UNIVERSITE
PIERRE & MARIE CURIE
LA SCIENCE À PARIS

# Module thématique 1

-

# Supervision

-

# SNMP – NetSNMP - MRTG

UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE A PARIS

# *Sommaire*

- SNMP
- Net-SNMP
- MRTG

# SNMP

- SNMP ( Simple Network Management Protocol)
  - Protocole de gestion de périphériques sur des réseaux IP
  - Supervision des équipements (récupération d'informations)
  - Contrôle des équipements (modification du comportement)
  - Quels équipements ? :
    - Routeur
    - Serveur
    - sonde de température,...

# SNMP

- Plusieurs version du protocole
  - SNMP v1
    - Sécurité basée sur des « communautés » en fait, des mots de passe en clair pour récupérer ou modifier les informations de l'équipement
    - 3 communautés : readonly, readwrite, trap
  - SNMP v2
    - Principes de sécurité identiques à la v 1
  - SNMP v3
    - Authentification forte entre manager et agent
- Attention : en fonction des versions de SNMP utilisées, les commandes et options peuvent être différentes

# SNMP

- Plusieurs version du protocole
  - SNMP v1
    - Sécurité basée sur des « communautés » en fait, des mots de passe en clair pour récupérer ou modifier les informations de l'équipement
    - 3 communautés : readonly, readwrite, trap
  - SNMP v2
    - Principes de sécurité identiques à la v 1
  - SNMP v3
    - Authentification forte entre manager et agent
- Attention : en fonction des versions de SNMP utilisées, les options des commandes peuvent être différentes

# SNMP

- 2 acteurs : manager et agent
- Manager  (ou NMS – Network Management Station)
  - Machine qui gère/supervise les équipements
  - Agent : partie logicielle de l'équipement supervisé qui fournit les informations au NMS
- 2 actions popssibles
  - Poll : interrogation d'un équipement sur les informations qui le caractérise (ex : t°, bombre d'octets transférés par une interface réseau,...)
  - Trap : information envoyée (« poussée ») de l'agent vers le NMS en réponse à un évènement (ex : une interface réseau vient de tomber)

# SNMP

- Structure des informations SNMP
- SMI (Structure of Management Information) : syntaxe de définition des objets SNMP
- MIB ( Management Information base) : base des objets définissant certaines caractéristiques d'un équipement
- MIB-II : base d'objets commune à tous les équipements. Correspond à des informations TCP/IP
- Chaque équipement peut disposer d'une MIB particulière qui décrit les caractéristiques propres à l'objet et qui ne sont pas couvertes par la MIB-II
  - Ex : la donnée température d'une sonde de t°

# SNMP

- SNMP et UDP
  - UDP port 161 : envoi de requêtes et réception d'informations
  - UDP port 162 : envoi de traps
  - Intérêt : rapide et faible overhead
  - Inconvénients :
    - gestion des datagrammes perdus à la charge de l(application
    - Risque de perte de traps
    - Risque de perte d'information envoyée

