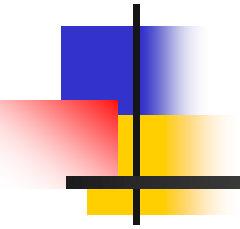


Gestion de Parc

Université Claude Bernard 1

Emmanuel.Reuter@ifsttar.fr

Mai 2017

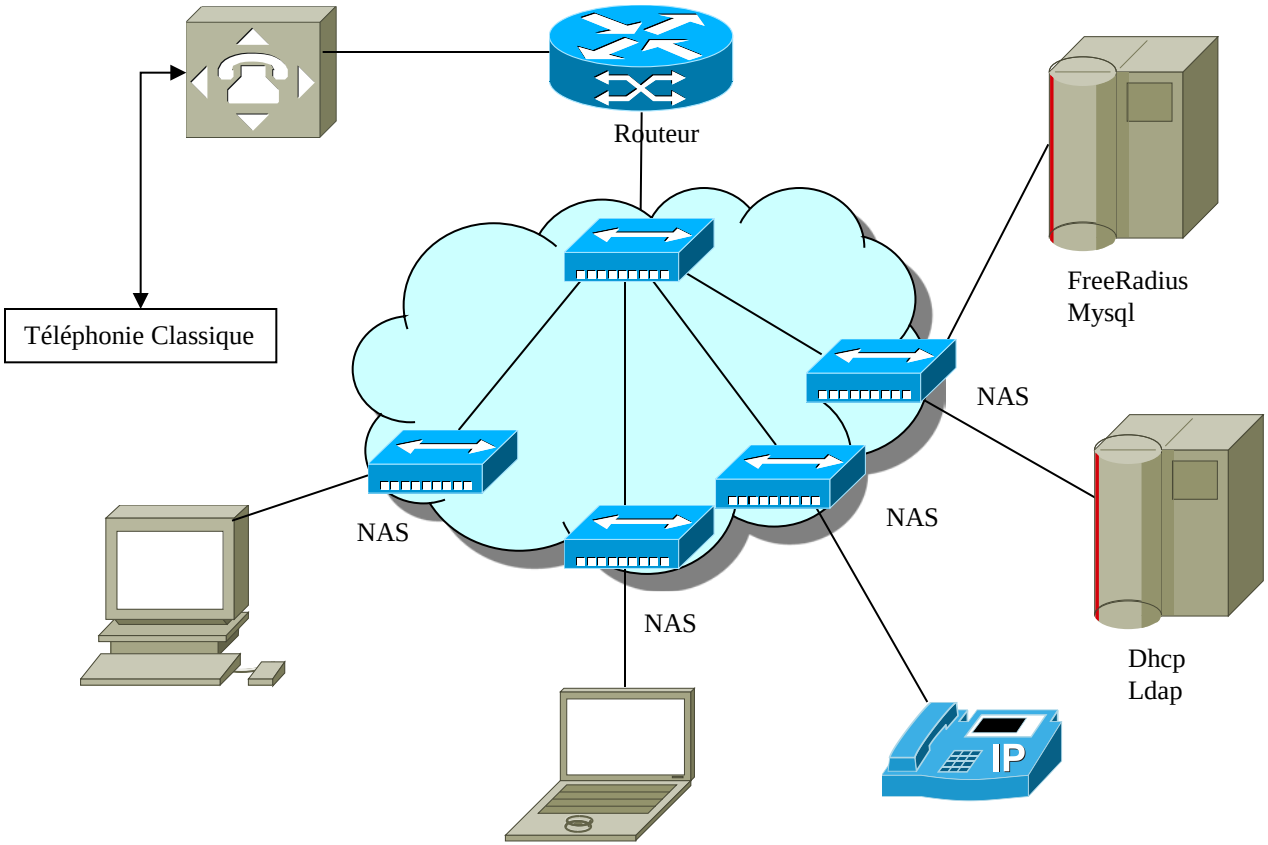
PLAN

- Réseau Niveau 2
- Sécurité & Management
- Métrologie / Cacti

I. Réseau niveau 2

- Contexte réseau
- Outils d’administration réseau
- VLAN : Pourquoi ?
- VLAN & GVRP
- Capture de trafic & VLAN
- Vlan et Qualité de service

I. Contexte réseau



I. Contexte réseau

- Intégration de plusieurs types de matériels
  - Réseau donc hétérogénétié
  - Systèmes : PC, portable, Téléphone IP, Imprimante, etc..
- Intérêt d'avoir une vue globale du réseau à gérer
- Avoir des outils pour faciliter le travail
  - Radius, Ldap (annuaire), Base de données (Mysql, ..), Cacti (monitoring réseau), etc..

I. Outils d’administration réseaux

- Ping : permet de vérifier la connectivité
- Traceroute : permet de trouver si un équipement actif du réseau est défaillant
- DIG - Host: permet la résolution du nom d’hôte

I. Outils d'administration de base : PING

- ping 137.121.1.112 –c 3 (version Linux)
  - PING arc-route (137.121.1.112) 56(84) bytes of data.
  - 64 bytes from arc-route (137.121.1.112): icmp_seq=1 ttl=254 time=0.355 ms
  - 64 bytes from arc-route (137.121.1.112): icmp_seq=2 ttl=254 time=0.368 ms
  - 64 bytes from arc-route (137.121.1.112): icmp_seq=3 ttl=254 time=0.364 ms
  - --- arc-route ping statistics ---
  - 3 packets transmitted, 3 received, 0% packet loss, time 1999ms
  - rtt min/avg/max/mdev = 0.355/0.362/0.368/0.016 ms

I. Outils d'administration : Traceroute

- Utilise le TTL du paquet IP (RFC 791)
- Fonctionne par HOP dont la valeur est décrémentée par chaque routeur sur le chemin
- traceroute 137.121.96.254
  - traceroute to 137.121.96.254 (137.121.96.254), 30 hops max, 38 byte packets
    - 1 137.121.13.101 (137.121.13.101) 0.323 ms 0.278 ms 0.276 ms
    - 2 arc-route (137.121.1.112) 0.374 ms 0.202 ms 0.214 ms
    - 3 137.121.96.254 (137.121.96.254) 6.564 ms * 6.563 ms

I. :DIG/HOST

- DIG proxy.ifsttar.fr

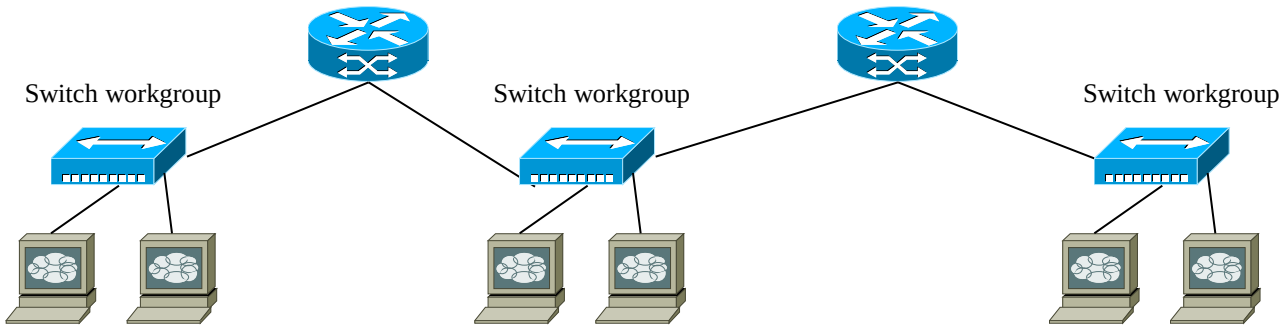
```
; <<>> DiG 9.7.3 <<>> proxy.ifsttar.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
47869
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 8,
ADDITIONAL: 8

;; QUESTION SECTION:
;proxy.ifsttar.fr.              IN      A

;; ANSWER SECTION:
proxy.ifsttar.fr.       172800  IN      A       137.121.1.26

;; AUTHORITY SECTION:
ifsttar.fr.             172800  IN      NS      dns1.ifsttar.fr.

;; ADDITIONAL SECTION:
dns1.ifsttar.fr.        172800  IN      A       137.121.3.4

;; Query time: 4 msec
;; SERVER: 137.121.162.24#53(137.121.162.24)
;; WHEN: Tue Nov 18 09:36:47 2014
;; MSG SIZE  rcvd: 346
```

- HOST –v proxy.ifsttar.fr

```
Trying "proxy.ifsttar.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65005
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 8,
ADDITIONAL: 8
;; QUESTION SECTION:
;proxy.ifsttar.fr.              IN      A
;; ANSWER SECTION:
proxy.ifsttar.fr.       172800  IN      A       137.121.1.26
;; AUTHORITY SECTION:
ifsttar.fr.             172800  IN      NS      remus.inrets.fr.
;; ADDITIONAL SECTION:
ns3.ifsttar.fr.         172800  IN      A       137.121.250.3
Received 346 bytes from 137.121.162.24#53 in 1 ms
Trying "proxy.ifsttar.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8688
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 0
;; QUESTION SECTION:
;proxy.ifsttar.fr.              IN      AAAA
;; AUTHORITY SECTION:
ifsttar.fr.             172800  IN      SOA     remus.inrets.fr.
hostmaster.inrets.fr. 2014111704 21600 3600 3600000 172800
```

