



Chap.9: SNMP: Simple Network Management Protocol

1. Présentation
2. L'administration de réseau
3. Les fonctionnalités du protocole
4. Les messages SNMP
5. Utilisation de SNMP



1. Présentation

- En 1988, le besoin d'un outil de gestion de réseaux TCP-IP s'est fait sentir.
- En 1991, la version 1.0 de SNMP est publiée (RFC 1155, 1212, 1213, 1157)
- En 1993, SNMP v2 incorpore sécurité et authentification et devient le standard.
- SNMP v3 devrait améliorer la sécurité et les fonctions administratives



Les différentes versions SNMP

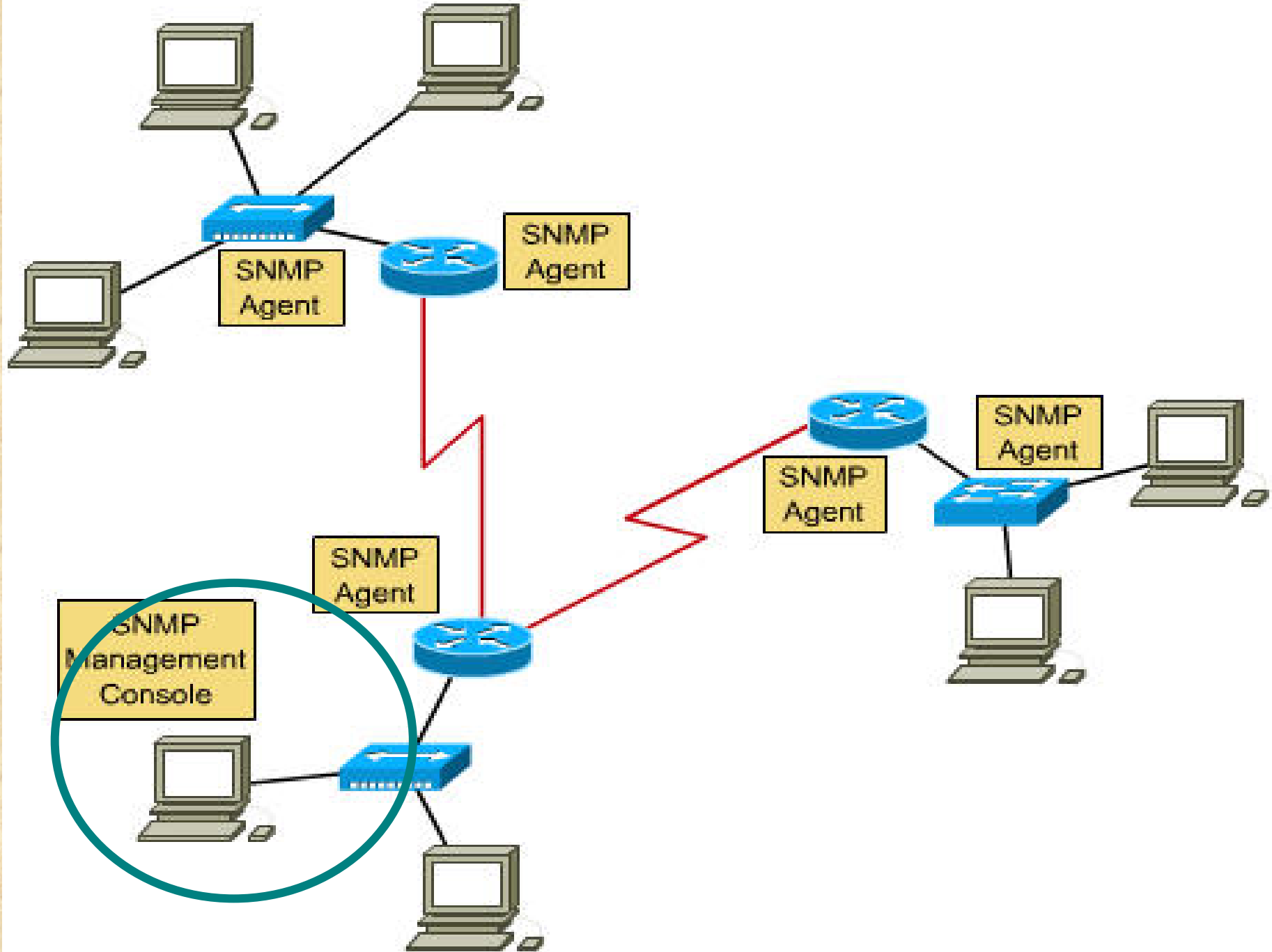
- ❑ SNMPv1: les modèles fonctionnels
- ❑ SNMPv2: SMI et MIB (Management Information Base)
- ❑ SNMPv3: la sécurité

SMI: Structure of Management Information

La norme SNMP est une norme de gestion réseau largement utilisée dans les réseaux TCP/IP et, depuis peu, dans les réseaux Internet Packet Exchange (IPX).

Définitions

- Agent : Logiciel qui permet à une composante du réseau (commutateur, routeur...) de répondre aux requêtes de la station de gestion.
- Station de gestion : (openview, ciscoworks...)
 - Trace un portrait du réseau
 - Analyse les info des MIBs
 - Fait des graphiques.
- MIB : Management Information Base
 - Base de données contenant les objets gérés dans chaque composante du réseau



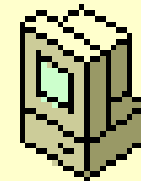
Informations d'état

Version de logiciel
Adresse IP
Espace disponible
sur le disque dur
Tables de session
Ouvrir les fichiers
Table ARP

