# L'ADMINISTRATION DES RESEAUX

**Les objectifs de l'administration des réseaux pour l'administrateur sont :**

- Supervision du fonctionnement des réseaux.
- Optimisation pour l'utilisation des ressources.
- Détection et prévision des erreurs.
- Signalisation des pannes.
- Calculs statistiques.
- Calculs de facturations à l'utilisation des ressources.
- Le support technique pour utilisateurs (help desk).

**Il existe deux approches qui sont :**

- OSI : **CMIP/CMIS**
- TCP/IP : **SNMP**

## L’administration selon OSI

couvrir tous les domaines de l’administration complexe

**Les activités d’administration sont :**

- De la maintenance (préventive ou curative).
- De l’exploitation.
- De la supervision.
- De la planification.
- De la sécurité.

**De plus, OSI a définit 5 modèles qui sont :**

- Le modèle informationnel : quoi gérer ? Quels objets ?
- Le modèle organisationnel : qui ?
- Le modèle fonctionnel : pourquoi gérer ? Quels domaines gérer ?
- Le modèle de communication : comment gérer ?
- Le modèle architectural : comment gérer ?

## Le modèle d'administration du monde TCP/IP : SNMP

« Simple Network Management Protocol » :
relation agent / gestionnaire de type **client/serveur**.

**Chaque équipement administré est vu comme un agent**
Sur chaque équipement administré est implanté un agent (programme)

L'agent contrôle et fournit **une représentation au travers d'un ensemble de variables**

**MIB (Management Information Base).**

**La station d'administration** contrôle au travers de cette base.

## CMIP / CMIS

**Common Management Information Service**

- M-CREATE — Un gérant crée une info chez un agent
- M-DELETE — Un gérant détruit une info chez un agent
- M-EVENT-REPORT — Un agent signale un changement à un gérant
- M-GET — Un gérant lit la valeur d'une info chez un agent
- M-SET — Un gérant écrit la valeur d'une info chez un agent
- M-ACTION — Un gérant demande une action plus complète
- M-INITIALIZE — Commence une association
- M-TERMINATE — Termine une association normalement
- M-ABORT — Termine une association brutalement
- M-CANCEL-GET — Ne veut pas recevoir le résultat du get
- …

## Common Management Information Protocol

SMAS (System Management Application System)
ACSE (Association Control Service Element)
ROSE (Remote Operation Service Element)

Protocole de niveau 7 : échange entre ASE ( Application Service Element)

MIB (Management Information Base)

## SNMP

standard du monde TCP/IP
incompatible avec OSI CMIP
le plus répandu

permet :

- De contrôler un réseau à distance en interrogeant les stations sur leurs états
- De modifier leurs configurations
- De faire des tests de sécurité et / ou de métrologie.
- Il peut même être utilisé pour gérer des logiciels.

