ITRAINONLINE MMTK

LA GESTION ET LA SURVEILLANCE DE RÉSEAUX

Préparé par : Alberto Escudero-Pascual <aep@it46.se>

Au sujet de ce document

Ces documents font partie du ItrainOnline MMTK. Le MMTK est un ensemble intégré de documents et de ressources de formation multimédia destiné à aider les médias communautaires, les centres multimédia communautaires, les télécentres et autres initiatives qui utilisent les technologies de l'information et des communications (TIC) à renforcer les communautés et soutenir le travail de développement.

Renseignements sur le droit d'auteur

Introduction

Faire le surveillance de divers aspects d'un système de télécommunication est une exigence minimale pour qui veut offrir un certain service. Savoir quelles sont les données valables et être capable de les recueillir à partir du système sont des pré-requis essentiels pour pouvoir prendre des décisions adéquates.

Malheureusement, les données elles-mêmes ne sont pas en mesure de résoudre votre problème. Les données ne sont pas nécessairement de l'information et avoir de l'information ne donne pas nécessairement la connaissance.

Un bon système de surveillance pour la gestion de réseau devrait :

- Recueillir l'information nécessaire du système
- Gérer et présenter ces données. Présenter différents niveaux de détails des données recueillis.
- Si cela est souhaité, prendre des décisions automatiques

C'est une erreur répandue dans le monde des fournisseurs de services Internet d'avoir une approche centrée sur un outil dans la prise de décision. Par exemple, lorsqu'un outil est mis en place dans un système de gestion de réseaux, toutes les décisions sont par la suite prises en fonction des possibilités techniques de l'outil et non plus en fonction de ce que sont les buts et priorités du fournisseur de services.

Cette unité choisit une approche centrée sur les buts pour la gestion de réseaux. À l'opposé d'une approche centrée sur l'outil, nous présentons ici une méthodologie qui commence par définir clairement les buts, lesquels nous servirons à choisir les bons outils.

Buts vs collecte de données

La principale et la plus importante chose qu'un fournisseur de services de télécommunication ou d'Internet doit considérer avant de mettre en place un outil de surveillance est de se demander quel but il veut atteindre et quels défis sont devant.

Avoir un but (1) représente nécessairement de réfléchir à quels (2) principes techniques sont requis pour acquérir l'information nécessaire sur le système. C'est en identifiant les principes techniques qu'il est possible de sélectionner certains outils (3). L'information fourni par l' outil nous donnera la connaissance nécessaire pour prendre une décision (4).

Buts ⇒ Principes techniques ⇒ Outils ⇒ Décisions

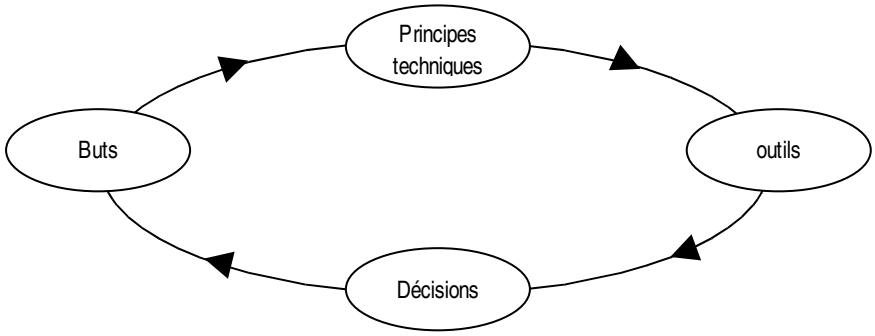

Image 1: Cette image montre la méthodologie centrée sur le but pour le surveillance (gestion de réseaux).

Surveillance des services pour l'atteinte des buts

De façon à faire la démonstration de cette approche méthodologique pour le surveillance, 3 buts différents buts vont être présentés, lesquels sont très communs dans la plupart des cas dans n'importe quel déploiement de réseau sans fil:

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

Les tableaux suivants vous montrent comment ces trois différents buts font usage des mêmes principes techniques et comment chacun d'eux requiert des informations de toutes les couches (modèle OSI) de notre système de communications.

Dans un réseau sans fil, comme dans tous les autres systèmes de télécommunication, les buts affectent normalement toutes les couches du modèle OSI. Pour assurer un bon service, il est nécessaire de comprendre plus que les aspects sans fil, il faut voir la communication comme un tout.

Épargnez des coûts de bande passante internationale

Couche	*Principes techniques*
Logiciel d'application	Intercepter, détecter, bloquer les Spam et les Virus (**Filtres Bayesiens**)
Transport	**Organisations du trafic (Principes de priorités)** **Comptage du trafic(SNMP, Promisc)**
Réseau	Contrôle d'accès au réseau (pare-feu) Organisations du Trafic Comptage du trafic (SNMP, Promisc)
Contrôle d'accès au Média	**Contrôle d'accès sans fil** Recueillir les données sans fil couche-2 (**SNMP**)

Fournir un service de meilleure qualité sur VoIP

Couche	*Principes techniques*
Logiciel d'application	
Transport	**Organisations du trafic (Principes de priorités)** **Comptage du trafic(SNMP, Promisc)**
Réseau	**Organisations du trafic (Principes de priorités)** **Comptage du trafic(SNMP, Promisc)**
Contrôle d'accès au Média	Recueillir les données sans fil couche-2 (SNMP) Diminuer le délais de transit

Gestion du service et croissance du réseau

Couche	*Principes techniques*
Logiciel d'application	Virus/Spam, SQL **(Service Balance du service)**
Transport	Recueillir les statistiques TCP/UDP, balance du Pare feu
Réseau	Recueillir les statistiques de la couche IP, **Principes de routage**
Contrôle d'accès au Média	Recueillir les données couche-2 (**SNMP**)

Ne pas être en mesure d'optimiser l'un ou l'autres des couches de protocole affectera la performance globale. Par exemple, un haut niveau de paquets corrompus dans le réseau aura un impact global sur la performance TCP et un long délai de transit sera perçu par l'usager qui utilise un logiciel d'application en temps réel.

La complexité ne vient pas seulement de la compréhension de chacune des couches de communication implique dans le système, mais aussi de comprendre les interrelations entre les deux.

Tout comme n'importe quel autre système de communication, créer un réseau sans fil n'est pas facile, mais créer un réseau sans fil avec une bonne performance nécessite temps et expérience. C'est le principe qui fait l'Internet aujourd'hui!

