

Ecole Centrale de Lyon – Option IC – Filière SI  
René CHALON

## Supervision et Contrôle ~ Administration de réseaux

- 1- Définitions et modèle général
- 2- L'administration dans le monde IP
- 3- Autres modèles d'administration

Bibliographie

Version du 27/10/2009

**1**

### Définitions et modèle général

- ◆ Administration:
  - ◆ Ensemble des moyens pour contrôler, coordonner et surveiller les différentes ressources mises en œuvre

**QUOI ?**

**COMMENT ?**

Buts  
POURQUOI ?

D'après Simoni & Znaty

R. CHALON Administration de réseau 2

## Le QUOI

---

- ◆ Il faut gérer:
  - ◆ des équipements matériels :
    - des ordinateurs (PC, serveurs), des équipements intermédiaires (ponts, commutateurs, routeurs)
  - ◆ des réseaux (niveau 2 et niveau 3):
    - Ethernet, WAN, Wi-Fi, GSM, X25, IP, etc...
  - ◆ des services distribués :
    - client/serveur, multimédia, mobile, annuaires, etc.
  - ◆ des applications génériques et applications métiers :
    - Web, télé-séminaire, applications bancaires
  - ◆ des clients :
    - help desk, interface homme-machine

## Gérer les équipements

---

- ◆ Gérer les ressources physiques, équipements actifs et liens physiques
- ◆ Equipements actifs :
  - ◆ Du simple terminal au gros serveur en passant par les commutateurs et les routeurs et les modems
  - ◆ Supporte des logiciels
    - Nécessitant une certaine capacité mémoire et une puissance d'exécution
    - Produisant une certaine capacité de traitement ou de communication
- ◆ Liens :
  - ◆ Câbles, fibres optiques mais aussi ondes hertziennes ou lumineuses
  - ◆ Caractérisés par un débit nominal
- ◆ Reliés ensemble par diverses topologies

## Gérer les réseaux

---

- ◆ Gérer les réseaux composés de logiciels d'acheminement des données et de liens de données
- ◆ Acheminement :
  - ◆ Logiciels de relayage, de multiplexage, de commutation, de routage, etc.
  - ◆ Caractérisé par des capacités de traitements (nb de trames ou paquets par seconde), des délais de traitement, des taux de perte, etc.
- ◆ Liaisons de données :
  - ◆ Transmission des trames, des paquets entre 2 nœuds
  - ◆ Caractérisé par des débits, des délais de transmission, des taux d'erreurs, etc.

## Gérer des services

---

- ◆ Gérer des services distribués sur un réseau
  - ◆ Briques logicielles plus ou moins génériques pour mettre en œuvre d'autres services ou des applications
- ◆ Exemples :
  - ◆ Service d'authentification et d'autorisation
  - ◆ Services de chiffrement de données
  - ◆ Annuaire distribué (DNS, X500)
  - ◆ Services multimédia (diffusion-broadcast d'images vidéo)
- ◆ Caractérisé par :
  - ◆ Sa configuration : nombre de points, nécessité de serveurs centralisés
  - ◆ Propriétés : durée, taux d'utilisation, coût

## Gérer des applications et des clients

- ◆ Les applications bâties sur des services distribués fournissent des fonctionnalités génériques (exemple : messagerie électronique) ou spécifiques à un métier (exemple : réseau de distributeurs bancaires)
  
- ◆ Les clients sont les utilisateurs des applications
  - ◆ Identifier le client, gérer ses caractéristiques, le facturer
  - ◆ Prendre en compte l'assistance (help-desk)
  - ◆ Ergonomie et IHM de la station d'administration à prendre en compte

R. CHALON

Administration de réseau

7

## Le POURQUOI

- ◆ But de l'administration:
  - ◆ Maintenir le service conformément à la QoS demandée
- ◆ Qualité de service attendue - QoS [Quality of Service]
  - ◆ Effet global produit par les caractéristiques d'un service fourni à un usager qui déterminent le degré de satisfaction que cet usager retire du service (Cf E800 de l'ITU-T)
  - ◆ La qualité d'un service est caractérisée par l'effet conjugué des notions suivantes:
    - logistique de service,
    - facilité d'utilisation du service,
    - faisabilité,
    - intégrité du service,
    - d'autres facteurs propres à chaque service
- ◆ Qualité de fonctionnement - NP [Network Performance]:
  - ◆ Aptitude d'un réseau ou d'un élément de réseau à assurer les fonctions liées à des communications entre usagers