## Composantes pour l'utilisation

1. **Une station de gestion NMS (*Network Management Station*)**

processeur relativement rapide

beaucoup de mémoire

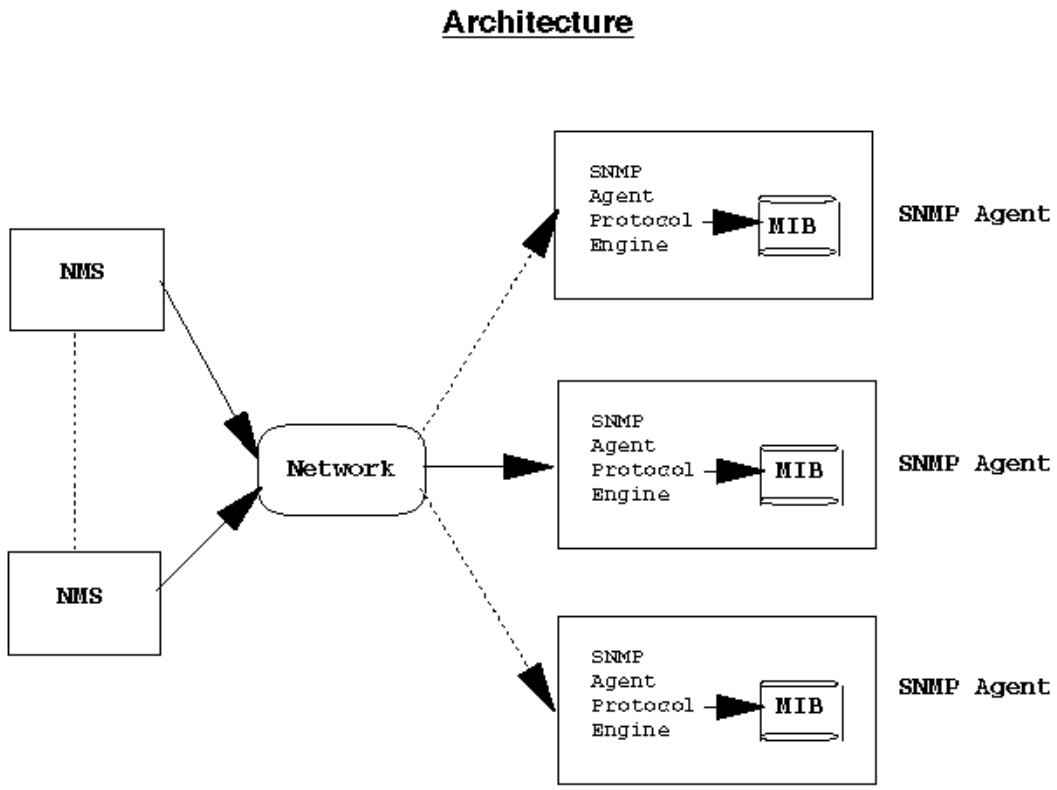
espace disque

2. **Des éléments de réseaux avec des agents**
3. **Les tables MIB**

transmissions de données

composantes de la station ou du routeur

# Architecture

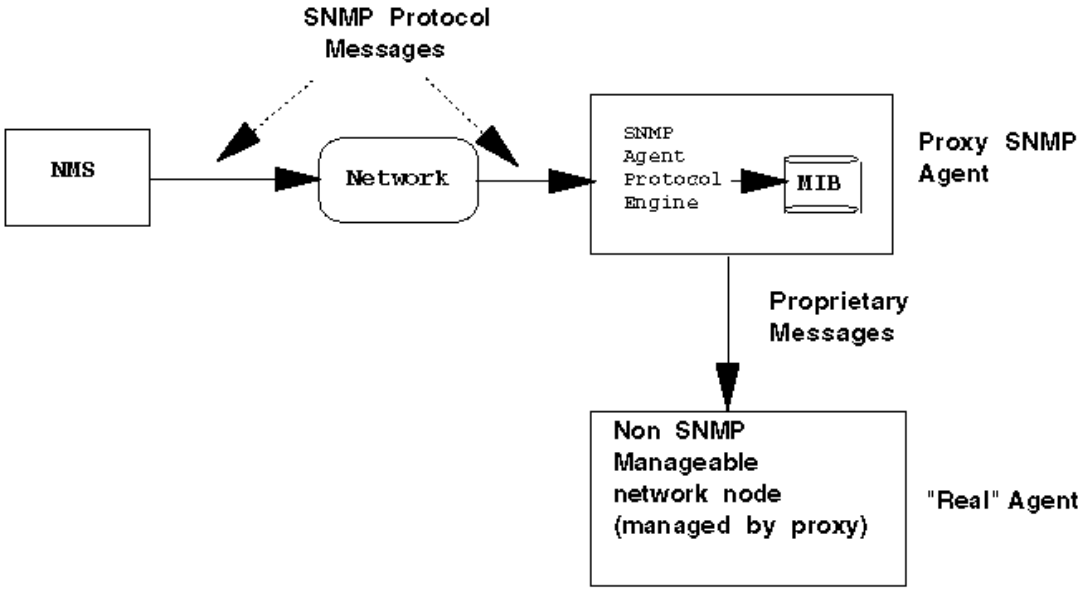


## Architecture Proxy

Le service de proxy

- c'est un agent SNMP qui agit pour d'autres périphériques (qui ne supportent pas par exemple TCP/IP)
- Le proxy connaît les objets MIB utilisés pour gérer le système mandaté (la vue de la MIB et les droits d'accès)

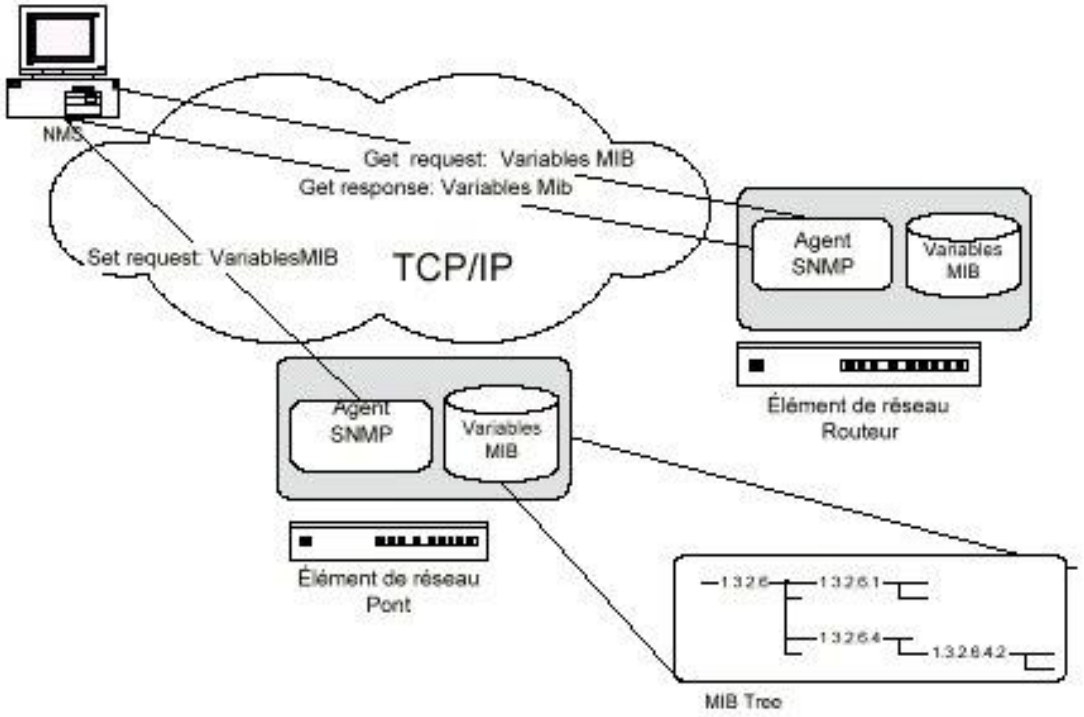
## Proxy Management of Agent




MIB in Proxy Agent reflects the current management information on the "real" agent, and not the proxy