I. VLAN : Pourquoi ?

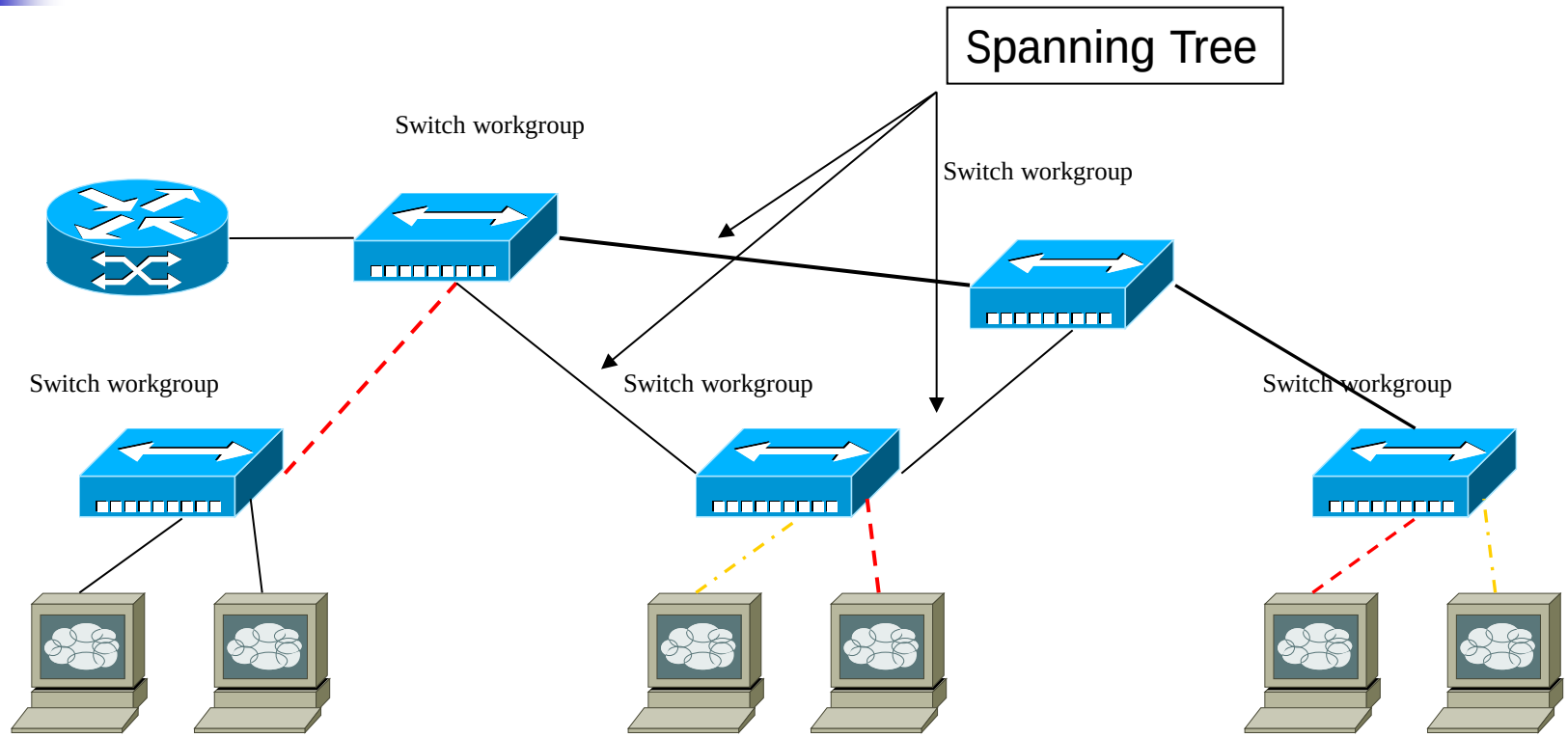
- **V**irtual **L**ocal **A**rea **N**etwork
- Segmentation des communautés / domaines de diffusion par les routeurs
- Protection / Sécurité



I. VLAN Première définition

- Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les noeuds, ce sont des domaines de diffusion gérés logiquement

I. VLAN Domaines de diffusion logique



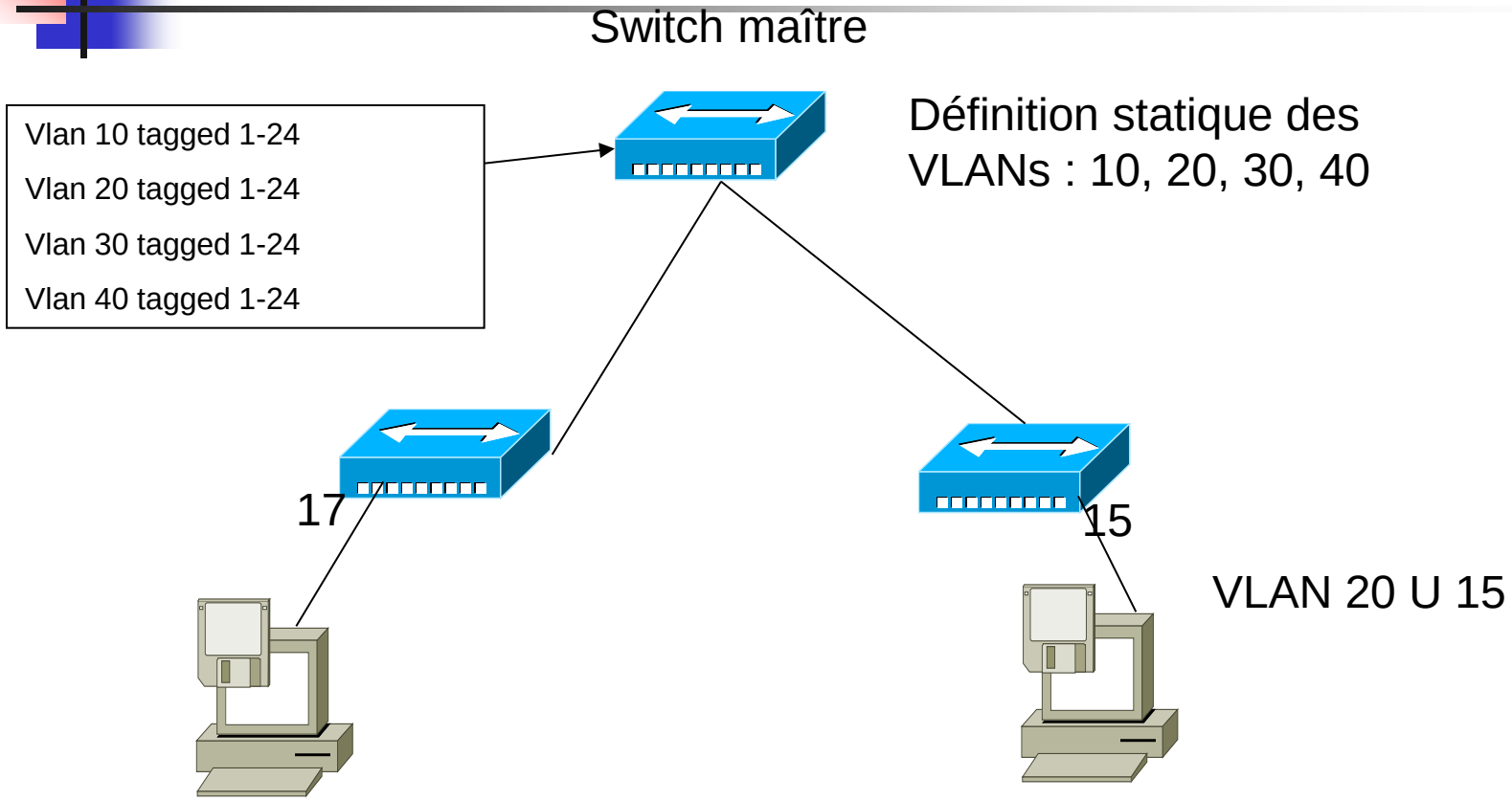
I. VLAN Domaines de diffusion logique

- Avantages
  - Réduction des messages de diffusion (ARP,Broadcast)
  - Création de groupes de travail indépendants
  - Possibilité de déplacer la station sans changer de réseau virtuel
  - Sécurité par le contrôle des échanges inter-VLAN (filtrage du trafic)
- Remarque : une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée

I. VLAN : 802.1q Types de trames

- La norme définit trois types de trames :
  - les trames non étiquetées (untagged frame)
  - les trames étiquetées (tagged frame)
  - les trames étiquetées par une priorité (priority-tagged frame)
- *Untagged :* Le port est associé qu'à un seul VLAN. C'est à dire que tout équipement raccordés à ce port fera partie du VLAN.
- *Tagged :* Signifie que les trames qui arrivent et sortent sur le port sont marquées par une en-tête 802.1q supplémentaire dans le champs Ethernet. (Port trunk Cisco)
- Un port peut être "tagged" sur plusieurs VLAN différents. L'avantage du mode Tagged est la possibilité d'avoir un serveur pouvant communiquer avec toutes les stations des VLANs sans que les VLANs ne puissent communiquer entre eux.

I. Réseau VLAN

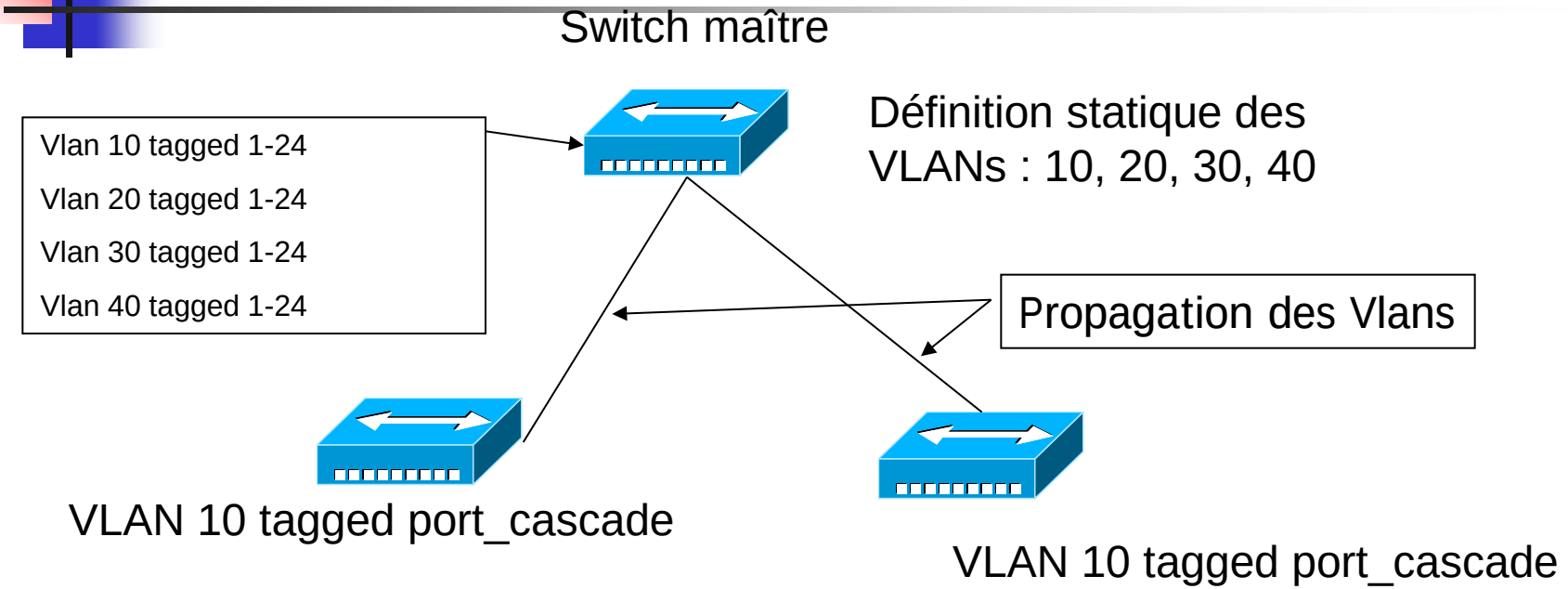


- Marche si les VLANS sont taggués
- Si les ports de connexion sont non taggués

I. VLAN & GVRP

- GARP VLAN Registration Protocol
- Generic Attribute Registration Protocol
  - Dans la norme 802.1Q
  - Configuration automatique des VLANs sur les switches
  - Distribution des VLANs sur le réseau

