Klask : un outil dédié à la cartographie du réseau local

Gabriel Moreau
Laboratoire des Ecoulements Geophysiques et Industriels (LEGI)
1023 rue de la piscine, BP53, 38041 Grenoble Cedex, France
Gabriel.Moreau@legi.inpg.fr

Résumé

Malgré la grande variété d'outils réseaux disponibles, l'administrateur d'un site de taille moyenne se retrouve rapidement devant les problématiques suivantes : où se trouve la machine qui a un problème de sécurité urgent à résoudre ? Quels sont les ports des commutateurs qui doivent être tagués pour qu'un VLAN soit transporté d'un commutateur vers un autre ?

Ces deux problématiques nécessitent de connaître la cartographie du réseau local, c'est à dire de savoir sur quels ports des commutateurs sont connectés les machines et les matériels actifs du réseau.

Afin de n'avoir plus à maintenir une version papier peu fiable, nous avons développé un outil dont les principales fonctions sont : trouver les connections entre commutateurs ; dessiner une carte du matériel actif sur le réseau local ; dresser un inventaire précis du port et du commutateur sur lequel est connectée chaque machine du réseau local.

Mots clefs

Cartographie, Réseau, Scanner, Commutateur, SNMP, VLAN

1 Introduction

De très nombreux outils réseaux existent mais la plupart permettent de tracer des cartographies de réseau basées sur la notion de route. Au niveau d'un réseau local commuté, cette notion de route n'apporte rien et ce genre d'outil n'est en général pas capable de structurer la carte locale des machines. L'administrateur d'un site de taille moyenne, quelques bâtiments, une quinzaine de commutateurs, se retrouvent rapidement devant les problématiques suivantes :

- Où est positionnée la machine *X ?* Elle est à l'origine d'un problème réseau urgent à traiter, quitte à la déconnecter en désactivant le port du commutateur ;
- Deux machines *A* et *B* de mon réseau local ne dialoguent pas. Quel est le chemin physique menant de la machine *A* vers la machine *B* ?

Rapidement, lorsque son parc machine augmente, il devient difficile de maintenir une version papier à jour de son réseau local, notamment s'il y a des mouvements de personnel... Il est possible d'améliorer les choses en configurant le matériel actif de manière à n'associer certaines adresses physiques (MAC) de machine qu'à certains ports de commutateur. Cependant, cela ne résout pas forcément tous les problèmes, notamment le second.

Les deux problématiques énoncées sont liées et une solution simple consiste à savoir sur quels ports des commutateurs sont connectés les machines et les matériels actifs dans un réseau local.

Des outils comme *traceroute* ne sont d'aucune aide sur le réseau local car l'information sur les routes ne permet pas d'en déduire les commutateurs par lequel transite les flux. Nous avons donc développé un outil nommé Klask. Ce mot signifie en Breton : "rechercher" et c'est exactement ce que nous voulions. Klask est un outil dont les deux principales fonctions sont :

- trouver les connexions entre commutateurs et de dessiner une carte du matériel actif sur le réseau local ;
- dresser un inventaire précis du port et du commutateur sur lequel sont connectés les machines du réseau local.

Klask est un petit outil, dans l'esprit des outils UNIX, de ne se préoccuper que des connections sur le réseau local.

2 Fonctionnement

Klask s'utilise en ligne en commande. Il est articulé autour des quatre fonctions principales : *updatesw*, *exportsw*, *updatedb*, *exportdb*. Ces fonctions agissent sur deux bases de données en fonction d'un fichier de configuration global.

3 Cartographie des commutateurs

3.1 Base de données des commutateurs

On ne s'intéresse qu'aux commutateurs ethernet *administrables par SNMP* qui seront simplement appelés par la suite commutateur. Les autres commutateurs, ne pouvant être interrogés, ne seront pas pris en compte dans notre cartographie. Il existe aujourd'hui des équipements réseaux n'ayant qu'une interface d'administration web. Ceux-ci seront peut-être pris en charge dans Klask dans une future version selon les possibilités de ceux-ci.

La liste des matériels actifs *administrables* doit être donnée dans le fichier de configuration global. Selon le modèle du commutateur, on spécifie dans ce fichier la version du protocole SNMP à utiliser, les paramètres SNMP ainsi que sa position physique (bâtiment, numéro de bureau). Ces données peuvent être globales et/ou surchargées par commutateur (par exemple le paramètre *community* de SNMP) ou bien peuvent-être écrites dans sa configuration interne lorsque cela est possible (par exemple la position géographique du commutateur).

