INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

# Module : Administration réseaux
# SNMP
# Simple Network Management Protocol

4ème année

Promotion 2022 Département STI

Année 2020-2021

# SNMP but

RFC 1157

Permettre une administration distante ou locale.
Protocole utilisé sur les réseaux de type Internet (à l'origine conçu pour les ponts et les routeurs) :

- Connaître l'état d'un nœud du réseau
- Mesurer le trafic et les erreurs à distance
- Configurer à distance les nœuds du réseau

# SNMP Historique

Problématique de gestion de réseaux :

- Organisations de tailles différentes
- Équipements divers

- 2 protocoles ont été développés pour la gestion réseau :

  SNMP Simple Network Management Protocol porté par l'IETF

  Common Management Information Services CMIS avec les protocoles CMIP (CMI Protocol) et CMOT (CMIS over TCP) porté par L'ISO

- SNMP devait servir en attendant CMOT, mais il reste aujourd'hui le plus utilisé. CMOT se rencontre surtout dans les réseaux de téléphonie

# SNMP principe :

- Une station de gestion
- Agent sur chaque élément du réseau à gérer (station, serveur, switch, hub, routeur…)

Supervision et contrôle : un nœud du réseau est vu comme un ensemble de variables qui peuvent être lues et/ou modifiées.

Un nœud avertit la station lors de certains événements (trap)

# SNMP contenu :

SNMP est constitué de :

Un langage de définition des structures SMI “Structure of Management Information” (arbre numéroté, nœuds et feuilles)

Des bases de données MIB (Management Information Base) contenant nœuds et feuilles

Un protocole (SNMP sur UDP, port 162,161) et un démon « snmpd »

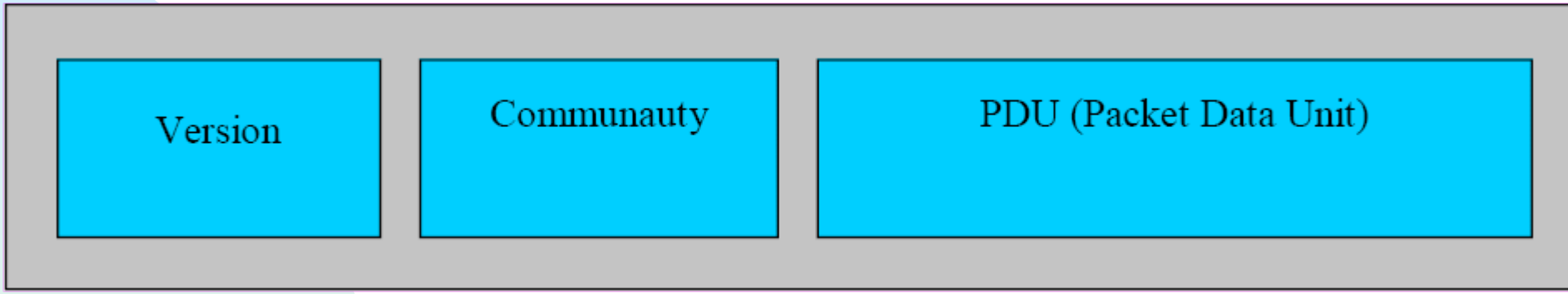
# SNMP les éléments

Équipements gérés (managed devices): des éléments du réseau (nœuds réseaux), contenant des "objets de gestion" (managed objects) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques.

Agents : applications de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP.

Systèmes de management de réseau (network management systems - NMS) : console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration.

