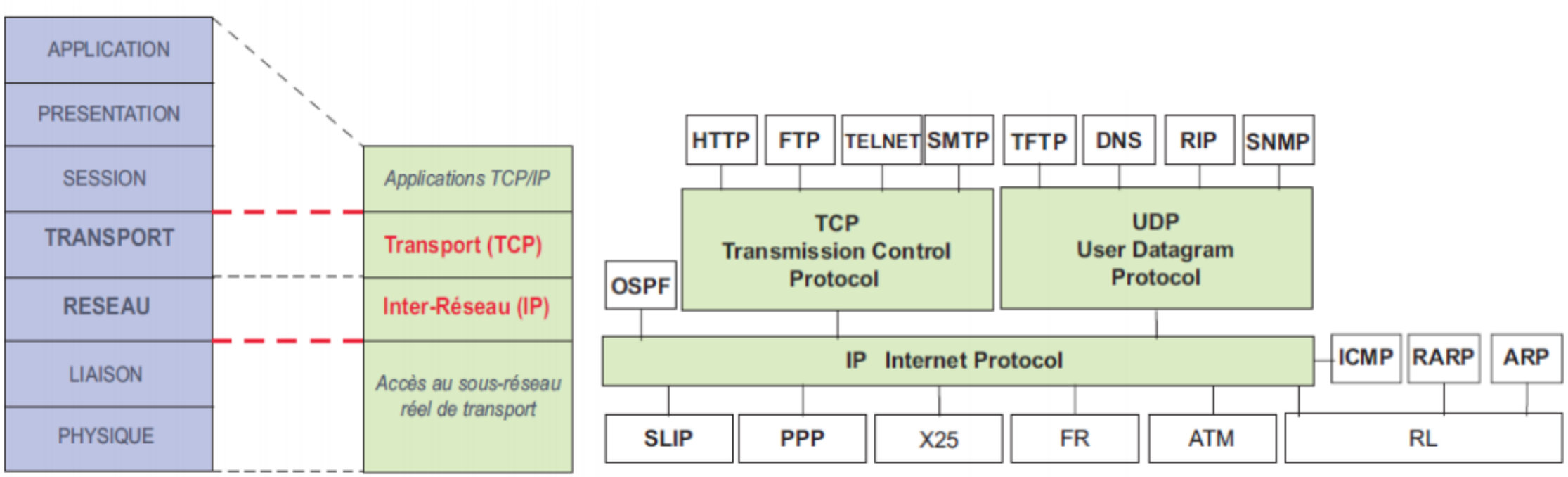
```
192.168.2.4:~ > ping www.cia.gov
PING e6221.dscna.akamaiedge.net (23.44.194.239) 56(84) bytes of data
```

```
00:12:a1:26:42:fe -> Broadcast ARP (Who has 192.168.2.111? Tell \
   192.168.2.4)
00:40:ff:12:27:49 -> 00:12:a1:26:42:fe ARP (192.168.2.111 is \
   00:40:ff:12:27:49 )
192.168.2.4 -> 192.168.2.111 DNS (Query www.cia.gov)
192.168.2.111 -> 192.168.2.4 DNS (Response CNAME \
   www.cia.gov.edgekey.net addr 23.44.194.239...)
192.168.2.4 -> 23.44.194.239 PING (Request)
23.44.194.239 -> 192.168.2.4 PING (Reply)
```

Observations:

- Trois types de noms/adresses utilisés (fqdn, ip, MAC)
- Trois protocoles apparemment utilisés (en réalité 5)
- Combien de machines impliquées

