



Administration Des Réseaux Informatiques

Cours 3 :

Le Protocole SNMP

Simple Network Management Protocol



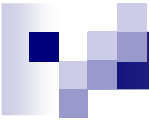
Plan

- ❑ Généralités sur l'administration
- ❑ Organisation de l'administration
- ❑ Les standards d'administration
- ❑ Le protocole SNMP
- ❑ Base de donnée d'informations de gestion (MIB)
- ❑ Les logiciels de supervision (monitoring)



Généralités sur l'administration

- ❑ Qu'est-ce que l'administration réseau ?
 - Les moyens de connaître l'état physique et logique du réseau
- ❑ Pourquoi ?
 - Permet une meilleure détection des problèmes utilisateurs
- ❑ Comment ?
 - Par l'intermédiaire d'outils déterminant l'accessibilité au réseau et ceux exécutant des statistiques



OUTILS système et réseau "natifs"

- ❑ Ifconfig / ping / fping
- ❑ Route
- ❑ Netstat
- ❑ telnet / SSH
- ❑ Interface Web



Type de fonctions d'administration

- ❑ Gestion du réseau réel
- ❑ Gestion du réseau logique (gestion des configurations,..)
- ❑ Gestion des performances et de la sécurité
- ❑ Gestion de la planification (gestion des informations comptables)



Exemple de Fonctions de Gestion

- ❑ Gestion **des erreurs**
 - Détecter, isoler, corriger les erreurs du réseau
- ❑ Gestion de **la configuration**
 - Configuration distante d'éléments du réseau
- ❑ Gestion **des performances**
 - Evaluation des performances
- ❑ Gestion **de comptes utilisateurs**
 - Faire payer l'utilisation du réseau en fonction de son utilisation
 - Limiter l'utilisation des ressources
- ❑ Gestion **de la sécurité**
 - Contrôle d'accès
 - Authentification
 - Cryptage



Stratégie d'administration

- ❑ « Plug and Play/Pray »
 - ❑ on branche et ça marche
 - ❑ aucun paramètre à définir
- ❑ Configuration « à la main »
 - ❑ ex : à chaque ajout de terminal, lui affecter statiquement des paramètres, définir les pilotes, ...
- ❑ But de l'administrateur :
 - Tirer le meilleur profit du matériel présent
 - Nécessité de trouver un compromis entre les deux approches précédentes
 - Une stratégie est propre à chaque entité gérante (entreprise, laboratoire, etc.)



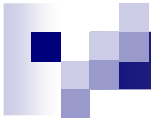
Les standards d'administration

- **Issus du modèle OSI**

- **Common Management Information Service (CMIS)**
 - *Définition de services pour l'administration*
- **Common Management Information Protocol (CMIP)**
 - *Définition de procédures et syntaxes pour l'administration*

- **Issus du modèle TCP/IP**

- **CMip Over TCP/IP (CMOT)**
 - *Dans une phase transitoire, version de CMIP adaptée à TCP/IP*
- **Simple Network Management Protocol (SNMP)**
 - *Au départ (1988) : une solution à court terme*
 - *A ce jour : le standard de fait adapté par tous les constructeurs*



Le protocole SNMP

- Composants SNMP
- Type des messages SNMP
- Management Information Base (MIB)
- Le format des messages SNMP

Qu'est ce que le protocole SNMP ?

- SNMP est un protocole de gestion réseaux proposé par l'IETF (Internet Engineering Task Force)
- Il s'appuie sur 3 composantes principales :
 - ✓ **Nœuds administrés**
 - ✓ **Stations d'administration**
 - ✓ **Information d'administration**

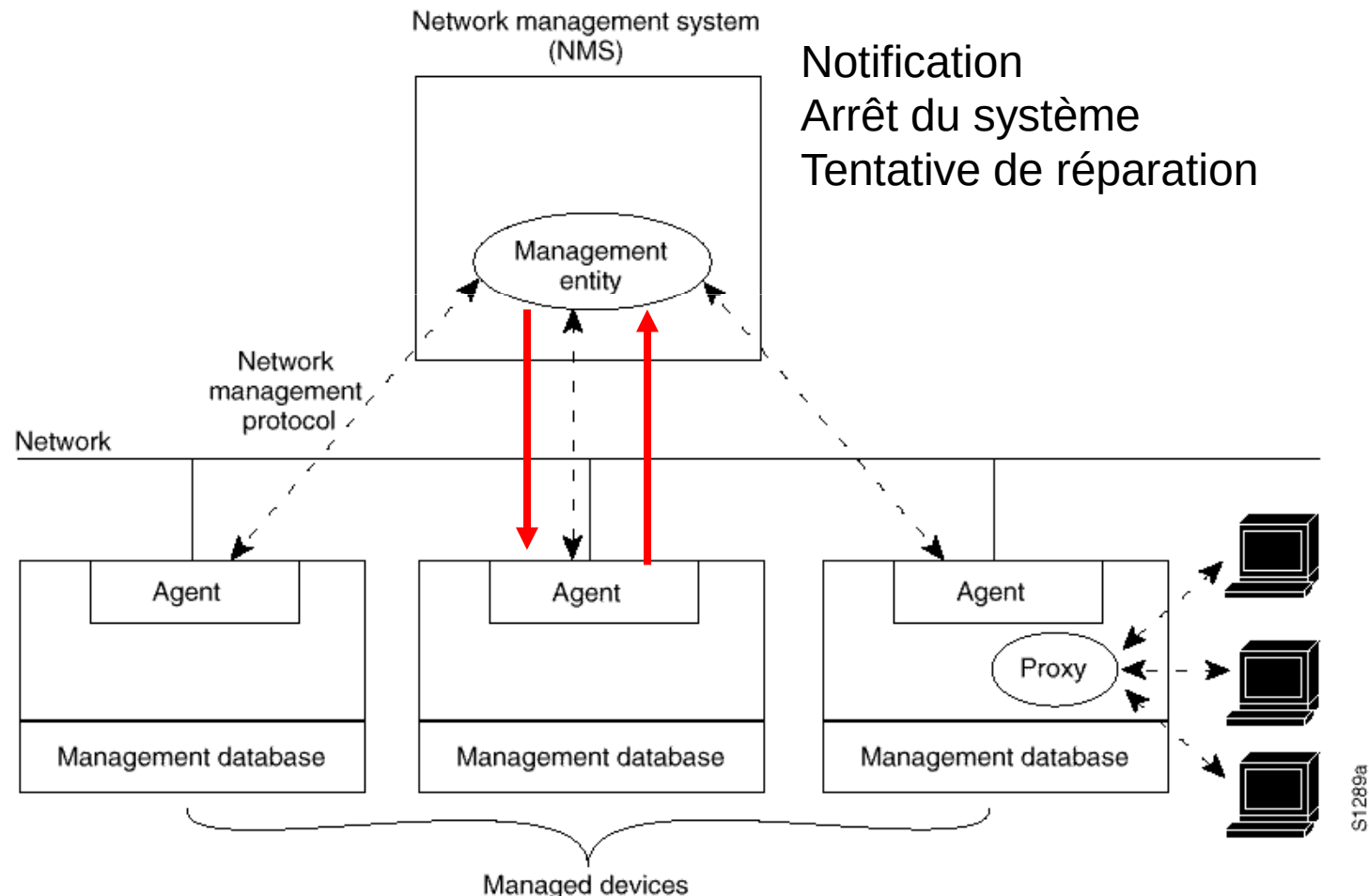
	Modèle OSI	Modèle TCP/IP (protocole)
7	Application	SNMP
6	Présentation	
5	Session	
4	Transport	<i>UDP</i>
3	Réseau	<i>IP</i>
2	Liaison	Interface réseau
1	Physique	

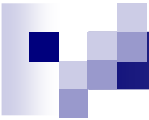


SNMP : Composants d'un réseau

- ❑ **Nœuds administrés** : Entité capable de communiquer des informations d'état
 - Hôtes, routeurs, ponts, imprimantes...
 - Exécute un agent SNMP qui gère une base de données locale de variables donnant l'état et l'historique
- ❑ **Stations d'administration** : Ordinateur exécutant un logiciel particulier
 - Communique avec les agents
 - Envoi de commandes/réception de réponses
- ❑ **Information d'administration** :
 - Chaque entité gère des variables décrivant son état,
 - Une variable est appelée objet.
 - L'ensemble des objets d'un réseau se trouve dans une base de donnée : la MIB (Management Information Base)

Architecture classique d'administration SNMP





Les différentes versions de SNMP

- **SNMPv1** (ancien standard) : Première version apparue en 1989.
- **SNMPsec** (historique): Ajout de sécurité par rapport à la version 1
- **SNMPv2p** (historique) : Ajout de nouveau type de données.
- **SNMPv2c** (expérimental) : Amélioration des opérations du protocole
- **SNMPv3** (nouveau standard) : La sécurité avant tout.

