Supervision

Bruno BEAUFILS

2021/2022

Principe SNMP

- Éléments
  - **manager** : machine qui centralise les informations
    - logiciel superviseur
    - interaction avec l'opérateur humain
    - station d'administration
  - **agents** : éléments à superviser
    - logiciel contrôleur de l'élément
    - gère un dépôt des informations de gestion
- Cas de fonctionnement
  - **consultation**
    1. le superviseur demande une donnée à un agent
    2. l'agent renvoie l'information demandée
  - **configuration**
    1. le superviseur demande une modification à un agent
    2. l'agent renvoie la nouvelle valeur
  - **notification**
    - l'agent envoie une information à un superviseur
- Périphériques habituellement ciblés :
  - **éléments réseaux actifs** (routeurs, commutateurs, etc.)
  - **imprimantes**
  - **carte de gestion de serveur** (*Baseboard Management Controller*)
  - **serveurs** (via logiciel)

Principe SNMP

- Éléments
  - **manager** : machine qui centralise les informations
    - logiciel superviseur
    - interaction avec l'opérateur humain
    - station d'administration
  - **agents** : éléments à superviser
    - logiciel contrôleur de l'élément
    - gère un dépôt des informations de gestion
- Cas de fonctionnement
  - **consultation**
    1. le superviseur demande une donnée à un agent
    2. l'agent renvoie l'information demandée
  - **configuration**
    1. le superviseur demande une modification à un agent
    2. l'agent renvoie la nouvelle valeur
  - **notification**
    - l'agent envoie une information à un superviseur
- Périphériques habituellement ciblés :
  - **éléments réseaux actifs** (routeurs, commutateurs, etc.)
  - **imprimantes**
  - **carte de gestion de serveur** (*Baseboard Management Controller*)
  - **serveurs** (via logiciel)

Principe SNMP

- Éléments
  - **manager** : machine qui centralise les informations
    - logiciel superviseur
    - interaction avec l'opérateur humain
    - station d'administration
  - **agents** : éléments à superviser
    - logiciel contrôleur de l'élément
    - gère un dépôt des informations de gestion
- Cas de fonctionnement
  - **consultation**
    1. le superviseur demande une donnée à un agent
    2. l'agent renvoie l'information demandée
  - **configuration**
    1. le superviseur demande une modification à un agent
    2. l'agent renvoie la nouvelle valeur
  - **notification**
    - l'agent envoie une information à un superviseur
- Périphériques habituellement ciblés :
  - **éléments réseaux actifs** (routeurs, commutateurs, etc.)
  - **imprimantes**
  - **carte de gestion de serveur** (*Baseboard Management Controller*)
  - **serveurs** (via logiciel)

Principe SNMP

- Éléments
  - **manager** : machine qui centralise les informations
    - logiciel superviseur
    - interaction avec l'opérateur humain
    - station d'administration
  - **agents** : éléments à superviser
    - logiciel contrôleur de l'élément
    - gère un dépôt des informations de gestion
- Cas de fonctionnement
  - **consultation**
    1. le superviseur demande une donnée à un agent
    2. l'agent renvoie l'information demandée
  - **configuration**
    1. le superviseur demande une modification à un agent
    2. l'agent renvoie la nouvelle valeur
  - **notification**
    - l'agent envoie une information à un superviseur
- Périphériques habituellement ciblés :
  - **éléments réseaux actifs** (routeurs, commutateurs, etc.)
  - **imprimantes**
  - **carte de gestion de serveur** (*Baseboard Management Controller*)
  - **serveurs** (via logiciel)

Principe SNMP

- Éléments
  - **manager** : machine qui centralise les informations
    - logiciel superviseur
    - interaction avec l'opérateur humain
    - station d'administration
  - **agents** : éléments à superviser
    - logiciel contrôleur de l'élément
    - gère un dépôt des informations de gestion
- Cas de fonctionnement
  - **consultation**
    1. le superviseur demande une donnée à un agent
    2. l'agent renvoie l'information demandée
  - **configuration**
    1. le superviseur demande une modification à un agent
    2. l'agent renvoie la nouvelle valeur
  - **notification**
    - l'agent envoie une information à un superviseur
- Périphériques habituellement ciblés :
  - **éléments réseaux actifs** (routeurs, commutateurs, etc.)
  - **imprimantes**
  - **carte de gestion de serveur** (*Baseboard Management Controller*)
  - **serveurs** (via logiciel)

Standards

SNMP définit 2 choses :

1. le **protocole de communication**
   - la façon dont est transportée l'information
2. les **informations dynamiques**, fournies par les différents agents SNMP
   - informations spécifiées dans la *MIB* (Management Information Base)

En détail ça donne 3 standards :

