INTRODUCTION
A
SNMP

Simple Network Management Protocol

INTRODUCTION

- Gestion d'un réseau
  - Gestion de la configuration des équipements
  - Gestion des problèmes du réseau
    - Pannes physiques, coupure, …
  - Gestion des performances, …

  - Les moyens utilisés :
    - Extraction des informations des éléments du réseau

    - Stockage de ces informations

      (avant ou après filtrage)

      -> de grandes quantités de données peuvent être présentes

    - Traitement et visualisation de ces données

PROTOCOLE SNMP (1)

- Protocole de gestion de réseau proposé par l'IETF
  - SNMPv1 : première version, 1989 -> RFC 1065
  - SNMPv2 est divisé en :
    - Snmpv2c : amélioration de la version 1 sur le protocole
    - Snmpv2u : amélioration de la version 1 sur la sécurité
    - Snmpv2 : un mixe des deux versions
  - SNMPv3 : orienté vers la sécurité
  - Actuellement SNMPv1 est encore très utilisé…

PROTOCOLE SNMP (2)

- SNMP est un protocole qui permet la gestion locale et à distante d'équipements tels que les routeurs, les switches, les serveurs,…

- Il permet :
  - De disposer d'une cartographie du réseau
  - De fournir un inventaire précis de chaque machine
  - De signaler les dysfonctionnements

FONCTIONNEMENT

- 3 éléments principaux :
  - **Agents :** chargés de superviser un équipement (agent SNMP)
  - **Stations de gestion** : capable de communiquer avec les agents et d'interpréter les données reçues (Manager)
  - **MIB :** Management Information Base

SNMP ET LE MODELE OSI

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

SNMP est fait pour le protocole TCP/IP et fonctionne au-dessus d'**UDP** sur le **port 161** (SNMP message) et **162** (SNMP trap message)

SNMP

- SNMP peut se décomposer en 3 parties:
  - **Protocole SNMP**
    - Définit le format des messages entre les agents et les managers (primitives get, getnext, trap,…)
  - **Structure of Management Information (SMI)**
    - Règles spécifiant le format des données que peut récupérer SNMP (RFC 1155)
  - **MIB :**
    - Base de données qui contient les informations du système, codées en respectant le SMI

LES OPERATIONS

- *GetRequest* : recherche d'une variable de la MIB sur un agent
- *GetNextrequest* : recherche de la variable suivante
- *GetBulkRequest* : recherche d'un groupe de variables

- *SetRequest* : permet de changer la valeur d'une variable d'un agent

- *Trap* : détection d'un accident

- Une seule réponse : *GetResponse*, soit avec la valeur, soit avec *NoSuchObject*

LA MIB

- Codé en respectant le SMI
  - Utilisation de ASN.1 pour définir les objets
  - Utilisation de BER pour encoder les messages

```
sysContact OBJECT-TYPE          -- OBJECT-TYPE décrit l'OID
    SYNTAX      DisplayString (SIZE (0..255))   -- champ qui décrit les infos
    ACCESS      read-write      -- ou read-write, write-only, not-accessible
    STATUS      mandatory       -- ou optional, deprecated, obsolete
    DESCRIPTION
            "Champ permettant de
             mettre l'information"
    ::= { system 4 }
```

OID (OBJECT IDENTIFIER)

