

Gestion et surveillance de réseaux

Préparé par Alberto Escudero Pascual/ IT +46

<aep@it46.se>

But

- Nous devons savoir ce que nous voulons pour savoir ce dont nous avons besoin
- Est-ce que la gestion et la surveillance sont la même chose?
- Ne suivez pas les outils! Suivez les méthodes!

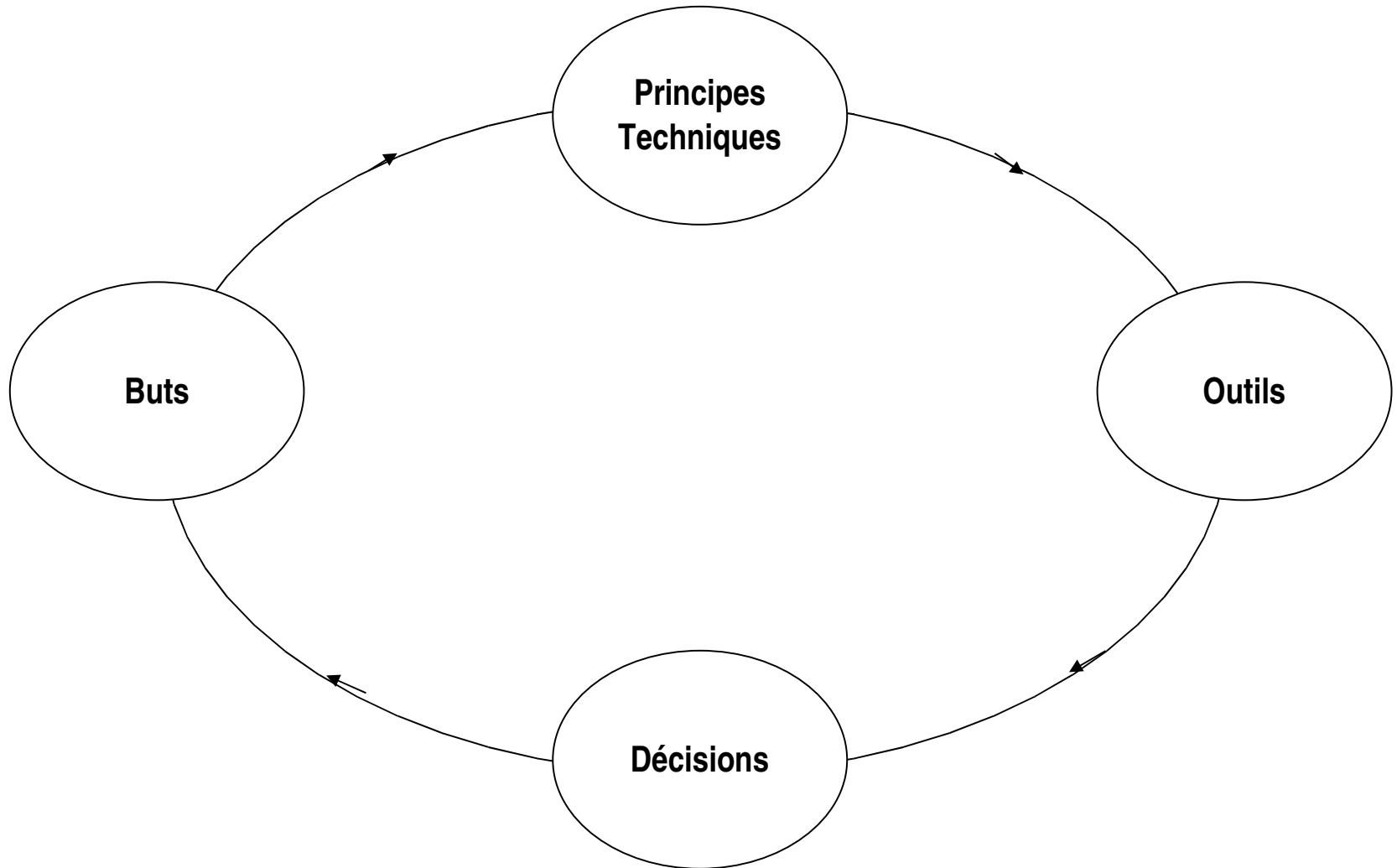
Comment?... Méthodologie

- Focus sur les buts, pas sur les outil
- Comprendre les princies techniques derrière les outils
- Comprendre de quels principes techniques nous avons besoin pour arriver à nos bus
- ... finalement, nous traiterons de quelques outils!