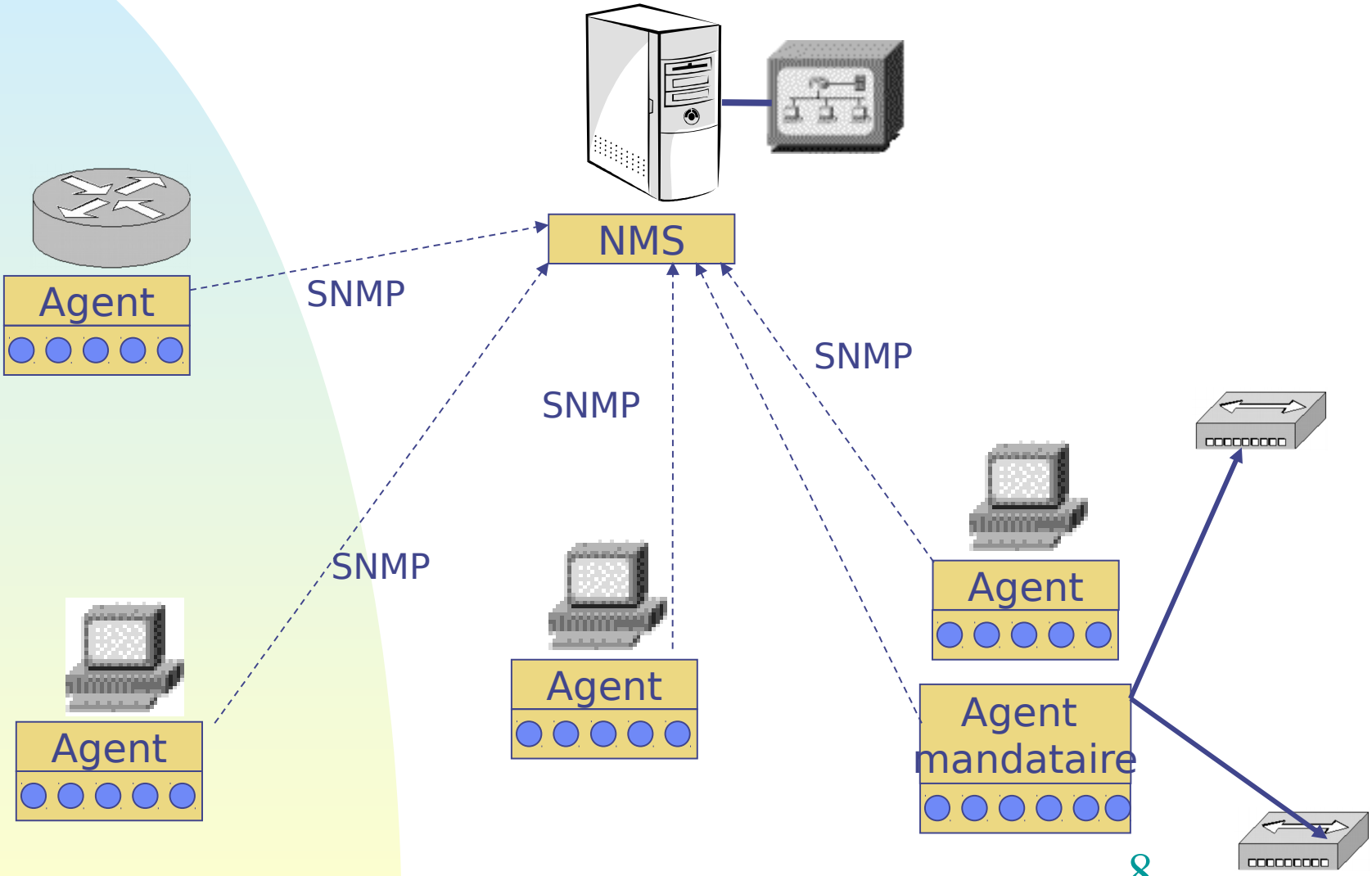
# Trame SNMP




Trame de requête

- Version du protocole : 1 (puis 2c et 3)
- Community : définit un profil d'utilisateur, sert à l'authentification.
- PDU : Packet Data Unit

# SNMP : Architecture



# ASN.1 (Abstract Syntax Notation)

Abstract Syntax Notation One (plus connu sous le nom d'ASN.1) est un langage de définition des normes sans tenir compte de l'implémentation (création 1984).

L'ASN.1 est un standard défini conjointement par l'organisation internationale de normalisation ISO, la commission électrotechnique internationale CEI et l'union internationale des télécommunications ITU-T.

Par exemple, les certificats d'authentification X.509 ont leurs structures décrites par l'intermédiaire de ASN.1

XML est un concurrent de ASN.1 moins complexe mais plus verbeux.Il existe des modules pour passer de XML à ASN.1 "Mapping W3C XML Schema definitions into ASN.1".http://www.itu.int/en/ITU-T/asn1/Pages/Mapping-from-XML-Schemas-to-ASN-1-modules.aspx

# ASN.1 (Abstract Syntax Notation)

SNMP va permettre l'échange d'informations sur des objets de chaque nœud. Les équipements étant hétérogènes, SNMP oblige de définir chaque objet dans un langage normalisé ASN.1.

Les objets de la MIB sont décrits dans le langage SMI (“Structure of Management Information”), qui est lui même un sous-ensemble de ASN.1

# ASN.1 (Abstract Syntax Notation)

ASN.1 définit entre autres :

- Ce qu'est un "type".
- Ce qu'est un "module" et à quoi il doit ressembler.
- Ce qu'est un ENTIER.
- Ce qu'est un BOOLÉEN.
- Ce qu'est un "type structuré".
- La signification de certains mots clés (par exemple, BEGIN, END, IMPORT, EXPORT, EXTERNAL, et ainsi de suite).
- Comment faire pour "baliser" un type afin qu'il puisse être codé correctement.
- Pour transmettre des données de type ASN.1, il faut des règles de codage sur le réseau .
  Les encodages les plus utilisés sont BER (Basic Encoding Rules) et DER (Distinguished Encoding Rules). Les deux se ressemblent, mais ce dernier est spécifié pour garantir l'unicité de l'encodage. DER est plutôt utilisé pour les certificats.

# ASN.1 syntaxe

Par exemple, ifDescr est décrite par :

```
ifDescr OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "A textual string containing
information about the interface.  This string should
include the name of the manufacturer, the product name
and the version of the hardware interface."
    ::= { ifEntry 2 }
```

# Encodage BER

- SNMP utilise les règles d'encodage BER.
- Cet encodage permet de transmettre les données de  l'objet de manière à les rendre lisibles par tout automate d'analyse BER.

