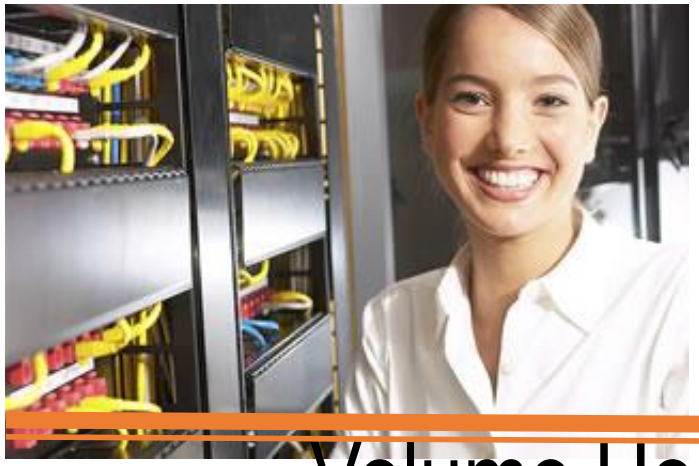


Introduction à l'Administration Réseau

Volume Horaire : 60 Heures (30 heures Théoriques + 30 heures pratiques)

G2 Réseaux : Administration Système

Chargé du Cours : Derick Khon K.

Tél : 099 10 59 100, 085 47 83 836
Email : derick.khon@gmail.com
derick.khon@esisalama.org

CHAPITRE II

ISO et l'ADMINSTRATION RESEAU

PLAN DU CHAPITRE

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

1. Modèles d'administration selon ISO
2. Fonctionnalités de l'administration réseau

    a) Gestion des anomalies
    b) Gestion de la configuration
    c) Gestion de performance
    d) Gestion de la Sécurité
    e) Gestion de la Comptabilité

3. Architecture de l'administration réseau
4. La Télé-administration
    - Le Monitoring Réseau
    - L'infogérance

DETAILS DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

5. Protocoles de Gestion des Réseaux

a) CMIP/CMIS
b) Netflow
c) SNMP

- Présentation de SNMP
- Principe de fonctionnement
- Structure d'un paquet SNMP
- Versions de SNMP

6. Eléments de gestion d'informations

a) Base d'Informations de Gestion (MIB)
b) Structure de Gestion d'Informations (SMI)

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

1. Modèles d'administration selon ISO

1. Fonctionnalités de l'administration réseau

   a) Gestion des anomalies
   b) Gestion de la configuration
   c) Gestion de performance
   d) Gestion de la Sécurité
   e) Gestion de la Comptabilité

3. Architecture de l'administration réseau
4. La Télé-administration
   - Le Monitoring Réseau
   - L'infogérance

MODELES D'ADMINISTRATION SELON ISO

L'administration d'une manière générale est basée sur un modèle qui définit les principes de la station de gestion du réseau dont nous allons parler plus bas.
Ainsi ISO définit quatre composantes

MODELES D'ADMINISTRATION SELON ISO

Modèle organisationnel

Définit l'interaction des entités du réseau en vue de permettre la bonne gestion (Manager - Agents)

MODELES D'ADMINISTRATION SELON ISO

Modèle organisationnel

La communication entre entités gérées est faite selon des primitives telles que :

Get : utilisée par le gérant pour lire la valeur des attributs des objets gérés
Set : fixe la valeur d'un attribut
Event : permet à un agent de signaler un événement
Create : génère un nouvel objet
Delete : permet à l'agent de supprimer un objet

MODELES D'ADMINISTRATION SELON ISO

Modèle Informationnel

- Définit la structure des informations et leur accès.
- Définit et normalise les objets administrés : leur nom, leur fonction, leurs relations, leurs attributs ainsi que les actions qui leurs sont applicables. Ces informations sont stockées dans une base d'informations appelée MIB.

MODELES D'ADMINISTRATION SELON ISO

Modèle de Communication

- Définit le protocole devant régir la gestion du réseau ainsi que l'ensemble de ses fonctionnalités

MODELES D'ADMINISTRATION SELON ISO

Modèle fonctionnel

- Définit la façon dont les échanges permettant la gestion devront s'effectuer entre entités du réseau à gérer.
- La plateforme de gestion de l'OSI définit cinq fonctionnalités qui nécessitent une gestion beaucoup plus particulière (Voir Plus bas).

RAPPEL DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

1. Modèles d'administration selon ISO

2. Fonctionnalités de l'administration réseau

   a) Gestion des anomalies
   b) Gestion de la configuration
   c) Gestion de performance
   d) Gestion de la Sécurité
   e) Gestion de la Comptabilité

3. Architecture de l'administration réseau
4. La Télé-administration
   - Le Monitoring Réseau
   - L'infogérance

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion des anomalies

- Permet de détecter, d'isoler et de corriger les problèmes du réseau dans le but d'optimiser les ressources et les moyens mis à la disposition des utilisateurs.

- Détecte les problèmes réseaux (logiciels ou matériels). Elle essaie d'isoler le plus précisément le problème en effectuant divers tests.

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion des anomalies

- Si possible, elle règle automatiquement l'anomalie. Sinon, elle alerte les personnes concernées par le type du problème afin de solliciter leur intervention.

- La gestion des anomalies garde dans une base de données, l'ensemble des problèmes survenus ainsi que leurs solutions, de manière à être encore plus efficace face à un incident récurrent.

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion de la configuration

- Permet aux administrateurs de changer la configuration des éléments de gestion du réseau à distance

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion de la configuration : Plusieurs possibilités offertes

- La gestion de la base d'informations du réseau (MIB) : l'inventaire, la gestion des noms, le retrait ou la modification des éléments gérés, l'initialisation et la modification des paramètres ou d'états, la modification, la création ou la suppression des relations entre les éléments gérés ;

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion de la configuration : Plusieurs possibilités offertes

- La visualisation du réseau : les zooms géographiques, la visualisation des sous-réseaux, l'affichage à la demande des caractéristiques des éléments gérés

FONCTIONNALITES DE L'ADMINISTRATION SELON ISO

La Gestion de performances

- Analyse de manière continue les performances du Réseau afin de le maintenir dans un état de performance acceptable dans le but de voir si le réseau est en mesure d'écouler le trafic pour lequel il a été conçu.