Principes techniques

Avant de discuter des outils disponibles pour le surveillance du réseau (et la gestion), les principes techniques derrière les outils seront expliqués. Certains principes techniques peuvent être utilisés pour arriver à différents buts. Les outils offrent normalement une sous-série de possibilités pour le principe technique.

Comprendre les principes techniques vous aidera non seulement à choisir le bon outil mais aussi à créer un nouvel outil si ceux qui sont disponibles ne correspondent pas à vos besoins.

SNMP

Le SNMP « *Simple Network Management Protocol* » est une opération et un protocole de maintenance conçu spécialement pour les réseaux d'ordinateurs et les réseaux d'équipements individuels.

La première version de SNMP (SNMPv1) a été développée par IETF en 1993. SNMPv3 est la norme actuelle, mais plusieurs équipements (sans fil) fonctionnent encore avec les versions anciennes les plus anciennes.

La cueillette de l'information est basée sur un architecture client/serveur ou le logiciel du client fait des commandes d'information statistique privée à distance. SNMP est la couche logiciel d'application du protocole qui est utilisé pour échanger de l'information.

Tous les équipements fonctionnant sous SNMP gèrent une base de données appelée MIB « *Management Information Base* ». La base de données contient des informations recueillies durant les opérations de l'équipement. SNMP, en mots simple, SNMP est un mécanisme pour acheminer des requêtes de recevoir des réponses sur la gestion de l'information des éléments actifs du réseau.

La grande force de SNMP, ce qui lui a donné sa grande popularité, c'est sa compatibilité entre les différents équipements du réseau. Les équipements qui utilisent des agents SNMP traversent des routeurs aux ordinateurs, des modems aux imprimantes.

Aussi, SNMP est suffisamment flexible qu'il peut être étendu à des équipements avec des données spécifiques. Plusieurs vendeurs sans fil mettent en place des outils propriétaires pour l'information sur les données sans fil dans leurs MIB. Malheureusement, cela implique que bien que tous les vendeurs mettre en œuvre SNMP, le mécanisme pour retrouver certaines types d'informations sans fil peut varier

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.

SNMP a aussi des faiblesses. Le protocole n'est pas simple pour les programmeurs due à ces règles de code complexes. Il a aussi été critiqué pour cause d'inefficacité et de perte de base passante. Tous les paquet SNMP

incluent beaucoup de données inutiles et les variables SNMP sont encodées de façon à créer des paquet trop large pour rien.

En mettant en place n'importe quel système basé sur SNMP, vous devriez savoir que :

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...

Comptage du trafic

Le comptage du trafic est une technique générale pour faire le surveillance des statistiques de trafic dans les réseaux d'ordinateurs . L'information engendrée par le comptage du trafic est de grande valeur lorsque vient le temps de prendre des décisions, régler les problèmes de réseau local « LAN » et surveiller différentes activités d'hébergement de services.

Habituellement, le comptage du trafic recueille des informations telles :

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

Il y a plusieurs façons de recueillir des informations reliées au trafic dans un réseau. La façon la plus simple est de permettre l'utilisation de SNMP dans tous les routeurs et passerelles du réseau. Il est intéressant de concevoir SNMP comme une manière **active** d'obtenir de l'information reliée au trafic. C'est actif parce qu'il requiert d'échanger du trafic SNMP avec les routeurs et passerelles pour obtenir cette information.

Une autre possibilité d'obtenir de l'information sur le trafic sans avoir à envoyer plus de trafic sur le réseau peut être de mettre le canal de communication « sous écoute». L'écoute d'un canal de communication est mécanisme passif qui n'implique pas l'utilisation de SNMP du tout. Cependant, il y a deux limites à cette approche. Vous devez avoir un accès direct aux données dans le canal de communication et dans le processeur « CPU » pour recueillir de digérer le volume d'information dans le canal.

Organisations du trafic « traffic shaping »

L'organisation du trafic est un méthode pour contrôler la circulation du trafic dans le réseau. L'organisation du trafic est le résultat de l'imposition d'une discipline pour prioriser les paquets dans les routeurs. En gérant ces règles intelligemment, vous pouvez ajuster le comportement de votre réseau concernant :

1. Les délais de transit et la gestion de la congestion
2. Gestion de la bande passante et l'équité

L'organisation du trafic se fait normalement dans la couche IP en changeant la priorité de livraison des paquets par les routeurs. En organisant le trafic dans la couche IP, nous affectons aussi la distribution des ressources dans le canal radio.

Il est important de mentionner que certain produits basés sur IEEE 802.11 ont tenté de mettre en œuvre des mécanismes similaires dans les passerelles sans fil en modifiant le comportement par défaut de la couche MAC IEEE 802.11. LA plupart de ces mécanismes demeurent propriétaires et la compatibilité entre les vendeurs n'est pas assurée.

Par exemple, Proxim utilise le mécanisme de sélection propriétaire « WORP » qui fonctionne par accélération de la bande passante asymétrique ce qui permet d'ajuster le ratio de données reçues et envoyées. WORP donne au réseau la capacité de donner de brèves périodes de temps à chacun des usagers qui souhaitent recevoir et envoyer des données et leur donne un tour pour utiliser la bande passante.

http://www.proxim.com/learn/library/techoverviews/TT10-0403.pdf

Queues, discipline et délais de transit.

Si vous souhaitez maintenir la compatibilité entre les vendeur et ne voulez pas installer un mécanisme propriétaire dans le réseau, l'organisation du trafic devra être fait au niveau IP.

L'organisations du trafic est faite en affectant la façon que nous priorisons et livrons le trafic aux divers éléments du réseau dit actifs. La discipline de priorité est la règle qui est appliquée aux paquets de données durant le processus d'acheminement. L'organisations du trafic implique divers règles dépendantes de la priorité du paquet ou du statut de la queue à ce moment.

Normalement dans un réseau, la priorité imposée à la queue du trafic sortant et de plus grande importante que celle du trafic entrant. Puisque le bouchon d'étranglement dans un réseau est normalement le lien sortant (le lien vers la connexion Internet) ou le trafic de tout le réseau local est comprimé dans une seule voie, la discipline imposée à la queue sortante doit être gérée avec précaution.

Une queue de paquets est une mémoire tampon qui conserve tous les paquets lorsque la quantité de paquets reçus excède la capacité d'envoyer. Quand la mémoire est pleine, le routeur doit laisser tomber les nouveaux paquets qui arrivent ce qui résultera en retransmissions

Un paquet qui reste coincé dans la queue trop longtemps devient périmé ce qui force l'envoyeur à ré-envoyer le paquet causant encore plus de trafic à gérer pour le routeur déjà à bout de souffle.