- BER d'ASN.1. est défini dans les recommandations ITU-T X.209 et X.690. C'est un ensemble de règles permettant de coder des données ASN.1 en un flux d'octets qui peut être transmis sur le réseau.

- Pour plus de détails sur ASN.1 et BER : http://support.microsoft.com/kb/252648/fr

# MIB : Espace de nommage

- Identification d'un objet :
  - un nom associé (OBJECT IDENTIFIER)
  - une syntaxe abstraite de données
  - une règle d'encodage pour les instances de cet objet
- l'ISO a défini un arbre d'enregistrement dans lequel tout objet administrable doit se retrouver de manière unique
  - à un nom d'objet est associé un nombre (OID Object IDentifier)

    Par exemple, les objets du sous-arbre internet commencent par 1.3.6.1

    Ceux des objets MIB I par 1.3.6.1.2.1

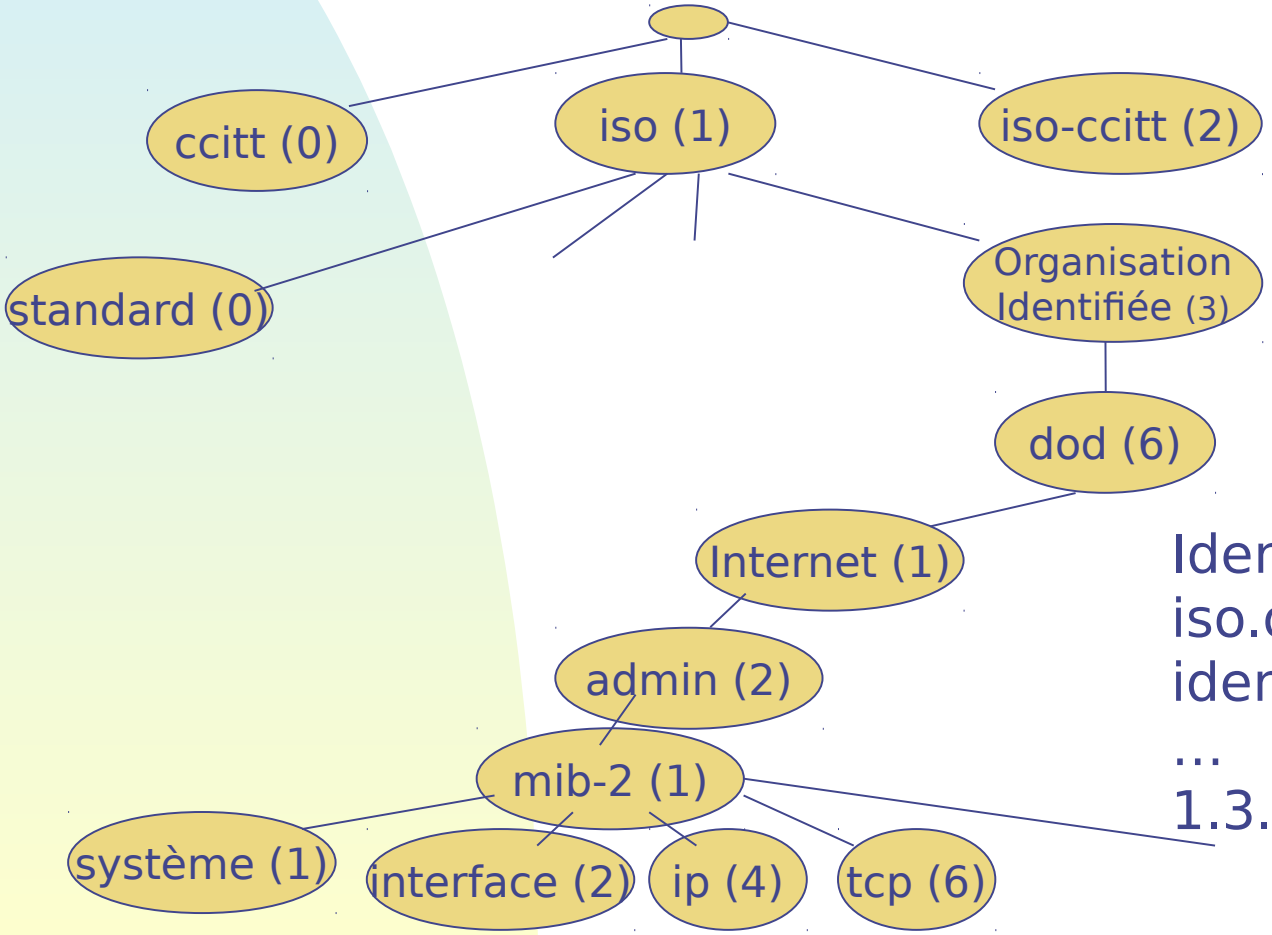
# MIB : Objet de la base

- 1.3.6.1.2.1.x.y... pour les variables de la MIB standard,
- 1.3.6.1.4.1.x.y… pour les variables MIB constructeurs, x étant No attribué au constructeur
- 1.3.6.1.6.3.x.y… pour les variables de l'architecture SNMPv3

# MIB : Management Information Base

Regroupe tous les objets SNMP possibles

Organisation hiérarchique – RFC 1066




Identification :
iso.organisation identifiée.dod.Internet
...
1.3.6.1...