FONCTIONNALITÉS DE L'ADMINISTRATION SELON ISO

La Gestion de sécurité

- Concerne le contrôle d'accès, l'authentification, l'encodage, la gestion des mots de passe et toutes les choses qui concernent directement la sécurité des informations ou de l'accès aux ressources du réseau.

FONCTIONNALITÉS DE L'ADMINISTRATION SELON ISO

La Gestion de sécurité

- La sécurité de l'administration de réseau : la gestion des droits d'accès aux postes de travail et l'autorisation d'accès aux informations d'administration ;

- La sécurité d'accès dans le réseau géré : gestion des fonctions liées aux mécanismes à mettre en œuvre et la définition des conditions d'utilisation, d'activation ou de désactivation, afin d'assumer la détection des tentatives d'accès frauduleuses ;

FONCTIONNALITÉS DE L'ADMINISTRATION SELON ISO

La Gestion de sécurité

- La sécurité de l'information : la gestion des mécanismes de protection, la gestion des clefs de cryptage et de décryptage, la détection des incidents.

FONCTIONNALITÉS DE L'ADMINISTRATION SELON ISO

La Gestion de comptabilité

Elle a pour but de mesurer l'utilisation des ressources afin de réguler les accès et d'instaurer une certaine équité entre les utilisateurs du réseau. Ainsi des quotas d'utilisation peuvent être fixés temporairement ou non sur chacune des ressources réseaux. De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur.

RAPPEL DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

1. Modèles d'administration selon ISO

1. Fonctionnalités de l'administration réseau

    a) Gestion des anomalies
    b) Gestion de la configuration
    c) Gestion de performance
    d) Gestion de la Sécurité
    e) Gestion de la Comptabilité

2. Architecture de l'administration
3. La Télé-administration
    - Le Monitoring Réseau
    - L'infogérance

La Télé-administration

L’administration à distance peut être définie comme n’importe quelle méthode de contrôle, de surveillance d’un dispositif en réseau à partir d’un endroit éloigné.

- Finalités : gain en temps, réduction des coûts énergétiques, suivi des équipements informatiques, Gestion des ressources IT à tout moment et n’importe où.

La Télé-administration

Le monitoring réseau (Supervision réseau)

Le principe de la supervision est de s'assurer du bon fonctionnement d'un système. Il peut étre appliqué sur plusieurs entités : serveurs, équipements réseaux, firewall, ...

- permet d'effectuer des actions proactives et ainsi détecter un éventuel problème avant qu'il survienne.
- La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble des équipements supervisés, et ceci en temps-réel.

La Télé-administration

Le monitoring réseau : pour quel objectif ?

" Mieux vaut prévenir que guérir "

Elle permet de visualiser à tout moment l'état des différents équipements configurés. Les objectifs sont multiples :

- Eviter les arrêts de service
- Remonter des alertes
- Détecter et prévenir les pannes

La Télé-administration

Le monitoring réseau : Quoi monitorer?

- Serveurs : CPU, mémoire, processus, espace disque, services, ...
- Matériels : Disques, cartes Raid, cartes réseau, température, alimentations, onduleurs, ...
- Réseaux : Bande passante, switchs, routeurs, Firewall, accès externes, bornes wi-fi, ...
- Protocoles : HTTP, SMTP, POP, IMAP, DNS, FTP, etc.

La Télé-administration

L’infogérance

- en anglais *facilities management* ou *outsourcing* : l'externalisation d'une partie de ses services, c'est-à-dire confier tout ou partie de la gestion du système d'information à un prestataire informatique tiers

La Télé-administration

L’infogérance : Le pour et le contre

- d'un côté elle permet à l'entreprise de se centrer sur son cœur de métier et de confier la gestion de son système informatique à une société possédant les compétences adéquates et capable de le maintenir 7 jours sur 7 24/24H (selon la convention de service)

- en contrepartie elle devient dépendante d'un tiers et se dépossède d'une part de compétences informatiques

DETAILS DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

4. Protocoles de Gestion des Réseaux
   a) CMIP/CMIS
   b) Netflow
   c) SNMP

      - Présentation de SNMP
      - Principe de fonctionnement
      - Structure d'un paquet SNMP
      - Versions de SNMP

5. Eléments de gestion d'informations

      a) Base d'Informations de Gestion (MIB)
      b) Structure de Gestion d'Informations (SMI)

Protocoles de Gestion des réseaux

Définition

Rappelons qu'un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier. Les protocoles sont hiérarchisés en couches, pour décomposer et ordonner les différentes tâches. Il existe plusieurs familles de protocoles ou modèles, chaque modèle étant une suite de protocoles entre diverses couches.

Protocoles de Gestion des réseaux

Aperçu

les organisations de standardisation internationales ont tâché de mettre en place des protocoles de gestion des réseaux telle que la gestion se fasse quelles que soient les plateformes matérielles utilisées. Ainsi, ISO a proposé la norme CMIP/CMIS, comme protocole d'administration de réseau ; en parallèle, l'IAB approuve le protocole SNMP comme solution à court terme dans l'administration et CMOT (*CMIP Over TCP*), à plus long terme. Par la suite, SNMP, devient alors standard et est adopté par des nombreux constructeurs.