La commande *updatesw* met à jour la base de données des interconnexions entre commutateurs.

```
# klask updatesw
```

En pratique, Klask commence par rechercher l'ensemble des adresse physiques (MAC) des équipements réseaux puis il interroge chaque commutateur afin de connaître sur quels ports de celui-ci sont détectés les autres commutateurs. Enfin un algorithme du type du plus court chemin donne la position respective des différents commutateurs entre-eux.

En précisant dans le fichier de configuration les adresses IP des routeurs, Klask ajoute à cette description des commutateurs les ports de sortie vers ceux-ci.

3.2 Interconnexion des commutateurs

La commande *exportsw* affiche le contenu de la base de données des commutateurs sous le format que l'on choisit.

```
# klask exportsw [-f format]
```

Par défaut, le format est *txt*, mais il est aussi implémenté le format *dot* qui permet de réaliser ensuite une vue graphique du réseau.

Le tableau suivant donne les ports d'interconnexion entre les équipements réseaux ainsi que le sens de la connexion sur un réseau fictif (domaine *exp.loc*). Chaque flêche indique la direction vers la sortie du réseau, en pratique le routeur d'entrée de site. Par exemple, ce tableau montre que le commutateur *sw2A2* est connecté via son port 25 sur le port *D4* du commutateur *sw1A0*, ce dernier étant lié au routeur via son port F1.

```
Switch inter-connection
-----------------------------------
sw1A0.exp.loc A1 <--+ 24 sw1B1.exp.loc
sw1A0.exp.loc D3 <--+ 25 sw1A2.exp.loc
sw1A0.exp.loc D4 <--+ 25 sw2A2.exp.loc
sw1A0.exp.loc F1 +--> router
sw1A2.exp.loc 25 +--> D3 sw1A0.exp.loc
sw2A2.exp.loc 25 +--> D4 sw1A0.exp.loc
sw1B1.exp.loc 23 <--+ 16 sw2B1.exp.loc
sw1B1.exp.loc 24 +--> A1 sw1A0.exp.loc
sw2B1.exp.loc 15 <--+ 16 sw3B1.exp.loc
sw2B1.exp.loc 16 +--> 23 sw1B1.exp.loc
sw3B1.exp.loc 16 +--> 15 sw2B1.exp.loc
```

3.3 Graphe des commutateurs

Le tableau des interconnexions est bien pratique et peut facilement être envoyé par courriel à un collègue mais il ne permet pas d'avoir une vue d'ensemble en quelques secondes. En demandant à Klask une sortie au format *dot* et avec le programme GraphViz, il est possible de générer une carte graphique représentant visuellement ces informations.

```
# klask exportsw -f dot > map.dot
# dot -Tpng map.dot > map.png
```

La figure 1 représente le résultat sur ce cas assez simple. La figure est coupée en deux, la partie haute dans les teintes rouge et jaune est une schématisation du site avec ses bâtiments. La partie inférieur représente les connexions entre commutateurs avec le point de sortie vers internet en bas du graphe. Chaque commutateur de couleur verte est dans un local technique, le port de sortie de celui-ci est de couleur bleu. Les ports d'un commutateur sur lequel sont branchés d'autres matériels actifs sont en violet.