# La spécification MIB

- SNMP définit un ensemble d'objets standards à administrer à travers MIB-I et MIB-II
- Une MIB est une collection structurée d'objets
- Groupés dans le sous-arbre 1.3.6.1.2.1 :
  - system : décrit le nœud géré : 7 objets
  - interface : états et trafic
  - ip : infos et stats sur le trafic IP : 42 objets
  - tcp : infos et stats sur le trafic TCP : 19 objets
  - udp : infos et stats sur le trafic UDP : 6 objets
  - snmp : infos et stats sur le trafic SNMP : 29 objets
  - ...

# Exemple

- la table des interfaces : l'objet ifTable [1.3.6.1.2.1.2.2] décrit toutes les interfaces physiques
- Elle possède une table ifEntry qui a des sous objets renseignant par exemple le débit de l'interface (ifSpeed (5)), le nombre de paquets reçus et volontairement détruits (ifInDiscards), ...

# Les MIBS spécifiques à des entreprises (1/2)

- Lorsqu'une entreprise veut définir sa propre MIB, elle va acheter un numéro de nœud sous le noeud iso.org.dod.internet.private.entreprise.
- Ces MIB sont dites privées.
- Elles correspondent à la racine 1.3.6.1.4.1

# Les MIBS spécifiques à des entreprises (2/2)

```
PRIVATE ENTERPRISE NUMBERS

SMI Network Management Private Enterprise Codes:

Prefix: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

Decimal
| Company
| | Contact
| | | Email
| | | |
0
  Reserved
    Joyce K. Reynolds
      jkrey@isi.edu
1
  NxNetworks
    Michael Kellen
      OID.Admin@NxNetworks.com
2
  IBM
    Bob Moore
      remoore@us.ibm.com
3
  Carnegie Mellon
    Mark Poepping
      host-master@andrew.cmu.edu
4
  Unix
    Keith Sklower
      sklower@okeeffe.berkeley.edu
```

# Définition des objets

- Les objets administrables sont une abstraction des ressources physiques (interfaces, équipements,etc.) et logiques (connexion TCP, paquets IP, etc.). Composés de :
  - un nom (Descripteur + identificateur d ’objet)
  - une syntaxe utilisant ASN.1 (Abstract Syntaxe Notation)
  - une définition qui est un texte de description de l ’objet
  - Des droits d ’accès à l ’objet (read only, read-write or not accessible)
  - statut qui spécifie s'il est mandatory, optional ou obsolète.
  - un schéma de codage BER (Basic Encoding Rules)

# Définition des objets

- exemple :
  - lostPackets OBJECT-TYPE
  - SYNTAX Counter32
  - DEFINITION "nombre de paquets perdus"
  - ACCESS read-only
  - STATUT optional
  - ::= {experimental 20}

lostPacket est identifié par [1.3.6.1.3.20]

# Accès aux objets

- L ’identification se fait par l'OID (Object IDentifier) suivi par un suffixe. La MIB de SNMPv2 est définie dans la RFC 1907
  - Le suffixe =0 pour une variable simple
  - le suffixe <> 0 pour désigner l ’index dans le cas d’une variable composée (un tableau)
- Chaque message SNMP (sauf les traps) contient :
  - un identificateur de requête
  - une liste de variables (noms et valeurs)
  - éventuellement une liste d’erreurs (tooBig, etc.)
  - un indice pour les erreurs.