I. Réseau VLAN / GVRP



A chaque fois que l'on connecte une machine sur les switches, le VLAN est appris automatiquement

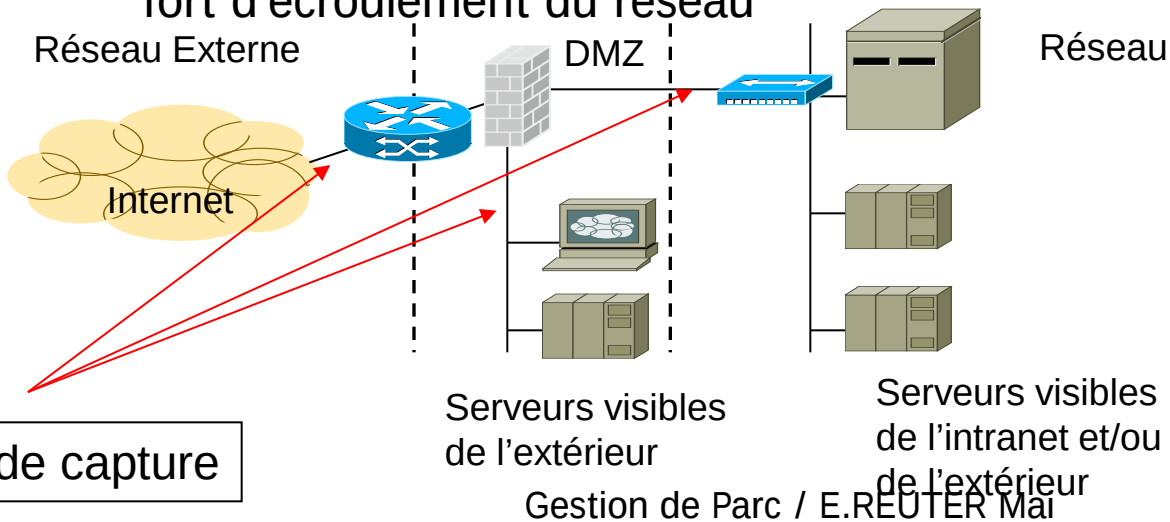
VLAN 10 : VLAN d'administration

I. Capture de trafic

- Quelques outils
  - Tcpdump (Linux), BackTrack v3
  - Whireshark (Winx + Linux)
  - Snoop (Solaris)
- Capture du trafic et analyse des trames
  - Voir les informations non visibles comme :
    - Admin prohibiter filter
    - Incohérence de configuration
    - Etc...

I. Capture de trafic

- Comment cela se réalise t-il ?
- Sur le même switch :
  - Recopie de trafic du port visé vers le port de connexion
- A distance
  - Assez compliqué du fait d'être obligé de recopier le trafic. Risque fort d'écroulement du réseau



Zones de capture

I. VLAN & Monitoring

- Si plusieurs VLANS, alors nécessité de pouvoir analyser le trafic passant sur d'autres VLANs
  - Utilité des ports mirroring
    - Port à analyser : en mode monitor
    - Port d'analyse : en mode miroir
    - Ex : (conf t) # mirror-port interface de monitoring
    - (conf t)# interface xx monitor (config hp)

I. VLAN & Classes de services

- CoS: Class Of Service
  - Champs de 3 bits dans l'entête de L2 de la trame Ethernet en IEEE 802.1Q (VLAN)
  - Spécifie la priorité du paquet entre les valeurs :
    - 0 équivaut au best-effort de l'IP
    - 7 signifie une priorité temps réel
- Cos : Méthode pour gérer le trafic dans un réseau local. Par exemple faire la difference entre :
  - Mails, Streaming Video
  - ToIP ou VoIP, Flux administration du réseau
- La Cos ne garantie pas un service minimal mais une priorisation du trafic au contrario de la QoS.

I. VLAN & Classes de services

- Il y a trois technologies de CoS
  - 802.1p Layer 2 Tagging
  - Type of Service (ToS)
  - Differentiated Services (DiffServ)
- Au niveau du switch :
  - Soit la valeur de PViD
  - Soit un mixte PVID + ToS ou PVID+DiffServ
  - Préparation du lissage du trafic pour la Qos IP

DHCP : intérêt

- Contrôle dynamique des adresses IP des clients
- Meilleure gestion des adresses
- Facilité pour le changement de routage
- Intérêt pour le contrôle d'accès au réseau
  - Filtrage, ACLs, etc..
- Port Udp 67 et 68 (bootp)

Dynamic Host Configuration Protocol

- Exemple

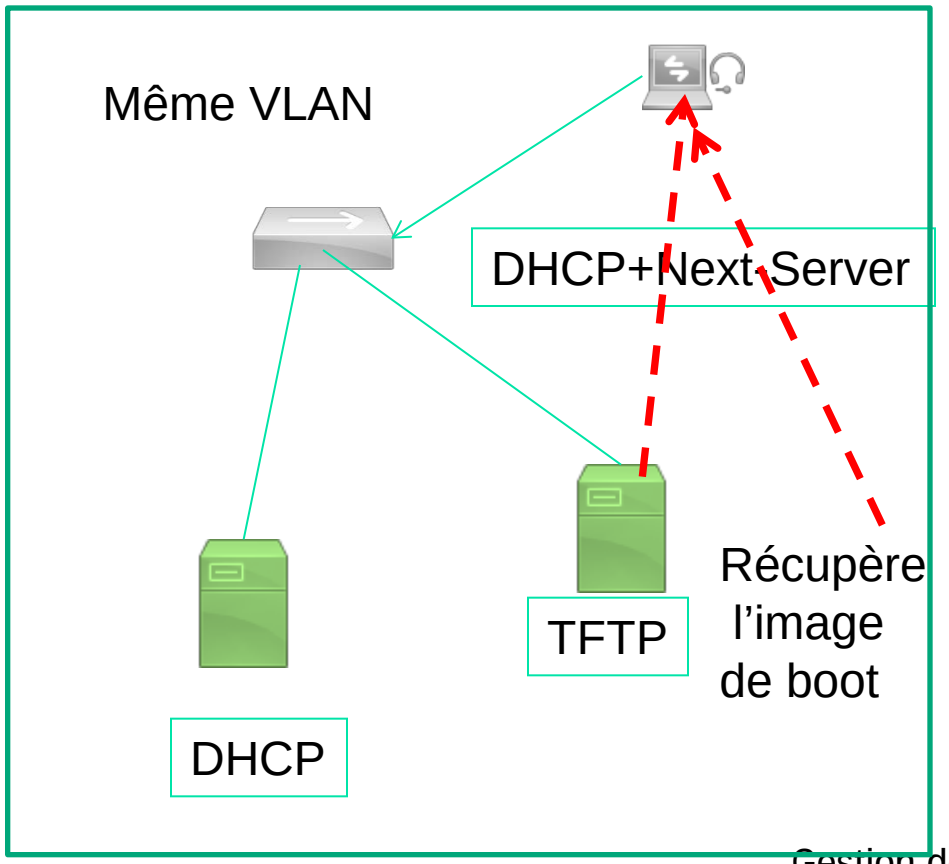
```
authoritative;
ddns-update-style none;
ignore client-updates;
log-facility local7;

option wpad code 252 = text;
option wpad "http://intranet.inrets.fr/proxy.pac";

option space CONNEXITY;
option CONNEXITY.call-server    code 001 = string;
option CONNEXITY.cfgname        code 002 = string;
option CONNEXITY.ftp-server     code 003 = string;
option CONNEXITY.ftp code 66 = string;

class "CONNEXITY" {
        match if substring(option vendor-class-identifier, 0, 13) = "CONNEXITY-000";
        option server.vendor-option-space CONNEXITY;
        option CONNEXITY.call-server  "192.168176.10";
        option CONNEXITY.cfgname  "0.0.0.0:9410";
        next-server 192.168176.10;
}
```

Dynamic Host Configuration Protocol

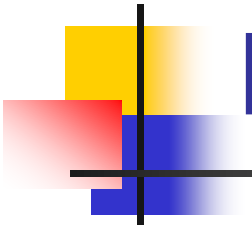
```
subnet 192.168.165.0 netmask 255.255.255.0 {
      default-lease-time 86400 ; max-lease-time 186400;
      option subnet-mask 255.255.255.0;
      option broadcast-address 192.168.165.255;
      option domain-name-servers  192.168.162.4, 192.1681.2;
      option routers 192.168.165.201;
      option netbios-name-servers  192.168.162.8;
      option domain-name "test.fr";
      option ntp-servers    192.168.162.12;
      next-server 192.168.163.10;
      range 192.168.165.18 192.168.165.200;
      filename « /tftpboot/pxe.img »;
      option tftp-server-name "10.15.201.222";
      option bootfile-name "boot\\x64\\wdsnbp.com";
      host Nxpp-165-41 {
                hardware ethernet 00:11:11:0f:e3:8b;  option host-name "Nxpp-165-41";
                fixed-address 192.168.165.41;
                next-server 192.168.163.18; filename « /tftpboot/tftpboot.pxe.img »;
      }
```

DHCP et PXE : fonctionnement

PXE

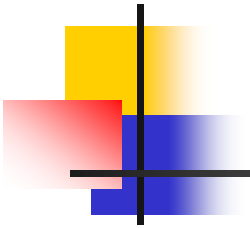


- DHCP Client cherche ses paramètres
- DHCP serveur retourne l'IP/MASK, next-serveur et filename
- Le client utilise son IP pour se connecter en tftp vers le serveur TFTP (next-serveur) pour récupérer son image de boot (« filename »)