# SNMP

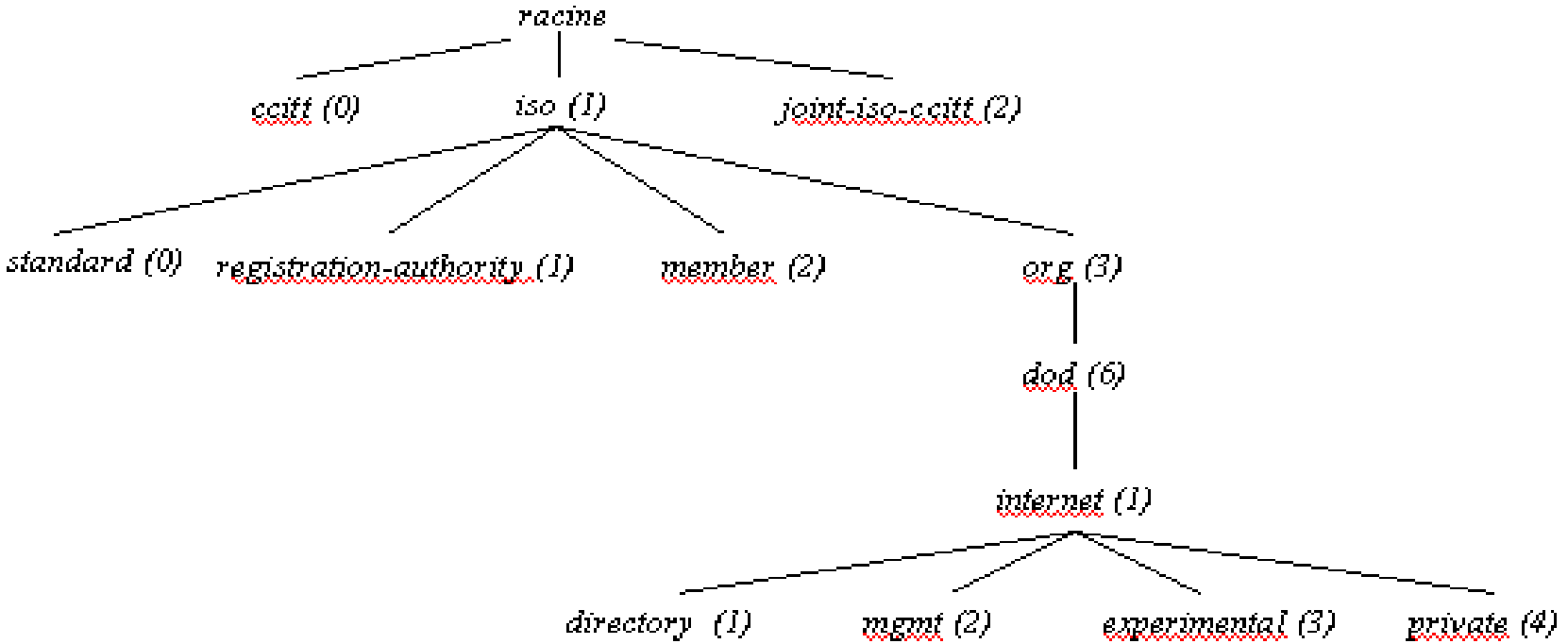
- Communautés SNMP
  - L'authentification entre le NMS et l'agent utilise des mots de passe (en clair) de 3 communautés
    - readonly (mot de passe par défaut : public) : communauté permettant uniquement la lecture d'information
    - readwrite (mot de passe par défaut : private) : communauté permettant la lecture et l'écrtiture d'information
    - trap : communauté permettant l'envoi de notification
  - D'un point de vue sécurité (en particulier en v1 et v2)
    - Modification des nom de communauté par défaut obligatoire
    - Filtrage IP

# SNMP

- Structure des objets SNMP
- Un objet SNMP est défini par 3 attributs
  - Nom ou OID (Object Identifier)
    - Forme numérique
    - Forme alphabétique « lisible »
    - Organisation dans une structure arborescente
  - Type de données : assure l'interopérabilité entre systèmes différents (Unix -> Windows)

