

OVS: Lab 3 NAT avec Openflow

Objet	mise en place d'un NAT à l'aide d'Open vSwitch.
Niveau requis	débutant, avisé
Débutant, à savoir	ovs-openflow-overview
Suivi	:DRAFT:

Un routeur fait du network address translation (NAT) (« traduction d'adresse réseau » ou « translation d'adresse réseau ») lorsqu'il fait correspondre des adresses IP à d'autres adresses IP. En particulier, un cas courant est de permettre à des machines disposant d'adresses qui font partie d'un intranet et ne sont ni uniques ni routables à l'échelle d'Internet, de communiquer avec le reste d'Internet en faisant semblant d'utiliser des adresses externes uniques et routables.

Ainsi, il est possible de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, afin de pallier l'épuisement des adresses IPv4.

La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale.

Ce procédé est très largement utilisé par les box internet (ou modem routeur) des fournisseurs d'accès pour cacher les ordinateurs domestiques derrière une seule identification publique. Il est également utilisé de façon similaire dans des réseaux privés virtuels

OVS prend en charge cette fonction avec OpenFlow . Un flux avec des actions NAT (changement d'adresse IP ou de port L4) peut être matériellement commuté. Les flux peuvent être associés aux actions suivantes: `mod_nw_dst`, `mod_nw_src`, `mod_tp_dst` et `mod_tp_src`.

NAT avec l'action nat

Dans OVS, NAT peut être configuré à l'aide de l'action openflow nat, qui fait partie du mécanisme de suivi de connexion (action ct).

NAT plusieurs-à-un

En utilisant l'outil `ovs-ofctl`, NAT dans OVS peut être configuré comme suit:

```
ovs-ofctl add-flow br0 idle_timeout=0,in_port=2,ip,action="ct(commit,zone=1,nat(src=12.34.56.78)),1"
```

Dans cet exemple, une seule adresse IP est spécifiée pour la traduction. Par conséquent, toutes les adresses sources "privées" seront traduites vers cette adresse particulière.

NAT plusieurs-à-plusieurs

C'est un autre exemple de configuration NAT. Cette fois, les adresses IP "privées" sont converties en

adresses IP sélectionnées dans la plage d'adresses spécifiée entre 12.34.56.64 et 12.34.56.79:

```
ovs-ofctl add-flow br0 idle_timeout=0,in_port=2,ip,action="ct(commit,zone=1,nat(src=12.34.56.64-12.34.56.79)),1"
```

L'adresse IP finale utilisée pour la traduction est sélectionnée par l'algorithme interne du mécanisme NAT. Cette adresse sélectionnée est ensuite utilisée pour traduire l'adresse IP source des paquets. Il n'y a aucun moyen de prédire quelle adresse IP sera sélectionnée dans la plage fournie.

NAT avec les actions mod

les actions `mod_nw_dst` et `mod_nw_src` permettent de faire du NAT à l'intérieur des switches OpenFlow

```
# Modification de l'adresse source du flux spécifié en utilisant mod_nw_src
ipv4
ovs-ofctl add-flow <bridge> <match-field> actions=mod_nw_src:<ip>
# Modification de l'adresse dest du flux spécifié en utilisant mod_nw_dst
ipv4
ovs-ofctl add-flow <bridge> <match-field> actions=mod_nw_dst:<ip>
```

Dans l'exemple suivant :

```
$ sudo ovs-vsctl set-controller br0 tcp:0.0.0.0:6633
$ sudo ovs-ofctl show br0
$ sudo ovs-ofctl dump-flows br0
$ sudo ovs-ofctl add-flow br0 "table=0 ip dl_type=0x0800 nw_proto=6
tp_dst=80 nw_dst=140.120.15.180 idle_timeout=0
action=mod_nw_dst:192.168.180.10,normal"
$ sudo ovs-ofctl add-flow br0 "table=0 ip dl_type=0x0800 nw_proto=6
tp_dst=80 nw_src=192.168.180.10 idle_timeout=0
action=mod_nw_src:140.120.15.180,normal"
$ sudo ovs-ofctl del-flows br0
Delete all flows and then insert initial flow.
$ sudo ovs-ofctl del-flows brLAN ; sudo ovs-ofctl add-flow brLAN
"table=0,priority=0,action=normal"
```

L'adresse dst 140.120.15.180 est natée vers l'adresse interne 192.168.180.10 et l'adresse src 192.168.180.10 est natée vers l'adresse externe 140.120.15.180

From:

<http://vps101364.serveur-vps.net/> - **dwndoc**

Permanent link:

<http://vps101364.serveur-vps.net/doku.php?id=labs:ovs-lab-3-nat>

Last update: **2025/02/19 10:59**

