ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Interpréter les valeurs des indicateurs.

www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1. Introduction : Indicateurs de performances et notions de valeurs seuils ... 2
1.1. Nombre limite de variables ... 2
1.2. Les principaux indicateurs clés de supervision ... 2
1.3. Suivi en continu ... 3
1.4. Le tableau de bord ... 3
1.5. Le pilotage du réseau ... 3
2. Les performances d'un réseau ... 4
2.1. Les performances de la carte réseau ... 5
2.1. Les facteurs d'amélioration d'une carte réseau ... 6
2.2. Les réseaux locaux ... 7
2.3. Des réseaux d'Interconnexion ... 7
2.4. Les analyseurs de protocoles et les sniffers ... 8
2.4.1. Cas pratique d'utilisation ... 8
2.4.2. Faiblesses ... 11
2.5. Les MIB's RMON et sondes RMON ... 11
2.5.1. la MIB RMON ... 11
2.5.2. La sonde RMON dédiée ... 13

1. Introduction : Indicateurs de performances et notions de valeurs seuils

La définition proposée pour les indicateurs de performance d'un réseau informatique en surveillance est la suivante : « variables en nombre limité, réunies dans un tableau de bord, qui permettent de calculer en continu le niveau de rationalisation et d'optimisation de l'infrastructure du système d'information afin d'en faciliter le pilotage ».

Les notions fondamentales, qui délimitent bien les objectifs et les enjeux de l'élaboration des indicateurs de performance, sont associées à cette définition.

1.1. Nombre limite de variables

Les indicateurs de performance doivent être globaux, peu nombreux et illustrer le fonctionnement du réseau informatique dans son ensemble.

Cette notion implique nécessairement que la méthode d'élaboration des indicateurs de performance permette d'obtenir un nombre limité d'indicateurs. Il n'est en effet pas réaliste d'avoir à suivre, ne serait-ce que pour des raisons pratiques telles que la possibilité de les calculer, un nombre important d'indicateurs.

Une liste trop longue risque en effet de n'être rapidement plus utilisée et donc inutile.

La méthode d'élaboration doit donc reposer sur le choix des indicateurs les plus pertinents, les plus globaux et donc les plus représentatifs du bon fonctionnement du réseau informatique en surveillance.

1.2. Les principaux indicateurs clés de supervision

Ils diffèrent fortement selon l'activité mesurée. En matière de supervision réseau, les principaux indicateurs sont :

- La bande passante,
- La variation du temps de latence des paquets,
- La perte de paquets
- La perception applicative vue de l'utilisateur.

Dans le stockage, en revanche, les indicateurs concernent

- La vitesse de lecture et d'écriture des disques,
- La capacité libre disponible,
- Le taux moyen d'occupation des supports et la dispersion des informations.

Enfin, la supervision de bases de données implique de se pencher sur des données telles que :

- le nombre de lignes par table,
- le nombre de requêtes de lecture ou de mise à jour par table,
- le temps d'exécution moyen d'une requête
- et le poids d'une table.

1.3. Suivi en continu

Les indicateurs de performance sont calculés de manière continue. Ils offrent ainsi une vision longitudinale du fonctionnement et de la surveillance de votre infrastructure informatique. Leur rôle est en effet de détecter de manière les plus précoces possibles tout défauts de fonctionnement du réseau qui aurait une répercussion sur la qualité du service informatique.

Les indicateurs de performance sont donc avant tout des variables dynamiques, c'est-à-dire susceptibles d'évoluer de manière significative dans le temps. Ces variables sont associées à des activités régulières menées dans le cadre de la surveillance et qui sont déterminantes pour un fonctionnement efficace du réseau.

Par leur caractère continu, les indicateurs de performance sont donc complémentaires des évaluations ponctuelles qui vont apprécier un nombre plus important de variables dont un grand nombre sont des variables structurelles, qui varient moins dans le temps et sont peu adaptées à un suivi en continu (existence d'un comité de pilotage par exemple).

1.4. Le tableau de bord

La notion de continuité nécessite de se doter d'un outil qui permette d'avoir une vision synthétique du fonctionnement d'un réseau à un moment donné. Le tableau de bord des indicateurs de performance offre une vision instantanée, facile à lire et à interpréter, de la situation du réseau informatique à superviser. Le principe du tableau de bord rejoint également la notion du nombre limité de variables représentatives du fonctionnement du réseau.