Le résultat de ces mémoires trop chargées sera que le routeur aura un délai de trafic très élevé quand le lien sortant devient congestionné. Les retransmissions dues aux délais peuvent rendre une mauvaise situation encore pire.

Une façon de réduire les inconvénients des délais de transit et de prioriser certains paquets par rapport à certains autres. Les paquets qui requérant l'interaction d'usager (comme des contrôleurs à distance, jeux en ligne, chat, VoIP, etc.) reçoivent une priorité plus importante que les protocole comme http, FTP ou SMTP. Cette politique des priorités peuvent être mis en place en donnant ces règles aux services (quels port TCP le paquet utilise)

Dans les cas ou plusieurs protocoles utilisent le même port TCP par défaut (comme SSH ou SCP), une autre politique de queue doit être imposée. SSH et SCP sont deux protocoles qui utilisent le port 22 TCP par défaut. Les paquets SSH sont normalement plus petits que les paquets SCP. Contrairement à SCP, SSH requiert une interaction avec l'utilisateur ce qui pourrait vous encourager à leur appliquer des politiques différentes. Le mécanisme pour donner organiser différents service utilisant le même port est de prioriser en fonction du volume des paquets.

Gestion de la bande passante par priorité des paquets

La gestion de la bande passante par la priorité des paquets peut permettre d'offrir un service de meilleur qualité au sein de votre réseau. La gestion de la bande passante implique de limiter votre bande à certain ratio de bits à un usager spécifique ou sous réseau ou de limiter globalement certain types de services.

La gestion de la bande passante peut-être fait pour diverses raisons. Vous ne voulez peut-être pas que de gros téléchargements affectent la qualité de votre service pour d'autres usagers qui requiert moins de bande passante. Ou vous souhaitez peut-être ouvrir un service équitable ou chaque usager bénéficient d'une bande en fonction de ce qu'ils payent pour le service.

Pour réaliser cela des disciplines avec ou sans classe peuvent être imposées au routeurs.

Une queue avec une discipline de classe *« classifull queuing »* (donc basée sur les classes) dispose d'une structure hiérarchique avec des relations parents-enfants et un héritage des caractéristiques. Chaque usager

appartient à une classe ayant des caractéristiques spécifiques : minimum et maximum de bande, algorithme de queue et le numéro du port et précisé.

Avec la gestion de la bande passante et la priorité par classes, un ratio de bits spécifique peut être attribué à un certain protocole dépendamment de son type (Port TCP). Aussi, différents usagers (appartenant à une certaine classe) peuvent recevoir un certain ratio de bits pour créer un réseau équitable.

Une des plus populaires disciplines de classe pour les queue et le HTB « *Hierarchical token bucket* » qui est utilisée pour distribuer les paquets de données à différentes branches du modèle d'arbre hiérarchique en fonction d'une certaine priorité et bande passante. Des sous-classes peuvent être créé pour permettre à la bande passante non utilisée d'être redistribuée entre les membres de la sous classes (les enfants du groupe).HTB est utilisé pour contrôler la bande sortante sur un certain lien. En appliquant des règles de queue à tous les paquets entrants, il utilise un lien physique pour simuler plusieurs liens plus lents et pour leur envoyer différents types de trafic sur ces liens simulés.

À l'inverse de la discipline de classes, la discipline de queue SANS classe impose les horaires, les délais ou laisse tomber des données.

Le SFQ « *Stochastic fairness queue* » est une discipline sans classe très populaire qui est utilisée quand le lien sortant et trop plein. Il n'impose pas d'organisations ou de priorité au trafic, mais établit un horaire de façon à ce que tous bénéficient d'un partage égal de la bande passante. Cette discipline n'a aucun effet sur le trafic quand le lien n'est pas plein.

La discipline SFQ tente de distribuer l'opportunité de transmettre des données au réseau au sein d'un nombre arbitraire de flux de trafic, d'une façon équitable.

Filtres Bayesiens[1]

Un autre principe technique qui peut être utilisé pour améliorer le service de votre réseau est l'utilisation de filtres *Bayesiens.* Ces filtres peuvent être utilisé pour mettre en place des systèmes anti-pourriel qui calcule la probabilité qu'un message soit un pourriel en fonction de son contenu.

Les filtres Bayesiens se basent sur l'idée que les pourriels peuvent être filtrés par la probabilité que certains mots ou combinaisons de mots peuvent désigner que le message est un courriel à l'inverse d'un message légitime.

Les filtres Bayesiens sont adaptatifs, c'est à dire qu'ils apprennent de leur expérience à distinguer le bon et le mauvais contenu et deviennent par la suite plus intelligents et plus robustes.

Les filtres Bayesiens sont basés sur le contenu comme plusieurs autres filtres. Une des différence est que la liste manuelle des caractéristiques des pourriels qui est la faiblesse de beaucoup de filtres basés sur le contenu est remplacée ici par une liste de mots que le filtre lui-même a créé en analysant le contenu. Cette liste initiale est créée par l'analyse des messages désignés comme pourriel et des autres classés « bon ».

La classification du bon contenu est aussi importante que celle du mauvais. Mieux le filtre est adapté à l'usager, plus il sera difficile au producteur de pourriel de le traverser.

Après avoir créé la liste initiale des caractéristiques, la liste grossira davantage plus le filtre sera utilisé. Le filtre sera adapté à l'utilisateur puisqu'il apprend à partir des choix de l'utilisateur sur ses courriels entrants.

Contrairement à d'autre filtres, les filtres Bayesiens recherche dans tout le contenu du message alors que d'autres filtres n'examinent que l'en-tête ou le champ sujet. En plus du contenu du message, il examine d'autres parties du message

- Entête (envoyeur et chemin parcouru par le message)
- Codes HTML intégrés (couleurs, etc.)
- Le mariage des mots et des phrases
- L'information globale

1Du nom du mathématicien Thomas Bayes

Une option intéressante valant d'être considéré est de placer votre anti-pourriel AVANT même que le courriel ne traverse votre 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

Les logiciels anti-virus ont la capacité de détecter les virus de même que d'autres formes de logiciels malicieux et de les éliminer. Cette détection est faites en examinant le programme exécutable et en recherchant des instructions spécifiques pour l'ordinateur que plusieurs Virus connus utilisent.