# SNMP

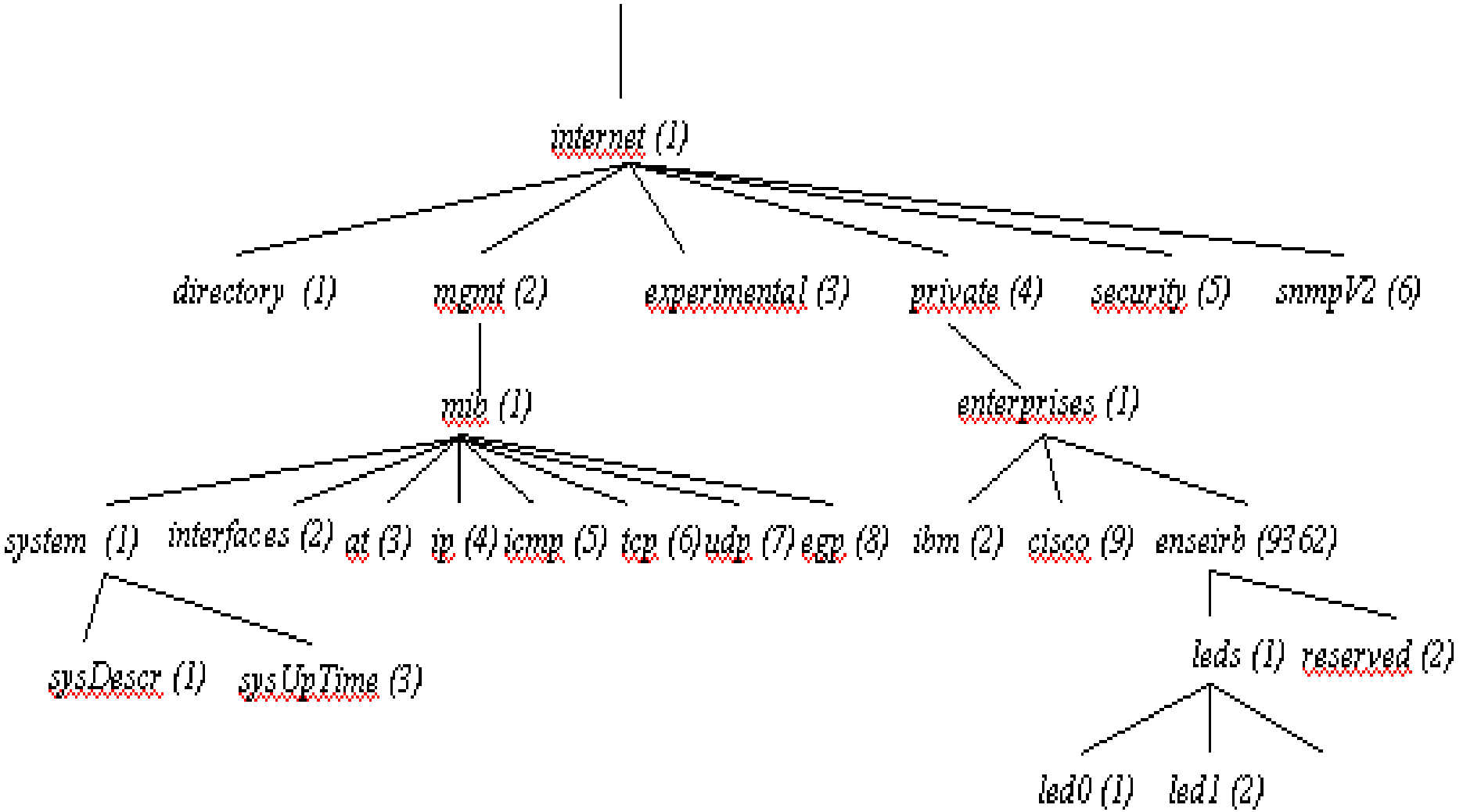
- OID
  - Formé d'une série d'entiers séparés par des points
  - Correspondance entre entiers et noms
  - Cette représentation permet d'identifier un objet géré par l'agent



# SNMP

- La branche 1.3.6.1 ou encore la branche iso.org.dod.internet concerne SNMP
  - Branche directory (1) : pas utilisée
  - Branche mgmt (2) : objets standards de gestion Internet
  - Branche experimental (3) : pour des tests
  - Branche private (4) : spécifique aux organisations « privées »
    - Branche entreprise (1) : permet de définir des entreprises privées
      - Sous cette branche on trouve des entiers par entreprise qui sont attribués par l'IANA
- On trouve dans cette branche les objets spécifiques aux équipements de chaque entreprise qui n'existent pas dans les autres MIB
- Ex : Cisco dispose de la branche 1.3.6.1.4.1.9 (9 = Cisco)