Protocoles de Gestion des réseaux

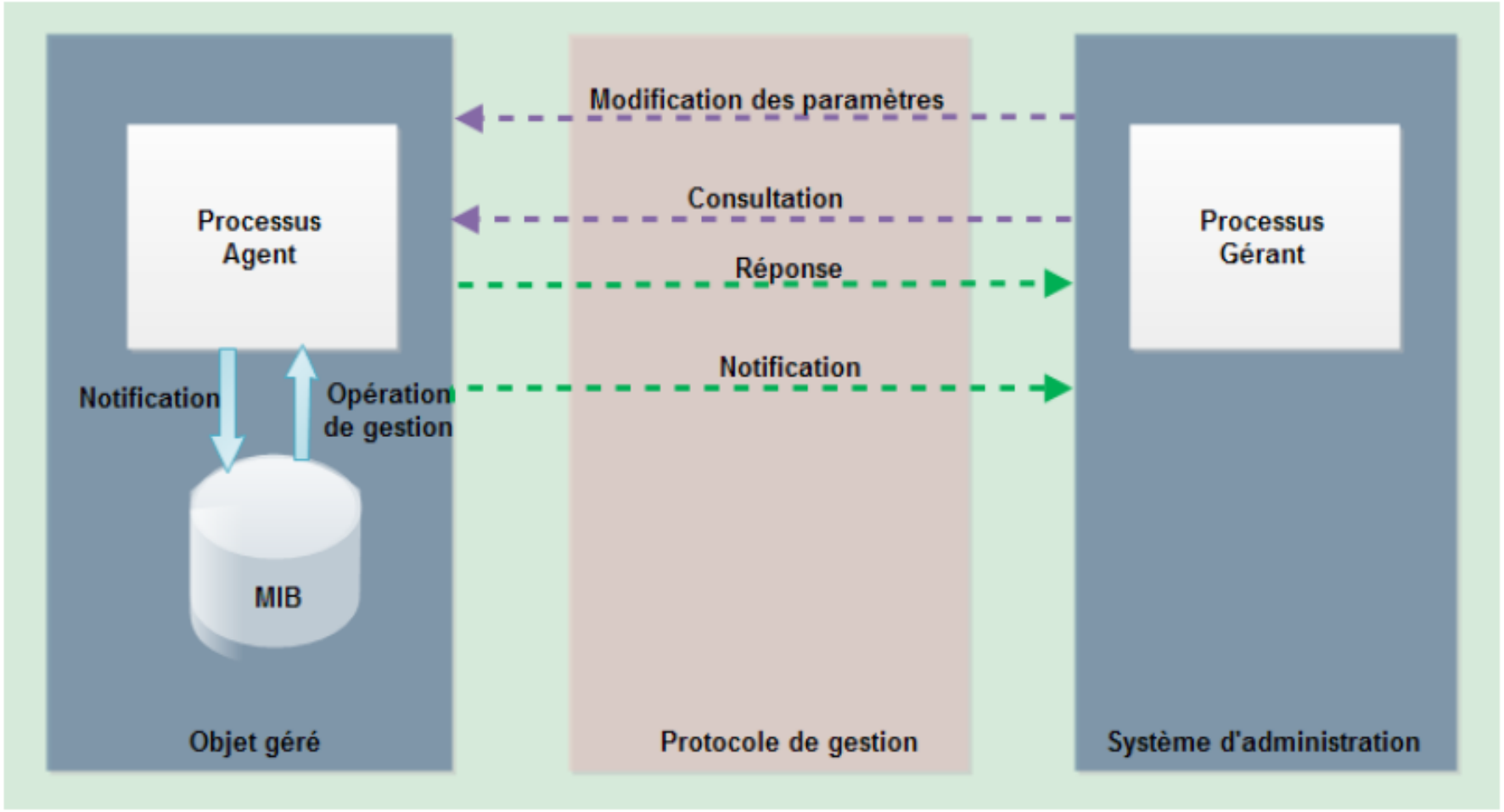
Architecture d'un système de gestion (NMS)

Sur le point de l'administration, un système de réseau informatique se compose d'un ensemble d'objets qu'un système d'administration (NMS) surveille et contrôle. Chaque objet est géré localement par un processus appelé agent qui transmet, régulièrement ou sur sollicitation, les informations de gestion relatives à son état et aux événements qui le concernent au système d'administration.

Les informations à transmettre sont hébergées dans une MIB.

Protocoles de Gestion des réseaux

Architecture d'un système de gestion (NMS)



DETAILS DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

4. Protocoles de Gestion des Réseaux
   a) CMIP/CMIS
   b) Netflow
   c) SNMP

      - Présentation de SNMP
      - Principe de fonctionnement
      - Structure d'un paquet SNMP
      - Versions de SNMP

5. Eléments de gestion d'informations

      a) Base d'Informations de Gestion (MIB)
      b) Structure de Gestion d'Informations (SMI)

Protocoles de Gestion des réseaux

CMIP/CMIS

Le rôle principal de ce protocole est de permettre l'échange entre deux stations de gestion et les différentes entités du réseau. ISO spécifie CMIP/CMIS en deux parties :

Protocoles de Gestion des réseaux

CMIP/CMIS

CMIP : protocole basé sur la norme OSI qui définit le format des messages et les procédures utilisées pour échanger les informations de gestion et d'administration de façon à administrer, exploiter, maintenir et approvisionner un réseau. Il repose sur l'utilisation des MIB contenant les informations utiles à l'administration de réseau.

Protocoles de Gestion des réseaux

CMIP/CMIS

CMIS : ensemble des services constitués des primitives décrivant comment doivent être consignés les événements survenant sur le réseau. Ces services permettent de normaliser l'ensemble des actions (échange d'informations & commandes des objets) dans un but de gestion.

DETAILS DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

4. Protocoles de Gestion des Réseaux
   a) CMIP/CMIS
   b) Netflow
   c) SNMP

      - Présentation de SNMP
      - Principe de fonctionnement
      - Structure d'un paquet SNMP
      - Versions de SNMP

5. Eléments de gestion d'informations

      a) Base d'Informations de Gestion (MIB)
      b) Structure de Gestion d'Informations (SMI)

Protocoles de Gestion des réseaux

NETFLOW

Netflow est un protocole propriétaire Cisco, qui s'appuie sur la notion de flux pour effectuer ces mesures. Ainsi, il permet de collecter des informations sur les flux IPv4 ou IPv6 traversant 1 équipement (Cisco) par les ports configurés pour recueillir les statistiques dites NetFlow.

Netflow définit un format d'exportation d'informations sur les flux réseau nommé NetFlow services export format (format d'exportation des services NetFlow, en abrégé protocole NetFlow). Il permet de superviser de façon fine les ressources du réseau utilisées.