1.5. Le pilotage du réseau

Cette notion de la définition des indicateurs de performance en est également la plus importante. Elle illustre la finalité essentielle de l'élaboration des indicateurs, le pilotage du réseau par ses animateurs. Ainsi les indicateurs de performance se démarquent de toute notion de comparaison du fonctionnement des différentes composantes du réseau pour les placer au centre d'une démarche interne de mise en oeuvre par et pour les acteurs du réseau.

Au même titre qu'une démarche qualité, l'élaboration d'indicateurs de performance est donc avant tout une démarche interne qui nécessite une décision stratégique la prise en charge de ce travail d'élaboration par une personne qualifiée et l'implication de l'ensemble des acteurs de la surveillance de l'infrastructure informatique.

L'implication de tous les acteurs est indispensable pour parvenir à une appropriation des indicateurs, seul gage de leur utilisation correcte et de leur suivi. La méthode d'élaboration des indicateurs doit donc tenir compte **des valeurs seuils pour les différents types d'indicateurs,** afin de réagir en cas de dépassement de ces valeurs synonyme de « criticité » ou d'arrête de service.

L'activité de pilotage implique la possibilité d'identifier les causes de dysfonctionnement du réseau informatique et d'en permettre la correction. A cette notion d'indicateurs de performance est donc associée celle d'indicateur de diagnostic qui est définie de la manière suivante : « liste de variables associées à un indicateur de performance permettant de calculer le niveau de réalisation des activités liées à cet indicateur de performance afin d'identifier, si nécessaire, les causes de non atteinte de ses valeurs attendues ».

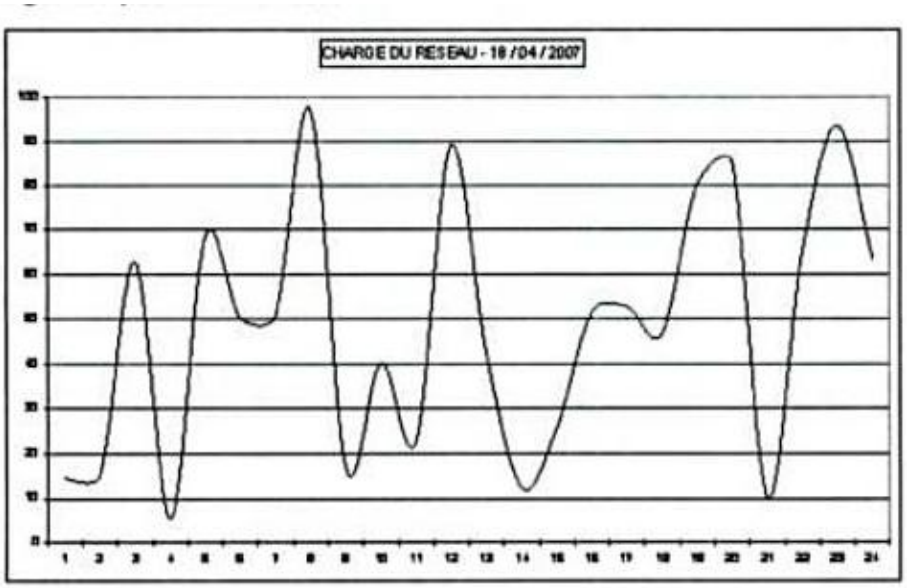
Comme leur dénomination l'indique, les indicateurs de diagnostic permettent de porter un diagnostic sur un dysfonctionnement du réseau de surveillance mis en évidence par un indicateur de performance. Les indicateurs de diagnostic sont donc plus précis, plus nombreux et attachés chacun à un indicateur de performance.

2. Les performances d'un réseau

Surveiller la performance d'un réseau implique une mesure efficace de l'occupation du réseau, des différents réseaux locaux et des interconnexions

En effet, il est courant de reporter systématiquement les difficultés d'accès aux ressources du système d'information de l'entreprise sur le réseau informatique et, de fait, d'engager la responsabilité du technicien ou de l'ingénieur en charge de son exploitation.

Dans la réalité la mesure de performance se résumera principalement à mesure de charge (exprimée en pourcentage).



