Administration de réseau : Outils publics et commerciaux

Christian LENNE, Christian.Lenne@grenet.fr
CICG, Grenoble

Nous présentons les solutions mises en œuvre sur le campus grenoblois pour la surveillance de la dorsale du réseau inter universitaire. Celle-ci nécessite la mise en place d'indicateurs différents en fonction des points et des matériels surveillés. Ces indicateurs sont fournis par des composants de plates-formes commerciales (SunNet Manager et CWSI) ou d'outils du domaine public (MRTG, Iptrafic, BigBrother). Nous définissons les indicateurs qui nous ont semblé pertinents pour une surveillance au jour le jour et nous montrons les liens à établir entre certains indicateurs pour mettre en évidence rapidement des dysfonctionnements sur le réseau. Enfin, nous présentons l'outil en cours de développement permettant, à partir d'une description de site, de générer le tableau bord associé.

Contexte

Le Centre Inter universitaire de Calcul de Grenoble a en charge le réseau fédérateur Grenet qui interconnecte les réseaux de quatre établissements universitaires de l'Académie de Grenoble. Ce réseau assure la connexion à Renater et l'interconnexion des campus. Il véhicule uniquement du protocole IP, soit sur une infrastructure de type Ethernet commuté, soit sur une infrastructure de type ATM. Nous proposons de faire un état des outils de surveillance utilisés par l'équipe réseau du CICG.

Il s'agit d'outils commerciaux (une plate-forme SunNet Manager, la plate-forme CWSI de Cisco) et d'outils du domaine public comme MRTG, Iptrafic ou BigBrother. Ces outils offrent des fonctionnalités complémentaires et permettent de surveiller des paramètres différents du réseau.

Nous avons regardé les réponses aux problèmes de suivi d'un réseau à grande échelle qui sont fournies par chacun des outils. Nous les avons placés de façon pragmatique à différents points du réseau pour surveiller les paramètres vitaux de ces points précis. Cette approche nous a conduit à développer une couche au-dessus de MRTG pour construire des tableaux de bord, adaptés à notre réseau et accessibles aux différents intervenants sur le réseau. Ces indicateurs répondent au besoin de suivi du réseau au jour le jour. Nous travaillons actuellement à la généralisation de notre approche en paramétrant cette couche pour utiliser l'outil sur les différents sites grenoblois que nous administrons.

Ces tableaux de bord, basés sur des pages HTML, mettent en relation visuelle des indicateurs (charge CPU, collisions, nombre de requêtes SNMP…) pour des routeurs et commutateurs. Ces tableaux de bords permettent (et ont permis) de mettre en évidence rapidement des anomalies sur le réseau (attaques, problèmes de routage, saturations de liens, défaillance de cache…).

Outils utilisés

A l'origine, la surveillance du réseau Grenet était basée sur la plate-forme d'administration SunNet Manager et sur Netscout Manager, outil spécialisé dans le pilotage de sondes matérielles Frontier. L'utilisation de ces logiciels a été peu à peu complétée par la mise en place d'outils d'administration du domaine public. Nous donnons ici les principales caractéristiques de ces différents outils.

Outils du domaine public

La surveillance des routeurs et du trafic de notre réseau se fait à l'aide des outils Iptrafic pour ce qui concerne le trafic entrant et sortant de Renater et de MRTG pour la surveillance des équipements actifs du réseau. Les serveurs qui supportent les services réseaux sont quant à eux suivis par Big Brother. Nous donnons dans les sections suivantes une rapide description de ces outils.

Iptrafic

Iptrafic est un outil développé par le CRU et se comporte en analyseur de réseau. Il capture toutes les trames IP pour en extraire et stocker le début de la trame : adresses IP, ports… Ces données sont stockées dans un journal et récupérées régulièrement par un client. Ce client synthétise ensuite ces informations suivant certains critères : volumétrie du trafic entrant ou sortant, volumétrie par machine, volumétrie par type de protocole… Ces synthèses sont ensuite présentées sous forme de camemberts, d'histogrammes ou de tableaux.

Iptrafic est un outil robuste, bien adapté à la surveillance d'un point d'entrée de site. Il est très précieux en aval du routeur d'entrée pour détecter les tentatives d'intrusions filtrées généralement sur l'équipement. Il nécessite toutefois la connaissance de la structure de l'outil pour développer des scripts d'extraction de données adaptés au site.