R. CHALON

Administration de réseau

8

## Critères de la QoS

- ◆ Les 4 critères de la QoS fournis:
  - ◆ **La disponibilité:** période de temps pendant laquelle le service offert est opérationnel
  - ◆ **La fiabilité:** aptitude d'un système, d'un matériel à fonctionner sans incident pendant un temps donné
  - ◆ **Le délai:** temps de transit de l'information dans le système
  - ◆ **La capacité:** nombre d'unités de traitement/seconde que peut assurer le système
- ◆ La QoS globale d'un réseau est mesurée à travers la QoS de chaque élément du réseau global
- ◆ Pour chaque critère on définit généralement:
  - ◆ une **valeur de conception**, qui indique les possibilités maximales,
  - ◆ une **valeur courante**, qu'il faut surveiller en phase d'exploitation,
  - ◆ une **valeur de seuil**, qui sert au déclenchement d'alarmes pour signaler les dysfonctionnements

R. CHALON

Administration de réseau

9

## Paramètres mesurables

Critères	Paramètres mesurables	Agrégation	Exemples pour 1 équipement
Disponibilité	Taux d'accessibilité (taux de rejet) Taux de connexion Taux de charge (mémoire)	Etat = $f$ (état de chaque composant)	MTBF, MTTR, mémoire disponible
Fiabilité	Taux d'erreur (lien) Taux de perte (nœud)	Etat = $f$ (état de chaque composant)	Taux de perte
Délai	Temps d'acheminement et de traitement Durée de vie d'une PDU Déséquilibrage des PDU Duplication des PDU	Somme des temps élémentaire	Temps de traversée de l'équipement
Capacité	Taux de charge (CPU) Débit (lien) Taille de PDU	Nb d'unités de traitement/seconde ( <i>min.</i> des valeurs)	Mips offertes

- ◆ Note:
  - ◆ MTBF [Mean Time Between Failure], MTTR [Mean Time To Repair]

R. CHALON

Administration de réseau

10

## Le COMMENT

---

- ◆ La mise en œuvre de la gestion se réalise au travers:
  - ◆ de modèles:
    - modèle informationnel,
    - modèle architectural,
    - modèle de communication,
    - modèle fonctionnel,
    - modèle organisationnel
  - ◆ de normes et de standards: CMIS, CMIP, MIB, SNMP, etc...
  - ◆ d'activités:
    - maintenance,
    - exploitation,
    - planification,
    - surveillance,
    - sécurité
  - ◆ d'outils: plate-formes et méthodes

## Les activités de l'administration (1/3)

---

- ◆ **La maintenance:**
  - c'est l'ensemble des actions permettant de maintenir ou de rétablir un équipement ou une installation dans un état spécifié ou en mesure d'assurer un service déterminé; on distingue plus particulièrement:
    - ◆ la **maintenance préventive** qui a pour objectifs:
      - diminuer les pannes et les imprévus de façon à réduire les coûts de la maintenance curative,
      - améliorer la qualité des produits,
      - prolonger la durée de vie du matériel,
      - améliorer la sécurité (pour le matériel comme pour le personnel)
      - améliorer la fiabilité et la maintenabilité du matériel
    - ◆ la **maintenance curative:**
      - il faut traduire la faute constatée par l'utilisateur en terme appropriés à la technologie réseau
      - il faut associer la panne à une catégorie aussi précise que possible: le composant ou la couche logicielle concernée

## Les activités de l'administration (2/3)

---

- ◆ **L 'exploitation:**
  - elle recouvre les actions prises en vue de fournir, modifier et supprimer la mise à disposition d 'équipements de services. Elle représente la phase opérationnelle pendant laquelle les décisions doivent être prises en temps réel. Elle comprend également la fourniture d 'information des ressources consommées à des fins de facturation
- ◆ **La supervision:** Elle se décline à travers les fonctions suivantes:
  - ◆ **Collecter** les informations traduisant le comportement des différentes ressources
  - ◆ **Analyser** les informations pour envisager et définir des actions
  - ◆ **Stocker** et archiver les informations
  - ◆ **Réagir** soit en émettant des commandes (pilotage) soit en informant l 'administrateur

## Les activités de l'administration (3/3)

---

- ◆ **La planification:**
  - Elle consiste à définir la topologie du système et à dimensionner chaque ressource du système de sorte que chaque usager puisse obtenir une communication dans des conditions optimales de qualité et de prix; il faut accomplir un certain nombre de tâches:
    - **mesurer** et prévoir la demande du trafic global entrant et sortant,
    - **choisir** pour chaque ressource une architecture adaptée,
    - **optimiser les investissements** en tenant compte des évolutions
    - **optimiser l 'utilisation** du système
- ◆ **La sécurité:**
  - ◆ Elle constitue un domaine à part entière à l'ISO (série 27000)
  - ◆ 5 groupes de propriétés: disponibilité, intégrité, confidentialité, auditableté, existence de preuve (non-répudiation)
  - ◆ des mesures pour éviter les sinistres: le contrôle d 'accès (authentification et gestion des autorisations), le chiffrement, le scellement, la signature, la notariation, etc...