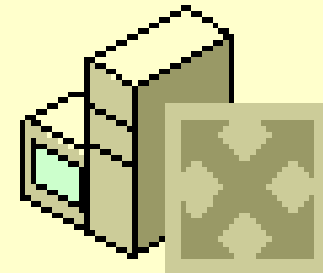


**Gestionnaire
SNMP**

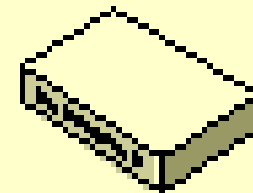
Agents SNMP



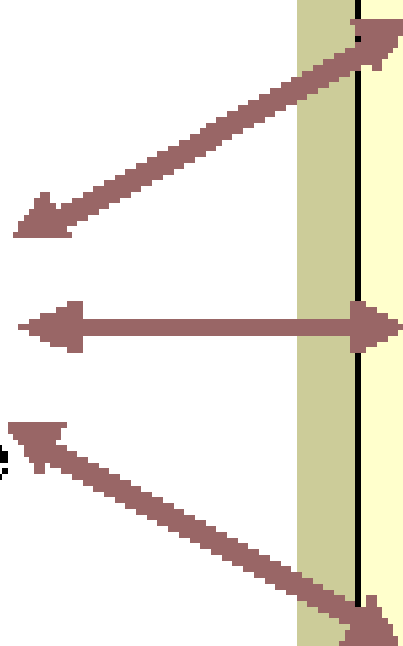
Ordinateur
Windows 2000



Routeur



Concentrateur
de câblage



[Agrandir la figure](#)



L'Audit de gestion des ressources

Rôle du gestionnaire SNMP vis à vis des agents:

- Configurer des périphériques distants.
- Surveiller les performances du réseau..
- Détecter les défaillances du réseau
- **Gestion des alarmes:** lorsqu'une alarme se déclenche, le périphérique transmet un message d'événement au système de gestion. Les types d'alarmes courants sont par exemple, l'arrêt et le redémarrage d'un périphérique, la détection d'un lien défaillant sur un routeur et un accès interdit.



2. L'administration de réseau

L'administration réseau implique les tâches ci-dessous:

- La surveillance de la disponibilité du réseau
- L'amélioration de l'automatisation
- La surveillance des temps de réponse
- La mise en place de fonctionnalités de sécurité
- Le réacheminement du trafic
- Le rétablissement de la fonctionnalité
- L'enregistrement d'utilisateurs

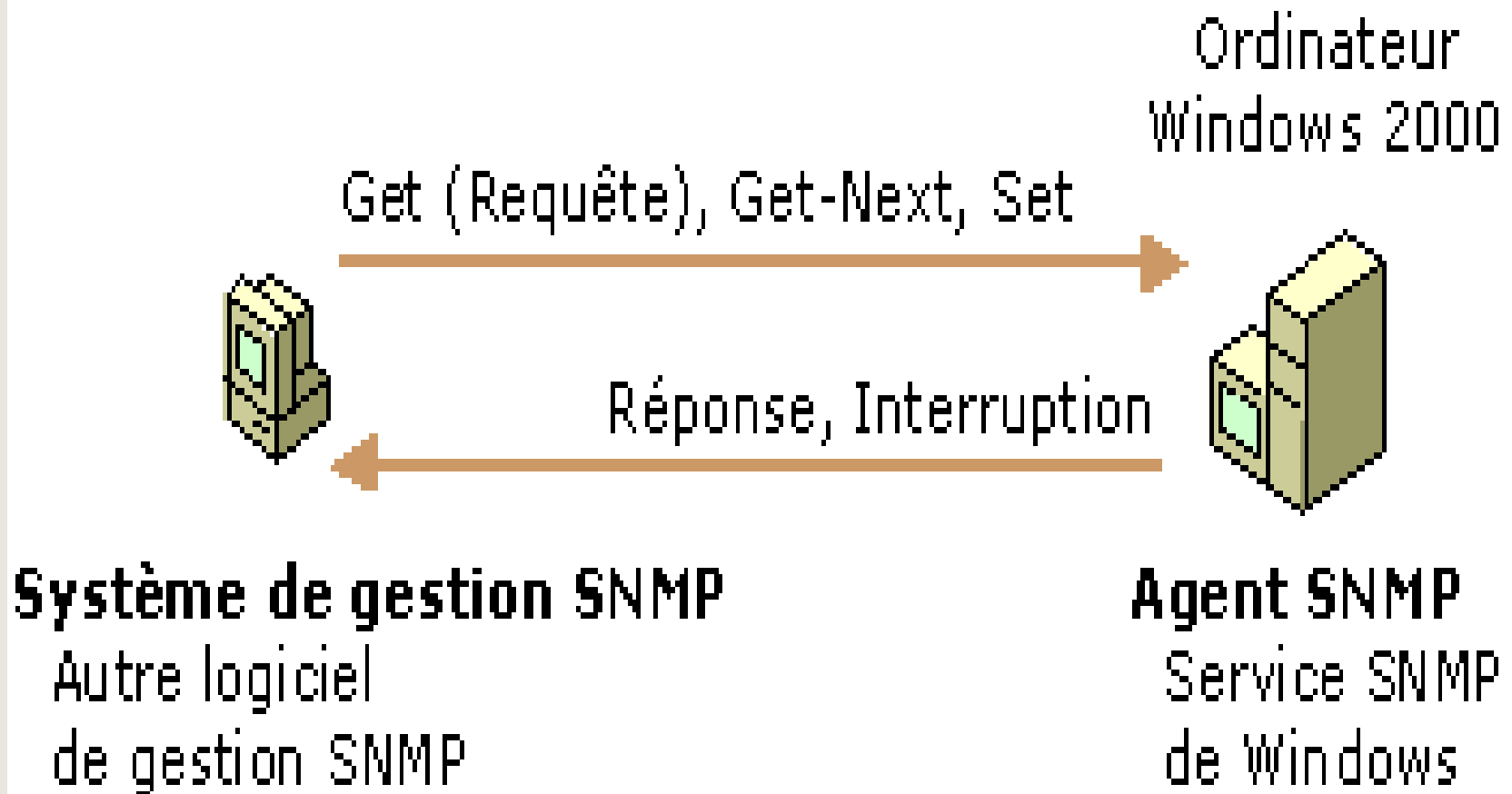
Communauté Internet - SNMP

- Protocole SNMP (Simple Network Management Protocol)
- Protocole, spécification de structure de base de données et ensemble d'objets de données
- Norme TCP/IP adoptée en 1989
- SNMPv2c en 1993 ; SNMPv3 est la version actuelle

Communauté OSI - CMIP

- Protocole CMIP (Common Management Information Protocol)
- Ensemble complexe de normes. Ce protocole définit un service d'administration, un protocole, une spécification de structure de base de données et un ensemble d'objets de données.