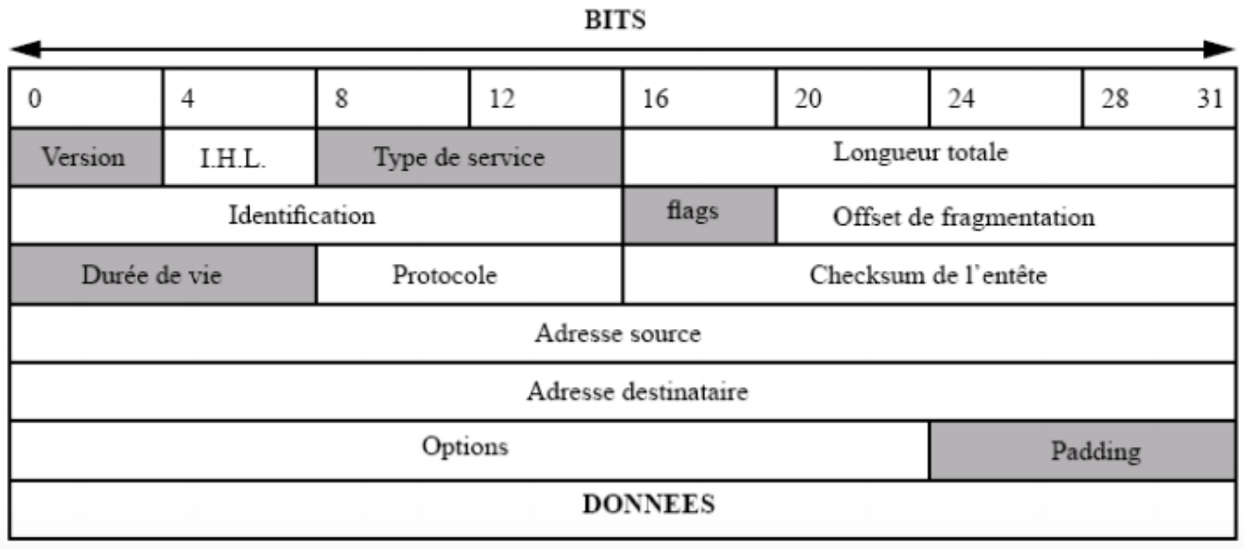
Rappel TCP/IP



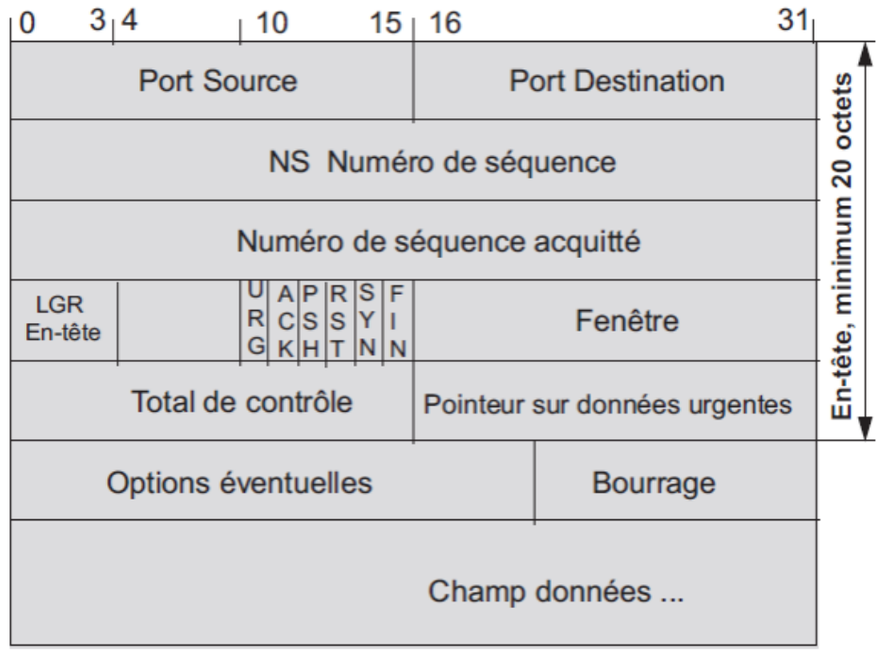
Rappel TCP/IP

Entête

Entête IP



Entête TCP



Rappel TCP/IP

Exemples de numéros de ports

Numéro de Port	Protocol et service
20	File Transfer Protocol (FTP) (Data Port)
21	File Transfer Protocol (FTP) (Control Port)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67 and 68	BootStrap Protocol (BOOTP); also used by the Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
119	Net News Transfer Protocol (NNTP)
137, 138, and 139	NetBIOS Name Service (Windows operating systems)
143	Internet Message Access Protocol version 4 (IMAP4)
161 and 162	Simple Network Management Protocol (SNMP)
389	Lightweight Directory Access Protocol (LDAP)
443	Secure Socket Layer (SSL) or HTTPS

Address Resolution Protocol

ARP

Résoud les adresses IPv4 en adresses physiques locales.