## Les modèles d'administration (1/3)

---

- ◆ **Le modèle informationnel:**
  - ◆ il fournit une vue à la fois unifiée et précise des ressources à gérer,
  - ◆ il structure l'information de gestion et présente un certain degré d'abstraction
  - ◆ L'ISO (ISO 10165) définit un modèle orienté objet.
  - ◆ L'IETF (qui se limite à la gestion de réseaux TCP/IP) perçoit les objets à travers des variables stockées dans une base de données virtuelle, la base d'information de gestion (MIB)
- ◆ **Le modèle organisationnel:**
  - ◆ Il décrit la nature distribuée de la gestion (norme ISO 10040)
  - ◆ Le gestionnaire et l'agent échangent des informations de gestion à travers un protocole:
    - soit par une demande du gestionnaire et réponse de l'agent
    - soit par un compte-rendu spontané de l'agent lors d'un événement

## Les modèles d'administration (2/3)

---

- ◆ **Le modèle fonctionnel:**
  - il définit les opérations qui sont appliquées aux données du modèle informationnel. Ces opérations concernent les aires fonctionnelles de gestion – SMFA [Specific Management Functionnal Areas] (ISO 7498):
    - **Fault-Management:** gestion des pannes
    - **Configuration-Management:** gestion des configurations matérielles et logicielles
    - **Accounting-Management:** gestion des informations comptables en vue de déterminer le coût d'utilisation d'une ressource réseau
    - **Performance-Management:** gestion des performances du réseau
    - **Security-Management:** gestion de la sécurité au niveau des accès aux ressources et aux services



## Les modèles d'administration (3/3)

- ◆ **Le modèle de communication:**
  - Il définit les protocoles qui permettent de recueillir les informations élémentaires et les statistiques auprès des agents représentant les ressources:
    - A l'ISO, norme CMIP [Common Management Information Protocol] (ISO 9596),
    - A l'IETF, norme SNMP [Simple Network Management Protocol] et SNMP version 2.
- ◆ **Le modèle architectural:**
  - ◆ Il décrit la structure générale de entités réalisant les activités de gestion ainsi que leurs interfaces

R. CHALON

Administration de réseau

17

## Outils d'administration (1/2)

### ◆ Exemple HP-OpenView

The screenshot displays three HP OpenView windows. The top-left window, titled 'HP OpenView - UNTITLED:ALL NETS', shows an 'Internetwork View' with a tree structure of nodes including '156.18.10.0', '192.168.1.0', '192.168.2.0', 'cisco', and 'eclgw'. The top-right window, titled 'HP OpenView - UNTITLED:156.18.10.0', shows a 'Network View: 156.18.10.0' with a 'GoTo' button and 'ALL NETS' label, and a 'Discovered Nodes' section listing 'cisco', 'eclgw', 'tic130', 'tic137', 'tic138', and 'tic140'. The bottom window, titled 'HP OpenView - UNTITLED:192.168.1.0', shows a 'Network View: 192.168.1.0' with 'Discovered Nodes' listing 'cisco' and '192.168.1.130'. The bottom-right window, titled 'HP OpenView Alarm Log', displays a table of alarm events.

Status	Date	Time	Description	Object
Info	02/03/0	11:07:37	Trap #1 From OID 1.3.6.1.4.1.9.9.41.2	cisco.tic.ec-lyon.fr
Normal	02/03/0	11:07:36	02/03/09 11:06:11 Link Up Port 1	cisco.tic.ec-lyon.fr
Critical	02/03/0	11:07:22	node down	192.168.1.130
Info	02/03/0	11:06:11	Trap #1 From OID 1.3.6.1.4.1.9.9.41.2	cisco.tic.ec-lyon.fr
Info	02/03/0	11:04:38	Trap #1 From OID 1.3.6.1.4.1.9.9.41.2	cisco.tic.ec-lyon.fr
Normal	02/03/0	10:56:31	node up	192.168.2.129
Normal	02/03/0	10:50:22	node up	cisco.tic.ec-lyon.fr
Normal	02/03/0	10:48:41	node up	tic138.tic.ec-lyon.fr
Normal	02/03/0	10:47:19	node up	192.168.1.130
Normal	02/03/0	10:45:39	node up	192.168.1.130
Normal	02/03/0	10:45:20	Link Up Port 1	cisco.tic.ec-lyon.fr

