ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DE LA
MAÎTRISE EN GÉNIE ÉLECTRIQUE
M.Ing.

PAR
GAUTHIER, Martin

SURVEILLANCE DES RÉSEAUX EN TEMPS RÉEL

MONTRÉAL, LE 16 JUIN 2009

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE

M. Michel Kadoch, directeur de mémoire
Département de génie électrique à l'École de technologie supérieure

M. Mohamed Cheriet, codirecteur de mémoire
Département de génie de la production automatisée à l'École de technologie supérieure

Mme Sylvie Ratté, présidente du jury
Département de génie logiciel et des TI à l'École de technologie supérieure

M. Jean-Marc Robert, membre du jury
Département de génie logiciel et des TI à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 26 MAI 2009

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

Je tiens d'abord à remercier M. Michel Kadoch, professeur à l'École de technologie supérieure de Montréal. D'abord pour m'avoir guidé dans ma démarche de recherche et pour m'avoir dirigé tout au long de la rédaction de ce mémoire ainsi que pour ses corrections rapides.

Je tiens à exprimer toute ma reconnaissance à M. Mohamed Cheriet, directeur de Sychromédia pour m'avoir soutenu matériellement sans quoi l'aboutissement de ce projet n'aurait pu être possible.

Par la suite j'aimerais remercier certaines personnes qui m'ont aidé lors du développement du projet. M. François Laurin, employé de l'École de technologie supérieure, qui m'a fourni une aide technique sur différents produits logiciels. M. Jean Charles Cazale, employé de l'École de technologie supérieure, qui m'a fourni une aide technique sur différents produits de la compagnie Cisco.

SURVEILLANCE DES RÉSEAUX EN TEMPS RÉEL

Martin GAUTHIER

RÉSUMÉ

La nouvelle génération d'outils de communication destinés au travail collaboratif amène une dépendance à des caractéristiques précises des réseaux de télécommunication Internet. Synchromédia est un tel système conçu et développé pour le travail collaboratif. Les caractéristiques exigées par la plateforme Synchromédia sont (1) un débit de trafic égal ou supérieur à la vidéoconférence en haut résolution (2) une latence inférieure à celle qu'exige la voix sur IP et (3) le partage d'énorme quantité de données propres aux applications parmi plusieurs correspondants ou usagers répartis sur un vaste territoire géographique.

Le développement de Synchromédia nécessite une adaptation aux caractéristiques du réseau. Afin d'adapter ces propriétés de fonctionnent, un banc d'essai a été conçu, développé et construit dans le Laboratoire de gestion des réseaux informatiques et de télécommunications (LAGRIT). Ce banc d'essai est constitué de plusieurs équipements réseautiques et équipements de perturbation ainsi qu'un générateur de trafic, mais aucun outil de mesure adéquat.

Ce mémoire explore la problématique de la mesure des réseaux de télécommunication afin d'identifier les caractéristiques recherchées pour l'évaluation et la mise en place de différents logiciels de surveillance des réseaux de télécommunication pouvant effectuer la collecte d'information en temps réel de façon intègre sur plusieurs sources simultanément.

Trois systèmes sont testés en exécutant sur le banc d'essai une batterie de scénarios caractéristiques des échanges de Synchromédia. Les résultats sont présentés sous forme de graphiques qui permettent d'analyser rapidement les caractéristiques résultantes.

Mots-clés : mesure, performance, expérience, logiciel.

REAL TIME NETWORK MONITORING

Martin GAUTHIER

ABSTRACT

In the new generation of communication tools toward collaborative work leads to depend on specific characteristics of Internet telecommunications networks. Synchromedia is a software designed and developed for collaborative work. The characteristics required for Synchromédia platform are a traffic flow equals or greater than the video-conference in high resolution with the characteristic latency required for voice over IP while sharing a huge amount of applications data among several corresponding users spread across a wide geographic area.

The development of Synchromédia requires adaptation to the network. To adapt to operate these properties, a network test bed was designed, developed and built in the research laboratory (LAGRIT) *Laboratoire de gestion des réseaux informatiques et de telecommunications*. The test bed includes several pieces of equipment, network equipment and perturbation traffic generator, but no proper measurement tool.

This research explores the problematic of the measurement of telecommunications network to identify theses features for the evaluation and implementation of different software for monitoring capabilities Internet networks that can carry out a collection of information in real time with integrity on several sources simultaneously.

Three systems are tested by running a series of scenarios characteristics of all Synchromédia exchange. The results are presented in graphical form that will quickly analyze the characteristics result.

Keywords: measurement, performance, experience, software.

TABLE DES MATIÈRES

Page

LISTE DES TABLEAUX

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

API	Application Programming Interface
ASN	Abstract Syntax Notation
BD	Base de Donnée
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CLI	Commande Line Interface
CMPI	Common Management Information Protocol
CMU	Carnegie Mellon University
COS	Class Of Service
FAQ	Frequently Ask Question
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LAGRIT	Laboratoire de gestion de réseaux informatique et de télécommunication
LAN	Local Area Network
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MRTG	Multi Router Traffic Grapher
NMS	Network Management Station

OID	Object IDentifier
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
PING	Packet Internet Groper
QOS	Quality of Service
RFC	Request For Comments
RMON	Remonte network MONitoring
RR	Round Robind
RID	Rtg Indentifier
RTG	Real Time Grabber
RTP	Real-time Transport Protocol
SGMP	Simple Gateway Monitoring Protocol
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice over IP
WAN	World Area Network

INTRODUCTION

Les réseaux de télécommunication constituent l'environnement structurel de technologies d'interaction entre les individus. Grâce aux hautes vitesses de transmission maintenant possible et les techniques d'encodage, le réseau offre de nouvelles perspectives notamment en termes d'application interactive voix/données. En contrepartie, les personnes deviennent dépendantes des réseaux. Les pannes et anomalies doivent donc être détectées le plus rapidement possible. La gestion des réseaux a été légèrement négligée lors de déploiements importants et des architectures plus complexes qui s'ensuivit fait que les réseaux sont devenus difficiles à maintenir. Deux aspects rendent la gestion de réseau complexe. D'une part l'hétérogénéité des technologies sous-jacentes et la difficulté d'offrir une vue unifiée du réseau à l'administrateur et d'autre part la grande quantité d'information à collecter et à traiter (Agoulmine et Cherkaoui, 2003).

Ce mémoire présente un modèle de détection de la perturbation par l'entremise d'un système de surveillance des réseaux de télécommunication Internet en temps réel. Il est conçu, développé et expérimenté au Laboratoire de gestion des réseaux informatiques et de télécommunications (LAGRIT) dans le cadre du projet de recherche sur le développement et mise au point d'un banc d'essai réseautique pour la plateforme de travail collaborative Synchromédia.

Le premier chapitre définit l'historique ainsi que la problématique du projet. Cette problématique fait ressortir qu'avec les équipements d'aujourd'hui l'information peut être obtenue beaucoup plus rapidement qu'avec les outils présentement utilisés.

Le second chapitre présente la gestion de réseau et du protocole *Simple Network Management Protocol* (SNMP) et les aspects possibles sur la performance de la mesure des réseaux de télécommunication. Ceci introduit les critères optimaux sur la performance de la mesure des réseaux et des outils de surveillance dont une sélection est analysée et décrite en détail dans le troisième chapitre.

Le quatrième chapitre présente le banc d'essai réseautique de Synchromédia conçu et construit dans le cadre de cette étude avec une description des équipements de commutation, de routage, de perturbation, d'encombrement et de surveillance.

Le cinquième chapitre présente les résultats de la surveillance du banc d'essai obtenus selon une série de scénarios conçus dans des buts précis pour mettre en évidence chaque aspect de la mesure et des impacts sur les différents types de communication que la plateforme Synchromédia permet. Une analyse sur la détection des anomalies est proposée afin d'identifier des éléments d'amorçage des alarmes pour prévenir le dysfonctionnement des équipements et du flux de trafic.

CHAPITRE 1

LA GESTION DE RÉSEAUX

1.1 Réseaux Internet

La voix sur IP, la vidéoconférence et la télé-présence sont de nouvelles applications qui se déploient à tous les niveaux de la société : les entreprises locales, nationales ou internationales, jusqu'aux domiciles des usagers. L'évolution de l'Internet a engendré un besoin de développer de nouvelles technologies de communication orientées vers le travail collaboratif. On peut maintenant envisager l'application de travail collaboratif associé à la médecine, au contrôle centralisé, au partage d'idée.

Le développement de ces applications dépendant du réseau ne s'effectue pas sans contrepartie. La gestion des réseaux est devenue essentielle pour assurer une fiabilité des communications de plus en plus congestionnées en raison de la croissance explosive de la demande sur Internet. Il est crucial que les services de communication du réseau soient disponibles en permanence. Les pannes et dysfonctionnements doivent être détectés très rapidement. La gestion des réseaux effectue cette tâche mais les résultats sont parfois difficiles à obtenir sur des architectures de réseaux très complexes. Un élément que la gestion des réseaux parvient difficilement à surveiller est la perturbation, un effet très contraignant pour la communication en temps réel. La perturbation se caractérise par le délai, la latence, la fragmentation et la perte de paquets. Cet effet est aléatoire, soudain et difficile à prédire et se manifeste surtout en encombrement de liens. Il engendre une dégradation pour toutes les communications en temps réel surtout pour les communications non classées de haute priorité.

Il existe des mécanismes qui permettent de gérer contractuellement des niveaux de services. La qualité de service (QdS) est un mécanisme qui traite le trafic de façon appropriée à sa classe de service. Il parvient à diminuer certains effets perturbateurs comme la congestion dans certaines conditions où la bande passante est restreinte, mais offre un faible degré d'efficacité sur le trafic en temps réel surtout pour le délai avec les équipements disponibles.

1.2 Problématique

Pour la gestion de réseau, la surveillance en temps réel est une solution pour détecter la perturbation. Cette option est possible à condition d'avoir une information précise sur les causes de la perturbation. C'est en grande partie le but de cette recherche de trouver une autre possibilité de détection des anomalies avec les technologies existantes sans engendrer un coût additionnel de matériel et logiciel et poser des actions préventives sur les équipements pour maintenir les flux de trafic. Les travaux de cette recherche sont effectués sur un banc d'essai du réseau de Synchromédia.

1.3 Objectif

Les objectifs définis pour mener à bien notre recherche sont les suivants :

- Déterminer les limites de fonctionnement des équipements pour des flux définis de trafics. Le but est de connaître des points de mesure à ne pas franchir afin de maintenir l'opérabilité des équipements du banc d'essai.
- Déterminer la limite opérationnelle des flux de trafics concernés. Le but est de connaître les caractéristiques de perturbation.
- Déterminer les frontières d'opérations afin de définir des références de détection de la perturbation et de permettre à l'action préventive de prendre effet.
- Déterminer les méthodes de corrections.
- Proposer un mécanisme de corrections.

1.4 Méthodologie

Le fonctionnement de l'application Synchromédia est affecté par différents effets perturbateurs. Le but d'un banc d'essai est de faire subir à l'application une série de perturbation et d'en mesurer les effets.

La première partie de cette recherche est de construire et de configurer le banc d'essai, et par la suite, trouver, adapter ou concevoir un outil de surveillance de tous les éléments de ce réseau en utilisant le protocole SNMP. Une caractéristique recherchée pour la surveillance du réseau est la précision du système d'information. Cette caractéristique est essentielle afin de répondre aux objectifs. L'ensemble est soumis à une série de tests afin de découvrir et d'ajuster les outils de mesure. Le chapitre 2 présente l'état de l'art sur la gestion de réseaux, du protocole SNMP ainsi que la performance de la mesure du trafic Internet. Le chapitre 3 décrit le cheminement sur la mise en place des outils de mesure du banc d'essai

La seconde partie consiste à générer du trafic d'encombrement ainsi que du trafic représentatif de l'application Synchromédia afin de mesurer les limites opérationnelles de l'application sur les équipements du réseau et ainsi obtenir une série de données sur différents aspects de l'effet de la perturbation. De cette façon, on obtient des résultats qui permettent de définir des amorces pour contrer la perturbation.

En troisième partie, l'étude se concentre sur le comportement et l'efficacité de différents mécanismes pour contrer la perturbation. Un des mécanismes étudiés est la qualité de service qui offre plusieurs opération de traitement et de classification. L'objectif principal est d'accorder la priorité aux classes de trafic importantes et sensibles aux variations des flux. Cependant la perception de l'effet bénéfique de la QdS n'a d'égale que l'adaptabilité des applications aux mauvaises conditions du réseau. Le but est d'obtenir dans un premier temps toutes les mesures nécessaires selon les scénarios utilisés pour atteindre les objectifs précédents, et dans un deuxième temps retenir la QdS la plus appropriée. Pour la dernière partie, il s'agit de concevoir le mécanisme qui régira l'ensemble.

CHAPITRE 2

ÉTAT DE L'ART

2.1 Présentation

Ce chapitre offre un bref aperçu de l'Internet, de la gestion de réseau et du standard de gestion de réseau SNMP (Case et al., IETF 1990). La mesure du trafic est définie à la section 2.4. Les critères de performances de la gestion de réseau en temps réel sont exposés à la section 2.6. Les sujets discutés sous SNMP incluent le protocole lui-même, l'architecture de la gestion et la communication des primitives SNMP aux sections 2.3 et 2.4. Aux sections 2.3.2 et 2.3.3 on décrit le modèle de l'agent de gestion qui est la base de tous les systèmes SNMP incluant le système de surveillance présenté au chapitre 3.