- Adresse IPv4 : 32 bits, écriture en décimal pointé de 4 octets : 192.168.1.1
- MAC : 48 bits, écriture en six nombres hexadécimal 02:12:4f:10:c1:56

Cache arp : se souvenir des MAC en fonction des IP pour éviter les requêtes ARP.

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/protocols,
- /etc/services
- /etc/hosts
- /etc/networks
- /etc/resolv.conf

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/protocols,

Permettre aux programmes de convertir les noms des protocoles en leurs nombres.

```
ip      0       IP # internet protocol, pseudo protocol number

icmp    1       ICMP # internet control message protocol

igmp    2       IGMP # internet group multicast protocol

ggp     3       GGP # gateway-gateway protocol

tcp     6       TCP # transmission control protocol

pup     12      PUP # PARC universal packet protocol

udp     17      UDP # user datagram protocol
```

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/services,

Permettre aux programmes de convertir les noms des services en leurs nombres (numéros des ports).

```
tcpmux          1/tcp # rfc-1078
echo             7/tcp
echo             7/udp
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp # SSH Remote Login Protocol
ssh             22/udp # SSH Remote Login Protocol
telnet          23/tcp # Telnet telnet 23/udp # Telnet
```

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/services,

Permettre aux programmes de convertir les noms des services en leurs nombres (numéros des ports).

```
tcpmux          1/tcp # rfc-1078
echo             7/tcp
echo             7/udp
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp # SSH Remote Login Protocol
ssh             22/udp # SSH Remote Login Protocol
telnet          23/tcp # Telnet telnet 23/udp # Telnet
```

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/network/interfaces,

La configuration d'un réseau peut être fait en passant par le fichier de configuration interfaces du répertoire **/etc/network/interfaces**.

Permet de donner à la carte de réseau une adresse IP statique ou dynamique (dhcp), configurer les informations de routage ou le masquage d'IP, le routage par défaut et bien d'autres paramètres.

La configuration des interfaces peut se faire en ligne de commande avec la commande **ifconfig** avec le paquet **net-tools**

iwconfig permet de configurer les interfaces sans-fils

Configuration de base de la pile TCP/IP

Les commandes habituelles dépréciées :

* arp ==> **ip** neigh show
* ifconfig. ==> **ip** address show
* route ==> **ip** route show
* netstat ==> **ss** (dumps socket statistics)

* iwconfig est dépréciée? mais répond encore

beaucoup passera par la commande **ip**

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/network/interfaces,

Configuration statique IPv4

```
auto eth0
  iface eth0 inet static
      address 192.0.2.7
      netmask 255.255.255.0
      gateway 192.0.2.254
```

Configuration dynamique IPv4

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

Configuration statique IPv6

```
iface eth0 inet6 static
      address 2001:db8::c0ca:1eaf
      netmask 64
      gateway 2001:db8::1ead:ed:beef
```

Configuration dynamique IPv6

```
iface eth0 inet6 dhcp

iface eth0 inet6 auto
```

Configuration de base de la pile TCP/IP

Fichiers de configuration

- /etc/network/interfaces,

% ifconfig [interface] [adresse] [options]