Table des matières

- Buts vs surveillance des données
- Surveillance des services pour l'atteinte des buts
- Principes techniques
 - SNMP/MIB
 - Comptage du trafic
 - Organisation du trafic
 - Filtres Bayesiens
 - Empreintes de Virus
- Outils
 - MRTG, Ntop, SpamAssassin, Clam AV

Buts vs surveillance des données



- Surveillance des services pour l'atteinte des buts

Trois exemples:

- Épargnez en réduisant les coûts de bande passante internationale
- Fournir un meilleur service qualité-prix pour les services VoIP
- Gérez le service et la grandeur du réseau

But 1: Épargnez des coûts de bande passante internationale

<i>Layer</i>	<i>Technical principle</i>
4	Caching, Detect/Block Spam/Viruses (Bayesian Filters)
3	Traffic shaping (Queueing Principles) Traffic accounting (SNMP, Promisc.)
2	Network Access Control (Firewalling) Traffic shaping Traffic accounting (SNMP, Promisc)
1	Wireless Access Control Collect Wireless Layer-2 Data (SNMP)

But 2: Fournir un service de meilleure qualité sur VoIP

<i>Layer</i>	<i>Technical principle</i>
4	
3	Traffic shaping (Queueing Principles) Traffic accounting (SNMP, Promisc)
2	Traffic shaping (Queueing Principles) Traffic accounting (SNMP, Promisc)
1	Collect Layer-2 Data (SNMP) Reduce wireless latency

But 3: Gestion du service et croissance du réseau

<i>Layer</i>	<i>Technical principle</i>
4	Virus/Spam, SQL (Service Balancing)
3	Collect TCP/UDP Statistics, Firewall Balancing
2	Collect IP Layer Statistics, Routing principles
1	Collect Layer-2 Data (SNMP)

Principes techniques

Five technical principles:

- SNMP/MIB
- Comptage du trafic
- Organisation du trafic
- Filtres Bayesiens
- Empreintes de virus

SNMP/MIB

- un protocole de maintenance conçu spécialement pour les réseaux d'ordinateurs et les réseaux d'équipements individuels.
- Architecture serveur/client
- Les Clients font des requêtes aux équipements éloignés dans le réseau
 - Information statistique , données privées
- Un équipement SNMP contient un base de données statistique (MIB)
- Compatibilité et capacité d'être étendu
 - règles du code très complexes, code inéficace

SNMP/MIB

1. SNMP représente aussi du trafic sur votre réseau. Essayer de diminuer le total en faisant de petites requêtes.
2. SNMPv1 ne permet pas un cryptage pour l'identification. Rappelez-vous de vos mots de passe.
3. SNMP consomme des cycles processeurs sur vos unités de réseau

SNMP/MIB



- Les vendeurs des équipements sans fil fournissent normalement aux acheteurs leurs propres outils de gestion qui utilisent SNMP pour communiquer avec les équipements sans fil.
- L'intégration de différents outils propriétaires de gestion est normalement très compliquée puisque le code varie passablement du logiciel libre.
- La meilleure option est probablement d'écrire votre propre système de gestion sans fil.

Comptage du trafic

une technique générale pour faire le surveillance des statistiques de trafic dans les réseaux d'ordinateurs

- Décisions sur le réseau
- Solutionner les problèmes
- Surveiller les activités de hôtes

Comptage du trafic

- Le comptage de bits et de paquets
- Les statistiques de distribution des protocoles (type, temps, %)
- Les erreurs des vérifications IP
- La découverte d'hôtes actifs
- L'activité des données entre les hôtes

Comptage du trafic

Actif:

Rend possible SNMP dans tous les routeurs et les passerelles du réseau

Passif:

Mode sous - écoute

requiert d'échanger du trafic SNMP avec les routeurs et passerelles pour obtenir cette information.

Organisation du trafic

- Contrôle le flux du trafic
- Garantie une certaine performance
- Disciplines des queues dans la couche IP
 - Délai de transit et congestion
 - Bande passante et équité

Organisation du trafic



- Modification dans IEEE 802.11 de couche de contrôle d'accès au média dans les produits basés sur IEEE 802.1 pour mettre en oeuvre des mécanismes propriétaires qui n'Assure pas la compatibilité entre les vendeurs.
- Proxim lance un mécanisme propriétaire de sélection (WORP) donnant au réseau la permission d'utiliser des périodes de temps

Queues, discipline et délais de transit.

