



# Gestion et Surveillance de Réseau

## Introduction à SNMP



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license  
(<http://creativecommons.org/licenses/by-nc/3.0/>)

# Présentation générale

- Qu'entend-on par SNMP ?
- OID
- MIB
- Interrogations et invitations à émettre
- Déroulements
- SNMPv3 (Option)

# Qu'entend-on par SNMP ?

SNMP – Simple Network Management Protocol

- Un standard de l'industrie avec des centaines d'outils pour l'exploiter
- Présent sur tout équipement de réseau digne de ce nom

Basé sur des interrogations–réponses : **GET / SET**

- GET sert principalement à la surveillance

Hiérarchie en arborescence

- Interrogations sur les identifiants d'objets (OID, "Object Identifiers")

Concept de bases d'informations de gestion (MIB)

- standard et propriétaire (entreprise)

# Qu'entend-on par SNMP ? (suite)

Protocole UDP, port 161

Différentes versions

- V1 (1988) – RFC1155, RFC1156, RFC1157
  - Spécification d'origine
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Etend la v1, nouveaux types de données, méthodes de recherche améliorées (GETBULK)
  - Nous utilisons la version v2c (sans modèle de sécurité)
- v3 – RFC3411 ... RFC3418 (avec sécurité)

Nous utilisons généralement SNMPv2 (v2c)

# Qu'entend-on par SNMP ? (suite)

## Terminologie :

- Le "manager" ("client" superviseur)
- L'agent (opérant sur l'équipement/le serveur)

# Qu'entend-on par SNMP ? (suite)

## Interrogations types

- Octets en entrée/sortie sur une interface, erreurs
- Charge de l'UC
- Temps utilisable
- température ou autres OID propres au fournisseur

## Pour les hôtes (serveurs ou postes de travail)

- Espace disque
- Logiciels installés
- Processus exécutés
- ...