2.2 L'Internet

L'Internet, signifiant « International network », est un réseau télématique international issu du réseau militaire ARPANET conçu en 1969 (*Le petit Larousse illustré 2008*, 2007). Trois éléments ont permis sa création. Le premier élément est l'adoption de la technologie de commutation par paquets. Le second élément est l'utilisation uniforme dans tous les réseaux du protocole de communication IP. Le troisième est que les réseaux ayant des propriétés différentes puissent communiquer entre eux. Le protocole IP qui est un protocole sans connexion est décrit par (Reynolds et Postel, IETF 1980). Les règles précises définissent de toutes les méthodes et mécanismes d'échange de paquets d'information entre les nœuds. Le paquet IP est une sorte d'enveloppe qui se compose de deux éléments principaux. Le premier est l'en-tête du paquet IP qui contient des informations de destination et de fragmentation. Le second élément est l'information que le paquet transporte de la source à la destination qui est généralement sous la forme d'un segment *Transmission Control Protocol* (TCP), *User Datragram Protocol* (UDP) ou *Internet Control Message Protocol* (ICMP). IP

a le rôle d'acheminer les paquets de donnée d'un routeur à un autre selon une adresse composée de quatre octets (l'adresse IP). Le protocole TCP (*Tranmission Control Protocol / Internet Protocol*) (Postel, IETF 1980b) qui est situé à la couche transport de la norme *International Organization for Standardization* (ISO) est orientée connexion, c'est-à-dire qu'il contrôle la transmission pendant qu'une session de communication est établie de bout en bout entre deux ordinateurs. Pour chaque paquet reçu, l'ordinateur destinataire transmet des accusés de réception à l'ordinateur émetteur. Si TCP détecte une erreur ou une perte de données, il amorce une retransmission des données jusqu'à la bonne réception des informations. Le protocole UDP (Postel, IETF 1980a) n'est pas orienté connexion, c'est-à-dire l'ordinateur qui émet les paquets IP ne reçoit aucune accusée de réception de l'ordinateur destinataire. Donc, il n'y a aucune correction d'erreur en cas de perte. Les données sont envoyées sous forme de blocs appelés segments. UDP est utilisé pour des diffusions d'information sans fiabilité.

ICMP (Postel, IETF 1981) est conçu pour transmettre des messages de test de contrôle sur des réseaux IP. Le réseau est constitué d'un ensemble de nœuds nommés routeurs connectés par des liens. Les routeurs examinent l'adresse du paquet IP et l'acheminent au nœud suivant jusqu'à sa destination.

2.3 La gestion de réseau

La gestion de réseau est définie comme un ensemble d'activités de surveillance et de services afin d'assurer leur fonctionnement. Ces activités sont regroupées selon leurs fonctionnalités. Plusieurs normes de gestion ont été établies par l'International Standard Organisation (ISO), l'Union International de Télécommunication (UIT) et l'Internet Engineering Task Force (IETF). L'UIT est conçu pour la gestion des réseaux opérateur (SDH, Sonet, ATM) tandis que l'IETF a élaboré le protocole SNMP principalement destiné à la surveillance d'équipement IP.

2.3.1 Domaines de gestion

L'Organisme de normalisation OSI a établi cinq domaines de gestion : (1) la gestion de la configuration, (2) la gestion des performances, (3) la gestion de la sécurité, (4) la gestion des fautes et (5) la gestion des coûts. La gestion de la configuration permet de paramétrer différents objets requis pour gérer la configuration qui comprend la collecte d'information, le contrôle de l'état du système et la sauvegarde de l'état dans un historique. La gestion des fautes permet la détection, la localisation, la réparation et l'enregistrement des historiques des fautes. La réparation nécessite une intervention pour prendre des mesures correctives. La gestion du coût permet de connaître les charges des objets gérés. Le coût est établi en fonction du volume et de la durée de la transmission. La gestion de la sécurité qui concerne le contrôle et la distribution des informations utilisées pour la sécurité. La gestion de la performance comporte la collecte de données et l'analyse statistique afin d'aboutir à la production de tableaux de bord. La gestion de la performance se divise en deux parties : traitement de la gestion de la performance (1) en temps réel et (2) en temps différé.

Pour gérer le réseau en temps réel, il faut avoir les fonctionnalités suivantes :

- Enregistrement des mesures de performance : il faut déterminer les critères et conditions de mesure, la gestion de la collecte d'information, le filtrage, la compilation de statistique, l'adoption de mesures à la demande ou encore la gestion des fichiers de collecte.
- Surveillance de l'activité du réseau par la visualisation de l'utilisation des ressources, le signalement des dépassements de seuil et l'analyse de la performance.
- Changement de configuration proactive et réactive des mesures correctives. La gestion réactive vise à établir lors de la détection d'un problème de performance des mesures de réaffectation des ressources.

La gestion de la performance en temps différé se caractérise par la gestion proactive, l'analyse des informations, les rapports et l'analyse provisionnelle.

- La gestion proactive consiste à prendre des mesures initiales pour éviter les situations critiques.
- L'analyse des informations par la compilation de statistiques, d'historique ou d'indicateur de qualité de service.
- Génération de rapports périodiques et effectués à la demande.
- Analyse prévisionnelle par la constitution de matrice de trafic et la détection de risque de saturation ou d'encombrement et par des simulations de scénarios.

Pour atteindre les objectifs de la recherche, nous ciblons la gestion de réseau sur l'utilisation du modèle de gestion de la performance. Les éléments de gestion est un ensemble d'outils basé sur une même technologie. L'IETF a défini une suite de standards sur la surveillance des réseaux, dont le protocole SNMP.

2.4 La mesure de l'Internet

La mesure du trafic Internet (Estan, 2003) doit être faite pour plusieurs raisons. Premièrement, elle permet de prendre des décisions sur la planification de la croissance des réseaux. Deuxièmement, elle permet d'établir une facturation selon la quantité d'information que le client aura transigée. Troisièmement, elle permet la surveillance des échanges malicieux. Quatrièmement elle engendre la collecte de statistiques des accès faits sur des serveurs de site web soit pour des fins de publicité sur Internet ou de statistique interne aux organisations. Dans les activités de ce mémoire, les principaux éléments d'un réseau sont mesurés afin de connaître le fonctionnement de tous les protocoles et de leurs interactions sur le nœud du réseau incluant l'effet de l'encombrement.

On distingue deux méthodes pour obtenir des données. À partir de l'équipement de réseau qui traite le trafic et par un dispositif spécialisé qui a pour but de capturer du trafic mesuré. Deux types de mesure sont distingués, la mesure passive et la mesure active. La mesure passive enregistre des données qui traversent les nœuds du réseau. Une règle générale est plus le nombre de points de mesure est élevé, plus détaillée et précise sera l'information sur

le comportement du réseau. En contrepartie, l'analyse sera plus complexe. La mesure active transmet des paquets qui mesure le comportement du réseau lorsque parcouru. La mesure active est utilisée pour mesurer les propriétés du réseau : le délai, la perte de paquets, la gigue, la largeur de bande, la stabilité symétrique et la topologie. La communication en temps réel, la qualité de service est les ententes de services *Service Level Agreements* SLA font usage de métrique de mesure active pour la surveillance des paramètres.

Afin de répondre à la problématique de la détection de la perturbation, les deux types de mesures sont employés. En général la mesure active est accomplie par l'utilisation d'une sonde de réseau qui est décrite à la section 3.5. La mesure passive fait utilisation du protocole SNMP.

2.5 Le protocole SNMP

SNMP signifie *Simple Network Management Protocol.* Ce protocole a été créé en 1988 afin de répondre au besoin d'une architecture générale de gestion de réseaux routés pour le protocole TCP/IP (Simoneau, 1999). C'est un protocole client-serveur.

2.5.1 Historique

La gestion des réseaux était accomplie au départ par des échanges de messages ICMP qui offraient des caractéristiques pratiques comme *echo & echo-reply* et *time stamp & time stamp reply* et sans doute la commande la plus connue utilisant ces messages est PING (Muuss, 1983). La famille d'outils ICMP permettait de vérifier la présence de l'équipement en spécifiant le temps de réponse entre l'hôte et le composant réseau. D'autres protocoles rudimentaires ont connu une brève existence comme *Common Management Information Protocol* (CMIP) ou *High-Level Entity Management System* (HEMS) (Stallings, 1999). Avec le temps SNMP, un descendant de *Simple Gateway Monitoring Protocol* (SGMP)(Ben-Artzi, Chandna et Warrier, 1990), a acquis de l'importance en intégrant des fonctionnalités comme

Remote network Monitoring (RMON) qui offre aux gestionnaires de réseau l'habilité de surveiller des réseaux ainsi que des sous réseaux. D'autres éléments comme *Management Information Base* (MIB), *Network Manager Station* (NMS) et les agents ont été développés afin d'intégrer une structure de gestion de l'information à SNMP. SNMP a été étendue à d'autres équipements réseau et informatiques. Il est devenu le protocole de surveillance par défaut étant donné l'importance de son utilisation dans l'internet.

2.5.2 Élément du protocole SNMP

Il existe plusieurs versions du protocole SNMP mais les principaux sont : SNMPv1, v2p, v2c, v2u et v3. SNMPv1 est la première version du protocole telle que définie dans le RFC1157 (Case et al., IETF 1990). SNMPv2p, SNMPv2c et SNMPv2u (Case et al., IETF 1996) incluent des mises à jour par rapport à la première version et l'ajout de nouvelles opérations, de nouveaux types de données. SNMPv3 (Case et al., IETF 1999) comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations de SNMPv2p. Pour cette recherche la surveillance a été faite avec le protocole SNMPv2c.

Tableau 2.1 Présentation des différences de versions SNMP
Tiré de (Agoulmine et Cherkaoui, 2003), p.32)

Version	**SNMPv1**	**SNMPv2**	**SNMPv3**
Réponse plus complète aux demandes		X	X
Getbulk		X	X
Authentication		X	X
Cryptage		X	X
MIB1 (MIBI)	X		
MIB2 (MIBII)		X	X
Architecture évolutive			X

SNMP se compose de quatre éléments. Pour cette recherche les trois éléments principaux sont utilisés pour la mesure du trafic :

- Agent de gestion
- Station de gestion NMS
- Base d'information de gestion MIB
- Protocole de gestion réseau

2.5.3 L'agent de gestion

L'agent de gestion est un module qui réside sur chaque équipement ou élément de réseau que l'on cherche à gérer. L'agent est fourni par le manufacturier de l'équipement et est essentiel à la collecte des données. C'est généralement un composant logiciel spécialement conçu pour chaque équipement. Il récolte continuellement les informations de l'équipement et les emmagasine dans la base de données de gestion MIB. Pour chaque requête reçue de la station de gestion, l'agent transmet une réponse spécifique. Il existe des alternatives pour la collecte des données pour des équipements qui ne sont pas équipés d'un agent. Ce mémoire ne traitera pas cette problématique.

2.5.4 Station de gestion

La station de gestion est une station de travail dotée d'une unité de traitement central rapide, d'une interface graphique et beaucoup d'espace disque; elle exécute les requêtes des applications qui contrôlent les éléments de réseau. Il existe deux types de requête. Le premier, effectué par la station de gestion, demande à l'équipement surveillé de fournir à chaque requête des données spécifiques. La seconde est la possibilité de transmettre, de la station de gestion, des requêtes spécifiques pour changer des paramètres de l'équipement. De nos jours de nombreux outils de gestion sont disponibles et certains gratuitement. Ces outils permettent aux logiciels gestionnaires de réseau d'emmagasiner les informations utiles

à l'analyse. Il est important que les outils puissent manipuler la base de données d'information de gestion des équipements MIB afin d'être en mesure d'effectuer des requêtes aux équipements.

2.5.5 La base d'information de gestion (MIB)

MIB signifie *Management Information Base.* Elle réunit deux éléments. Le premier est la gestion de l'objet *Managememement Object* (MO). La seconde est l'identifiant de l'objet *Object Identifier* (OI). Le mot objet signifie l'entité unique de l'équipement pour laquelle une information SNMP existe. L'équipement possède plusieurs milliers d'objets qui lui sont propres. Afin d'uniformiser les objets, ils sont regroupés dans une identité distincte à chaque objet. Cette identité unique est classée selon un regroupement numéroté de la forme standardisée définie à la section 2.5.6.

Il existe deux façons d'identifier un objet. Chaque objet possède un nom unique qui décrit plus ou moins bien le contenu de ce dernier. Par exemple, un objet qui contient la description textuelle de l'entité est appelé *sysDescr*. Une autre façon d'identifier le même objet est par la représentation numérique *1.3.6.1.2.1.1.1.* Cette méthode facilite l'indexation des objets dans MIB. La gestion de l'objet est accomplie par l'accumulation de donnée propre à chaque objet de l'entité.