# Accès aux objets

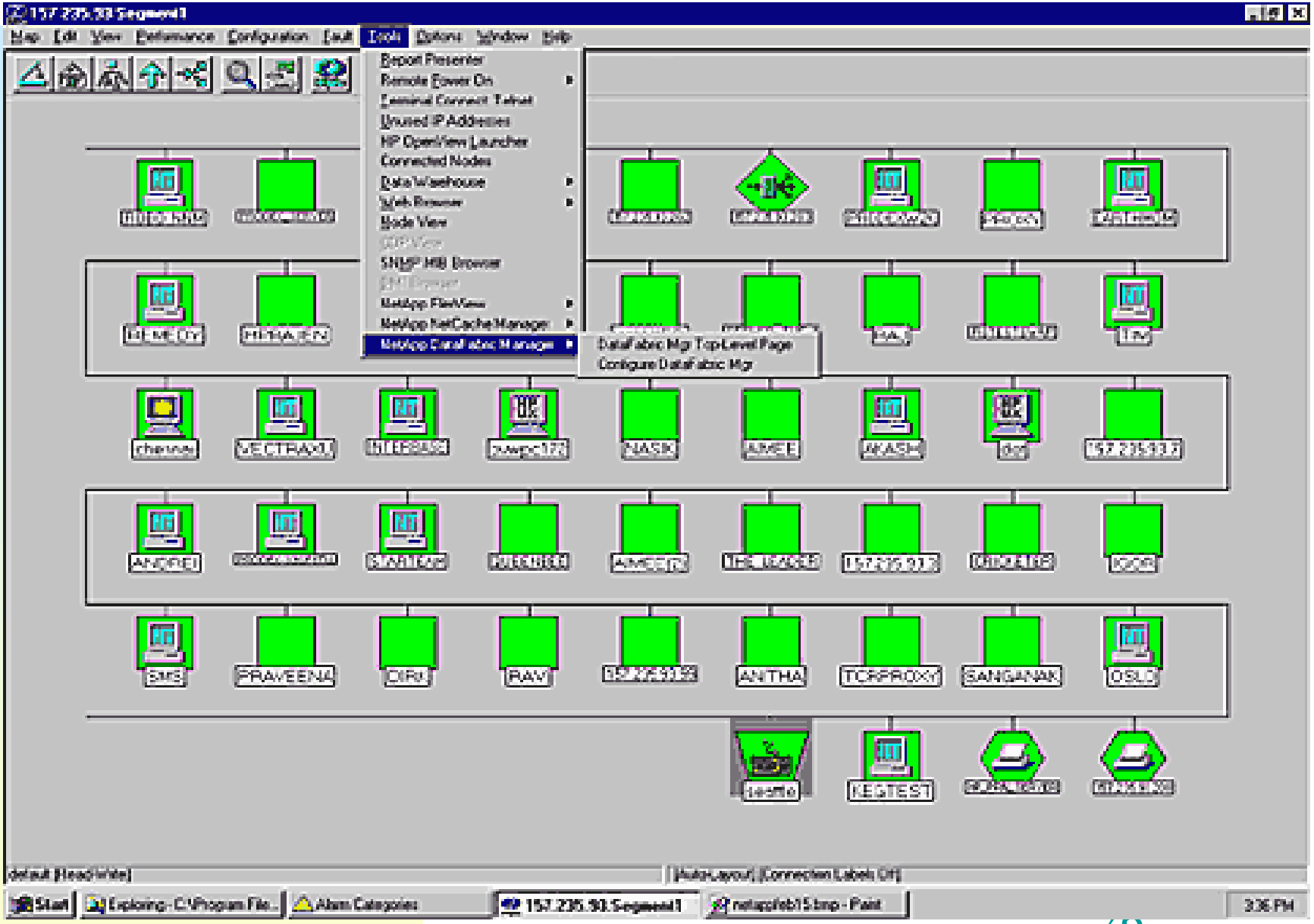
- Pour visualiser les objets dans la MIB, on peut utiliser un navigateur (Browser) de MIB.

# Message SNMP

- Set-request : mise à jour d'une ou plusieurs variables
- Alarmes
  - Snmpv2-trap : signale un changement d'état
- Get
  - Get-request : demande la valeur d'une ou plusieurs variables
  - Get-next-request : demande la valeur de la variable suivante
  - Get-bulk-request : chargement d'une grande table
- Réponses

Communication : UDP, ports 161 (get, set), 162 (trap)

# Visualisation



# Modèle deux-tiers

- Le modèle utilisé par SNMP est un modèle client serveur de type deux-tiers (two tiers) soient deux paliers ou gradins.
- Il est possible de transformer cette architecture en architecture trois tiers en incluant une sonde RMON “Remote networking Monitoring” SNMPv2.
- Cette sonde permet de faire la collecte d'informations et quelques traitements avant  le traitement par la console NMS.
- Lorsque l'on utilise des sous agents on parle d'agentx

# SNMPv1 SNMPv2

- Le protocole original  SNMPV1 est décrit dans les RFC 1155 à 1157 début en 1980.
  Peu de sécurité, la communauté passe en claire.
- SNMPv2 en version initiale (1993) devait corriger d'une part les imperfections de SNMPv1 et surtout apporter le volet sécurité.
- Les imperfections ont été corrigées par SMIv2. SNMPv2p (p pour party based) reposait sur un dialogue entre entités appelées « party »,qui n'a pas abouti. Le bénéfice des avancées du SMIv2 a été gardé, on conserve l'enveloppe du message SNMPv1 (communauté) et  on utilise le SMIv2 dans les MIB. C'est ce qu'on appelle SNMPv2c(C pour community)

# Différences v1 v2

- Manipulation des tableaux améliorée par le SNMPv2c.
- Protocole inefficace (pas de transfert de masse dans V1), corrigé dans V2c (PDU getbulk)
- Alertes (TRAP) non acquittées dans SNMPv1, corrigé dans V2C
- Entiers limités à 32bit (V1), SMIv2 compteur 64 bits
- Une erreur dans la requête annule toute la requête , corrigé par V2
- ...

# SNMPv3

- Architecture plus modulaire
- Sécurité renforcée :

- **Drapeaux**

  Trois bits sont utilisés pour indiquer :
  - Si une réponse est attendue à la réception de ce paquet. (Reportable Flag)
  - Si un modèle de cryptage a été utilisé (Privacy Flag)
  - Si un modèle d'authentification a été utilisé (Authentification Flag)

# SNMPv3

**Le modèle de sécurité**

Ce module identifie le type de sécurité qui est utilisé pour encrypter le PDU du paquet.

Cet identificateur doit identifier de façon unique chaque module de sécurité.

Actuellement, l'algorithme de cryptage DES (Data Encryption Standard) et l'algorithme d'authentification HMAC-MD5-96 ont été choisis comme algorithmes utilisés dans SNMPv3.