Protocoles de Gestion des réseaux

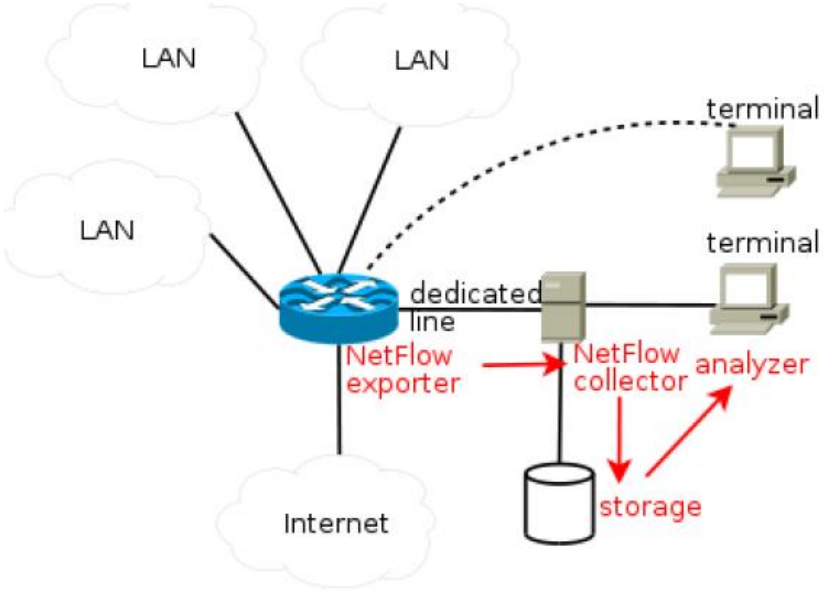
NETFLOW : Flux

Un Flux est constitué d'une adresse IP Source, une adresse IP de destination, la version du protocole IPv (4 ou 6), un port source (UDP ou TCP) et un port destination (UDP ou TCP) ; ainsi que d’un TOS (Type Of Service).

Protocoles de Gestion des réseaux

NETFLOW : Flux

Ces fluxs une fois analysé par l'équipement Cisco sont envoyés à un **Collecteur NetFlow** qui se charge de stocker les fluxs et peut se faire requêter par l'administrateur réseaux afin d'analyser le traffic passant par les interfaces de l'appareil configuré.
Traditionnellement ces analyses de Fluxs sont envoyés en UDP sur le port 2055 du NetFlow Collector



Protocoles de Gestion des réseaux

NETFLOW : Flux

NetFlow dégage les Fluxs traversant un appareil Cisco, cela permet donc dans un cas pratique de déterminer le plus gros consommateur de bande passante sur un réseau local. Ou encore le type d'application le plus utilisé. Tout cela permet à l'administrateur réseaux de mieux dimensionner le réseau ainsi que d'appliquer des règles de QoS pour prioriser certaines applications, ou encore mieux prévenir les éventuels dysfonctionnements du réseau.

Protocoles de Gestion des réseaux

NETFLOW : Cache netflow

Un routeur sur lequel Netflow est activé possède en cache une table des flux actifs : le "Cache NetFlow". Celui ci permet de compter le nombres de paquets et d'octets reçus pour chaque flux. Ansi, à chaque paquet reçu le routeur met à jour le cache soit en créant une nouvelle entrée soit en incrémentant les compteurs d'une entrée existante.

Protocoles de Gestion des réseaux

NETFLOW : Différentes versions

De nombreuses versions du protocole Netflow existent: 1, 5, 6, 7, 8, 9. La version 5 est actuellement la plus couramment utilisée, et permet d'exporter une grande quantité d'information vers un collecteur. La version 7 n'est utilisé que pour switches Catalyst et diffère peu de la version 5. La version 8 introduit les schémas d'agrégation (environ une quinzaine actuellement). Chaque version a ainsi apporté son lot de changements et demandé une modification des collecteurs. De plus, jusqu'à la version 8, le multicast, IPv6 et MPLS n'étais pas prise en charge. La version 9 quand à elle prend en charge IPv6 et le MPLS

Protocoles de Gestion des réseaux

NETFLOW :
Différentes versions

Version	Commentaire
v1	Première implémentation, à présent dépassée. Limitée à IPv4 sans masque réseau ni numéro de système autonome.
v2	Version interne à Cisco, jamais publiée.
v3	Version interne à Cisco, jamais publiée.
v4	Version interne à Cisco, jamais publiée.
v5	La version la plus courante (en 2009) sur de nombreux équipements de différentes marques, mais restreinte aux flux IPv4.
v6	Version qui n'est plus prise en charge par Cisco.
v7	Comme la version 5, avec un champ « routeur source ».
v8	Agrégation de plusieurs informations.
v9	S'appuie sur des modèles (*templates*), ce qui permet d'ajouter des champs sans redéfinir le standard. Permet de rapporter des flux IPv6, MPLS, ou le prochain saut BGP en IPv4.
v10	Connue comme IPFIX. Champs définis par les utilisateurs, champs en longueur variable.

Protocoles de Gestion des réseaux

NETFLOW : Autres protocoles basés dessus

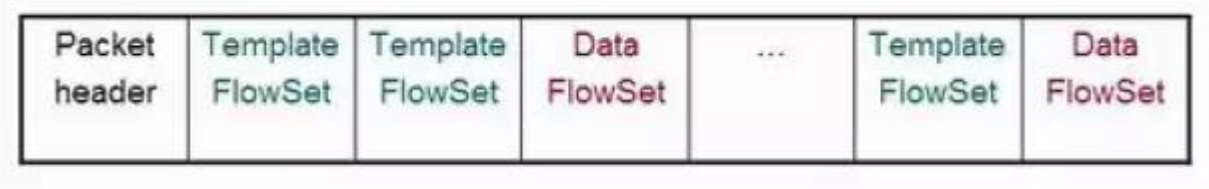
Le standard IPFIX est un concurrent à NetFlow qui est ouvert à tous et possède une norme IETF ainsi que de la RFC 3917, IPFIX se base
sur la version 9 de Netflow

NetFlow est propriétaire à Cisco et connaît donc d'autres implémentations de différents constructeurs tel que **JFlow** de Juniper ou **sFlow** qui est soutenu par un grand nombre de constructeurs

Protocoles de Gestion des réseaux

NETFLOW : Structure de trame

Une trame Netflow contient ainsi une entête et une succession de Data FlowSets et de Templates FlowSets :



Protocoles de Gestion des réseaux

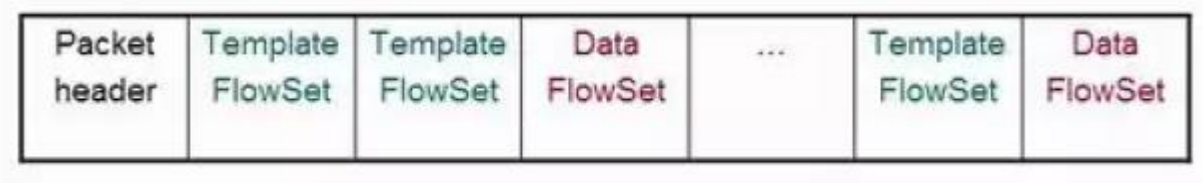
NETFLOW : Structure de trame

Une trame est donc constituée d'une suite de Flowset : les Templates Flowset représentent l'organisation des données, alors que les Data Flowset contiennent les données en elles-même. Chaque Data Flowset est ainsi associé a un Template Flowset, que le collecteur aura à recevoir au préalable.