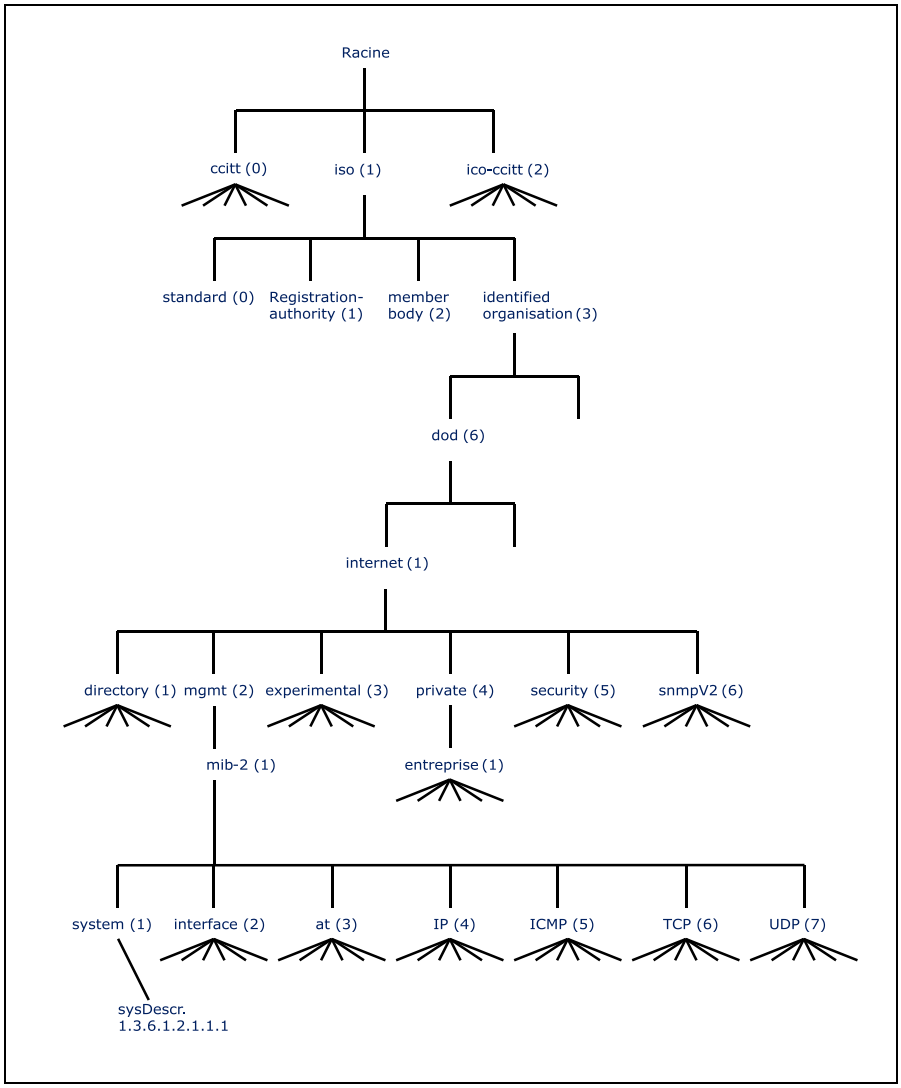


Figure 2.1 Schéma de l'arborescence MIB.

Le regroupement des objets d'une même entité se nomme MIB. MIB est une table à structure permanente qui permet de classer chacune des informations contenues à l'intérieure des équipements surveillés, et ce, dans un ordre bien précis. Il existe deux standards de table MIB, soit MIB-I et MIB-II. MIB-II est l'extension de MIB-I à laquelle ont été ajoutés des objets pour contenir différentes valeurs supplémentaires de l'équipement. Dans l'arborescence de MIB-II, on retrouve le groupe *Private Entreprise MIB*. Cette branche des MIB permet aux équipementiers de définir leur propre classe de MIB. Comme la convention de la norme sur l'attribution des numéros des adresses machine des interfaces Internet, MIB

offre selon la convention IANA un numéro d'entreprise sous le préfix OID 1.3.6.1.4.1.*. Sur le site de l'organisation, on dénombre 32,103 tables MIB (*SMI Network Management Private Enterprise Codes:* , Octobre 2008). Cette recherche est en partie basée sur l'information que ces MIBs peuvent contribuer à la mesure du trafic.

2.5.6 La syntaxe de l'objet MIB

Tous les objets contenus dans MIB sont définis de façon formelle. SNMP utilise des sous structures de la notation *Abstract Syntaxe Notation One* (ASN.1) (Simoneau, 1999) pour définir chaque objet individuel ainsi que la structure de table MIB dans son entier. Cette définition spécifie le type de donnée de l'objet. ASN.1 est un standard international ISO dont le but est la structure des données utilisées dans le protocole de communication. Il existe plusieurs types d'objet définis dans ASN.1. Le type de l'objet est important, car il donne la nature de l'information aux requêtes SNMP exécutées par la station de gestion et des agents de gestion.

Pour cette étude, différents types sont utilisés, mais les types principaux des objets sont *gauge* et *counter*. On peut comparer ces types à une variable entière positive. Dans le cas de *counter* c'est une valeur de 2^{32} pour un système fonctionnant à 32 bits ou 2^{64} pour les systèmes à 64 bits qui incrémentent sans pouvoir décrémenter.

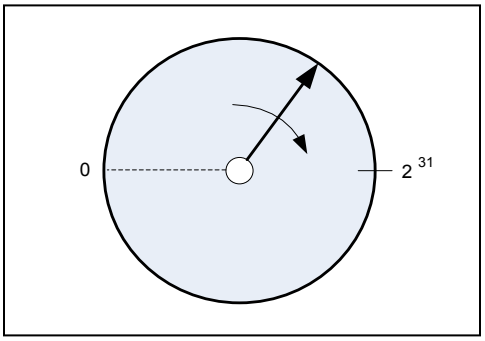


Figure 2.2 Représentation de counter.
Tiré de (Stallings, 1999)

Lorsque la valeur atteint le maximum de 2^{32}-1 (4,294,967,295), elle redémarre à zéro, (*Voir* Figure 2.2). C'est le type le plus fréquemment défini. Il est utilisé principalement pour compter les paquets ou les octets reçus ou transmis. La *gauge* à la différence de *counter* incrémente et décrémente continuellement (*Voir* Figure 2.3). Elle comprend un entier positif qui fluctue selon une échelle de précision de 2^{32}. La *gauge* est souvent utilisée pour mesurer une valeur actuelle d'une entité. Un exemple serait le nombre de paquets contenu dans une queue ou la température de l'unité de traitement central.

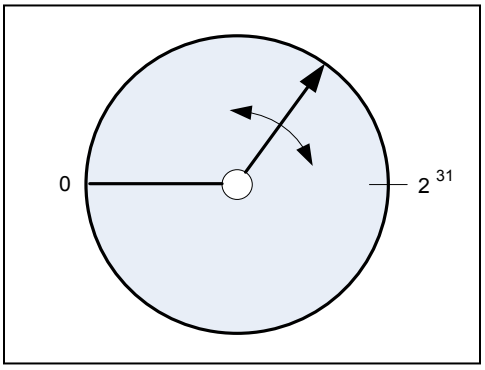


Figure 2.3 Représentation du pas incrémental gauge.
Tiré de (Stallings, 1999)

D'autres types comme *string, timer, byte*, ou *ipaddress* sont une infime partie des types définis. Mais l'ASN.1 ne fait pas l'objet de cette recherche. On note qu'il existe plusieurs autres types d'objet, mais les plus importants pour cette étude sont *counter* et *gauge*.

2.5.7 Message du protocole de gestion de réseaux

La station de gestion fait des requêtes pour lesquelles elle a l'autorisation et demande les valeurs de divers éléments d'information. L'agent retourne les valeurs contenu dans la MIB pour chaque requête à la station de gestion (*Voir* Figure 2.4). Les requêtes peuvent être spécifiques, par une liste d'un seul ou de plusieurs noms de variables, de rapporter des informations répondant à certains critères.

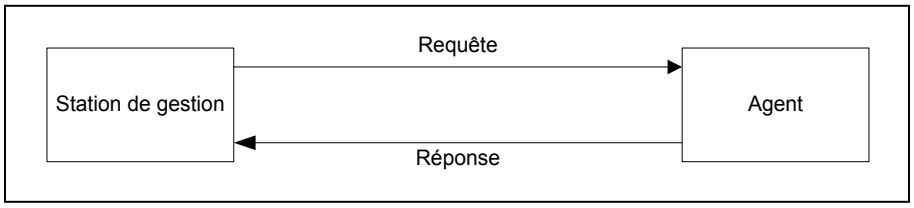


Figure 2.4 Structure des échanges SNMP.

Le protocole fonctionne sur UDP/IP par les ports 161 et 162. Les opérations de base supportées par toutes les versions de SNMP sont l'inspection et l'altération des variables MIB. Ces opérations sont :

Get : Permets à la station de gestion de récupérer la valeur MIB de la variable à l'agent.

Set : Permets à la station de gestion d'assigner la valeur MIB à la variable à l'agent.

Trap : Permets à un agent d'aviser la station de gestion d'un évènement significatif.

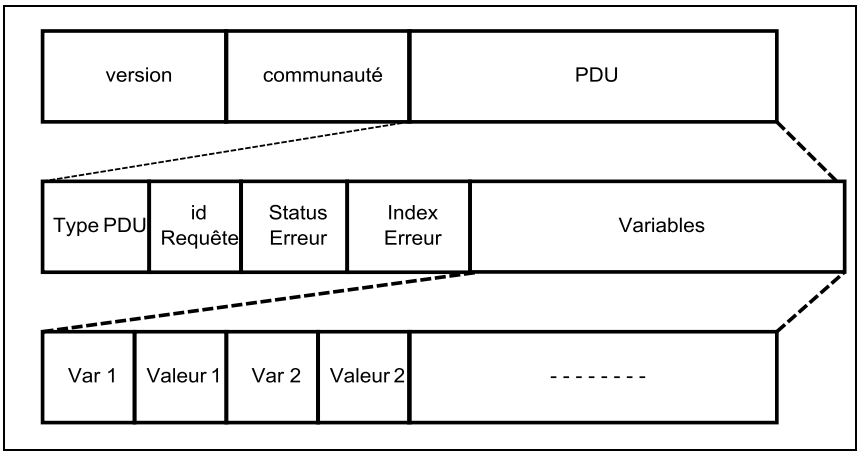


Figure 2.5 Contenu du paquet SNMP.

Le message SNMP est composé de trois éléments:

Version du protocole : 0 pour la version 1 (Case et al., IETF 1990) elle correspond à la version SNMP -1. La version doit être identique pour chaque requête entre l'agent et la station de gestion afin d'obtenir une réponse de l'entité.

Nom de communauté : C'est une chaîne de caractères commune entre l'agent et la station de gestion qui autorise la requête à l'entité.

PDU : C'est le message de la requête SNMP. Ce sont des *Protocol Data Unit* (PDU) de la couche applications.

Il existe cinq types de messages SNMP que la station de gestion demande ou obtient des données.

Get Request : Pour obtenir une donnée individuelle unique d'un objet géré. La commande *GetRequest* est transmise par la station de gestion, elle inclut une liste de variables de gestion pour laquelle elle requiert la valeur MIB de l'agent désigné. Une réponse est reçue si la commande *GetResponse* de l'agent récupère une valeur avec succès.

Get Next Request : Pour obtenir une donnée individuelle unique ordonnée d'un objet géré. Elle est similaire à la commande *GetRequest*. L'agent recueille la variable MIB suivante ordonnée par le classement lexicographique par rapport à la variable précédente. L'utilisation de cette commande est destinée principalement à parcourir l'arbre et à déterminer tous les éléments de la table MIB.

Get Respond : Provient de l'agent afin de répondre à une requête *GetRequest*, *GetNextRequest*, ou *SetRequest* avec un message PDU, qui contient la valeur de l'objet ou un message d'erreur en cas de problèmes. L'agent de gestion vérifie la valeur dans le message PDU reçu et traite la requête par la suite.

Set Request : Provient de la station de gestion qui tente d'altérer la valeur d'une variable MIB spécifique au lieu d'en faire la lecture. L'agent vérifie que chaque variable MIB existe et traite le mode d'accès approprié pour l'écriture ou lecture et écriture pour écrire une nouvelle valeur à l'objet géré.

Trap Response : Provient de l'agent qui transmet à la station de gestion de manière asynchrone un message amorcé par un événement pré programmé. Ces évènements sont définis dans le MIB et sont connus de la station de gestion et de l'agent.

À noter que *SetRequest* et *TrapResponse* n'ont pas été utilisés pour les scénarios de test sur la mesure du trafic. Le champ ***Id.Requête*** qui est l'identificateur de la requête est défini par la station de gestion lors de l'envoi d'une requête et utilisé par l'agent dans sa réponse. Cela permet d'associer la réponse à la requête. Le statut d'erreur est défini par l'agent. Il est toujours à zéro dans une requête.

Tableau 2.2 Message d'erreur aux requêtes SNMP
Tiré de (Case et al., IETF 1990)

Statut d'erreur	Nom	Description
0	*noError*	Pas d'erreur
1	*tooBig*	Réponse de taille trop grande
2	*noSuchName*	Variable inexistante
3	*badValue*	Écriture d'une valeur invalide
4	*readOnly*	Essai de modification d'une variable en lecture seulement
5	*genErr*	Autre erreur

L'index d'erreur indique la variable qui a provoqué l'erreur uniquement dans les cas *noSuchName*, *badValue* et *readOnly.* Une liste des noms des *variables* et de leur *valeur* termine le message SNMP.

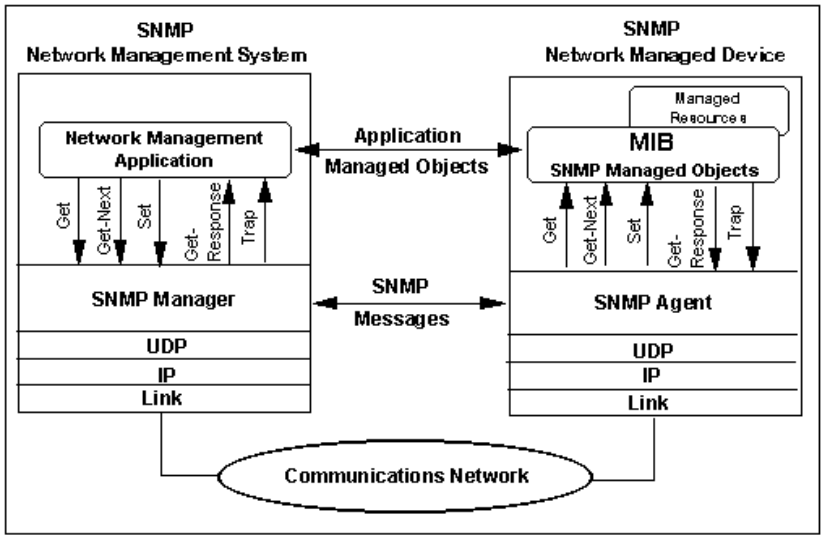


Figure 2.6 Topologie de fonctionnement session SNMP.
Tiré de (Stallings, 1999)

La figure 2.6 résume les points décrits tout au long de ce chapitre. Il présente la structure par laquelle le protocole SNMP prend la mesure de l'internet.