## Fonctionnement

**des requêtes, des réponses et des alertes !**



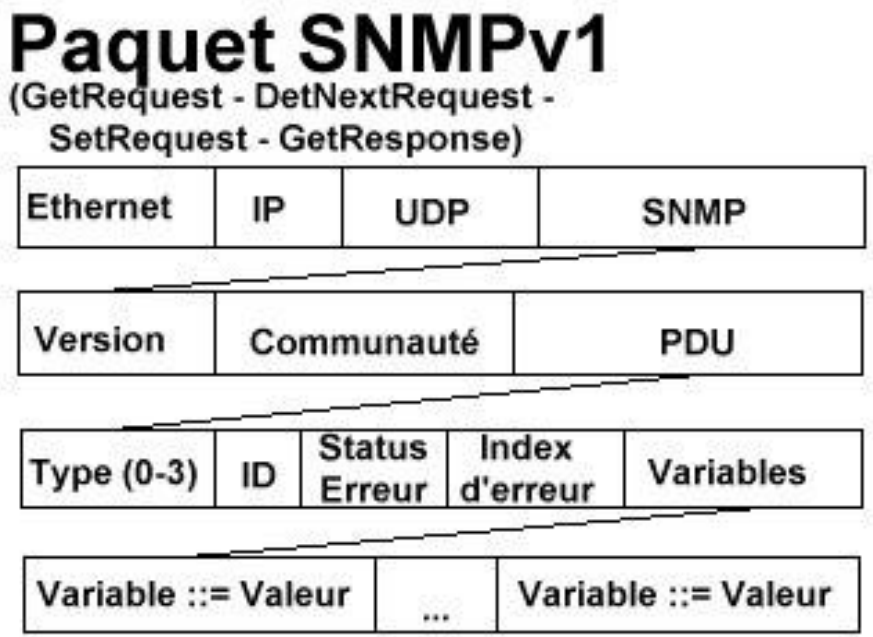
**Il existe 6 sortes de requêtes :**

- GET-REQUEST lecture d'un paramètre
- GET-NEXT-REQUEST lecture du paramètre suivant
- SET-REQUEST modification de la valeur d'un paramètre
- GET-RESPONSE par l'agent pour répondre à une requête

- TRAP par l'agent pour émettre une alerte

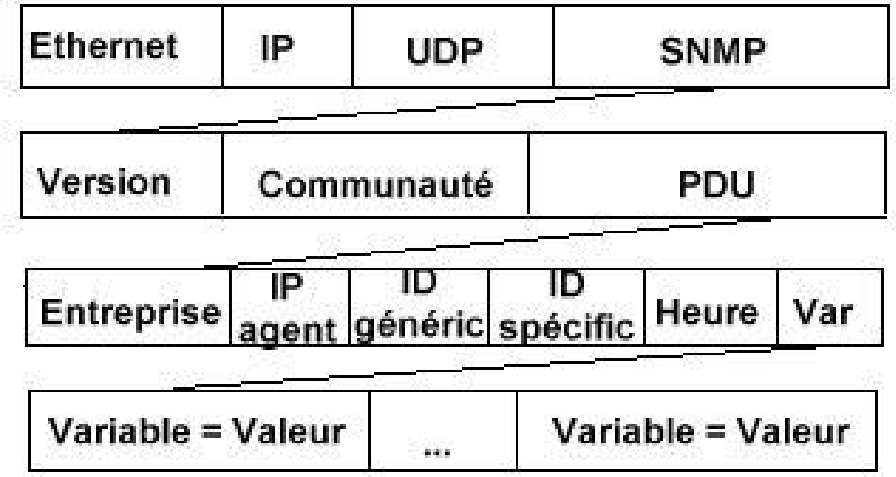
- NoSuchObject variable non pas disponible.

## Le paquet SNMPv1




La seule notion de sécurité réside dans le champ ‘community’ qui permet d’identifier l’émetteur à l’aide d’un mot de passe qui circule en clair sur le réseau.

# Paquet SNMPv1
(Trap)




- UDP est utilisé ici comme protocole transport, mais SNMP peut aussi être implanté sur TCP, X.25, la couche Ethernet directement, etc.
- L'agent écoute au port 161 et envoie ses réponses au port 162.
- Il peut y avoir plusieurs PDU (requêtes) dans un message

## Versions 2 de SNMP

Il prend en compte les limites de SNMP suivantes :

- **L'absence de sécurité.**
- La gestion des erreurs.
- Le transfert de données importantes.
- La communication inter manager.

Il est constitué d'un jeu de sept primitives qui sont les suivantes :

- GetRequest.
- GetNextRequest.
- SetRequest.
- Response.
- SNMPv2-trap.
- GetBulkRequest : transfert en une fois d'une importante quantité de données.
- InformRequest : communication entre gestionnaires.