# SNMP


internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
security (5)
snmpV2 (6)
mib (1)
enterprises (1)
system (1)
interfaces (2)
at (3)
ip (4)
icmp (5)
tcp (6)
udp (7)
egp (8)
ibm (2)
cisco (9)
enseirb (9362)
sysDescr (1)
sysUpTime (3)
leds (1)
reserved (2)
led0 (1)
led1 (2)

# SNMP

- Les types de donnée (définis par l'attribut SYNTAX)
  - Integer : ex : état d'une interface (1 : up; 2 : down)
  - Octet String : suite d'octets
  - Counter : ex : nombre d'octets traités par une interface réseau
  - Object identifier : 1.3.1...
  - Sequence : liste de données
  - Sequence of :
  - Ip adress
  - Network address
  - Gauge : ex : température
- SNMP v2 agrémente le protocole d'autres types et améliorations

# SNMP

- MIB-II
- Présente dans tout équipement supportant SNMP
  - 1.3.6.1.2.1 : définit la MIB-II. On y trouve des sous arbres dont :
    - System : 1.3.6.1.2.1.1
    - Interfaces : 1.3.6.1.2.1.2
    - Ip : 1.3.6.1.2.1.3
    - Tcp : 1.3.6.1.2.1.6
    - Udp : 1.3.6.1.2.1.7

- Opérations SNMP
  - **get**
    - Demande de récupération de la valeur d'un OID envoyé vers l'agent
    - **get-response** : envoi de l'info demandée
    - Implémentation Net-SNMP :
      **`snmpget`** `equipement community-string OID`
      La réponse est une association OID = valeur
  - **get-next**
    - Permet la récupération d'un groupe d'OID d'un sous-arbre
    - Implémentation Net-SNMP :
      **`snmpwalk`** `equipement community-string sous-arbre`

- Opérations SNMP (suite)
  - **get-bulk**
    - Demande de récupération de lgroupes d'élements d'une table
    - Implémentation Net-SNMP : **`snmpgetbulk`**
  - **set**
    - Permet de modifier la valeur d'un OID définit comme read-write ou read-only dans la MIB
    - Implémentation Net-SNMP : **`snmpset`**

# SNMP

- Traps SNMP
- Un évènement survient sur l'équipement : l'agent envoie un message particulier (une « trap ») vers le NMS
- La destination de la trap (le NMS) est configuré dans l'agent par son @ IP
- Quelles infos sont envoyées ?
  - Un numéro de trap
    - Coldstart (0)
    - Warmstart (1)
    - Linkdown (2)
    - Linkup (3)
    - Entreprise specific (6)
  - Une association OID = valeur

UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE À PARIS

# *Sommaire*

- SNMP
- Net-SNMP
- MRTG

# Net-SNMP

- Net-SNMP : suite d'outils qui implémentent SNMP
  - Création en 1992 - Carnegie Mellon University (Steve Waldbusser)
  - Code source rendu public en 1995 – Projet amélioré et maintenu par l'Université Davis de Califorine (UCD-SNMP)
  - Changement de nom en 2000 : Net-SNMP
  - Fonctionne sous différents SNMPv1, SNMPv2, SNMPv3

# Net-SNMP

- Net-SNMP : suite d'outils qui implémentent SNMP
  - Outils de récupération d'information : `snmpget, snmpgetnext, snmpwalk, snmptable, snmpdelta,...`
  - Outil pour modifier les informations: `snmpset`
  - Outils pour récupérer des collections d'informations d'un équipement: `snmpdf, snmpnetstat, snmpstatus`
  - Outil pour convertir les infos numériques dans leur forme textuelle: `snmptranslate`
  - Un browser de mib graphique : `tkmib`
  - Un agent répondant aux requêtes SNMP fourni avec un ensemble de MIB : `snmpd`
  - Un daemon permettant de revoir les notifications SNMP (traps) : `snmptrapd`
  - Une librairie pour développer des applis SNMP