1. Définir (décrire) les données et leur accés : **SMI**
   - *Structure of Management Information*
   - RFC 1155 puis RFC 2578-RFC 2580
   - format de description les bases d'informations disponibles
   - sous ensemble de ASN.1
2. Lister les données disponibles : **MIB**
   - *Management Information Base*
   - RFC 1156 puis RFC 1213 puis ...
   - 2 rôles
     - Description des données disponibles
     - Base des données disponibles
3. Communiquer : **SNMP**
   - *Simple Network Management Protocole*
   - RFC 1157 puis RFC 1441-RFC 1452 puis RFC 3411-RFC 3418

Standards

SNMP définit 2 choses :

1. le **protocole de communication**
   - la façon dont est transportée l'information
2. les **informations dynamiques**, fournies par les différents agents SNMP
   - informations spécifiées dans la *MIB* (Management Information Base)

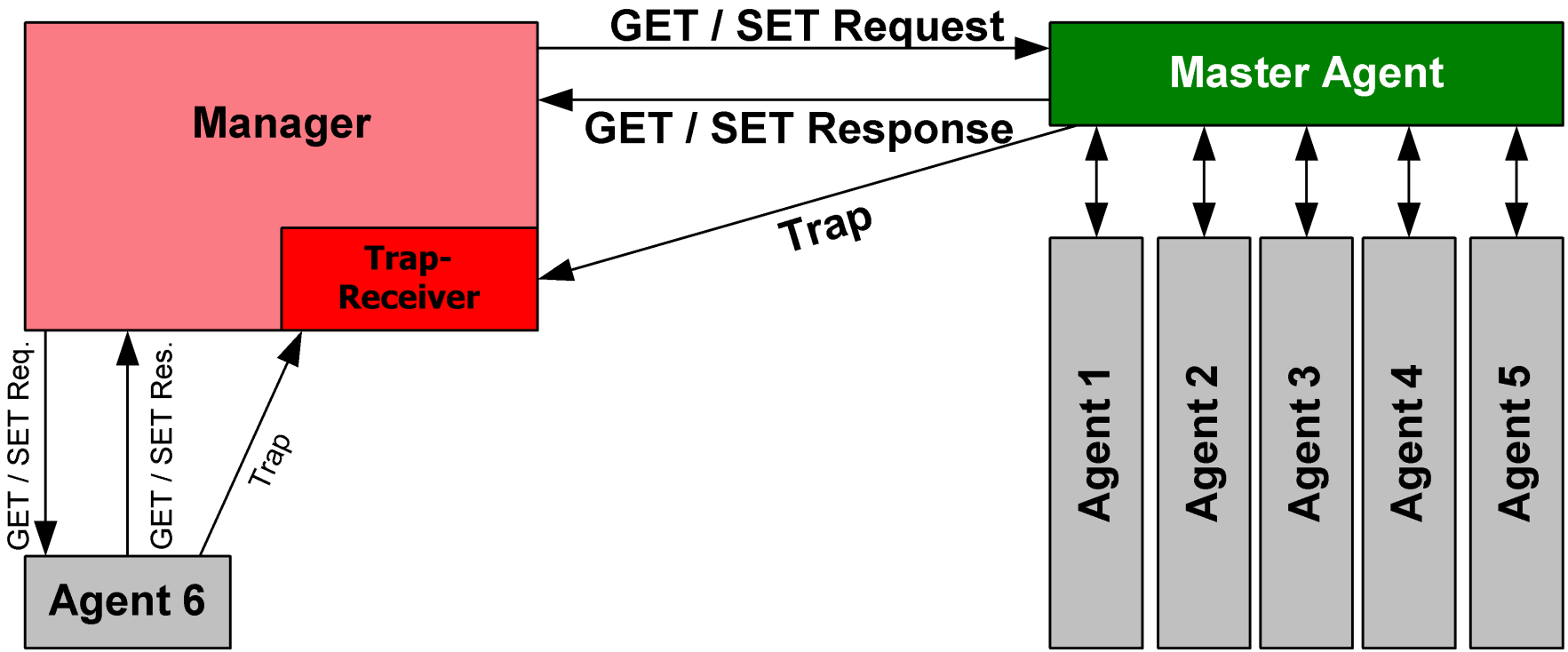
En détail ça donne 3 standards :

1. Définir (décrire) les données et leur accés : **SMI**
   - *Structure of Management Information*
   - RFC 1155 puis RFC 2578-RFC 2580
   - format de description les bases d'informations disponibles
   - sous ensemble de ASN.1
2. Lister les données disponibles : **MIB**
   - *Management Information Base*
   - RFC 1156 puis RFC 1213 puis ...
   - 2 rôles
     - Description des données disponibles
     - Base des données disponibles
3. Communiquer : **SNMP**
   - *Simple Network Management Protocole*
   - RFC 1157 puis RFC 1441-RFC 1452 puis RFC 3411-RFC 3418