Il existe trois niveaux de sécurité qui sont :

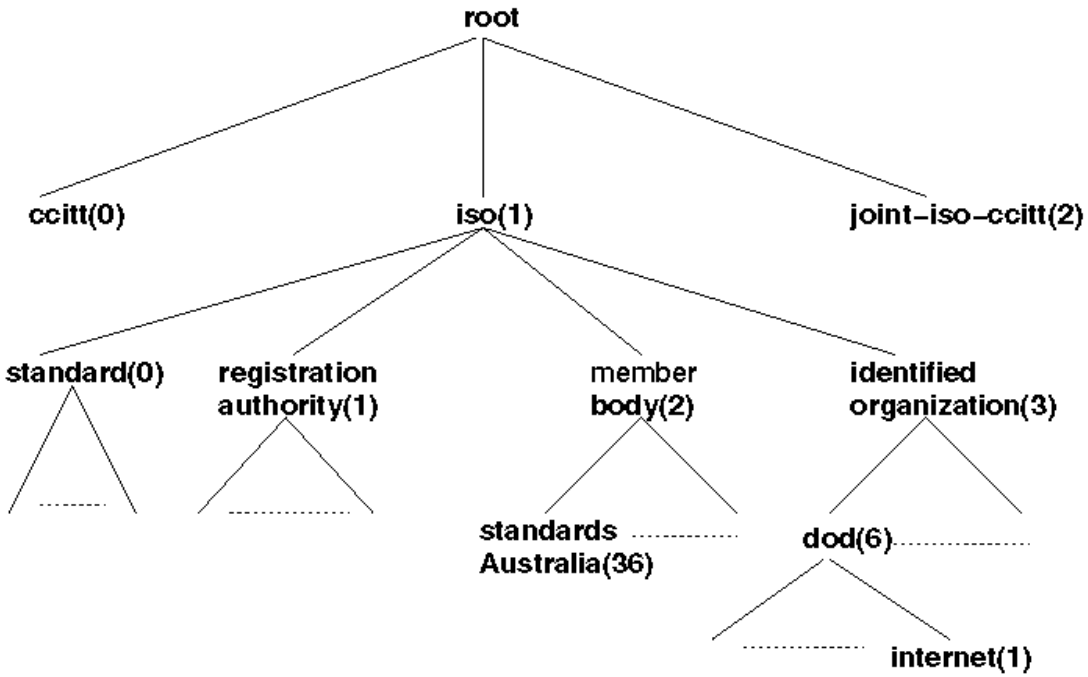
- Aucun.
- Avec authentification.
- Avec cryptage.

plus complexe que la version 1
un niveau hiérarchique d'administration : petits NMS dans le réseau
sécurité
gamme de messages d'erreurs plus vaste
les MIB II, plus d'éléments.

Cette version n'a cependant pas remplacé la version 1 du protocole, puisqu'il ne s'agît toujours pas d'un standard complet (*Full Standard* ), mais d'une ébauche (*Draft Standard*).

## Les Tables MIB (Management information base)

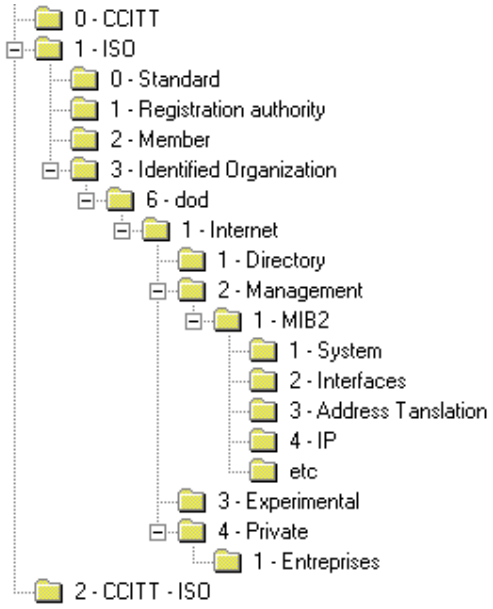
| Nom du groupe | Description |
|---|---|
| System | Description de toutes les entités gérées. |
| Interface | Interface de données dynamiques ou statiques. |
| Address Translation | Table d'adresses IP pour les correspondances d'adresses MAC |
| IP | Statistiques du protocole IP, adresse cache et table 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 |




**SMI (Structure of Management Information) :**

recherche nom de variable ou arbre de classification

# variable *System* : **OID (Object IDentification) 1.3.6.1.2.1.1**



## La Station d'administration (NMS) : Supervision

L'administration du réseau met en oeuvre un ensemble de moyens pour :