Ces instructions à l'ordinateur sont appelées l'empreinte ou la signature. L'utilisation d'empreintes est un principe technique qui permet au programme anti-virus d'être capable de rechercher des formes connus dans les codes suspects.

Un programme anti-virus qui souhaite demeurer performant doit constamment maintenir à jour une base de données des empreintes.

Malheureusement, la détection de code malicieux n'est pas simple et les code virus peuvent muer et se modifier eux-mêmes pour changer leur empreinte. Des algorithmes à vérification heuristique, qui testent plusieurs permutations de virus connus, sont utilisés pour prévoir et analyser comment un virus peut muer et détecter le nouveau virus avant qu'il puisse se répandre

Ne mésestimez pas l'impact des codes malicieux dans la performance globale de votre réseau sans fil. Savoir identifier et éliminer les virus du courrier des utilisateurs ou encore bloquer le trafic provenant d'usager infectés est aussi important que d'avoir un bon ratio signal-bruit dans vos liens sans fil.

Outils

Cette section s'attarde à quelques uns des outils libres qui peuvent être utilisés pour suivre votre réseau. Certains de ces outils incluent des mécanismes pour réagir quand un mauvais comportement arrive.

Les outils présentés sont des outils de gestion de réseaux (ntop, MRTG), des filtres pourriel (SpamAssassin) et des programmes anti-virus (CLAM AV).

Surveiller le « sans fil »

Tous les vendeurs d'équipements sans fil fournissent un outil pour surveiller les activités dans leurs équipements. La configuration et la surveillance est faites via un logiciel spécifique fonctionnant sous un certain système d'opération. Malheureusement, en construisant et opérant de grands réseaux sans fils, vous trouverez ces outils très limités. Les outils qui viennent qui viennent avec l'équipement sans fil ne peuvent pas être intégrés dans votre système de surveillance du réseau. De plus, si des éléments différents sont mis en fonction dans le réseau, vous finirez par devoir utiliser des outils de surveillance différents de façon à garder de ce qui se passe dans votre réseau sans fil.

Pour intégrer des outils de gestion différents dans une même interface, il est possible d'obtenir l'information par l'utilisation de SNMP MIB dans tous les produits sans fil et de placer toutes les données ensembles en utilisant des outils auxiliaires comme MRTG.

MRTG

MRTG « Multi Router Traffic Grapher » et un outil de gestion de réseaux sur le Web qui peut surveiller et présenter l'évolution des paramètres du réseau durant un certain temps. MRTG utilise SNMP pour recueillir l'information provenant de divers routeurs SNMP et de certaines librairies graphiques pour construire des graphiques sur l'information.

MRTG fut originalement conçu pour présenter des graphique du trafic et de l'utilisation de la bande passante, mais qui permet maintenant de présenter presque tous les paramètres qui changent dans le temps.

Surveiller les paramètres sans fil utilisant MRTG

Dans l'exemple qui suit, les principes de base pour construire votre propre système de surveillance sans fil utilisant SNMP et MRTG seront expliqués. L'exemple est basé sur la famille de produit Orinoco, mais la méthodologie peut être appliquée à d'autres équipements sans fil.
Assumons que nous avons un lien sans fil point à point et que nous voulons surveiller l'utilisation totale de la bande passante (couche 3) et le statut du lien radio (2e couche)

Surveiller la passerelle sans fil pour obtenir l'utilisation de bande passante est aussi simple que de surveiller la bande passante de n'importe quel équipement SNMP (Routeur, commutateur, etc.)

Les étapes pour configurer MRTG peuvent être résumées ainsi :

1. Soyez certain d'avoir tous les prérequis : un serveur WEB en fonction, MRTG installé, l'adresse IP et le mot de passe SNMP de l'équipement que vous souhaitez surveiller
2. Créer une configuration pour MRTG. Cette étape peut être faites manuellement ou utilisant un outils auxiliaire comme *cfgmaker*
3. Créer un processus « cron » qui met en oeuvre MRTG en utilisant la configuration périodiquement.

Surveillance de la bande

Après l'installation de (1) MRTG et Apache Web Server, Nous utiliserons l'outil **cfgmaker** pour créer une configuration par défaut (2) pour mrtg:

Le fichier de configuration par défaut est obtenu par :
[aep@it46-d505 mrtg2]$ cfgmaker password@IP > /etc/mrtg_b.cfg

où <password> et <IP> sont respectivement les mots de passes à lire seulement SNMP et les adresses IP de la passerelle sans fil .

Le seul changement nécessaire est le fichier de configuration par défaut *mrtg_b.cfg* pour indiquer l'endroit où nous voulons que les pages Web MRTG se retrouvent.

Par exemple:
WorkDir: /var/www/mrtg
Indique que les pages Web MRTG avec les graphiques seront placés dans le répertoire /var/www/mrtg
Finalement, nous devons créer une tâche spécifique en ajoutant la ligne, /etc/crontab comme suit :

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

MRTG va choisir les données en provenant de la passerelle sans fil chaque 5 minutes.

Surveillance du ratio bruit signal

Pour surveiller le signal et le bruit d'un équipement sans fil, nous devons avoir accès au MIB de ce produit. Le MIB du produit nous dira quelles sont les entrés dans la base de données que nous cherchons.

Avoir accès au MIB d'un équipement sans fil n'est pas toujours facile. Beaucoup des paramètres sans fil que vous voudrez peut-être mesurer font partie du MIB « propriétaire », une extension incluse dans les vendeurs de produits sans fil avec assez peu documenté publiquement.

Si vous n'avez pas accès au MIB, vous pourrez peut-être avoir besoin de la trouver par vous-même « i.e. reverse engineering ».

Nous devons trouver quels ODI sont utilisés pour l'information que nous désirons surveiller. ODI « *Object Identifier* » est un nombre qui identifie la position d'un objet dans le MIB. Le ODI est le façon par laquelle nous pouvons référer à certaines positions dans la base de données de gestion. Quand un outil de surveillance requiert une informations d'un équipement sans fil, il exécute un groupe d'opérations SNMP utilisant certains OID. Le OID indique quel partie du MIB nous voulons voir ou écrire.

La meilleure façon d'obtenir le OID que nous recherchons est de choisir l'outil réseau qui vient avec le produit et de surveiller tout le trafic qui s'échange entre le l'outil de surveillance et l'équipement sans fil.