R. CHALON

Administration de réseau

18

## Outils d'administration (2/2)

The screenshot displays two windows from a network management interface. The top window, titled 'system - cisco.tic.ec-lyon.fr', shows system configuration for Cisco IOS (tm) 3600 S. It includes a table of variables and their values:

Variable	Value
sysDescr	Cisco Internetwork Operating System Software
sysObjectID	1.3.6.1.4.1.9.1.338
sysUpTime	0 days 16 hours 18 mins 40.18 secs.
sysContact	cours-admin-reseaux
sysName	cisco-labnet.ec-lyon.fr
sysLocation	ECL-H9
sysServices	78

The bottom window, titled 'ip - cisco.tic.ec-lyon.fr', shows a traffic monitoring graph for 'cisco.tic.ec-lyon.fr - 156.18.10.253'. The graph plots four metrics over time (from 10:51:32 to 10:56:32):

- ip Forw Datagrams (blue line)
- ip In Delivers (green line)
- ip In Receives (red line)
- ip Out Requests (purple line)

The graph shows several peaks in traffic, with 'ip In Receives' and 'ip In Delivers' reaching approximately 35 units. The 'ip Forw Datagrams' and 'ip Out Requests' lines remain near zero.

R. CHALON Administration de réseau 19

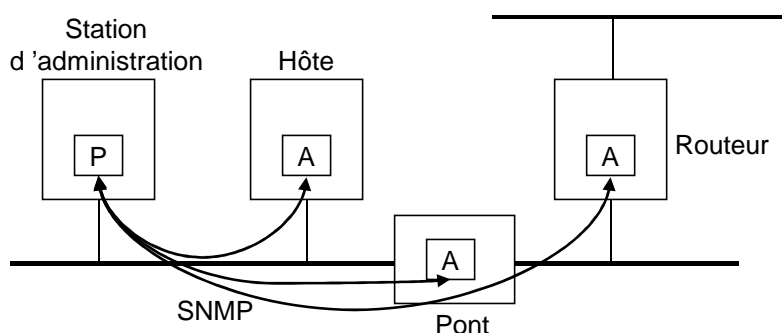
## 2 L'administration dans le monde IP

- ◆ Seuls deux modèles sont définis:
  - ◆ un modèle informationnel comprenant:
    - le SMI [Structure of Management Information], RFC 1902, qui décrit la structure et le nommage de l'information de gestion
    - la MIB [Management Information Base], RFC 1066 (et MIB-II, RFC 1213), qui décrit la base d'information de gestion
  - ◆ un modèle de communication basé sur le protocole SNMP [Simple Network Management Protocol], RFC 1157, et SNMP version 2, RFC 1441 et 1452
- ◆ SNMP est orienté:
  - ◆ vers la gestion des équipements et des réseaux, les dimensions services et applications n'étant pas prises en compte,
  - ◆ vers les réseaux fonctionnant sur IP, bien que d'autres protocoles soient maintenant pris en compte comme IPX

R. CHALON Administration de réseau 20

## Modèle SNMP

- ◆ Le modèle SNMP comporte:
  - ◆ des nœuds d'administration, qui intègrent un agent d'administration (A)
  - ◆ des stations d'administrations, comportant un processus d'administration (P)



R. CHALON

Administration de réseau

21

## Structure de l'information de gestion (SMI)

- ◆ La SMI, qui peut être vu comme un sous-ensemble du langage ASN.1, est utilisé pour décrire la MIB
- ◆ Chaque type d'objet possède:
  - ◆ un nom représenté par l'identificateur d'objet (OBJECT IDENTIFIER)
  - ◆ une syntaxe abstraite de donnée
  - ◆ une règle d'encodage pour les instances de ce type d'objet
- ◆ **Nom d'objet:**
  - ◆ Chaque objet possède un identificateur repéré dans l'arbre d'enregistrement de l'ISO
  - ◆ Chaque nœud possède un nom et un nombre. Il est identifié de manière unique par la concaténation des nombres (ou des noms) jusqu'à la racine
  - ◆ L'ensemble des objets gérés par l'IAB sont sous le nœud: internet OBJECT IDENTIFIER = { iso(1) org (3) dod(6) 1 }
  - ◆ Les objets du sous-arbre internet ont donc pour préfixe: **1.3.6.1**