MRTG

C'est un outil simple d'utilisation qui permet de mettre en place rapidement, sur un serveur Web, les courbes de trafic sur les différentes interfaces d'un routeur Cisco. Il est écrit en Perl et utilise les MIBs publiques.

La mise en place de mesures se fait en deux temps. Dans une première étape, on crée des fichiers de configuration pour chaque équipement à surveiller. Pour cela une commande simple est fournie. Puis ce fichier est réutilisé régulièrement dans un « cron » pour mettre à jour les images gif créées. Un exemple de courbe est donné dans la section 4.

Big Brother

Très simple à configurer, Big Brother est plus destiné à surveiller des systèmes ou des services réseaux. Il remonte des alarmes sur des seuils ou sur l'absence de réponses d'un composant de l'équipement surveillé. Il mémorise l'historique des différents problèmes survenus. Nous donnons ici un exemple de configuration tiré du manuel.

```
# BIG BROTHER HOSTS FILE
   204.101.110.102 solario4  # ftp smtp pop3
   204.101.110.95 admin      # http://admin/
   204.101.110.108 ctnet
```

Dans cette configuration, on demande à BigBrother de surveiller les services ftp, messagerie et pop3 supportés par la machine solario4. Le serveur Web supporté par admin doit être surveillé en tentant de récupérer l'URL http://admin/. Enfin, on vérifie que la machine ctnet est bien active.

Outils commerciaux

SunNet Manager

C'est une plate-forme vieillissante qui donne entièrement satisfaction pour l'utilisation que nous en faisons, à savoir : la cartographie du réseau, la gestion des remontées d'alarmes et la génération de requêtes SNMP.

Le plus gros reproche que nous faisons aux plates-formes d'administration de réseau est leur complexité de mise en œuvre. Le changement d'outil nécessite, outre l'investissement financier, un lourd investissement humain pour leur mise en œuvre et pour les exploiter au maximum de leurs possibilités. Leur complexité rend également difficile leur évaluation avant achat.

CWSI

C'est un ensemble d'outils fourni par Cisco pour la configuration et le suivi du matériel de même marque. Il permet de configurer les réseaux virtuels (Vlan Director), d'exploiter les sondes de fond de panier des commutateurs (Traffic Director) et de configurer les équipements (Cisco View). Ces outils s'intègrent parfaitement dans une plate-forme d'administration comme SunNet Manager.

Dans cette batterie d'outils nous utilisons essentiellement Traffic Director qui nous permet de suivre également nos sondes Frontier. La stabilité des réseaux virtuels fait que Vlan Director est peu utilisé sauf pour cartographier le réseau sous cet aspect.

L'apport essentiel de Traffic Director est une prise en charge assez rapide de l'outil et une visualisation agréable des indicateurs observés. Toutefois, il est plus adapté à une surveillance « temps réel » qu'à un suivi régulier dans le temps comme l'offre MRTG. La figure 1 nous montre un exemple de graphique de suivi d'un commutateur.