PLAN

- Réseau Niveau 2
- Protocole SNMP
- Métrologie / Cacti



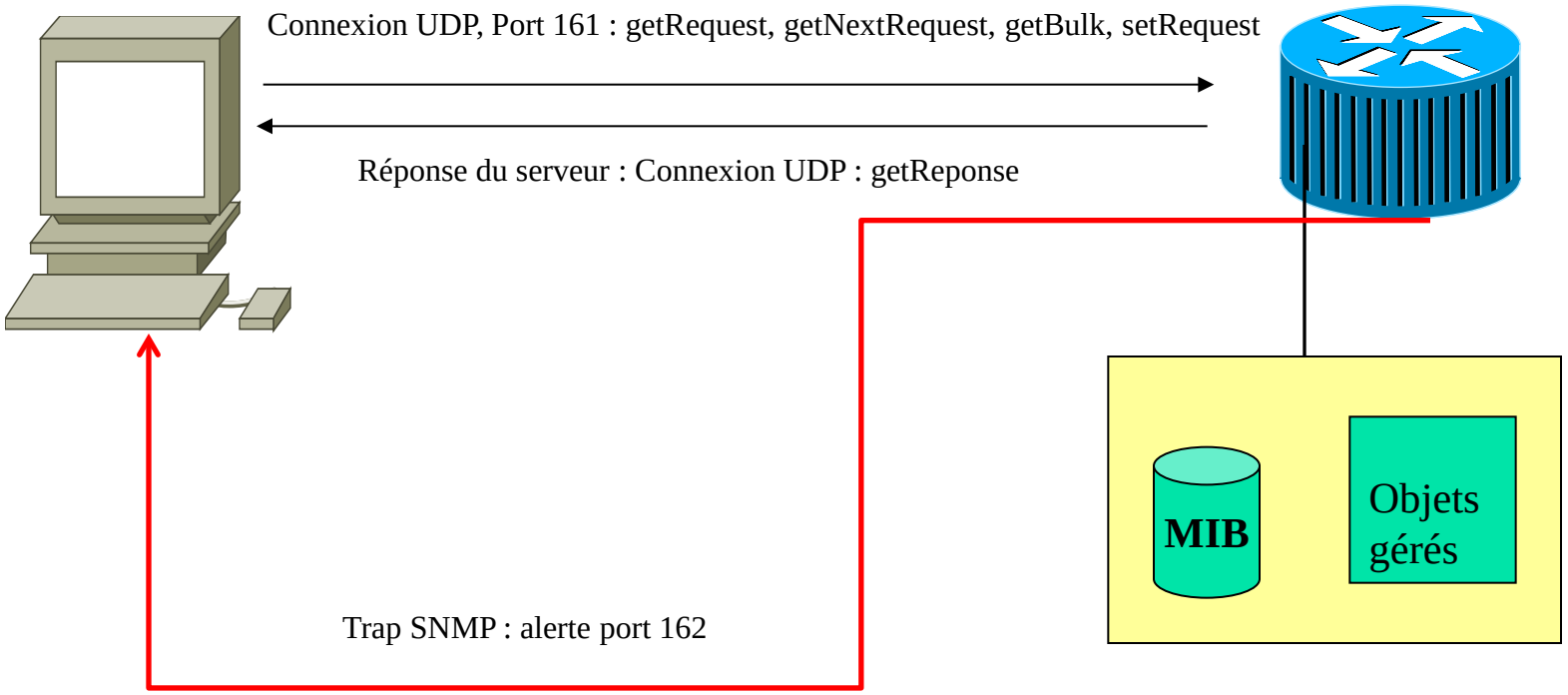
II. Protocole SNMP

- SNMP
  - Fonctionnement
  - Sécurité
  - MIBs
  - SNMP Trap
- SNMP Divers
  - Outils, trucs et astuces

II. SNMP

- Le protocole SNMP permet la communication entre les équipements réseau et les logiciels de supervision
- Interrogation, modification et notification
- SNMP repose sur
  - Un protocole de communication
  - Un ensemble de variables qui représentent l'état d'un matériel de réseau
  - Un standard d'encodage des informations transportées

II. SNMP : Fonctionnement du protocole



II. SNMP Communauté

- Trois types de communautés
  - Read-only (*public*)
  - Read-write (*private*)
  - Trap
- Nom de communauté ≈ mot de passe
- L'authentification en v1/v2 repose sur ces communautés, non cryptées
- Sauf avec SNMPv3 (cryptage style SSH)

II. SNMP : MIB

L'ensemble des variables qui décrivent l'état d'un équipement constituent une base de données : La Management Information Base (MIB)

- Chaque variable est identifiée par un numéro unique
- Organisation arborescente

- Les variables sont définies suivant le standard « Structure of Management Information »
  - SNMP v1 → SMI v1 (RFC 1155)
  - SNMP v2 → SMI v2 (RFC 2578)
  - Définit les types de variable autorisés (ASN.1), des termes, la gestion des tables

II. SNMP : MIB

- Un élément comprend 3 attributs :
  - Nom ou OID ex 1.3.6.1.2.1
    - Forme numérique et textuelle
- Type et syntaxe
  - Défini à l'aide d'un sous ensemble du langage ASN.1
- Encodage
  - Règles d'encodage en une chaîne d'octets (Basic Encoding Rule) pour la transmission sur le réseau

II. SNMP : MIB

- Une feuille correspond à une variable
  - Nom : ISO.Org.DOD.Internet.Management.MIB.System.SysObjectID
  - Identifiant (OID) : 1.3.6.1.2.1.1.2
  - La branche MIB-2 est commune à tous les équipements
  - La branche private.enterprises contient les extensions spécifiques
    - Ex 1.3.6.1.4.1.9 = Cisco

II. SNMP Valeur des variables

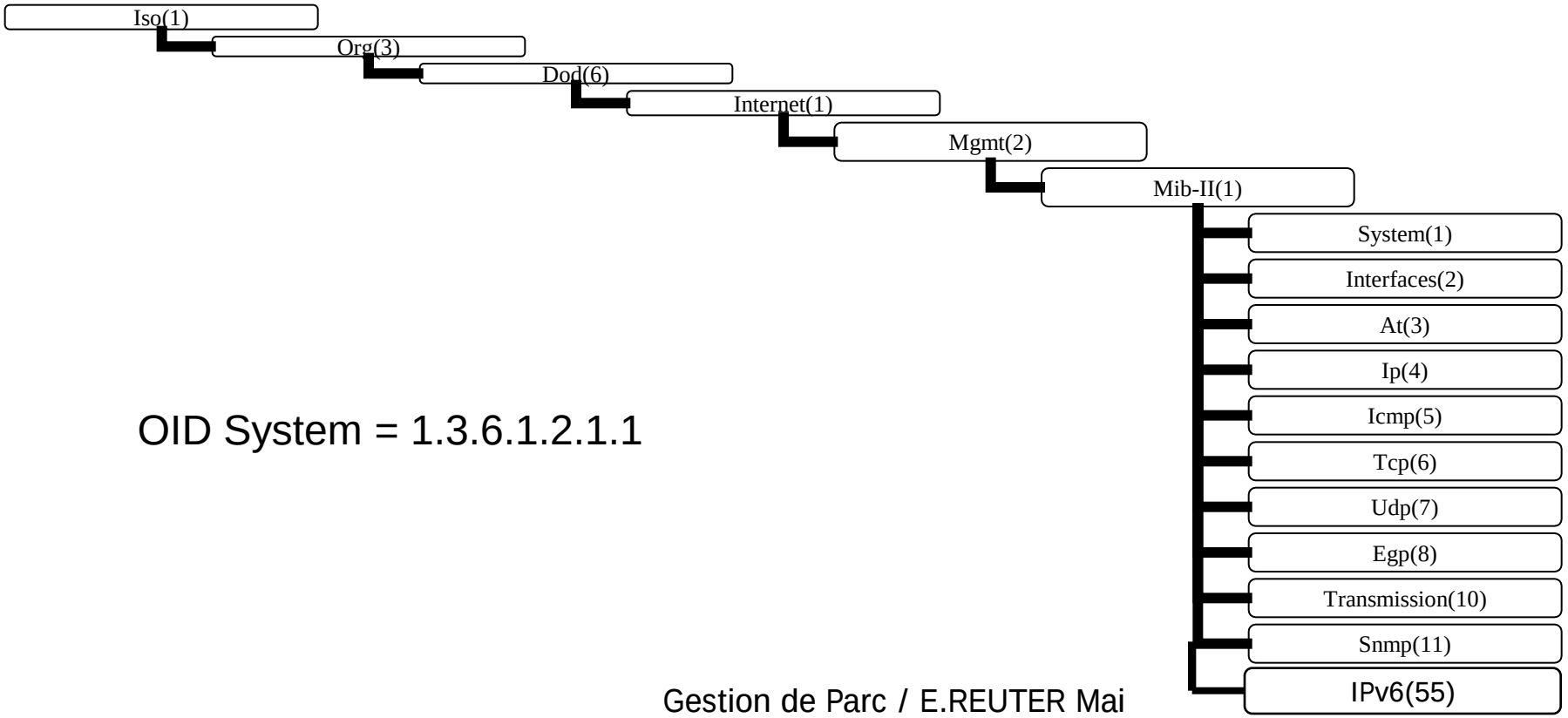
- Un objet simple est manipulé avec l'index 0
  - Ex. SysObjectID = 1.3.6.1.2.1.1.2**.0**
- Un index est utilisé quand il y a plusieurs instances du même périphérique
  - Ex. interfaces.ifTable.ifEntry.ifDescr.1 = lo0
  - interfaces.ifTable.ifEntry.ifDescr.2 = eth0
- Il existe une variable donnant le nombre d'occurrences
  - Ex. interfaces.ifNumber.0 = 2

II. SNMP Commandes

Il existe 3 types de commandes

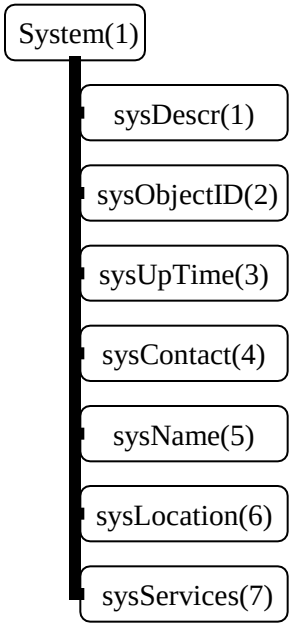
- Consultation :
  - GET : consultation d'une variable de la MIB
  - GET-NEXT : permet de passer à l'OID suivant
  - GET-BULK (v2/v3) : permet de consulter une branche complète
- Modification
  - SET : modification d'une variable, l'agent acquitte
- Notification
  - TRAP : cette commande est envoyée spontanément par l'agent (alerte)