SNMPv1 : généralités

- **RFC-1157**
- Protocoles sur UDP
  - port 161 pour les requêtes
  - port 162 pour les notifications
  - détection de panne par polling (interrogation) et temporisateur (par le manager)
  - pas de stockage d'état côté agent
- 3 opérations
  - `get` récupération de valeurs scalaires
  - `set` modification de valeurs scalaires
  - `trap` envoi de valeur scalaire à un manager

SNMP : principe



Crédits SNMP Center

SNMPv1 : structure des paquets

1. Version
2. Community
3. SNMP PDU (Packet Data Unit)
    1. PDU Type
    2. Request ID
    3. Error Status
    4. Error Index
    5. Variable Bindings
        1. Nom1
        2. Valeur1
        3. Nom2
        4. Valeur2
        5. etc.

SNMPv1 : opérations

- `get`
  - récupérer une ou plusieurs variables (valeurs)
  - erreurs
    - `noSuchName` objet inconnu
    - `tooBig` la réponse ne tient pas dans un paquet
    - `genErr` autre erreur
- `get-next`
  - récupérer la ou les variables suivantes (valeurs)
  - parcours dans l'ordre lexicographique
  - erreurs
    - `noSuchName` fin de la MIB
    - `tooBig` la réponse ne tient pas dans un paquet
    - `genErr` autre erreur
- `set`
  - assigner une valeur à une ou plusieurs variables
  - erreurs
    - `noSuchName`
    - `badValue`
    - `tooBig`
    - `genErr`

SNMPv1 : opérations (suite)

- `trap`
  - envoyer une notification à un manager
  - pas d'acquittement
  - configuration du manager dans l'agent
  - utilisation un `TrapID` et un `OID`
  - `TrapID`
    - 0 -> `coldStart`
    - 1 -> `warmStart`
    - 2 -> `linkDown`
    - 3 -> `linkUp`
    - 4 -> `authenticationFailure`
    - 5 -> `egpNeighborLoss`
    - 6 -> `entrepriseSpecific`

SNMPv1 : communautés

- Communauté
  - regroupement d'éléments (*managers* et *agents*) sous un nom
  - sert à fixer les relations d'administrations (politiques d'accès)
  - ≈ mot de passe
- 3 types
  - lecture seule (public)
  - lecture-écriture (private)
  - notification (trap)
- circulent en clair

Généralités

- Permet de définir (décrire) le contenu des *objets* gérés par les agents
  - au final ce sera une hiérarchie (un arbre) d'objets gérés (*MIB*)
- SMIv1 (RFC-1155)
- SMIv2 (RFC-2578, RFC-2579, RFC-2580)
- Description compacte des MIB (RFC-1212)

Un langage

- Basé sur ASN.1
  - Abstract Syntax Number 1
  - standard spécifiant une notation pour décrire des structures de données
  - description indépendante d'un encodage (comme XDR)
  - Tout SNMP est spécifié en ASN.1 (y compris les trames réseau)
  - Lisible par les humains et pas ambigu
- Compilation de la notation lisible vers la notation codée
  - description (MIB) écrite au format ASN.1
  - correspondance syntaxe abstraite vers format de transfert défini par BER
    - Basic Encoding Rules
    - valeur encodée par une chaîne d'octet
    - format : type, longueur, valeur

Concepts

2 types d'objets

- valeurs uniques (scalaire)
- type complexes (tableaux)

SNMP ne manipule que des scalaires

Types SMIv1

- Types simple

  `INTEGER`
  `OCTET STRING`
  `OBJECT IDENTIFIER`

- Types applicatifs

  `Gauge`
  `Counter`
  `TimeTicks`
  `IpAddress`
  `Opaque`
  `NetworkAddress`

Types SMIv2

- Types simples

  `INTEGER`
  `OCTET STRING`
  `OBJECT IDENTIFIER`
  `Integer32`

- Types applicatifs

  `Unsigned32`
  `Gauge32`
  `Counter32`
  `Counter64`
  `TimeTicks`
  `IpAddress`
  `Opaque`

- Pseudo type

  `BITS`

Définitions

- Définition d'un objet (syntaxe SMIv1)