Messages SNMP

➤ Recherche d'informations :

- ✓ **GetRequest** : recherche d'une variable sur un agent.
- ✓ **GetNextRequest** : recherche de la variable suivante.
- ✓ **GetBulkRequest** : recherche d'un groupe de variables

➤ Modification de valeurs :

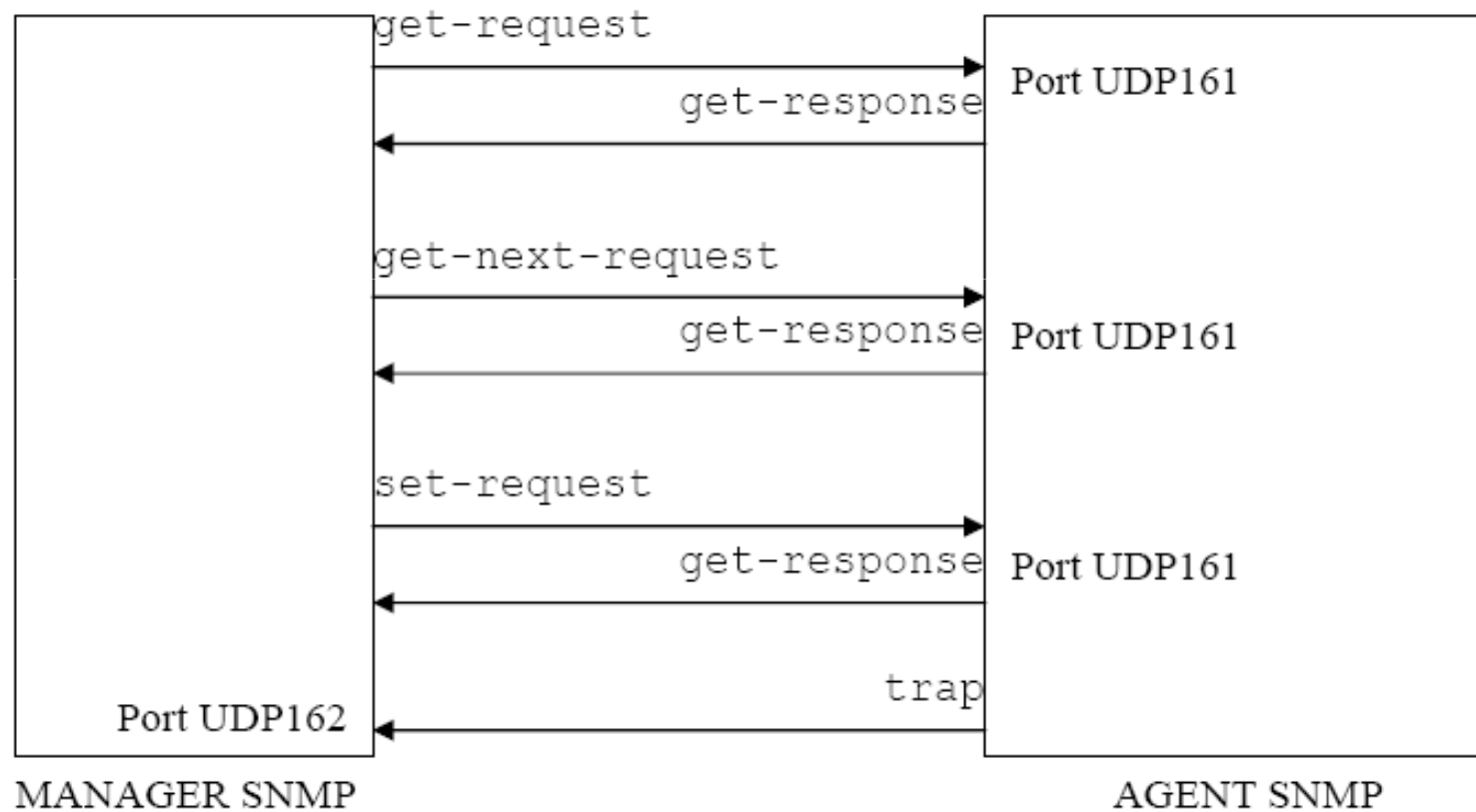
- ✓ **SetRequest** : permet de changer la valeur d'une variable d'un agent.

➤ Envoie d'informations

- ✓ **Trap** : détection d'un incident

Message	Signification
Get	Demande de la valeur d'une variable
Get-next	Demande de la variable suivante
Get-bulk	Chargement d'une grande table (SNMPv2)
Set	Mise à jour d'une ou plusieurs variables
Inform	Message de description d'une MIB locale (SNMPv2)
Trap	Indication de déroutement provenant d'un agent
Response	Réponse

Echanges des messages SNMP





Base de donnée d'informations de gestion

- ❑ **Management Information Base (MIB)** : Ensemble des informations nécessaires à l'administration.

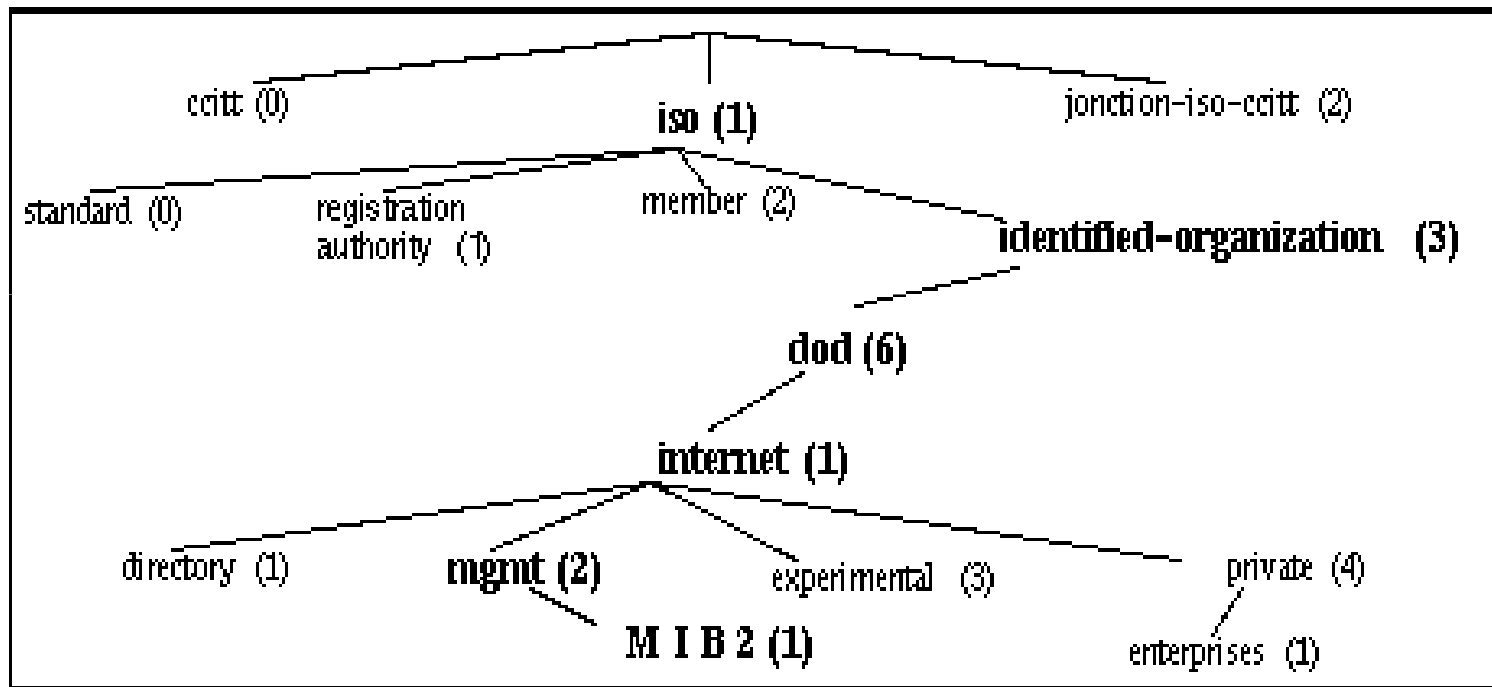
Exemples d'objets :

table de routage, nombre de collisions, taille des files d'attentes
beaucoup de compteurs : charge du CPU, paquets reçus ...

- ❑ La **MIB** est la base de données des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.
- ❑ Un fichier **MIB** est un document texte écrit en langage ASN.1 qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB.
- ❑ SNMP procède de deux façon pour nommer les objets d'une **MIB** :
 - la première est un nom unique par objet (ex:sysUpTime),
 - la seconde utilise les notations d'ASN.1

MIB

- ❑ La classification des objets est arborescente. L'identificateur d'un objet est défini, en ASN.1 par le chemin qui conduit à l'objet.



