



Surveillance du réseau et de gestion

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/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.



Présentation générale

- Qu'entend-on par SNMP ?
- OID
- MIB
- Interrogations et invitations à émettre
- Déroutements

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 superviser

Hiérarchie en arborescence

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

Base d'informations de gestion (MIB, "Management Information Base")

- 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
 - étend 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'est-ce que 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 stations de travail)

- espace disque
- logiciel installé
- processus exécutés
- ...

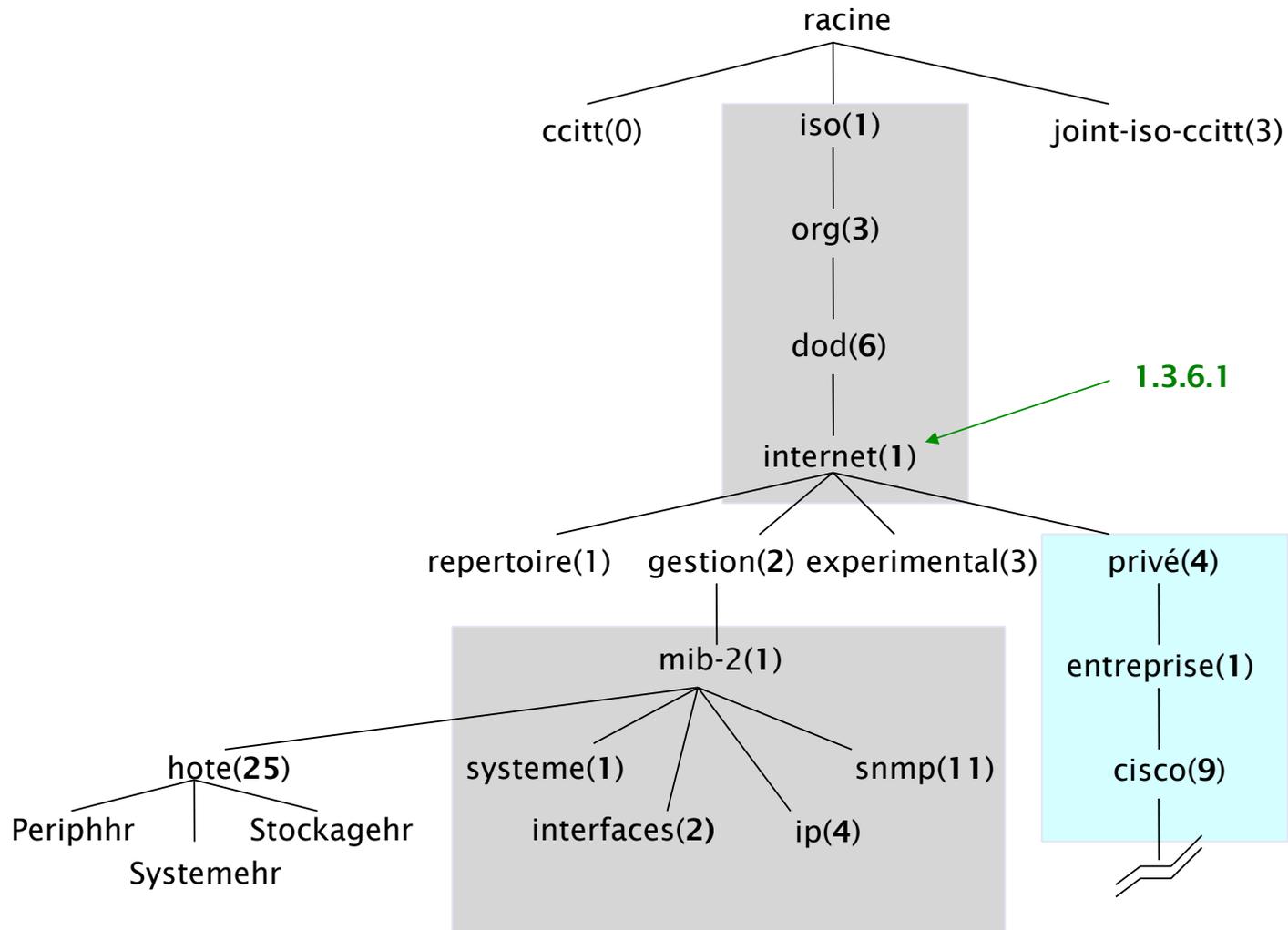
Windows et UNIX ont des agents SNMP.