2.6 Fonction de la surveillance et de la performance

Un préalable essentiel pour la gestion des réseaux de communication est l'habilité de mesurer la performance du réseau. La sélection des indicateurs appropriés devient souvent une difficulté que les points suivants définissent :

- Il y a trop d'indicateurs en utilisation.
- La signification de l'indicateur n'est pas bien comprise.
- Certains indicateurs proviennent seulement d'un fournisseur d'équipement.
- Certains indicateurs ne sont pas comparables entre eux.
- Les indicateurs offrent une mesure précise, mais sont incorrectement interprétés.
- Le traitement des indicateurs prend trop de temps et le résultat final ne peut être utilisé pour contrôler l'environnement du réseau.

2.6.1 Les indicateurs de performance

Les indicateurs de performance (Stallings, 1999) sont catégorisés en deux groupes. Le groupe de service qui inclut les indicateurs selon la disponibilité, le temps de réponse, la précision et le groupe d'efficacité inclut les indicateurs selon le débit et le taux d'utilisation. Pour cette étude l'intérêt se porte sur tous les indicateurs.

La disponibilité est définie comme l'accès au réseau, à l'équipement, à l'application, à un OID, ou à l'agent d'information exprimé en pourcentage du temps. Cette disponibilité est basée sur la fiabilité de tous les composants, mais pour cette recherche la disponibilité est synonyme d'engagement de l'activité à tout instant. Une diminution du pourcentage de la disponibilité est jugée comme un indicateur en soit.

Le temps de réponse est défini comme le temps pris pour qu'une réponse apparaisse à la station de gestion après avoir initié la requête. Plusieurs éléments contribuent au délai du temps de réponse, dont la puissance de fonctionnement de l'unité centrale de traitement. L'intrusion des processus peut pénaliser le traitement de la requête; plus le processus de traitement des requêtes de la station de gestion est prioritaire, plus court sera le temps de réponse. Il faut comptabiliser les délais occasionnés par le passage de la requête à travers des différents éléments et composants réseau notamment :

- Le délai de transmission qui est directement occasionné par la vitesse du lien.
- Le délai de commutation qui est directement lié à la vitesse de commutation de l'équipement.
- Le délai de traitement de la requête par l'agent occasionné par le niveau d'importance accordé au processus, le taux d'occupation de l'unité de traitement central et la latence des divers éléments nécessaires comme disque, mémoire, base de données.
- Le délai de la queue qui est occasionné si un trop grand nombre de requêtes sont transmises en même temps sur le même lien.

L'addition de tous les éléments donne le temps de réponse d'une requête. Le temps de réponse est facile à obtenir et pour cette recherche est considéré comme l'indicateur le plus important.

L'indicateur de la précision est défini comme la transmission valide de donnée entre l'agent et la station de gestion. Généralement il est rare avec le protocole de la couche liaison et la couche de transport d'avoir des erreurs de données, mais pour cette recherche la précision de la donnée est synonyme d'objectivité dans le contexte du moment qui à lieu sur-le-champ par rapport aux autres donnés obtenus.

L'indicateur de l'utilisation est la mesure du degré d'occupation en pourcentage de temps de l'activité de traitement de l'équipement à accomplir les tâches usuels. Plus fréquemment cette mesure est obtenue, plus précise et granulaire sera l'information. Elle permet ainsi d'obtenir une mesure fiable du comportement du réseau. Pour cette recherche le taux d'occupation est perçu comme une limitation de la non-disponibilité de la ressource à effectuer des tâches additionnelles par rapport à l'emploi habituel. L'utilisation la plus importante de cet indicateur est la recherche de goulot d'étranglement potentiel et des aires de congestion. Le temps de réponse augmente souvent avec l'accentuation croissante d'utilisation d'une ressource. Ceci est surtout vrai avec le traitement des files d'attente.

Le dernier indicateur de performance est l'indicateur du débit. Elle indique le degré de circulation ou de l'écoulement du trafic sur le réseau par unité de temps tout simplement. Pour cette recherche aucune autre signification ne l'accompagne. Cette mesure est orientée au niveau de l'application. Voici des exemples :

- Le nombre de transactions accumulées pour un type pendant une période de temps.
- Le nombre de sessions pour une application pendant une période de temps.
- Le nombre d'appels pour un environnement à commutation de circuits.
- Le nombre d'enregistrements fait simultanément pour une période de temps.

Avec les cinq indicateurs de performance, on obtient un système d'information qui offre un inventaire d'élément accru pour l'aide aux décisions.

2.6.2 Surveillance optimale

Trois composants sont nécessaires pour colliger tous les indicateurs de la performance. Le premier est l'optimisation de la mesure qui accumule des statistiques sur le trafic réseau. Le second est l'optimisation du logiciel de présenter l'information des donnés et du résultat d'analyse. Le troisième est la capacité de générer du trafic afin de mesurer le comportement du réseau selon une charge contrôlée.

La mesure optimale est d'ordinaire accomplie par les agents d'équipements comme des commutateurs et des routeurs. Ces agents sont en position d'observer tout le trafic entrant et sortant du nœud. Le nombre de connexions et le taux de trafic par connexion. Ceci procure une information détaillée sur le comportement des nœuds. Cependant, cette mesure s'obtient avec une accentuation sur le taux d'occupation de l'unité de traitement centrale.

La capacité de générer du trafic permet de mesurer avec détail la performance réelle du réseau. Que ce soit avec un appareil ou un composant logiciel, cet outil programmable peut générer du trafic afin d'obtenir des résultats aux différents scénarios suivants :

- Quel est l'effet de la charge de trafic sur l'utilisation, le débit, et le temps de réponse?
- À quel moment la performance du réseau se dégrade?
- Quels sont les compromis entre la stabilité, le débit et le délai?
- Quelle est la capacité maximum des chemins en condition normale?
- Quel est l'effet de petits paquets sur la performance du débit et du délai?

L'optimisation de l'analyse ne sera pas approfondie dans cette recherche. Elle est néanmoins un composant essentiel à l'analyse des résultats. Nous retenons de la surveillance optimale, l'indicateur sur la précision des données et leurs intégrités.

2.6.3 Fréquence d'échantillonnage

Pour tous réseaux, il ne suffit pas de saisir au démarrage de la station de gestion les informations et d'être à l'écoute des indications transmises par les agents. Les gestionnaires de réseaux appliquent une politique sur la collecte des informations perçues des requêtes SNMP aux équipements.

Cette politique est en relation avec la taille du réseau, ce qui comprend un nombre élevé d'agents et de stations de gestion. Trouver le juste équilibre entre le maximum d'information que l'on cherche sans atténuer la performance des équipements est un facteur qui peut se calculer avec l'équation suivante (Stallings, 1999) (Ben-Artzi, Chandna et Warrier, 1990) :

$$N \leq T / \Delta \tag{2.1}$$

- N = nombre d'éléments
- T = l'intervalle de temps en minute entre chaque échantillonnage
- Δ = temps moyen minimum requis pour exécuter un seul échantillonnage. Ce temps inclus les éléments suivants :
  - a = le temps pour initier la demande.
  - b = le délai du réseau entre la station de gestion et l'agent.
  - c = la réception et le traitement de la requête.
  - d = la réponse de l'agent.
  - e = le délai du réseau entre l'agent et la station de gestion.
  - f = la réception et le traitement de la requête.

Pour simplifier l'équation, on assume que $a = c = d = f$ pour le temps de traitement et que $b = e$ pour le délai du réseau alors on obtient :

$$N \leq T / (4a + 2b) \tag{2.2}$$

Soit un réseau qui transmet des requêtes SNMP toutes les cinq minutes. L'exécution de la requête prend 50ms et le délai dans le réseau est de 1ms. La grosseur du paquet est de 1000 octets. Le Δ est de 0.202 secondes. Donc

$$N \leq (5\ x\ 60)/0.202 \approx 4{,}500 \tag{2.3}$$

Dans cet exemple un seul gestionnaire de réseau peut gérer un maximum de 4,500 objets toutes les cinq minutes. Pour notre recherche, un des sous objectifs est d'obtenir le maximum d'information toutes les secondes par des requêtes SNMP. Dans un exemple du banc d'essai décrit au chapitre 4, l'exécution de la requête *GetRequest* et *SendRespond* prend 6.5 millisecondes, le délai dans le réseau est inférieur à 8 nano secondes donc négligeable.
Donc

$$N \leq (\tfrac{1}{60}\ x\ 60)/0.0065 \approx 153 \tag{2.4}$$

Pour cette recherche, le gestionnaire peut gérer un maximum de 153 objets toutes les secondes. Donc un système de surveillance comprenant dix gestionnaires, c'est le cas du gestionnaire du banc d'essai, ils peuvent gérer un maximum de 1,530 objet. Ainsi, on obtient un système d'information qui offre une vision plus complète et plus précise du comportement du réseau en temps réel. Conséquemment, l'aide à la décision sera plus évidente afin de valider ou non le trafic perturbateur sur tous les équipements du réseau. Ceci à condition que les cinq indicateurs de performance soient respectés.

2.7 Fonction de la qualité de service

Pour répondre à la problématique de cette recherche, un élément qui contribue à minimiser les effets perturbateurs aux interfaces des équipements est la qualité de service. Dans le cas des applications qui exigent souvent une grande largeur de bande sans avis, sensible à la perte de donnée, le paramètre du pire cas de la performance est généralement appelé la qualité de service. Dans l'Internet, la qualité de service réfère à l'habilité du réseau de fournir un traitement approprié pour les différentes classes de trafic. L'objectif principal est d'accorder la priorité aux classes de trafic importantes et sensibles aux variations des flux. Il offre un mécanisme aux interfaces encombrées de prendre des décisions sur le traitement des files d'attente et le rejet « drop » des paquets. La perception de l'effet bénéfique n'a d'égale

qui l'adaptabilité des applications aux mauvaises conditions du réseau ou que ce dernier offre des performances accrues. Mesurer et surveiller les besoins des mécanismes existants de la qualité de service permet de peindre un portrait du fonctionnement même si le réseau possède des qualités acceptables qui sont loin d'être idéales.

2.7.1 Mécanisme de la qualité de service

La définition de la qualité de service de réseau Internet est basée sur une variété de paramètres qui déterminent la métrique du modèle de la QdS. Les paramètres d'ingénierie principaux sont déterminés par :

- La largeur de bande. Elle signifie la portion de la capacité du chemin réseau de bout en bout disponible pour les flux de données pour les applications.
- Le délai. Il correspond au temps que prend un paquet d'information à être transporté à la destination. Le délai réseau est une combinaison du temps de propagation, du temps de traitement du processus et le temps passé dans les files d'attente et du temps de routage entre la source et la destination.
- La gigue ou la variation de délai. Cette variation est souvent causée par le remplissage des zones tampons des routeurs durant une période d'encombrement.
- Perte de paquets. La perte de paquets survient lorsque le paquet parcourant le réseau n'atteint pas sa destination. Pour la communication en temps réel, la perte de paquets survient lorsque le paquet met trop de temps à atteindre sa destination. L'utilité de l'information n'étant plus valable, le paquet est rejeté.

Le mécanisme de la qualité de service est la classification du trafic. Elle est le squelette sur lequel se joint une multitude d'algorithmes de traitement. La classification est un traitement selon des règles variées qui s'appliquent au niveau 2 du modèle ISO sur la valeur du champ *Class of Service* (CoS) de l'en-tête du vlan, au niveau 3 sur la valeur du champ *DiffServ code point* (DSCP) de l'en-tête IP du paquet et au niveau 4 sur le numéro de port des segments TCP ou UDP.

2.7.2 Le marquage de la qualité de service

Le marquage est l'action qui impose aux trames, paquets et segments, la classe de trafic. Ce marquage définit le traitement subséquent que subira l'information sur son trajet au travers des équipements de commutation et de routage dans le réseau entre la source et la destination. Le marquage de la trame Ethernet est constitué de trois bits ce qui définit huit niveaux de classification ou priorité (0 à 7)(Postel, IETF 1981). Le marquage du paquet IP utilise six bits, ce qui définit jusqu'à 64 niveaux de classification (0 à 63). Cependant, ces niveaux ont été catégorisés selon six classes de priorité afin d'avoir le marquage des trames (Blake, IETF 1998) au niveau des paquets : une classe prioritaire *Expedited Forwarding* (EF) (Jacobson, Nichols et Poduri, IETF 1999), quatre classes *Assured Forwarding* (AF) qui déterminent pour chacune d'entre elles trois priorités de rejet des paquets (Heinanen et al., IETF 1999) et une classe *Best Effort* (BE).

2.7.3 L'ordonnancement

L'ordonnancement est la méthode par laquelle le trafic est réparti par classe de priorité. C'est un des mécanismes qui permet de gérer le traitement de la file d'attente d'un routeur encombre lorsque plusieurs flux réseau une même interface. Le but est d'obtenir une garantie des flux prioritaires par l'isolement des autres par une répartition contrôlée et équitable. On dénombre sept configurations de traitement des files d'attente :

- Priority Queuing
- Custom Queuing
- Weighted Fair Queuing
- Class-Based Weighted Fair Queuing
- Low Lantency Queuing
- IP RTP Priority
- Modified Deficit Round-Robin

2.7.4 La surveillance « policing »

La surveillance a pour but de prescrire la conformité du flux, donc l'accès au réseau en préservant les autres flux d'un comportement excessif d'une source. La surveillance peut marquer, modifier ou refuser un flux non conforme. Il impose son action sur le trafic entrant sur une interface. Le *policing* utilise le sceau à jeton selon trois différents mécanismes de mesure (Odom et Cavanaugh, 2004).

2.7.5 Le lissage

Le lissage du trafic consiste à réguler la vitesse des flux par le contrôle de la cadence du débit des paquets selon les classes de trafic afin de le conformer aux règles programmées. Deux méthodes sont utilisées, le lissage par sceau percé (leaky bucket) et le lissage par sceau à jeton (token bocket).