Exemples

– ifconfig eth0 192.168.2.9 netmask 255.255.255.0 up

– ifconfig eth0:0 10.0.8.10

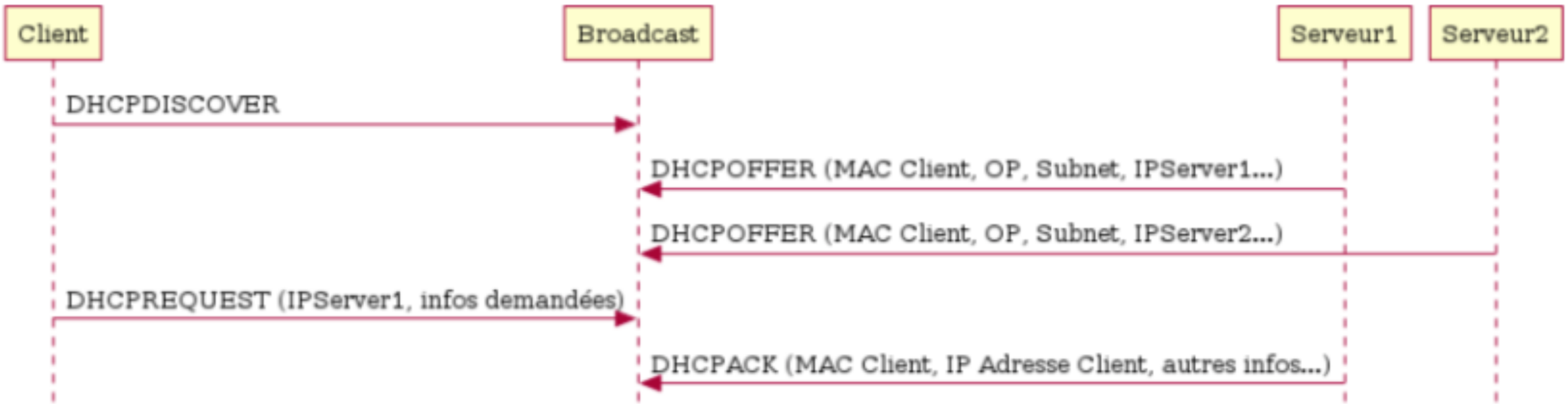
%ip address add adresse/prefixe dev interface

ip address add 192.168.0.77/24 dev eth0

Service DHCP

- Dynamic Host Configuration Protocol
- Distribuer les informations nécessaires à l'arrivée d'une machine sur le réseau => adresse IP, passerelle
- Fonctionne sous UDP
  - Serveur port : 67
  - Client port : 68
- Informations supplémentaires
  - Masque de sous réseau
  - Serveur de nom, de temps, de fichier, de log, d'impression

Service DHCP



- Politiques de distribution
  - Spécifier les intervalles d'IP
  - Choisir une adresse IP en fonction de l'adresse MAC
  - Baux révocables

Service DHCP

- Coté Serveur :
  - Installation de isc-dhcp-server
    - *% apt-get install isc-dhcp-server*
  - Editer le fichier /etc/dhcp/dhcpd.conf
    - Messages d’erreur => sudo tail /var/log/syslog
- Coté client:
  - Utilitaire dhclient [interface]
  - Exemple
    - -linux : *%dhclient eth0*
    - Windows : *% ipconfig /renew*

Service DHCP

- Exemple de configuration coté serveur

```
# /etc/network/interface
# L'interface réseau « loopback » (toujours requise)
auto lo
iface lo inet loopback
# Assigner une adresse IP statique pour ce serveur DHCP avec eth0 :
auto eth0
iface eth0 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