2.1 Systèmes de gestion et agents

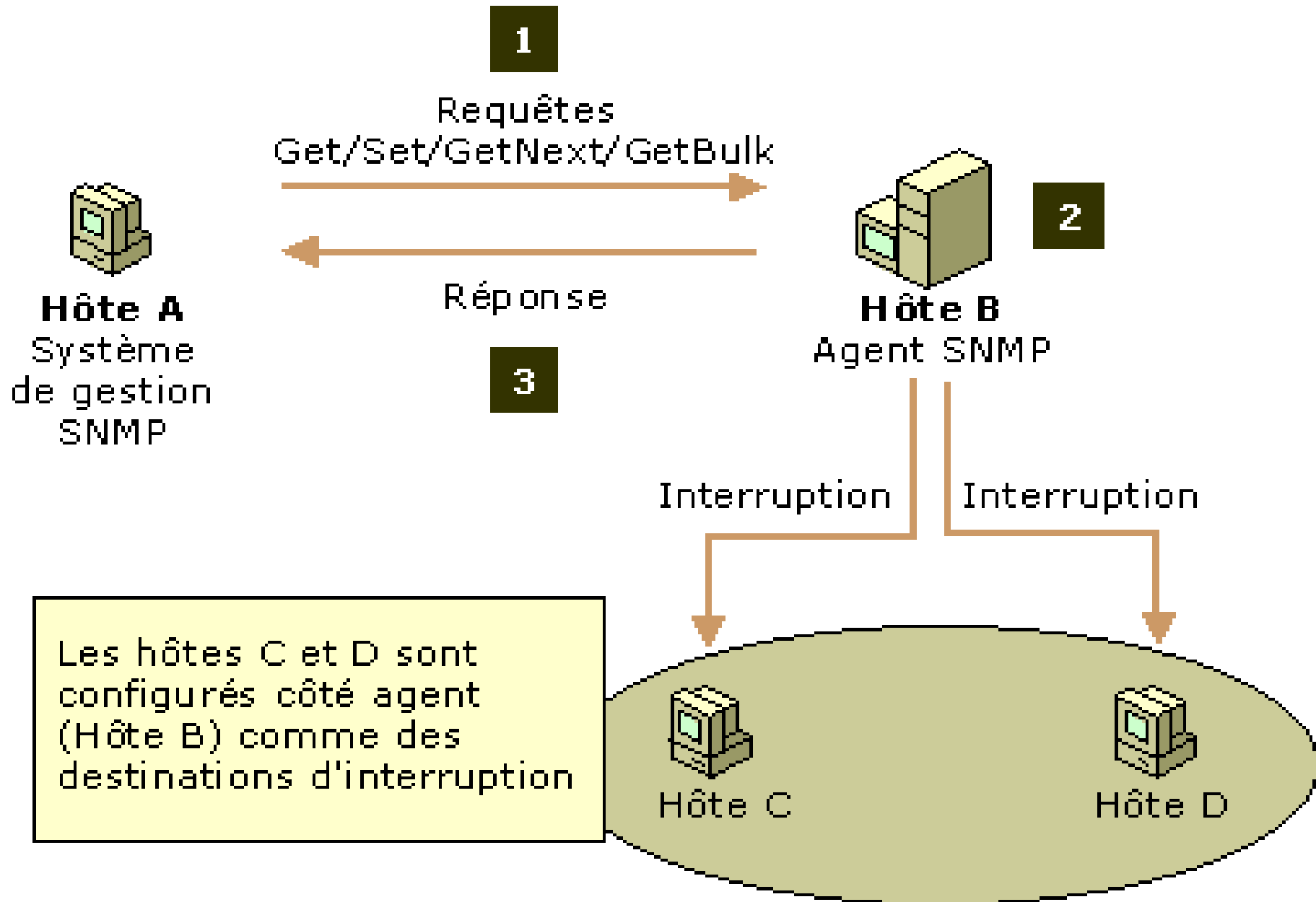




2.1 (suite)

- **Système de gestion SNMP:** le système de gestion, également appelé *console de gestion*, envoie les demandes d'informations et de mises à jour à un agent
- **Agent SNMP :** Généralement, les agents n'envoient pas de messages, mais ne font qu'y répondre. Un message d'interruption est la seule communication SNMP déclenchée par un agent. Une interruption est un événement qui déclenche une alarme chez un agent, par exemple le redémarrage du système

2.2 Mode de fonctionnement du Protocole SNMP





2.2. (suite)

- **Le système de gestion (Hôte A)**, envoie un datagramme SNMP à l'agent (Hôte B), en utilisant le nom d'hôte de l'agent, son adresse IP ou IPX.
- **L'agent SNMP** reçoit le datagramme et vérifie le nom auquel est rattaché le système de gestion. Si valide, l'agent extrait les données demandées, sinon l'agent envoie une **interruption « échec d'authentification »** à ses destinations d'interruptions (Hôtes C et D).
- **L'agent SNMP** renvoie le datagramme au système de gestion avec les informations demandées.