- Sceau percé fournit un mécanisme qui permet de rendre une rafale de trafic à un flux constant de trafic sur le réseau en fixant le débit à un nombre maximum fixe bits par seconde.
- Sceau à jeton fournit un mécanisme de contrôle de basé sur l'apport de jeton qui détermine le flux de trafic par un nombre de paquets comparable. Ce mécanisme permet aussi de paramétrer les rafales de trafic.

Quatre paramètres sont utilisés pour configurer le lissage.

- Tc : Intervalle de temps en milliseconde sur lequel Bc peut transmettre des données
- Bc : Nombre de bits par seconde qui peut être transmit dans l'intervalle de temps Tc.
- Be : Quantité de bits transmis sur une période d'inactivité. Doit être supérieure à Bc.
- CIR : Taux de données transmises en bits par seconde.

Les interfaces peuvent transmettre sur leur interface de sortie un nombre limité de bits à un taux équivalent au taux de la cadence de l'horloge. Pour obtenir un lissage d'une valeur inférieure au taux du débit moyen de l'interface, il faut transmettre des données sur une

période de temps inférieure. Les valeurs sont calculées comme suit pour une interface d'un débit de 1536 Kbps à laquelle on désire un lissage qui représente la moitié.
Si

$$Bc = Tc * CIR \tag{2.5}$$

Avec un scénario ces formules lissent le trafic selon un taux (CIR) de 128 kbps et le Tc de 125 ms.

Donc.

$$Bc = 0.125\ seconde * 128{,}000\ bits/seconde = 16{,}000\ bits \tag{2.6}$$

Avec un second taux CIR de 1,536,000 Tc sera de

$$Tc = 16{,}000 / 1{,}536{,}000 = 10\ ms \tag{2.7}$$

Ceci permet seulement une transmission de 10 millisecondes par tranche de 125 millisecondes pour cette interface afin de lisser le trafic à un taux de 128 kbps.

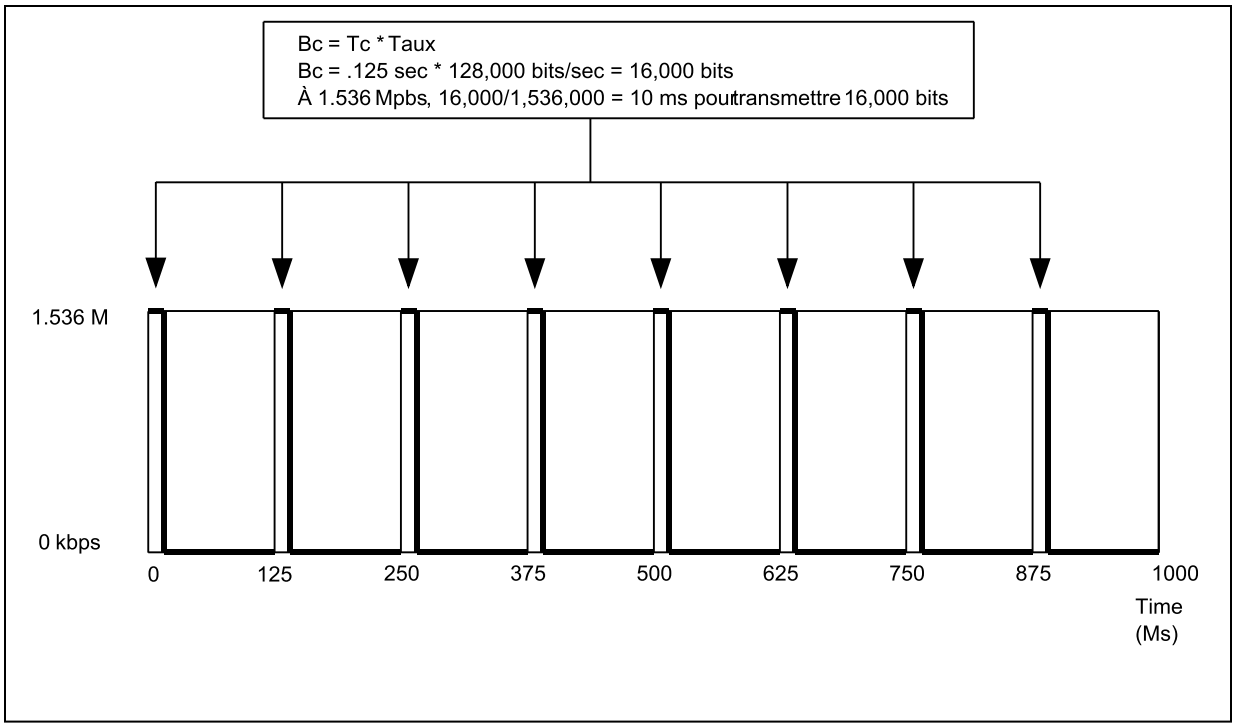


Figure 2.7 Fonctionnement du lissage.

2.7.6 Le lissage par sceau à jeton

Le sceau à jeton (Bc) permet la conformité et l'excès du trafic. Le nombre de jetons admissibles dans le sceau (Bc) représente le droit de transmettre ou de recevoir 1 octet, car un jeton équivaut à un octet. Si le paquet contient un nombre égal ou inférieur d'octets à la quantité de jetons dans le sceau (Bc) alors le paquet est conforme. Le système supprime les jetons du sceau égal au nombre d'octets selon le contrat et exécute l'action de la règle programmée. Cependant si le nombre d'octets du paquet est plus grand que le nombre de jetons dans le sceau, le système ne supprime aucun jeton et effectue l'action sur l'excès.

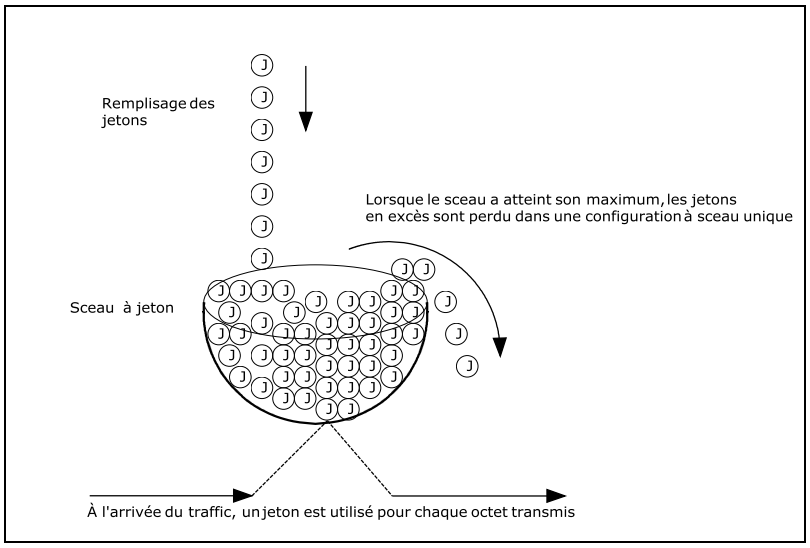


Figure 2.8 Fonctionnement du lissage par sceau à jeton.

2.7.7 Le lissage par double sceau à jeton

Double sceau à jeton permet la conformité (Bc), l'excès (Be) et la violation du trafic. Le principe est le même que le sceau à jeton simple, cependant si le nombre d'octets est plus grand que le nombre de jeton (Bc) mais égal ou inférieur à la somme des deux sceaux à jeton (Bc + Be) alors l'action du paramètre de l'excès sera traitée. Si un paquet contient un nombre qui est supérieur au nombre de jeton (Bc) et (Be) alors l'action de violation sera traitée.

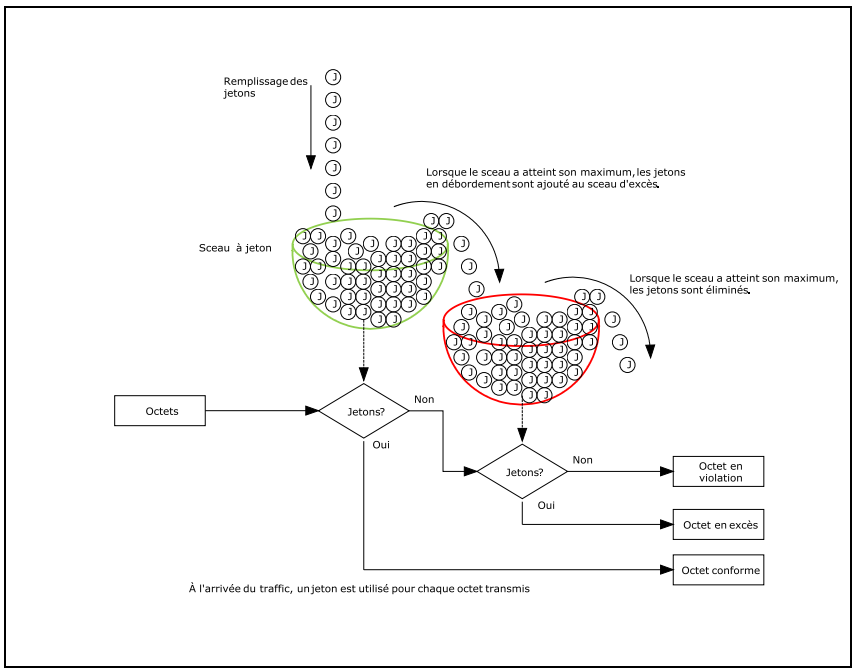


Figure 2.9 Fonctionnement du lissage par double sceau à jeton.

2.7.8 Sceau à jeton à taux fixe

Sceau à jeton à un taux de débit selon le paramètre (Cir). Le principe est semblable au lissage. Le remplissage des sceaux et déterminé par un paramètre Tc qui est déterminé par :

$$Tc = Bc / Policed\ rate \tag{2.8}$$

Le système regarnit le sceau à jeton Bc à tous les Tc secondes en rajoutant un nombre Bc de jetons. Le principe de fonctionnement est le même qu'avec le système à deux sceaux, avec l'ajout que le système ajoute des jetons dans le sceau Bc et l'excédentaire des jetons sont ajoutés dans le second sceau Be. Les jetons reçus par la suite seront perdus.

2.7.9 Les queues et la congestion

Un des fondements de la qualité de service est l'évitement de l'encombrement des interfaces par des mécanismes de traitement selon des principes de rejet des paquets lorsque les queues deviennent saturées. On dénombre cinq mécanismes :

- (RED) *Random Early Detection* réduit l'encombrement dans une queue en rejetant délibérément un pourcentage de paquets aléatoires avant que la queue sature. Ceci a pour effet de réduire la charge des connexions TCP.
- (WRED) *Weighted RED* est presque identique à RED. La seule différence est la sélection est basée sur la valeur de la préséence IP ou de la valeur de différence associée au code de service (DSCP) du paquet. Sur les équipements du banc de test, WRED ne peut être associé avec un autre mécanisme de traitement des queues. Le rejet des paquets selon WRED est basé sur un pourcentage suivant quatre facteurs :
    - La taille moyenne de la queue
    - Le seuil minimum
    - Le seuil maximum
    - Le MPD *Mark Probability Denominator*
- (FRED) *Flow-based WRED* permet de résoudre le problème du trafic UDP dont la source est insensible à la perte de paquet comme TCP avec RED ou WRED. FRED est caractériser par un flux de trafic unidirectionnel entre une source et une destination qui partage la même couche transport et le même protocole. Sept champs sont utilisés pour déterminer si le paquet est parmi le flux existant :
    - L'adresse IP de la source
    - Le numéro de port de la source
    - L'adresse IP de destination
    - Le numéro du port de destination
    - Le protocole de la couche 3
    - Le numéro de préséance ou DSCP
    - L'interface sur laquelle le paquet est reçu

- (CBWRED) *Class-based WRED* permet d'effectuer le comportement du rejet aléatoire basé sur la classe de service DSCP au lieu du rejet basé sur le chargement de la file d'attente.
- (TD) *Tail Drop* permet d'effectuer le rejet des paquets qui arrive lorsque le chargement de la file d'attente de l'interface de sortie est remplie. Le rejet affecte toutes les classes de service et s'effectue jusqu'au moment où la file d'attente peut faire usage de son espace.

2.7.10 Les queues et la gestion de la congestion

Un des objectifs de cette recherche est de mettre en place un mécanisme pour contrer l'effet de la perturbation. Les éléments de la qualité de service présentés aux sections précédentes décrivent tous les composants employés pour le mécanisme retenu qui est la qualité de service par *Low Lantency Queuing* LLQ.

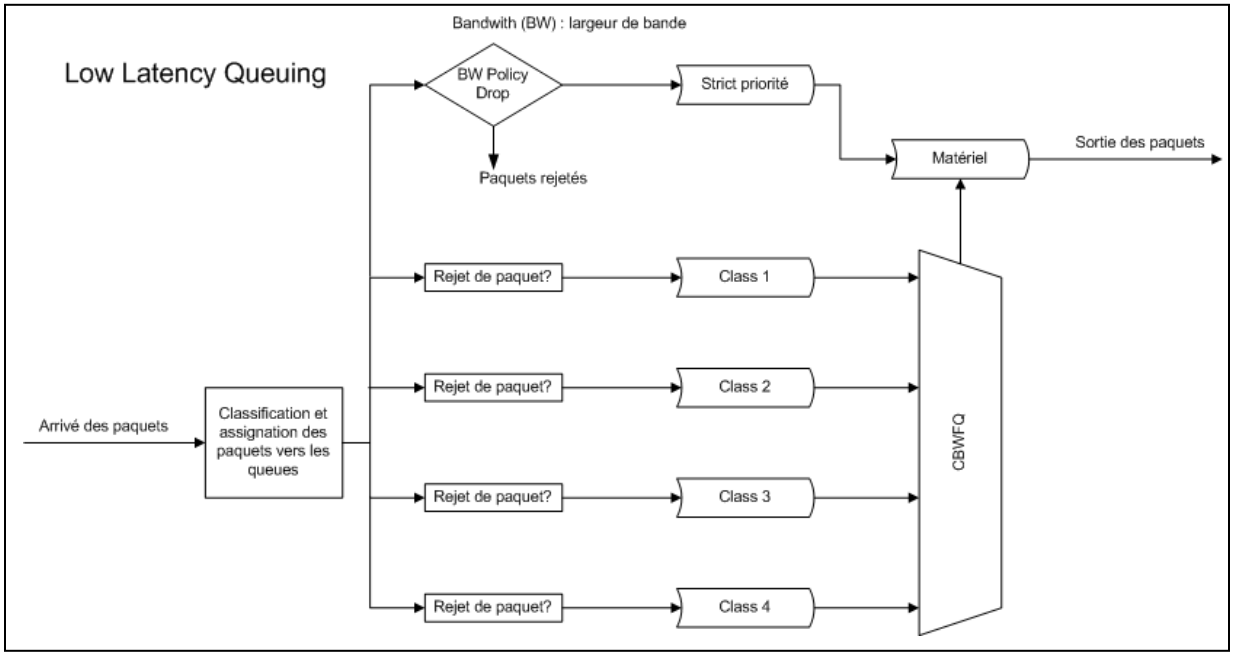


Figure 2.10 Algorithme de la QdS L.L.Q.