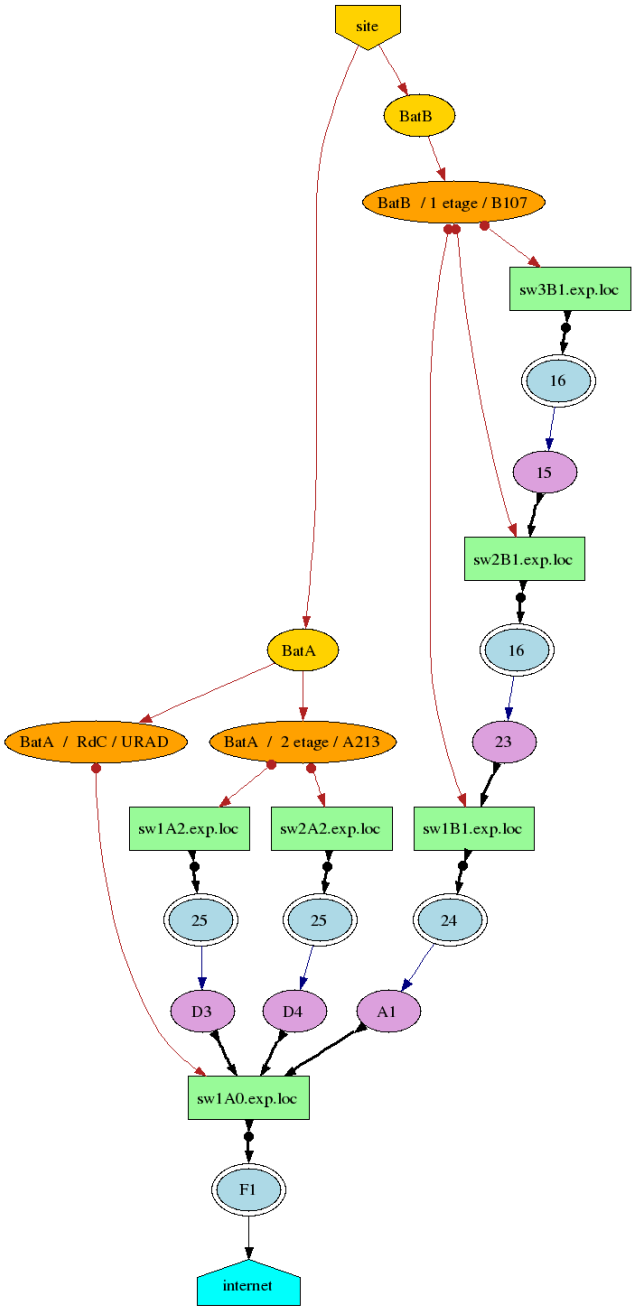

Figure 1 - *Carte des commutateurs*

3.4 Analyse du graphe

Dans ce cas de figure, le graphe est vertical car il est petit mais c'est exceptionnel, la tendance est d'obtenir des graphes larges et peu hauts.

Il est assez facile de faire sur ce cas une critique de la configuration réseau. En effet, on remarque au bâtiment B trois commutateurs cascadés les uns derrières les autres alors que le commutateur *sw3B1* aurait été plus judicieusement placé directement derrière *sw1B1*. Il n'est pas possible cependant de connecter tous les commutateurs du bâtiment B sur le commutateur d'entrée de site comme cela est réalisé pour le bâtiment A pour une raison de coût ; les bâtiments étant généralement interconnectés en fibre optique et le nombre de fibres étant limité.

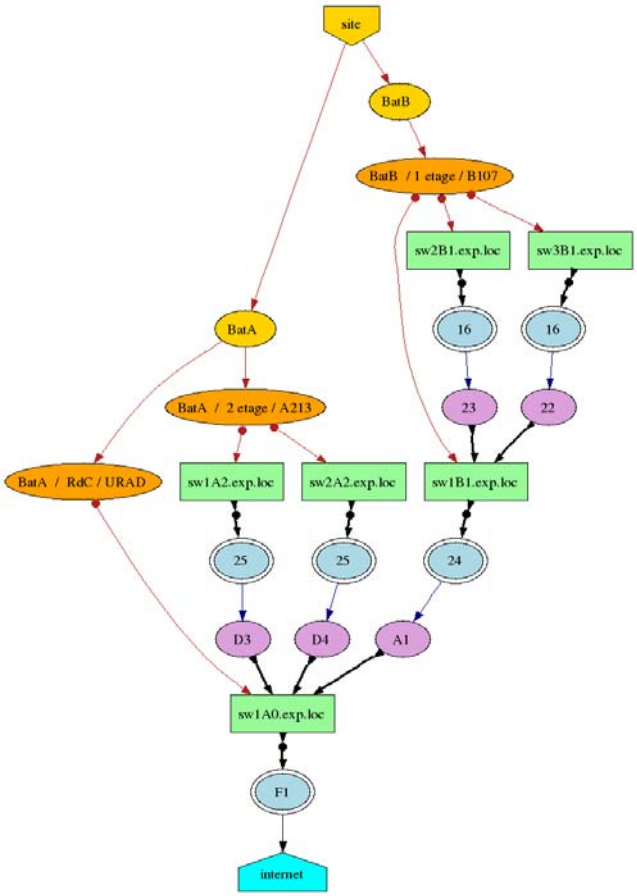

Figure 2 - *Optimisation de la carte*

La figure 2 est le résultat de l'analyse faite avec Klask après avoir physiquement fait ce changement de connexion sur les équipements réseaux du bâtiment B.