Protocoles de Gestion des réseaux

NETFLOW : Structure de trame

L'entête contient les données suivantes :
Version : la version de Netflow
Count : Nombre de Flowset
System Uptime : Depuis combien de temps le système est démarrer
UNIX Seconds : L'heure actuelle, en notation UNIX
Sequence Number : Un numéro de séquence, incrémenter à chaque trame envoyé.
Source ID : Champs de 32 bits, utilisé pour garantir la pérennité des données.



Protocoles de Gestion des réseaux

NETFLOW : Structure de trame

Un Template représente donc une suite de champs, représenté par un type et une longueur. Chaque champ peut être n'importe quelle donnée contenue dans le cache Netflow.

Protocoles de Gestion des réseaux

NETFLOW : Collecteur Netflow

Le collecteur (NetFlowCollector) est un serveur qui récupère et stocke les données reçues des différents équipements (routeurs par ex.). Il réalise également une première phase de traitement en appliquant des règles de filtrage, afin notamment de trier puis d'agréger les données.

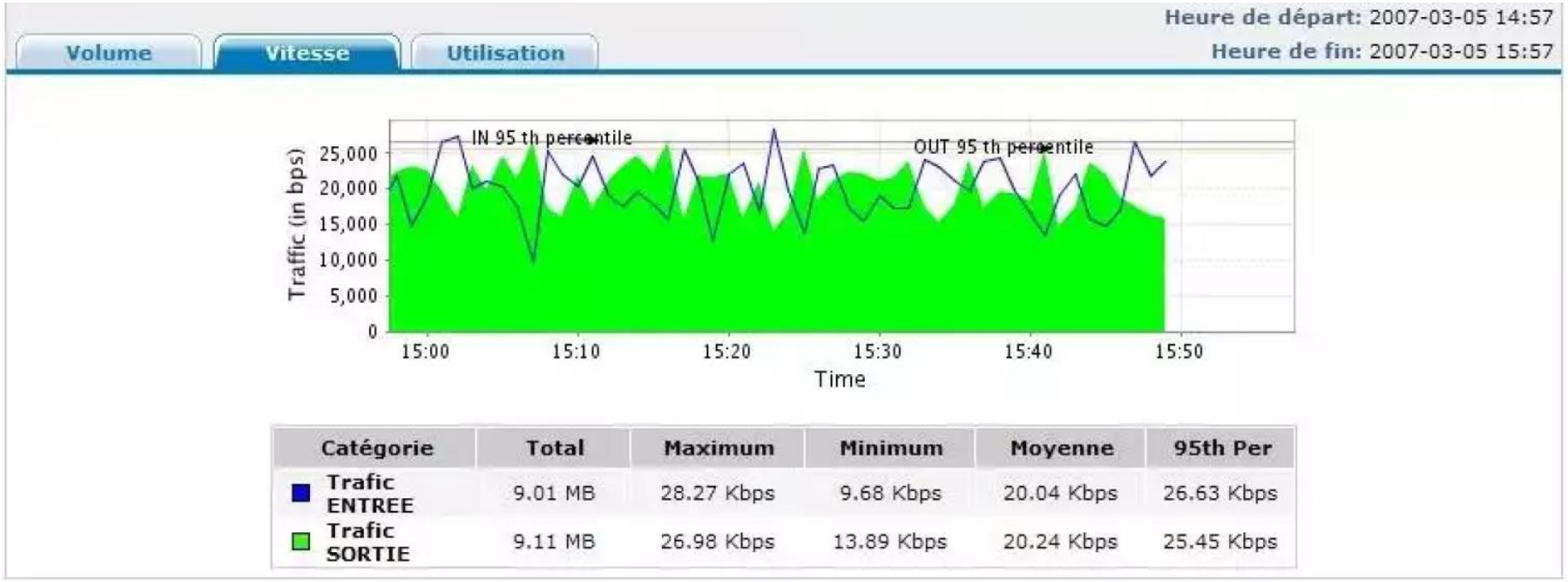
Protocoles de Gestion des réseaux

NETFLOW : Analyseur Netflow

L'analyseur produit des graphes en fonction des données stockées sur le serveur. Nous voyons donc ci dessous un rapport sur un routeur, pour une durée d'une heure. On trouve tout d'abord un aperçu du trafic global, minute par minute. Dans un deuxième temps, le trafic est décomposé par application. Enfin la troisième partie indique les adresses sources et destinations ayant généré le plus de trafic.

Protocoles de Gestion des réseaux

NETFLOW : Analyseur Netflow



Catégorie	Total	Maximum	Minimum	Moyenne	95th Per
Trafic ENTREE	9.01 MB	28.27 Kbps	9.68 Kbps	20.04 Kbps	26.63 Kbps
Trafic SORTIE	9.11 MB	26.98 Kbps	13.89 Kbps	20.24 Kbps	25.45 Kbps

Protocoles de Gestion des réseaux

NETFLOW : Analyseur Netflow

Traffic par application

Application en ENTREE [9.01 MB]		
Application	**Trafic**	**Pourcentage de trafic**
MANAGER	3.71 MB	41%
Web	3.38 MB	37%
ftp-data	45.37 KB	1%
la-maint	30.29 KB	<1%
xns-auth	26.93 KB	<1%
bootps	19.33 KB	<1%
acas	18.86 KB	<1%
xns-ch	17.38 KB	<1%
tftp	17.33 KB	<1%

Application en SORTIE [9.11 MB]		
Application	**Trafic**	**Pourcentage de trafic**
Web	3.58 MB	39%
MANAGER	3.48 MB	38%
finger	36.11 KB	<1%
gopher	26.03 KB	<1%
rje	24.11 KB	<1%
netrjs-2	23.45 KB	<1%
name	19.55 KB	<1%
mpm	19.26 KB	<1%
covia	17.94 KB	<1%

Protocoles de Gestion des réseaux

NETFLOW :
Analyseur Netflow
Traffic par consommateur

Source en ENTREE [7.54 MB]

