SNMP et Java : monitoring

Soutenance intermédiaire présentée en octobre 2017 par

Benoît SCHNEIDER
Mathilde CORSIGLIA

en vue de l'obtention de la LP SIL ASR

UNIVERSITÉ DE LORRAINE | IUT Metz Informatique

Sommaire

Introduction

- « Simple Network Management Protocol »
- Créé en 1988
- Initiative de CISCO, HP et Sun Microsystems
- Décliné en **3 versions**
- Objectif : **supervision d'équipements réseau** à distance

Sommaire

Fonctionnement

- SNMP : un ensemble de requêtes, de réponses et d'alertes
- Les « **nœud manageable** »
- Les « **agents** »
- Le « **manager** »
- Le modèle client/serveur

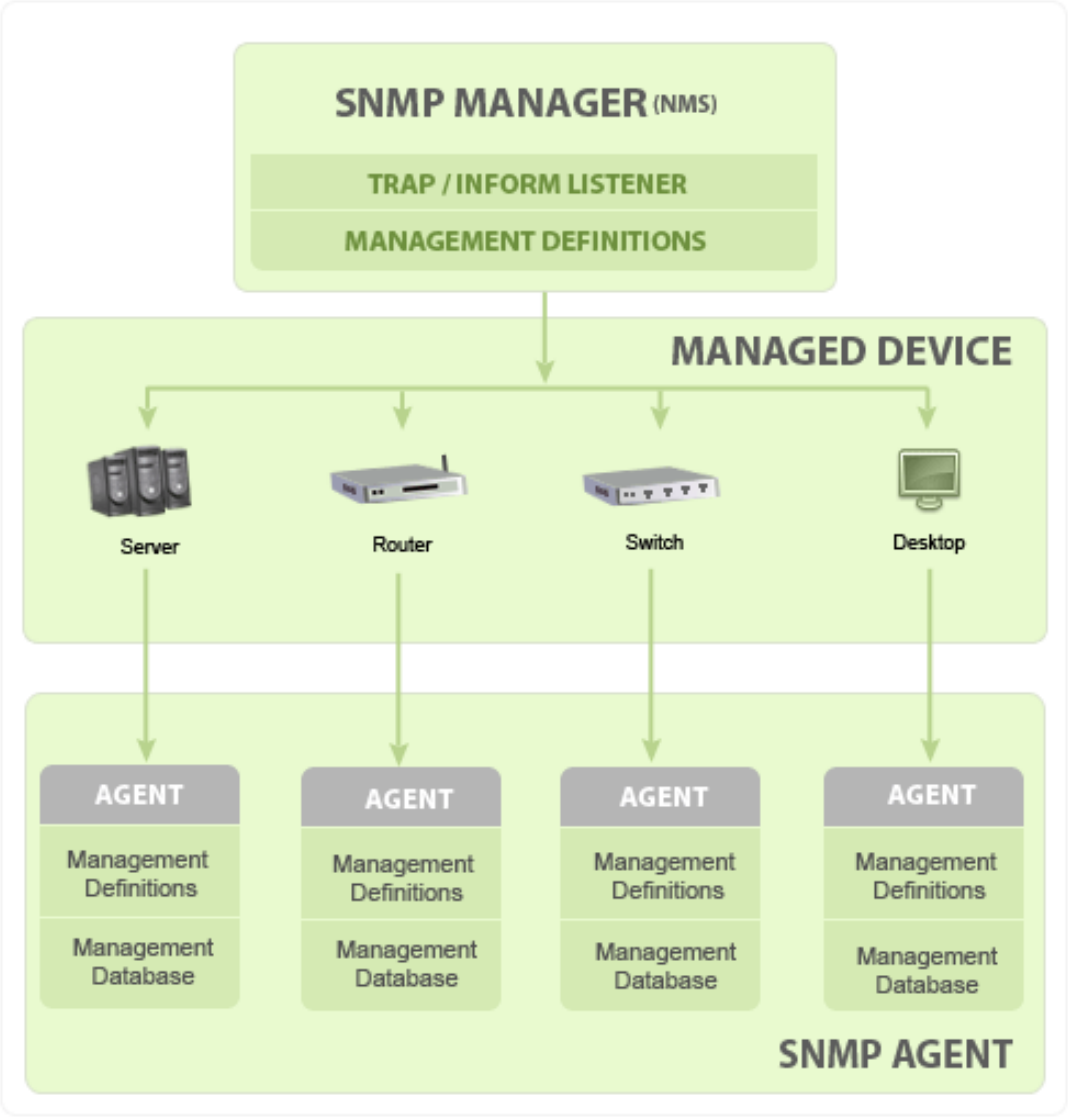


Illustration des composants du protocole SNMP

Fonctionnement

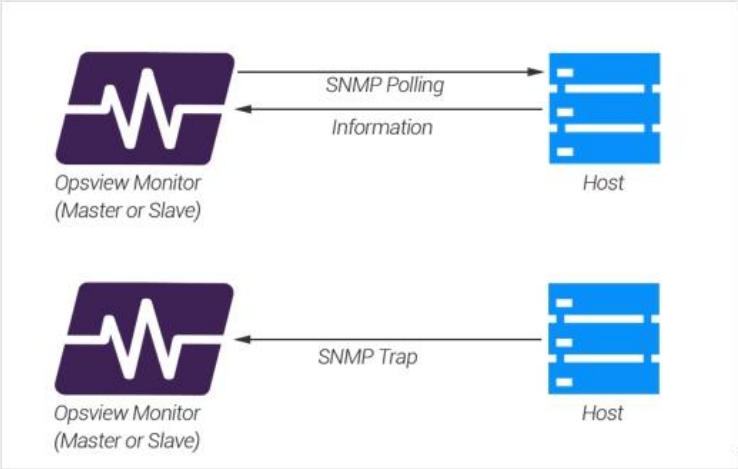
- SNMP : 7e niveau du modèle OSI

7	Application Layer	Management and Agent APIs
		SNMP
6	Presentation Layer	ASN.1 and BER
5	Session Layer	RPC and NetBIOS
4	Transport Layer	TCP and UDP
3	Network Layer	IP and IPX
2	Data Link Layer	Ethernet, Token Ring, FDDI
1	Physical Layer	

- Protocole **UDP**
  - Modèle « interrogation-réponse »
  - Aucun contrôle des données

- Ports utilisés
  - (10)**161** : requêtes et réponses
  - (10)**162** : alertes