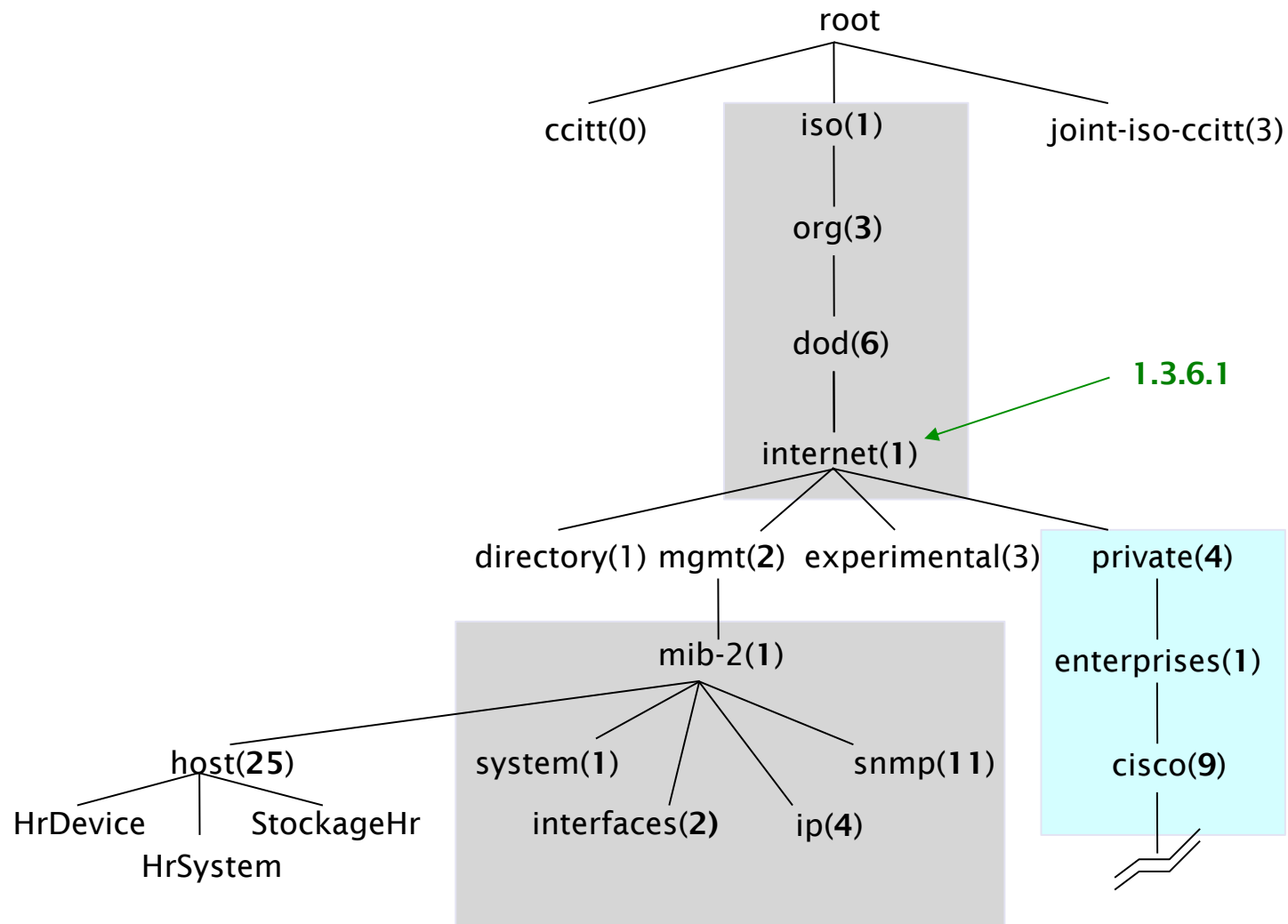
Windows et UNIX ont des agents SNMP

# Principes de fonctionnement

## Commandes de base

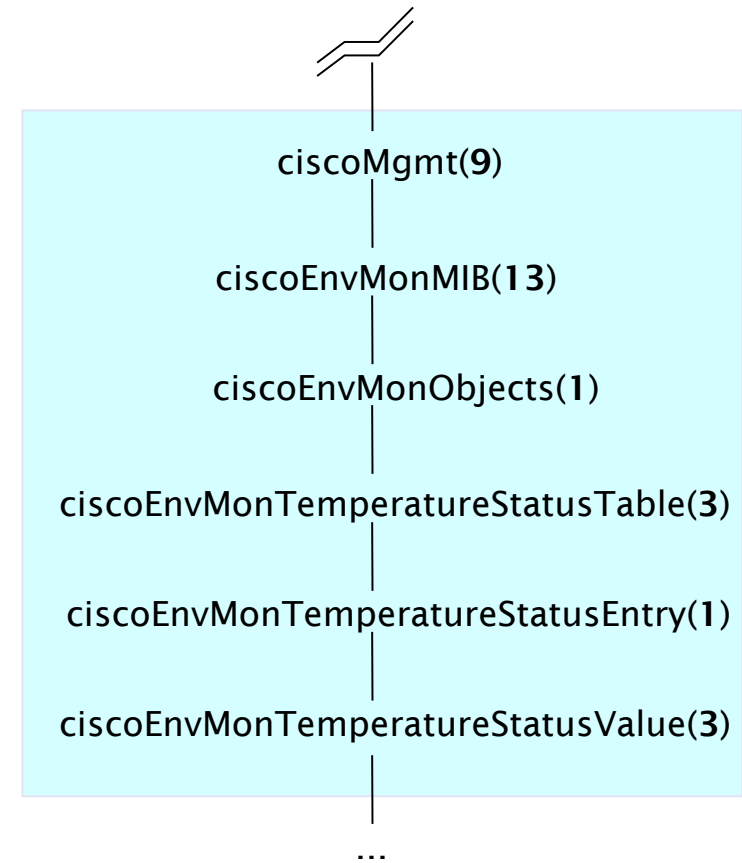
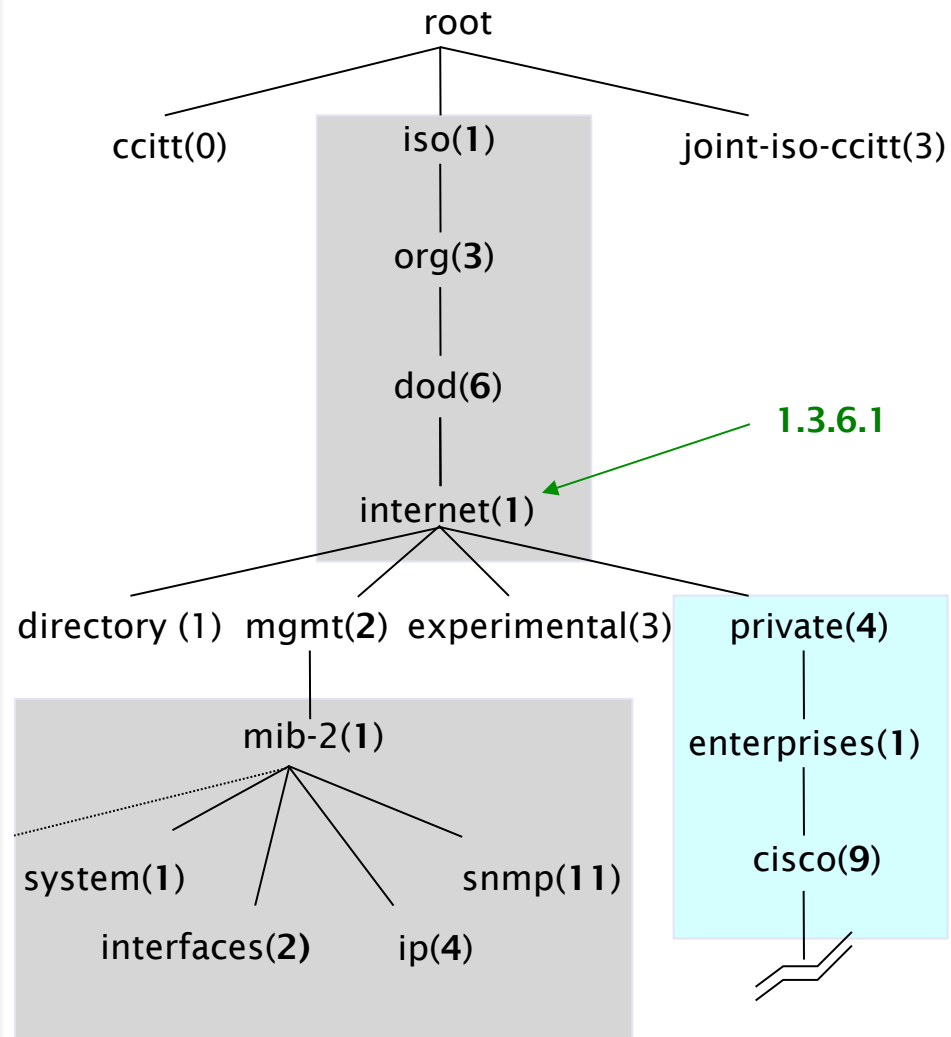
- GET (manager -> agent)
  - Demande une valeur
- GET-NEXT (manager -> agent)
  - Récupère la valeur suivante (liste de valeurs d'une table)
- GET-RESPONSE (agent -> manager)
  - Répond à GET/SET ou erreur
- SET (manager -> agent)
  - Définit une valeur ou réalise une action
- TRAP (agent -> manager)
  - Notification spontanée de l'équipement (arrêt, température au-dessus du seuil...)