4 Cartographie des machines

4.1 Base de données des machines

Avoir la carte des commutateurs ne suffit pas, dans de nombreux cas, il faut connaître sur quel port sont connectées les machines. Klask permet donc de dresser un inventaire précis du port et du commutateur sur lequel sont connectées les machines sur le réseau local. Cependant, les machines, contrairement aux matériels actifs, ne sont pas connectées en permanence sur le réseau et sont bien plus versatiles (plusieurs adresses IP pour une même adresse MAC, changement d'adresse IP...), la date de la dernière détection est donc une information importante à conserver.

Pour le moment Klask ne détecte pas de lui-même une nouvelle machine sur le réseau et doit être lancer régulièrement via une tâche dans le CRON du système, par exemple toutes les deux heures. Par ailleurs, une machine connectée à l'instant *t* sur le réseau dans un bâtiment pourrait très bien être déplacée quelques temps après dans un autre bâtiment. Pour détecter ce déplacement, il faudrait lier l'utilisation de Klask à la mise en place de VMPS sur les commutateurs. Ce choix n'a, pour le moment, pas été pris.

Une machine est identifiée dans Klask via le couple adresse IP – adresse physique (MAC). C'est avec l'adresse physique que l'on retrouve la position d'une machine en interrogeant les commutateurs via SNMP.

Il est possible actuellement d'analyser séquentiellement plusieurs réseaux dans plusieurs VLAN. Cependant, il faut dans ce cas charger la pile *802.1Q* du noyau Linux et configurer une adresse IP virtuelle par VLAN. En effet, le serveur Klask a besoin de communiquer directement avec les machines terminales au niveau ARP afin d'établir de manière fiable la correspondance entre l'adresse IP et l'adresse physique de celles-ci. Klask est pour le moment suffisamment rapide en analysant plus de 1000 adresses IP (dont 400 machines effectives) en moins de 6mn.

Une seule commande met donc à jour la base de données des machines détectées.

```
# klask updatedb
```

Cette commande doit être lancée en ayant une base de données des commutateurs à jour. Cependant, il n'est pas forcément nécessaire de mettre à jour cette dernière toutes les deux heures.

4.2 Tableau des machines

Une autre commande permet l'affichage de la base de données.

```
# klask exportdb
```

Celle-ci envoie sur la sortie standard le tableau suivant :

```
Switch      Port      Hostname      Ipv4-Address
                MAC-Address       Date
-----------------------------------------------
-
sw1A2.exp.loc 17 <--- pc163.exp.loc
192.168.24.163
                00:0C:F1:6C:A4:E2 2007-02-20
17:37
sw1A2.exp.loc 12 <--- pc249.exp.loc
192.168.24.249
                00:14:4F:23:5D:65 2007-01-31
18:09
sw1A2.exp.loc 15 <--- pc11.exp.loc  192.168.66.11
                00:07:E9:65:31:9B 2006-09-14
14:15
sw1A2.exp.loc 10 <--- pc196.exp.loc
192.168.66.196
                00:0F:1F:0D:F2:F6 2007-02-16
10:56
```

L'affichage est normalement d'une ligne par machine, ce qui nécessite un terminal de plus de 80 colonnes si on souhaite une lecture facile. Cependant, dans le cadre de cet article et vu les limites imposées à la largeur des colonnes, nous avons dû tricher quelque peu sur les espacements.

Par défaut, le résultat est donné trié par adresse IP, ce qui s'avère le plus pratique dans une recherche par machine. La date permet aussi de connaître les machines qui ne sont plus actives sur le réseau local depuis un temps certain et donc de pouvoir éventuellement récupérer leur adresse IP.

Il est possible de trouver plusieurs machines connectées sur le même port d'un commutateur. Deux cas sont alors possibles :

- Si la date diffère fortement, il s'agit d'un changement de poste donc l'une des deux machine est obsolète ;
- Si la date est quasi-identique, il y a certainement un équipement réseau non *manageable* connecté derrière le commutateur et plusieurs machines sont alors branchées dessus.

