Calcul du trafic IP

Amirouche AITSAIDI, aitsaidi@inrets.fr

Octobre 1995

1 Introduction

La maîtrise et la consolidation du réseau constituent un objectif important pour une entreprise. Il faut mesurer les performances du réseau, les temps de réponse, la satisfaction des utilisateurs ; il faut planifier l'évolution de la croissance des besoins, anticiper les changements d'architecture nécessaires, surveiller l'évolution des coûts : ces tâches sont celles de l'administrateur de réseaux. Il dispose pour ce faire de nombreux outils plus ou moins automatisés.
L'application que j'ai réalisé permet à l'administrateur de connaître l'utilisation d'un réseau (réseau public par exemple) par les sites et les sous-réseaux qu'il a en charge, pour des buts de facturation, de gestion (détection d'anomalies), analyse du dimentionnement des différentes branches d'accès au réseau (débit nécessaire, ...), contrôle de flux ou autre. L'objet de l'application est de calculer la part de trafic qui transite par le routeur (qui est le point d'accès au réseau par les différents sites) :

- flux global ;
- part de trafic de chaque sous-réseau (donc de chaque site) ;
- consommation des protocoles applicatifs (différents services) ;
- etc ...

Pour réaliser cette application, on a besoin des informations suivantes pour chaque paquet qui passe par le routeur :

- taille du paquet,
- type du protocole niveau 3 (IP ou autre),
- type du protocole niveau 4 (TCP, UDP ou autre),
- adresses source et destination,
- ports source et destination (permettent de savoir le service utilisé).

2 Réalisation

Pour écrire l'application, deux solutions sont importantes à étudier :

1. Utiliser les informations que détient le routeur, ces informations sont décrites dans des MIB (Management Information Base). La récupération des informations passe par l'utilisation du gestionnaire de surveillance réseau SNM (SunNet Manager). SNM est bâti sur un modèle gestionnaires-agents. Les informations collectées (objets de gestion) sont stockées dans une base de données MIB. L'utilisation d'un agent SNM permet d'accèder à la MIB et de récupérer des informations sur le trafic qui transite par le routeur.

2. Placer un PC (ou une station) entre le routeur et le réseau pour capturer tous les paquets qui passent par le routeur. La capture d'un paquet permet de consulter son en-tête (adresse source, adresse destination, port source, port destination etc...), et permet de réaliser l'application.

Après étude des deux méthodes :

– L'agent SNM ne donne que la taille du paquet et les adresses source et destination (informations insuffisantes pour réaliser l'application).

– Même l'utilisation d'une **rmon MIB** (MIB particulière) n'est pas une solution intéressante pour réaliser cette application, car il y a une rapide saturation des buffers internes et elle permet de capturer les paquets sur le réseau mais seulement toutes les 5 secondes (perte énorme de paquets), qui est une contrainte liée à l'utilisation des sondes. Le but de la rmon MIB est de mettre à la disposition des administrateurs réseaux un moyen pour interfacer par SNMP (donc à distance) les actions d'écoute du réseau (statistiques ou capture de paquets) qu'il est possible de faire effectuer à un analyseur de réseau. Cette MIB est l'une des plus complexes développées à ce jour. Sa mise en œuvre nécessite des ressources importantes tant matérielles (mémoire, cache, CPU, ...) que logicielles (code pour traiter les requêtes).

D'où l'utilisation de la première solution pour réaliser l'application.

2.1 Utilisation d'un PC

La première solution est de mettre un PC entre le routeur et le réseau en question pour capturer les paquets qui transitent par ce routeur. Les moyens utilisés pour ce traitement sont les suivants :

– **Un PC**.

– **Carte ETHERNET** pour le PC.

– **Analyzer** : un logiciel pour PC récupéré sur le ftp anonyme *"mojo.ots.utexas.edu"*, dans le répertoire *"/pub/netinfo/src/pc_analyzer"*.

– **NE2100** un driver de paquet NCSA, un logiciel qui permet à analyzer d'accéder à la carte ETHERNET. Ce driver est disponible via le ftp anonyme *"sun.soe.clarckson.edu"* dans le répertoire *"/pub/packet-drivers"*.

Les étapes de calcul du trafic :

1. **Première étape :** Le programme *"analyzer"* est lancé sans arguments pendant une durée de temps donnée (avant saturation disque), avec une redirection des données vers un fichier au lieu de la sortie standard. Par exemple :

   analyzer > *analyzer.out*
   "analyzer" sauvegarde dans un fichier les en-têtes (sous un format particulier) de tous les paquets qui passent sur la ligne Ethernet surveillée.

2. **Seconde étape :** Le fichier *"analyzer.out"* est exploité hors-ligne par un programme *"count"* qui calcule le trafic :

   – IP ;
   – TCP, UDP ou ICMP;
   – des protocoles applicatifs ;

   de chaque site et de chaque sous-réseau appartenant aux sites.

2.2 Utilisation d'une station

La capture des paquets est faite par une station en utilisant par exemple le mécanisme du STREAM (ouverture d'un flux entre le driver Ethernet et le processus utilisateur pour récupérer les trames Ethernet). Il existe des outils du domaine public qui permettent de réaliser des captures sur le réseau : SNOOP, ETHERFIND, ...

Contrairement au PC, le traitement est réalisé en parallèle, deux processus tournent en parallèle et communiquent entre eux par un tube nommé :

– Le premier réalise la capture des paquets et redirige le résultat vers un tube nommé ouvert en écriture.

– Le second lance le programme **"count"** qui réalise le même traitement que celui utilisé avec *"analyzer"*, la différence c'est que les données sont récupérées à partir d'un tube nommé ouvert en lecture, donc le format des messages n'est pas le même.

2.3 Comparaison des 2 utilisations

Les traitements qui sont faits dans les deux cas reposent sur la structure des messages envoyés (qui est différente) par les programmes :

– **"analyzer"** pour le PC.

– **"capture"** (SNOOP ou autre) pour la station.

2.4 PC

– La sauvegarde est faite dans un fichier jusqu'à saturation disque, donc il y a des sauvegardes par morceaux et traitement après chaque sauvegarde.

– La simplicité d'utilisation, car il suffit d'avoir une carte Ethernet et d'installer le driver de paquet ne2100.

2.5 Station

– Le traitement est fait en parallèle alors pas de sauvegarde dans un fichier et pas d'arrêt pour saturation de disque.

– L'utilisation est plus complexe car la station doit seulement se contenter de recevoir des données (tuer tous les démons qui émettent sur le réseau), et il faut que la station ait son propre disque.