# Net-SNMP

- Configuration
  - `/etc/snmp/snmp.conf` : optionnel, il permet de configurer l'ensemble des outils Net-SNMP
  - `/etc/snmp/snmd.conf` : configuration de l'agent
  - `/etc/snmp/snmptrapd.conf` : configuration des notifications SNMP
  - Un utilitaire en perl permet de créer et modifier les fichiers de configuration SNMP : `snmpconf`
  - `# snmpconf -g basic_setup` Sans option snmpconf fonctionne sur un mode « menu »
  - Permet facilement de modifier les community string par défaut

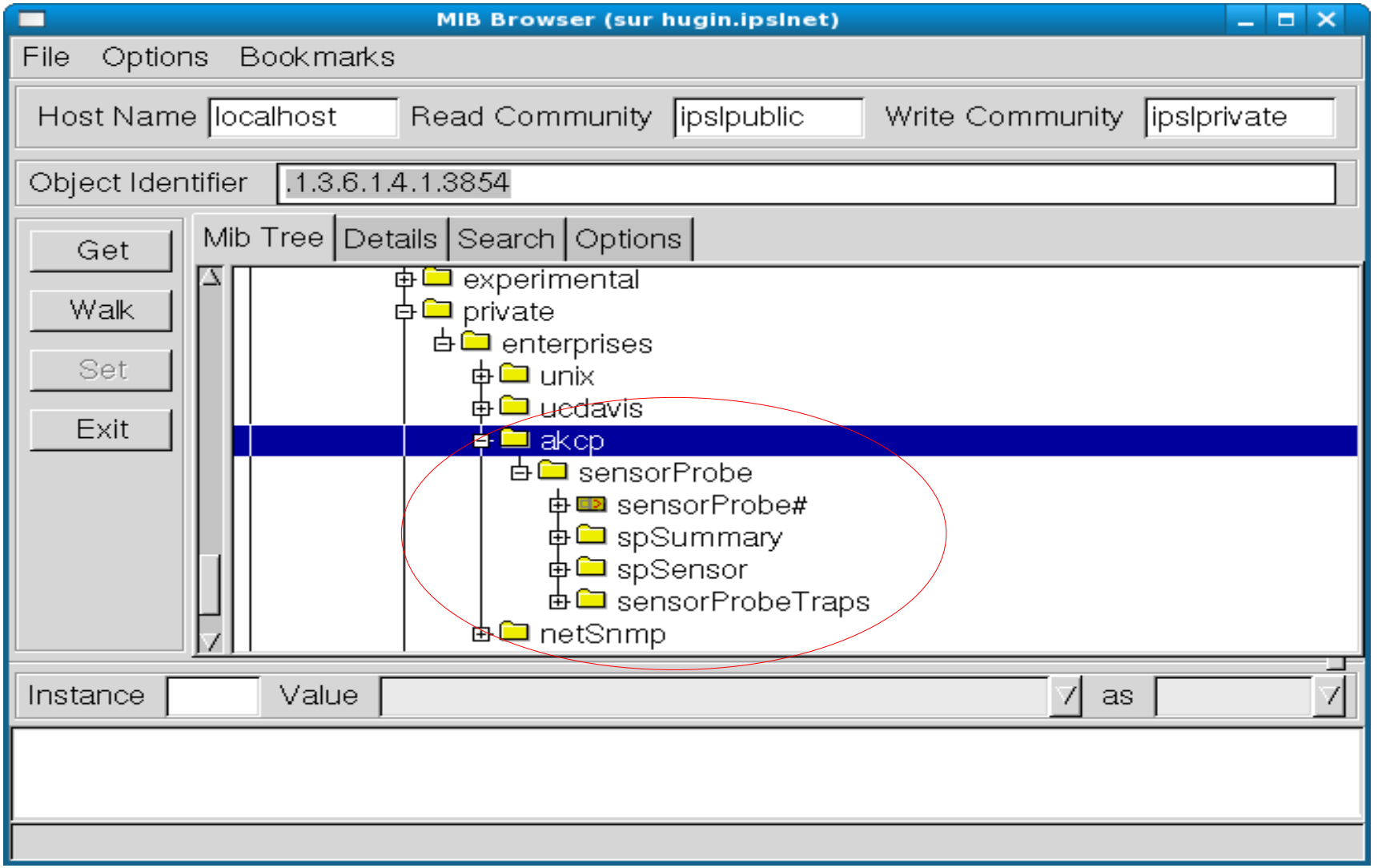
- Configuration des MIBs
  - pour pouvoir accéder aux données d'un équipement il faut tout d'abord connaitre soit leur nom soit leur numéro
  - Ces informations sont stockées dans les MIB qui se trouvent par défaut dans `/usr/share/snmp/mibs`
  - Comment trouver l'information à récupérer ?
    - Directement en « lisant » le fichier de la MIB
    - En utilisant un browser de mib graphique
    - En utilisant la documentation fournie avec l'équipement
  -