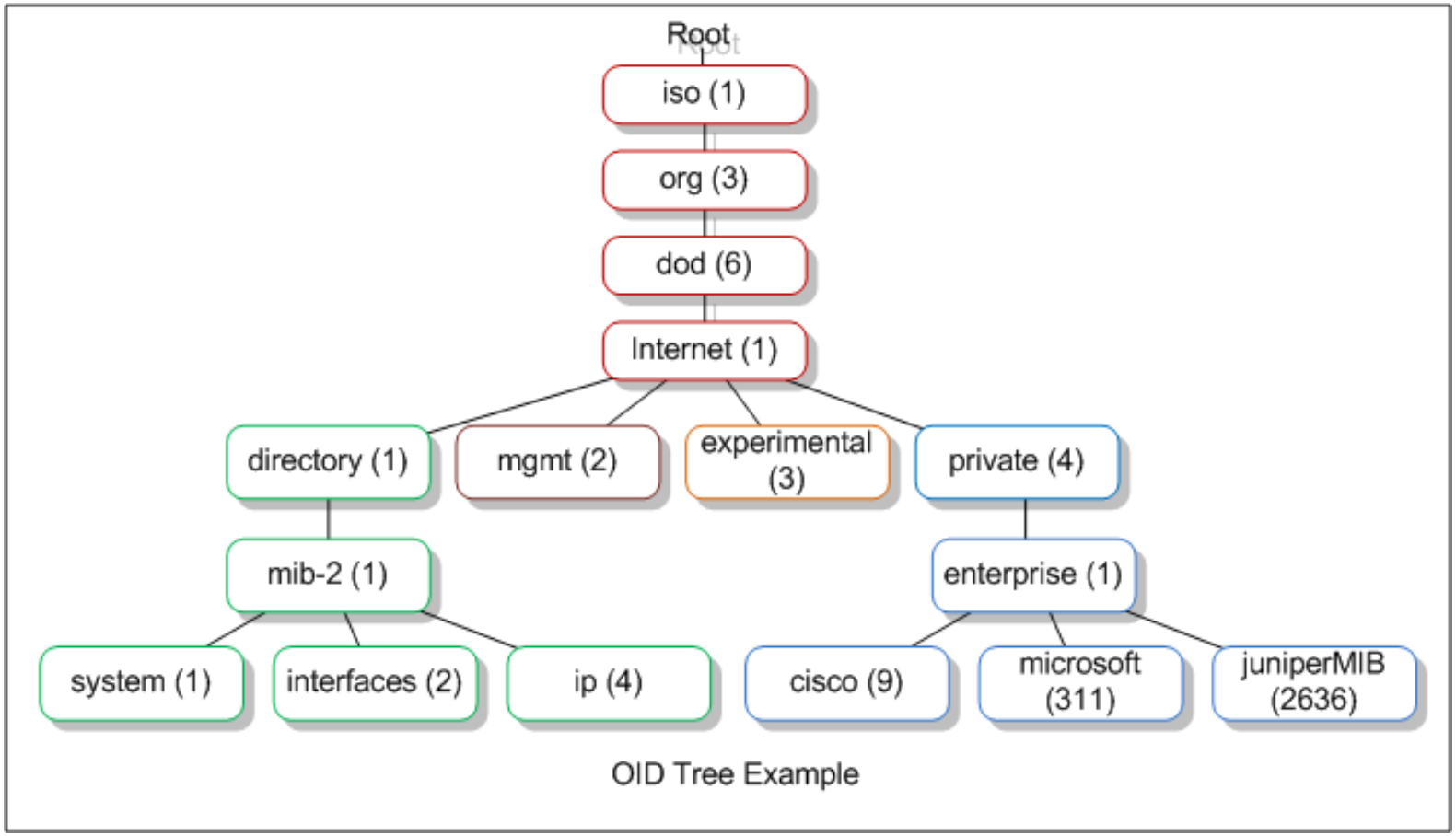
- Types de supervision
  - Active : requêtes à intervalles réguliers
  - Passive : utilisation d'alertes



Sommaire

La MIB

- « Management Information Base »
- Base de données propre à chaque agent
- Document texte (ASN.1)
- Arborescence **SMI** (« Structure of Management Information »)
- Les **OID** (« Object Identifier »)
- Structure variant d'un appareil à l'autre



Exemple d'arborescence SMI

iso.org.dod.internet.directory.mib-2.system ⇔ 1.3.6.1.1.1.1.

iso.org.dod.internet.private.entreprise.cisco ⇔ 1.3.6.1.4.1.9.

Sommaire

Versions 1 et 2

Les requêtes (manager)	GetRequest	Cherche la valeur d'une variable sur un agent
	GetNextRequest	Permet de lire la valeur d'une variable suivante
	SetRequest	Modifie la valeur d'une variable sur un agent
Les réponses (agents)	GetResponse	Permet de renvoyer une réponse à une requête
	NoSuchObject	Envoyée dans le cas où la variable est indisponible
Les alertes (agents)	Trap	Déclenchée un évènement inattendu (ColdStart, WarmStart, Linkdown, LinkUp, Authentification failure)