2.2 (suite)

Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments:

- La station d'administration : NMS
- L'agent de supervision
- La base de données de gestion :MIB
- Le protocole de gestion de réseau

NMS: Network Management System

MIB: Management Information Base

Architecture d'administration réseau hiérarchique

FIGURES

1

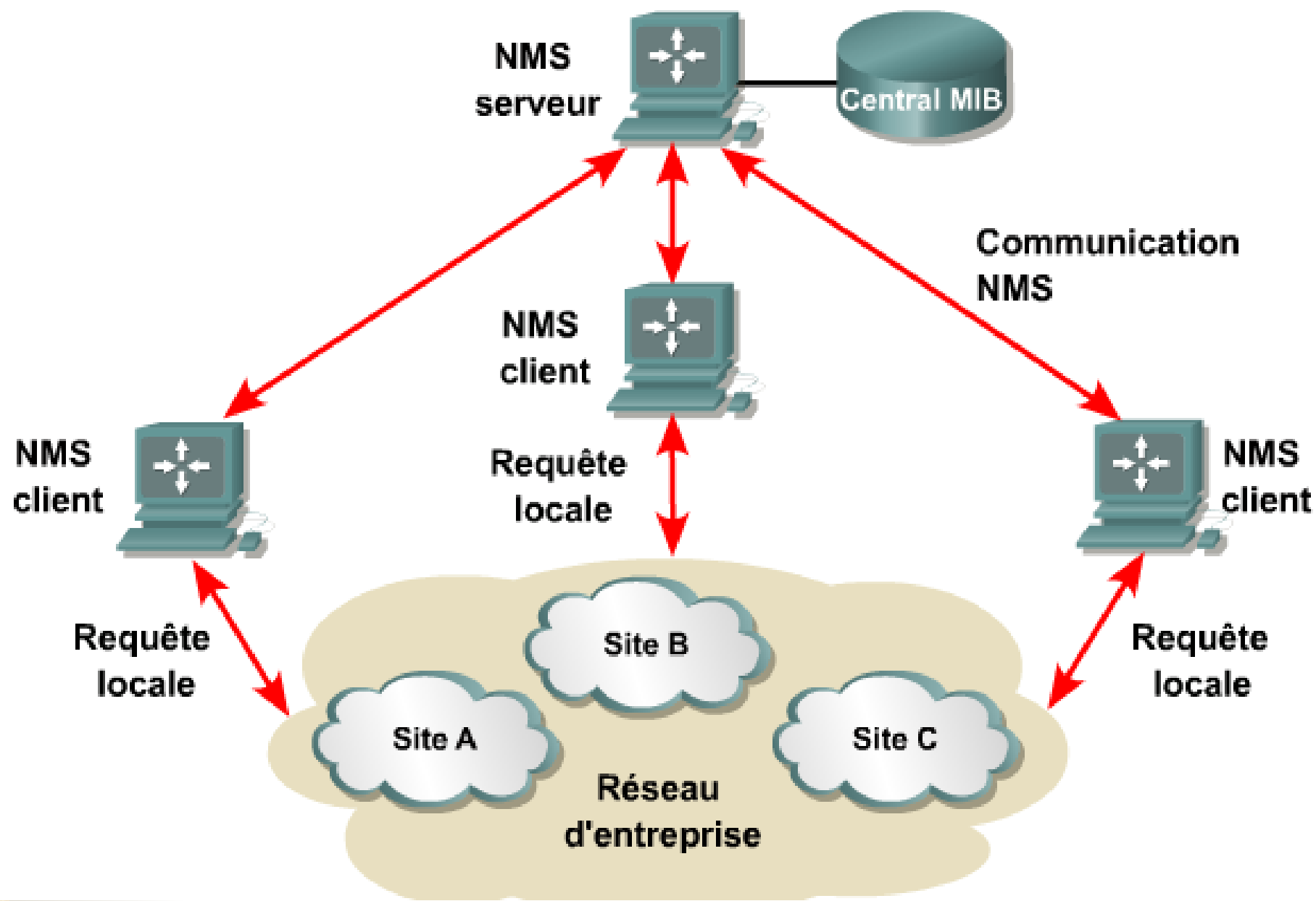
2

3

4

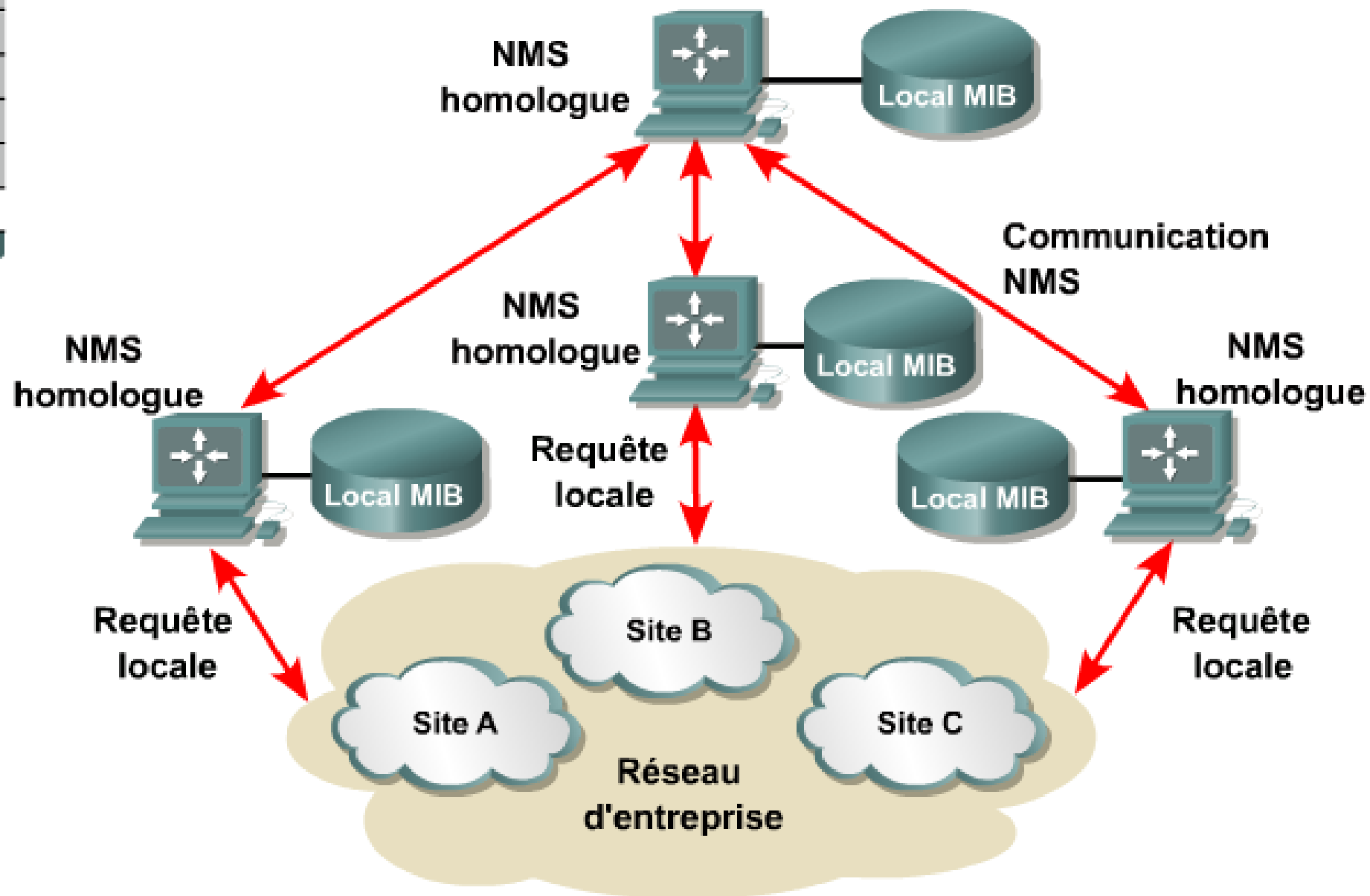
5

6



FIGURES

1
2
3
4
5
6





Unités dans l'administration du réseau

Nom du groupe	Description
System	Description de toutes les entités gérées.
Interface	Interface de données dynamiques ou statiques.
Address Translation	Table d'adresses IP pour les correspondances d'adresses MAC
IP	Statistiques du protocole IP, adresse cache et table de routage
ICMP	Statistiques du protocoles ICMP