# Net-SNMP

- Comment ajouter des MIBs ?
  - Récupérer la mib auprès du constructeur et la copier dans (pour qu'elle soit accessible à tous les utilisateurs) `/usr/share/snmp/mibs`
  - C'est tout
- Ajouter des MIB au niveau des outils ou du NMS n'est pas obligatoire mais cela permet d'utiliser les noms d'objets plutôt que leur numéros
- Exemple : j'ajoute la mib (récupérée auprès du constructeur) correspondant à un boitier de supervision d'infos environnementale (t°, humidité, capteurs,...)

```
# cp sp.mib /usr/share/snmp/mibs
```

- Avec l'utilitaire `mbrowse` je vois qu'une mib privée supplémentaire apparait



# Net-SNMP

- Avec l'utilitaire `snmpwalk` je peux parcourir les infos de mon équipement

```
# snmpwalk -v 1 -c public temp.ipslnet system
SNMPv2-MIB::sysDescr.0 = STRING: ServSensor JR.v2.0 SP2329 Sep 22,05
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.3854.1.2.2.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2212790760) 256 days, 2:38:27.60
SNMPv2-MIB::sysContact.0 = STRING: svp@ipsl.jussieu.fr
SNMPv2-MIB::sysName.0 = STRING: Temp.Ipslnet
SNMPv2-MIB::sysLocation.0 = STRING: Tour 45 Couloir 45-46 Salle 505
SNMPv2-MIB::sysServices.0 = INTEGER: 10
```

- Avec l'utilitaire `snmpget` je peux récupérer une OID particulière

```
# snmpget -v 1 -c public temp.ipslnet .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0
SNMPv2-SMI::enterprises.3854.1.2.2.1.16.1.3.0 = INTEGER: 28
```

- Je peux récupérer la valeur d'un objet par son nom aussi

```
# snmpget -v 1 -c public temp.ipslnet .iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: ServSensor JR.v2.0 SP2329 Sep 22,05
```

# Net-SNMP

- Comment faire pour traduire un nom d'objet en OID ?
  - Commande `snmptranslate`
- Je connais le nom de l'objet qui contient la température d'une sonde et je souhaite récupérer son OID

```
# snmptranslate -m /usr/share/snmp/mibs/sp.mib -On  -IR sensorProbeTempDegree

.1.3.6.1.4.1.3854.1.2.2.1.16.1.3
```

- Je peux également obtenir son nom absolu

```
# snmptranslate -m /usr/share/snmp/mibs/sp.mib -Onf  -IR sensorProbeTempDegree

.iso.org.dod.internet.private.enterprises.akcp.sensorProbe.spSensor.sensorProbeDetail.sensorProbeEntry.sensorProbeTempTable.sensorProbeTempEntry.sensorProbeTempDegree
```

# Net-SNMP

- Une erreur classique
  - Je récupère une OID que je souhaite interroger et cela ne fonctionne pas !

```
# snmpget -v 1 -c public temp.ipslnet .1.3.6.1.4.1.3854.1.2.2.1.16.1.3
Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: SNMPv2-SMI::enterprises.3854.1.2.2.1.16.1.3
```