- S'applique sur le trafic sortant
 - Le sortant est généralement embouteillés
- Surcharge de la mémoire
 - Abandonner des paquets TCP ->Retransmission
 - Délai de transit
- Prioritisation of paquets
 - Interaction avec les usagers (ssh, rtp)
 - Bulk traffic (ftp, http)

Gestion de la bande passante par priorité de queues de paquets

Peut assurer:

- La qualité du service
 - A certain bitrate to a specific host
 - Limited throughput for a specific service
- Réseau équitable
 - Consommateurs reçoit ce pour quoi il paye

Gestion de la bande passante par priorité de queues de paquets

- Queues en disciplines de classe
 - Structure Hiérarchique
 - classes ayant des caractéristiques spécifiques : minimum et maximum de bande, algorithme de queue, etc..
- HTB (en classes)
 - Contrôle la bande passante en simulant des liens lents
- SFQ (sans classes)
 - Équité dans les liens surchargés

Filtres Bayésiens

- Un filtre anti-pourriel basé sur le contenu
 - Entête (envoyeur et chemin parcouru par le message)
 - Codes HTML intégrés (couleurs, etc.)
 - Le mariage des mots et des phrases
 - L'information globale
- Adaptif – self learning by error reports
- Liste mots nom manuel
 - Liste initial créée en analysant le contenu

Filtres Bayésiens



- Placez votre filtre anti-pourriel avant que le courrier n'entre dans l'infrastructure sans fil
- Placer le programme de gestion de votre courrier avec un anti-pourriel de l'autre côté de votre lien international peut amener une épargne de 10 à 20 % de la bande passante.

Empreintes des virus (signatures)

- Empreintes: Instructions spécifiques pour l'ordinateur que plusieurs Virus connus utilisent.
 - Utilise les empreintes pour balayer le code
 - Base de données constamment mises à jour
- Algorithmes à balayage heuristique
 - Créer des permutation de virus connus pour prédire les virus qui vont muer dans le futur

Outils de surveillance

Outils libres:

- MRTG
- Ntop
- SpamAssassin
- Clam Antivirus (Clam AV)

Surveiller le « sans fil »



- Des outils de surveillance spécifiques des vendeurs (pour certains systèmes d'opération)
 - Entraîne un usage limité
- N vendeurs impliques n outils de surveillance réseau
- Une seule interface par l'integration (SNMP/MIB -> MRTG)

MRTG

- Multi Router Traffic grapher
- Surveille et présente les paramètres du réseau (processeur, trafic)
- Utilise des données des équipements utilisant SNMP
- Interface Web graphique

MRTG

Configuration de MRTG:

- Pré-requis: server Web, MRTG installé, adresse IP et mot de passe SNMP de l'équipement que vous souhaitez surveiller
- 2. Créer un fichier de configuration pour MRTG (*avec cfmaker*)
- Créer un processus « cron » qui met en oeuvre MRTG

MRTG: Surveillance de la bande

1. Créer un fichier de configuration par défaut pour mrtg
> `cfgmaker password@IP > /etc/mrtg_b.cfg`

2. Changer le répertoire de travail de MRTG dans `mrtg_b.cfg`
`WorkDir: /var/www/mrtg`

3. Créer des tâches périodiques en ajoutant la ligne suivante dans `/etc/crontab`

```
*/5 * * * * root /usr/bin/mrtg /etc/mrtg_b.cfg
```

MRTG: Surveillance SN/R

- Besoin de données provenant des MIB des équipements sans fil
- Comment trouver la bonne requête (OID)?
 - **Reverse engineering!**
- Utilise un gestionnaire de réseau propriétaire pour surveiller le trafic (lien-test)

MRTG: Surveillance SN/R

```
19:41:21.448323 10.10.10.12.1260 > 10.10.10.254.snmp:
GetRequest(29) .1.3.6.1.4.1.762.2.1.7.0
0x0000  4500 0048 77b2 0000 8011 99d5 0a0a 0a0c      E..Hw.....
0x0010  0a0a 0afe 04ec 00a1 0034 64bb 302a 0201      .....4d.0*..
0x0020  0004 0670 7562 6c69 63a0 1d02 0201 0302      ...public.....
0x0030  0100 0201 0030 1130 0f06 0b2b 0601 0401      .....0.0...+....
0x0040  857a 0201 0700 0500                          .z.....
19:41:21.448854 10.10.10.254.snmp > 10.10.10.12.1260:
GetResponse(30) .1.3.6.1.4.1.762.2.1.7.0=2 (DF)
0x0000  4500 0049 0037 4000 4011 1150 0a0a 0afe
E..l.7@.@..P....
0x0010  0a0a 0a0c 00a1 04ec 0035 62b5 302b 0201      .....5b.0+..
0x0020  0004 0670 7562 6c69 63a2 1e02 0201 0302      ...public.....
0x0030  0100 0201 0030 1230 1006 0b2b 0601 0401      .....0.0...+....
```