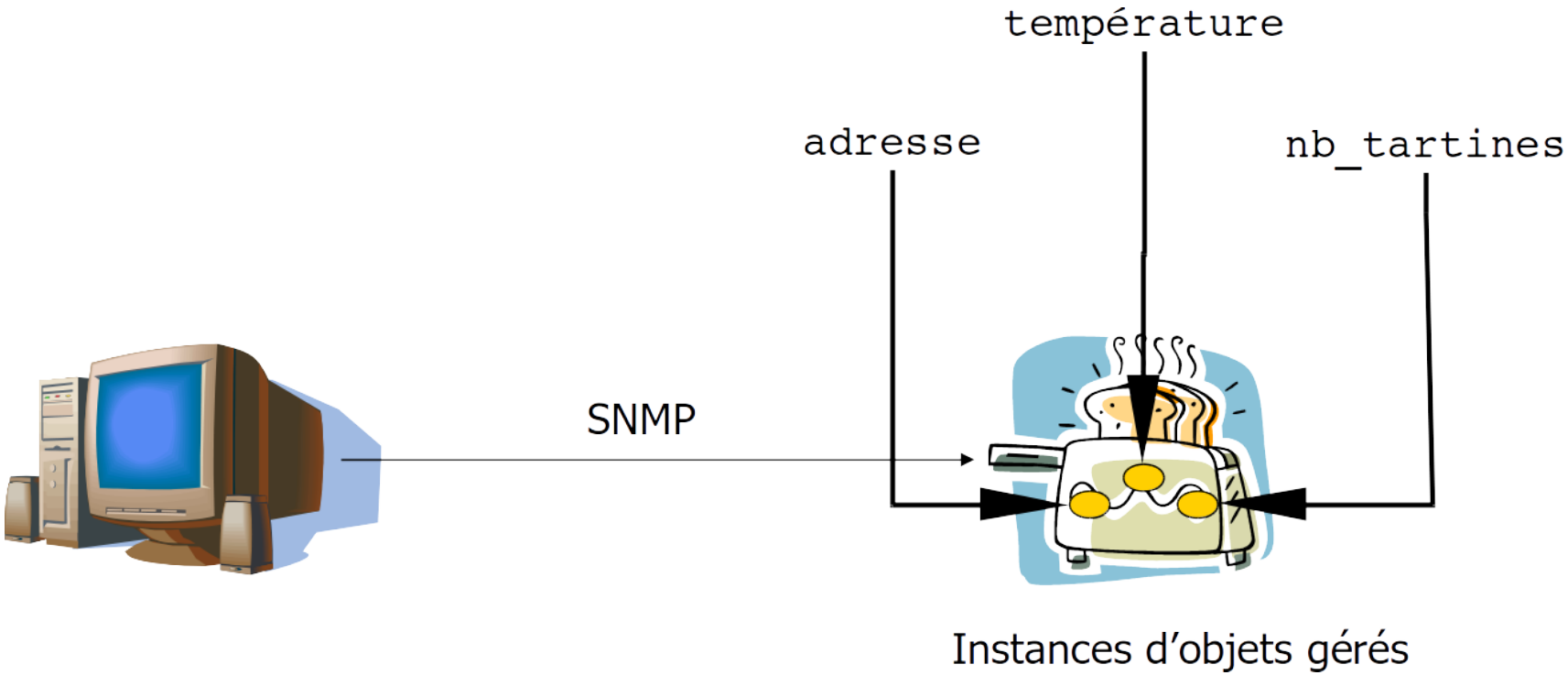
```
<name> OBJECT-TYPE
        SYNTAX <datatype>
        ACCESS <read-only|read-write|write-only| not-accessible>
        STATUS <mandatory|optional|obsolete>
        DESCRIPTION « description de l'objet »
::= { <OID unique>}
```

- Définition d'un objet (syntaxe SMIv2)

