

# **R5B08 - Continuité de services**

## **SNMP**

Bruno BEAUFILS

2025/2026

# 1. Généralités

2. Protocole de communication : SNMP

3. Langage de définition des objets : SMI

4. Base de données des objets : MIB

# Principes 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)

# Principes 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)

# Principes 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)

# Principes 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)

# Principes 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 accès : **SMI**
  - ▶ *Structure of Management Information*
  - ▶ RFC-1155 puis RFC-2578 à RFC-2580
  - ▶ format de description les bases d'informations disponibles
    - sous ensemble de ASN.1
- 2 Lister les données disponibles sur un agent : **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 à RFC à 1452 puis RFC 3411 à 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 accès : **SMI**
  - ▶ *Structure of Management Information*
  - ▶ RFC-1155 puis **RFC-2578** à **RFC-2580**
  - ▶ format de description les bases d'informations disponibles
    - sous ensemble de ASN.1
- 2 Lister les données disponibles sur un agent : **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** à **RFC à 1452** puis **RFC 3411** à **RFC 3418**

1. Généralités

2. Protocole de communication : SNMP

3. Langage de définition des objets : SMI

4. Base de données des objets : MIB

# SNMP : 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.

# SNMP : généralités

## v1 RFC-1157

- Protocoles sur UDP
  - ▶ port 161 pour les requêtes
  - ▶ port 162 pour les notifications
  - ▶ détection de panne par interrogation (*polling*) et temporisateur (par le manager)
  - ▶ pas de stockage d'état côté agent
- type de PDU
  - ▶ get-request
  - ▶ get-next-request
  - ▶ get-response
  - ▶ set-request
  - ▶ trap

## v2 RFC-3416

- introduction de nouveaux PDU dont
  - ▶ get-bulk-request récupération d'un grand nombre de valeurs

# SNMP v2 : opérations

## Principales opérations

- `get` : récupérer une ou des variables (valeurs)
- `get-next` : récupérer la ou les variables suivantes (valeurs)
- `get-bulk` : récupérer plusieurs variables (gros volume de données)
- `set` : assigner une valeur à une ou plusieurs variables
- `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

# SNMP (v1 et v2c) : communautés

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

1. Généralités

2. Protocole de communication : SNMP

**3. Langage de définition des objets : SMI**

4. Base de données des objets : MIB

# Généralités

- Permet de définir (décrire) le contenu des *objets* gérés par les agents
  - ▶ 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

- Sous-ensemble de [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)
  - ▶ valeurs complexes (groupes, tableaux)

## **SNMP ne manipule que des scalaires**

- identification des objets (OID)
  - ▶ chaîne de nombre
  - ▶ liaison chaînes / nom
  - ▶ ordre lexicographique (cf MIB)

# Types SMIv1

- Types de base

INTEGER

OCTET STRING

OBJECT IDENTIFIER

- Types applicatifs

Gauge

Counter

TimeTicks

IpAddress

Opaque

NetworkAddress

# Types SMIv2

- Types de base

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>}
```

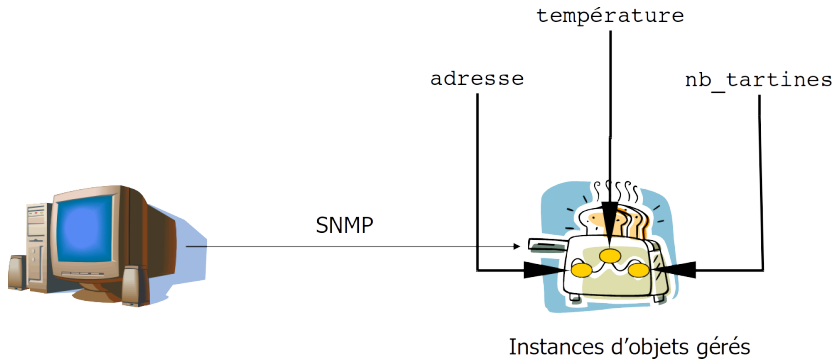
- Définition d'un objet (syntaxe SMIV2)

```
<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

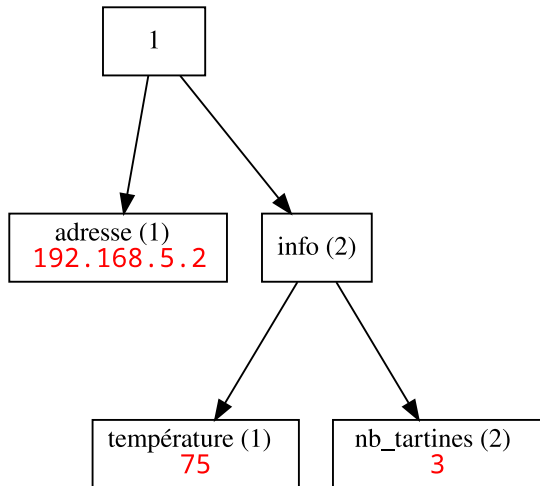
- ▶ Commentaires commencent par --
- ▶ nom commençant par des minuscules : objets