TCP	Paramètres TCP, statistiques et table de connexion
UDP	Statistiques UDP
EGP	Statistiques EGP, table d'accessibilité
SNMP	Statistiques du protocole SNMP



2.3 Les messages SNMP

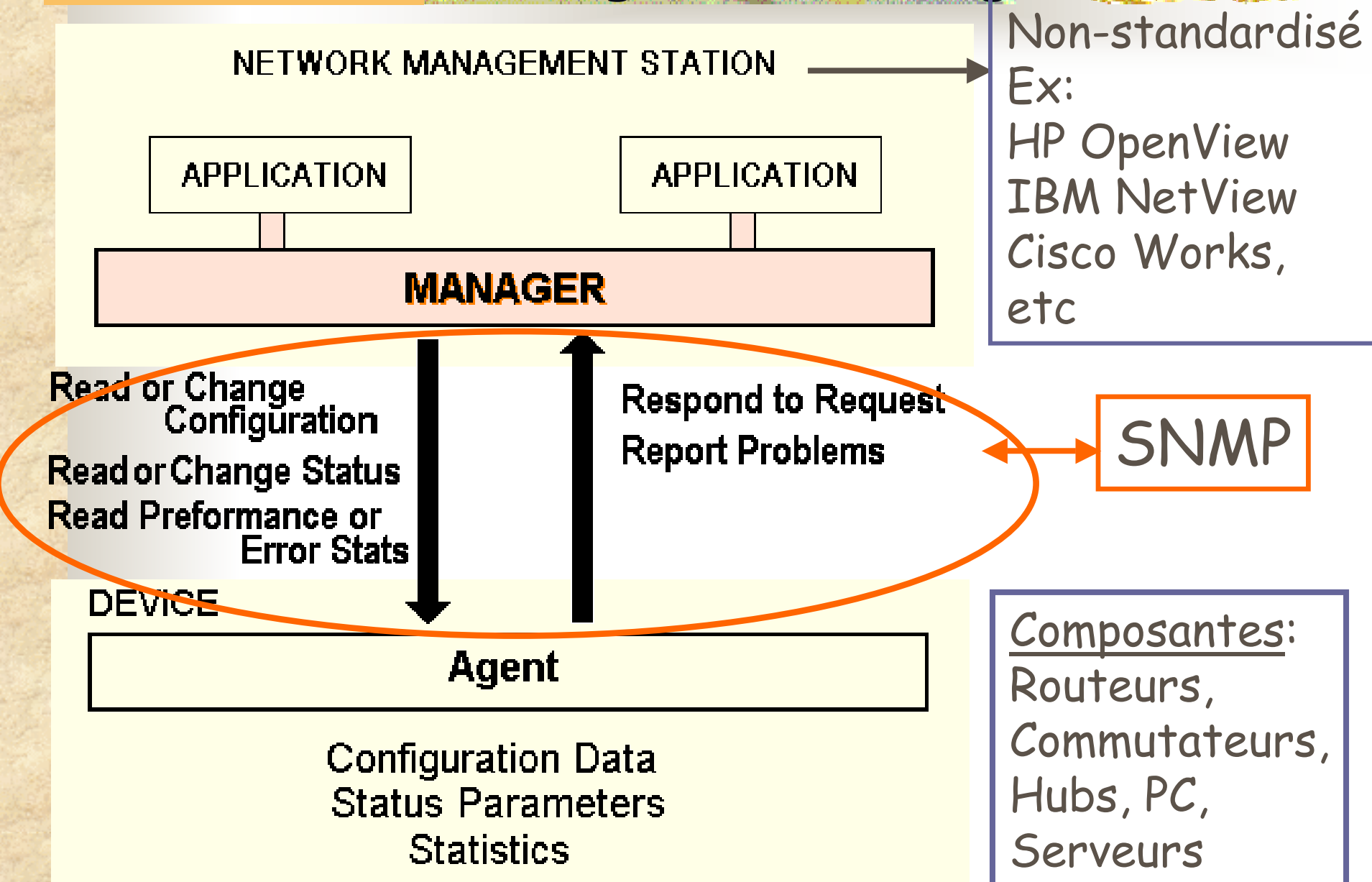
- Le NMS exécute une fonction de surveillance en récupérant les valeurs dans la MIB. La NMS peut occasionner l'exécution d'une action au niveau d'un agent.
- Le protocole SNMP utilise le protocole UDP et communique sur les ports 161 et 162. Il est fondé sur un échange de messages. **Il existe trois types de message courants:**
- **Get** – Permet à la station d'administration de récupérer la valeur des objets MIB à partir de l'agent.
- **Set** – Permet à la station d'administration de définir la valeur des objets MIB au niveau de l'agent.
- **Trap** – Permet à l'agent d'avertir la station d'administration lors d'événements



