Récupérer des débits, via SNMP, sur JunOS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 avril 2013

https://www.bortzmeyer.org/rate-mib-juniper.html

Le protocole de gestion de réseau SNMP permet de récupérer la valeur de compteurs sur une machine distante. Ces compteurs sont en général des valeurs cumulées, pas des débits et le gestionnaire SNMP doit donc faire plusieurs requêtes, puis calculer le débit lui-même. Est-il possible de récupérer des débits directement ?

SNMP est normalisé (pour sa version 3, utilisée ici) dans le RFC 3411 [1] et suivants. Mais ces RFC ne normalisent que le protocole. Le modèle de données (arborescent) est dans le RFC 2578. Et la liste des variables qu'on peut récupérer en SNMP est décrite dans des MIB dont la plus célèbre est la standard MIB-II, décrite dans le RFC 1123. Elle offre un certain nombre de variables par interface, comme `ifInOctets` (nombre d'octets étant rentrés via cette interface), `ifOutUcastPkts` (nombre de paquets "*unicast*" sortis par cette interface), etc. Ces variables ont en commun d'être des compteurs depuis un instant T (typiquement le démarrage de la machine). En général, on est plutôt intéressés par le débit que par le nombre total d'octets ou de paquets. Les programmes comme Cacti, qui affichent des jolis graphes, interrogent à intervalles réguliers l'agent SNMP (la machine surveillée) et calculent ensuite des débits.

Ce n'est pas très pratique lorsqu'on veut déclencher des alarmes (par exemple depuis un logiciel de supervision comme Icinga <https://www.bortzmeyer.org/icinga.html>). Les scripts de surveillance n'ont pas de mémoire et stocker des résultats sur disque n'est pas pratique (si vous utilisez les "*plugins*" Nagios officiels, `check_snmp` a une option `--rate` qui peut servir : lisez la section "*Rate calculation*" de sa documentation.) Peut-on récupérer ces débits directement sur l'agent ?

À ma connaissance, pas de manière standard. Le but de SNMP est de pouvoir tourner sur des machines simples, ayant peu de moyens. Pas question donc de devoir retenir des valeurs compliquées, ou de faire des calculs. Je crois qu'il n'existe rien dans les MIB standards.

Mais ce n'est pas la fin de l'histoire. Tout équipement réseau met en œuvre des MIB non standards qui offrent en général des tas de possibilités supplémentaires intéressantes, dans le sous-arbre `1.3.6.1.4.1` du SMI, sous-arbre dit `enterprises`. Essayons sur un commutateur/routeur Juniper SRX, avec JunOS. Un examen de la MIB Juniper <http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-if-extensions.txt> montre des variables prometteuses :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc3411.txt`

```
ifIn1SecRate OBJECT-TYPE
SYNTAX      Gauge32
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
"The number of bits per second (bps), delivered by
this (sub-)layer to its next higher (sub-)layer."
::= { ifJnxEntry 1 }
```

Il reste à configurer l'engin pour faire du SNMP. Cela ressemble à :

```
snmp {
    location "Dans le nuage";
    contact "Happy Sysadmin";
    v3 {
        usm {
            local-engine {
                user USERNAME {
                    authentication-md5 {
                        authentication-key "SECRETDATA";
                    }
                }
            }
        }
        vacm {
            security-to-group {
                security-model usm {
                            }
                        }
                    }
                }
            }
        }
        snmp-community all {
            security-name all;
        }
    }
    view all {
        oid .1 include;
        oid system include;
        oid internet include;
    }
}
```

Si vous ne connaissez pas JunOS, notez que, pour obtenir ce résultat, il a fallu charger ce fichier, ou bien taper dans la console une série de commandes comme :

```
set snmp v3 usm local-engine user USERNAME authentication-md5 authentication-password MOTDEPASSESECRET
```

Testons que cela marche avec Net-SNMP sur le routeur d'adresse IP `198.18.0.2` :

```
% snmpget -v3 -u USERNAME -a MD5 -A MOTDEPASSESECRET \
      -l authNoPriv 198.18.0.2 1.3.6.1.4.1.2636.3.3.1.1.3.513
SNMPv2-SMI::enterprises.2636.3.3.1.1.3.513 = Gauge32: 11965
```

Deux explications : l'OID a été trouvé manuellement en suivant la MIB (2636 = Juniper). La liste complète des variables qui m'intéressent est :

```
1.3.6.1.4.1.2636.3.3.1.1.1.ifIndex :  in rate bits/s
1.3.6.1.4.1.2636.3.3.1.1.2.ifIndex :  in rate bytes/s
1.3.6.1.4.1.2636.3.3.1.1.3.ifIndex :  in rate packets/s
1.3.6.1.4.1.2636.3.3.1.1.4.ifIndex : out rate bits/s
1.3.6.1.4.1.2636.3.3.1.1.5.ifIndex : out rate bytes/s
1.3.6.1.4.1.2636.3.3.1.1.6.ifIndex : out rate packets/s
```

Pour trouver le `ifIndex`, on peut demander au Juniper avec `show interface`. Ou tout afficher avec snmpwalk et regarder les noms des interfaces.

L'affichage de l'OID ci-dessus est un peu triste et on voudrait plutôt avoir les noms des variables de la MIB Juniper. Il faut donc copier celle-ci localement. Sur une machine Debian ou Ubuntu, le plus simple est d'installer le paquetage `snmp-mibs-downloader`, de copier le fichier de configuration d'exemple `/usr/share/doc/snmp-mibs-downloader/examples/junos.conf` et `/usr/share/doc/snmp-mibs-download` dans `/etc/snmp-mibs-downloader`, et de faire un `download-mibs junos`. Après, on indique à snmpget d'utiliser cette MIB :

```
% snmpget  -v3 -M +/var/lib/mibs/juniper -m JUNIPER-IF-MIB -u USERNAME \
        -a MD5 -A MOTDEPASSESECRET  -l authNoPriv 198.18.0.2 \
        1.3.6.1.4.1.2636.3.3.1.1.3.513
JUNIPER-IF-MIB::ifIn1SecPkts.513 = Gauge32: 11914
```

Et voilà, on a un joli nom de variable (nombre de paquets/seconde).

Un exemple pendant une période d'activité (en fait, un test d'attaque DNS par réflexion) ? 511 est l'interface où est connectée la victime de l'attaque, 512 celle où est connecté le réflecteur :

```
% snmpget  -v3 -M +/var/lib/mibs/juniper -m JUNIPER-IF-MIB -u USERNAME -a MD5 -A MOTDEPASSESECRET  -l authNoPriv
JUNIPER-IF-MIB::ifOut1SecPkts.512 = Gauge32: 2721

% snmpget  -v3 -M +/var/lib/mibs/juniper -m JUNIPER-IF-MIB -u USERNAME -a MD5 -A MOTDEPASSESECRET  -l authNoPriv
JUNIPER-IF-MIB::ifOut1SecPkts.511 = Gauge32: 5358
```

À cause de la fragmentation, il y a deux fois plus de paquets qui sortent du réflecteur qu'il n'en entre.

Et les autres variables ? Par exemple le débit en bits/s :

```
JUNIPER-IF-MIB::ifOut1SecRate.511 = Gauge32: 98481600
```

Presque 100 Mb/s, le maximum de la carte Ethernet en face.

Merci à Jean-Philippe Pick pour sa recherche (réussie) dans les MIB.