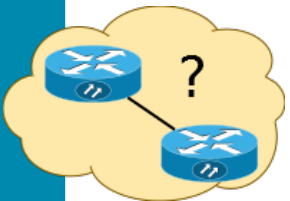


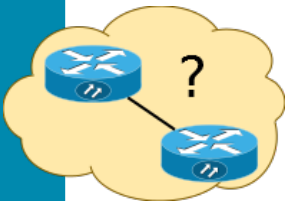
05 : DHCP - iptables

- Services réseaux les plus importants
 - NAT (traduction adresses IPs)
 - DNS (résolution de nom)
 - DHCP (attribution IPs dynamiques)
- Pourquoi sont-ils si importants ?



05 : DHCP

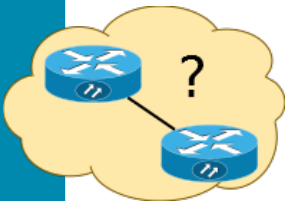
- DHCP utilisé
 - Envoi automatique des informations IP à une machine
 - Adresse IP - masque
 - Passerelle par défaut
 - Serveur DNS
 -



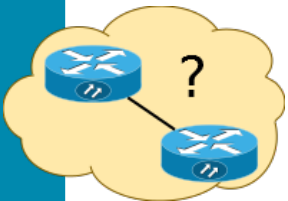
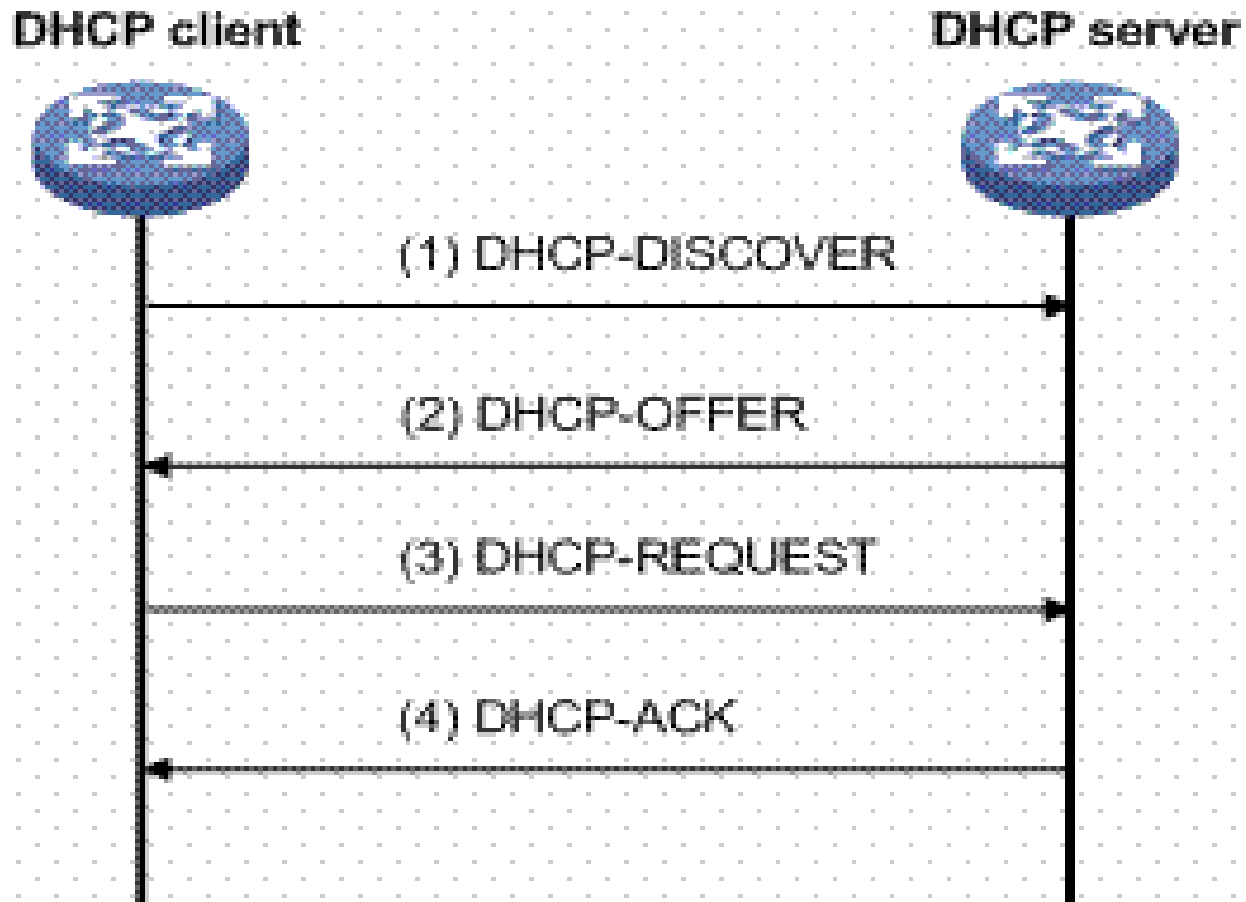
05 : DHCP

- Configuration DHCP
 - `/etc/dhcp3/dhcpd.conf`

```
# distribution d'adresses IP 10.0.0.0/8
subnet 10.0.0.0 netmask 255.0.0.0 {
# restriction de la distribution au range défini
range 10.0.0.10 10.0.0.250 ;
# envoi de la passerelle par défaut (gateway)
option routers 10.0.0.1 ;
}
```
 - démarrer le serveur DHCP
 - `/etc/init.d/dhcp3-server start`