HMAC-SHA1 est optionnel ainsi que AES pour l'encryptage.

# SNMPv3

- L'intégrité
  a pour rôle d'assurer que le paquet reste inchangé pendant la transmission, et que le mot de passe est valide pour l'usager qui fait la requête.
  Le mot de passe partagé sert d'authentification
- On utilise des fonctions de hachage :
  HMAC-MD5-96 et HMAC-SHA-1.
  Empreinte de 16 octets pour MD5, 20 octets pour SHA-1.
- L'ensemble du paquet SNMP est authentifié

# SNMPv3 horodatage 1/2

- L'horodatage
  Si une requête est capturée, on peut tenter de la réutiliser plus tard, sans modification.
- Pour éviter ceci, le temps est estampillé (horodaté) sur chaque paquet.
  Quand on reçoit un paquet SNMPv3, on compare le temps actuel avec le temps dans le paquet. Si la différence est supérieure à 150 secondes, le paquet est ignoré.

# SNMPv3 horodatage 2/2

- L'horodatage
  On utilise une horloge différente dans chaque agent.
  L'agent utilise deux compteurs :
  - BOOTS (Nombre d'allumages de l'agent )
  - TIME (Nombre de secondes depuis la dernière mise en route).
- La combinaison du BOOTS et du TIME donne une valeur qui augmente toujours qui sert à estampiller.
- La plate-forme de gestion doit garder une horloge qui doit être synchronisée pour chaque agent qu'elle contacte.

# SNMPv3

- La confidentialité

  Avec SNMPv3, le cryptage de base se fait sur un mot de passe « partagé » entre le manager et l'agent.

  Pour des raisons de sécurité, SNMPv3 utilise deux mots de passe : un pour l'authentification et l'intégrité et un pour le cryptage.

  Ceci permet au système d'authentification et au système de cryptage d'être indépendants. Un de ces systèmes ne peut pas compromettre l'autre.
- Seul le PDU est crypté

# SNMPv3

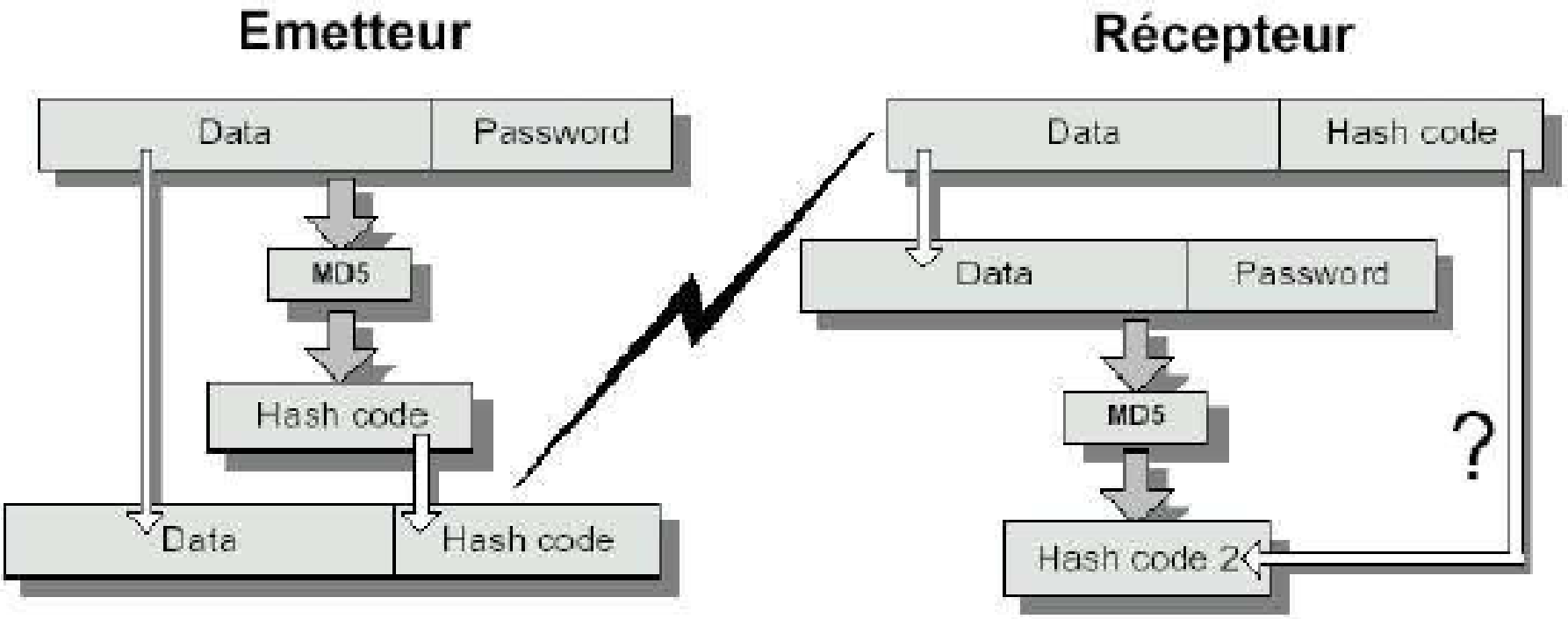
- Le View Access Control Model (VACM)

Permet le contrôle d'accès au MIB.
Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur.