Usagers connectés à l'AP

Write Integer 50 in OIDs:

1.3.6.1.4.1.762.2.5.5.1, 1.3.6.1.4.1.762.2.5.5.1,
1.3.6.1.4.1.762.2.5.5.3

Write Integer 3 in OIDs:

1.3.6.1.4.1.762.2.5.4.1, 1.3.6.1.4.1.762.2.5.4.2,
1.3.6.1.4.1.762.2.5.4.3

Retrieve the OID:

1.3.6.1.4.1.762.2.5.1.0

Paramètres de bruits et signal

Write Integer 1500, 25, 80 in OID

1.3.6.1.4.1.762.2.5.2.1.27.n

1.3.6.1.4.1.762.2.5.2.1.26.n

1.3.6.1.4.1.762.2.5.2.1.25.n

Retrieve signal by reading:

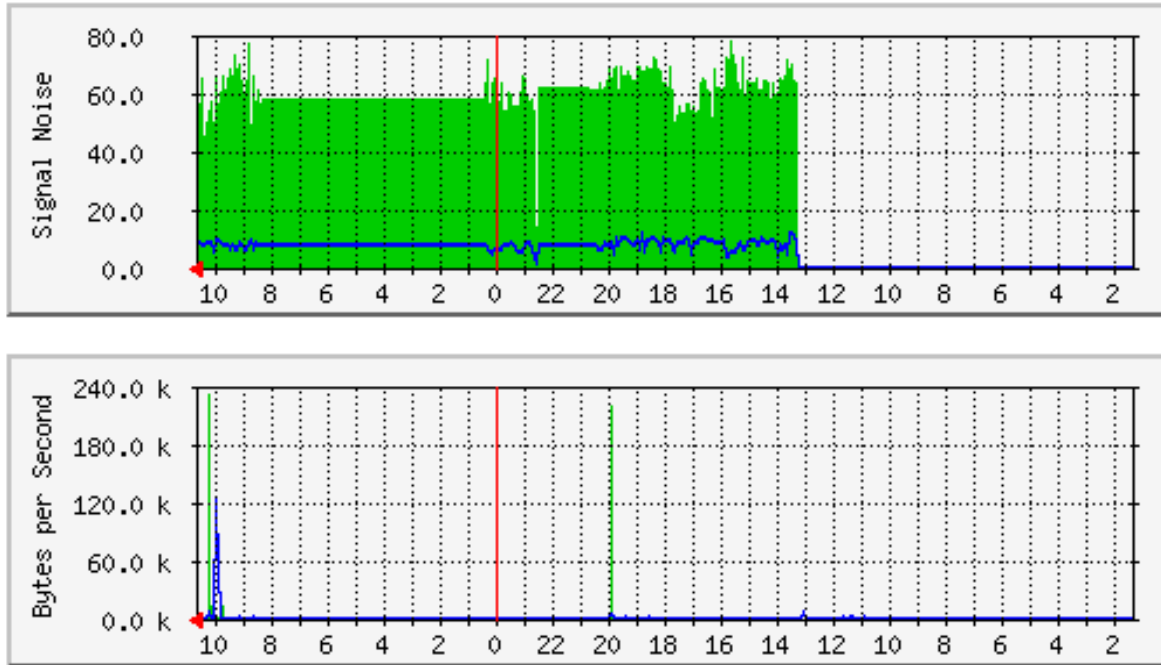
1.3.6.1.4.1.762.2.5.2.1.32.n

Retrieve noise by reading:

1.3.6.1.4.1.762.2.5.2.1.33.n

where <n> refers to the integer assigned to the wireless device

Le sans fil avec MRTG



MRTG - IP information (Layer 3) and wireless information (Layer 2)

Ntop

Logiciel libre (GPL)