Dans exemple, Le gestionnaire **Orinoco AP** est installé:

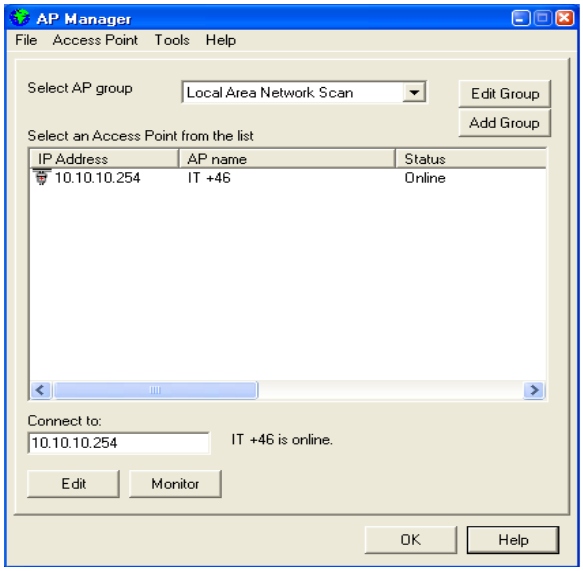

Image 2: Utilisant un outil Windows pour surveiller un point d'Accès.

Après avoir connecté le point d'accès sans fil, nous choisissons l'option « *perform a link-test* » et notons tout le trafic entre l'AP et l'outil de surveillance.

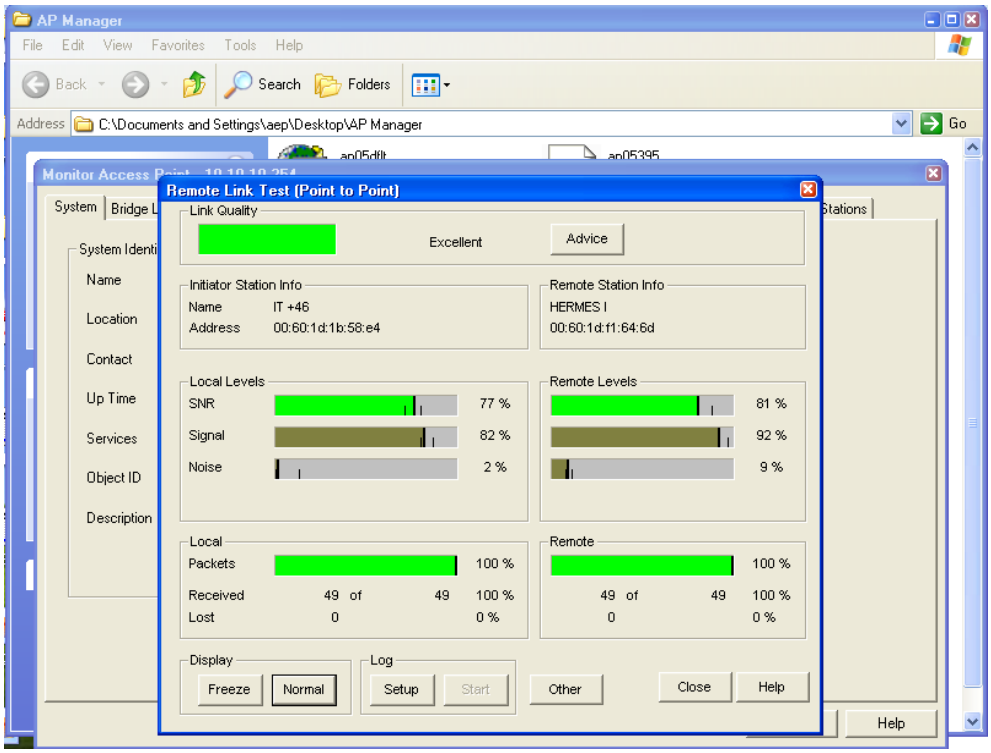

Image 3: Test d'un lien Point à Point mesurant SNR et les pertes en paquets. *En utilisant n'importe quel outil d'analyse* (tcpdump, ethereal etc), nous pouvons obtenir des informations sur l'échange du trafic entre le AP et son gestionnaire qui ressembleront à ceci :

```
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..I.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...+....
0x0040   857a 0201 0700 0201 02                       .z.......
```

Le MIB propriétaire de Lucent MIB recueille toutes les information sans fil en utilisant les variables MIB 1.3.6.1.4.1.762.2.5. Ce MIB est partagé par plusieurs points d'accès sans fil comme le Airport de Apple et Lucent RG1000.

Le nombre d'usager connectés à l' **AP** peut être retrouvé en faisant les opérations SNMP suivantes:
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
Retrive the OID:
1.3.6.1.4.1.762.2.5.1.0

Paramètres Signal Bruits de l'équipement sans fil <n> peuvent être obtenus par:
Write Integer 1500 in OID
1.3.6.1.4.1.762.2.5.2.1.27.n
Write Integer 25 in OID
1.3.6.1.4.1.762.2.5.2.1.26.n
Write Integer 80 in OID
1.3.6.1.4.1.762.2.5.2.1.25.n

The signal can be retrieved by reading the OID
1.3.6.1.4.1.762.2.5.2.1.32.n
The noise can be retrieved by reading the OID
1.3.6.1.4.1.762.2.5.2.1.33.n

Lorsque que nous avons obtenu les informations reliées au OIDs/MIB , nous devons écrire un script qui exécutera des opérations SNMP similaires à celles du gestionnaire Windows AP (N'oublions pas que l'idée est de retirer les gestionnaires AP et d'avoir la possibilité d'intégrer les données dans un seul système de gestion du réseau).

UN script qui retrouve l'information sur les test de lien écris en utilisant **Linux snmp-tools** est inclus en annexe à cette unité.

Le script recueille les valeurs du signal et du bruit et retourne des valeurs dans un format que MRTG peut utiliser:

```
[aep@it46-d505 etc]$ /usr/local/bin/monitoring_PtP.sh
79
12
2:596
aep
```

Les 4 valeurs sont le signal (79), le bruit (12), le temps « *timestamp* »(2:596) et le nom de l'usager (aep).

Nous sommes maintenant prêts à mettre ensemble, dans la même interface, les données de bande passante (information IP) in les informations sur le signal, et le bruits (Informations sans fil).

En représentant ensemble sur la même interface la bande passante et le ratio signal-bruits, nous obtenons une image sur ce qui se passe dans le réseau.