```
#demarrage du service dhcp
sudo service isc-dhcp-server stop
sudo service isc-dhcp-server start
sudo ifdown eth0
sudo ifup eth0
```

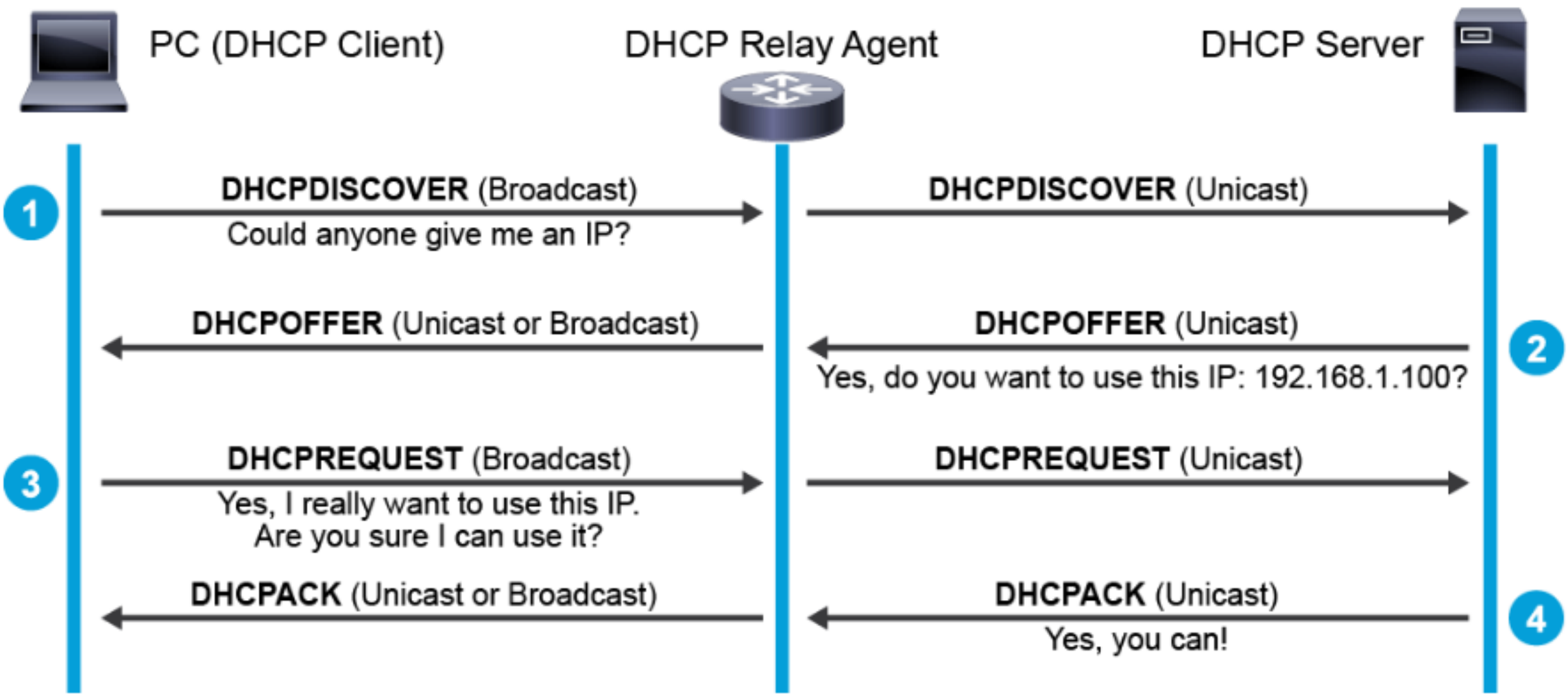
```
#/etc/dhcp/dhcpd.conf

option domain-name "mydebian";

# Utilisation du serveur DNS public de Google

option domain-name-servers 8.8.8.8, 8.8.4.4;