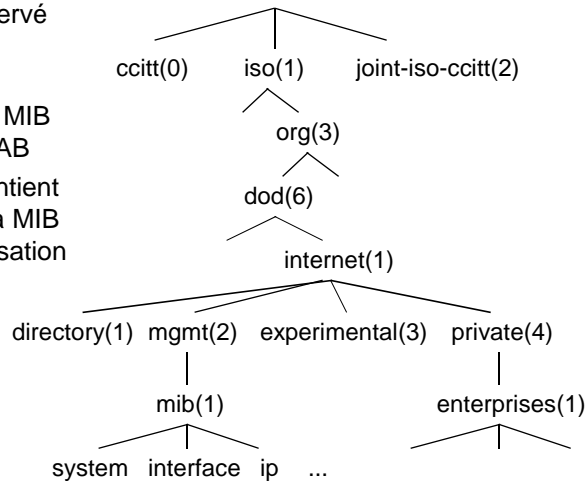
R. CHALON

Administration de réseau

22

## Hierarchie d'enregistrement

- ◆ **directory(1)** est réservé pour un usage futur (abandonné)
- ◆ **mgmt(2)** contient la MIB standardisée par l'IAB
- ◆ **experimental(3)** contient des extensions de la MIB en cours de normalisation
- ◆ **private(4)** contient des objets hors standards, par exemple définis par des constructeurs pour leur propre usage



R. CHALON

Administration de réseau

23

## Syntaxe

- ◆ La syntaxe définie par la SMI est un sous-ensemble de ASN.1 et de nouveaux type d'objets:
  - ◆ les types primitifs retenus sont:
    - INTEGER: nombre entier
    - OCTET STRING: chaîne de caractères de longueur variable
    - OBJECT IDENTIFIER: liste d'entiers (référence d'un objet)
    - NULL
  - ◆ les types composés conservés sont:
    - SEQUENCE: ensemble de données (Cf structure C ou Pascal)
    - SEQUENCE OF: tableau de données
  - ◆ les types ajoutés sont:
    - NsapAddress: adresse NSAP OSI
    - IpAdresss: adresse IP sous forme décimale pointée
    - Counter: compteur (sur 32 ou 64 bits) repassant par zéro
    - Gauge: compteur (sur 32 ou 64 bits) ne repassant pas par zéro
    - TimeTicks: temps compté en 100<sup>ème</sup> de secondes

R. CHALON

Administration de réseau

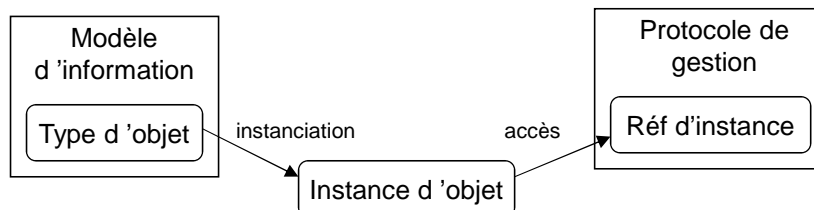
24

## Définition d 'objet

- ◆ Tout objet est défini par:
  - ◆ un **nom de type d'objet** associé à un « object identifier »
  - ◆ une **syntaxe** en ASN.1 du type d 'objet
  - ◆ une définition textuelle de la sémantique de l 'objet
  - ◆ le mode d 'accès: read-only, read-write, write-only, not-accessible
  - ◆ le statut: mandatory, optional, obsolete
- ◆ Exemple (hypothétique):
  - ◆ lostPackets **OBJECT-TYPE**
  - SYNTAX** Counter32
  - DEFINITION** « nombre de paquets perdus depuis le démarrage »
  - ACCESS** read-only
  - STATUS** optional
  - ::=** {experimental 20}

## Type d 'objet et instance

- ◆ Les **types d 'objet** sont identifiés par un identificateur d 'objet (chaîne d 'entiers le positionnant dans la hiérarchie d 'enregistrement)
  - exemple: lostPackets est identifié par 1.3.6.1.3.20
- ◆ Les **instances d 'objets** sont des variables associées à un type d 'objet et comportant une valeur; ils sont identifiés par: l'identificateur d'objet + l'identificateur d'instance:
  - ◆ pour un type simple, l'identificateur d 'instance est 0:
    - exemple: lostPackets.0 est une instance de l 'objet lostPackets
  - ◆ pour un tableau, c'est l 'indice dans le tableau