- Chaque objet possède une instance correspondant à la réalité physique de l'objet. Pour récupérer la valeur d'un objet il faut donc l'instancier même si cet objet ne possède qu'une seule valeur
  - Ajouter « .n » à la fin de l'OID où n correspond à l'instance de l'objet. Soit « .0 » s'il n'y a qu'une seule instance

```
# snmpget -v 1 -c public temp.ipslnet .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0
SNMPv2-SMI::enterprises.3854.1.2.2.1.16.1.3.0 = INTEGER: 23
```

# Net-SNMP

- Comment traiter les notifications (trap) d'un agent
  - Avec Net-SNMP on dispose de `snmptrapd` qu'il faut configurer soit à la main, soit via l'utilitaire `snmpconf`
  - A suivre ...

UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE À PARIS

# *Sommaire*

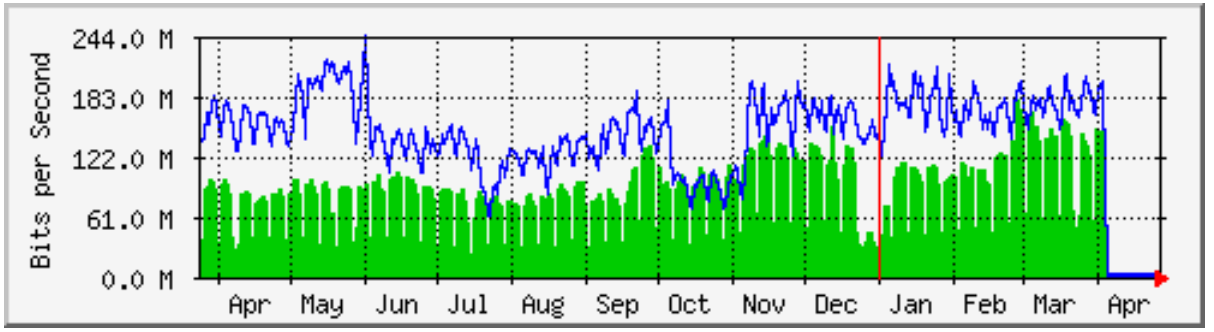
- SNMP
- Net-SNMP
- MRTG

# MRTG

- MRTG – Multi Router Traffic Router
- Développé par Tobias Oetiker
- Outil libre de supervision de charge de réseau d'interface réseau. Il génère des pages html contenant des graphiques représentant les évolution des données récoltées
- Plate-forme Unix et Windows
- Ecrit en Perl (récolte des infos SNMP) et en C (fichiers journaux et graphes)
- Supporte SNMP v2
- Stabilité des fichiers journaux par consolidation des données
- Ensemble d'utilitaires (cfgmaker) qui permettent de créer facilement les fichiers de conf et les pages html

# MRTG

- Les fichiers journaux contiennent les données permettant de suivre l'évolution d'un indicateur pendant 2 ans
- Utilisable pour superviser n'importe quelle variable SNMP ou n'importe quelle données récupérable via un programme externe
- Possibilité de suivre 2 sources de données sur un seul graphe



# MRTG

- Démo : superviser l'interface réseau d'un serveur
- Etapes
  - Installation et configuration de snmpd
  - Installation et configuration de mrtg
    - cfgmaker + indexmaker
  - Exécution périodique de mrtg
- Cf. l'installation pour une mise en situation de MRTG

# Bibliographie

- Bibliographie
  - Essential SNMP – Edition O'Reilly
  - Site officiel de MRTG : http://oss.oetiker.ch/mrtg/
  - Site officiel de Net-SNMP : http://www.net-snmp.org/
  - Howto installation mrtg sous Ubuntu : http://www.lanforums.com/tutorial-25_mrtg_:_monitorer_son_serve
  - http://www.snmplink.org
  - http://www.simple-time.org