L'image montre l'intégration avec MRTG de la surveillance sans fil avec la surveillance du trafic IP.

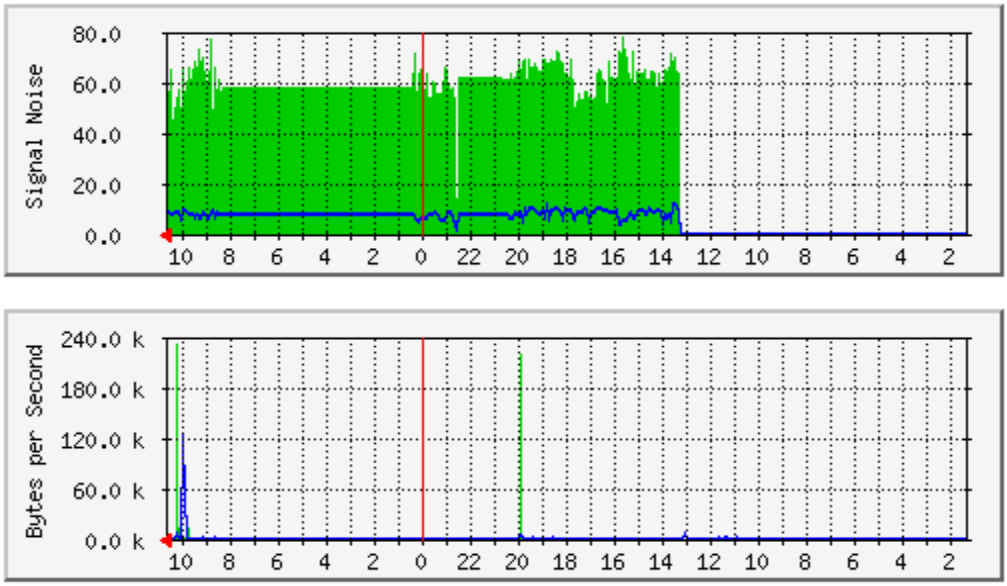

Image 4: Utilisant MRTG pour la présentation, SN est le lien sans fil est l'usage du la bande passante et du lien sans fil simultanément

(Note: Discuter quels informations ressortent du diagramme)

Ntop

Ntop est un logiciel libre multi-plateforme de surveillance et mesure du trafic IP. Toutes les fonctions de Ntop sont accessibles (configuration et surveillance) par une interface Web.

Nous entendons par la mesure du trafic IP qu'aucune information spécifique sur le sans fil n'est enregistrée par Ntop. Il ne prend pas note d'informations comme le ratio des signal et bruit, le nombre de postes associés, etc. Ntop ne devrait pas être combiné avec un outil spécifique de la couche 2 tels que ceux décrits plus haut.

Les fonctions de Ntop s'attadent sur:

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

Une description détaillée des fonctions de Ntop se trouve en annexe.

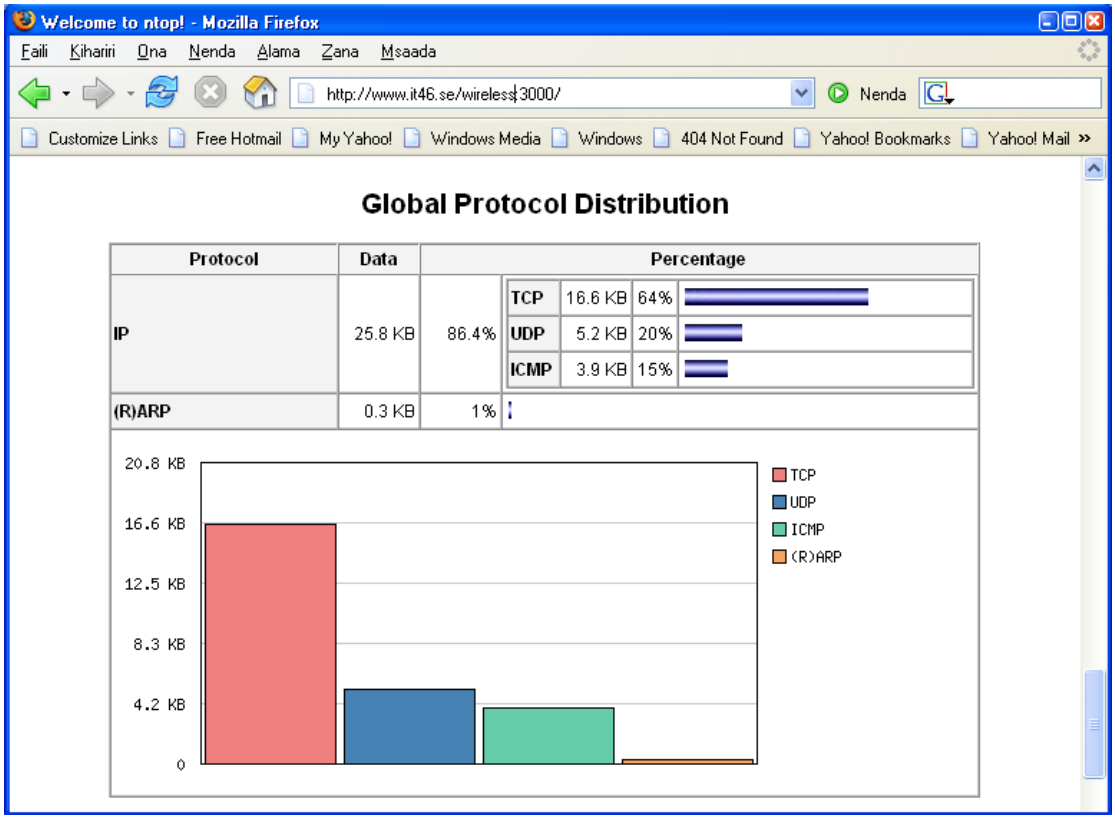

Image 5: Utiliser Ntop pour surveiller le protocole de distribution d'un lien.

Spam-assassin

Cette unité inclus une section spéciale sur la façon de combattre les pourriels. Le pourriels sont devenus le pire cauchemar dans la gestion de réseau. Savoir empêcher les pourriels d'atteindre vos usagers et obligatoire pour tous les fournisseurs de service.

SpamAssasin est l'un des plus fameux et plus répandus logiciel de luttes contre les pourriels. C'est un filtre intelligent qui utilise plusieurs différentes méthodes pour différentier les pourriel du courriels désirés. SpamAssassin peut être utilisé autant par les serveurs que par client, autant pour les courriels sortant que entrant.