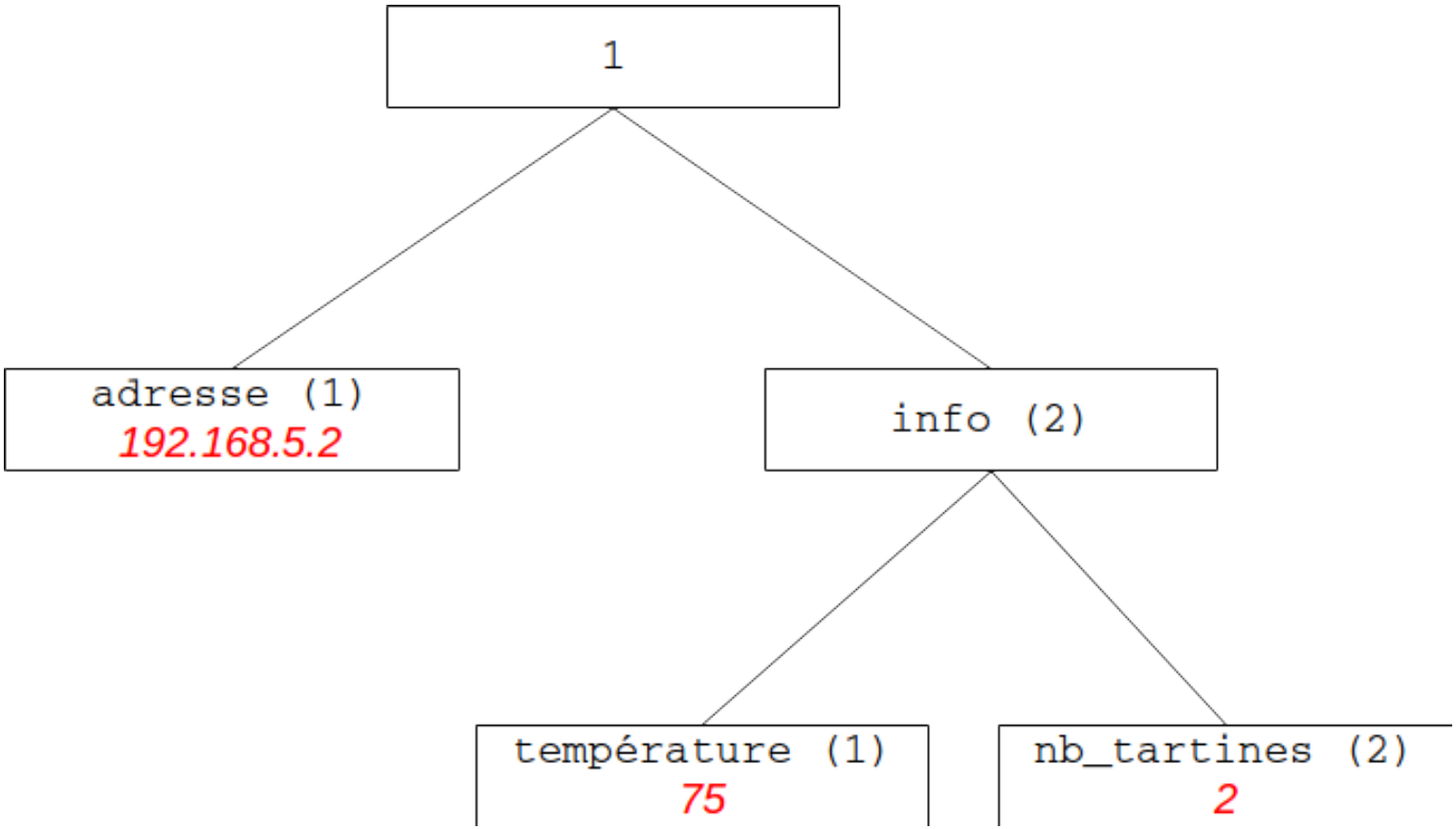
```
<name> OBJECT-TYPE
        SYNTAX <datatype>
        UnitParts <unité de mesure>
        MAX-ACCESS <read-only|read-write|read-create|not-accessible|accessible-for-notify
        STATUS <mandatory|optional|obsolete>
        DESCRIPTION « description de l'objet »
        AUGMENTS { <nom de table> }
::= { <OID unique>}
```

- Autres conventions
  - Commentaires commencent par --
  - nom commençant par des minuscules : objets

Exemple : schéma



Exemple : arbre des données



Exemple : objets gérés

- `adresse`
  - OID : 1.1
  - Instance : 1.1.0
  - Valeur : 192.168.5.2
- `température`
  - OID : 1.2.1
  - Instance : 1.2.1.0
  - Valeur : 75
- `nb_tartines`
  - OID : 1.2.2
  - Instance : 1.2.2.0
  - Valeur : 2