Augmenter les performances d'un réseau signifie accélérer la transmission des données (le débit) ou augmenter la quantité de donnée qu'il est possible de transmettre (la bande passante).

Les performances d'un réseau peuvent être mesurées par le débit, c'est à dire la quantité de Méga Octets transmis sur le câble par secondes. Plus le nombre de Méga Octets par seconde est élevé et plus le réseau est performant. On dit que le réseau « s'effondre » quand plus aucune machine ne peut transmettre de message.

Les performances d'un réseau dépendent de **nombreux facteurs** :

- Le nombre de machines connectées au même câble
- Le débit théorique maximal du câblage
- Le tuning
- Les cartes réseaux
- etc.…

2.1. Les performances de la carte réseau

La carte réseau est un élément crucial de la performance d'un réseau. Si la carte réseau est lente, alors les données seront transmises lentement sur le réseau. Dans un réseau en bus par exemple, personne ne peut utiliser le réseau tant que le réseau n'est pas libre, et une carte lente augmente les délais d'attente pour les autres utilisateurs.

Les stations qui produisent un volume important de données sur le réseau sont généralement les serveurs. **La carte réseau des serveurs** doit être équipée en priorité des modèles les plus performants.

La carte réseau d'une station de travail n'a généralement pas besoin d'être performante, bien sûr tout dépend de la nature de l'activité de la station. Une station qui n'exécute que des applications bureautiques ne génère pas beaucoup

de trafic, mais une station qui travaille sur une application réseau comme une base de données ou une application d'ingénierie génère rapidement beaucoup de trafic.

Une carte réseau produite par un **fabricant connu depuis longtemps** aura une meilleure pérennité, fiabilité, et les pilotes auront plus de chance d'être mis à jour par la suite.

2.1. Les facteurs d'amélioration d'une carte réseau

Les facteurs d'amélioration des performances sont de deux ordres, soit la carte réseau accède directement aux ressources de l'ordinateur, soit elle dispose de ses propres ressources. Quoiqu'il en soit, il faut une quantité de mémoire vive suffisante et un processeur rapide :

- **Un accès direct à la mémoire (DMA) de l'ordinateur.** La carte réseau transfère directement les données depuis la mémoire tampon de la carte réseau vers la mémoire de l'ordinateur (RAM), sans passer par le microprocesseur.

- **Le contrôle du bus (bus mastering) de l'ordinateur**. La carte réseau prend le contrôle du bus de l'ordinateur, les données sont transmises directement à la mémoire vive (RAM) de l'ordinateur sans passer par le microprocesseur de l'ordinateur qui peut s'occuper d'autres traitements. Ces cartes réseaux sont onéreuses, mais elles peuvent améliorer les performances du réseau de 20 à 70 %. Les cartes réseaux EISA et MCA permettent de prendre le contrôle du bus de l'ordinateur.

- **La mémoire partagée de la carte réseau**. La carte réseau possède de la mémoire vive (RAM) qu'elle partage avec l'ordinateur. L'ordinateur considère cette mémoire comme la sienne et les données sont directement adressées à la mémoire vive de la carte réseau.
- **La RAM tampon de la carte réseau**. La carte réseau possède de la mémoire vive (RAM) qui lui sert de mémoire tampon. Les données circulent généralement beaucoup plus vite sur le réseau que ne peut les traiter la carte réseau ; afin d'absorber le flux trop important de données provenant du réseau, la carte réseau les stocke dans la mémoire tampon. La mémoire tampon permet d'éviter les goulets d'étranglement.

- **Un microprocesseur intégré à la carte réseau**. La carte réseau possède son propre processeur qui traite les données sans passer par le processeur de l'ordinateur.

- **La mémoire système partagée**. La carte réseau possède un processeur et utilise une partie de la mémoire vive (RAM) de l'ordinateur pour traiter les données du réseau.