Source	Trafic	Pourcentage de trafic
192.167.66.47	19.53 KB	<1%
192.167.17.117	17.87 KB	<1%
192.167.17.220	17.48 KB	<1%
192.167.44.92	17.03 KB	<1%
192.167.12.5	16.76 KB	<1%
192.167.46.109	16.42 KB	<1%
192.167.16.219	15.56 KB	<1%
192.167.41.165	15.2 KB	<1%
192.167.47.51	15.15 KB	<1%
192.167.66.251	15.02 KB	<1%
Autres	7.37 MB	98%

Source en SORTIE [7.55 MB]

Source	Trafic	Pourcentage de trafic
192.167.29.61	16.68 KB	<1%
192.167.21.235	16.39 KB	<1%
192.167.40.189	16.25 KB	<1%
192.167.106.81	15.53 KB	<1%
192.167.55.158	15.27 KB	<1%
192.167.88.1	14.95 KB	<1%
192.167.63.173	14.32 KB	<1%
192.167.48.178	14.31 KB	<1%
192.167.55.71	14.17 KB	<1%
192.167.87.239	14.16 KB	<1%
Autres	7.4 MB	98%

Destination en ENTREE [7.54 MB]

Destination	Trafic	Pourcentage de trafic
192.167.110.218	17.79 KB	<1%
192.167.17.208	17.74 KB	<1%
192.167.85.207	17.67 KB	<1%
192.167.67.76	16.87 KB	<1%
192.167.25.49	16.69 KB	<1%
192.167.70.124	16.56 KB	<1%
192.167.109.157	16.2 KB	<1%
192.167.72.45	15.35 KB	<1%
192.167.80.216	14.81 KB	<1%
192.167.25.228	14.69 KB	<1%
Autres	7.37 MB	98%

Destination en SORTIE [7.55 MB]

Destination	Trafic	Pourcentage de trafic
192.167.98.249	18.07 KB	<1%
192.167.44.227	18.06 KB	<1%
192.167.86.226	17.23 KB	<1%
192.167.117.209	16.92 KB	<1%
192.167.16.240	16.07 KB	<1%
192.167.21.232	15.97 KB	<1%
192.167.60.221	15.62 KB	<1%
192.167.36.177	15.14 KB	<1%
192.167.108.198	14.91 KB	<1%
192.167.91.193	14.74 KB	<1%
Autres	7.39 MB	98%

Protocoles de Gestion des réseaux

NETFLOW : Conclusion

NetFlow est un protocole permettant de récupérer de nombreuses données sur le réseau et donne ainsi la possibilité de configurer plus finement le réseau et d’y détecter des dysfonctionnements anormal. Tout cela se fait en partie via le stockage des données NetFlow afin d'avoir une chronologie des différents fluxs intervenant sur le réseau. L'accumulation de ces données permet de fixer des "baselines" du réseau qui vont représenter les flux "classiques" en temps normal. NetFlow est donc une solution permettant de compléter une solution de monitoring réseau déjà mise en place auparavant.

DETAILS DU PLAN

CHAP. II. ISO ET L'ADMINISTRATION RESEAU

4. Protocoles de Gestion des Réseaux
   a) CMIP/CMIS
   b) Netflow
   c) SNMP

      - Présentation de SNMP
      - Principe de fonctionnement
      - Structure d'un paquet SNMP
      - Versions de SNMP

5. Eléments de gestion d'informations

      a) Base d'Informations de Gestion (MIB)
      b) Structure de Gestion d'Informations (SMI)

Protocoles de Gestion des réseaux

SNMP

Pour répondre aux exigences liées à la conception d'une plateforme de gestion de réseau efficace pour des réseaux TCP/IP hétérogènes, la norme SNMP a été définie et approuvée par l'IAB de l'IETF comme une norme Internet.

Il est utilisé par les agents et les stations de gestion pour communiquer.

C'est un protocole de type question/réponse asynchrone

Protocoles de Gestion des réseaux

SNMP

Ce protocole est situé au niveau application du modèle OSI et utilise les ports UDP 161 (pour l'émission des requêtes) et UDP 162 (pour l'écoute les réponses) pour la communication entre les agents et les NMS, c'est lui qui définit la structure formelle des communications. Il est encapsulé dans des trames UDP

Protocoles de Gestion des réseaux

SNMP : Historique

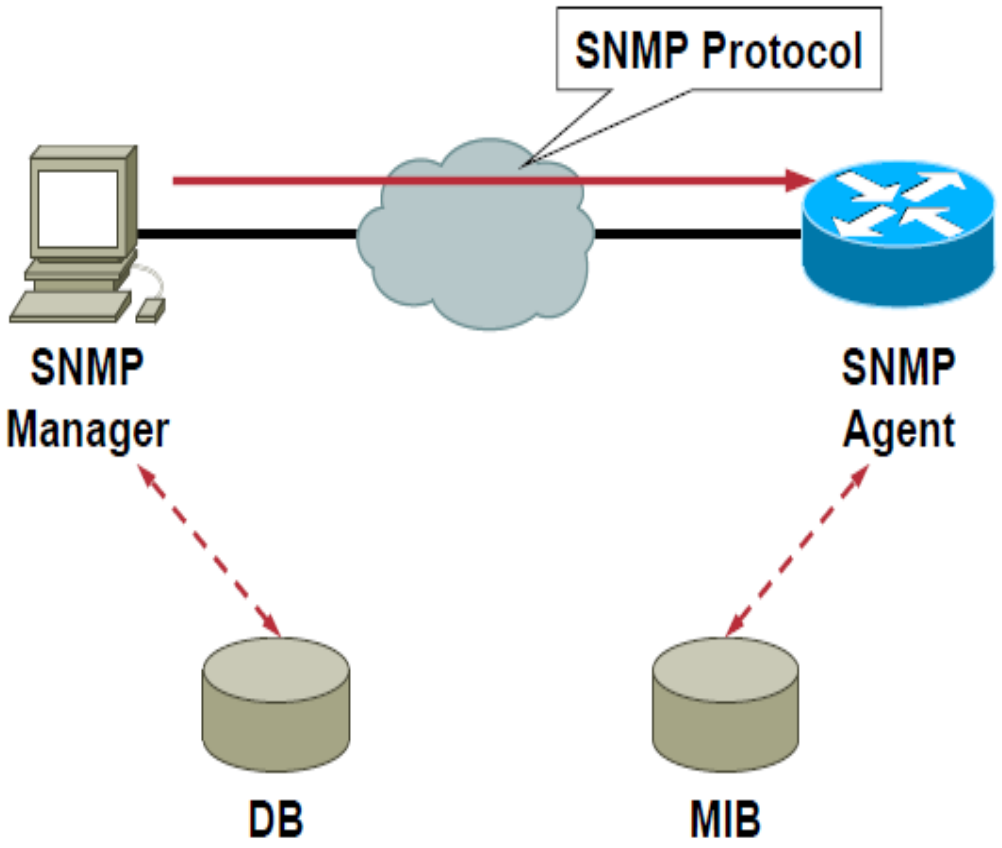
- La 1ère version de SNMP, SNMPv1 : conçue à la fin des années 80 et standardisée au cours de l'année 1990. caractérisée par un certain nombre de lacunes : manque de hiérarchie, peu de codes d'erreur et de notifications, faibles performances, sécurité laxiste, etc.
- SNMPv2, (conception débutée en 1993). Toutefois, plusieurs éditeurs ont rejeté les standards proposés, conduisant à la création d'autres normes dont la plus utilisée est SNMPv2c.
- En 1999, SNMPv3 a été mis en place afin de remédier à plusieurs défaillances des versions précédentes dont la principale est la Sécurité.

