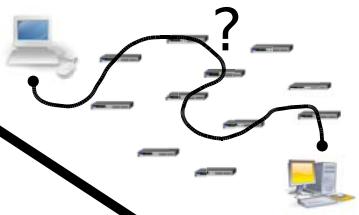
Klask : un outil dédié à la cartographie du réseau local

Quel est le chemin entre deux machines de mon réseau ?
Comment sont interconnectés mes éléments actifs ?



Sur quel port de quel commutateur est branchée ma machine ?

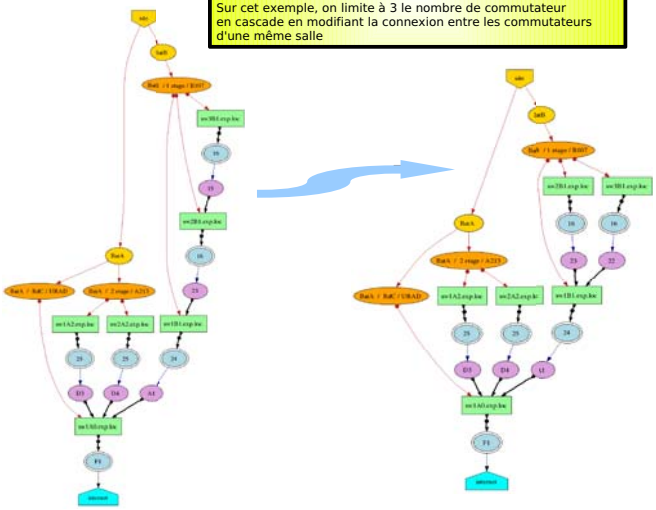
Pourquoi faire ?
* Dé-activer un port d'un commutateur pour isoler une machine infecté du réseau
* Configurer les commutateurs pour pour faire transiter un VLAN entre deux point du réseau
* ...

Klask-Web : Listing des connections sur un réseau des machines.
Classement par :

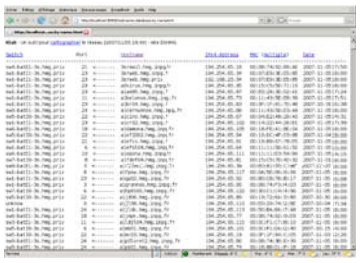
- Commutateur
- Nom DNS
- Ipv4
- Adresse Physique (MAC)
- Date de dernière détection

Optimisation de la topologie d'un réseau
A partir d'une certaine complexité de la topologie du réseau, il y a un risque non négligeable de ne pas avoir une topologie optimale.

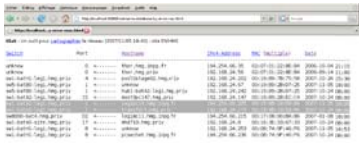
Sur cet exemple, on limite à 3 le nombre de commutateur en cascade en modifiant la connexion entre les commutateurs d'une même salle



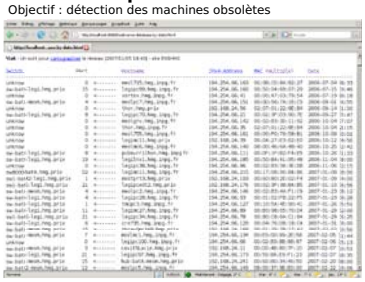
Classement par adresse IP



Adresse physique (MAC) en double sur un même VLAN ayant une date différente
Objectif : détection des machines ayant changé d'adresse IP



Classement par date
Objectif : détection des machines obsolètes



Objectif
Selon l'état de son propre réseau, à chacun de voir à quoi pourrait lui servir ces résultats.
Les exemples donnés sont là en tant que support.

Le moteur Klask en quelques mots
- **Ecrit en Perl**
- **Multi-VLAN**
- **Multi-Réseau**
- **Scanne les réseaux via FPING et ARPING sur les bonnes interfaces**
- **Collecte avec ARPWATCH les traces des paquets Ipv4 des machines**
- **Interroge les commutateurs administrables en SNMP v2 et v3**
- **En production sur un réseau constitué de commutateurs de marque HP**
- **Existe en paquetage Debian (sur demande)**

OID SNMP
Les commutateurs sont interrogés via SNMP en version 2 ou en version 3.
Les résultats suivants ont été validé sur un certain nombre de commutateur administrable de marque HP (HP1600, HP2424, HP2524, HP2626, HP2810, HP2824, HP8000)

Selon la génération du commutateur, il est possible d'avoir les informations suivantes :

```
+ description -- OID -> 1.3.6.1.2.1.1.5.0
+ location    -- OID -> 1.3.6.1.2.1.1.6.0
+ contact     -- OID -> 1.3.6.1.2.1.1.4.0
```

L'OID le plus intéressant est celui qui permet de connaître le numéro du port sur lequel est connecté une machine. Il faut commencer par écrire l'adresse MAC de la machine en notation décimale.
Exemple

```
00:D0:B7:7F:2C:78 -- DEC -> 0.208.183.127.44.78
```

On ajoute alors le préfixe `1.3.6.1.2.1.17.4.3.1.2` pour avoir l'OID final

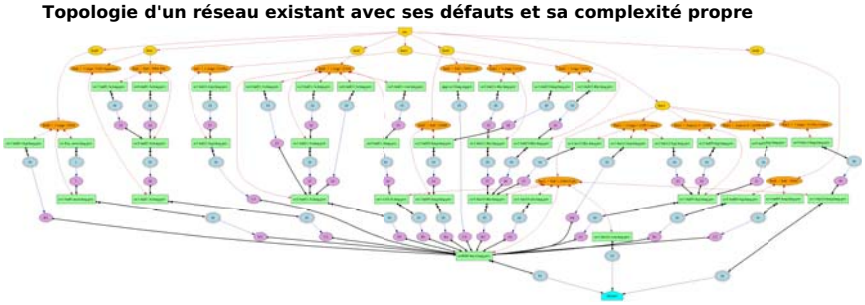
```
00:D0:B7:7F:2C:78 -- OID -> 1.3.6.1.2.1.17.4.3.1.2.0.208.183.127.44.78
```

Algorithme en deux temps
L'algorithme de découverte du réseau est rapide et n'est lancé que lors d'une modification de la topologie du réseau. La découverte des machines est exécutée régulièrement via un CRON (toutes les deux heures).

Découverte du réseau
- Collecte le couple IP / MAC de tous les commutateurs
- Collecte le couple IP / MAC des routeurs de sortie
- Sur chaque commutateur, via des requêtes SNMP
  - Détecte le port de connexion de chacun des autres switchs
  - Détecte le port de sortie du switch (port ou l'adresse MAC du routeur est trouvée)
- Déduction du plan du site via un algorithme maison du plus court chemin

Découverte des machines
- Lance un FPING sur l'ensemble des adresses IP à trouver
- Corrélation entre IP et adresse MAC via les tables d'ARPWATCH
- Mise à jour du TIMESTAMP de la dernière détection via ARPWATCH
- Requête DNS pour avoir le nom complet d'une machine
- Si le TIMESTAMP n'est pas trop vieux :
  - Recherche la machine sur le commutateur où la machine a déjà été détectée
  - Si non, on recherche la machine sur tous les autres commutateurs
- Si non on empile l'adresse IP dans la liste des machines non détectées
- Met à jour la base de données contenant les machines détectées
- Lance un ARPING sur le bon VLAN pour chaque adresse IP non détectée

Topologie d'un réseau existant avec ses défauts et sa complexité propre



Gabriel Moreau – IR CNRS

Laboratoire LEGI, Grenoble, France