Ce mécanisme possède une queue de priorité stricte dédiée au trafic de haute importance comme la voie sur IP afin de minimiser le délai de bout en bout et la variation du délai dans le flux des paquets. Cette queue obtient toujours la priorité sur les autres queues associées aux autres classes de trafic pour accéder la file d'attente de l'interface de sortie. Cette queue permet d'assurer ainsi un débit minimum de trafic. Cependant lorsque cette queue subit un encombrement de trafic, elle ne peut transmettre plus que le minimum garanti et le surplus de trafic est rejeté.

Les classes de trafic inférieures sont traitées par l'ordonnancement *Class-Based Weighted Fair Queing* CBWFQ pour accéder la file d'attente de l'interface de sortie.

CHAPITRE 3

OUTIL DE SURVEILLANCE

3.1 La surveillance des réseaux

Dans les grandes organisations, plusieurs applications et services utilisent fréquemment les réseaux d'ordinateurs pour tout type de communication. La plupart des nouvelles technologies ont adopté le réseau IP comme moyen de communication par défaut. Le réseau IP transporte maintenant de la voix sur IP, la vidéo des caméras de surveillance ainsi que les informations de contrôle des systèmes CVAC (*chauffage, ventilation, air conditionné*). La gestion des réseaux est nécessaire afin d'organiser de façon la plus rentable le comportement du réseau pour toutes ces applications. Cependant, cette recherche porte sur la problématique de la perturbation du réseau et l'effort est dirigé vers un composant nécessaire à la gestion de la surveillance. La surveillance a pour but d'observer avec attention le comportement du réseau de façon à exercer un contrôle.

3.2 Famille des outils de surveillance

Il existe trois modèles d'outils de surveillance pour les réseaux IP. Le premier modèle est la surveillance des nœuds d'un réseau via le protocole SNMP. Trois outils logiciels ont été testés sur le banc d'essai, soit MRTG, CACTI et RTG. Le second modèle de surveillance se base sur le flux du trafic réseau. Celui-ci fait la classification selon des critères précis de toutes les communications sur IP qui passe au travers des équipements. Deux d'outils sont présentés à la section 3.4 soit Netflow (Liu et al., 2006), (Welcher, 2005) un protocole propriétaire à la compagnie Cisco et sFlow (Atsushi et Katsuyasu, 2007). Le troisième modèle est de type renifleur de trafic IP. Le renifleur capture toutes les trames, paquets et segments qui traversent une interface réseau. Il décode et affiche selon un inventaire de protocoles, le contenu de chaque élément du trafic. WireShark (Orebaugh, Syngress Media Inc. et Books24x7 Inc., 2007) descendant d'Ethereal est le renifleur le plus répandu du fait

qu'il est gratuit et fonctionne avec plusieurs types de systèmes d'exploitation. Il existe également des analyseurs de protocole ou analyseurs de trafic qui sont des logiciels spécialement conçus pour analyser le trafic réseau. Ils sont souvent rattachés à une plateforme matérielle qui inclut un ordinateur dédié. Pour cette recherche trois types de plateforme matérielle sont utilisés. Le détail de ces équipements est décrit au chapitre 4.

3.3 Net-SNMP

L'outil logiciel le plus simple pour effectuer des requêtes SNMP mais néanmoins essentiel à plusieurs autres logiciels de surveillance et de gestion réseau est Net-SNMP (Net-SNMP, mars 2007). Net-SNMP est une suite de logiciels à ligne de commande qui permettent d'utiliser le protocole SNMP de la version 1 à la version 3. Ces logiciels fonctionnent en IP v4 et IP v6. Net-SNMP trouve racine en 1992 dans le groupe de développement de *Carnegie-Mellon University* (CMU). Le code a été rendu disponible à la communauté et adopté aujourd'hui pour un grand nombre de systèmes incluant Linux et Unix-BSD. Des interfaces utilisateur (*Application Programming Interface* (API)) ont été développées pour mieux supporter et rendre plus conviviale l'utilisation de SNMP. Des applications de gestion de réseau comme *Multi Router Traffic Grapher* (MRTG) et CACTI sont des environnements qui utilisent à la base les outils Net-SNMP.

Net-SNMP est composé des logiciels suivants :

- *SNMPGET* et *SNMPGETNEXT* font des requêtes uniques d'information sur un équipement.
- *SNMPWALK, SNMPTABLE* et *SNMPDELTA* font des requêtes multiples d'information sur un équipement.
- *SNMPSET* manipule les configurations d'un équipement.
- *SNMPDF*, *SNMPNETSTAT* et *SNMPSTATUS* font des requêtes de l'information fixe d'un équipement.
- *SNMPTRANSLATE* fait la conversion entre la forme numérique et la forme textuelle d'un OID de MIB et affiche la structure du MIB.

Dans le cadre de cette recherche, cinq logiciels de cette suite ont été utilisés. Le logiciel *snmpwalk* a été utilisé pour explorer tous les MIB et OID des équipements du banc d'essai décrit à la section 4.1. Le but est de sonder l'apport supplémentaire que peuvent représenter ces OID au système d'information. Pour un équipement, l'exécution de cette commande génère 15,102 OID différentes. Avec une grande quantité d'information, le choix des OID à surveiller en temps réel devient tout un casse-tête. Afin d'effectuer une sélection d'objets pertinents pour cette recherche, un script en Perl a été conçu afin de présenter l'information de chaque objet en trois éléments. Le premier élément identifie chaque objet par le MIB et l'OID sous la forme textuelle avec le type de variable et son contenu. Le deuxième élément identifie le même objet sous sa forme numérique. Le troisième élément indique la définition contenue dans la table MIB de cet objet. Un exemple du résultat est illustré à la figue 3.1

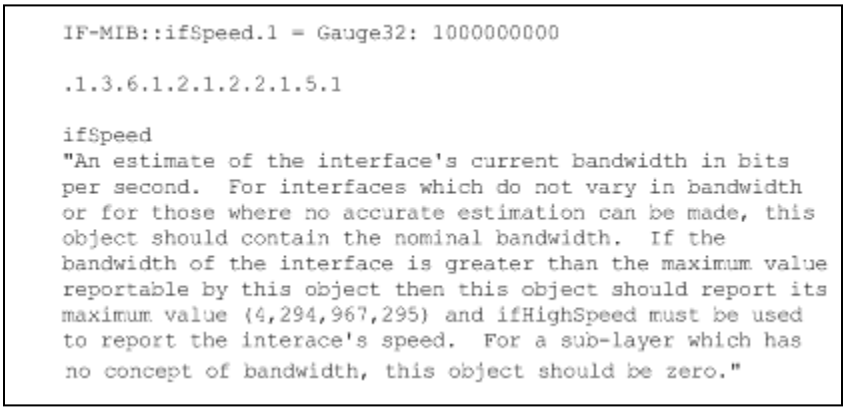


Figure 3.1 Description de l'information OID.

Le choix des OID est fait en fonction de la pertinence des informations pour la surveillance du réseau. Cette liste est présentée au chapitre 4

3.4 Les flux de trafic réseau NetFlow et sFlow

Les outils d'analyse du flux de trafic réseau sont généralement constitués de deux éléments. Le premier est le générateur de flux soit un commutateur ou un routeur équipé d'analyseur de flux de trafic réseau. Chaque équipement transmet un flux de données constant qui contient

des informations comme l'adresse IP source et destination, le protocole et l'interface. Le second élément est le collecteur de flux qui reçoit ces données d'un ou plusieurs générateurs de flux. Le collecteur accumule et emmagasine l'information afin de publier des rapports et offrir une analyse aux administrateurs de réseaux.

3.4.1 NetFlow

C'est un protocole de la compagnie Cisco créé en 1996 (Cisco Systems, 2007). Il permet de caractériser le trafic qui passe au travers d'un routeur ou un commutateur. Chaque paquet est examiné selon une sélection de cinq à sept critères qui sont :

- L'adresse IP source du paquet.
- L'adresse IP de destination du paquet.
- Le numéro du port du paquet source.
- Le numéro du port du paquet de destinations.
- Le type de protocole de niveau 3.
- La classe de service du paquet.
- L'interface logique du routeur ou du commutateur par lequel le paquet traverse.

NetFlow regroupe les paquets selon les mêmes caractéristiques *fingerprint* dans une base de données. L'information peut être consultée directement sur l'équipement ou être exportée sur un serveur. À la différence de SNMP où un serveur doit extraire l'information de l'équipement, NetFLow exporte périodiquement l'information par la détection du flux par TCPFIN/RST et selon la charge du réseau. De plus, une horloge interne aide à déterminer la fréquence d'exportation des données qui varie de 15 secondes à 30 minutes. Une famille d'outils comme Flow-Tools (Fullmer) collecte les informations NetFLow afin d'enregistrer celles-ci dans des fichiers ou dans une base de données. D'autres outils comme *FlowScan* (*FlowScan - Network Traffic Flow Visualization and Reporting Tool*), *Ntop* (Deri et Carbone, 1998) ou *Nfsen* (*NfSen - Netflow Sensor*) permettent de consulter via un site Web

les différentes statistiques que représentent ces informations. Les expériences avec Netflow ont été faites avec la version 9 et les utilitaires NFcapd et NFdump (Haag, 2007).

Le rapport du trafic NetFlow obtenu dépend de l'outil utilisé. Ntop et NFsen sont des outils qui génèrent des rapports identifiant les adresses IP et les ports les plus utilisés et aussi ils permettent de rapporter le flux de trafic par interface des équipements. Les outils utilisés pour cette recherche ne permettent pas de suivre ni de rapporter des flux de trafic de bout en bout qui aide à l'analyse. L'échantillonnage du trafic avec la version de Netflow présent sur les équipements n'est pas offert, de plus les paramètres de l'exportation des données sont limités. Dans ce contexte l'utilité de NetFlow n'est que le rapport des flux trafic classé selon différents paramètres. Une description des expériences avec les équipements de test ainsi que des résultats obtenus sont présentés au chapitre 5.

3.4.2 sFlow

Une autre technologie populaire est sFlow (Phaal, Panchen et McKee, IETF 2001). Basé sur l'échantillonnage des paquets, sFlow consiste d'un algorithme d'échantillonnage représenté par un agent implémenté dans l'équipement de commutation ou de routage. Il définit le format des échantillons transmis au collecteur de données central. Il a été développé pour la surveillance continue des trafics à des vitesses du giga-octet ou plus. Il emploie deux mécanismes d'échantillonnage, le premier est l'échantillonnage statistique des paquets des flux de commutation. Le second est l'échantillonnage statistique selon un intervalle de temps des interfaces réseau. Ces mécanismes font partie intégrante de l'équipement et sont exécutés par le gestionnaire logiciel du réseau.

En raison du type des équipements disponibles pour la partie pratique des essais, aucun de ces équipements ne possède un agent de collecte sFlow. Aucune expérience n'a donc été tentée sur la surveillance des réseaux avec sFlow.

3.5 MRTG

Le premier outil de surveillance installé sur le banc d'essai est MRTG (Seagren et Books24x7 Inc., 2007) (Oetiker, octobre 2008) qui signifie *Multi Router Traffic Grapher*. C'est un outil constitué de scripts en langage Perl pour lire les requêtes SNMP et un programme en langage C pour auditer le trafic et créer des graphiques représentant la collection de données. Ces graphiques sont contenus dans une page *World Electronic Broadcast* (WEB) qui peut être consultée de façon anonyme. Cet outil n'a pas été retenue favorisée par son successeur CACTI.

3.6 CACTI

Le second outil de surveillance testé est CACTI (*Cacti - a complete network graphing solution* Aout 2008). C'est un environnement semblable à MRTG qui offre une convivialité plus intéressante pour la configuration et le graphisme. Basé sur l'utilisation de RRDTools (Oetiker, 2008), CACTI offre des éléments de plus par rapport à MRTG. D'une part, la configuration des éléments est plus simple. On peut y insérer des items externes à SNMP. Selon la quantité d'information, les graphiques peuvent afficher plusieurs éléments simultanément. Cette visualisation peut s'effectuer par le choix d'un intervalle de temps variable. La base de CACTI et d'autres outils de cette famille sont l'utilisation de RRDTools. RRDTools est une suite d'outils logiciels dont l'élément principal est une base de données à taille prédéfinie qui contient les résultats comme des requêtes SNMP obtenus par le programme *snmpget* et archivés selon le principe de l'ordonnancement de la répartition mieux connu par l'expression *Round Robin*. Le contenu de la base de données s'obtient sous forme d'un graphique, ou sous forme textuelle. Lors de la création de la base de données RRD, il faut spécifier trois éléments : la source de donnée, les archives de donnée et la quantité de données archivées. Une fois la base de données créée elle est immuable à la variation des sources des données et à la granularité des échantillonnages.