# Exemple : schéma



# Exemple : arbre des données / objets gérés

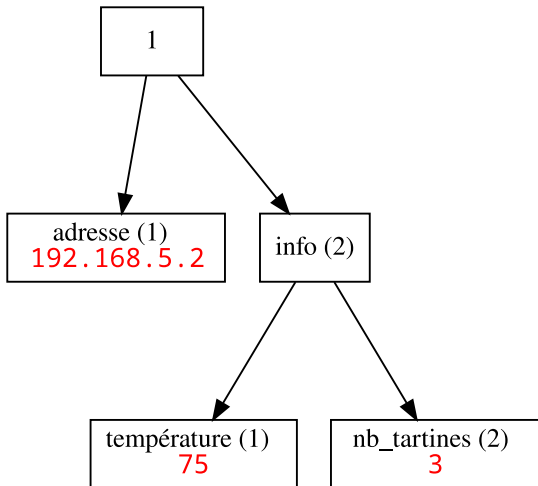
Un choix possible :



- 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 : 3

# Exemple : arbre des données / objets gérés

Un choix possible :



- 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 : 3

# Tableaux

- Un objet tableau a pour syntaxe SEQUENCE OF <TrucBidule>
  - ▶ l'accès n'est pas permis directement (not-accessible)
- <TrucBidule> définit 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 et accessible par ses **colonnes**
  - ▶ Une (ou plusieurs) de ses colonnes constitue un index (une clé)
  - ▶ La ligne est repérée par le numéro de l'instance (**la valeur des index**)

## 1. Généralités

## 2. Protocole de communication : SNMP

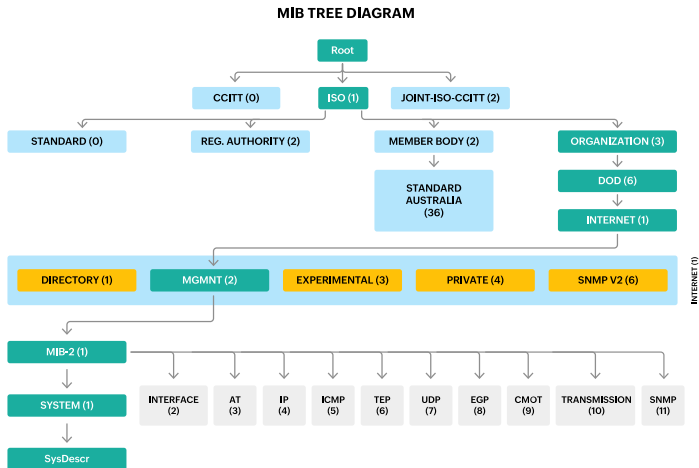
## 3. Langage de définition des objets : SMI

## 4. Base de données des objets : MIB

# 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
  - ▶ **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)



**MIB2 : 1.3.6.1.2.**

# MIB 2

- Définit les variables permettant de gérer la pile TCP/IP
  - ▶ 170 variables
- 1.3.6.1.2

| <b>nom</b>   | <b>#</b> | <b>description</b>                               |
|--------------|----------|--|
| system       | 1        | infos générales sur le système                   |
| interfaces   | 2        | infos sur chacune des interfaces réseaux         |
| at           | 3        | table de correspondance ip <-> physique          |
| ip           | 4        | infos sur IP                                     |
| icmp         | 5        | infos sur ICMP                                   |
| tcp          | 6        | infos sur TCP                                    |
| udp          | 7        | infos sur UDP                                    |
| egp          | 8        | infos sur EGP                                    |
| transmission | 10       | infos sur modes de transmission/accès interfaces |
| snmp         | 11       | infos sur SNMP                                   |

# Quelques références

- **MIB-II (RFC-1213)** - MIB of TCP/IP-based internets
  - ▶ IF-MIB (RFC-2863) - MIB for interfaces
  - ▶ IP-MIB (RFC-4293) - MIB for IP
- **Autres**
  - ▶ 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
    - FIBRE-CHANNEL-FE-MIB : RFC-2837 Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard
  - ▶ HPR-IP-MIB : RFC-2584 - Definitions of Managed Objects for APPN/HPR in IP Networks;

# Outils

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