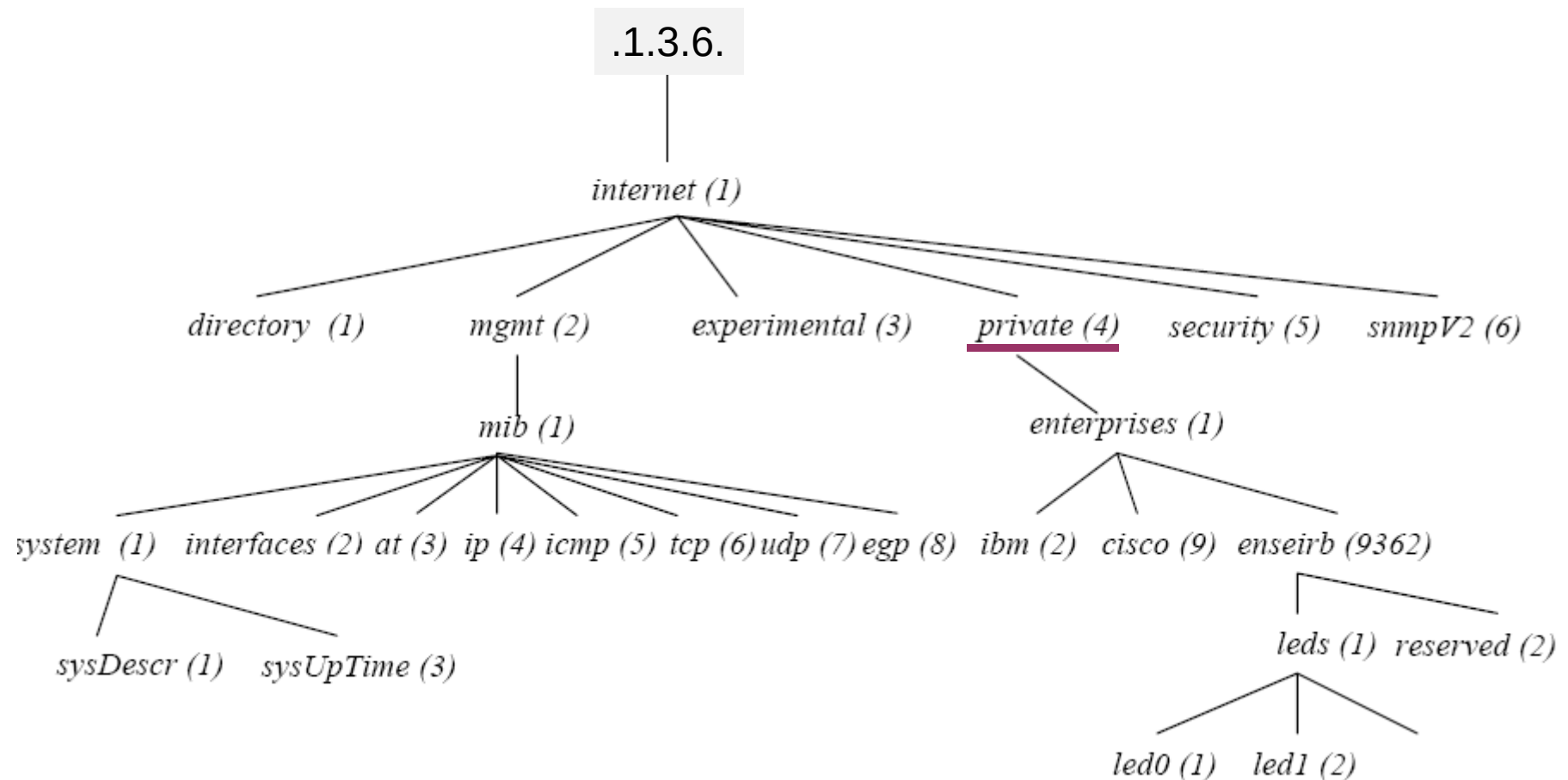
- ❑ Par exemple, pour accéder à un objet d'administration, son identificateur Autrement appelé OID commencera par **1.3.6.1.2** (**iso.org.dod.internet.mgmt**).



MIB

- ❑ Pour qu'un client accède à ces objets, il faut qu'il soit au courant de leur existence. Une MIB contient un certain nombre d'informations standards : c'est la **MIB standard**.
- ❑ Or pour la plupart des éléments réseau, on rajoute un certain nombre d'objets propre à un agent pour en exploiter les possibilités : c'est la **MIB privée**.
 - ❖ Lorsqu'une entreprise veut définir son propre ensemble de variables de gestion, elle va enregistrer son numéro d'objet sous le noeud :
iso.org.dod.internet.private.entreprise.
 - ❖ Ces MIB seront dites privées. Elles correspondent à la racine 1.3.6.1.4.1.

MIB : Zoom de la branche internet





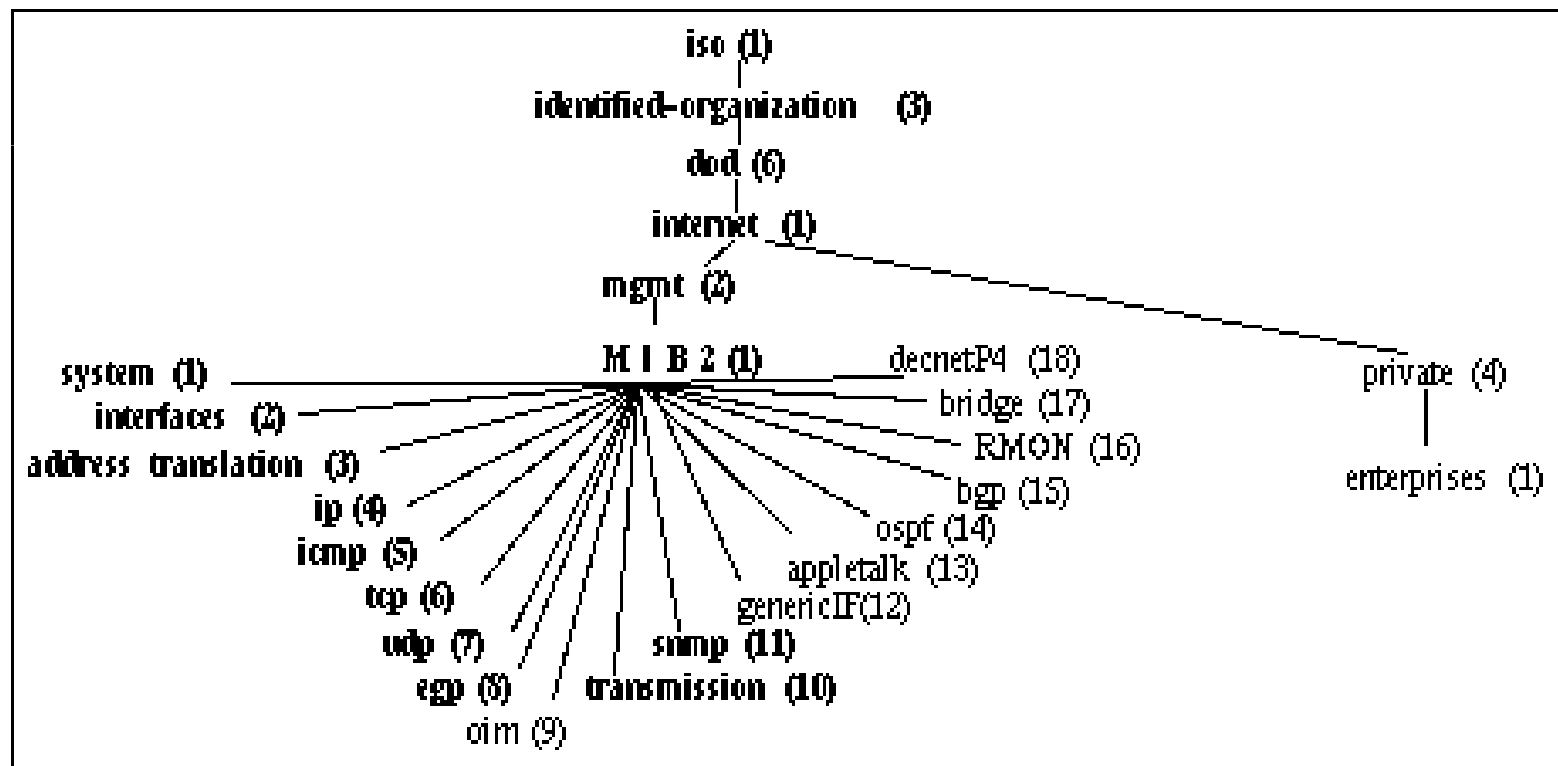
MIB-I

- ❑ On peut donc dire que la MIB standard désigne le plus petit dénominateur commun entre tous les types de matériel que l'on peut rencontrer sur un réseau.
- ❑ Le premier standard utilisé pour la définition des objets d'administration de la MIB standard fut la MIB-I.
- ❑ Son OID est : 1.3.6.1.2.1 et sa définition est la suivante:

Numéro	Objet	Nombre de sous-objets
1	system	3
2	interfaces	23
3	at	3
4	ip	33
5	icmp	26
6	tcp	17
7	udp	4
8	egp	6

MIB II

- Un second standard fut défini pour rajouter des objets dans quelques unes des catégories de la MIB standard. Ce standard est appelé MIB-II et, fort de ses 172 éléments, a remplacé actuellement la MIB I. Son OID est aussi : 1.3.6.1.2.1



La définition de MIB II

Numéro	Objet	Nombre de sous-objets	Description
1	System	<u>7</u> (3)	Information générales concernant l'agent à travers le système
2	Interfaces	23	Informations concernant chaque interface IP de l'agent
3	Address Translation	3	La table de translation d'adresses qui réalise la correspondance entre l'adresse MAC et l'adresse IP
4	IP	<u>38</u> (33)	Compteurs IP
5	ICMP	26	Compteurs ICMP
6	TCP	<u>19</u> (17)	Compteurs TCP
7	UDP	<u>7</u> (4)	Compteurs UDP
8	EGP	<u>18</u> (6)	Compteurs EGP
9	CMOT	0	Compteurs pour CMOT (protocole OSI équivalent à SNMP)
10	Transmission	0	modes de transmission et protocoles d'accès de chaque interface. Remplacera <i>at</i>
11	SNMP	30	Statistiques du trafic SNMP

Dans le groupe Interfaces, vous pourrez trouver les variables suivantes :

ifIndex numéro de l'interface

ifDescr description de l'interface

ifType type de l'interface

ifInOctets / ifOutOctets nombre total d'octets reçus / emis par l'interface



Les objets du groupe « system » de MIB II

Identifiant de l'objet	Nom	Type	Description
1.3.6.1.2.1.1.1	sysDescr	OCTET STRING	description du type de matériel, du SE, et des logiciel réseau
1.3.6.1.2.1.1.2	sysObjectID	OBJECT IDENTIFIER	Identifiant de l'objet attribué par le fabricant
1.3.6.1.2.1.1.3	sysUpTime	TimeTicks	Temps depuis l'activation de l'administration systeme
1.3.6.1.2.1.1.4	sysContact	OCTET STRING	Personne travaillant sur le nœud administré
1.3.6.1.2.1.1.5	sysName	OCTET STRING	Nom du nœud administré
1.3.6.1.2.1.1.6	sysLocation	OCTET STRING	Emplacement géographique du noeud
1.3.6.1.2.1.1.7	sysServices	Integer32	Le type de service administré