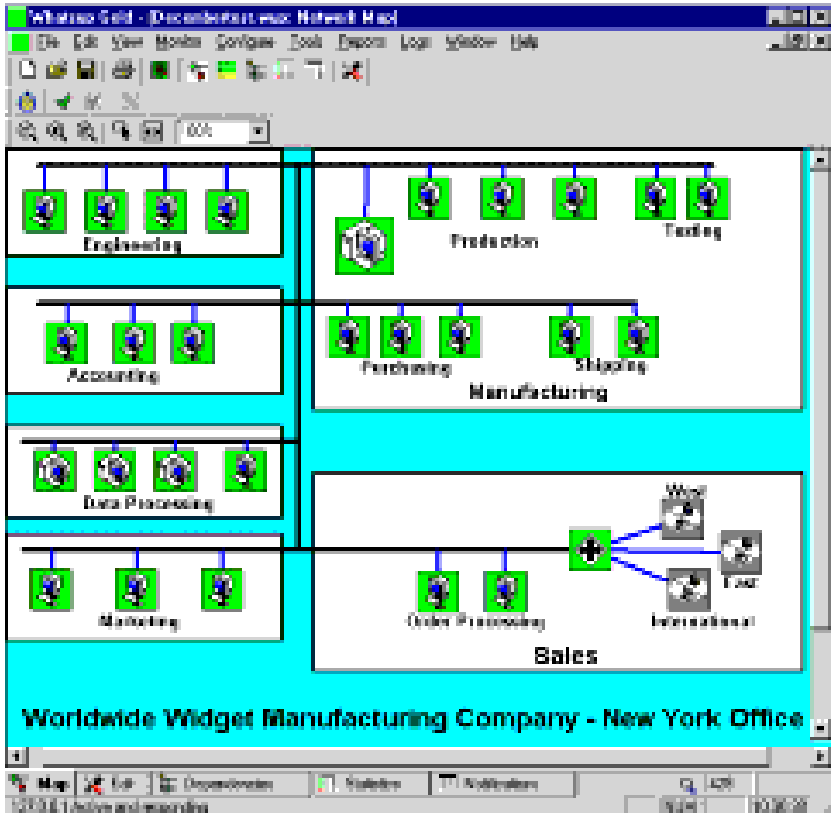
- offrir aux utilisateurs un service de qualité,
- permettre l'évolution du système en incluant des nouvelles fonctionnalités
- optimiser les performances des services pour les utilisateurs
- permettre une utilisation maximale des ressources pour un coût minimal.

La station d'administration doit permettre :

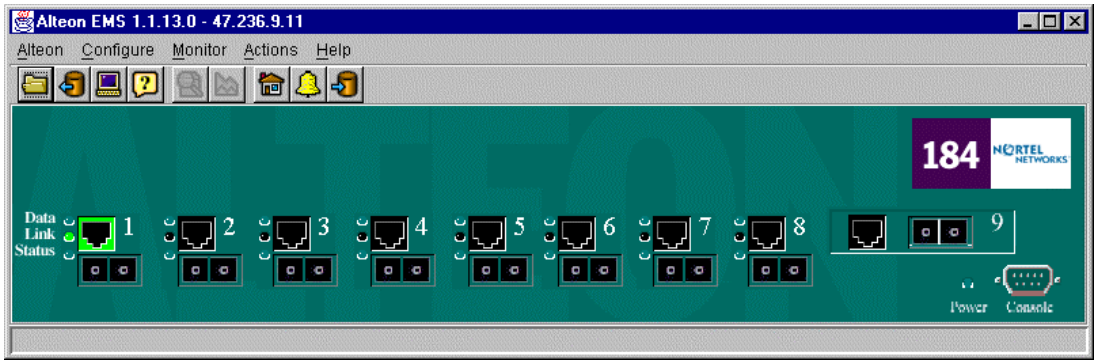
- l'extraction des informations des éléments du réseau au moyen d'outils d'un grand nombre d'informations.
- la réduction du volume d'informations au moyen de filtres afin de sélectionner les informations significatives.
- le stockage des informations retenues dans une base de données d'administration
- des traitements sur ces informations
- offrir des interfaces (utilisateur d'administration administration, opérateur réseau).

# Fonctionnalités d'une station d'administration

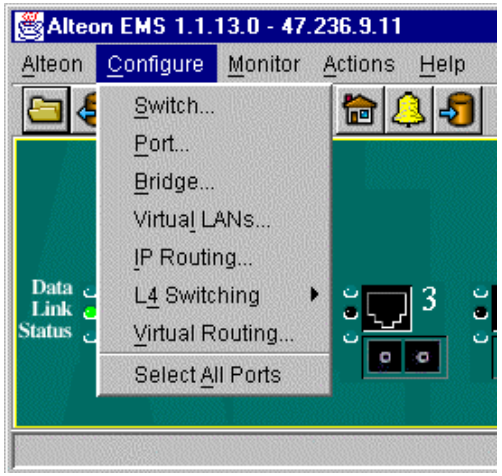
## Cartographie (Mapping)