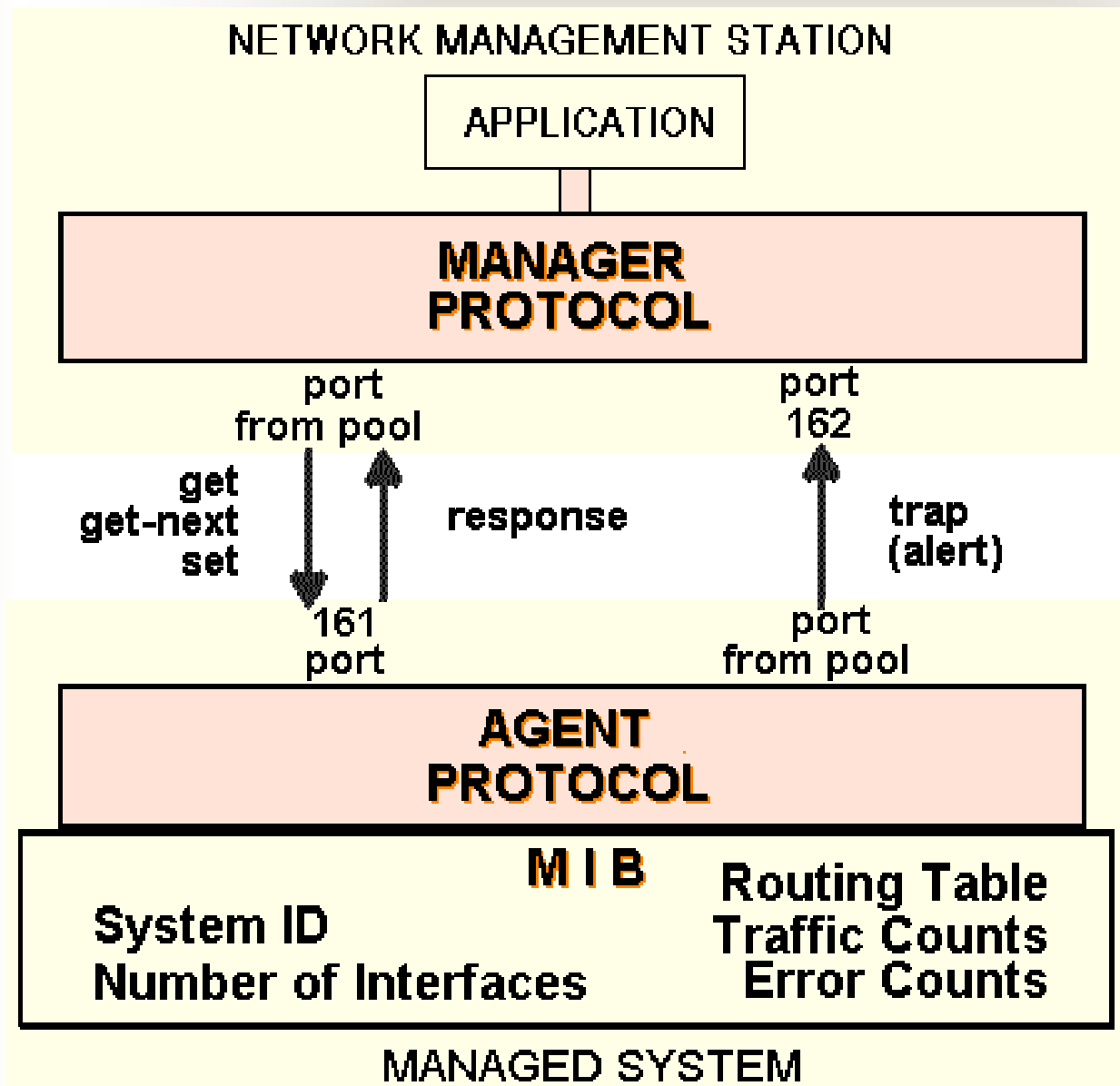
2.3 (suite) Autres messages

- **Getbulk :** demande que les données transférées par l'agent hôte soient aussi importantes que possible, tout en respectant les contraintes de taille du message.
- **Interruption:** message non sollicité, envoyé depuis un agent SNMP à un système de gestion SNMP, lorsque l'agent détecte sur l'hôte géré, un événement local d'un certain type. **Par exemple, un message d'interruption peut être envoyé à un événement de redémarrage du système.**