# SNMP Exemple de trame

```
⊞ Frame 2 (120 bytes on wire, 120 bytes captured)
⊞ Ethernet II, Src: Cisco_3e:e3:c0 (00:12:80:3e:e3:c0), Dst: 00:00:00_00:00:02 (00:00:00:00:00:02)
⊞ Internet Protocol, Src: 172.16.30.254 (172.16.30.254), Dst: 192.168.101.2 (192.168.101.2)
⊟ User Datagram Protocol, Src Port: snmp (161), Dst Port: 3187 (3187)
    Source port: snmp (161)
    Destination port: 3187 (3187)
    Length: 86
    Checksum: 0xb712 [correct]
⊟ Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: RESPONSE (2)
    Request Id: 0x00000025
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.4.1.9.2.1.58.0 (SNMPv2-SMI::enterprises.9.2.1.58.0)
    Value: INTEGER: 16
    Object identifier 2: 1.3.6.1.4.1.9.2.1.57.0 (SNMPv2-SMI::enterprises.9.2.1.57.0)
    Value: INTEGER: 16
    Object identifier 3: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
    Value: Timeticks: (11915034) 1 day, 9:05:50.34
```

# SNMPv3 Authentification



# Fichier snmpd.conf

```
#       sec.name          source
community
com2sec                 local     localhost                 sz
Com2sec                 localnet 192.168.179.0/24      public
#####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   RWGroup                 v1          local
group   ROGroup                 v1          localnet.
```

# Fichier snmpd.conf

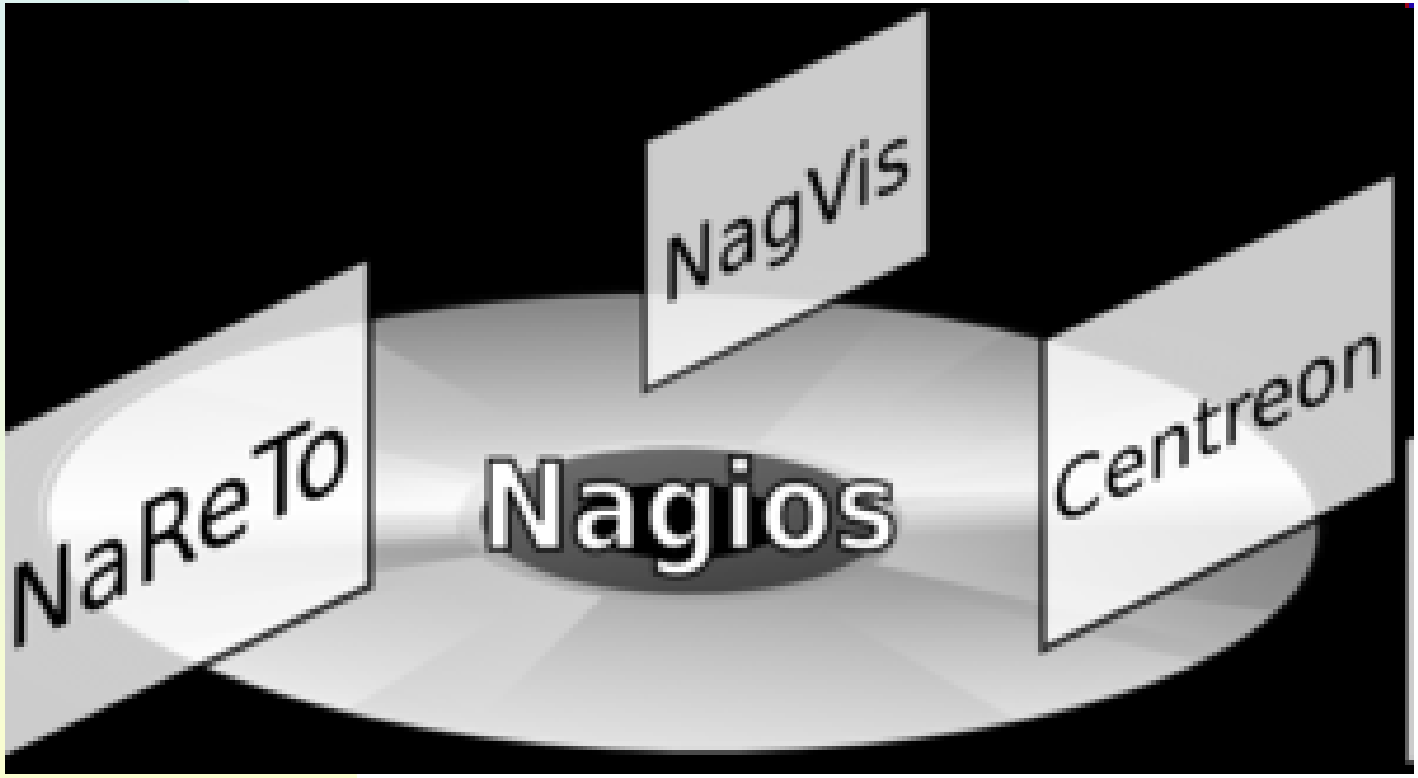
```
#       name            incl/excl     subtree   mask(optional)
view      tout            included    .1
```