# Configuration de votre sous-réseau (subnet) souhaité :

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.101 192.168.1.254;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.100;
    option domain-name-servers home;
}
default-lease-time 600;
max-lease-time 7200;
# Indique que nous voulons être le seul serveur DHCP de ce réseau :
authoritative;
```

Service DHCP

- Agent de Relais DHCP
  - L'agent de relais DHCP agit en tant qu'intermédiaire et s'assure que les demandes des clients DHCP locaux sont transmises aux serveurs DHCP centralisés.
  - Tous les périphériques compatibles Layer 3 tels que les routeurs ou les commutateurs peuvent fonctionner en tant qu'agent de relais DHCP.
  - La principale fonction d'un agent de relais DHCP est de transférer les messages DHCP des clients locaux au serveur DHCP distant

Service DHCP

- Agent de Relais DHCP



Service DHCP

- Agent de Relais DHCP
  - Lorsqu'un agent de relais DHCP reçoit un paquet de diffusion d'un client connecté, il examine le champ **giaddr**. Si le champ a une adresse IP de 0.0.0.0, l'agent de relais DHCP change le champ **giaddr** des paquets DHCP de zéro à l'adresse IP de l'agent de relais et transmet le message au sous-réseau distant où se trouve le serveur DHCP.
  - Le serveur DHCP utilise cette adresse IP pour sélectionner un pool d'adresses IP à partir duquel attribuer les adresses IP au client DHCP.
  - Les paquets de retour du serveur DHCP sont directement envoyés à l'agent de relais identifié dans le champ **giaddr**. L'agent de relais DHCP transmet ou transmet la réponse au client DHCP.

Service de routage

- Routage
  - Trouver des routes (chemins) dans un réseau (graphe) pour acheminer les donnée
    - génère des tables de routage qui sont utilisées par chaque noeud
    - Algorithme : trouver les plus courts chemins
- Afficher les tables de routage (sous linux) :
  - netstat -r
  - ip route show (à partir de debian 9)

Service de routage

- Fonction de routage sous linux
  - La fonction de routage est activée par :

sysctl -w net.ipv4.ip_forwad=1

- Remarques:
  - Pour rendre permanente la modification, décommenter la ligne **net.ipv4.ip_forwad=1** du fichier **/etc/sysctl.conf**
  - La commande **sysctl -p** permet de recharger les valeurs présentes dans le fichier /etc/sysctl.conf
  - *% sysctl net.ipv4.ip_forwad* permet de connaitre la valeur associée

Service de routage

- Fonction de routage sous linux
  - Une fois la fonction de routage activée, la table de routage doit être configurée de façon cohérente
  - Routes courantes obtenues via la commande **ip route**

```
default via 10.9.8.254 dev enp0s3 onlink
10.9.8.0/22 dev enp0s3 proto kernel scope link src 10.9.8.200
169.254.0.0/16 dev enp0s3 scope link metric 1000
```

- Ancienne commande : % **route -n**

Service de routage

- Fonction de routage sous linux
  - Ajouter une passerelle par défaut

% *ip route add default <Adresse IP de la passerelle>*

- Ancienne commande :

% *route add default gw <Adresse IP de la passerelle>*

Service de routage

- Fonction de routage sous linux
  - Ajouter une route statique vers un réseau

    % *ip route add <IP>/<MASK> via <GW> dev <interface>*
  - ou bien éditer le fichier /etc/network/interfaces et ajouter les lignes de routages
- Suppression d'une route :

  % *ip route del <IP>/<MASK>*
- Anciennes commandes :

  % *route add -net <IP> netmask <MASK> gw <GW> dev <interface>*

  % *route del -net <IP> netmask <MASK>*

Service de routage

- Routage dynamique: quagga
  - Implémentation libre de protocoles de routages dynamiques (RIP, OSPF, BGP)
  - Fichier de configuration :
    - /etc/quagga/zebra.conf : fichier de conf principal
    - /etc/quagga/deamons : liste des protocoles de routage
    - /etc/quagga/debian.conf : options pour le lancement des processus associés
    - chaque algorithme est configuré dans un fichier. Ex: /etc/quagga/ospfd.conf
- Packagé sous debian

% apt-get install quagga

- Les exemples de configurations de routage sont localisés dans

% /usr/share/doc/quagga-core/examples

vtysh_enable=yes zebra=yes bgpd=yes ospfd=no ospf6d=no ripd=no ripngd=no isisd=no

Service de routage

```
# Exemple du fichier /etc/quagga/deamons
vtysh_enable=yes
zebra=yes
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
```

```
#démarrage du service quagga
sudo /etc/init.d/quagga restart
Ou
sudo systemctl restart zebra
```