Une carte réseau avec son propre processeur et sa propre mémoire vive (RAM) sera plus rapide que n'importe quelles autres cartes réseaux. Une carte réseau avec de la mémoire partagée sera plus rapide qu'une carte réseau avec un accès

directe à la mémoire de l'ordinateur (DMA) et à fortiori bien plus rapide qu'une carte réseau avec des E/S normales…

2.2. Les réseaux locaux

Avec l'utilisation aujourd'hui des réseaux locaux Fast-Ethernet voire Gigabit-Ethernet, les problèmes de saturation de bande passante sont rarissimes (10 Gb/s en cours de standardisation). Tout au plus peut on constater des incidents sur le fonctionnement principalement liés à des problèmes de câblage ou d'environnement (ex : rayonnement électromagnétique intense à proximité des câbles de transmission). Ces incidents sont de type

-Trame erronées (CRC déterminé faux)
-Trame dont la taille est inférieure à 64 octets
-Trame dont la taille est supérieur à 1518 octets
-Trame constitué d'un nombre de bit non multiple de 8

Assez facile à mettre en œuvre dans les réseaux Ethemet traditionnels, basés sur des hubs, la collète d'information se complique grandement avec les réseaux de Commutateurs Ethernet de niveau Il ou de niveau III.
Dans le cas d'un réseau de hubs, un analyseur de protocole pour le réseau local sera utilisé. Pour la mesure de performances (et la collecte d'éventuelles erreurs) une sonde RMON sera utilisée, équipement dédié ou embarqué dans l'élément actif.
Dans le cas de réseaux de commutateurs, architecture classique désormais, il conviendra d'interroger les éléments actifs pour recueillir les données associées à chacun des ports.

2.3. Des réseaux d'Interconnexion

Là est le réel problème de saturation de la bande passante.

les performances d'un lien WAN (Wide Area Network) sont, dans la plupart des cas, nettement inférieures à celles d'un réseau local. En effet si 100 Mb/s ou 1 Cb/S sont courants sur le LAN, les débits disponibles sur les liens inter-réseaux dépassent rarement le Mb/s. Notez à ce sujet qu'un accès Internet de type ADSL (Asymétrique) avec un débit descendant (download) de 10 ou 20 Mb/s n'est pas considéré comme un lien inter-réseau.

Les raisons de cette limitation sont les suivantes :

- Technologie et protocoles différents de ceux mis en oeuvre dans les réseaux locaux et adaptés aux distances plus importantes et à l'éloignement des éléments actifs

- Coût sans commune mesure avec les réseaux locaux.

Notez que les réseaux d'interconnexion sont souvent exploités par des opérateurs publics, dans le cas des réseaux métropolitains, mis en œuvre par des structures de type Syndicats Mixtes, Groupements d'Intérêt Economique, ou confiés à des opérateurs .

Ceci étant, la mesure de performances d'un lien inter-réseau se: résumera le plus souvent à la constatation de l'occupation à 100 % de la bande passante disponible.

Il est malgré tout 0pportun d'exploiter un outil tel MRTG (Multi Router Traffic Grapher) qui, en interrogeant régulièrement la MIB du routeur, va permettre de construire un graphe dont l'échelle de temps varie d'une journée à un an. MRTG présente l'avantage d'être assez facile à mettr en œuvre et surtout d'être entièrement gratuit

2.4. Les analyseurs de protocoles et les sniffers

2.4.1. Cas pratique d'utilisation

Pour le technicien ou l'ingénieur réseau, l'utilisation de l'analyseur de protocole se limitera à des travaux de tests ou de dépannage dans des conditions très précises.

L'appellation sniffer mène à penser qu'il s'agit d'un équipement d'écoute voire d'espionnage, Il permet effectivement de capturer un échange de trames sur un réseau local et de décoder les protocoles de tous niveaux jusqu'à l'application.

L'exemple le plus simple est de découvrir aisément le mot de passe d'une ouverture de session Telnet, transmis caractère par caractère à la manière d'une communication asynchrone.