Principes de fonctionnement

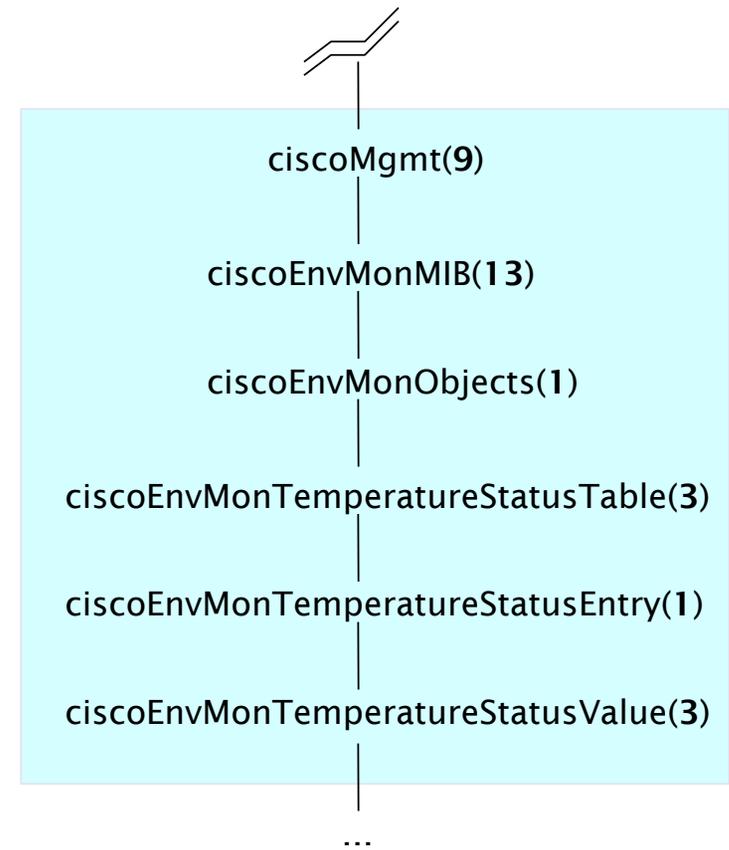
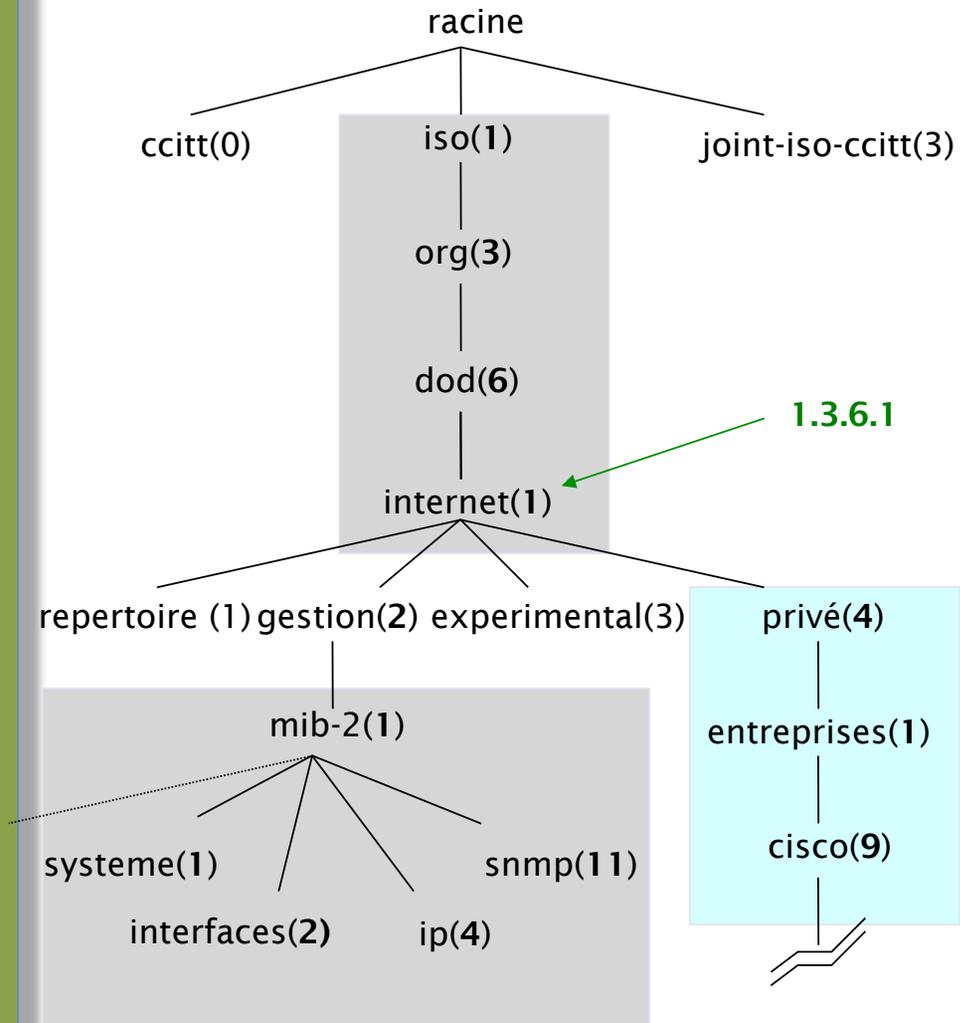
Commandes de base