```
# Exemple du fichier /etc/quagga/debian.conf
/etc/quagga/debian.conf
vtysh_enable=yes
zebra_options=" --daemon -A 127.0.0.1 -P 2601 -u quagga -g quagga"
bgpd_options=" --daemon -A 127.0.0.1 -P 2605 -u quagga -g quagga --retain -p 179"
ospfd_options=" --daemon -A 127.0.0.1 -P 2604 -u quagga -g quagga"
ospf6d_options=" --daemon -A ::1 -P 2606 -u quagga -g quagga"
ripd_options=" --daemon -A 127.0.0.1 -P 2602 -u quagga -g quagga"
ripngd_options=" --daemon -A ::1 -P 2603 -u quagga -g quagga"
isisd_options=" --daemon -A 127.0.0.1 -P 2608 -u quagga -g quagga"
babeld_options=" --daemon -A 127.0.0.1 -P 2609 -u quagga -g quagga »<<
```

Parfeu
Motivation

- Protéger le réseau ou une machine contre:
  - Intrusion de l'extérieur
  - Opérations internes non souhaitées
  - Paquets erronés
  - Déni de service

- Permettre néanmoins des communications

Parfeu
Principe

- Filtrage : choisir pour un paquet, si l'on va
  - l'accepter si on est le destinataire
  - l'acheminer vers sa destination
    - le jeter
    - y répondre négativement
    - le logguer
- Firewalls entre un ou plusieurs réseaux

Parfeu

Critères de filtre

- Usage du réseau ?
  - Déduire les flux utilisés
- critères de filtre des paquets
  - Facilité de forger des paquets
  - Difficultés de représenter tout ce qui se passe sur le réseau

Parfeu

Filtrage simple de paquets

- On a un paquet, on se base sur ses informations
  - IP
  - UDP/TCP
  - Type de trames
  - aucunes connaissances des paquets déjà passés

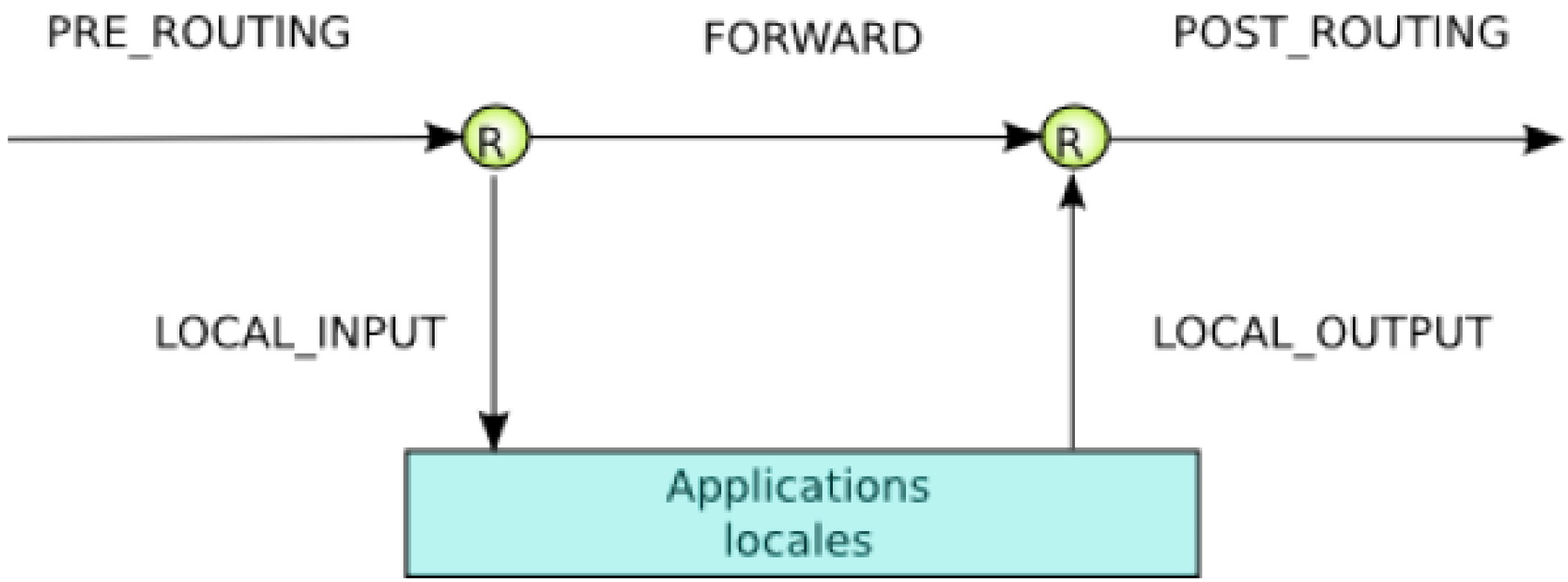
Parfeu
Autres usages

- NAT/PAT
  - NAT : Translation d'adresses IP à la volet
  - PAT : translation de ports
  - sNAT : NAT à la source / Masquerading
  - dNAT : NAT de la destination => DMZ

Parfeu

implémentation sous linux

- Netfilter
- Iptable
- Hooks : endroit dans la couche réseau pour recevoir des chaines => points de passage des paquets



Parfeu

implémentation sous linux

- Tables de filtrage : ensemble de chaines
- Table par défaut filter
- Chaines : un ensemble de règles que va subir un paquet :
  - Règle évaluée dans l'ordre
- Exemple : filter a les chaines : INPUT, FORWARD et OUTPUT

Parfeu

implémentation sous linux

- Notion de règles :
  - Partie sélection du paquet (motif, match)
    - Adresses MAC/IP/, source destination
      - Port