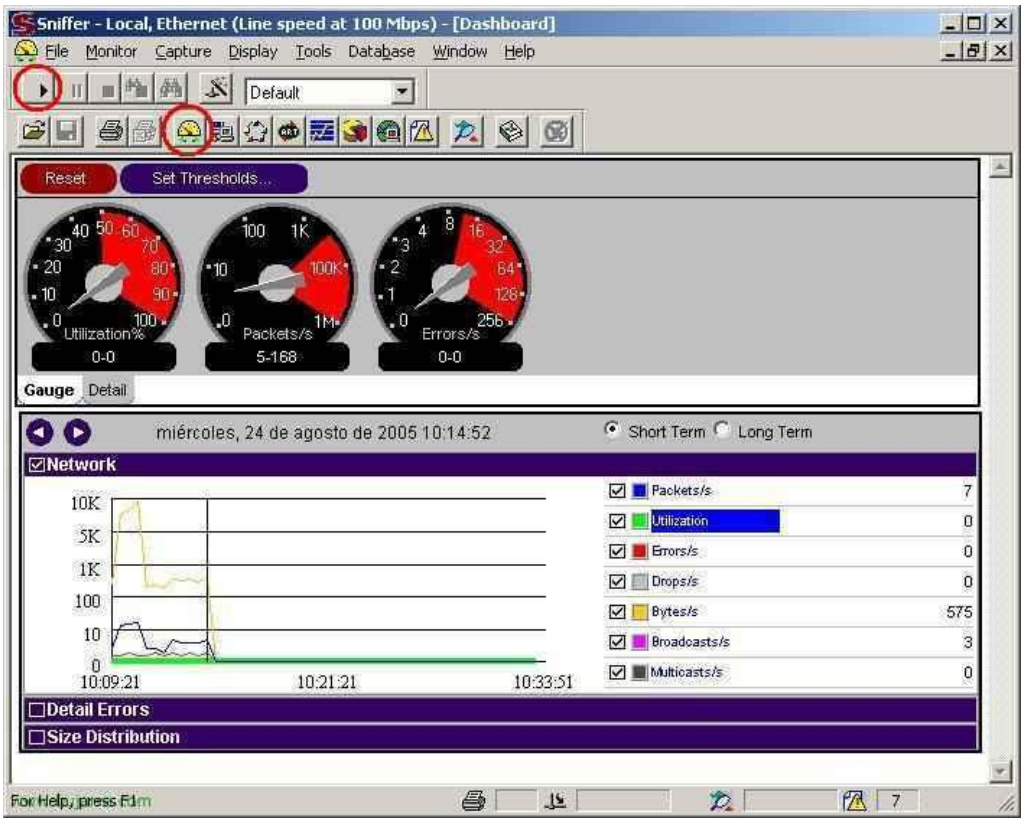
Les analyseurs de protocole serviront principalement à des analyses de dialogue dans le but de régler des difficultés de fonctionnement du réseau (analyse des échanges de tables de routage, de requête DHCP...).

Des fonctions annexes, rarement présentes sur les produits libres, permettront de renseigner le technicien ou l'ingénieur sur l'activité instantanée du segment sur lequel est connectée la machine (et non sur la charge du réseau), un peu comme un compte-tours indique le régime de rotation d'un moteur ou un ampèremètre sur la charge d'un circuit électrique.

De même, l'affichage des machines présentes sur Je réseau local, annoncées au rur et à mesure de ['émission des t rames (l'analyseur raisonne sur J'adresse MAC source de la station Ethernet), la table (dite matrice) construite en fonction des échanges de clients à serveurs. Cette fonctionnalité est très intéressante pour vérifier l'association des postes de travail et des serveurs applicatifs dans les bons VLAN's.

Utiliser un logiciel de gestion de projet

Le logiciel Sniffer Pro propose au technicien ou à l'ingénieur les informations suivantes:
- un état instantané du segment sur lequel est raccordé l'analyseur de protocole
- application Dashboard (tableau de bord) : taux d'utilisation exprimé en %, nombre de trames par secondes, nombre de trames erronées par seconde (voir figure 5.4).
- la table Host (strictement équivalente à la table Host de la MIB RMON + la table statistiques)
- une vue graphique correspondant à la table Matrix de la MIS RMON - le graphe pouvant être présenté sous forme de tableau, plus exploitable dans le cas de gros réseaux composé de multiples nœuds à fort trafic.
- une répartition du trafic par taille de trames.