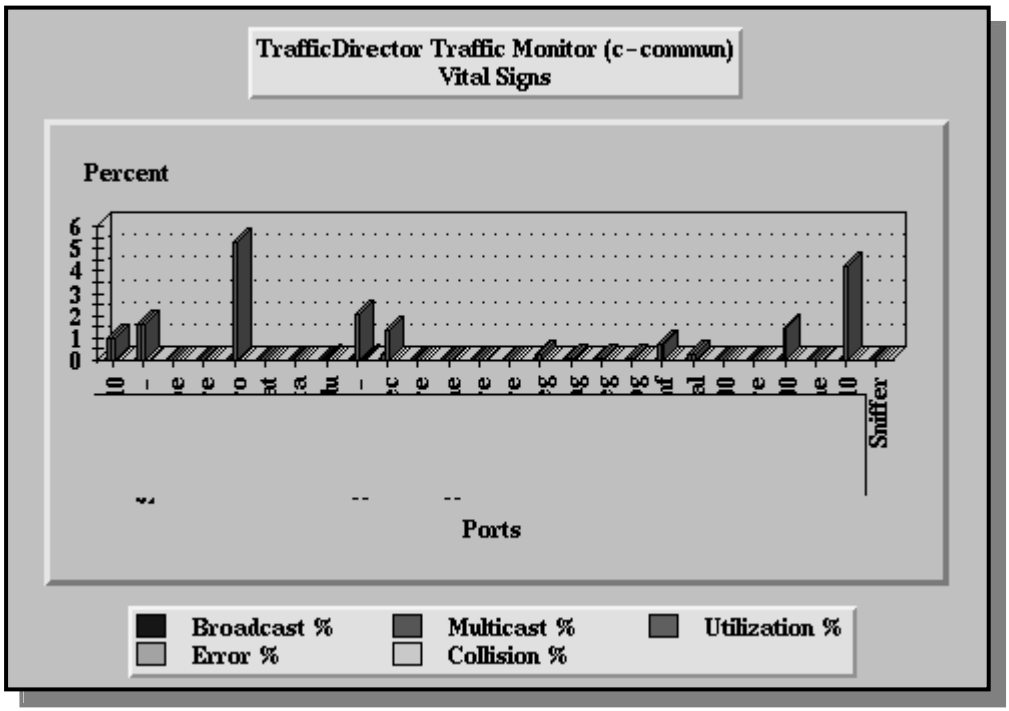

Figure 1. Suivi d'un commutateur sous Traffic Director.

■ Les matériels et services réseau surveillés

En fonction des points et des équipements, nous surveillons des indicateurs importants pour le suivi et l'évolution du réseau. Ainsi, la connexion à Renater nécessite une surveillance particulière, d'une part parce qu'un grand nombre d'utilisateurs en dépend, d'autre part pour prévenir les saturations de ce point. Enfin, ce lien demande une vigilance particulière au niveau de la sécurité, car une grande partie des intrusions passent par-là. Nous surveillons également l'adéquation du matériel qui assure la connexion physique de cet accès en mesurant, par exemple, la charge du CPU ou la gestion des tampons.

En liaison directe à cet équipement, un cache WEB est en place. Nous sommes amenés à le surveiller de près, car un passage forcé des requêtes par le cache est mis en place. Nous devons donc assurer que ce dernier est opérationnel, sous peine de couper pour tout un campus, l'accès à Internet.

Enfin, les commutateurs Ethernet sont surveillés pour mesurer la charge de chaque lien et caractériser le trafic.

Côté dorsal ATM, notre culture dans ce type de réseau étant plus jeune, nous nous bornons actuellement à surveiller quelques indicateurs liés essentiellement à la volumétrie par chemin virtuel et à la qualité de service sous l'angle acceptation/rejet de cellules ATM.

Les dorsales Ethernet et ATM sont constituées en très grande partie de matériel de marque CISCO. Dans un souci de portabilité et de généralité, nous avons essayé d'exploiter au maximum les informations de la partie publique des MIB. Toutefois, et particulièrement pour la partie ATM, nous avons été amenés à rajouter des indicateurs de la MIB privée.

Pour tout ce qui est service réseau, nous utilisons des serveurs Unix. Ceci couvre, soit des services supportés par des matériels SUN sous Solaris, soit par des matériels spécialisés et pilotés par des Unix « libres » comme FreeBSD ou Linux.

La figure 2 met à évidence les composants sous surveillance et les outils utilisés pour ce faire.