Protocoles de Gestion des réseaux

SNMP : Principe de Fonctionnement

2 éléments clés

- Manager
  - ❑ Base de données
- Agent
  - ❑ MIB



Protocoles de Gestion des réseaux

Agent

Il reste à l'écoute (sur le port UDP 161) du manager des éventuelles requêtes.

S'il reçoit une requête, il y répond, s'il y est autorisé ; ceci explique le fait que nous ayons dit que SNMP est de type Question/Réponse asynchrone.
Il est considéré comme un serveur dès par sa fonction de rendre des services (alertes, état,…) au manager.

Protocoles de Gestion des réseaux

Agent

Ils peuvent se retrouver sur des ordinateurs mais aussi sur des routeurs, des ponts, des switches, des imprimantes et sur tant d’autres équipements.

Protocoles de Gestion des réseaux

Manager

la station d'administration dispose d'un outil dit "manager" qui interroge périodiquement les agents pour observer leur fonctionnement. C'est avant tout un client, dans la mesure où c'est lui qui envoie les requêtes aux divers agents SNMP du réseau. Il devra aussi disposer d'une fonction serveur car il doit rester à l'écoute, sur le port UDP 162, des alertes que les divers équipements sont susceptibles d'émettre à tout moment.

Protocoles de Gestion des réseaux

Manager

Les divers états des services et/ou des équipements du réseau reçus peuvent ensuite être interprétés et supervisés sur un écran ou envoyés dans la boîte de messagerie de l'administrateur ou mieux encore sur son téléphone portable, ce qui lui permet d'en effectuer un suivi de près afin de lui permettre la prise de décision en cas de nécessité.

Protocoles de Gestion des réseaux

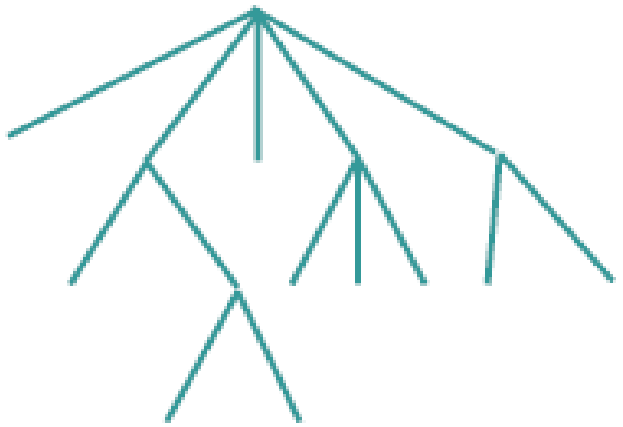
MIB (Management Information base)

- C’est la base des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.
- C’est un document texte écrit en langage ASN.1 (Abstract Syntax Notation 1) qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB.

Protocoles de Gestion des réseaux

MIB (Management Information base)

Elle est une structure arborescente dont chaque nœud est défini par un nombre appelé OID (Object Identifier) dont les premiers niveaux (top level) sont contrôlés par l'IANA.

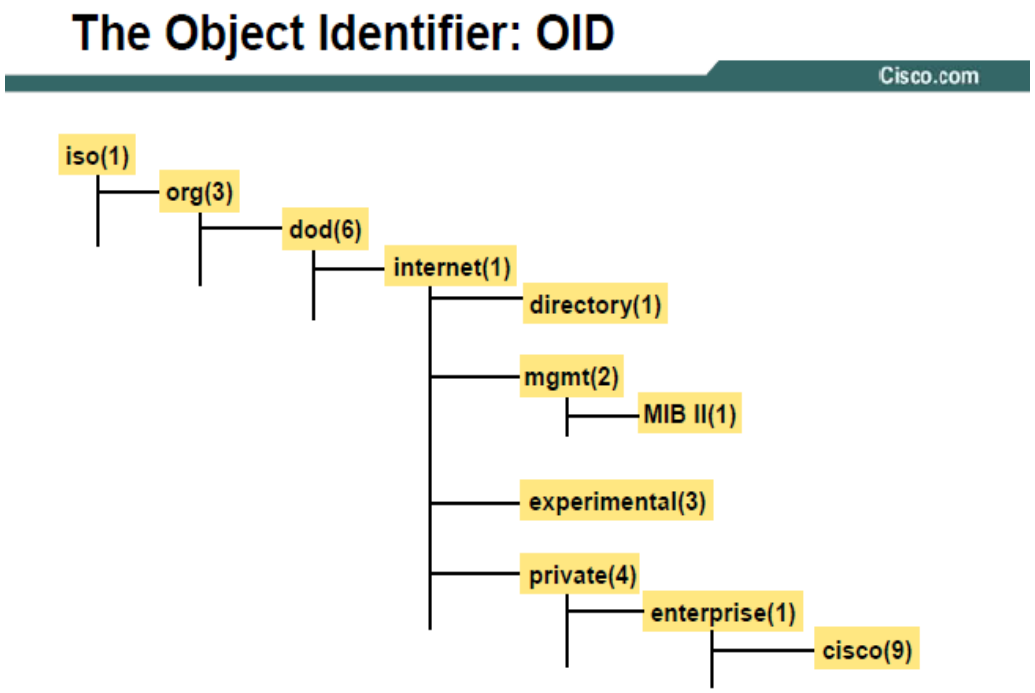


Protocoles de Gestion des réseaux

MIB (Management Information base)

Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. Non seulement la structure est normalisée, mais également les appellations des diverses rubriques.