Sniffer pro Dashboard

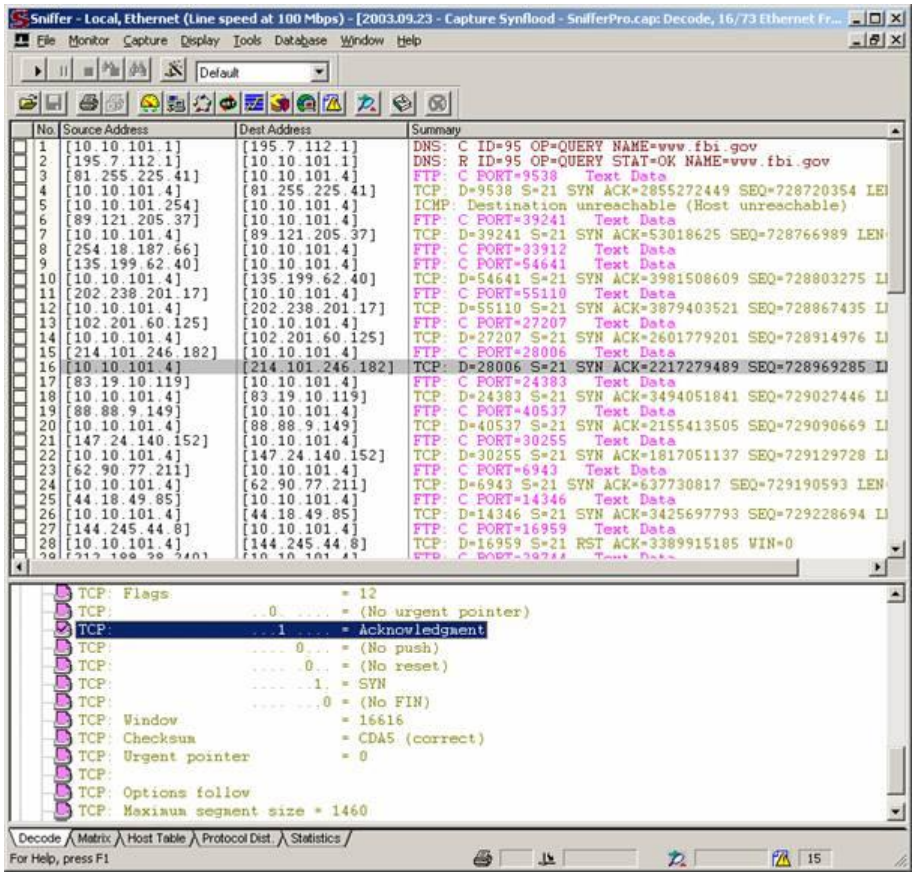
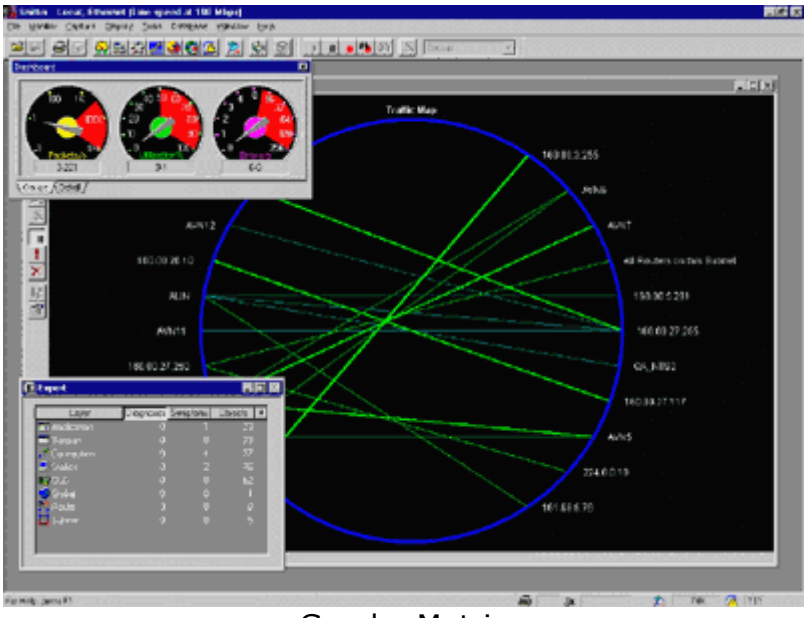


Table Host – Sniffer Pro



Graphe Matrix

Utiliser un logiciel de gestion de projet

Dashboard Colasoft

2.4.2. Faiblesses

Si l'analyseur de protocole offre le net avantage d'être mes en œuvre très simplement, il a l'inconvénient d'avoie une visibilité réduite au domaine de collision, dans la mesure où les réseaux locaux sont organisés en VLAN's.