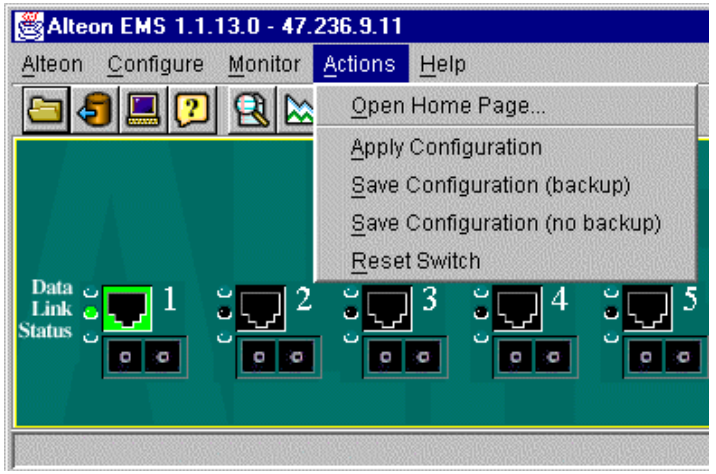


# Contrôle des équipements par EMS (Element Management System)

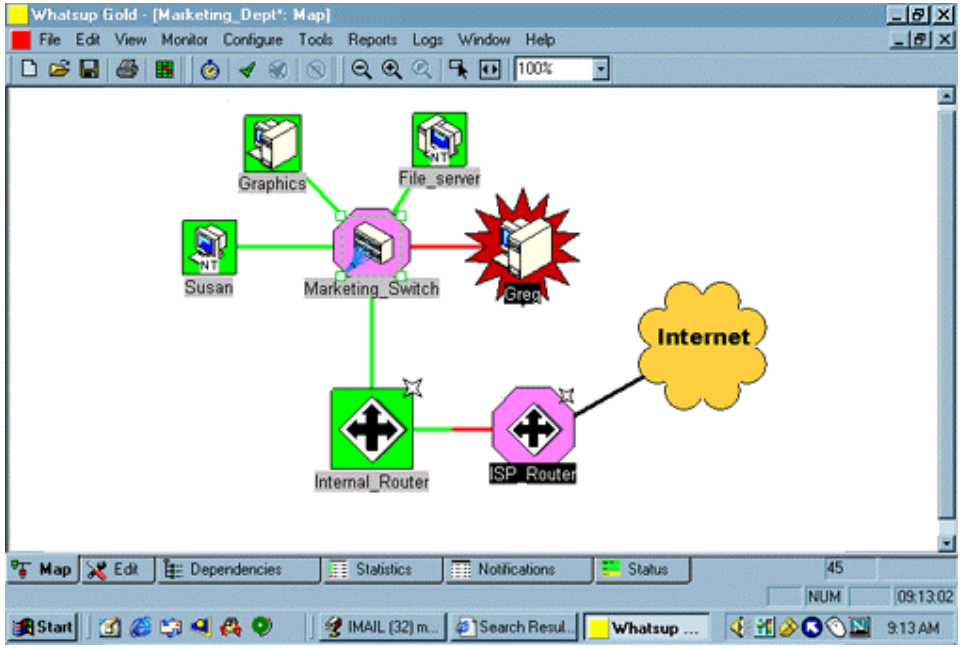




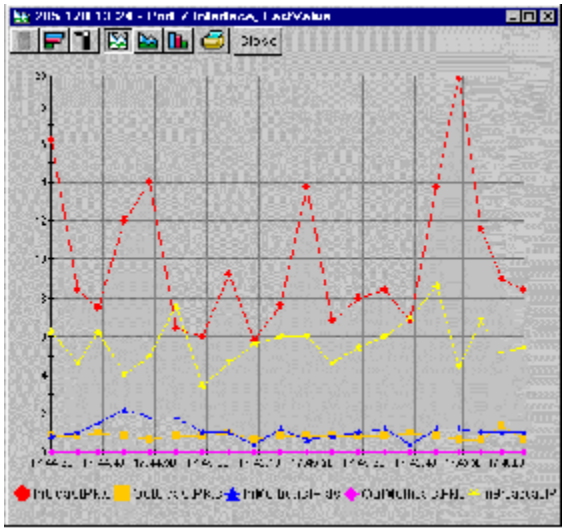



# Monitoring et pooling



# Diagnostic

## Visualiseur SNMP

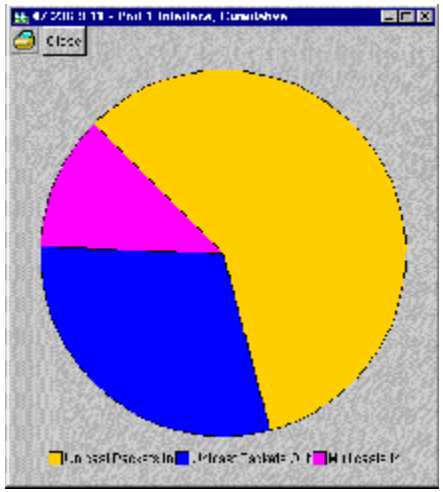


47.236.9.11 - Switch

IP | ICMP In | ICMP Out | RIP | SNMP | MP CPU Stats | WebOS Stats | Stats

| | AbsoluteValue | Cumulative | Average | Minimum | Maximum | LastValue |
|---|---|---|---|---|---|---|
| Good Packets In | 599,787 | 90 | 3.75 | 1 | 10 | 10 |
| Header Error Packets In | 0 | 0 | 0 | 0 | 0 | 0 |
| Address Errors In | 228,164 | 20 | 0.833 | 0 | 2 | 2 |
| Packets Routed | 0 | 0 | 0 | 0 | 0 | 0 |
| Packets In with Unknown Protocol | 0 | 0 | 0 | 0 | 0 | 0 |
| Inbound Dropped Packets | 0 | 0 | 0 | 0 | 0 | 0 |
| Packets Consumed | 247,949 | 57 | 2.375 | 1 | 7 | 7 |
| Packets Out | 162,115 | 51 | 2.125 | 1 | 4 | 4 |
| Outbound Dropped Packets | 18 | 0 | 0 | 0 | 0 | 0 |
| Non-Routable Dropped Packets | 18 | 0 | 0 | 0 | 0 | 0 |
| Successful Packet Fragmentation | 0 | 0 | 0 | 0 | 0 | 0 |
| Failed Packet Fragmentation | 0 | 0 | 0 | 0 | 0 | 0 |
| Fragments Created | 0 | 0 | 0 | 0 | 0 | 0 |
| IP Fragments Reassembled | 0 | 0 | 0 | 0 | 0 | 0 |
| Packet Reassembly Successes | 0 | 0 | 0 | 0 | 0 | 0 |
| Packet Reassembly Failures | 0 | 0 | 0 | 0 | 0 | 0 |
| Routing Discards | 0 | 0 | 0 | 0 | 0 | 0 |