II. MIB-II Standard



OID System = 1.3.6.1.2.1.1

II. Groupe System



- Linux : snmpwalk -c public -v 1 localhost system

  sysDescr.0 (octet string) Linux leo 2.6.8-2-686 #1 Tue Aug 16 13:22:48 UTC 2005 i686

  sysObjectID.0 (object identifier) enterprises.8072.3.2.10

  sysUpTime.0 (timeticks) 0 days 01h:48m:27s.80th (650780)

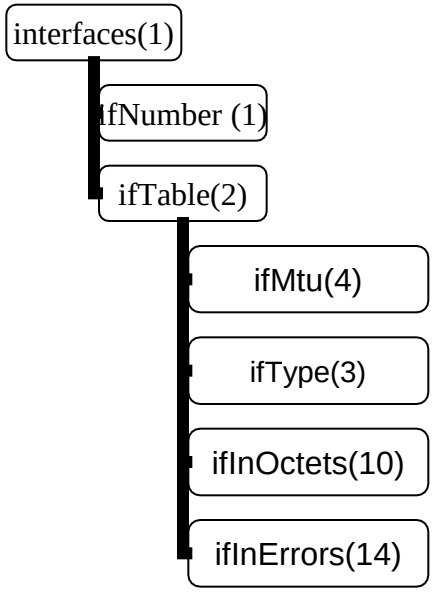
  sysContact.0 (octet string) Root <root@leo.inrets.fr>

  sysName.0 (octet string) leo

  sysLocation.0 (octet string) Salle Machine / Front de Neige

Remarque : « **System** » équivaut à «**1.3.6.1.2.1.1** »

II. Groupe Interfaces



- Linux : snmptable -c public -v 1 localhost interfaces.ifTable
- Ex : 5, eth3, ethernetCsmacd, 1500, 10000000, 0:22:19:65:80:76,... Etc..

II. Trap SNMP

- L’agent envoie une exception avec un TrapID et un OID
  - TrapID :
    - 0 = coldStart, 1 = warmStart, 2 = linkDown, 3 = linkUp, 4 = authenticationFailure, 5 = egpNeighborLoss, 6 = enterpriseSpecific
- En SNMP v2 et v3 l’exception est acquittée

II. Trap SNMP : Exemple

UDP: [10.10.100.100]:63337
DISMAN-EVENT-MIB::sysUpTimeInstance 245:20:56:24.10
SNMPv2-MIB::snmpTrapOID.0 IF-MIB::linkDown
IF-MIB::ifIndex.1 1
IF-MIB::ifDescr.1 GigabitsEthernet0/2
IF-MIB::ifType.1 ethernetCsmaCd
SNMPv2-SMI::enterprises.9.2.2.1.1.20.12 "link Down"
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 10.10.100.100
SNMP-COMMUNITY-MIB::snmpTrapCommunity.0 "public"
SNMPv2-MIB::snmpTrapEnterprise.0 SNMPv2-MIB::snmpTraps

II. SNMP Discovery Protocol

- Collecter la MIB SNMP
  - Ieee802dot1mibs.lldpMIB.lldpRemoteSystemsData
  - OID : 1.0.8802.1.1.2.1.4

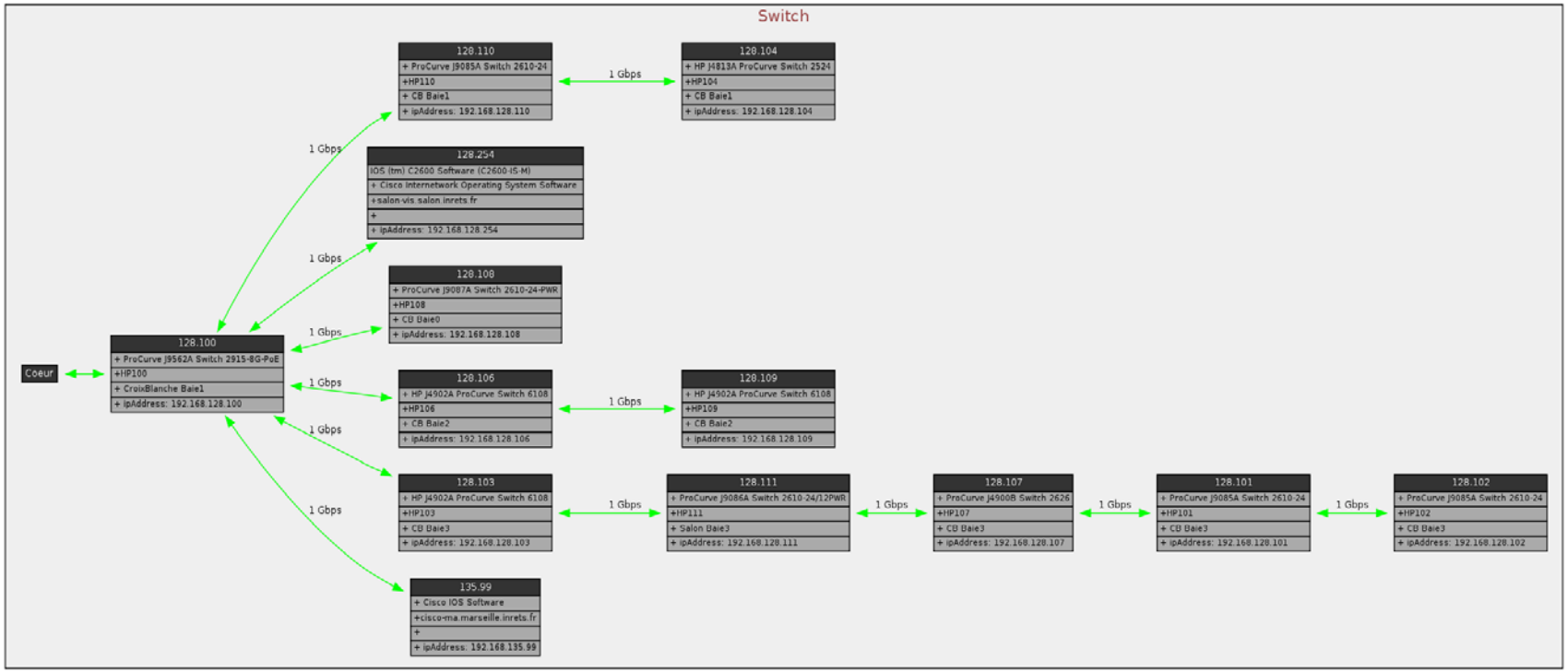
  - Intérêt : Avoir tous les liens entre les différents éléments qui constituent le réseau

II. SNMP Discovery Protocol

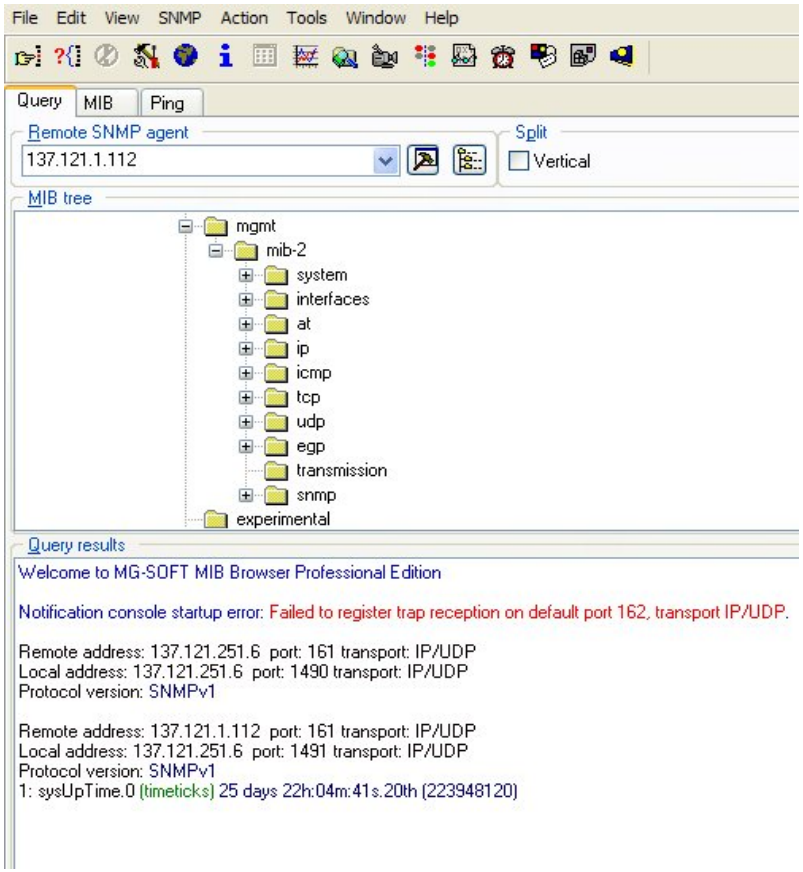
- Informations collectées de l'hôte distant
  - Nom du système et sa description
    - SysName : HP-43 2524 test-Vero
    - System Descr : HP J4813A ProCurve Switch 2524, revision F.05.72, ROM F.0...
  - Port physique local de connexion
    - Local Port : 2
  - Port physique distant de connexion et sa description
    - PortId : 25
  - Nom du VLAN (optionnel)
  - Adresse IP de gestion
    - Remote Management Address
    - Type : ipv4
    - Address : 137.121.161.143