- GET (manager -> agent)
 - demande une valeur
- GET-NEXT (manager -> agent)
 - demande de la valeur suivante (liste de valeurs d'une table)
- GET-RESPONSE (agent -> manager)
 - réponse au 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)



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 vers le bas de l'arborescence
- OID séparés par '.'
 - 1.3.6.1.4.1.9. ...
- OID correspond à une étiquette
 - .1.3.6.1.2.1.1.5 => sysName
- Chemin complet :
 - .iso.org.dod.internet.mgmt.mib-2.system.sysName
- Comment passer des OID à des étiquettes (et inversement ?)
 - utiliser des fichiers MIB !

Les MIB

- Les MIB sont des fichiers définissant des objets pouvant faire l'objet d'interrogations, dont :
 - des noms d'objet
 - des descriptions d'objet
 - des types 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

- si l'état d'un ventilateur est 1,2,3,4,5,6 – quelle est la signification de cette valeur ?

MIB - exemple

```
sysUpTime OBJECT-TYPE
    SYNTAX TimeTicks
    ACCESS lecture uniquement
    STATUS obligatoire
    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 `get`).

STATUS mandatory
Cet objet doit être mis en oeuvre 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

```
CiscoEnvMonState ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "Represents the state of a device being monitored.
        Valid values are:

        normal(1):          the environment is good, such as low
                           temperature.

        warning(2):        the environment is bad, such as temperature
                           above normal operation range but not too
                           high.

        critical(3):       the environment is very bad, such as
                           temperature much higher than normal
                           operation limit.

        shutdown(4):       the environment is the worst, the system
                           should be shutdown immediately.

        notPresent(5):     the environmental monitor is not present,
                           such as temperature sensors do not exist.

        notFunctioning(6): the environmental monitor does not
                           function properly, such as a temperature
                           sensor generates a abnormal data like
                           1000 C.

        "
```

Interrogation d'un agent SNMP

Commandes de requête classiques :

- snmpget
- snmpwalk
- snmpstatus

Syntaxe :

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

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

Interrogation d'un agent SNMP

Prenons un exemple

- snmpstatus -c s3cr3t -v1 169.223.142.1
- snmpget -c s3cr3t -v1
169.223.142.10 .iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0
- snmpwalk -c s3cr3t -v1 169.223.142.20
ifDescr

Interrogation d'un agent SNMP (suite)

Communauté :

- chaîne de "sécurité" (mot de passe) définissant l'accès - RO (lecture uniquement) ou RW (lecture-écriture) – du gestionnaire d'interrogations
- forme d'authentification la plus simple dans SNMP

OID

- une valeur, .1.3.6.1.2.1.1.5.0, par exemple, ou son nom
- .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 ?



A suivre...

- Utilisation de snmpwalk, snmpget
- Configuration de SNMPD
- Chargement des MIB

Références

- 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
- Wikipedia
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- Navigateur MIB de supervision d'IP
http://support.ipmonitor.com/mibs_byoidtree.aspx
- Navigateur MIB Cisco
<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>
- Navigateur MIB Java libres
<http://www.kill-9.org/mbrowse>
<http://www.dwipal.com/mibbrowser.htm> (Java)
- Liaison SNMP – ressources SNMP
<http://www.snmplink.org/>
- Outils SNMP Net-SNMP libres
<http://net-snmp.sourceforge.net/>
- Intégration avec Nagios
<http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html>