- Mesures du trafic
- Caractéristiques du trafic et la surveillance
- Détection des violation de la sécurité du réseau
- Optimisation du réseau et planification

Les mesures du trafic

- Données reçues ou envoyées par protocole
- IP **multicast**
- Histoire de la session TCP
- Services TCP/UDP utilisés et distribution du trafic
- Utilitaires de bande passante (actuel, en moyenne, pointes)
- Distributions Trafic (dans les sous réseaux)

Caractérisation du trafic et surveillance

Identifier des situations où le trafic du réseau ne respecte pas les règles créées par l'administrateur du réseau:

- Adresses IP utilisées deux fois
- Usagers dont l'identifiant est mal configuré.
- mauvaises configurations des logiciels d'applications
- Mauvaise utilisation du service (proxy serveurs etc.)
- Utilisation excessive de la bande passante

Détection des violations de sécurité par Ntop

Détection des attaques telles que:

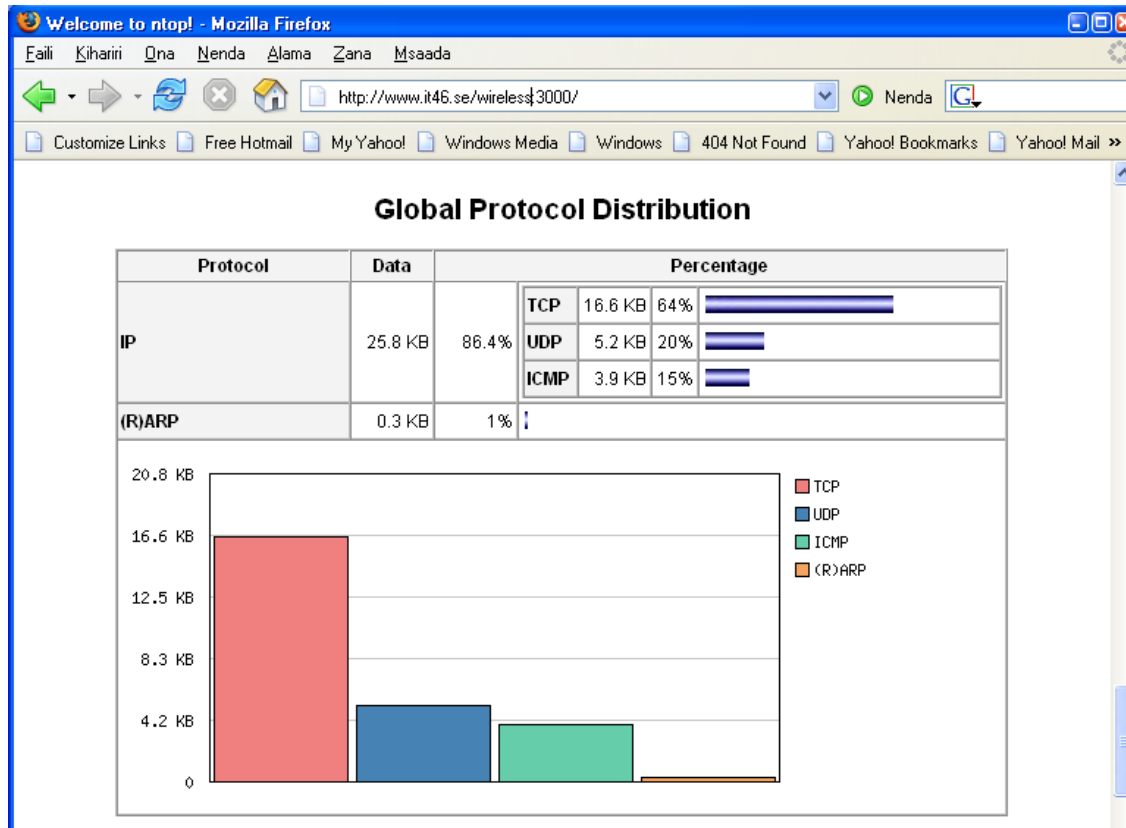
- Portscan
- Spoofing
- Espions
- Cheval de Troie
- Refus de service (DoS)

Optimisation du réseau et planification avec NTOP

Identifie les configuration sub-optimales et l'utilisaiton non efficace de la bande passante

- Protocoles non nécessaires
- Routage sub-optimal (redirige ICMP)
- Forme et distribution du trafic

Ntop



SpamAssassin

Pas un blocage, des étiquettes!