      - Temps
  - Partie décision (Verdict ou target)
    - ACCEPT, DROP, REJECT, RETURN, LOG

Parfeu

implémentation sous linux

- Verdict

ACCEPT	Accepte le paquet
DROP	Poubelle en silence
REJECT	Refuse poliment le paquet
RETURN	Retour à la chaîne appelante
LOG	Log (via syslog) et continue les règles
DNAT	Réécrit la destination
SNAT	Cache la source
MASQUARADE	Cas particulier de SNAT où source = passerelle

Parfeu

implémentation sous linux

- Lister les règles iptables

  iptable –L

  Iptable –L INPUT #Lister une chaine

  Iptable –L –t nat # Lister une table

- Option – n permet d’éviter les résolutions de noms dns

Parfeu

implémentation sous linux

Option iptables pour Ajout/Retrait de règles

-F *chaîne*	Vide (*flush*) *chaîne*
-A *chaîne*	Ajoute la règle à *chaîne* (fin)
-I *chaîne position*	Ajoute la règle à *chaîne* à la position *position*
-D *chaîne num*	Détruit la *num*-ième règle de *chaîne*

Option iptables pour choix de la table

-t *table*	**filter, nat, mangle, raw, security**
filter	Table par défaut: Chaînes INPUT, FORWARD, OUTPUT
nat	Pour nouvelle connexion. Chaînes PREROUTING, POSTROUTING
mangle	Table pour la modification de paquet. Toutes chaînes
raw	Exceptions ...
security	Voir SELinux...

Parfeu

implémentation sous linux

Activer le relayage de paquets

```
echo "1" > /proc/sys/net/ipv4/ip_forward

modprobe ip_tables
modprobe ip_conntrack
# modprobe ip_conntrack_ftp
```

Grand ménage (vidage des tables et chaines)

```
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F POSTROUTING -t nat
iptables -F PREROUTING -t nat
```

Autoriser un serveur web et ssh

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT     # ssh
iptables -A INPUT -p tcp --dport 80 -j ACCEPT     # apache
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT  # ICMP
```

Laisser revenir les ack

```
iptables -A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
```

Laisser revenir les connexions

```
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state RELATED -j ACCEPT
```

Interdire le reste

```
iptables -A INPUT -i eth2 -j REJECT
```

Parfeu

implémentation sous linux

Port forwading et port masquerading

```
iptables -t nat -A PREROUTING -p tcp -d $PUBLIC --dport 80 -j DNAT --to $WEB
iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
```

FIN COURS