UREC

# ADMINISTRATION RESEAU

**&**

**OUTILS DU DOMAINE PUBLIC**
**(2 ème partie)**

**Bernard TUY**



UREC

## PLAN

- **Rappels sur la 1 ère partie**
- **SNMP**
- **Plateformes "Intégrées"**
- **Outils du Domaine Public**

## DEFINITIONS

UREC

- Administrer un réseau : Qu'est-ce à dire ?
  - Préliminaires :
    - » CONCEVOIR
    - » METTRE en OEUVRE
  - Tâches qui assurent le fonctionnement optimal du réseau
    - » => SURVEILLER
    - » => DEPANNER
  - Recueillir les informations nécessaires à l'évolution du réseau.

## GENERALITES (1)

UREC

- Administrer : Quoi ?
  - Un (plusieurs) Réseau(x) Informatique(s) :
    - . les supports physiques (câbles)
    - . les équipements actifs (coupleurs, hubs, routeurs...)
    - . les services applicatifs (DNS, messagerie...)
    - . les applications réseau (telnet, ftp,...)

## GENERALITES (2)

UREC

- Administrer : Avec qui, avec quoi ?
  - administrateur réseau, opérateurs...

    => organisation des ressources humaines
  - plateformes d'administration réseau "intégrées"

    => constructeurs, commerciales
  - outils du domaine public

## GENERALITES (3)

UREC

- Administrer : Comment ?
  - Définition d'un protocole dédié aux taches de surveillance :
    - » Simple Network Management Protocol
  - Centralisé versus décentralisé

## SNMP

- Simple Network Management Protocol
- décrit dans le RFC 1157
- Utilise UDP (port 161 pour agent, 162 pour traps)
- Protocole simple d'administration d'équipements sur un réseau IP :
  - passerelle, routeur, pont, étoile, hub, multirépèteur, serveur de terminaux ...
- Equivalent OSI : CMIS

## SNMP : Sur les équipements

- MIB Management Information Base (Base de Données)
  - » RFC1155, 1156 (MIB I) et RFC 1213 (MIBII) ...
  - » Elle contient des objets standards (définis par les RFCs) et des extensions propriétaires .

  Exemples d'objets :

  table de routage, nombre de collisions, longueur des files d'attentes

  beaucoup de compteurs : utilisation du CPU, paquets reçus et émis,.....
- Un agent SNMP (daemon Unix) :
  - répond aux requêtes des stations d'administration
  - envoie des alarmes (traps) à ces stations

## SNMP : Sur la station d'administration :

- Envoie des commandes
  - Get : lecture d'une variable
  - Set : mise à jour d'une variable sur les équipements
- Reçoit les alarmes envoyées par les agents sur les équipements
  - peut déclencher une action sur réception d'évènement (programmes C, scripts shells, mails, Nos de tel. ...)



## SNMP

- Avantages
  - Simple donc implémenté sur de nombreux équipements
  - Permet d'administrer du matériel hétérogène
  - C'est le seul protocole utilisable à ce jour
- Inconvénients
  - Brut de fonderie. Il faut un administrateur compétent sur la station d'administration SNMP
  - Sécurité limitée à un contrôle sur la communauté (community string)
  - Administration répartie ou hiérarchique pas possible

## SNMPv2

UREC

- Simple Network Management Protocol Version 2
  - RFC 1441-1452
- Corrige la plupart des défauts de jeunesse de SNMP (v1)
  - sécurité, lecture groupée de variables ...
- Administration hiérarchique

## Plateformes "intégrées"

UREC

- Sun Net Manager
- HP Openview
- Netview
- Spectrum

SNMPc

## Sun Net Manager

UREC

- Plateforme de base supportant de nombreux "packages" d'administration de constructeurs divers :
  - Cisco, Novell, Sun et compatibles ...
- Utilise également les RPC (surveillance des ressources système)
- Version courante :
- Prix :
- Investissement :

## HP Openview

UREC

- Ensemble de logiciels assez complet (trop ?)
  - Noyau HP Openview
  - Rapports statistiques, modélisation des flux de données (EASY) ...
- Version courante :
- Prix
- Investissement :

## Netview 6000

UREC

- Comparable à HP Openview dont il est issu
  - pour plate-formes IBM (Risk 6000 ...)
  - administration distribuée
  - administration et surveillance multiprotocole
  - base de données associée
- Version courante :
- Prix :
- Investissement :

## Spectrum

UREC

- Ensemble de logiciels très complets développés par Cabletron
  - permet de gérer la plupart des matériels habituellement rencontrés (y compris AppleTalk)
- Version courante :
- Prix :
- Investissement :