Clear | Close | Poll Interval: 1s



# La métrologie

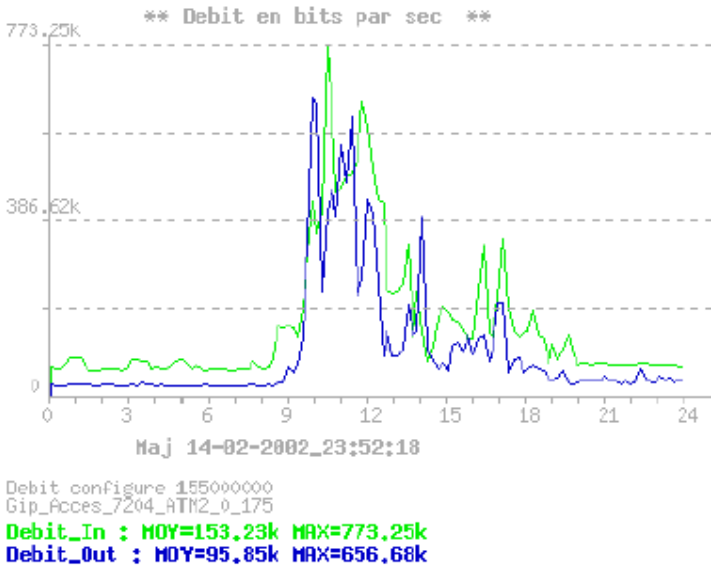
## But de la métrologie

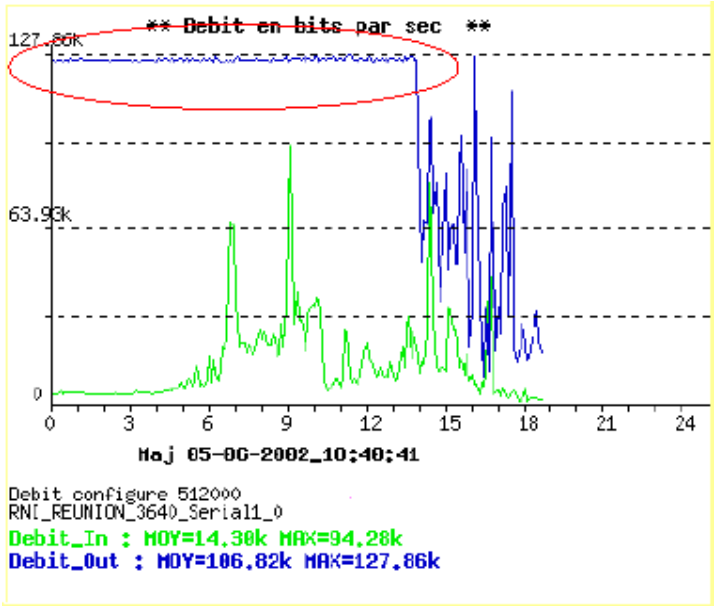
- Optimiser l'architecture et le dimensionnement du réseau dans le futur
- Permettre la modélisation
- Renforcer la sécurité sur le réseau en détectant mieux les incidents ou attaques et en quantifiant leurs conséquences
- Gérer la qualité de service à long terme
- Permettre une bonne corrélation entre les sources de financement et les usages qui sont faits du réseau