SpamAssassin ne bloque pas automatiquement les courriels suspects. Il leur assigne des étiquettes et une note dépendamment du contenu. Le plus haut score obtenu représente la plus haute probabilité qu'un message soit un pourriel. Dans tous les cas, c'est au client de décider si le message est un pourriel.

Une de ses plus grandes forces est son architecture mudulaire qui permet l'intégration de nouvelles technologies dans le filtre et le fait qu'il peut être mis en fonction sur presque tous les systèmes de courriel.

Ses méthodes élémentaires d'analyse du courriel et de détermination de la probabilité que ce soit un pourriel sont :

- 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 Bayesien
- 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 locals

Base de données collaborative d'identification des pourriels

Un des mécanismes pour la détection des pourriels est d'utiliser une base de données collaborative d'identification des pourriels . Il s'agit d'une base de données en ligne que tout le monde peut appeler pour identifier un pourriel.

Pour calculer la probabilité qu'un message suspect arrivant au serveur de courriel soit un pourriel , la base de données peut vérifier si ce message a été déjà reporté avant par quelqu'un d'autres. Si c'est le cas, le pointage du message augmente.

SpamAssassin utilise trois bases de données différentes pour l'identification:

- Razor, http://razor.sourceforge.net
- Pyzor, http://pyzor.sourceforge.net
- DCC « *Distributed Checksum Clearinghouse* », http://www.rhyolite.com/anti-spam/dcc/

Listes de blocage DNS

Les listes de blocage DNS sont une autre forme de base de données pour la détection des pourriels. Il sont aussi connus comme des listes noires DNS « DNS Blacklists – DNSBLs » La liste inclus les adresses IP des serveurs reconnus (ou suspectés) de servir de rampe de lancement pour les pourriels

Certaines des configurations du serveur de mail qui font réagir DSNBL sont :

- Ouvrir le relais SMTP
- Ouvrir le Proxy
- Ouvrir « *form to mail HTTP gateways* »
- Sélection IP dynamique

Un relais de courriel ouvert est un serveur de courrier (mal) configuré permettant à quiconque de ré-envoyer du courrier à partir de lui.

Aujourd'hui, les fournisseurs n'utilisent plus les relais ouverts pour permettre l'accès aux usagers. Des solutions comme le SMTP AUTH et POP avant SMTP sont utilisées. Cela signifie que les courriels ont dû adopter d'autres techniques.

Une ressource intéressante sur le DNSBL sont disponibles ici :
http://www.scconsult.com/bill/dnsblhelp.html

Clam Antivirus (Clam AV)[2]

Les virus d'ordinateur peuvent arrêter un réseau sans fil en moins de deux.

Certains virus déclanchent des balayages du réseau pour ou des refus de service. La première conséquence en est que le lien sans fil devient surchargé. Les virus peuvent rendre un lien VSAT inutile si des listes d'accès ne sont pas placées rapidement.

Clam AntiVirus est un outil anti-virus GPL pour Unix conçu pour le balayage des courriels et des passerelles de courrier. Clam AV utilise la mise à jour automatique de l'empreinte virus. La base de données des empreintes est mis à jour par l'Internet.

Certaines des fonctions de Clam Antivirus sont:

- Balayage rapide et puissant des courriels et répertoires
- Détection de plus de 30000 virus, vers et cheval de Trois (incluant les macros de Microsoft Office et MacOffice)
- Balaie les archives et les fichiers compressés avec des algorithmes comme Zip, Rar (2.0), Tar, Gzip, Bzip2, MS OLE2, MS Cabinet Files, MS CHM (Compiled HTML), et les format de compression MS SZDD
- Supporte les fichiers exécutable compressés avec UPX, FSG et Petite
- Mise à jour des base de données incluant les signatures digitales des virus et les requêtes sur les base de données DNS

Clam Antivirus n'élimine, ni ne renomme ni de nettoie un fichier infecté. Il détecte simplement et averti l'usager.

Conclusion

La gestion d'un réseau (sans fil ou pas) requiert que nous commencions par définir nos objectifs en tant que fournisseur de services. Si nous ne savons pas ce que nous souhaitons réaliser, il sera très difficile de décider quoi surveiller. Si nous ne savons pas quoi surveiller, il sera très difficile de choisir un outils qui nous aideront à prendre des décisions.

Recueillir des données brutes ou des outils d'installation n'est pas assez pour avoir un bon réseau opérationnel. Trouver l'outil adéquat ne devrait pas être un problème si vous avez une bonne analyse de ce que vous avez besoin.

Surveiller le statut du lien radio ne sera pas suffisant si votre réseau est surchargé par l'activité de virus. Arrêter les virus ne sera pas suffisant si votre lien sans fil n'est pas stable.
En installant des système de surveillance ou de gestion du réseau, vous devrez apprendre comment intégrer les différents outils pour rendre facile d'accès l'information nécessaire pour la prise de décision. Pensez que si les outils ne satisfont pas vos besoins, c'est éventuellement plus simple d'écrire un outil simple qui correspond à vos besoins plutôt que de vous battre pour trouver un outil conçu pour répondre aux besoins d'un autre.

Définissez vos besoins ⇒ Identifiez les principes techniques ⇒ trouvez ou écrivez les outils ⇒ prenez des décisions.

2 http://www.clamav.net/, dernière lecture: 20050223

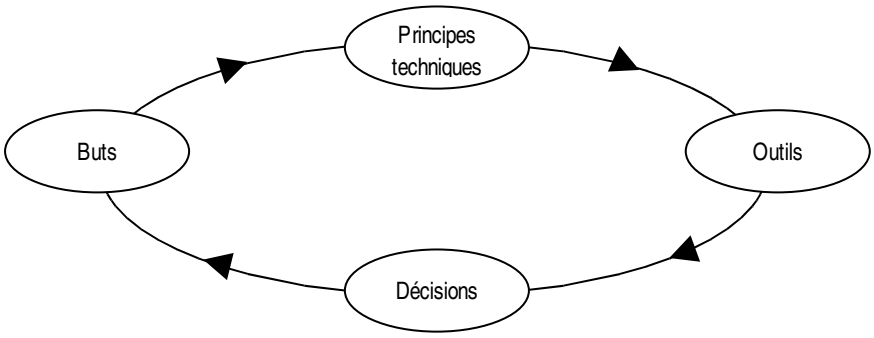

Image 6: L'image montre la méthodologie centrée sur les buts pour la surveillance.