2.5. Les MIB's RMON et sondes RMON

2.5.1. la MIB RMON

La MIR RMON (Remote Network Monitoring Management information Base), définie par la RFC 2819 de mai 2000) est une MIS, implémentée comme la MIB II dans un élément actif et utilisée par l'Agent pour renseigner un Manager sur le fonctionnement des interfaces réseau. Prévue à l'origine pour un hub, on peut la trouver aujourd'hui dans un commutateur (sous forme de MIB réduite), mais aussi dans un boîtier dédié appelé sonde RMON.

Alors que la MIS II (MIB standard) correspond à la configuration de la machine, la MIB RMON comprend des tables permettant [a collecte des statistiques liées à la couche Interface Réseau du modèle Tep/IP. Dans la pratique, les informations de la MIN RMON correspondent à une interface Ethernet et une interface WAN (interface série).

La MIS RMON comprend 10 groupes, associés aux services suivants:
- Ethernet Statistics Group : contient les statistiques colletées pour chaque interface Ethernet d'un commutateur. Ce groupe est représenté par la table etherStatsTable.

Les informations disponibles sont les suivantes:
- etherStatsDataSource : identifiant de l'interface.
- etherStatsDropEvents : nombre d'évènements reje tés.
- etherStats()çtets : nombre d'octets échangés sur l'interface.
- etherStatsPhs : nombre de trames échangées sur l'interface.
- etherStatsSroadcastPkts : nombre de trames de broaOCast.
- etherStatsMulticastPkts : nombre de trames de multicast.
- etherStatsCRCAlignErrors : nombre de trames échangées avec un CRC faux.
- etherStatsUndersizePkts : nombre de trames dont la taille est inférieure à 64 octets.
- etherStatsOversizePkts nombre de trames dont la taille est supérieure à 1518 octets.
- etherHistoryFragments : nombre de trames collectées tronquées résultant d'une mauvaise gestion de collision (seule l'en-tête de la trame est observé).
- etherHistoryJabbtrs : émissions anormales de bits.
- etherHistoryCollisions : nombre de collisions collectées.
_ etherHistoryUtilization : taux d'utilisation du réseau (exprimé en %).
- Alarm Group : produit des statistiques en cas de dépassement de seuils préalablement paramétrés. Chaque dépassement provoque un évènement (Trap SNMp) stock~ dans les tables du groupe Event.
- Host Group: contient des statistiques associées à chaque host (station Ethernet) découvert sur le réseau local. Les tables hostContromTable, hostTable et hostTimeTable sont alimentées au fur et à mesure des 6changes de trames en fonction des adresses MAC source et destination. Les informations disponibles sont les suivantes:
- hostAddress : adresse MAC de la machine Ethernet.
- hostCreationOrder : numéro d'ordre de découverte du host.
- hostlndex : numéro d'index dans la table.
- hostlnPkts : nombre de paquets reçus sur l'interface pour le host d'index n.
- hostOutPkts : nombre de paquets émis par l'interface pour le host d'index n.
- hostOutOctets : nombre d'octets émis par l'interface pour le host d'index n.
- hostOutf:rrors : nombre d'erreurs émises par l'interface pour le host d'index n.
- hostOutBroadcastPkts ; nombre de broadcasts émis par j'interface pour le host d'index n.
- hostOutMulticastPkts nombre de multkasts émis par J'interface pour le host d'index n.
- Host Top N Croup : util i~ pour générer des rapports avec pour objectif de classer les stations Ethernet en fonct ion des statis tiques des tables du groupe Host. C'est le Manager SNMP qui choisit le nombre de machines à classer et les critères de tri. Ce groupe utilise les tables hostTopNControlTable et hostTopNTable.
- Matrix Group ce groupe associe des statistiques concernant un échange de trames entre deux stations Ethernet. Lorsqu'un nouveau dialogue est détermine, une nouvelle enute est crée dans les tables matrixControlTable, matrixSDTable et matrixDSTable. Les informations disponibles sont les suivantes :
- matrixSDSouroeAddress : adresse MAC source.
- matrixSDOestAddress : adresse MAC destination.