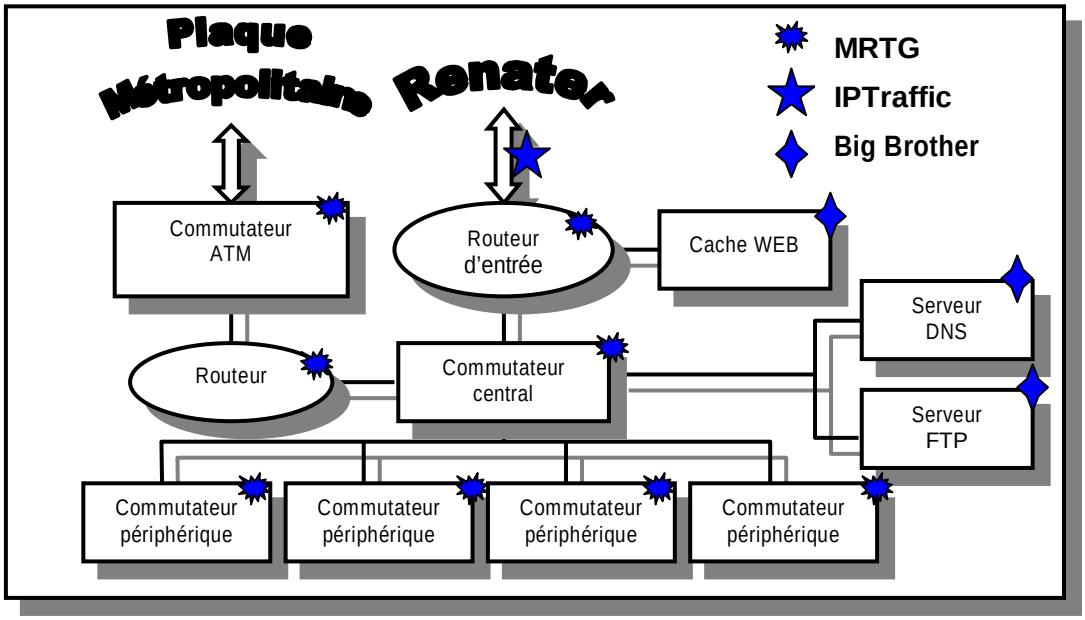

Figure 2. Points surveillés et outils utilisés.

■ Indicateurs mis en place

Les indicateurs de l'état du réseau sont disponibles sur un serveur WEB du centre et servent à deux types de population. Le premier est constitué des utilisateurs du réseau. Ces derniers doivent avoir accès aux mesures touchant la volumétrie du trafic entrant et sortant sur Renater. Une courbe simple et à jour, ne nécessitant pas d'information particulière quant à son interprétation est fournie. Le second type de population est constitué des équipes réseau des Centres de Ressources Informatiques des établissements. Nous leur fournissons des éléments plus précis concernant leur trafic spécifique ainsi que des informations sur les équipements de la dorsale. Ces informations sont données sous forme de tableau de bord.

Notion de tableaux de bord

Nous appelons « tableau de bord » un ensemble de courbes ou de valeurs visualisées sur une même page WEB afin d'être interprétées simultanément, dans le but de mettre en évidence une anomalie sur le réseau. Cette page est également agrémentée d'images ou de textes situant les indicateurs, ainsi que d'une image « cliquable » permettant de se déplacer dans le réseau. Chaque courbe donne accès à un autre tableau de bord qui permet d'affiner l'analyse pour valider ou réfuter les premières suppositions. Ainsi, nous avons pu mettre en évidence des intrusions sur notre site et un problème de sous dimensionnement d'un lien dont l'effet se propageait sur la dorsale.

Page principale

La page d'accueil présente la courbe du trafic Renater en entrée et en sortie. Sous cette courbe un ensemble de pointeurs vers les autres indicateurs est proposé : cache WEB, éléments actifs de la dorsale, informations particulières… Cette page est accessible par tout le monde et permet de se faire une idée du trafic instantané.

Point d'entrée Renater

La figure 2 nous montre les outils utilisés pour la surveillance de ce point. Nous ne reviendrons pas sur toutes les informations que nous donne Iptrafic, mais nous présentons simplement les indicateurs choisis pour surveiller l'équipement lui-même. Ces indicateurs produits par MRTG sont intégrés dans une page mettant en corrélation des informations concernant le volume de trafic entrant et sortant, la charge CPU du routeur et le nombre de collisions sur une liaison de desserte sensible. La figure 3 nous donne une image de ces indicateurs qui semblent montrer une anomalie réseau entre 3 et 4 heures du matin (pics en milieu de courbe). L'analyse plus détaillée des données nous a montré qu'il s'agissait d'une attaque venant de l'extérieur. La machine relayant l'attaque a pu être localisée à partir des informations relevées par Iptrafic.