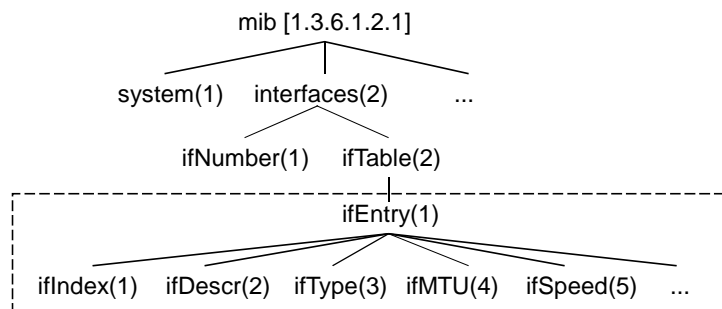


### La base d'information de gestion (MIB)

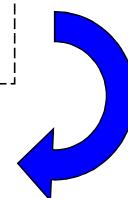
- ◆ SNMP définit une collection d'objets « standards » à administrer à travers la spécification de la MIB-II (RFC 1213)
- ◆ Tous ces objets sont définis dans le sous-arbre mib [1.3.6.1.2.1] dans plusieurs groupes:
  - ◆ system(1): décrit le nœud géré (7 objets)
  - ◆ interfaces(2): infos sur les interfaces et le trafic mesuré (23 objets)
  - ◆ at(3): correspondances entre adresses réseau et adresses physique (3 objets)
  - ◆ ip(4): infos et statistiques sur les paquets IP; il possède en particulier 2 tables: ipAddrTable et ipRoutingTable (42 objets)
  - ◆ icmp(5): stats sur les messages ICMP (26 objets)
  - ◆ tcp(6): infos et stats sur les connexions TCP (19 objets)
  - ◆ udp(7): infos et stats sur les datagrammes UDP (6 objets)
  - ◆ snmp(11): stats sur le trafic SNMP (29 objets)

### Exemple (1/3)

- ◆ Table des interfaces: ifTable [1.3.6.1.2.1.2.2]; elle décrit toutes les interfaces physiques présent sur le noeud



ifIndex	ifDescr	ifType	ifMTU	ifSpeed	...



### Exemple (2/3)

**ifDescr:** Description de l'interface  
**ifType:** Identification du type d'interface  
**ifMtu:** Taille max en octets des datagrammes IP  
**ifSpeed:** débit de l'interface en bits/s  
**ifPhysAddress:** adresse physique de l'interface  
**ifAdminStatus:** état administratif de l'interface (up/down)  
**ifOperStatus:** état opérationnel de l'interface (up/down)  
**ifLastChange:** date du dernier passage de l'interf à l'état opérationnel  
**ifInOctets:** nb total d'octets reçus sur l'interface  
**ifInUcastPkts:** nb de paquets unicast transmis au niveau supérieur  
**ifInNUcastPkts:** idem pour les paquets broadcast et multicast  
**ifInDiscards:** nb de paquets reçus et volontairement détruits  
**ifInErrors:** nb de paquets reçus contenant des erreurs  
**ifInUnknownProtos:** nb de paquets détruits car d'un protocole inconnu  
**ifOutOctets:** nb total d'octets transmis sur l'interface  
**ifOutUcastPkts:** nb de paquets unicast reçus du niveau supérieur

R. CHALON

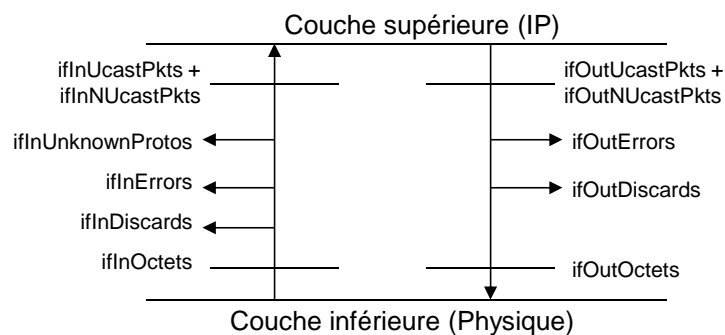
Administration de réseau

29

### Exemple (3/3)

**ifOutNUcastPkts:** idem pour les paquets broadcast et multicast  
**ifOutDiscards:** nb de paquets émis et volontairement détruits  
**ifOutErrors:** nb de paquets émis contenant des erreurs  
**ifOutQLen:** taille en paquet de la file d'attente de sortie  
**ifSpecific:** objet spécifique à un type d'interface