MIB : Exemple

- ❖ 1.3.6.1.2.1.1.3.0 : " l'uptime " de la machine locale (le temps depuis lequel le système est en service)

```
[root@gw mibs]# snmpget -v 1 -c public localhost .1.3.6.1.2.1.1.3.0
```

```
system.sysUpTime.0 = Timeticks: (23599841) 2 days, 17:33:18.41
```

- ❖ si nous nous étions trompés dans le chemin, nous aurions obtenu :

```
[root@gw mibs]# snmpget -v 1 -c public localhost .1.3.6.1.2.1.1.3.1
```

```
Error in packet Reason: (noSuchName) There is no such variable name  
in this MIB. Failed object: system.sysUpTime.1
```


Les objets du groupe « Protocole IP » de MIB II

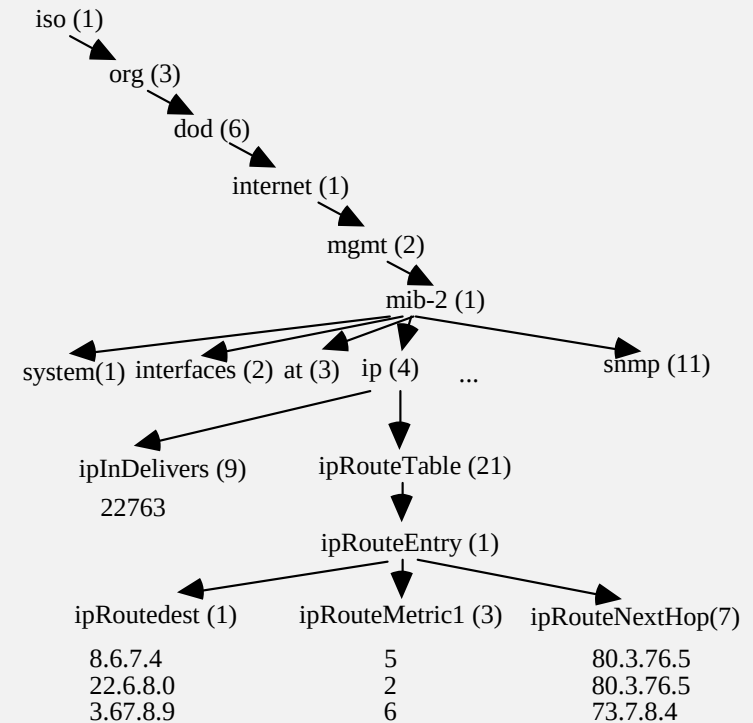
Le schéma suivant représente la branche associée à l'Internet et on s'intéresse au protocole IP.

✓ **ipInDelivers** : donne le nombre de paquets correctement délivrés (22763 paquets).

❑ L'OID de l'objet ipInDelivers est : **1.3.6.1.2.1.4.9.**

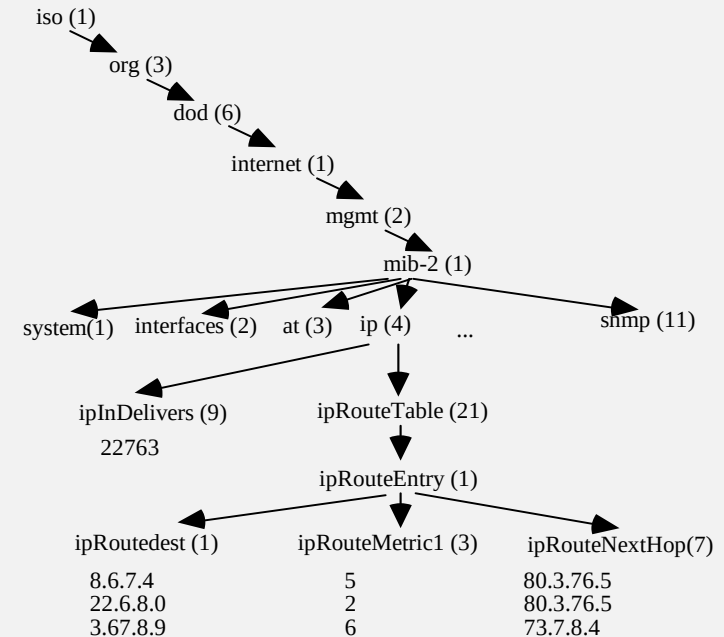
➤ GetRequest (1.3.6.1.2.1.4.9) produit la réponse :

GetResponse (*ipInDelivers = 22763*)



Les objets du groupe « Protocole IP » de MIB II

- ✓ **ipRouteTable**: la table de routage
- ✓ **ipRoutedest**: le destinataire à atteindre
- ✓ **ipRouteMetric1** : Le coût du chemin pour atteindre le destinataire (un entier).
- ✓ **ipRouteNextHop** : L'adresse du prochain routeur pour rejoindre le destinataire .



❖ On souhaite maintenant consulter la table de routage par la commande Get Request et GetNextRequest .

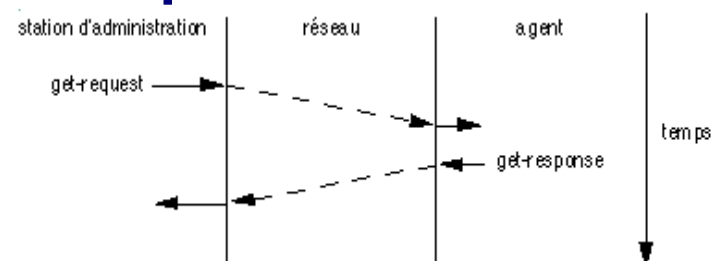
➤ GetRequest (ipRoutedest, ipRouteMetric1, ipRouteNextHop) produit la réponse :

GetResponse ((*ipRoutedest.8.6.7.4="8.6.7.4 "*), (*ipRouteMetric8.6.7.4="5"*), (*ipRouteNextHop 8.6.7.4="80.3.76.5"*))

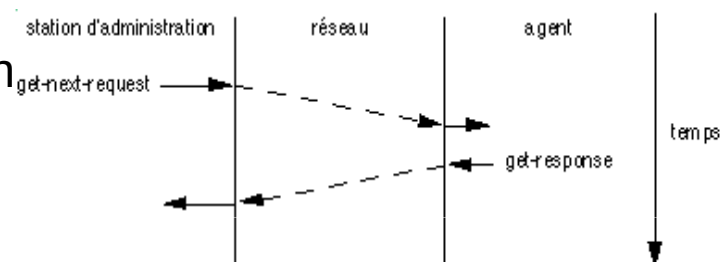
On continue la consultation de la table par GetNextRequest

SNMP: Récapitulatif des opérations

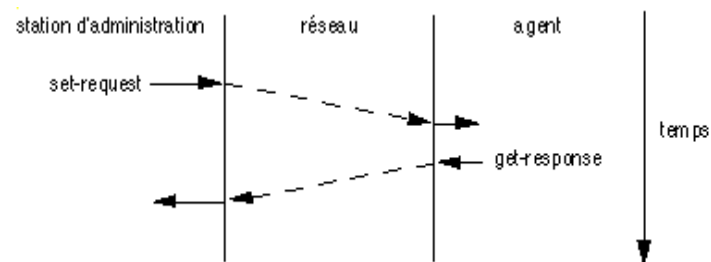
- ❑ get-request/get-response: la station d'administration interroge l'agent



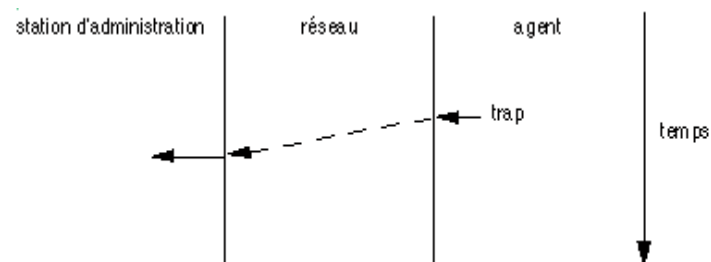
- ❑ get-next-request/get-response: la station d'administration interroge une table de l'agent



- ❑ set-request/get-response: la station d'administration enregistre des données au niveau d'un agent

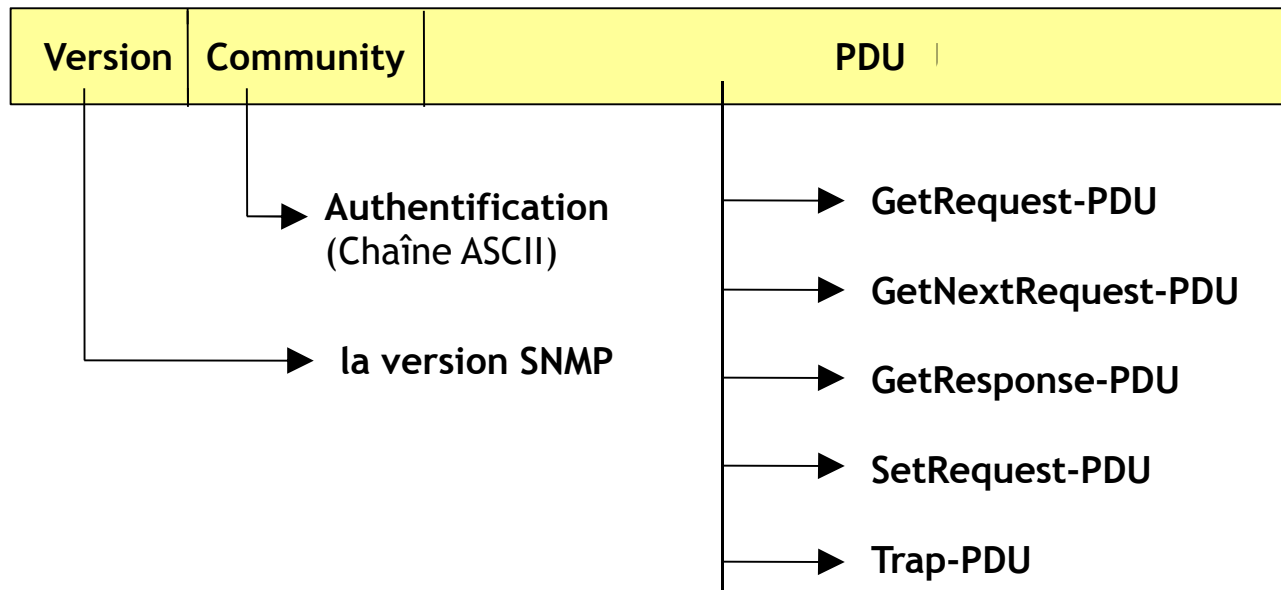


- ❑ trap: l'agent envoie un événement "extraordinaire" vers la station d'administration