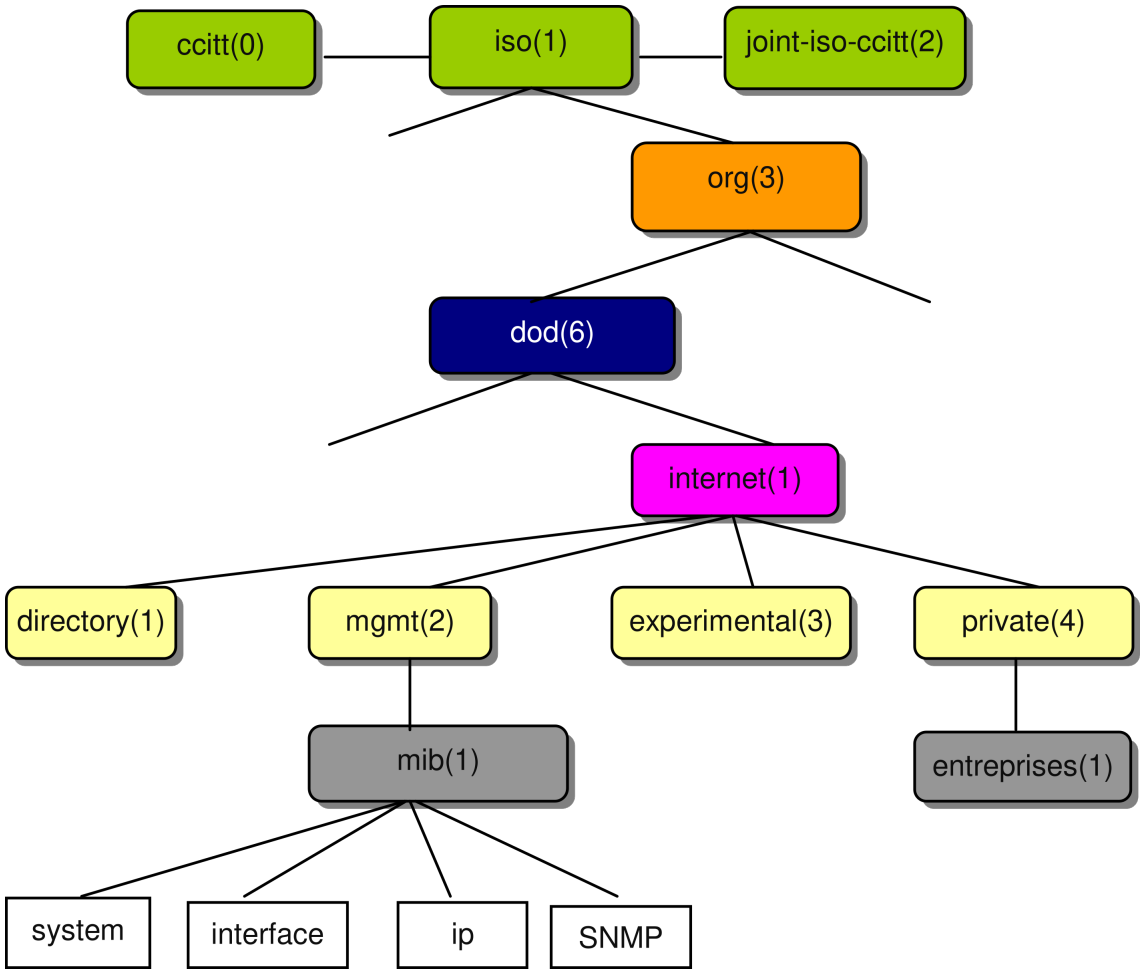
Tableaux

- Un objet tableau a pour syntaxe `SEQUENCE OF <TrucBidule>`
  - l'accès n'est pas permis directement (`not-accessible`)
- `<TrucBidule>` défini les colonnes (nom et types) du tableau
  - la syntaxe est une `SEQUENCE`
  - le nom est capitalisé par convention
  - liste les objets dans les colonnes
- Il faut ensuite définir les lignes par des objets
  - définition contient un `INDEX`
- En résumé
  - Un tableau est défini par ses colonnes
  - Une des colonnes est un index (une clé)
  - La ligne est repérée par le numéro d'instance