Schéma des échanges de messages



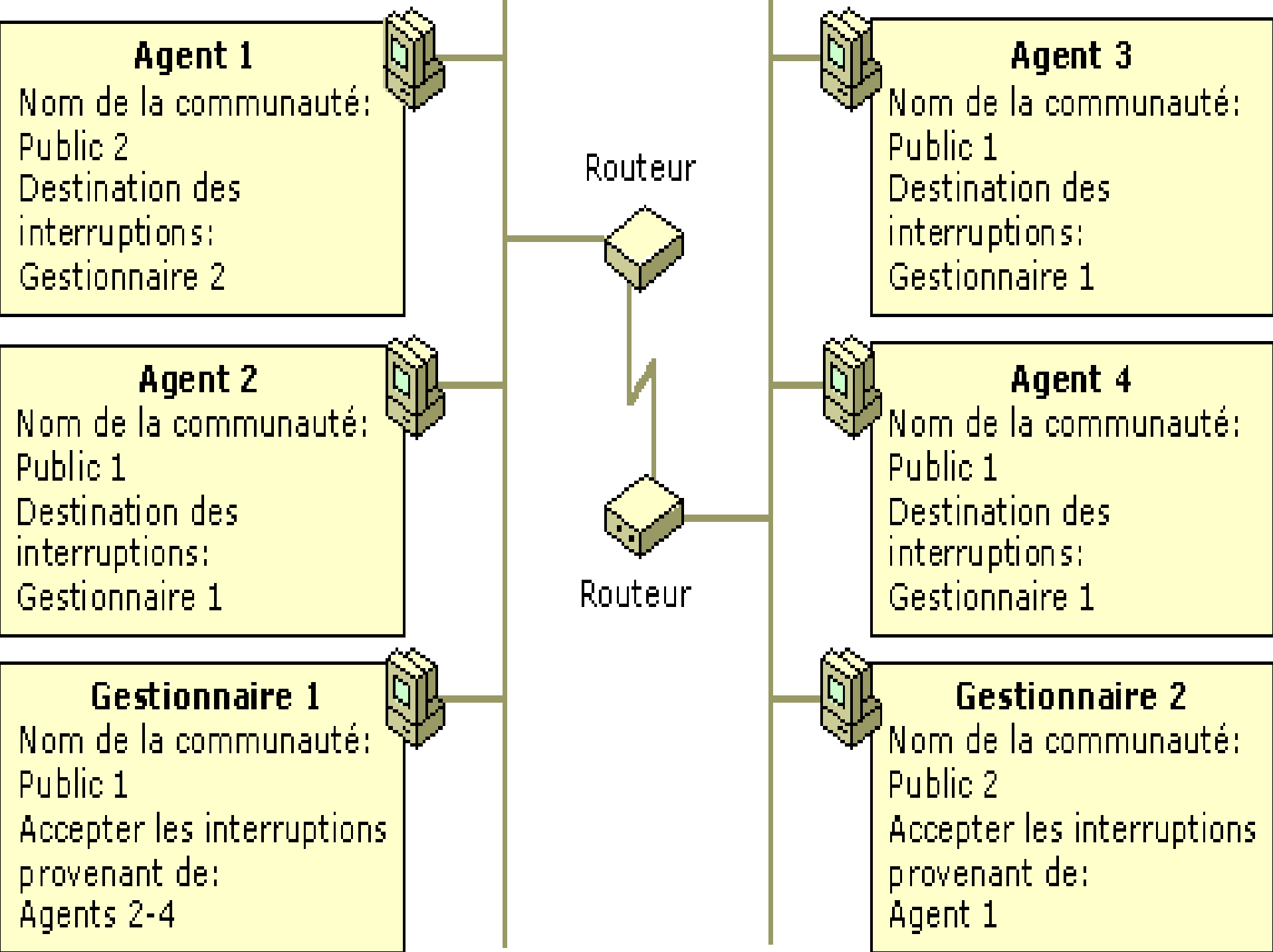
Ports et MIB





3. Utilisation de SNMP

- **3.1 Définition des communautés**
- Vous pouvez affecter des groupes d'hôtes aux communautés SNMP pour un contrôle restreint de la sécurité des agents et des systèmes de gestion, ou pour des besoins administratifs.
- Les communautés sont identifiables par les noms que vous leur attribuez. Un hôte peut appartenir à plusieurs communautés à la fois, mais un agent refuse toute requête de la part d'un système de gestion figurant hors de sa liste des noms de communautés acceptables.





3.2 Propriétés de l'agent

- L'agent SNMP offre un système de gestion des informations sur les activités se déroulant au niveau de la couche réseau IP
- Le service SNMP envoie à l'agent des informations en réponse à une requête SNMP ou à un message d'interruption SNMP.