Format des messages SNMP

- Format des messages SNMP :



<i>Version</i>	SNMP v1	SNMP v2c	SNMP v3
<i>Valeur du champ</i>	0	1	3

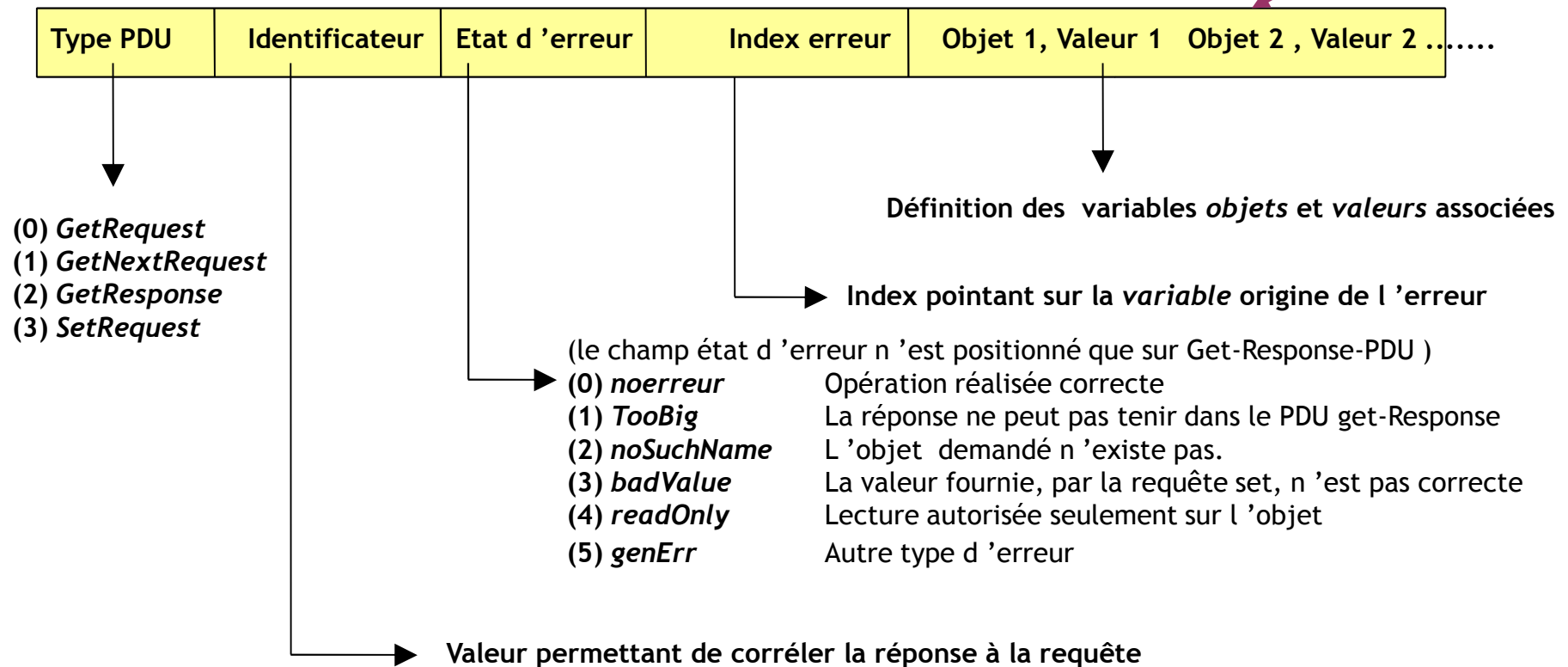


Format du message SNMP

- ❑ Le champ version permet de s'assurer que l'administrateur et l'agent utilisent la même version du SNMP
- ❑ La communauté est une authentification triviale utilisée par SNMPv1, La plupart des équipements permettent de configurer des noms de communauté différents en lecture et en écriture
 - Le nom de communauté de "lecture" est souvent "public", par défaut
 - Envoyé sous forme de chaîne de texte ASCII dans les PDU
 - Quiconque possédant un analyseur de protocole peut le capturer
- ❑ La section "données" contient une des cinq PDU SNMP
 - On définit seulement deux formats de PDU
 - **GetRequest**, **GetNextRequest**, **GetResponse**, **SetRequest** utilisent le même format de PDU
 - Le **Trap** de SNMP utilise un format de PDU différent

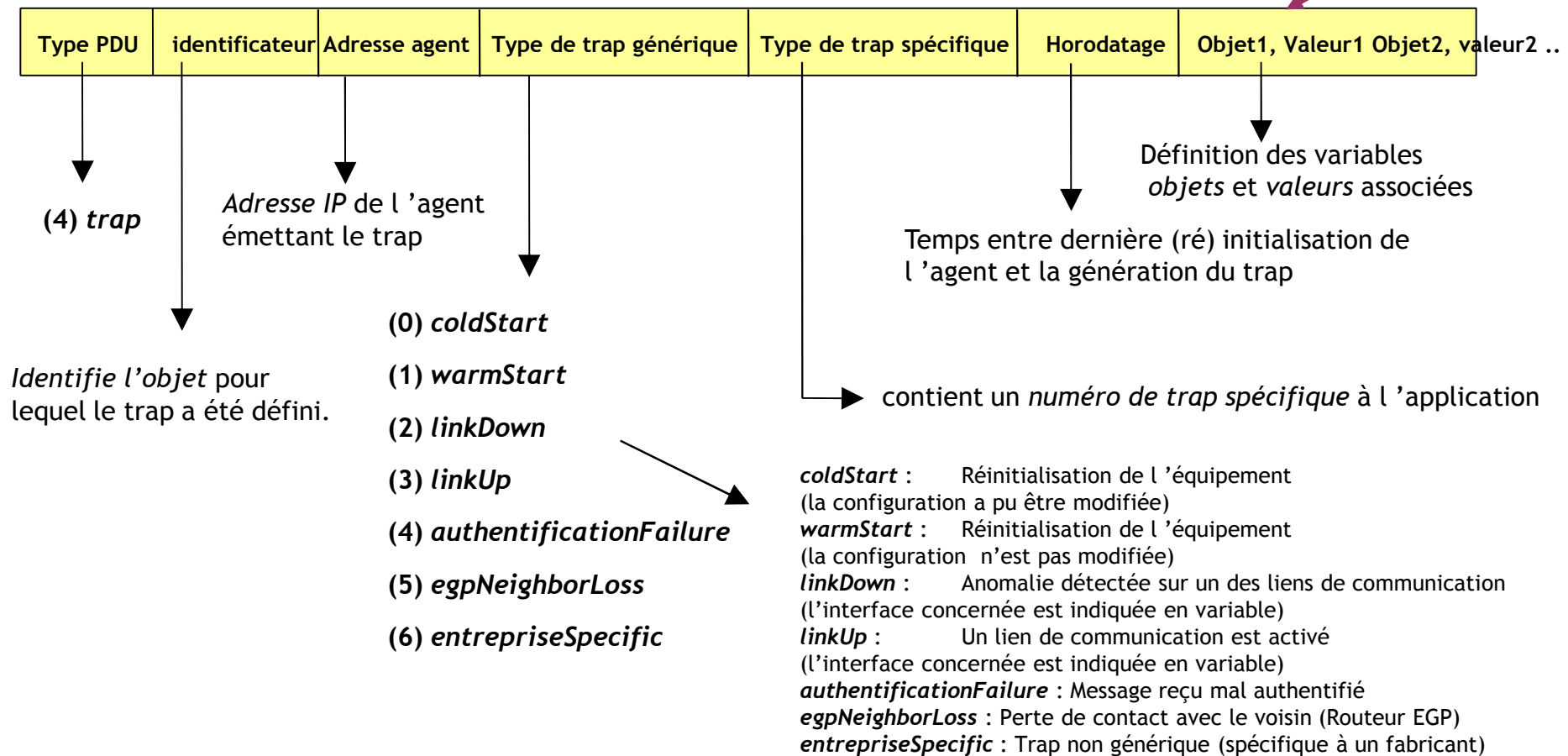
Formats des PDU : Get, Set et Response

L'approche TLV



Format de la PDU Trap

L'approche TLV





Format de la PDU Trap

- ❑ Le champ “identificateur” identifie l’objet de l’équipement qui a émis le Trap
 - Par exemple : Le préfixe OID **1.3.6.1.4.1.121** identifie FTP Software comme objet dans l’émission du Trap
- ❑ Le champ “**Agent Address**” contient l'adresse IP de l'agent envoyant le Trap
- ❑ Le champ “**Specific Trap Type**” précise le type de trap constructeur, quand le champ “generic” indique trap constructeur (entreprise specific)
- ❑ Le champ “**Timestamp**” contient la valeur de l'objet sysUpTime de l’agent au moment de l’envoi de ce trap