- ◆ fonctionnement des compteurs:



R. CHALON

Administration de réseau

30

## SNMP [Simple Network Management Protocol] (1/2)

- ◆ Protocole de communication entre la station d'administration et l'agent situé dans les nœuds (RFC 1067)
- ◆ Les objets ASN.1 sont codés en utilisant BER [Basic Encoding Rules] et transportés dans des datagrammes UDP
- ◆ Il y a cinq messages:
  - ◆ **GetRequest**: permet d'obtenir la valeur d'un objet
  - ◆ **GetNextRequest**: permet d'obtenir la valeur suivante d'un objet dans une table
  - ◆ **SetRequest**: permet de modifier la valeur d'objets dans la MIB de l'agent
  - ◆ **GetResponse**: message de réponse de l'agent aux 3 requêtes ci-dessus
  - ◆ **Trap**: message généré par l'agent sur un événement particulier spécifié a priori; il y a 6 événements possibles qui peuvent être augmentés d'événements « propriétaires »

R. CHALON

Administration de réseau

31

## SNMP (2/2)

- ◆ Exemples:
  - ◆ **GetRequest** *iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0* retourne le nombre d'interfaces disponibles sur un nœud (par exemple: 2)
  - ◆ **GetRequest** *iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.1* retourne le type de l'interface 1
  - ◆ **GetNextRequest** *iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.1* retourne le type de l'interface 2
- ◆ Format des messages:
  - ◆ **version**: numéro de version
  - ◆ **community**: nom de communauté; seul moyen d'assurer l'authentification de la provenance du message
  - ◆ **data**: qui contient une PDU (GetRequest, etc...)

R. CHALON

Administration de réseau

32



## Evolutions de SNMP: SNMP v2 et v3

---

- ◆ SNMP v2 (RFC 1902 à 1907) :
  - ◆ Amélioration des performances:
    - création d'un nouveau message **GetBulkRequest** permettant d'obtenir le contenu d'une table en une seule opération
  - ◆ Gestion hiérarchique ou distribuée:
    - création d'un nouveau message **InformRequest** permettant l'échange d'information entre gestionnaires
  - ◆ Mais la diffusion de SNMP v2 reste très limitée (trop complexe?)
- ◆ SNMP v3 (RFC 3410 à 3415) :
  - ◆ Amélioration de la sécurité:
    - Authentification par signature et chiffrement
    - Autorisation et contrôle d'accès
  - ◆ Amélioration de la gestion:
    - gestion des utilisateurs
    - Configuration à distance, etc...

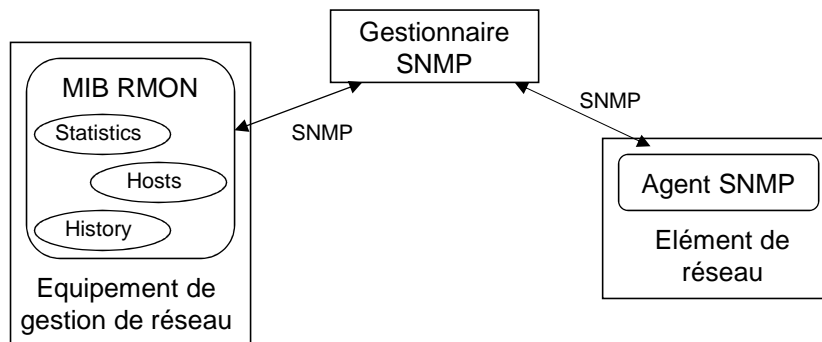
## Extensions de la MIB

---

- ◆ La branche **transmission(10)** permet de rajouter des extensions spécifiques à des médias :
  - ◆ Exemple : **dot3(7)** pour Ethernet
- ◆ Interface group MIB (RF2233) {mib-2 31} étend la table ifTable pour lever des ambiguïtés:
  - ◆ Les interfaces représentent des entités logiques ou physiques
  - ◆ Selon le type d'interface tous les objets ne sont pas supportés (défini à l'aide de *conformance statements*)
  - ◆ Possibilité de trous pour ifNumber et ifIndex
  - ◆ Table ifXTable avec des compteurs à 64 bits
  - ◆ Table ifStackTable définit la manière dont s'empile les couches définies par les interfaces
  - ◆ ifLinkUpDownTrapEnable pour déterminer la remontée des traps
  - ◆ Etc.