## SNMPc

UREC

- Package réduit mais fonctionnalités d'administration de base bien implantées.
- Pour plate-forme PC DOS Windows
- Version courante :
- Prix :
- Investissement :

## OUTILS du Domaine Public (2 ème partie)

UREC

- ttcp (adm)
- tcpdump (adm)
- nnstat (adm)
- netman (ana + stat)
- Internet Rover
- MIT snmp toolkit (adm)
- CMU snmp (adm)

## Ttcp

UREC

- ttcp est un outil d'évaluation de performances (débit)
- établissement d'une connexion en mode socket entre 2 machines :
  - la quantité de données à transférer et la taille des buffers est paramétrable ...
- Attention à la charge induite sur le réseau !



## Tcpdump

UREC

- tcpdump permet de visualiser et d'analyser le trafic entre plusieurs machines.
- comparable à snoop et etherfind (filtres, analyse au vol ou off-line ...)
- tcpview : variante graphique de tcpdump :
  - plus facile à utiliser
  - meilleure exploitation des résultats

## Nnstat(1)

UREC

- nnstat est un outil d'analyse statistique, il permet d'accéder aux informations habituelles :
  - @Eth, @IP, #port, type ...
- SAA : Acquisition des données sur chaque élément à surveiller (filtres)
- SCH: Centralise les données recueillies par les différents SAA installés sur le(s) réseau(x).

## Nnstat(2)

UREC

nnstat ne dispose :

- ni d'outils de traitement des données
- ni d'outils de présentation des données

- la programmation de l'outil (fichier de commandes) nécessite... un peu de temps !

=> évaluer ce dont on a réellement besoin ...

## NeTraMet

UREC

- netramet est assez comparable à nnstat...
- la syntaxe du fichier de configuration est franchement ésotérique !
- pas d'outils d'analyse

=> On peut oublier ce produit...



## Netman (1)

UREC

Netman est composé de 3 modules:

- Etherman
  - Visualise la matrice instantanée du trafic
  - Fournit des statistiques sur ces flux
- Interman
  - Visualise les sessions simultanées entre machines de plusieurs réseaux
  - Permet de voir les concentrations de connexions

## Netman (2)

UREC

- Packetman
  - Capture des paquets et analyse
  - Filtres

## Internet Rover

UREC

Ensemble de fonctions permettant :

- surveiller la présence des équipements sur le réseau (ping)
- de vérifier la disponibilité des services
  - (messagerie, service de noms, ftp ...)
- Log des évènements

Fonctionne en mode console ou fenêtre X11

## MIT SNMP toolkit

UREC

- Kit de développement SNMP fournit :
  - snmpd et snmptrapd
  - snmpget, snmpset, snmpgetnext et snmptrap
- Applications graphiques :
  - map (sur X11) dessin d'un réseau sans interactivité
  - xsnmp:
    - » Représentation graphique d'un réseau hétérogène
    - » Couleur des liens en fonction de leur BP
- Facile d'utilisation

## CMU SNMP(1)

UREC

- Kit de développement SNMP, contient les primitives :
  - snmpget, snmpset, snmpgetnext et snmptrap
  - snmptrapd, snmpd
  - snmpstatus et snmptest => récupérer l'état d'un agent.

## CMU SNMP(2)

- **LAPP_SNMP : sur-ensemble pour rendre CMU plus facile à utiliser.**

  **Fournit les primitives :**
  - **lapp_snmp_get**
  - **lapp_snmp_set**
  - **lapp_snmp_getNext**



## Récapitulatif

| | | | |
|---|---|---|---|
| SunNet Manager | Admin Rés | Sun, HP + ? | Bsd + Solaris |
| HP Openview | Admin Rés + Anal | HP, Sun | Syst V |
| NetView 6000 | Admin Rés | Risk 6000 | Syst V |
| Spectrum | Admin Rés | Sun, HP, ... | Syst V + Bsd |
| SNMPc | Admin Rés | PC | DOS / Windows |
| | | | |
| Snoop | Admin Rés + Anal | std | Solaris |
| Etherfind | Admin Rés + Anal | std | SunOS 4.x |
| | | | |
| Ttcp | Perf | DP | |
| Tcpdump | Admin Rés + Anal | DP | Bsd |
| Nnstat | Stat | DP | Bsd + Solaris |
| Netman | Admin Rés + Anal | DP | Bsd |
| InetRover | Admin Rés | DP | Bsd + Solaris ? |
| | | | |
| MIT snmp | Admin Rés | DP | Bsd + ? |
| CMU snmp | Admin Rés | DP | Bsd + BSDi |