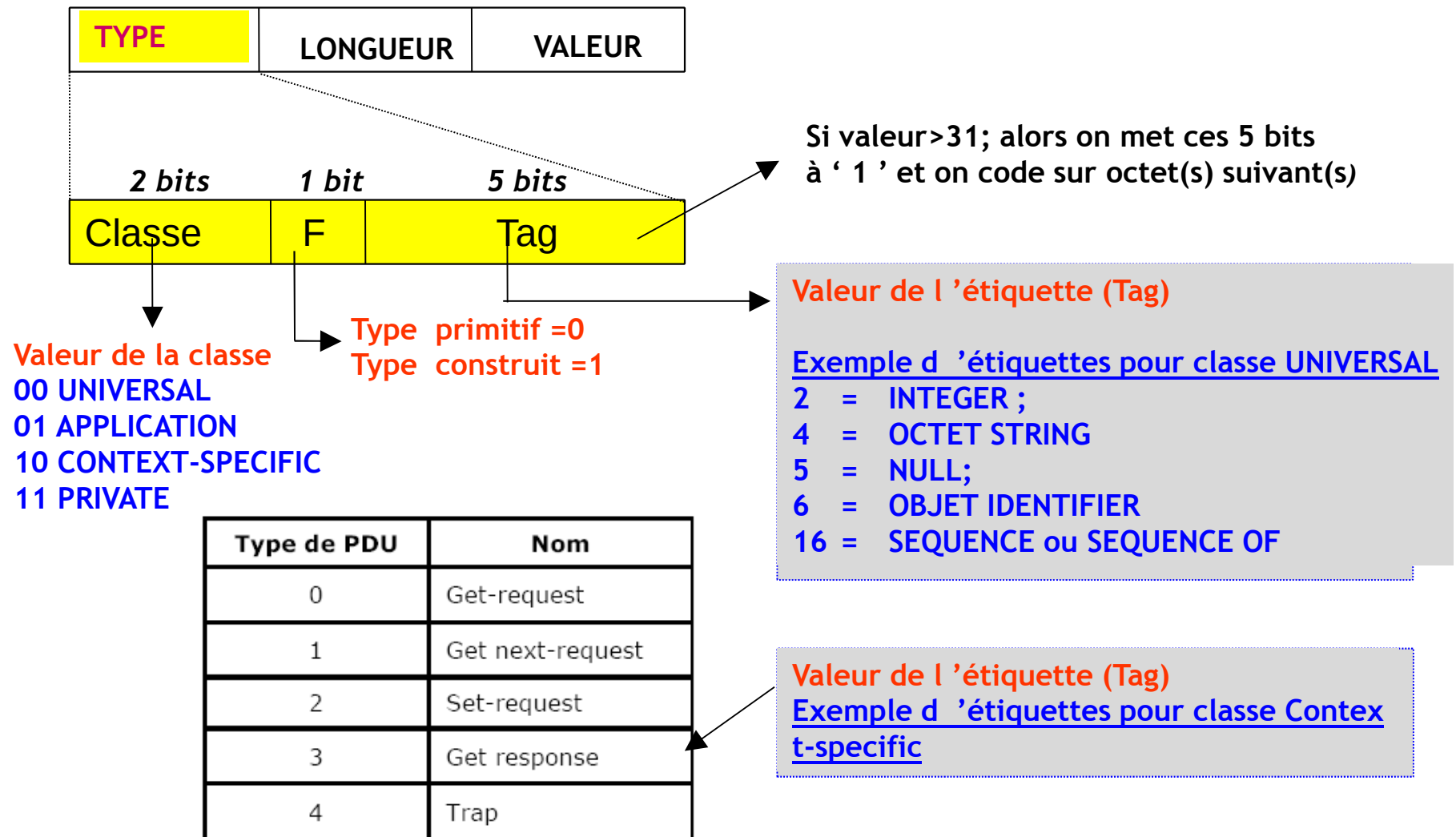
Encodage TLV

- Le SMI (Structure of Management Information) définit toutes les propriétés d'un objet de la MIB
- ASN.1 définit le *type* d'un objet et éventuellement des limites de *valeurs*
- Pour la transmettre des informations de gestion, SNMP utilise un encodage **TLV (Type, Longueur, Valeur)**

Type	Longueur	Valeur
------	----------	--------

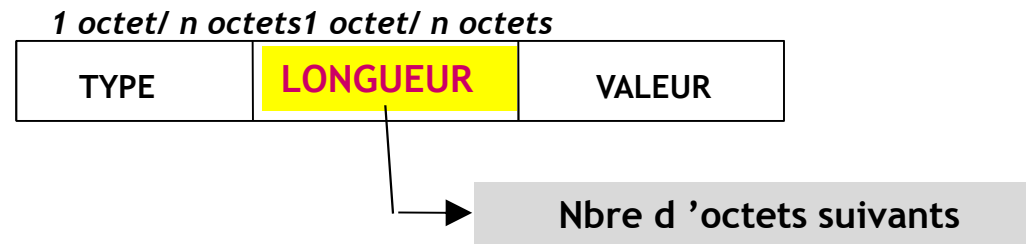
Encodage TLV

1. Encodage du champ TYPE



Encodage TLV

2. Encodage du champ LONGUEUR



3. Encodage du champ VALEUR

<i>1 octet/ n octets</i>	<i>1 octet/ n octets</i>	<i>1 octet/ n octets</i>
TYPE	LONGUEUR	VALEUR



Exemple de valeurs pour classe UNIVERSAL

- INTEGER :** Nbre minimum d'octets pour représenter l'entier
OCTET STRING : Valeurs de la chaîne d'octets
NULL : Pas de valeur
OBJET IDENTIFIER : Il s'agit de coder la valeur de l'OID

Pour l'OID On code selon la formule :

- 1er composant x (40)_{décimal} + 2ème composant
- Les autres valeurs de composants sont codés indépendamment

Exemple :

Le codage de l'OID **1.3.6.1.2.1.200** sera :

$40 \times 1 + 3 = (43)$ _{décimal} ; puis 6; puis 1 etc

le codage de VALEUR en hexadécimal sera: **2B 06 01 02 01 81**

Donc le Codage TLV de l'OID **1.3.6.1.2.1.200** est **2B 06 01 02 01 81**



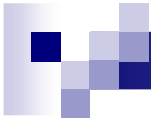
Exemple d'encodage TLV

- INTEGER (Classe = 00, Forme = 0, Tag = 2)
 - La représentation utilisant le plus petit nombre d'octets possible
 - Exemple : 500 codé **02 02 01 f4** (en hexadécimal)

- OCTET STRING (Classe = 00, Forme = 0, Tag = 4)
 - Les contenus représentent exactement les valeurs de la chaîne d'octets
 - Exemple : 55 ff 00 codé **04 03 55 ff 00** (en hexadécimal)

- NULL (Classe = 00, Forme = 0, Tag = 5)
 - Il n'y a pas de contenu
 - Exemple : Null codé 05 00 (en hexadécimal)

- OID (Classe = 00, Forme = 0, Tag = 6)
 - Il s'agit de coder la valeur de l'OID
 - Exemple : OID = 1.3.6.1.2.1.1 .1 codé **06 08 2B 06 01 02 01 01 01 00**
= (Syst Descr)



Analyse d'une trame SNMP



Ethernet

Destination: 00:00:00:00:00:00 (00:00:00_00:00:00)
Source: 00:00:00:00:00:00 (00:00:00_00:00:00)
Type: IP (0x0800)

MIB : Exemple Capture de trame

Internet Protocol,

Src Addr: localhost.localdomain (127.0.0.1),
Dst Addr: localhost.localdomain (127.0.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP
Total Length: 71
Identification: 0x0000 Flags: 0x04 .
1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64

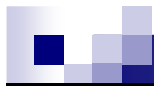
Protocol: UDP (0x11)

Header checksum: 0x3ca4 (correct)
Source: localhost.localdomain (127.0.0.1)
Destination: localhost.localdomain (127.0.0.1)
User Datagram Protocol,
Src Port: 1867 (1867),
Dst Port: snmp (161)
Checksum: 0xd027 (correct)

Simple Network Management Protocol

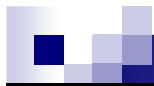
Version: 1
Community: public
PDU type: GET Request (code 0000)
Id: 0x34339329
Error Status: NO ERROR Error
Index: 0 Object
identifier 1: 1.3.6.1.2.1.1.3.0
Value: NULL

Type de PDU	Nom
0	Get-request
1	Get next-request
2	Set-request
3	Get response
4	Trap



Séquence	30	27
----------	----	----

27 = 39 octets



Séquence	30	27
----------	----	----

27 = 39 octets

Entier	02	01	:	00
--------	----	----	---	----

Séquence 30 27 27 = 39 octets

Entier 02 01 : 00

Caractère 04 06 : 70 75 62 6C 69 63
P U B L I C

Header

Séquence	30	27
----------	----	----

27 = 39 octets

Entier	02	01	:	00
--------	----	----	---	----

Caractère	04	06	:	70	75	62	6C	69	63
				P	U	B	L	I	C

Séquence	A0	1A
----------	----	----

A0 = 1010 0000 (Get Request)