SNMP Name Structure

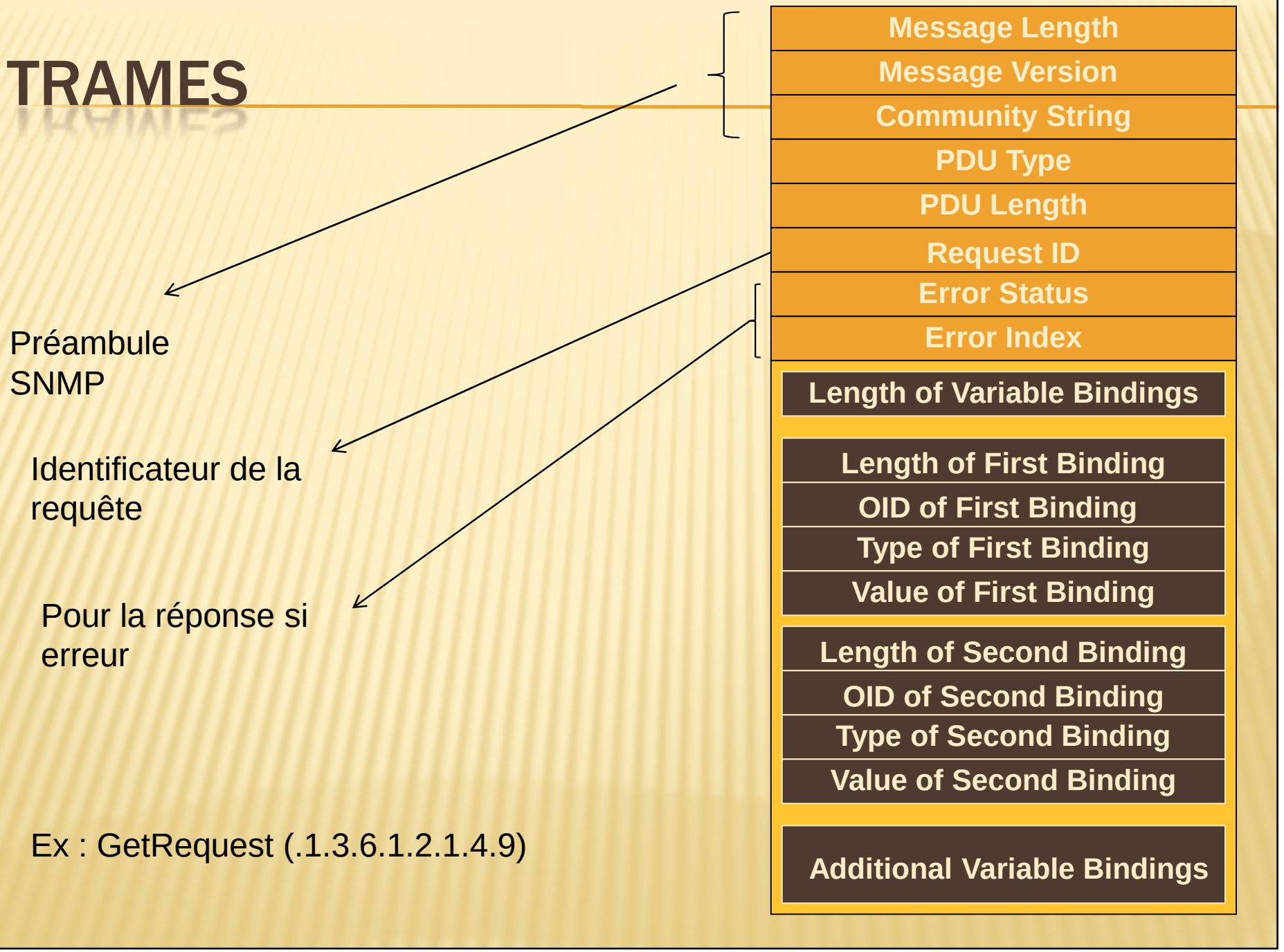
Oid : .1.3.6.1.2.1.2.1.1.2

Chaque entreprise va avoir sa MIB…

RÉCUPÉRATION D'INFORMATION

- Remontée d'information
  - Soit en utilisant le polling
  - Soit par émission de Trap
- Notion de communauté
  - Un agent n'envoie que vers sa communauté
    - Permet de mettre un peu de sécurité
    - Permet de distinguer les flux d'informations

TRAMES


Message Length
Message Version
Community String
PDU Type
PDU Length
Request ID
Error Status
Error Index
Length of Variable Bindings
Length of First Binding
OID of First Binding
Type of First Binding
Value of First Binding
Length of Second Binding
OID of Second Binding
Type of Second Binding
Value of Second Binding
Additional Variable Bindings
Préambule SNMP
Identificateur de la requête
Pour la réponse si erreur
Ex : GetRequest (.1.3.6.1.2.1.4.9)

LOGICIELS

- De nombreux logiciels utilisent SNMP
  - HP OpenView
  - CiscoWorks
  - Nagios
  - Cacti,
  - …