Donne chaque message une note basée sur:

- Test d'entête (envoyeur, champs sujet)
- Tests sur le corps du message avec un ensemble de règles de 3e part (mot de passe, code Html, adresse IP, URL)
- Filtre Bayésien
- Listes noire et blanche d'adresses
- Manuel de listes noire et blanche d'adresses
- Base de données collaborative d'identification des pourriels
- Listes de blocage de DNS blocklists « RBL=RealTime Blackhole Lists »
- Ensemble de caractères et locaux

Clam Antivirus

- N'élimine, ni ne renomme ni de nettoie un fichier infecté. Il détecte simplement et averti l'utilisateur.
- Balayage rapide et puissant des courriels et répertoires
- Détection de plus de 30000 virus, vers et cheval de Troie
- Balaie les archives et les fichiers compressés
- Mise à jour des base de données incluant les signatures digitales des virus et les requêtes sur les base de données DNS

Inonder le réseau

```
18:12:36.432838 172.168.0.36.2231 > 172.168.82.53.445: S 1068540375:1068540375(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 119f 4000 8006 3d7f aca8 0024   E..0..@...=...$
0x0010      aca8 5235 08b7 01bd 3fb0 a1d7 0000 0000   ..R5....?.....
0x0020      7002 faf0 f088 0000 0204 05b4 0101 0402   p.....
18:12:36.441460 172.168.0.23.1433 > 172.168.227.122.445: S 2018273998:2018273998(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 8a9c 4000 8006 3349 aca8 0017   E..0..@...3l...
0x0010      aca8 e37a 0599 01bd 784c 6ace 0000 0000   ...z...xLj....
0x0020      7002 faf0 60db 0000 0204 05b4 0101 0402   p...`.....
18:12:36.441731 172.168.0.23.1435 > 172.168.196.106.445: S 2018316905:2018316905(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 8a9d 4000 8006 5258 aca8 0017   E..0..@...RX....
0x0010      aca8 c46a 059b 01bd 784d 1269 0000 0000   ...j...xM.i....
0x0020      7002 faf0 d84d 0000 0204 05b4 0101 0402   p....M.....
18:12:36.443252 arp who-has 172.168.0.247 tell 172.168.0.27
0x0000      0001 0800 0604 0001 0006 5ba6 3815 aca8   .....[.8...
0x0010      001b 0000 0000 0000 aca8 00f7 0000 0000   .....
0x0020      0000 0000 0000 0000 0000 0000 0000   .....
18:12:36.445470 172.168.0.27.2367 > 172.168.160.143.445: S 767169456:767169456(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 3f8b 4000 8006 c141 aca8 001b   E..0?.@....A....
0x0010      aca8 a08f 093f 01bd 2dba 13b0 0000 0000   ....?-.....
0x0020      7002 faf0 41cd 0000 0204 05b4 0101 0402   p...A.....
18:12:36.447728 172.168.0.36.2235 > 172.168.217.194.445: S 1068598455:1068598455(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 11a0 4000 8006 b5f0 aca8 0024   E..0..@.....$
0x0010      aca8 d9c2 08bb 01bd 3fb1 84b7 0000 0000   .....?.....
0x0020      7002 faf0 8616 0000 0204 05b4 0101 0402   p.....
18:12:36.448124 172.168.0.36.2232 > 172.168.97.176.445: S 1068654094:1068654094(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000      4500 0030 11a1 4000 8006 2e02 aca8 0024   E..0..@.....$
0x0010      aca8 61b0 08b8 01bd 3fb2 5e0e 0000 0000   ..a.....?^.....
0x0020      7002 faf0 24d4 0000 0204 05b4 0101 0402   p...$......
```

But1: Épargnez des coûts de bande passante internationale

<i>Layer</i>	<i>Technical principle</i>
4	Caching, Detect/Block Spam/Viruses (Bayesian Filters)
3	Traffic shaping (Queueing Principles) Traffic accounting (SNMP, Promisc.)
2	Network Access Control (Firewalling) Traffic shaping Traffic accounting (SNMP, Promisc)
1	Wireless Access Control Collect Wireless Layer-2 Data (SNMP)

Conclusions

- La surveillance de données brutes n'aide pas!
- Vous devez surveiller pour avoir une bonne gestion de réseau
- Ayez des buts, trouvez le principe technique et choisissez votre outils.
- Si cet outil ne fait pas ce que vous voulez, ou est loin de faire ce que vous coulez, envisagez d'en construire un.