1A = 26 octets

PDU

Séquence 30 27 27 = 39 octets

Entier 02 01 : 00

Caractère 04 06 : 70 75 62 6C 69 63
P U B L I C

Séquence A0 1A A0 = 1010 0000 (Get Request)
1A = 26 octets

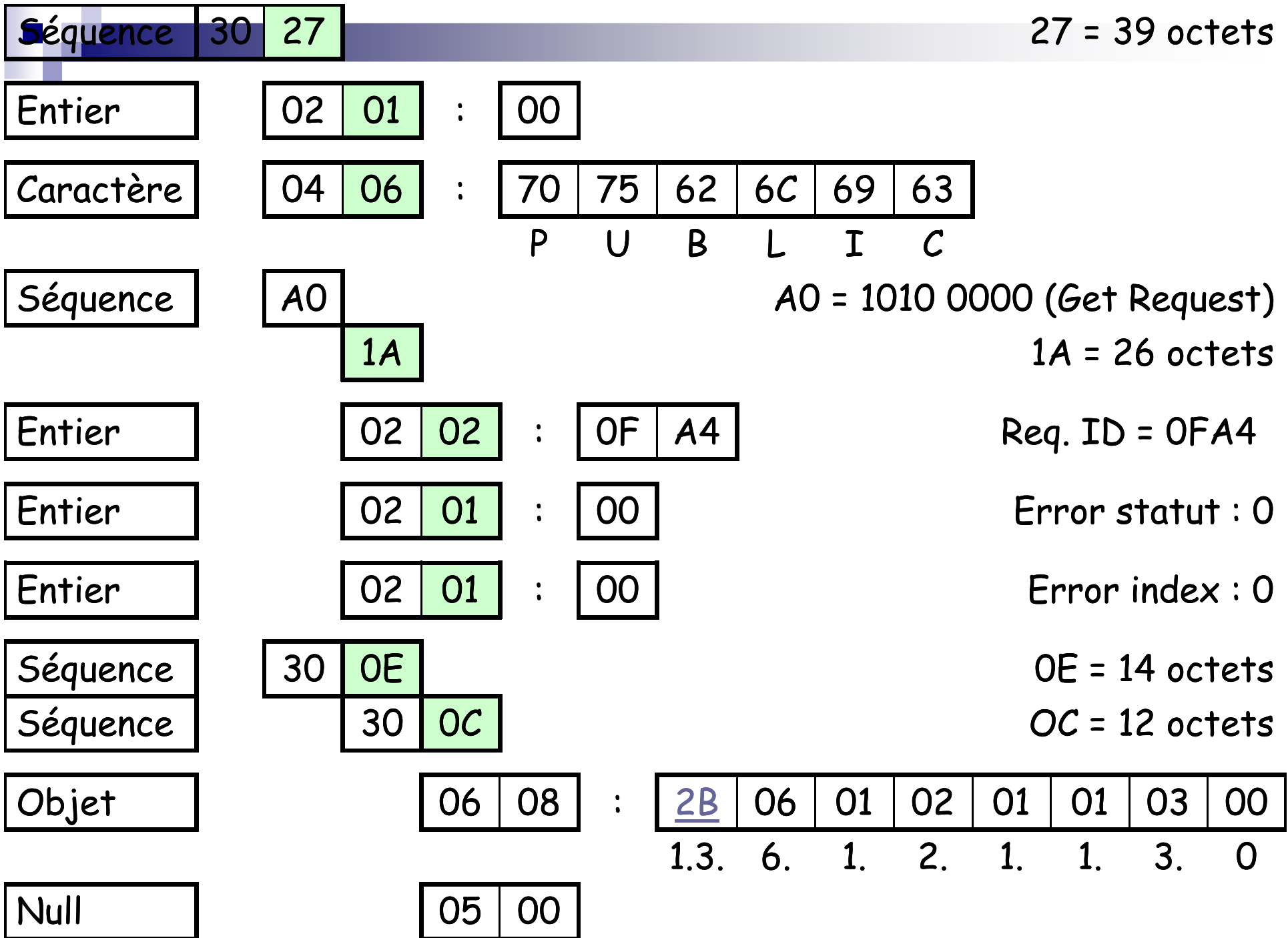
Entier 02 02 : 0F A4

Entier 02 01 : 00

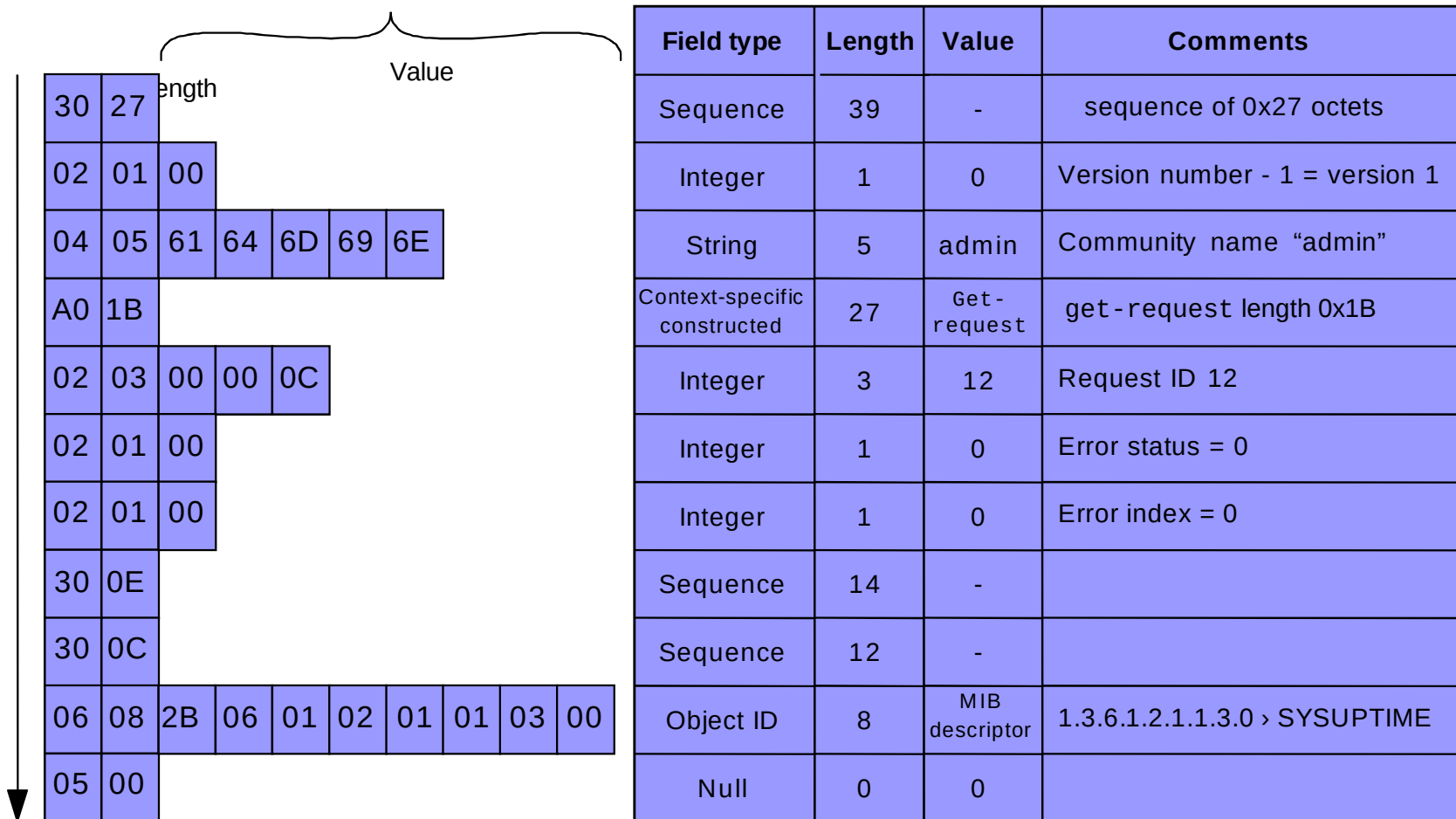
Entier 02 01 : 00

PDU

Req. ID = 4004
Error status : 0
Error index : 0

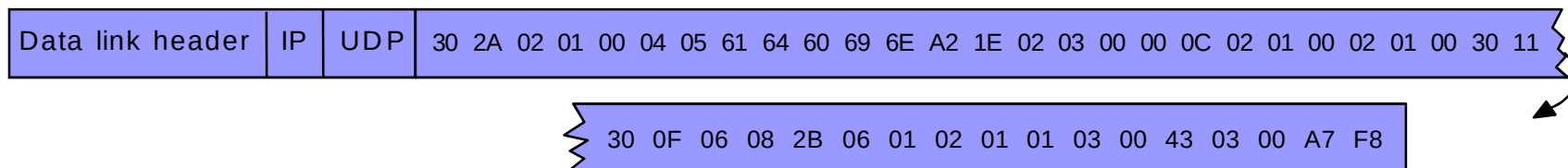
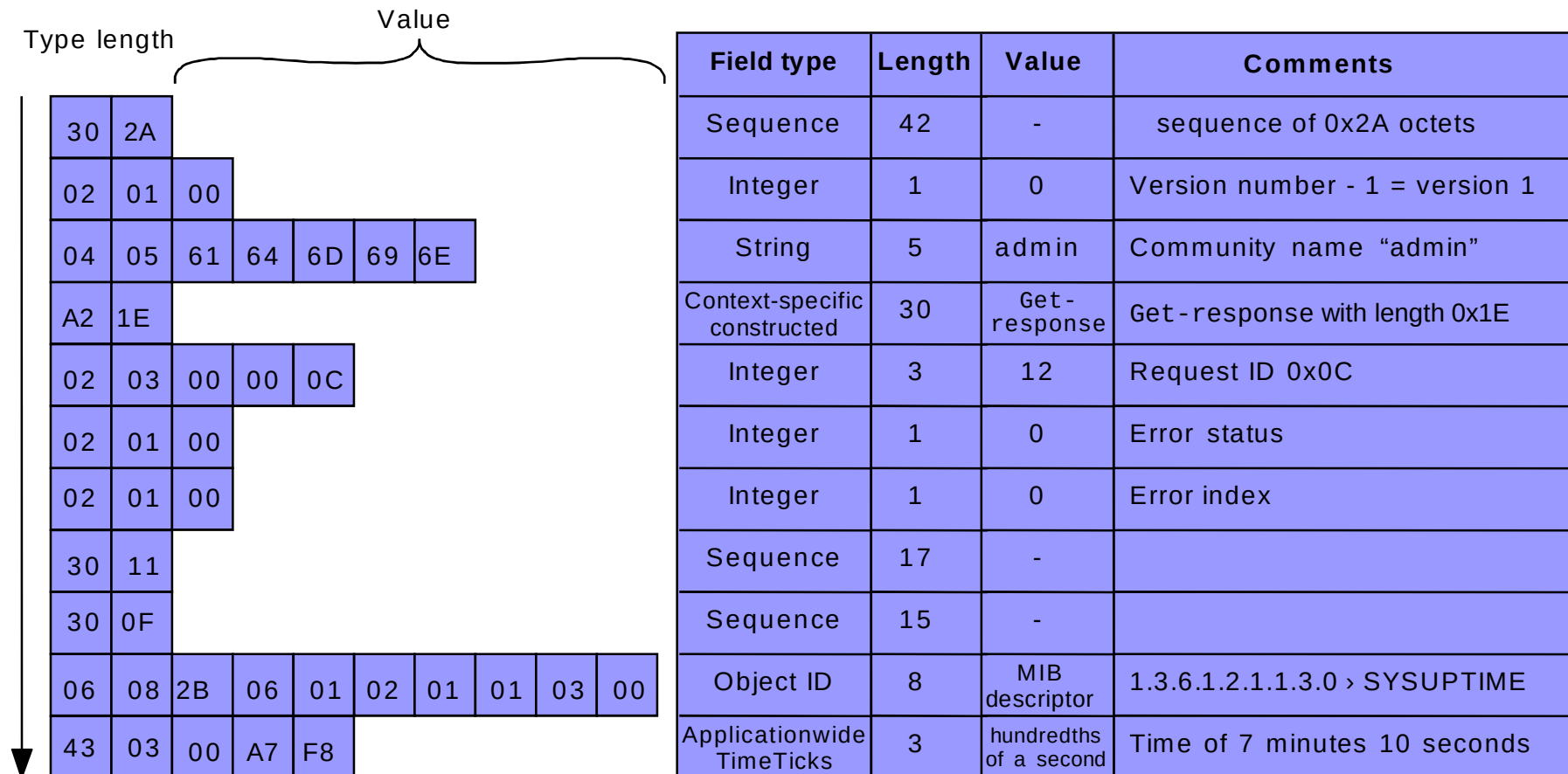


Message *Get Request* avec SNMP



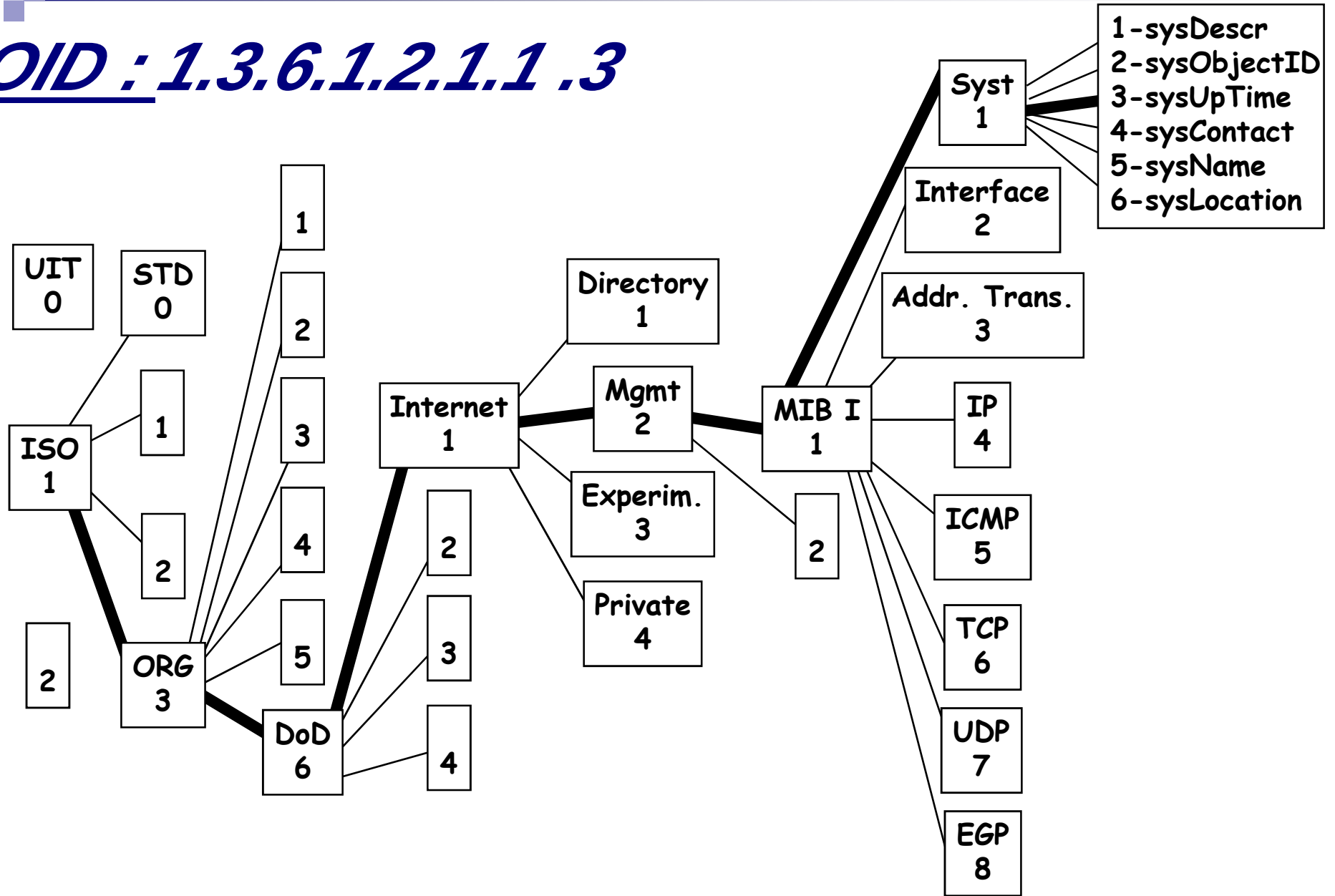
30 27 02 01 00 04 05 61 64 6D 69 6E A0 1B 02 03 00 00 0C 02 01 00 02 01 00 30 0E 30 0C 06 08 2B 06 01 02 01 01 03 00 05 00

Message *Get Response* avec SNMP





OID : 1.3.6.1.2.1.1.3





SNMP : Avantages

- ❑ L'avantage majeur dans le fait d'utiliser SNMP est qu'il est de conception simple ; il est donc aisé de l'implémenter sur un réseau, puisqu'il ne prend pas longtemps à configurer et qu'il est de petite taille.
- ❑ Un autre avantage de SNMP est qu'il est vraiment beaucoup répandu aujourd'hui. Presque tous les grands constructeurs de matériel hardware inter-réseaux, tels que les ponts ou les routeurs, conçoivent leurs produits de manière à ce qu'il supportent SNMP, rendant ce dernier très facile à implémenter.
- ❑ Enfin, SNMP est basé sur le protocole de transport UDP ce qui nécessite moins de ressources et de connexions simultanées qu'avec TCP. Il n'y a pas de récupération d'erreurs et un faible overhead UDP au niveau des messages. Et enfin, c'est une solution peu chère.



SNMP : Inconvénients