II. SNMP Discovery Protocol

- Construire de manière automatique les schémas des réseaux

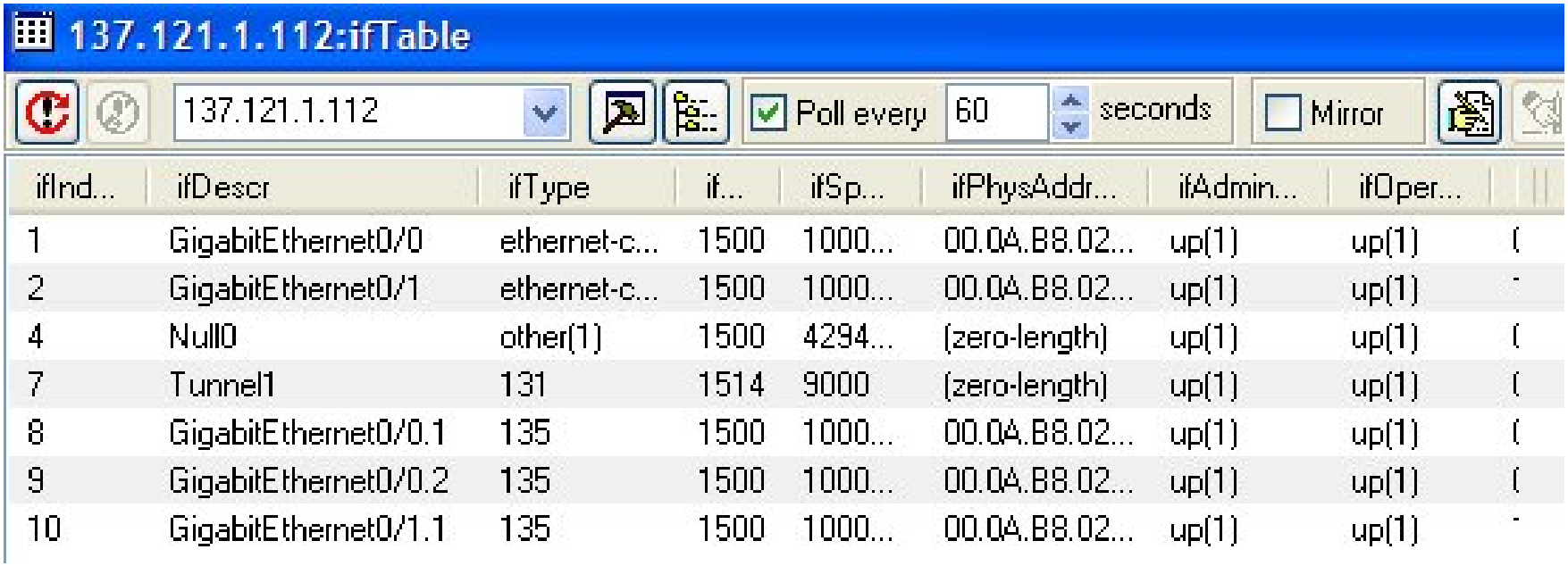


II. SNMP : Outil MibBrowser



- Permet de naviguer dans la hiérarchie des MIBs SNMP
- Collecte de valeur
- Changer les valeurs
- Une IHM conviviale

II. Interfaces.ifTable

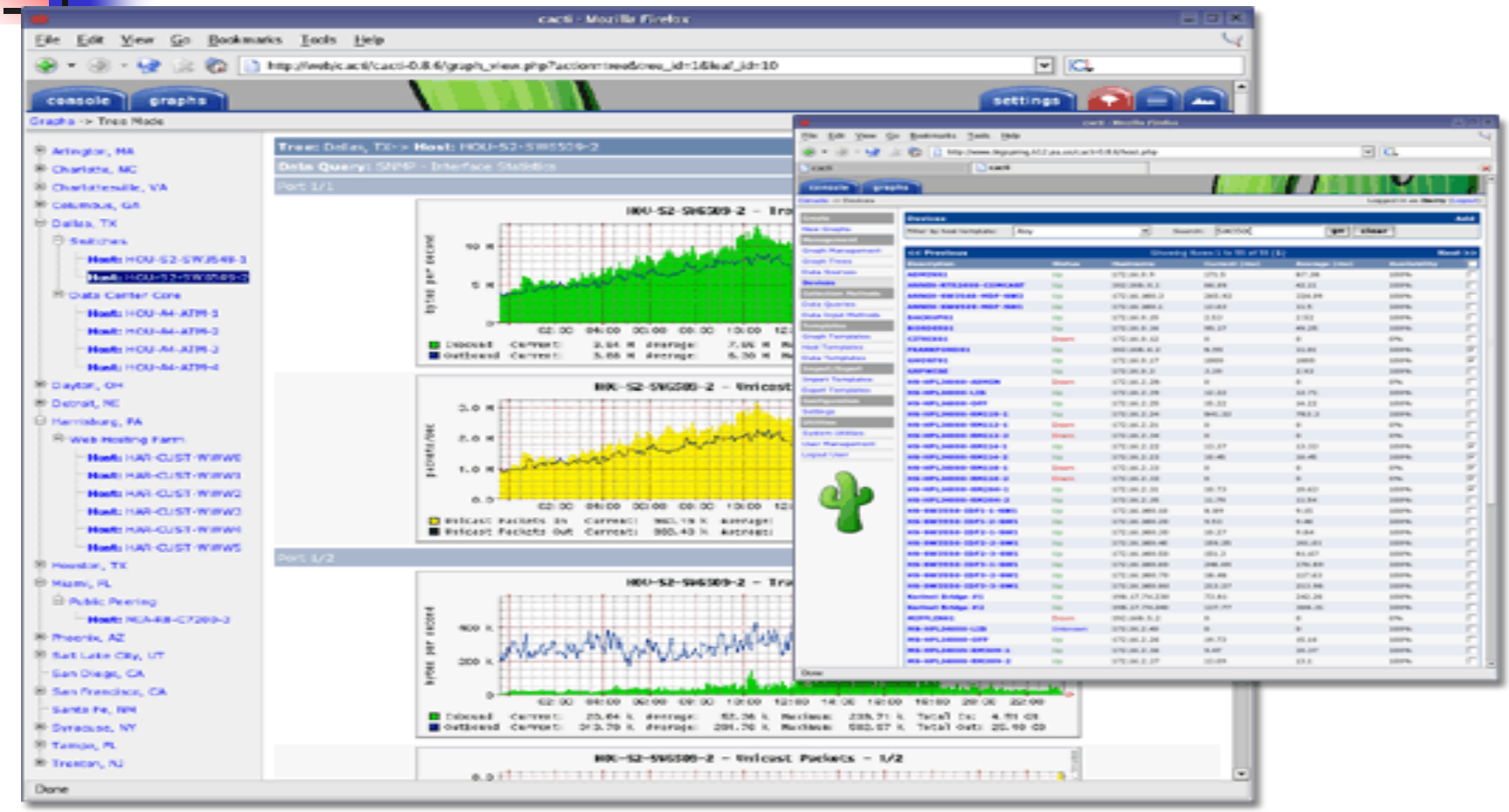


ifInd...	ifDescr	ifType	if...	ifSp...	ifPhysAddr...	ifAdmin...	ifOper...
1	GigabitEthernet0/0	ethernet-c...	1500	1000...	00.0A.B8.02...	up(1)	up(1)
2	GigabitEthernet0/1	ethernet-c...	1500	1000...	00.0A.B8.02...	up(1)	up(1)
4	Null0	other(1)	1500	4294...	(zero-length)	up(1)	up(1)
7	Tunnel1	131	1514	9000	(zero-length)	up(1)	up(1)
8	GigabitEthernet0/0.1	135	1500	1000...	00.0A.B8.02...	up(1)	up(1)
9	GigabitEthernet0/0.2	135	1500	1000...	00.0A.B8.02...	up(1)	up(1)
10	GigabitEthernet0/1.1	135	1500	1000...	00.0A.B8.02...	up(1)	up(1)