# Fichier snmpd.conf

```
#        group       context sec.model sec.level prefix read    write
access  ROGroup      ""      v1        noauth    exact  tout    none
access  RWGroup      ""      v1        noauth    exact  tout    tout
```

# Utilitaires de monitoring réseau

- NAGIOS outil libre

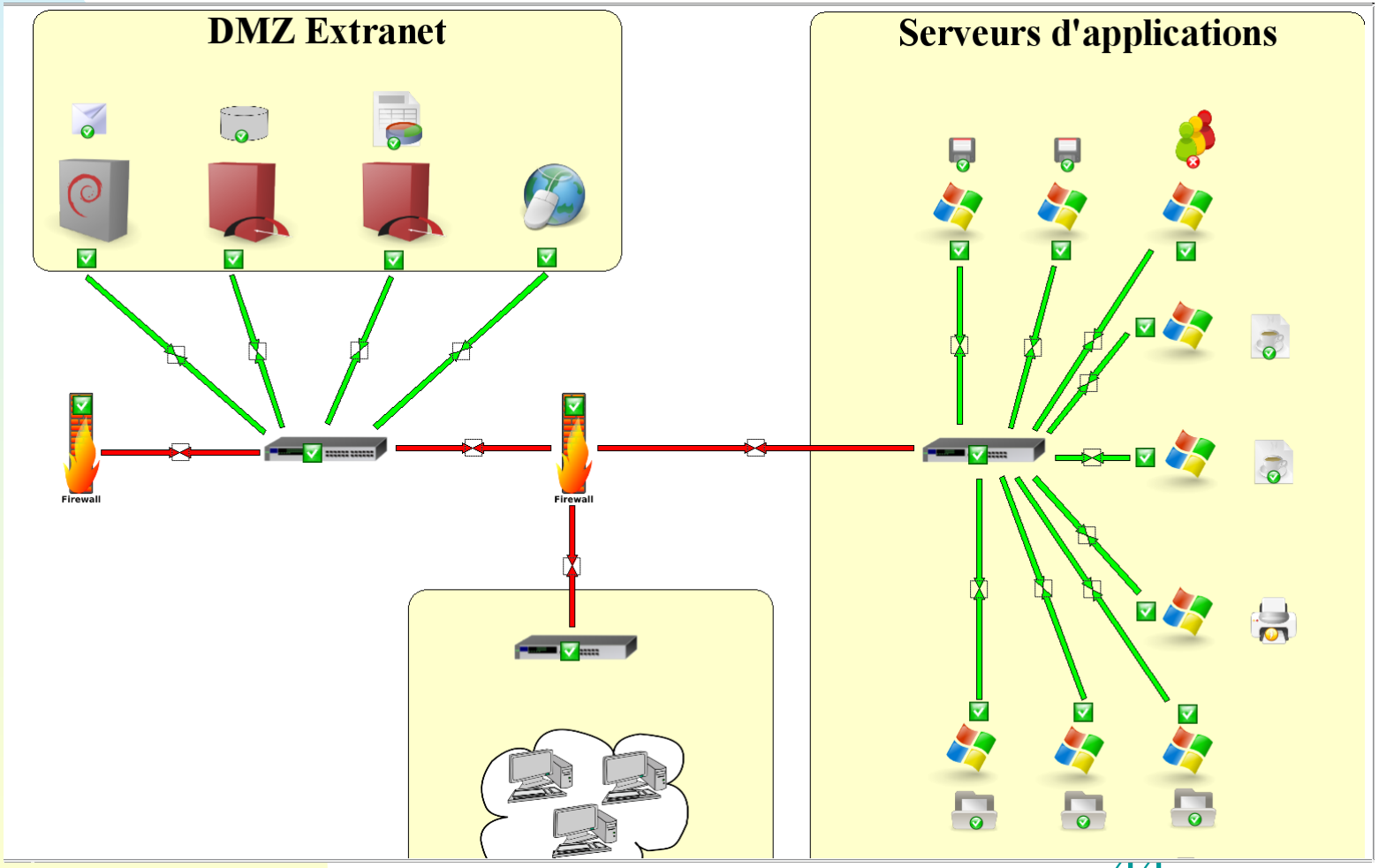


# Utilitaires de monitoring réseau

- NAGIOS outil libre
  peut être complété par :
  - Nagios plugins: plugins pour surveiller les serveurs
  - Centreon: Web frontend pour Nagios
  - NagVis: un outil pour la configuration des cartes de visualisation
  - NDOUtils: Nagios module pour stocker les données de surveillance en MySQL
  - NaReTo (Nagios Reporting Tools): un très bon outil pour faire des rapports de disponibilité
- Live cd  projet FAN (Fully Automated Nagios)
  http://www.fullyautomatednagios.org/

# Utilitaires de monitoring réseau

Captures d'écran



# Utilitaires de monitoring réseau

## Captures d'écran