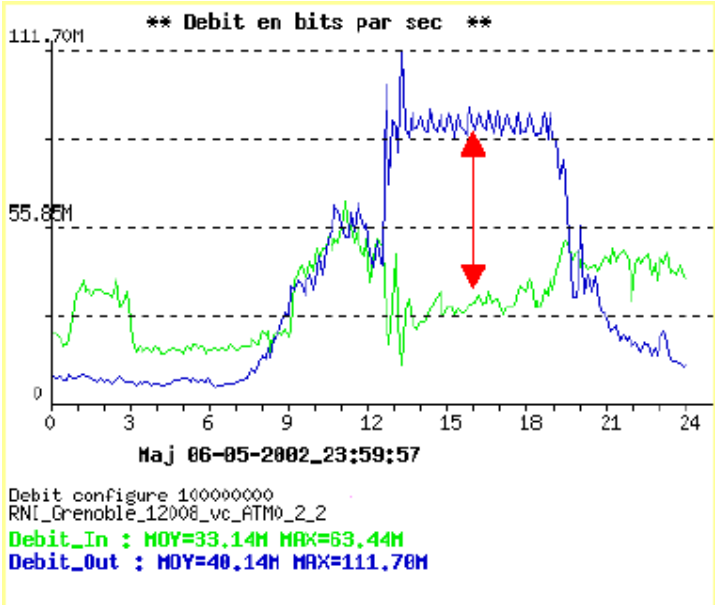
## Source d'approvisionnement

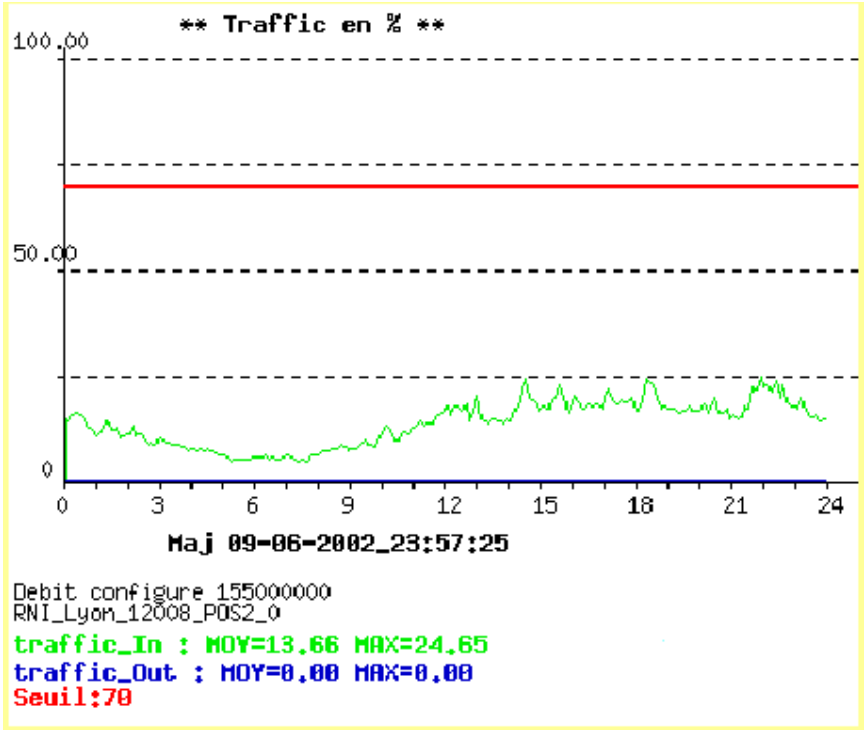
La métrologie peut utiliser plusieurs sources d'approvisionnement soit directement SNMP (mais on fait double emploi avec la supervision), soit les bases de données de la NMC, soit d'autres protocoles spécifiques comme NetFlow de Cisco.

# Exemple d'outil de métrologies : Mrtg



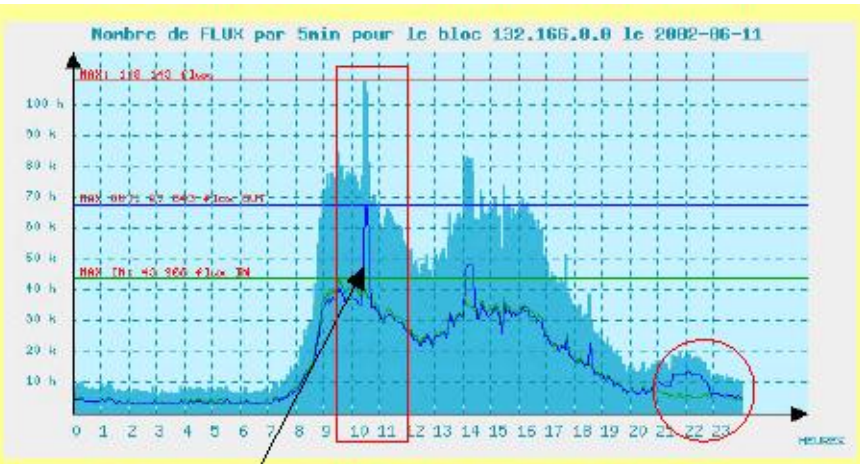


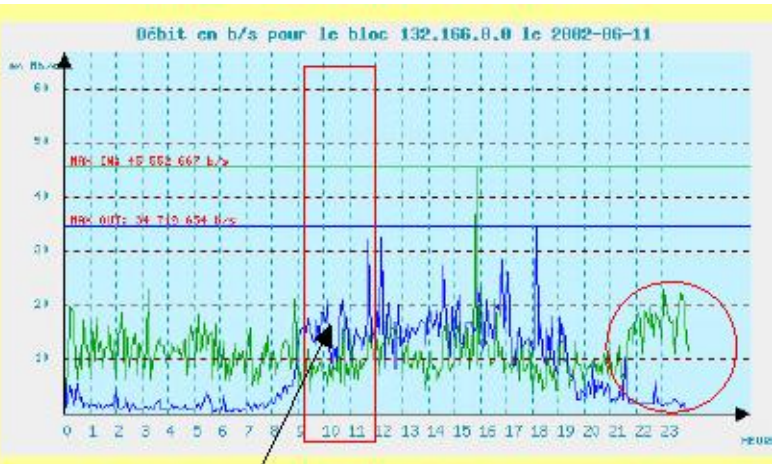
# Notion de fluxs

## Nombre de fluxs et débit.

## Répartition des fluxs par protocole




Le nombre de flux double pendant 20min.




Le débit n'augmente pas sur la même période, C'est donc des flux de petites tailles (scan, DoS attack…).