Protocoles de Gestion des réseaux



MIB (Management Information base)

Ces appellations ne sont présentes que dans un souci de lisibilité. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique et SNMP n'utilise que celui-ci pour y accéder.

Protocoles de Gestion des réseaux

MIB Privées

La plupart des constructeurs ont défini pour leurs équipements des arborescences de MIB spécifiques, ainsi l'outil devant être choisi pour la gestion de ces équipements devra prendre en charge leurs MIB privées. Notons que les constructeurs le font afin de définir des MIB qui collent au plus près des fonctionnalités de leurs équipements.

Protocoles de Gestion des réseaux

SNMP : Types d'opération

Deux situations sont possibles pour les échanges de données. Soit le système d'administration demande une information à un agent et obtient une réponse, soit l'agent envoie de lui-même une alarme (**trap**) à l'administrateur lorsqu'un événement particulier arrive sur le réseau.

Protocoles de Gestion des réseaux

SNMP : Types d'opération

4 types de requêtes (PDU)

- GetRequest : permet d'obtenir une variable.
- GetNextRequest : permet d'obtenir la variable suivante (si existante, sinon retour d'erreur).
- GetBulk : " permet la recherche d'un ensemble de variables regroupées. " NMS (Nouveau dans SNMPv2)
- SetRequest : permet de modifier la valeur d'une variable.

Protocoles de Gestion des réseaux

SNMP : Types d'opération

3 types de réponses

- GetResponse : permet à l'agent de retourner la réponse au NMS.
- NoSuchObject : informe le NMS que la variable n'est pas disponible.
- InformRequest : permet de renvoyer un événement survenu sur l'agent (trap). C'est un événement qui s'enclenche sans aucune demande la part du NMS (Nouveau dans SNMPv2)

Protocoles de Gestion des réseaux

SNMP : Format de paquet

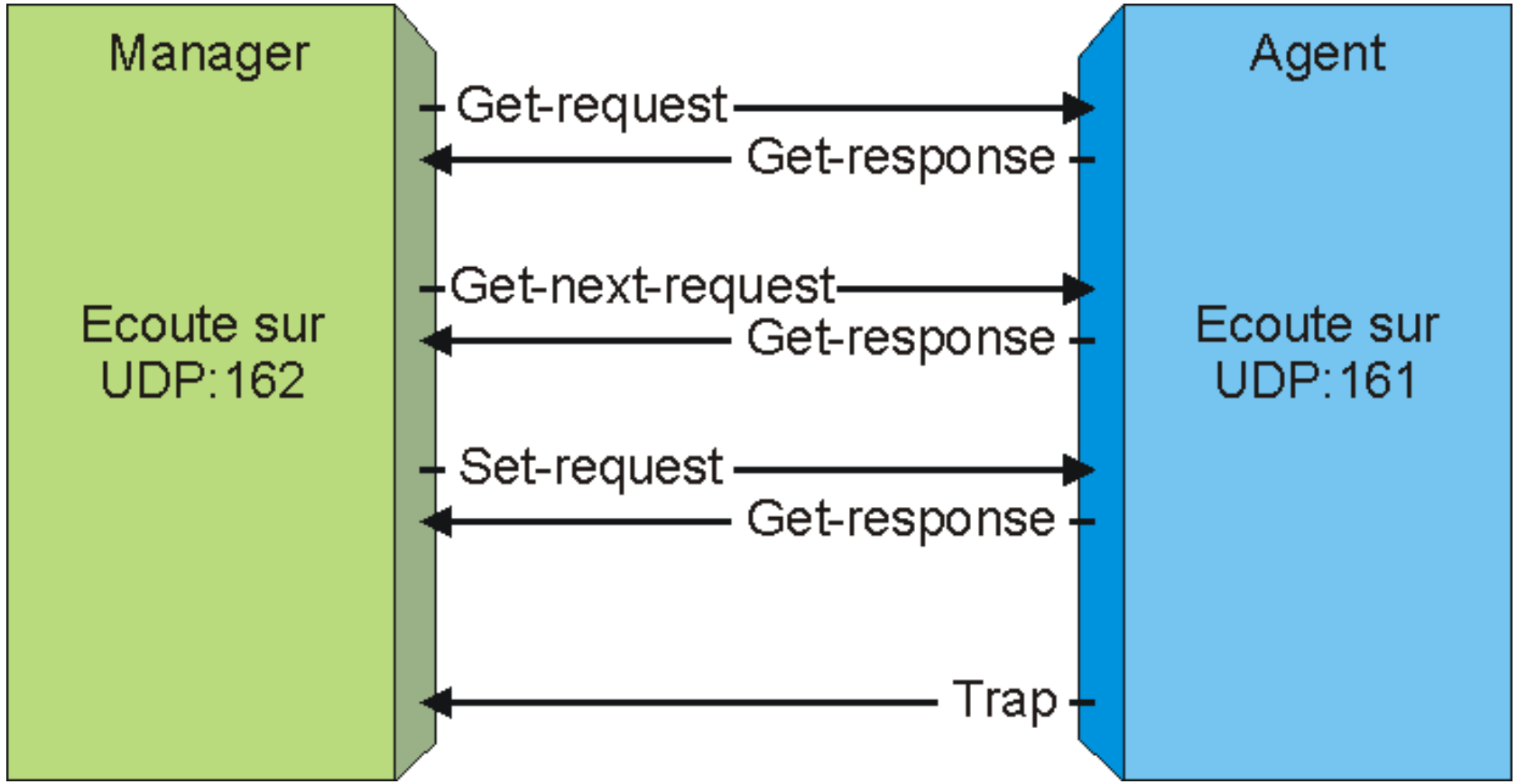
VERSION	COMMUNITY	PDU SNMP

Identifiants de PDU

Type de PDU (Protocol Data Units)	Nom
0	GetRequest
1	GetNextRequest
2	SetRequest
3	GetResponse
4	Trap

Protocoles de Gestion des réseaux

SNMP : Communication entre NMS et Agent



FIN DU CHAPITRE