En effet, l'inventaire des machines ne peut être réalisé qu'au niveau du matériel actif administrable. Il n'est donc pas possible de dissocier deux ou plusieurs machines connectées sur ces équipements réseaux d'entrée de gamme.

4.3 Carte globale

La sortie standard au format *txt* de l'outil Klask a été conçue pour permettre la fusion avec l'affichage du plan des commutateurs. Il est ainsi possible d'obtenir un tableau de toutes les connexions au niveau des commutateurs.

```
# (klask exportsw; klask exportdb)|sort
```

5 Commandes secondaires

Klask permet, via une commande secondaire, d'activer ou de désactiver facilement le port d'un commutateur afin d'isoler une machine du réseau local. Cette fonctionnalité est très utile lorsqu'on n'a pas accès physiquement à la machine pour cause de bureau fermé.

Dans l'exemple ci-dessous, le port 10 du commutateur *sw1A2* est désactivé.

```
# klask disable sw1A2.exp.loc 10
```

La commande *enable* effectue l'opération inverse. Il est possible d'utiliser ces commandes dans un CRON pour, par exemple, protéger un sous réseau physique la nuit ou le week-end.

Une autre commande utile consiste à supprimer une machine de la base de données. En effet, celle-ci garde en mémoire la trace de toutes les machines et n'a aucun moyen de savoir qu'elles sont les machines obsolètes.

```
# klask delete pc249.exp.loc
```

6 Le coeur de Klask

D'un point de vu technique, Klask est écrit en Perl et tourne sur une machine de type UNIX. Il est en fonctionnement opérationnel sur des serveurs *GNU/Linux debian* et *fedora.*

Il utilise le plus largement possible des outils de plus bas niveau comme *arpwatch*, *fping* et *arping* pour la collecte des informations sur les machines (correspondance adresse IP, adresse physique). La bibliothèque Perl SNMP permet d'interroger les commutateurs (correspondance adresse MAC, port d'un commutateur). Enfin les outils de la suite GrahViz tracent les cartes aux formats *png*, *pdf*...

Au niveau du fichier de configuration et des bases de données, la syntaxe utilisée est en YAML. Ce format représente un bon compromis entre lisibilité et traitement automatisé. La base de données des machines sera cependant portées à terme vers SQLite pour des raisons de performance.

7 Conclusion et perspectives

Au niveau d'un réseau local conséquent, ayant des salles étudiants et des laboratoires de recherche, avec des nouvelles machines arrivant quasiment toutes les semaines, Klask s'avère à l'usage un outil indispensable, le compagnon idéal des serveurs DNS et DHCP.

Klask poursuit son développement (dernièrement, la partie multi-VLAN et la partie GrahViz) et des améliorations sont envisagées, dont la recherche d'une machine dès la détection de son adresse IP, par exemple en utilisant *arpalert* et/ou en configurant le VMPS sur les commutateurs.

D'autres types de graphe sont à l'étude en utilisant les possibilités de GrahViz. Par ailleurs, en interrogeant le matériel actif par SNMP, un graphe enrichi pourrait faire apparaître le mode (10HD, 100FD, 1000FD...) et le type (cuivre ou fibre) des connexions.

Un autre développement à court terme sera de générer des pages web récapitulant les résultats et permettant une consultation plus facile et plus conviviale de la carte du réseau local. Il est notamment prévu de pouvoir cliquer sur un commutateur et d'avoir ainsi directement la liste des machines connectées dessus.

Annexe

Extrait du fichier de configuration /`etc/klask.conf`

```
default:
  community: public
  snmpport: 161

network:
  labo:
    ip-subnet:
      - add: 192.168.66.0/24
      - add: 192.168.67.0/24
    interface: eth0
    main-router: gw66.exp.loc

  ecole:
    ip-subnet:
      - add: 192.168.24.0/24
    interface: eth0.43
    main-router: gw24.exp.loc

router:
  - hostname: gw66.exp.loc
    mac-address: 00:08:7C:23:55:03
```

```
switch:

  - hostname: sw1A0.exp.loc
    location: BatA / RdC / URAD
    type: HP8000

  - hostname: sw1B1.exp.loc
    location: BatB / 1 etage / B107
    version: 3
    username: Administrator
```