Tableau récapitulatif des instructions existantes sous SNMPv1

Versions 1 et 2

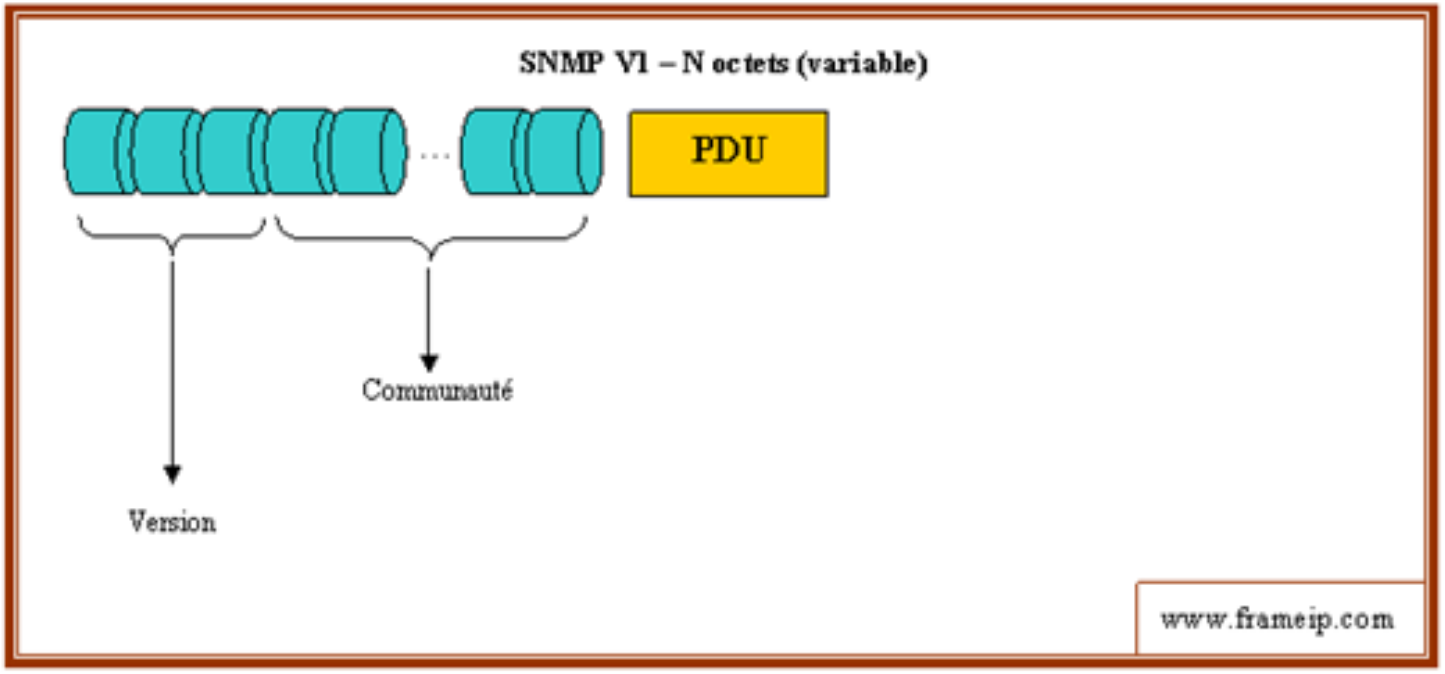


Schéma de l'entête d'une trame SNMPv1 (UDP)