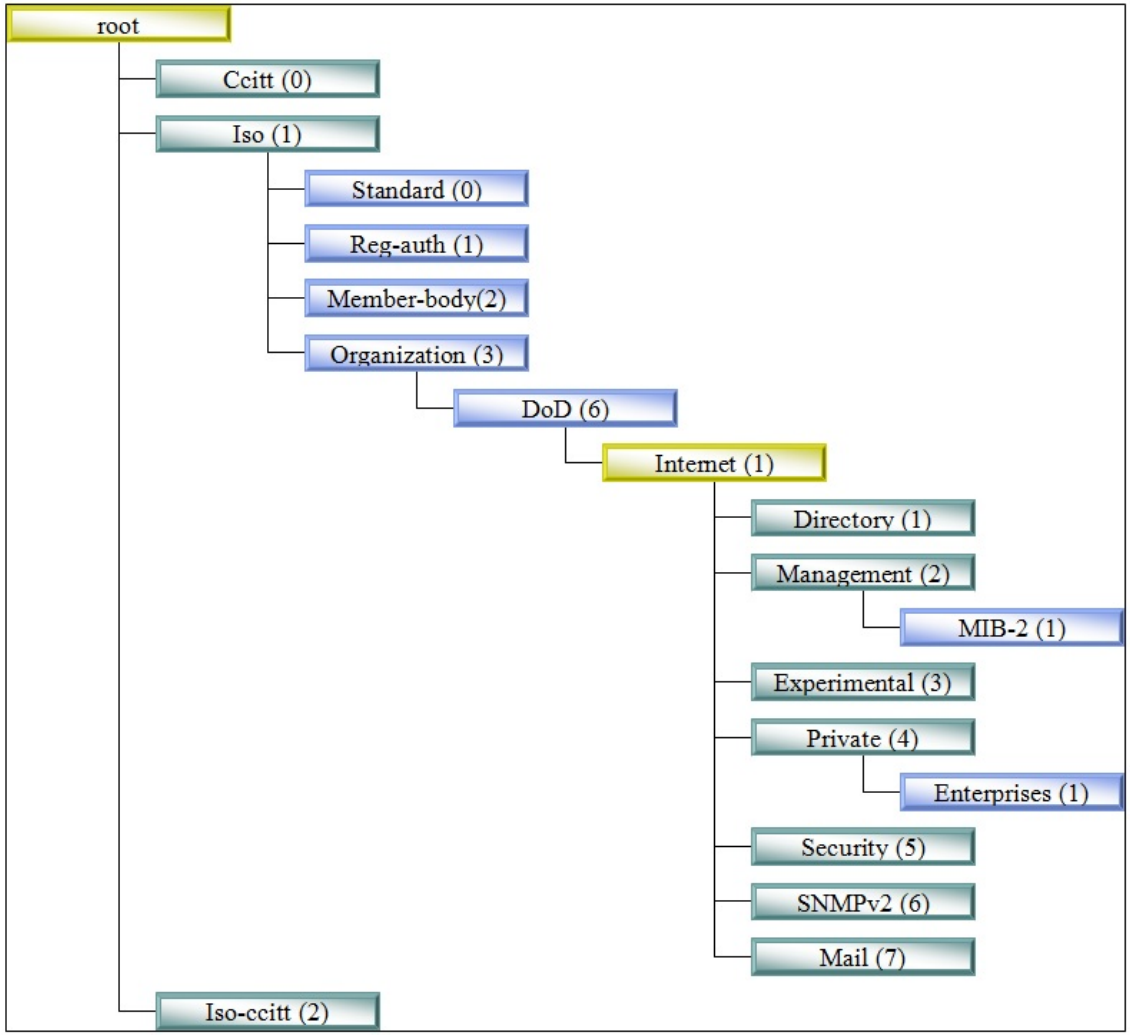
Définition

- la **MIB** (*Management Information Base*) est à la fois
  - la description des données disponible, structurée comme un **arbre**
  - la **base des données** (valeur) gérés par un agent
- chaque données (variable et valeur) est identifiée par un identifiant
  - **OID** (*Object Identifier*) : séquence de nombre séparé par des points
  - exemple `ifDescr` est identifié par `1.3.6.1.2.1.2.2.1.2`
- MIB = arbre hiérarchisé très dense
  - plusieurs milliers d'OID dans la MIB
  - impossible de décrire tous ces OID dans un seul fichier MIB
  - comme pour le DNS différentes parties de la MIB dans différents fichiers MIB
    - chaque fichier MIB est responsable d'une branche particulière
- une branche particulière : **private enterprises** (OID 1.3.6.1.4.1)
  - MIB spécifique à chaque entreprise qui le demande
  - exemple :
    - Cisco avec un OID 1.3.6.1.4.1.9
    - HP avec 1.3.6.1.4.1.11

Arbre des OID (supervision)



Arbre des OID (supervision) (suite)



MIB2 : **1.3.6.1.2.**

Quelques MIB

- SNMP - SMI : RFC 1155 - Defines the Structure of Management Information (SMI)
- MIB-I : RFC 1156 - Historically used with CMOT , not to be used with SNMP ;
- SNMPv2-SMI : RFC 2578 - Structure of Management Information Version 2 (SMIv2) ;
- **MIB-II** : RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets
- SNMPv2-MIB : RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- TCP-MIB : RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP)
- UDP-MIB : RFC 4113 - Management Information Base for the User Datagram Protocol (UDP)
- IP-MIB : RFC 4293 - Management Information Base for the Internet Protocol (IP)
- IF-MIB : RFC 2863 - The Interfaces Group MIB
- ENTITY-MIB : RFC 4133 - Entity MIB (Version 3)
- ENTITY-STATE-MIB : RFC 4268 - Entity State MIB
- ALARM-MIB : RFC 3877 - Alarm Management Information Base (MIB)
- FC-MGMT-MIB : RFC 4044 Fibre Channel Management MIB