# L'arborescence MIB





# L'arborescence MIB (Suite)



# Si les adresses e-mail étaient des OID

user@nsrc.org

*ressemblerait à ceci :*

user@nsrc.entreprises.private.internet.dod.org.iso

user@99999.1.4.1.6.3.1

*sauf que nous écrivons la partie supérieure à gauche :*

1.3.6.1.4.1.99999.117.115.101.114

Un OID est juste une clé unique (dans un dispositif géré) pour un élément d'information.

Il convient de veiller à ce que les fournisseurs n'aient pas d'OID en conflit.

# La MIB internet

- **directory** (1)            répertoire OSI
- **mgmt** (2)                objets RFC standard
- **experimental** (3)       expérimentations sur internet
- **private** (4)            propriétaire
- **security** (5)            sécurité
- **snmpV2** (6)            SNMP interne

# OID et MIB

- Navigation descendante dans l'arborescence
- OID séparés par '.'
  - 1.3.6.1.4.1.9. ...
- Un OID correspond à une étiquette
  - .1.3.6.1.2.1.1.5 => sysName
- Le chemin complet :
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName
- Comment passer des OID à des étiquettes (et inversement ?)
  - Utiliser des fichiers MIB !

# MIB

- Les MIB sont des fichiers définissant des objets pouvant faire l'objet d'interrogations ; ces fichiers intègrent :
  - Le nom de l'objet
  - La description de l'objet
  - Le type de données (entiers, textes, listes)
- Les MIB revêtent la forme de texte structuré en notation ASN.1
- Les MIB types incluent :
  - MIB-II – (RFC1213) – groupe de sous-MIB
  - HOST-RESOURCES-MIB (RFC2790)

# MIB - 2

Les MIB permettent également d'interpréter une valeur retournée par un agent

- Par exemple, si l'état d'un ventilateur est 1,2,3,4,5,6 – que signifie cette valeur ?

# MIB - exemple

```
sysUpTime OBJECT-TYPE
    SYNTAX TimeTicks
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "The time (in hundredths of a second) since the
        network management portion of the system was last
        re-initialized."
    ::= { system 3 }
```

**sysUpTime OBJECT-TYPE**  
Définit l'objet `sysUpTime`.

**SYNTAX TimeTicks**  
Objet de type `TimeTicks`. Les types d'objet sont spécifiés dans le SMI mentionné précédemment.

**ACCESS read-only**  
Cet objet peut être uniquement lu par SNMP (requête `get`) ; il ne peut être modifié (requête `set`).

**STATUS mandatory**  
Cet objet doit être mis en œuvre sur n'importe quel agent SNMP.

**DESCRIPTION**  
Description de l'objet

**::= { system 3 }**  
L'objet `sysUpTime` constitue la troisième branche de l'arborescence du groupe d'objets système.

# MIB - exemple (suite)

```
CiscoEnvMonState ::= TEXTUAL-CONVENTION
```

```
STATUS current
```

```
DESCRIPTION
```

```
Représente l'état d'un dispositif supervisé.
```

```
Les valeurs valides sont :
```

```
normal(1):          l'environnement est bon, par exemple  
faible température.
```

```
warning(2):         l'environnement est mauvais, par exemple  
température au-dessus de la plage de  
fonctionnement normal, mais pas trop élevée.
```

```
critical(3):        l'environnement est très mauvais, par exemple  
température très supérieure à la limite  
de fonctionnement normal.
```

```
shutdown(4):        l'environnement est le pire, le système  
doit être arrêté immédiatement.
```

```
notPresent(5):      le moniteur de l'environnement est absent, par  
exemple il n'y a pas de capteurs de  
température.
```

```
notFunctioning(6):  le moniteur de l'environnement ne fonctionne pas  
correctement, par exemple un capteur de  
température génère des données anormales par  
exemple une température de 1000° C.
```