Annexe 1

NTOP mesure du trafic

Ntop associe chaque paquet capturé avec son envoyeur et son receveur. De cette façon, toutes les activités qui sont reliées à un seul hôte peuvent être extraites par le nom de l'usager ou l'Adresse IP.

Pour chaque hôte, l'information suivante peut être retrouvée par Ntop :

- Données reçues et envoyées: somme totale du trafic généré ou reçu (volume et paquets), classifiés selon le protocole de réseau (IP, IPX, AppleTalk, etc.) et le protocole IP (FTP, HTTP, NFT etc.)
- *« IP multicast »*: Montant total du trafic multicast généré et reçu par l'usager.
- Histoire de la session TCP: il liste les sessions actuellement actives, initialisées ou acceptées par l'usager et lui associe les statistiques de trafic.
- Le trafic UDP: montant total du trafic UDP trié par port.
- Les services TCP/UDP utilisés: Liste les services basés sur IP fourni par l'usager et les derniers 5 usagers qui l'ont utilisé
- Système d'opération utilisé par l'usager.
- Pourcentage de bande passante utilisée (actuellement, en moyenne et les pointes)
- Distribution du trafic (au sein des sous réseaux)
- Distribution du trafic IP (UDP vs TCP, Distribution relative du protocole IP)

Ntop recueille aussi l'information globale (pas orienté sur l'usager) liée à la distribution du trafic, la distribution des paquets et l'utilisation de la bande.

Caractéristiques de NTOP sur le trafic et la surveillance

La surveillance du trafic implique d'identifier des situations où le trafic du réseau ne respecte pas les règles créées pas l'administrateur du réseau. Ntop peut découvrir les situations suivantes :

- Utilisation double d'une adresse IP
- Identification de tous les routeurs des sous réseaux
- Identification de tous les usagers dont l'identifiant est mal configuré.
- Détecte les mauvaises configurations des logiciels d'applications
- Détection des mauvais usages des services (tels que les hôtes qui n'utilisent pas les proxis spécifiés)

- Mauvaise usage des protocoles (identification des usagers qui utilisent des protocoles non nécessaires tels que NetBEUI et IXP)
- Détection des usagers avec une utilisation excessive de bande passante.

Détection des violations de sécurité par Ntop

La plupart des attaques dans un réseau proviennent du réseau lui-même et non de l'extérieur. Ntop fournit à ses usagers des éléments pour rechercher les attaques et identifier les trous de sécurité dans leur ordinateur en offrant les fonctions suivantes:

- Détection « *Portscan* » et « *Slow Portscan* »: ntop rapporte les noms des trois derniers hôtes qui ont envoyés des paquets à chaque postes moins de 1024. *Portscan* est détecté dans tous les hôtes où Ntop surveille.
- « Spoofing detection » pour les paquets appartenant au même sous réseau où ntop travaille. Le Spoofing signifie qu'un hôte prétend en être un autre dans le but d'intercepter des paquets. Ntop averti l'usager quand deux adresses IP pointe vers le même ordinateur dans le sous réseau.
- Détection des espions. Un espion est un hôte avec sa carte réseau en mode malicieux ce qui lui permet de capturer des paquets indépendamment de sa destination.
- Cheval de Troie : Les chevaux de Troie apparaissent comme des codes « amis » mais contiennent des codes cachés malicieux qui peuvent détruire votre ordinateur. Les chevaux de Troie utilisent normalement des ports très connus. Ntop peut donc détecter leur présence en surveillant ces ports.
- Le refus de service « *Denial of Service - DoS* » est le comportement d'un hôte qui envoie des paquets avec le
- Le refus de service « DoS »: Le DoS est le comportement d'un hôte qui envoi des paquets avec le SYN flag set (à la connexion TCP) jusqu'aux ports de la « victime » sans exécuter les procédures de connexion.. Éventuellement les connexions de la « victime » sont toutes occupées et l'hôte ne peut plus accepter de nouvelles connexions.

Optimisation du réseau et planification avec NTOP

Les configurations sub-optimales de l'hôte et l'utilisation non efficace de la bande passante disponible apportent des diminutions de la performance globale du réseau. Ntop fournit le support pour améliorer la performance du réseau :

- Identifier les protocoles non nécessaires (des hôtes qui utilisent des protocoles qui n'est pas utilisée dans le réseau)
- Identifiez le routage sub-optimal en suivant les ICMP rediriger les messages et analyser les routeurs du sous réseau.
- La caractérisation du trafic et la distribution en étudiant les formes du trafic
- Meilleur usage de la bande: Étudier la distribution du trafic au sein des protocoles peut aider les administrateurs à identifier les applications qui ont besoin d'un Proxy Web.

NTOP supporte les bases de données SQL si l'usager veut sauver les données recueillis dans une session de surveillance.

/etc/mrtg_b.cfg

```
##################################################################
# Multi Router Traffic Grapher – Orinoco PtP signal/noise monitoring
##################################################################

# Global configuration
WorkDir: /var/www/mrtg
WriteExpires: Yes

Interval: 5
Target[load]: `/usr/local/bin/read_signal_noise.sh <password> <IP>`
Title[load]: SIGNAL NOISE
PageTop[load]: <H1>Signal Noise PtP</H1>
Options[load]: gauge,nopercent,integer
YLegend[load]: Signal Noise
ShortLegend[load]: -dbm
MaxBytes[load]: 100
LegendI[load]: Signal
LegendO[load]: Noise
```

read_signal_noise.sh <password> <IP>

```
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.1 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.2 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.5.3 i 50 >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.1 i 3  >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.2 i 3  >/dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.4.3 i 3 >/dev/null
users=`snmpget -c public -v 1 10.10.10.254 1.3.6.1.4.1.762.2.5.1.0 | awk '{print $4}'`
#echo The number of users is $users
#echo "TESTING LINK...."
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.27.1 i 1500 > /dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.26.1 i 25 > /dev/null
snmpset -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.25.1 i 8000 > /dev/null
signal=`snmpget -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.32.1 | awk '{print $4}'`
noise=`snmpget -c $2 -v 1 $1 1.3.6.1.4.1.762.2.5.2.1.33.1 | awk '{print $4}'`

#Return values for MRTG
echo $signal
echo $noise
UPTIME=`uptime | awk '{print $3$4}' | sed -e "s/,//g"`
echo $UPTIME
```