Outils

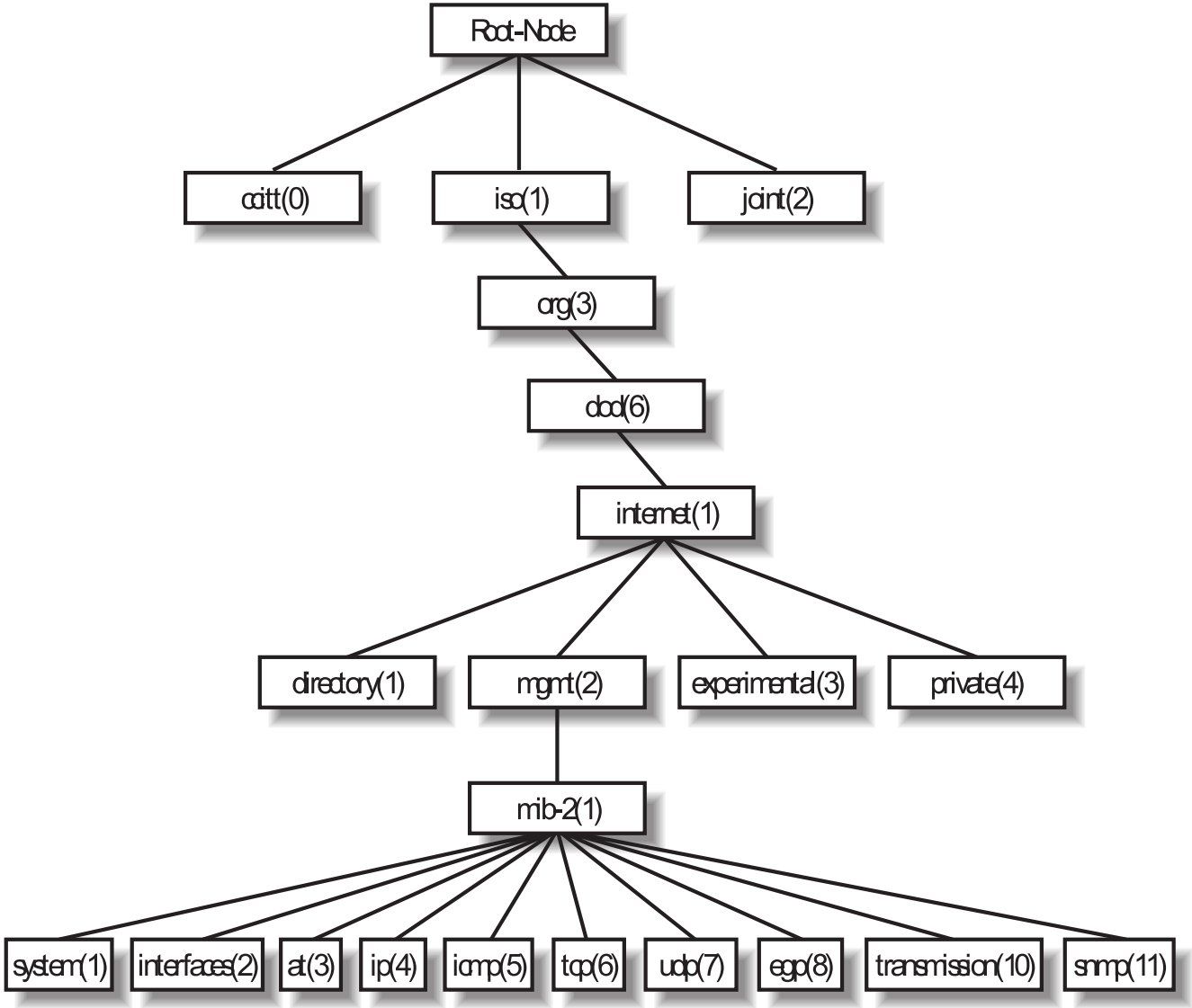
- Liens intéressant
  - OID registry : http://www.oid-info.com/
  - Liste de MIB : http://www.simpleweb.org

MIB II

- Définit les variables permettant de gérer la pile TCP/IP
  - 170 variables
  - SMIv1 (RFC 1213) puis améliorations (RFC 1156)
- Groupes

```
mib-2 (1)
+-- system(1)          : informations générales sur le système
+-- interfaces (2)     : informations sur chacune des interfaces réseaux
+-- at(3)              : table de correspondance ip <-> physique
+-- ip (4)             : informations sur l'implémentation et le fonctionnement
+-- icmp (5)           : informations sur l'implémentation et le fonctionnement
+-- tcp (6)            : informations sur l'implémentation et le fonctionnement
+-- udp (7)            : informations sur l'implémentation et le fonctionnement
+-- egp (8)            : informations sur l'implémentation et le fonctionnement
+-- transmission (10)  : informations sur les modes de transmission et les proto
+-- snmp (11)          : informations sur l'implémentation et le fonctionnement
```

MIB II


Root-Node
ccitt(0)
iso(1)
joint(2)
org(3)
dod(6)
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
system(1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
udp(7)
egp(8)
transmission(10)
snmp(11)