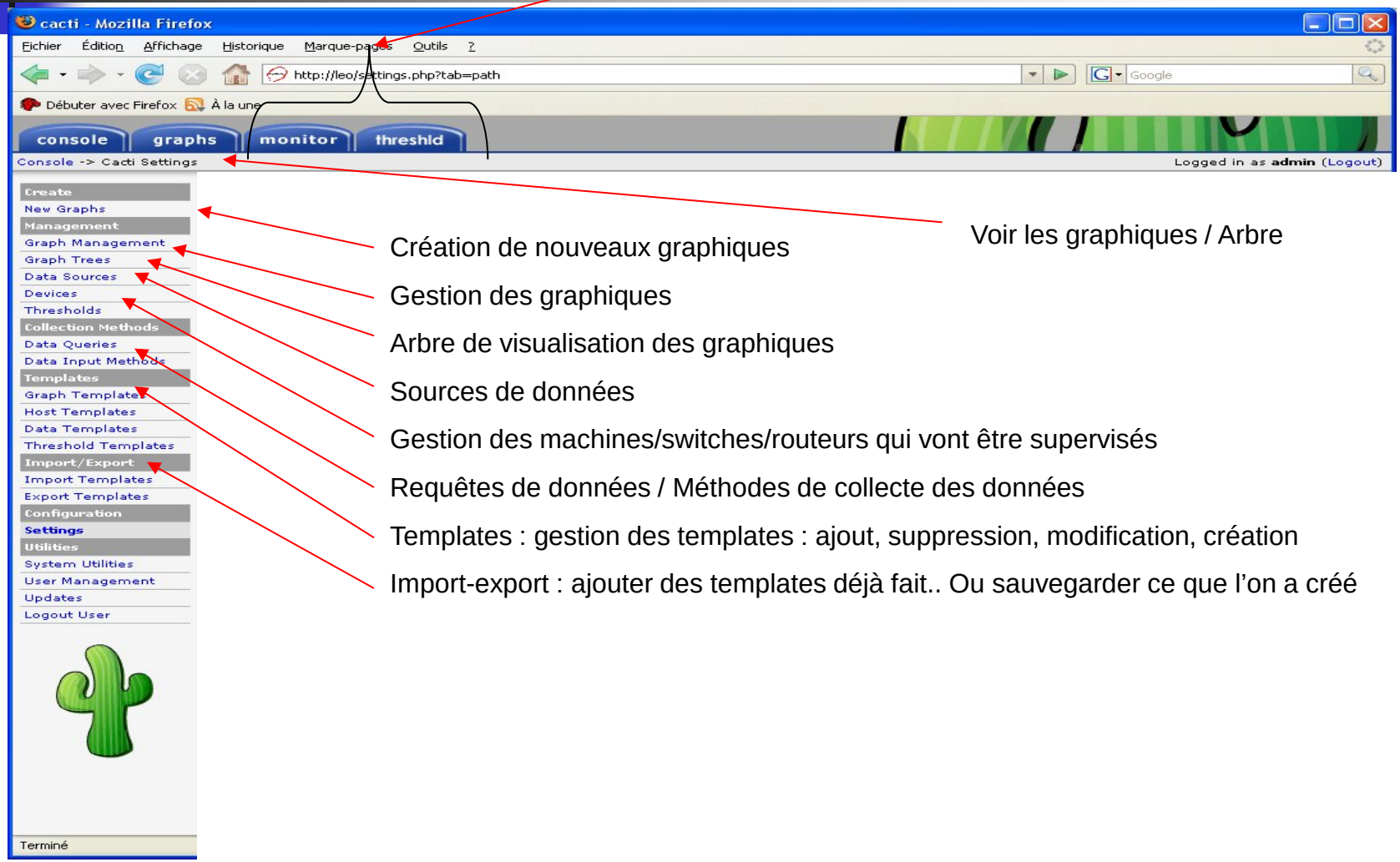
PLAN

- Réseau Niveau 2
- Sécurité & Management
- Métrologie / Cacti

III. Cacti : Outil de supervision



III. Cacti : Menu



Voir les graphiques / Arbre

Création de nouveaux graphiques

Gestion des graphiques

Arbre de visualisation des graphiques

Sources de données

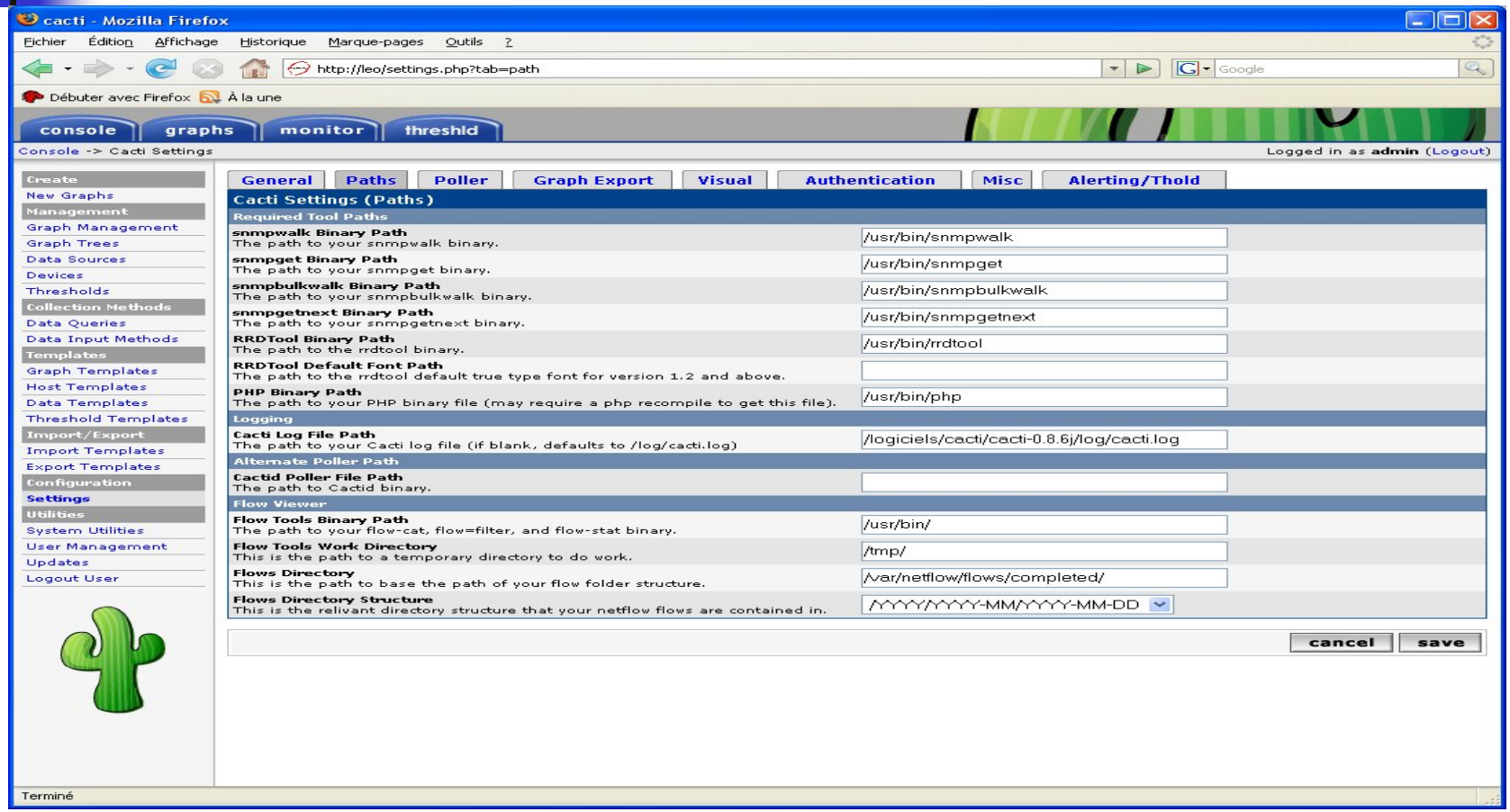
Gestion des machines/switches/routeurs qui vont être supervisés

Requêtes de données / Méthodes de collecte des données

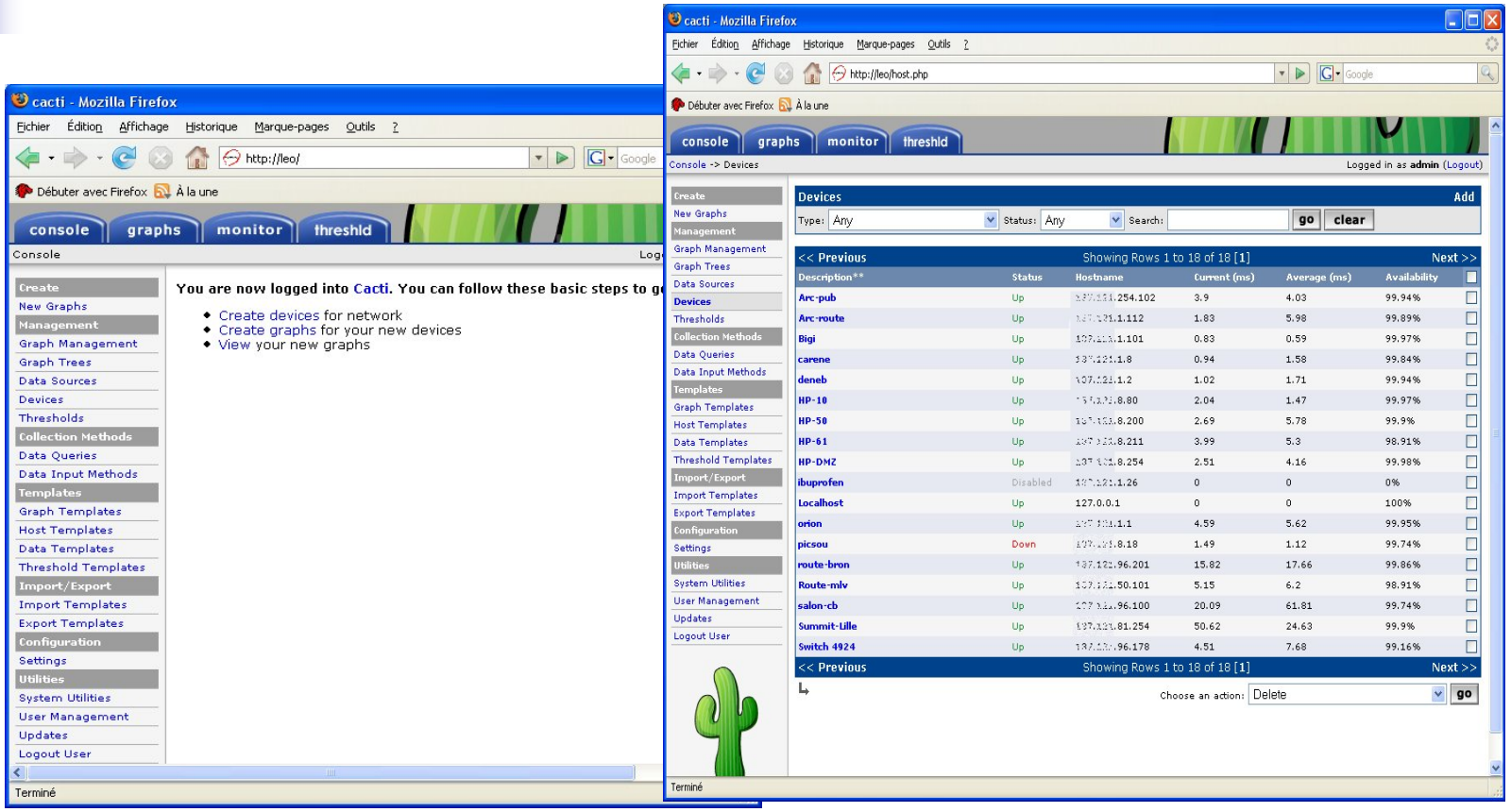
Templates : gestion des templates : ajout, suppression, modification, création

Import-export : ajouter des templates déjà fait.. Ou sauvegarder ce que l'on a créé