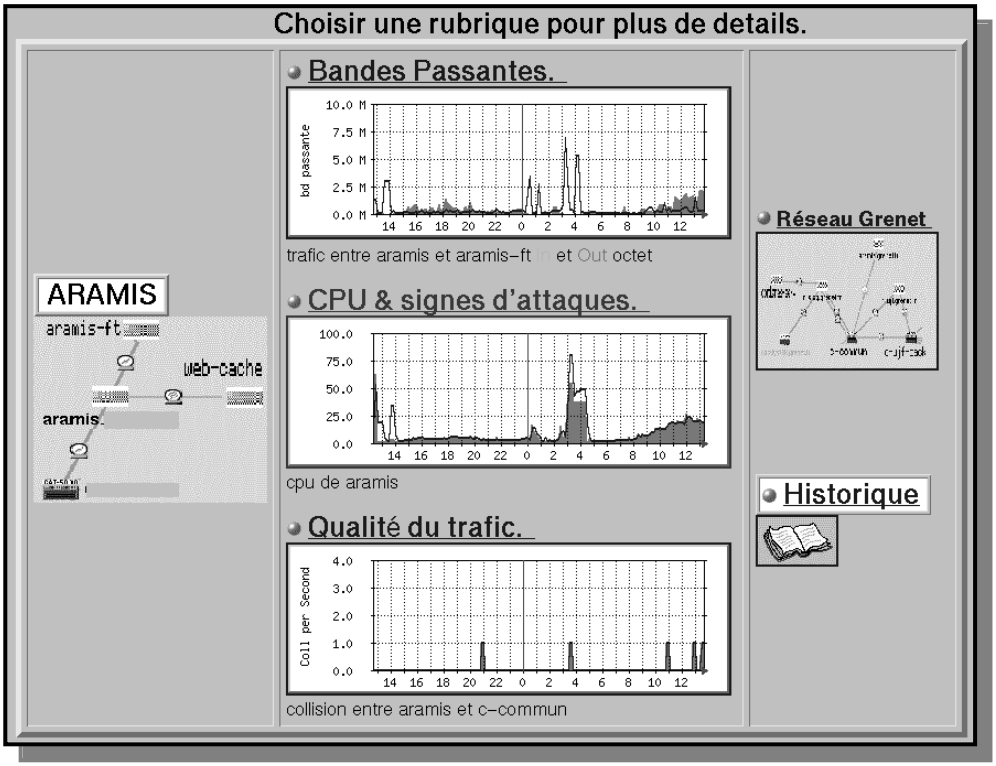

Figure 3. Surveillance du routeur d'entrée de site.

Le graphique associé à la bande passante nous permet de visualiser un tableau de bord plus précis de cette bande passante. En effet, nous visualisons le temps nécessaire au transit d'un paquet, le trafic sur le lien entre le cache Web et le routeur, le total cumulé de trafic entrant et sortant. La qualité du trafic est, quant à elle, évaluée sur des critères comme le nombre total de paquets circulants, le nombre de paquet « multicast » et « broadcast », ainsi que des graphes associés au nombre de collisions, de paquets erronés (taille trop petite, taille trop grande…) et le nombre de paquets rejetés.

Enfin, la courbe « CPU & signes d'attaques » nous fait pointer vers le tableau de bord qui permet de vérifier l'adéquation du matériel à la fonction assurée, en particulier sa capacité CPU et sa capacité mémoire. Ce dernier élément est donné par le pourcentage des tampons libres et par le nombre de paquets rejetés. Enfin, deux courbes nous donnent des informations sur la sécurité : le nombre d'ICMP adressés au routeur ainsi que le nombre de requêtes SNMP.

Tous les tableaux de bord que nous venons de décrire peuvent être déployés pour les routeurs de la dorsale.

Commutateurs

Les commutateurs de cœur de réseau sont suivis par des tableaux de bord spécifiques. La figure 6 nous montre les éléments qui y figurent. Outre quelques courbes qui permettent de surveiller l'équipement, les différents liens partant de ce commutateur font l'objet de tableaux de bords spécifiques. Ces tableaux de bord permettent de caractériser le trafic, tant sur le plan de la volumétrie que sur la caractérisation des échanges transitant sur le lien.

Enfin, les tableaux de bord des commutateurs d'extrémités se réduisent aux simples courbes fournies directement par MRTG.