Versions 1 et 2

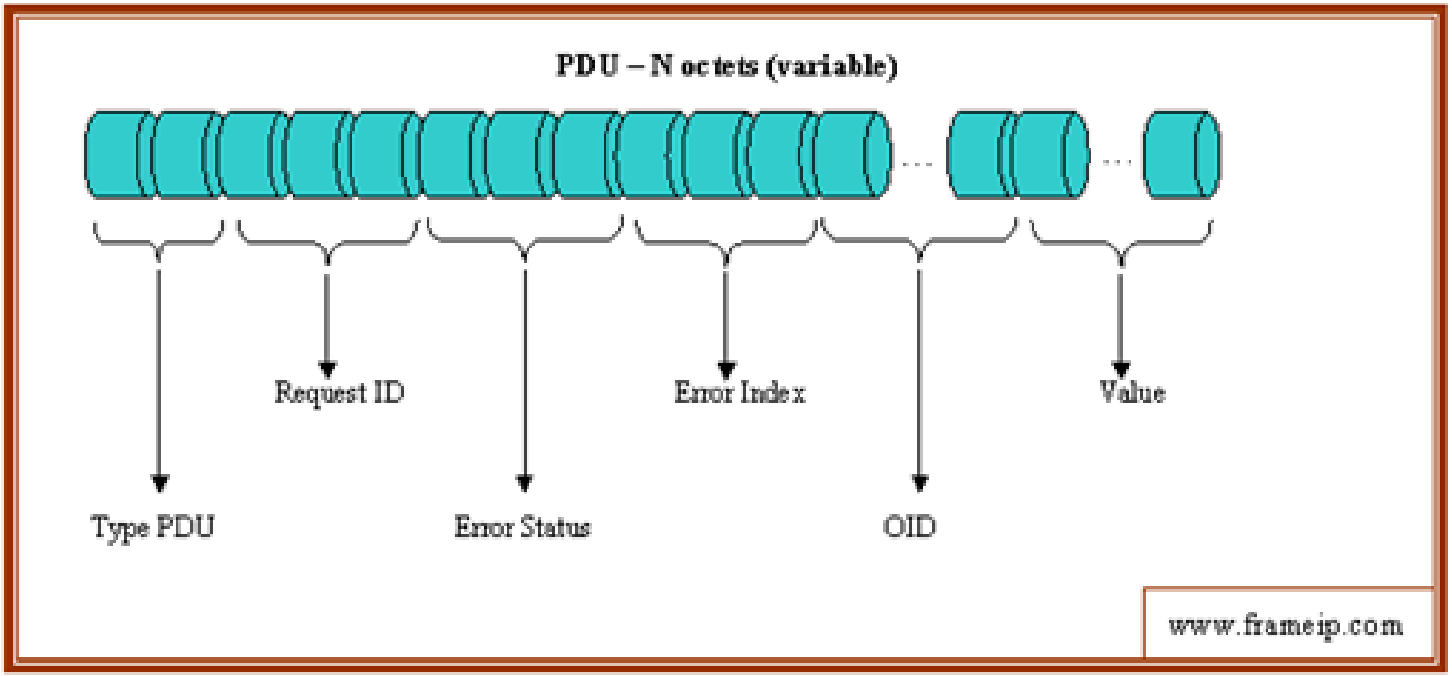


Schéma du contenu d'une trame SNMPv1 (UDP)