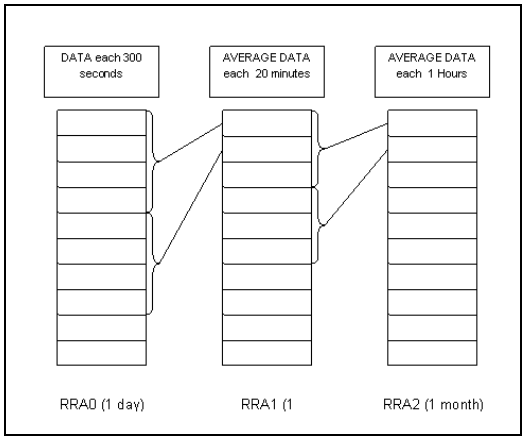


Figure 3.2 Topologie des tables de données de Cacti.

Comme illustré (*Voir* Figure 3.2), le nombre d'espaces fixes est déterminé à la création de la base de données. Dans le principe de *Round Robin* lorsque la table est remplie et qu'on insérer une nouvelle donnée, celle-ci prend la place de la plus ancienne information et ainsi de suite, comme dans un carrousel. Avec cette méthode la base de donnée ne grossit jamais. Si on désire emmagasiner une grande quantité de données, il faut créer le fichier dont la taille pourrait être limitée par le système de fichiers. La taille du fichier pour conserver à toutes les secondes pour une année serait de 252 MB. Pour le projet de recherche, cela signifie avoir de l'espace pour plus de 800 OID donc 201,600 MB d'espace disque. On pourrait utiliser la méthode d'archivage proposé dans les exemples de création des bases de données c.-à-d. créer une table d'échantillonnage pour les secondes, une seconde table pour les minutes, un troisième pour les heures et ainsi de suite. Lorsque la table des secondes est pleine, la moyenne de tous les échantillons est inscrite comme une seule entrée dans la table des minutes et ainsi de suite pour les heures. Selon cette méthode la taille du fichier sera de 146 Kb, mais on perdrait l'intégrité des données ce qui est à l'encontre des critères de performance du projet de recherche. En plus de la version graphique, on peut exporter les données sous forme textuelle. Cependant, les données exportées ne sont pas les données importées dans la base de données de RRD, mais une proportion entre le maximum et le minimum selon le temps.

Sans référence, les données exportées n'ont aucune relation et aucune signification. De plus pour le projet il faut être en mesure de pouvoir combiner plusieurs sources de données dans le même graphique. Avec RRD la combinaison doit se faire à la création de la base de donnée si on désire obtenir un graphique à plusieurs courbes. L'inconvénient est la flexibilité et la grosseur du fichier du DB qui peut atteindre la capacité du système de fichier.

Malgré les avantages de la surveillance que procurent l'application CACTI et RRDTools pour ce projet de recherche, une autre plateforme de surveillance doit pouvoir contenir une énorme quantité de données, un taux d'échantillonnage dans la moyenne par seconde et la représentation graphique flexible multi courbe programmable ainsi que de pouvoir exporter les données de façon intègre. RTG est l'outil qui répond le mieux aux attentes.

3.7 RTG

Le défi de recueillir une très grande quantité d'information et d'emmagasiner une vaste quantité de données dans un temps donné sans avoir un impact sur les équipements du réseau est en principe l'idée derrière *Real Time Grabber* (RTG) (Beverly, 2002). Les concepteurs devaient supporter plusieurs centaines d'équipements avec plusieurs milliers d'objets et avoir l'habilité de retenir toute cette information dans son état original, et ce, indéfiniment. RTG est un environnement flexible, extensible (*Scalabable)* et très performant pour la récolte des requêtes SNMP. RTG a été développé et expérimenté en partie chez WorldCom. Les administrateurs devaient surveiller les équipements de la dorsale OC-48 qui était en constante évolution. Ce réseau était composé d'une centaine d'équipements OC-48 équipés d'une centaine d'interfaces. Les systèmes de surveillance qu'ils utilisaient étaient inappropriés pour maintenir la gestion d'un environnement en forte croissance. RTG est un programme qui recueille l'information SNMP pour l'insérer dans une base de données relationnelle et procure une interface pour générer des requêtes d'information complexes et des rapports. RTG est doté des caractéristiques uniques suivantes : il est conçu pour fonctionner sur Unix en service. Donc, il ne dépend pas du contrôle direct de l'usager ou du système. Il est écrit

en langage C ce qui lui procure une grande rapidité sans solliciter un interpréteur de commande. Il est en mode d'opération multifile (*multithread*) dans un fonctionnement asynchrone pour l'échantillonnage est l'insertion des donnés dans la base de donnée.

3.7.1 RTGPOLL

RTGPOLL est le programme principal de la suite RTG qui recueille les données SNMP et les insère dans une BD. Par l'utilisation multifile, il permet des requêtes en mode multitraitement et asynchrone ainsi une requête ne peut être bloquée par d'autres. La conception permet d'avoir plusieurs requêtes simultanément ce qui accroît la performance et diminue le temps de réponse. De plus selon la liste séquentielle des OID, RTGPOLL sélectionne de façon aléatoire les objets par lesquels il transmet les requêtes SNMP afin de prévenir la surcharge de plusieurs requêtes SNMP sur le même équipement. Le programme fait la lecture de deux fichiers *rtg.conf* et *targets.cfg*. Ce dernier contient la liste des OID pour tous les équipements ainsi que les entrées dans la base de données. Il est créé avec un programme en langage Perl *rtgtarmakr.pl*. Selon un intervalle de temps configuré dans *rtg.conf*, les résultats des requêtes SNMP sont insérés dans une base de données MySQL. RTG offre au projet de recherche plusieurs éléments essentiels, d'une part une rapidité pour la saisie d'un grand nombre de requêtes simultanés, et la conservation intègre des données. Les caractéristiques vitales pour observer en temps réel le réseau et de pouvoir appliquer les correctifs nécessaires.

3.7.2 MySQL

MySQL (Williams et Lane, 2004), une base de données relationnelle très populaire avec 11 millions d'installations et 100 millions de téléchargements, est devenu la base de données de choix. MySQL possède l'habilité de s'interfacer avec plusieurs logiciels comme Apache, PHP, Perl et Python. Elle fonctionne sur plus d'une vingtaine de plateformes comme

Windows, Linux, Hp-UX, etc. Un avantage de MySQL est qu'il est possible de consulter l'information via une ligne de commande.

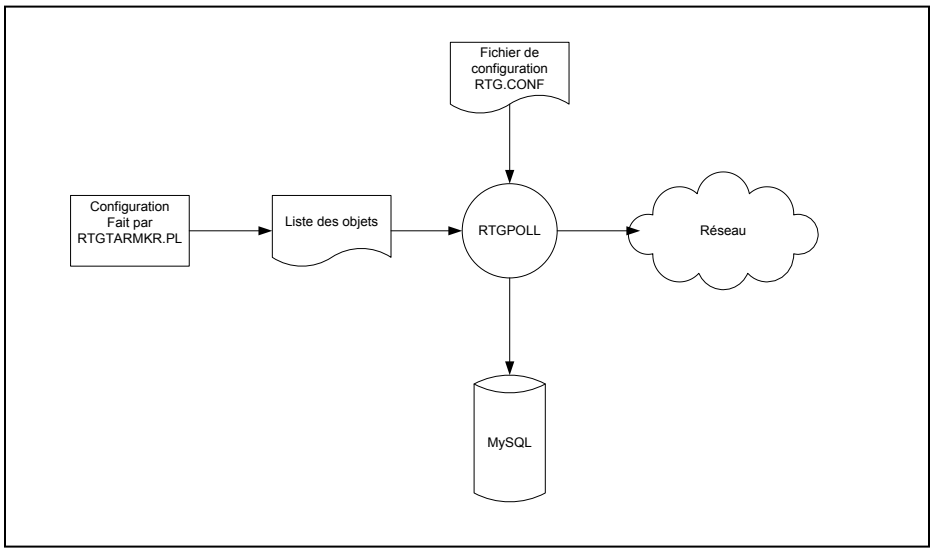


Figure 3.3 Diagramme de fonctionnement de RTG.

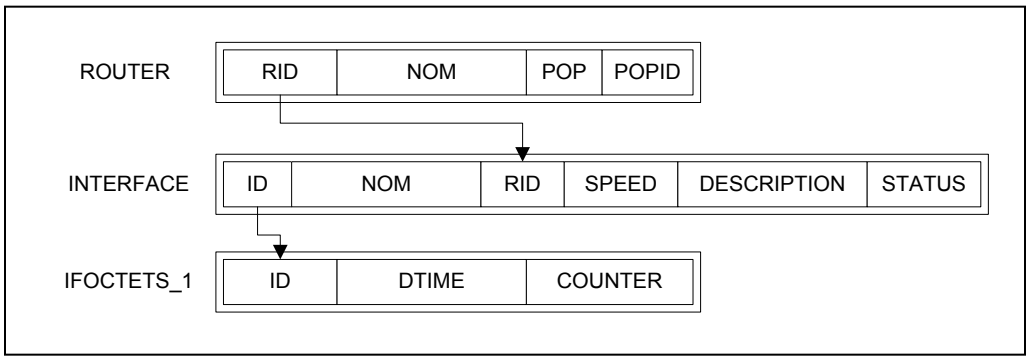
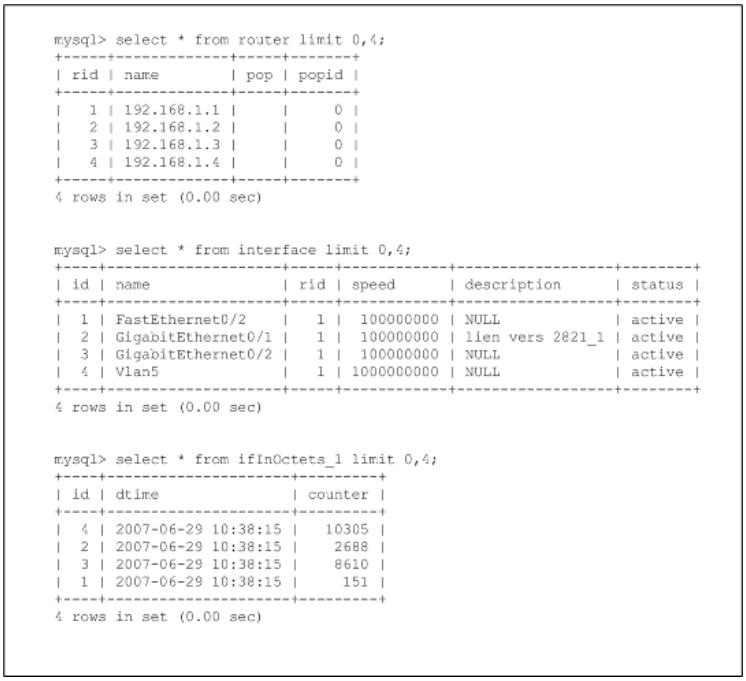


Figure 3.4 Schéma de la base de données RTG.

La table *Router* contient les équipements numérotés selon un *Rtg IDentifier* (RID) unique. Dans le cas présent, les équipements sont numérotés de 1 à 4. Le champ POP et POPID ne sont pas utilisés. La table *INTERFACE* contient toutes les interfaces de tous les équipements. Cette table contient 176 entrées uniques qui proviennent du fichier *targets.cfg*. Dans le cas

présent, les interfaces de l'équipement #1 (*Voir* Figure 3.5). Pour chaque équipement, plusieurs types de tables sont construits par exemple



```
mysql> select * from router limit 0,4;
+-----+-------------+-----+-------+
| rid | name        | pop | popid |
+-----+-------------+-----+-------+
|   1 | 192.168.1.1 |     |     0 |
|   2 | 192.168.1.2 |     |     0 |
|   3 | 192.168.1.3 |     |     0 |
|   4 | 192.168.1.4 |     |     0 |
+-----+-------------+-----+-------+
4 rows in set (0.00 sec)


mysql> select * from interface limit 0,4;
+----+--------------------+-----+------------+------------------+--------+
| id | name               | rid | speed      | description      | status |
+----+--------------------+-----+------------+------------------+--------+
|  1 | FastEthernet0/2    |   1 |  100000000 | NULL             | active |
|  2 | GigabitEthernet0/1 |   1 |  100000000 | lien vers 2821_1 | active |
|  3 | GigabitEthernet0/2 |   1 |  100000000 | NULL             | active |
|  4 | Vlan5              |   1 | 1000000000 | NULL             | active |
+----+--------------------+-----+------------+------------------+--------+
4 rows in set (0.00 sec)


mysql> select * from ifInOctets_1 limit 0,4;
+----+---------------------+---------+
| id | dtime               | counter |
+----+---------------------+---------+
|  4 | 2007-06-29 10:38:15 |   10305 |
|  2 | 2007-06-29 10:38:15 |    2688 |
|  3 | 2007-06-29 10:38:15 |    8610 |
|  1 | 2007-06-29 10:38:15 |     151 |
+----+---------------------+---------+
4 rows in set (0.00 sec)
```

Figure 3.5 Contenu sommaire des tables de la BD pour l'équipement #1.

IfInOctets_X, *IfOutOctets_X*, *IfInUniCast_X*, etc. dans le tableau 3.1 ou *X*, est le numéro de l'équipement *RID*. Dans le cas présent, la table *IfInOctect_1* contient les quatre premières données de SNMP. Les configurations SNMP sont créées par le fichier *RTGTARMAKR.PL* et par l'ajout manuellement de configuration.