■ Couche d'intégration

Comme nous l'avons dit en introduction, nous avons développé une couche au-dessus de MRTG écrite en langage de commande pour générer les fichiers de configuration et les « cron » nécessaires à la collecte des données. La première version de ce système nous a permis de définir un langage très simple permettant de décrire en quelques lignes les différents éléments à surveiller. Un « compilateur » de ce langage en cours de mise au point va nous permettre de générer des tableaux de bord pour tous les sites que nous administrons tant pour les dorsales Ethernet qu'ATM. Nous travaillons également sur un outil graphique permettant de décrire le réseau. L'architecture de notre système est donnée en figure 4.

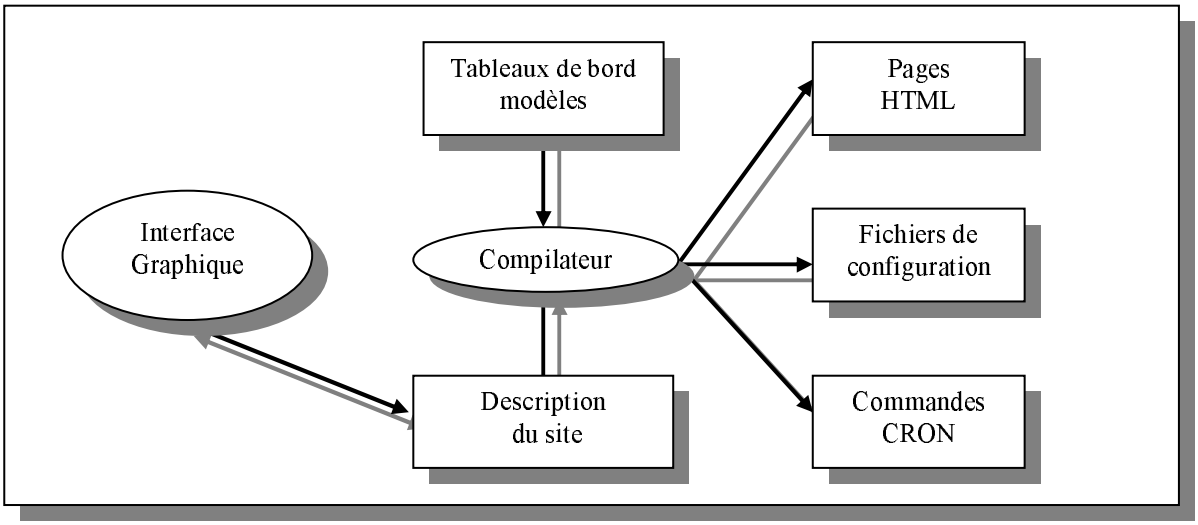

Figure 4. architecture de la couche d'intégration.

■ Conclusion

La surveillance de grosses dorsales de réseaux nécessite la définition d'indicateurs permettant de suivre le comportement du réseau. Ce suivi est particulièrement important pour détecter ou prévenir les incidents sur la dorsale ou mettre en évidence les intrusions. Ces indicateurs peuvent être fournis, soit par des outils du domaine public, soit par des plates-formes commerciales. La plus grosse difficulté est de sélectionner les bons indicateurs et de les corréler de façon significative. Les trois outils que nous utilisons au CICG nous paraissent suffisants pour la supervision d'un gros « backbone » comme celui du campus de Saint Martin d'Hères et des services réseau standards qui sont fournis. Ces outils ont l'avantage d'être simple d'utilisation et disponible sur différents systèmes. Néanmoins, les plates-formes commerciales offrent des fonctions intéressantes de gestion de l'infrastructure et par-là même des outils permettant de faire de la cartographie. Les outils commerciaux testés ne nous ont pas convaincus quant à l'apport d'éléments de supervision de réseau, ceci en comparaison avec les outils en libre diffusion et de SunNet Manager.

La surveillance d'un réseau nécessite la surveillance très régulière des indicateurs. On s'aperçoit que les courbes sont toujours identiques sauf bien entendu lors de dysfonctionnement ou d'intrusion. Dans ce cas, la ou les personnes qui suivent le réseau ne peuvent pas passer à côté de ces informations. Reste alors le difficile travail de localisation précise du problème qui nécessite souvent l'utilisation d'un analyseur de réseau ou le traitement particulier des données d'Iptrafic.