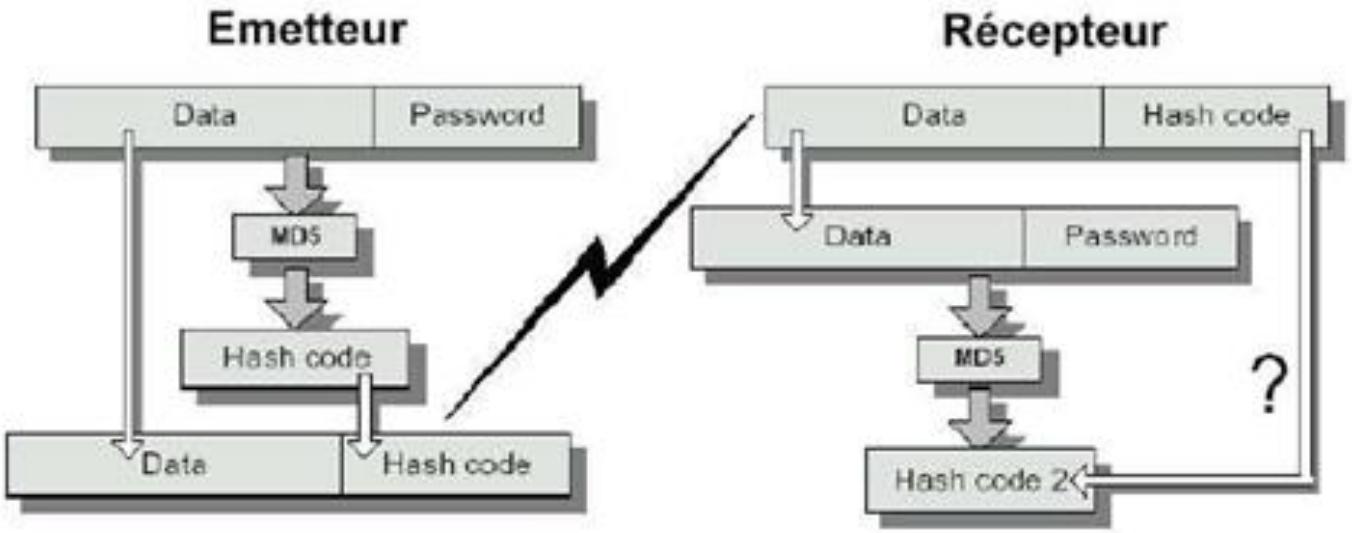
Versions 1 et 2

- Données et mot de passe non chiffrés
- GetNextRequest
- « SHOW AND TELNET »
- GetBulk
- Inform
- Messages cryptés (**DES**) , Hachage (**MD5**)

Sommaire

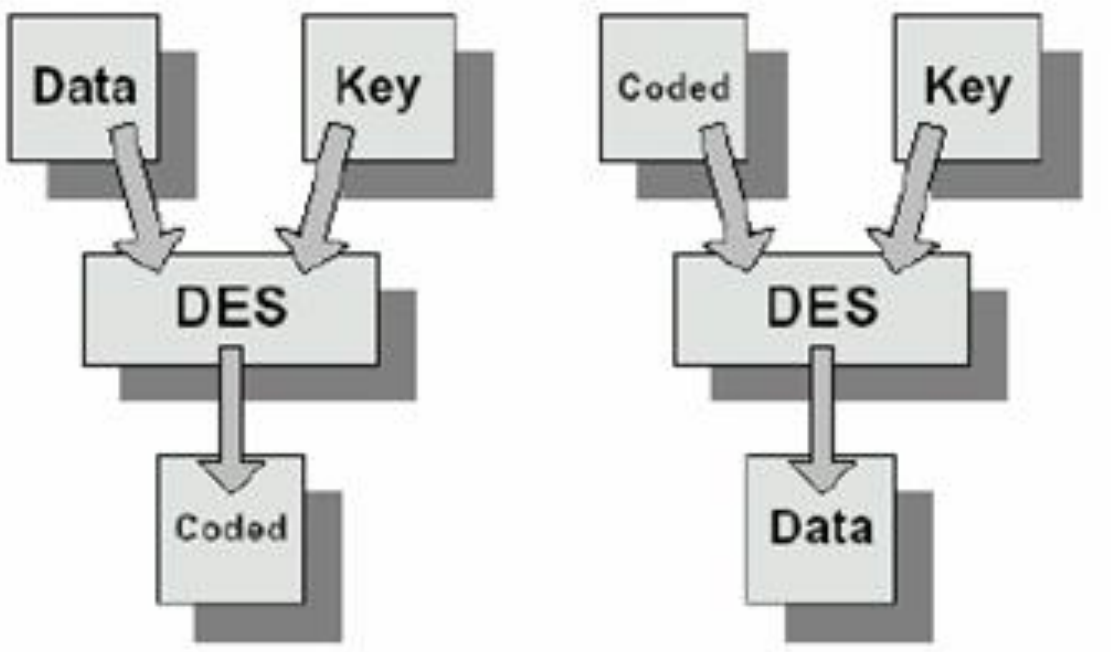
Version 3

- USM (« User-based-Security-Model »)
- L'authentification en une image :



Version 3

- Chiffrement : clé de 64 bit et le chiffrement **DES**



Version 3

- L’estampillage du temps
- Time
- Boots

- VACM (« View Assec Control Model »)

Sommaire

Conclusion

- Un outil incontournable pour les administrateurs réseau
  - Gestion des équipements réseau
  - Diagnostiquer pannes et anomalies
  - Contrôle des accès/performances
- 3 versions à ce jour
  - SNMPv1 est la version la plus courante…
  - … malgré ses lacunes
  - SNMPv2 est resté expérimental
  - SNMPv3 est considéré comme standard depuis 2002

Merci de votre attention

Des questions ?