- matrixSDIndex : numro d'index dans la table.
- matrixSDPkts : nombre de trames échangées entre les deux machines Ethernet.
- matrixSDOctets : nombre d'octets échangés entre les deux machines Ethernet.
- mauixSDErrors : nombre d'erreurs comptabilisées pour un échange.
- Filter Group: ce groupe consiste à établir des filtres permettant de marquer des trames pour les capturer ou déclencher un évènement. Ce groupe utilise les tables filterTable et channelTable.
- Packet Capture Croup contient les trames capturées en fonction de critères établis dans le groupe Filter. Les trames sont stockées dans les tables captureBufferTable et bufferControlTable.

- Event Croup: gère la production d'évènements et la notification (sous forme de Trap SNMP) vers un Manager. Contient les tables eventTable et log table. Intègreles informations suivantes:
- eventIndex : identifiant de l'évènement dans la table.
- eventDescription : descriptif de l'événement (message texte).
- eventType : type d'évènement (1 - non dkrit 1 2 - log / 3 - SNM PTrap / 4 -log & SNMP Trap).
- eventCommunity : nom de la communauté associé au message T rap
- eventLastTimeSent : durée écoulée depuis la mise sous tension de l, machine (UpTime) au moment de l'évènement.
- eventOwner : éventuelle restriction de notification de l'évènement.
- eventStatus : indique (si le champ n'a pas pour valeur 1) que l'évènement peut être détruit par l'Agent.

la MIS RMON est une MIS avant tout. Cela signifie qu'elle sera interrogée par le Manager SNMP. Les messages échangés seront les mêmes que ceux l'interrogation et la modification des MIB's standards et des MIBs privées.
Les noms de communautés configurés dans les éléments actifs et connu du Manager et seront repris également.

Compte tenu de la richesse fonctionnelle de la MIS RMON, de la puissance nécessaire à la collecte des données (capture de trames notamment) et de la mémoire important pour le stockage, les MIB's RMON sont parfois implémenté incomplètement dans les éléments actifs, dont le rôle, n'est pas faire de la supervision, mais bien de la commutation ou du routage.

2.5.2. La sonde RMON dédiée

Il est extrêmement rare de voir tout les groupes RMON implémentés dans un élément actif. En particulier les groupes Host,
Matrix et Capture, gros consommateurs de mémoire.

Seront fréquemment rencontrées des "mini-RMON" composées de trois ou quatre groupes, apportant essentiellement des informations statistiques sur le trafic et sur les erreurs (CRC alignement) qui, rappelons-le, sont souvent produites par des problèmes de câblage, bien plus que par des adaptateurs Ethernet en défaut, faits rarissimes aujourd'hui.

La sonde RMON, qui n'est autre qu'une MIB RMON "packagée" que l'on appelle aujourd'hui « Appliance » ne traite que les deux premières couches du modèle OSI (couche Physique, couche Liaison de données), soit la couche Interface Réseau du rnodèle TCP/ IP.

Ces boîtiers, qui présente l'intérêt d'être autonome (équipement dédié), est doté d'un port série pour la configuration initiale IP (adresse, masque, passerelle par défaut, communautés SNMP RO ct RW, adresse du Manager SNMP) et d'une interface Ethernet. A ce sujet, il convient de veiller à ce 'lue cette interface puisse supporter des débits de 10, 100 ct 1000 Mb/s, avec un mode de communication half-duplex ct full-duplex ct une auto-configuration possible pour s'adapter à tout environnement.

Pour approfondir le sujet....

Proposition de références utiles permettant d'approfondir le thème abordé

Le livre **Réseaux informatiques** Par François Pignet

livre sur les réseaux Informatiques s'adresse aux techniciens et ingénieurs en charge de l'exploitation d'un réseau informatique ou qui ont pour projet de déployer, de façon maîtrisée, une infrastructure de communication de données, de visioconférence ou de téléphonie sur IP. Au fil des pages, le lecteur découvrira les enjeux et les intérêts d'une solution de supervision (surveillance, mesure de la charge dans les réseaux, optimisation des performances, appréhension des incidents et des pannes) et aussi d'une administration maîtrisée (sauvegarde et déploiement automatisés des configurations, mise à jour des systèmes d'exploitation) avec la présentation d'outils logiciels de la plate-forme CiscoWorks LMS de Cisco Systems, d'utilitaires et outils d'administration courants.

Sources de référence

Le livre **Réseaux informatiques** Par François Pignet