# Interrogation d'un agent SNMP

## Commandes de requête classiques :

- snmpget
- snmpwalk
- snmpstatus
- snmptable

## Syntaxe :

```
snmpXXX -c community -v1 host [oid]  
snmpXXX -c community -v2c host [oid]
```

# Interrogation d'un agent SNMP (Suite)

## Prenons un exemple

```
-snmpstatus -c NetManage -v2c  
10.10.0.254
```

```
-snmpget -c NetManage -v2c  
10.10.0.254 .iso.org.dod.internet.m  
gmt.mib-2.interfaces.ifNumber.0
```

```
-snmpwalk -c NetManage -v2c  
10.10.0.254 ifDescr
```

# Interrogation d'un agent SNMP (Suite)

## Communauté :

- Chaîne de "sécurité" (mot de passe) définissant le niveau accès du manager - RO (lecture uniquement) ou RW (lecture-écriture)
- Forme d'authentification la plus simple dans SNMP

## OID

- Une valeur, .1.3.6.1.2.1.1.5.0, par exemple, le nom correspondant
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0

## Demandons le nom du système (avec l'OID ci-dessus)

- À quoi correspond le .0 ? Que remarquez-vous ?

# Prochains exercices...

- Utilisation de snmpwalk, snmpget
- Configuration de SNMPD
- Chargement des MIB
- Configuration de SNMPv3 (facultatif)

# Références

- *Essential SNMP* (O'Reilly Books) Douglas Mauro, Kevin Schmi
- *SNMP de base avec Cisco*  
<http://www.cisco.com/warp/public/535/3.html>  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/snmp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm)
- Wikipedia:  
[http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol)
- Navigateur MIB de supervision d'IP  
[http://support.ipmonitor.com/mibs\\_byoidtree.aspx](http://support.ipmonitor.com/mibs_byoidtree.aspx)  
Navigateur MIB Cisco : <http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>
- Navigateur MIB Java open source  
<http://www.kill-9.org/mbrowse>  
<http://www.dwipal.com/mibbrowser.htm> (Java)
- Liaison SNMP – recueil de ressources SNMP  
<http://www.snmplink.org/>
- Outils SNMP open source Net-SNMP  
<http://net-snmp.sourceforge.net/>
- Intégration avec Nagios <http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html>

# Documents optionnels

## SNMP Version 3

# SNMP et Sécurité

- Les versions SNMP 1 et 2c ne sont pas sûres
- La version 3 de SNMP a été créée pour résoudre ce problème
- Composants
  - Dispatcher
  - Sous-système de traitement des messages
  - Sous-système de sécurité
  - Sous-système de contrôle d'accès

# SNMP version 3 (SNMPv3)

Le module le plus commun repose sur l'utilisateur ou un "modèle de sécurité utilisateur"

- **Authenticité et intégrité** : Les touches sont utilisées pour les utilisateurs et les messages ont une signature numérique générée par hachage (MD5 ou SHA)
- **Confidentialité** : Les messages peuvent être cryptés au moyen d'algorithmes (DES) à clé secrète (privée)
- **Validité temporaire** : Utilise une horloge synchronisée avec une fenêtre 150 secondes et contrôle de séquence.



# Niveaux de sécurité

## **noAuthPriv**

- Pas d'authentification, pas de confidentialité

## **authNoPriv**

- Authentification sans confidentialité

## **authPriv**

- Authentification avec confidentialité

# Configuration SNMPv3 avec Cisco

```
snmp-server view vista-ro internet included
snmp-server group ReadGroup v3 auth read vista-ro
snmp-server user admin ReadGroup v3 auth md5 xk122r56
```

Ou encore :

```
snmp-server user admin ReadGroup v3 auth md5 xk122r56
priv des56 D4sd#rr56
```

# Configuration SNMPv3 avec Net-SNMP

```
# apt-get install snmp snmpd
# net-snmp-config --create-snmpv3-user -a "xk122r56" admin
  /usr/sbin/snmpd
# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56"
  127.0.0.1
```