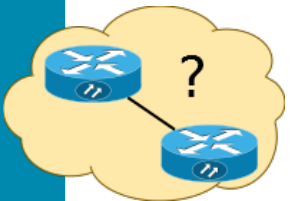


05 : DHCP



05 : DHCP

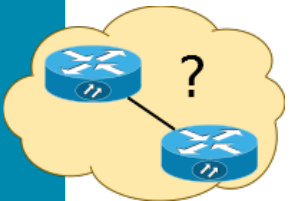
- DHCP remarque importante !!!
 - Le DHCP utilise le broadcast
 - Le broadcast ne traverse jamais les routeurs → DHCP relay



05 : DHCP

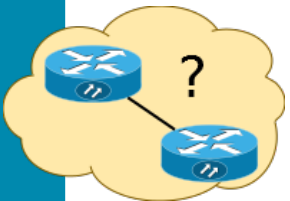
- Configuration DHCP avec DNS
 - `/etc/dhcp3/dhcpd.conf`

```
# distribution d'adresses IP 10.0.0.0/8
subnet 10.0.0.0 netmask 255.0.0.0 {
# restriction de la distribution au range défini
range 10.0.0.10 10.0.0.250 ;
# envoi de la passerelle par défaut (gateway)
option routers 10.0.0.1 ;
option domain-name « reseau.truc.brol.be » ;
option domain-name-servers 10.0.0.1 ;
}
```



05 : IPTABLES

- 3 chaînes
 - INPUT : trafic entrant
 - FORWARD : trafic de redirection
 - OUTPUT : trafic sortant
- L'ordre des règles a de l'importance
- Pare-feu à état
- 3 tables
 - mangle
 - nat
 - filter (table par défaut)



05 : IPTABLES

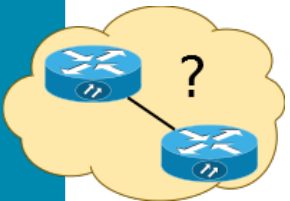
- Commandes principales
 - Afficher les règles :

```
iptables -L -n -v -line-numbers
```
 - Définir la politique par défaut d'une chaîne

```
iptables -P OUTPUT DROP
```
 - Ajouter une règle

```
iptables -A INPUT -p TCP --dport 22 -j ACCEPT
```

```
iptables -A INPUT -p icmp -j ACCEPT
```

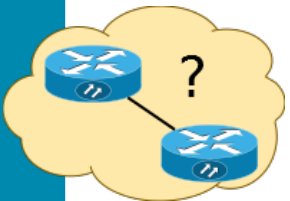


05 : IPTABLES

- Ajouter une règle

```
iptables -A INPUT -p TCP --dport 22 -j  
ACCEPT
```

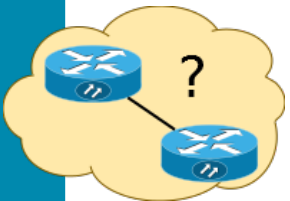
```
iptables -A INPUT -p icmp -j ACCEPT
```



05 : IPTABLES

- Options

- -A : chain (INPUT / OUTPUT / FORWARD)
- -p : protocol (udp, tcp, icmp)
- --dport, --sport : port destination ou source
- -j : décision (ACCEPT / REJECT / DROP)
- -d : destination (192.168.1.0/24)
- -s : source (192.168.1.0/24)
- -i : interface (eth0, lo, ...)



05 : IPTABLES

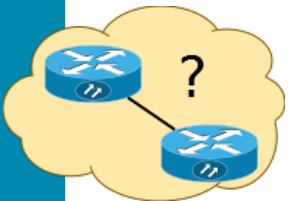
- Supprimer une règle

```
iptables -D INPUT 5
```

- Insérer une règle

```
iptables -I INPUT 1 -p tcp --dport 80 -j  
ACCEPT
```

- Line-numbers !!!



05 : IPTABLES

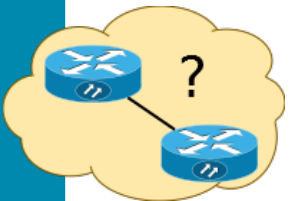
- Supprimer une règle

```
iptables -D INPUT 5
```

- Insérer une règle

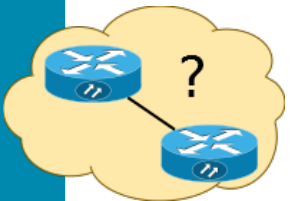
```
iptables -I INPUT 1 -p tcp --dport 80 -j  
ACCEPT
```

- Line-numbers !!!



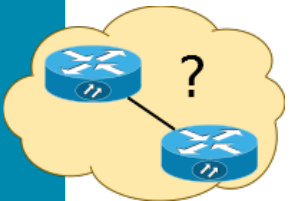
05 : IPTABLES

- Règles avec état
 - `iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
- NEW, ESTABLISHED, RELATED



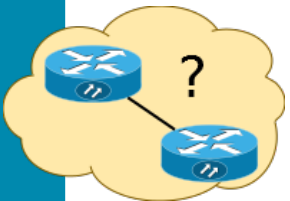
05 : IPTABLES

- Logging
 - `iptables -A OUTPUT -j LOG`
 - `iptables -A OUTPUT -j DROP`
- A placer à l'endroit adéquat !



05 : IPTABLES

- Règles avec état
 - `iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
- NEW, ESTABLISHED, RELATED



05 : IPTABLES

- Script au démarrage
 - Les règles iptables doivent être placées dans un script au démarrage → configuration permanente
 - Netkit → fichiers .startup