- ❑ Le premier défaut de SNMP est qu'il contient quelques gros trous de sécurité à travers lesquels des intrus peuvent accéder aux informations transitant sur le réseau. Ces intrus pourraient aussi bien provoquer un shut-down sur certains terminaux. La solution à ce problème est apportée dans SNMPv2 qui implémente des mécanismes de sécurité en ce qui concerne le caractère privé des données, l'authentification et le contrôle d'accès.
- ❑ Puisque SNMP se trouve au dessus de UDP, il n'y a pas de reprise sur erreur, ni de contrôle de flux. La requête ou la réponse peut être égarée, ce qui peut être gênant dans le cas du trap. Le Manager surveille donc son environnement en procédant à des interrogations régulières de ses agents, c'est ce que l'on appelle le Polling. SNMP est donc un protocole bavard. Cette surcharge de trafic n'est pas trop gênante sur un réseau local mais devient embarrassante via le réseau public.



Exercice : SNMP et charge du réseau

Si la période de polling est fixée à 10 secondes, le débit du lien de 64 kbit/s et la taille moyenne d'un message SNMP de 100 octes.

Question : Quelle est l'influence de la consultation de 100 objets SNMP à travers un lien WAN?



Solution : SNMP et charge du réseau

Le nombre de sollicitations est de 100 toutes les 10 secondes, ce qui correspond à 10 sollicitations par seconde. Dans ces conditions, le volume à transférer est de :

$$(100 * 8) * 10 = 8000 \text{ bits/s}$$

Ce qui correspond pour une ligne à 64 Kbits/s à 12,5 % de ses capacités de transfert.

Conclusion : Le protocole SNMP est un protocole Bavard.