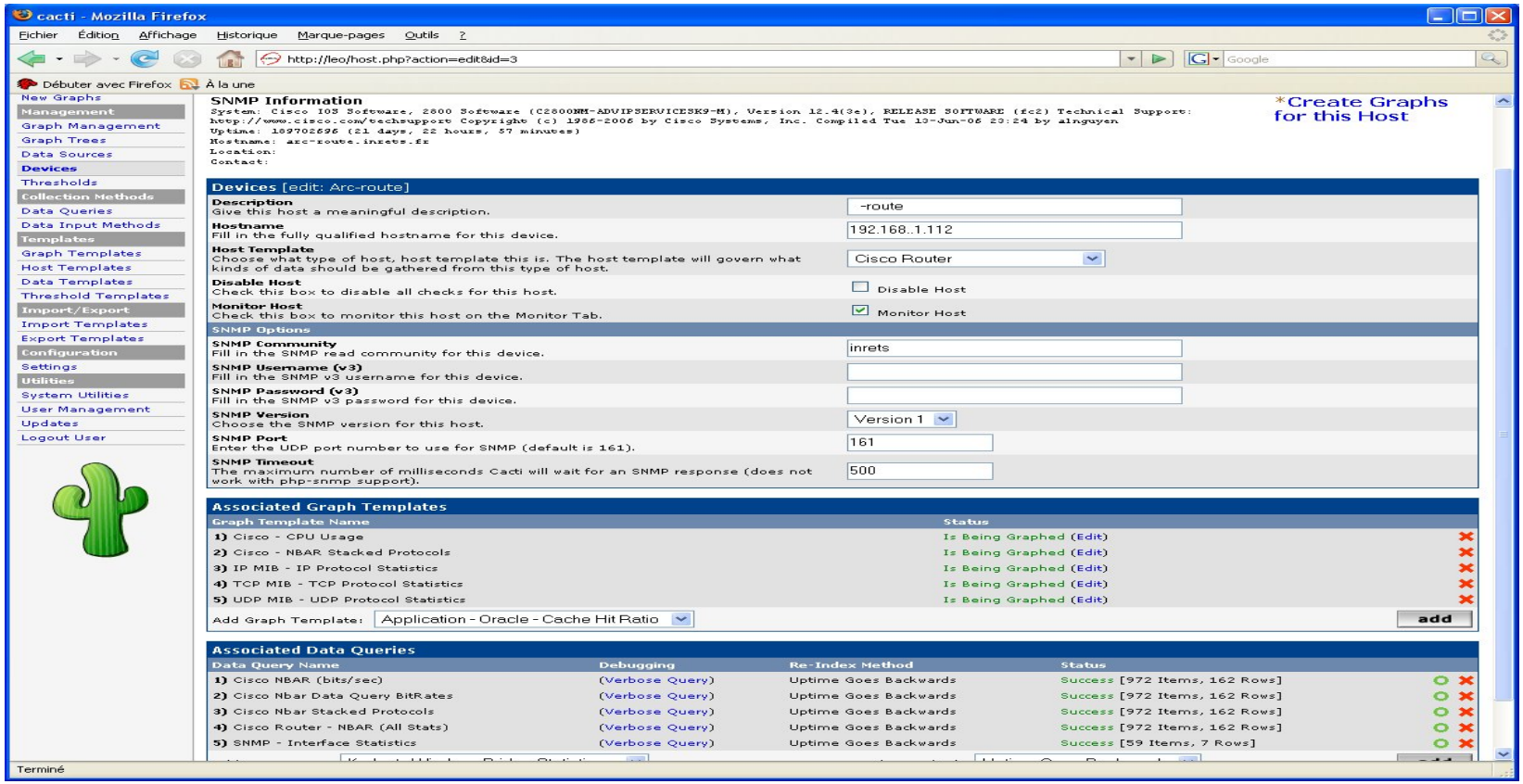
III. Cacti : Installation



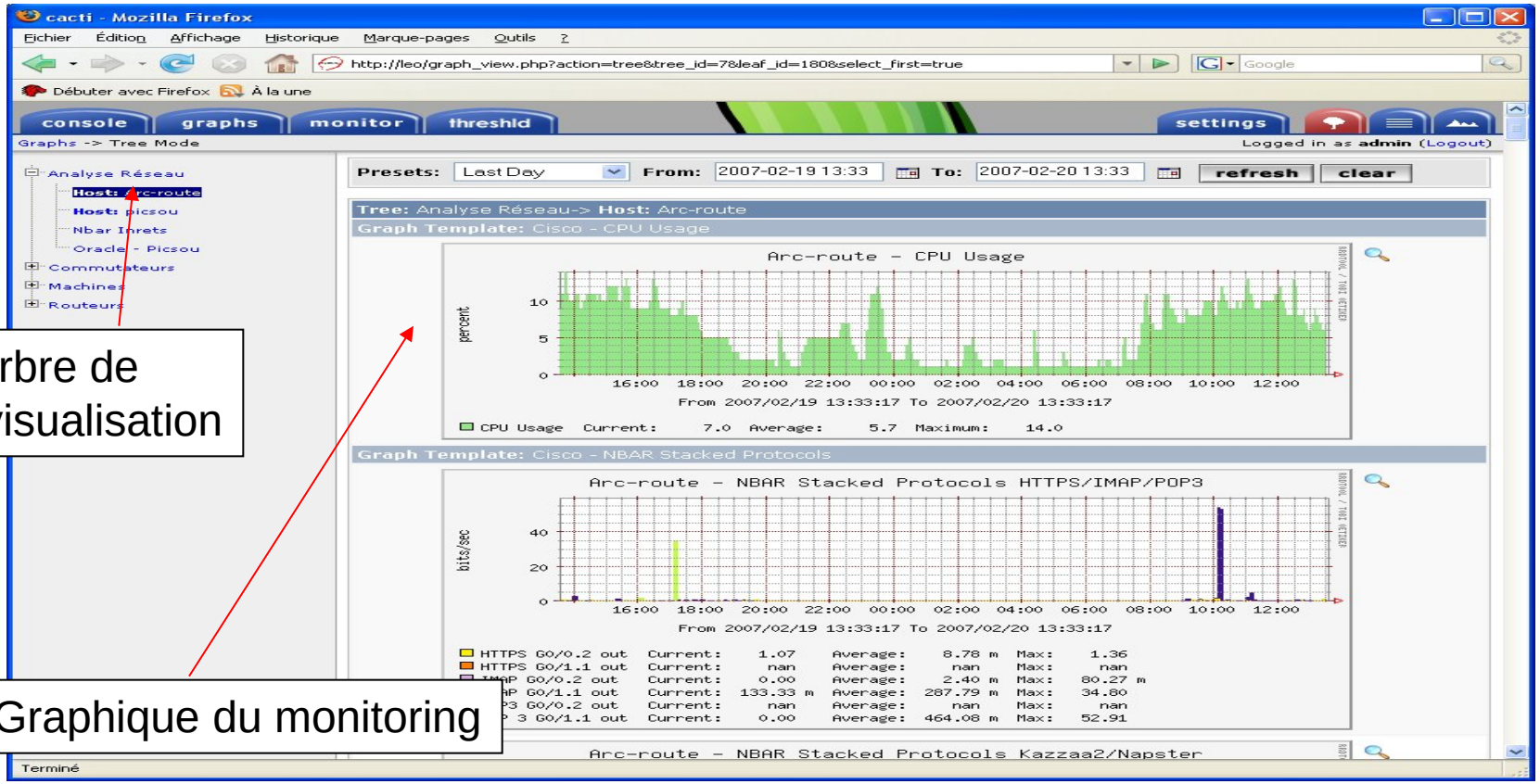
III. Cacti : Create Device



III. Cacti : Device



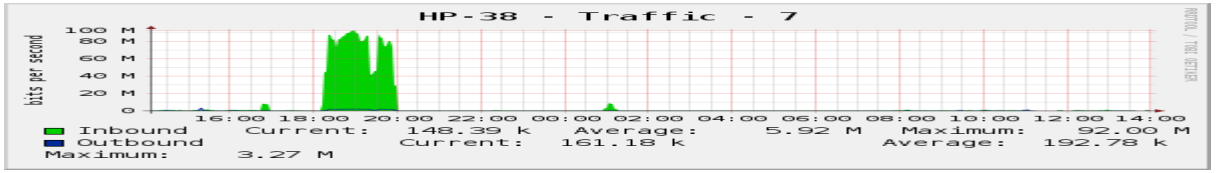
III. Cacti : Graphs

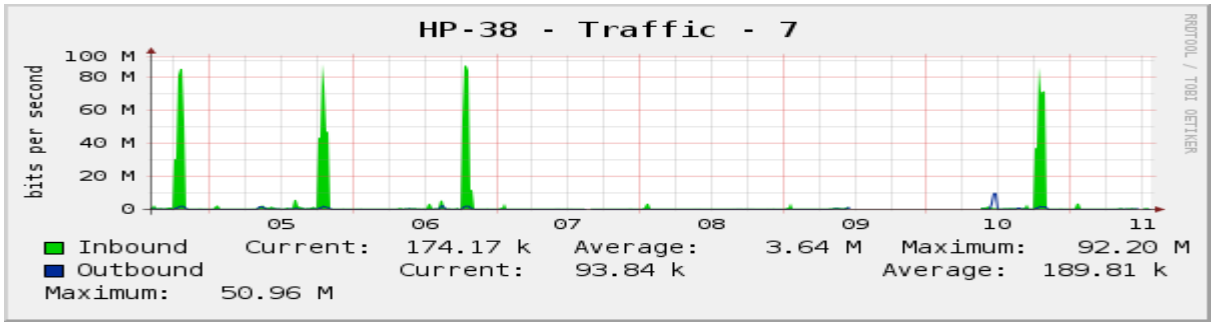


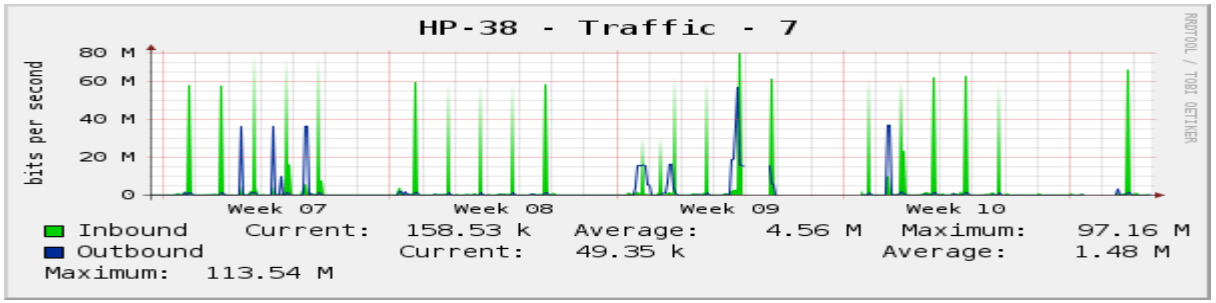
Arbre de visualisation

Graphique du monitoring

III. Cacti : Analyse des graphiques





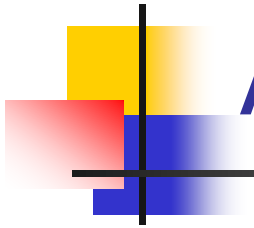


- Visualisation du trafic sur un port d'un switch
- Fort trafic le soir entre 19 et 20H
- Répétitif toutes les semaines et sur le mois

- Intérêt majeur : que faut-il faire au niveau de l'architecture du réseau (voir trunk)

III. SNMP MIBs

- Où trouver les MIBs
  - http://www.assure24.com/databases/snmp-mib/enterprise/
  - http://www.mibdepot.com/index.shtml
  - http://www.netdisco.org/
  - http://www.oidview.com/
- Code Source Perl :
  - http://www.otterbook.com/materials/lisa02nph1-src.txt
- Module Perl SNMP
  - http://search.cpan.org/~emiller/SNMP-Info-1.04/



Administration de réseaux

Questions ?