## MIB RMON [Remote Network Monitoring] (1/2)

- ◆ Extensions des MIB-I et II (RFC 1757 et 2074):
  - ◆ statistiques, détection de seuils d'alarmes, gestion des nœuds, filtrage de capture de paquets, gestion des notifications d'événements
  - ◆ fournit une vue d'ensemble de la gestion du réseau à travers une surveillance à distance



R. CHALON

Administration de réseau

35

## RMON (2/2)

- ◆ 9 groupes définis:
  - ◆ Statistics: gestion de stats sur le nœud pour chaque interface
  - ◆ History: enregistrement d'infos à des fins d'analyse par le gestionnaire
  - ◆ Alarm: mécanisme de définition de seuils
  - ◆ Host: stats sur chaque « host » générant du trafic sur le réseau
  - ◆ HostTopN: extension du groupe host
  - ◆ Matrix: fournit une matrice de trafic au niveau de la couche MAC
  - ◆ Filter: permet de définir des filtres de capture de paquets
  - ◆ Packet Capture: capture des paquets en fonction du filtre
  - ◆ Event: contrôle la génération et la transmission d'événements
- ◆ Nouvelle version RMON2 (RFC 2021) :
  - ◆ Traite complètement la couche 3 (et les couches supérieures) alors que RMON se charge de la couche 2 (et surtout d'Ethernet!)
  - ◆ 10 nouveaux groupes définis

R. CHALON

Administration de réseau

36

**3** *Autres modèles d'administration*

- ◆ **A I 'OSI:**
  - ◆ **CMIS** [Common Management Information System] et son protocole associé **CMIP** [Common Management Information Protocol]
- ◆ **A I 'OSF** [Open Software Foundation]:
  - ◆ **DME** [Distributed Management Environment] propose une gestion à partir d'objets encapsulés sur un ORB [Object Request Broker] conforme à **CORBA** [Common Object Broker Architecture]
  - ◆ Propose des outils au-dessus de ceux de l'OSI
- ◆ **A I 'ITU-T:**
  - ◆ **ODMA** [Open Distributed Management Architecture] cherche à couvrir les besoins en répartition de l'administration non-couverts par l'OSI ou l'OSF
- ◆ **A I 'OMG** [Object Management Group]:
  - ◆ Définition d'une architecture **OMA** [Object Management Architecture] et de **CORBA**

R. CHALON Administration de réseau 37

**Gestion OSI (1/3)**

- ◆ La gestion de systèmes OSI est définie au niveau application par une entité d'application: **SMAE** [System Management Application Entity]:

- ◆ **CMISE** [Common Management Information Service Element]
- ◆ **SMASE** [System Management ASE] définit la sémantique des informations échangées entre processus de gestion

R. CHALON Administration de réseau 38

### Gestion OSI (2/3)

---

- ◆ CMIS [Common Management Information Service] (ISO 9595) définit les services communs:
  - ◆ 7 primitives:
    - M-CREATE,
    - M-DELETE,
    - M-ACTION,
    - M-SET,
    - M-GET,
    - M-CANCEL-GET,
    - M-EVENT-REPORT
- ◆ CMIP [Common Management Information Protocol] (ISO 9596) définit le protocole commun supportant CMIS
- ◆ la MIB [Management Information Base] renferme l'ensemble des informations de gestion qui existent dans un système ouvert donné. L'organisation et la mise en œuvre de la MIB n'est pas normalisée

### Gestion OSI (3/3)

---

- ◆ Les fonctions de gestion spécifiques sont regroupés dans 5 domaines, les **SMFA** [Specific Management Functional Area]:
  - ◆ **Fault-Management**: gestion des pannes
  - ◆ **Configuration-Management**: gestion des configurations matérielles et logicielles
  - ◆ **Accounting-Management**: gestion des informations comptables en vue de déterminer le coût d'utilisation d'une ressource réseau
  - ◆ **Performance-Management**: gestion des performances du réseau
  - ◆ **Security-Management**: gestion de la sécurité au niveau des accès aux ressources et aux services

**4*****Bibliographie***

---

- ◆ Bibliographie :
  - ◆ Simoni N., Znaty S., Gestion de réseau et de service, Masson, 1997, ISBN 2-225-82980-2
  - ◆ The Simple Web, <http://www.simpleweb.org/>
  - ◆ Willm O., Administration de réseaux informatiques : protocole SNMP, In *Techniques de l'Ingénieur*, H2 840, mai 2003.