Composants du modèle d'organisation

FIGURES

1

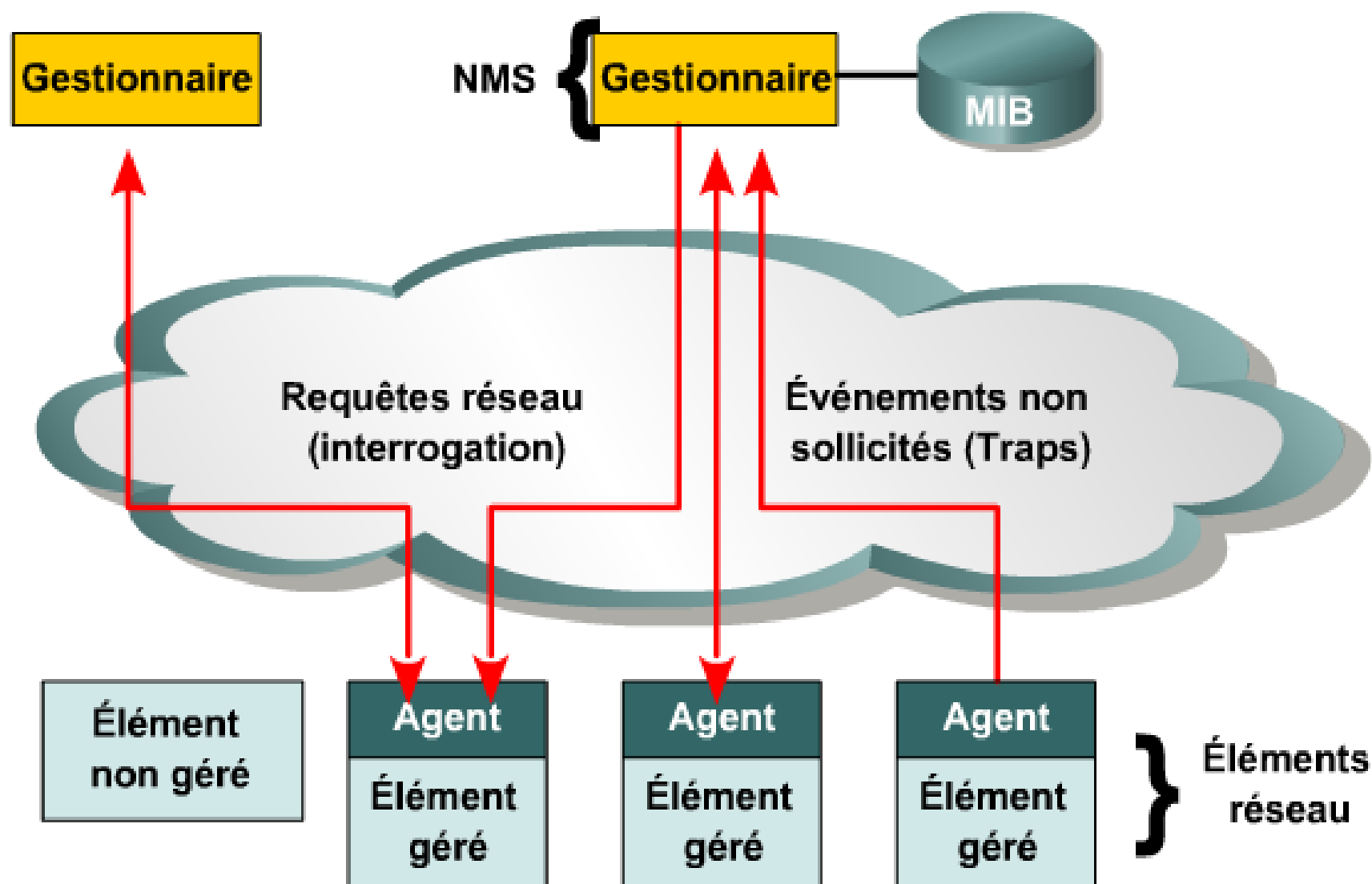
2

3

4

5

6





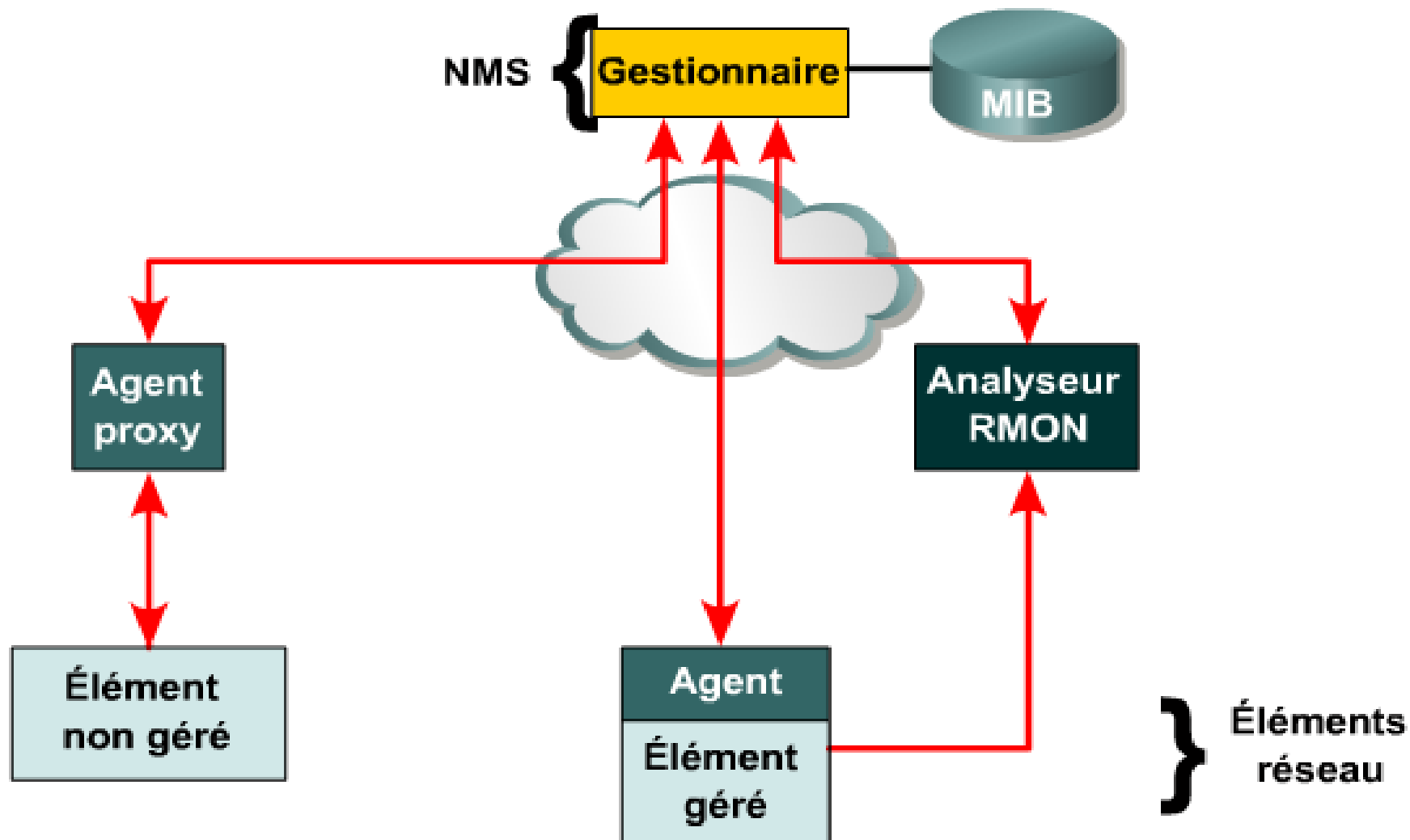
Que fait l'agent ?

- L'agent est une fonction logicielle intégrée à la plupart des équipements de réseau, tels que les routeurs, les commutateurs, les concentrateurs administrés, les imprimantes et les serveurs.
- Il est responsable du traitement des requêtes SNMP provenant de la station d'administration. Il est également responsable de l'exécution de routines de gestion de variables définies dans les diverses bases MIB prises en charge.
- L'interaction entre la station d'administration et l'agent est facilitée par le protocole SNMP.

Composants du modèle d'organisation (suite)

FIGURES

1
2
3
4
5
6





RMON – Remote MONitoring

- Extension de SNMP
- Ne peut pas exister sans SNMP
- Améliore la surveillance des réseaux en créant de nouvelles catégories d'information.
- Utilise des sondes (probes) qui sont des agents avec des fonctionnalités accrues.

Catégories d'info avec RMON