Tableau 3.1 Exemple de contenu du fichier targets.cfg

Host	OID	Bits	Community	Table	ID	Description
192.168.1.1	.1.3.6.1.2.1.2.2.1.10.2	32	public	ifInOctets_1	1	(FastEthernet0/2)
192.168.1.1	.1.3.6.1.2.1.2.2.1.10.25	32	public	ifInOctets_1	2	lien vers 2821_1 (GigabitEthernet0/1)
192.168.1.1	.1.3.6.1.2.1.2.2.1.10.26	32	public	ifInOctets_1	3	(GigabitEthernet0/2)
192.168.1.1	.1.3.6.1.2.1.2.2.1.10.29	32	public	ifInOctets_1	4	(Vlan5)

Cette méthode implique que chaque équipement possède plusieurs tables ce qui peut restreindre MySQL a traité un grand nombre d'équipements. Cependant, il est possible de

sélectionner les objets SNMP sur lesquels le programme principal exécutera sa surveillance très minutieuse et au besoin on pourra démarrer un second programme pour approfondir la surveillance des équipements pour une liste d'objets SNMP supplémentaires. De cette façon, les équipements et le réseau ne sont jamais surchargés inutilement.

3.7.3 RTGPLOT

La consultation des informations se fait, comme tout autre outil de surveillance, par un graphique. RGTPLOT est le programme qui génère le graphique selon les OIDs et l'intervalle de temps choisi. RTG propose une page WEB avec code et des API en PHP pour sélectionner un équipement et une interface selon un intervalle de temps. Cet aspect de l'outil est très simple. Pour le projet de recherche, une nouvelle interface a été crée, basée également sur une page HTML et codée en PHP pour l'interrogation et du JavaScript pour sélectionner l'intervalle de temps désiré. Le ou les graphiques sont générés via RTGPLOT qui contient avec la version de base seulement deux courbes par graphique. La dernière version obtenue permet de générer quatre courbes et plus. Une modification a été apportée au code source pour tenir compte à l'affichage du graphique des très courts intervalles choisis pour la sélection des données.

3.8 Ping

L'utilisation du Ping (Muuss, 1993) ne vérifie pas la présence d'une ressource, mais est plutôt utilisée comme un sonar afin d'obtenir le degré de performance de la qualité de réseau. En temps réel, lorsque le réseau montre des signes de dégradation perceptible par les usagers, comme dans l'échange de communication par voix sur IP, l'utilisation d'une sonde indépendante des équipements permet de surveiller la QdS des liens entre les équipements, mais surtout de la mesurer selon des critères choisis. Le programme utilisé comme sonde est FPing (Schemers, 2002) sur Linux. Il permet selon les options de transmettre à plusieurs entités en parallèle des paquets ICMP, ECHO_REQUEST afin obtenir des paquets ICMP

ECHO_RESPONSE pour chaque entité. Une série de paquets est transmise avec un délai très court entre les paquets. L'analyse entre la transmission et la réception de cette suite de paquets permet de mesurer le délai, la latence, la gigue, l'ordonnancement, la fragmentation, la QdS, la route, etc.

3.9 Tshark

La surveillance des réseaux utilise plusieurs outils afin d'obtenir un portrait de l'état du réseau. Le renifleur de trafic a le rôle de prendre une copie de tous les éléments d'échange perçu par une interface sur le réseau. Il permet aux administrateurs d'en faire l'analyse détaillée. Tshark est le renifleur par ligne de commande. Ce renifleur est semblable à son grand frère WireShark qui est le successeur d'Ethereal. Tshark capture, selon ces options, une partie du trafic pour être analysé par WireShark si la granularité du problème l'exige. Dans le montage du banc de test, Tshark est utilisé sur un serveur interconnecté à tous les équipements du réseau. Une configuration des ports est effectuée afin de prendre copie du trafic suspect. Ce mécanisme est amorcé selon le comportement du réseau afin d'éviter d'enregistrer une trop grosse quantité de données.

CHAPITRE 4

BANC D'ESSAI ET EXPÉRIMENTATION

4.1 L'expérimentation

On définit l'expérimentation comme un ensemble d'opérations par lequel une série de modèles sont confrontés à des données observables. Dans le cadre de ces expériences, on cherche à obtenir par la pratique, des données pertinentes observables dans un espace de temps restreint sur lesquelles des mesures comparatives peuvent êtres obtenu. Dans les expériences, chaque modèle représente une structure de fonctionnement du réseau soumis à une variation. La structure du modèle est détaillée à la section 4.3 ainsi que la méthodologie employée. Les données observables sont les résultats des requêtes SNMP sur lesquelles les analyses sont effectuées. L'expérimentation comportent trois aspects importants. Le premier aspect est d'avoir l'instrument capable de fournir les informations adéquates et nécessaires pour tester les hypothèses. Ici l'instrument est le banc d'essai avec les outils de mesure. Le second aspect est de tester cet instrument d'observation afin d'assurer un degré convenable d'usage approprié. Le troisième aspect est de mettre en œuvre et de procéder à la collecte des donnés pour chaque modèle d'expérimentation. Le second et troisième aspect sont décrits au chapitre 5.

4.2 La nécessité d'un banc d'essai

Le banc d'essai et les outils de mesure procurent aux expériences, des évaluations en condition réelle bénéfiques pour le développement des applications afin de vérifier leurs comportements sur l'Internet. Le banc d'essai permet de reproduire et de simuler le comportement du trafic réseau en temps réel comme des pertes de paquets et des délais.

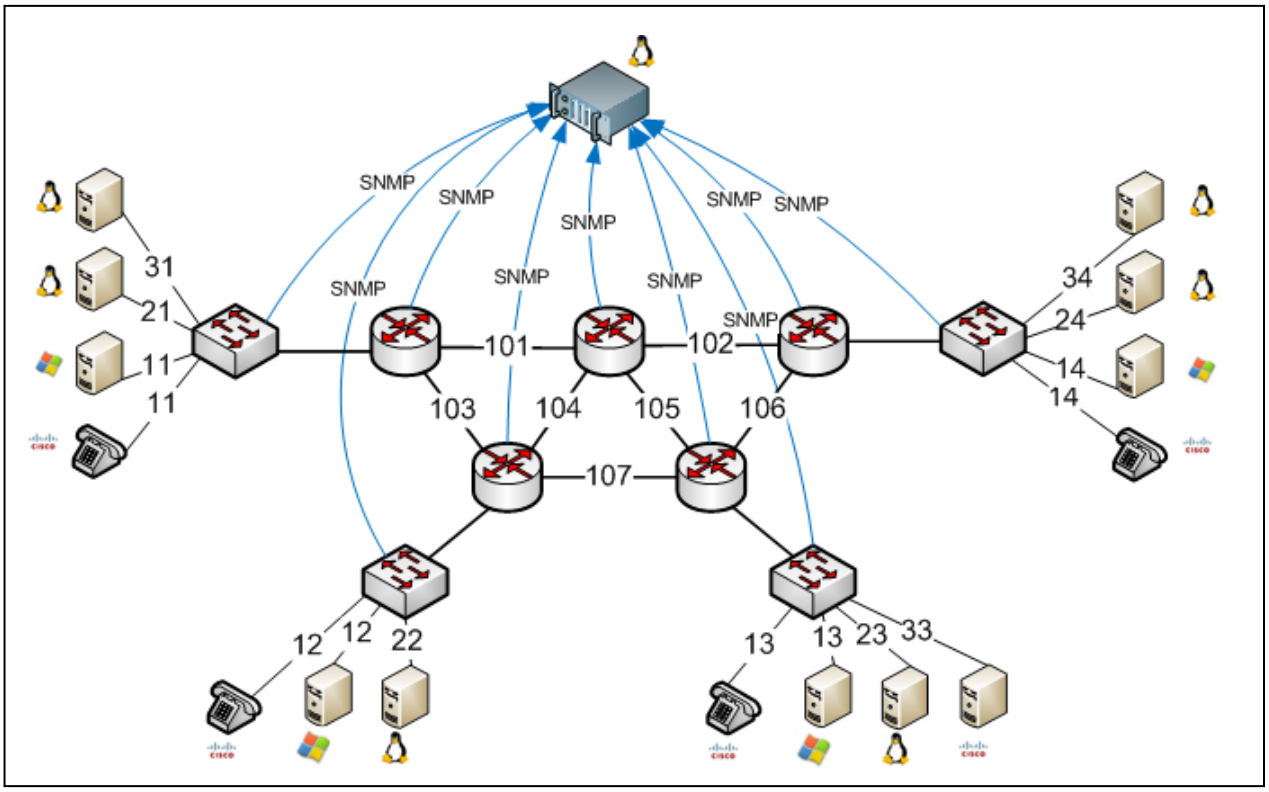


Figure 4.1 Banc d'essai de Synchromédia.

4.2.1 Architecture du banc d'essai

L'architecture du banc d'essai (*Voir* Figure 4.1) est pourvue des équipements suivants :

- Cinq routeurs Cisco 2821
- Quatre commutateurs Cisco 2950
- Un commutateur 3Com 4226T
- Un commutateur Netgear FS116
- Quatre téléphones Cisco 7941
- Un gestionnaire d'appel Cisco 7815
- Dix serveurs d'applications DELL PE-1850
- Un perturbateur de trafic TestWor PacketStorm
- Un analyseur de trafic Radcom

- Un analyseur et générateur de trafic Fluke Optiview
- Un générateur de trafic Axia
- Deux serveurs de surveillance réseau DELL PE-1850

Les serveurs d'applications se composent de six plateformes de test Linux et quatre plateformes de test Windows. La gestionnaire d'appel téléphonique IP est le Call Manager 4.1.5. de Cisco. Les plateformes Linux et Windows servent à créer différents types de trafic tel que http, ftp, et autre, tout comme le générateur de trafic Axia et Fluke Optiview. Les plateformes Linux servent également à RTG et l'utilisation des outils de mesure du délai et gigue comme décrite en la section 3.7. Chaque réseau de diffusion de trames ou vlan (Kadoch, 2004) est unique et représenté par une numérotation identifiant la couche réseau qu'il lui ait associée. Chaque réseau comporte une adresse IP de la classe 192.168.0.0 et 10.0.0.0. Le protocole de routage configuré est *Open Short Path First* (OSPF). Tous les équipements sont interconnectés selon les standards *Fast Ethernet* et *Gigabit Ethernet* toutefois toutes les expériences sont faites sur le standard *Fast Ethernet*.

4.2.2 Équipement de test PacktStorm & Optiview

Afin de reproduire le plus fidèlement aux problèmes souvent rencontrés dans l'Internet, le banc d'essai utilise un PacketStorm de TestWork et un Optiview de Fluke .

4.2.3 PacketStorm

Le PacketStorm (PS) est un équipement qui permet d'émuler du trafic IP en reproduisant plusieurs types d'anomalie et en modifiant plusieurs paramètres sur un inventaire de protocoles de paquets IP qui traversent le réseau via ces deux interfaces réseau gigabit (*Voir* Figure 4.2).

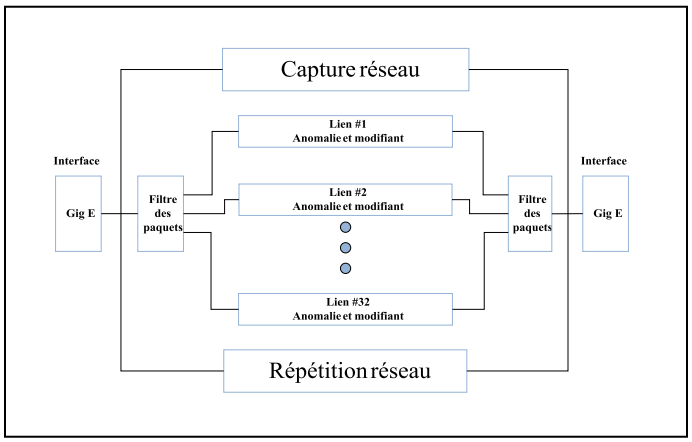


Figure 4.2 Bloc des fonctions de l'émulateur de réseau PacketStorm.

Le PS reproduit des anomalies dans un environnement de test contrôlé et répétitif pour tout type de trafic. Le PS effectue les anomalies suivantes : le délai, la gigue, la largeur de bande, la perte sélective de paquets, la perte aléatoire de paquets, l'ordonnancement aléatoire des paquets, la duplication, la fragmentation, la perte *burst* en rafale, la détermination maximale de *Maximum Tranmission Unit* (MTU), la destruction, l'accumulation et le relâchement en rafale, et finalement, l'insertion des erreurs de bits.

Le PS modifie les éléments suivants : l'adresse source, l'adresse de destination, le *Time To Live* (TTL), la décrémentation du TTL, le port source, le port de destination, le code correcteur du protocole de transport, le code correcteur sur le réseau, le type de service, le code *Differentiated Service Code Point* (DSCP), le vlan, l'étiquette MPLS ainsi que l'adresse machine. Les actions du PS sont effectuées par une sélection d'adresses IP, par numéro de port ou par type de protocole de la source ou destination. Il peut également prendre action selon la valeur de *Type Of Service* (ToS) ou selon l'heure ou selon la largeur de bande mesurée. Le menu de commandes graphique permet la sélection de blocs de fonction qui s'additionnent entre eux afin de concevoir une panoplie d'anomalies.

4.2.4 Optiview

L'Optiview de Fluke est un Protocol Analyser. Dans le cadre des manipulations l'Optiview a été utilisé pour générer le trafic IP d'encombrement. Il a la capacité de transmettre des paquets selon un débit et de taille variable et avec un en-tête de paquet UDP ou ICMP. La taille minimum du paquet est de 64 octets et la taille maximum est de 1518 octets.

4.2.5 La gestion du réseau de test de Synchromdia

La gestion du réseau de test de Synchromédia est constituée de deux opérations. La première opération est l'acheminement de toutes les transactions des requêtes SNMP et requêtes *NetFLow* aux serveurs de gestion via un commutateur dédié. La seconde opération est l'acheminement des captures sélectives du flux de trafic aux mêmes serveurs ou via un autre commutateur dédié. L'utilisation d'un réseau commuté parallèle confiné à la collecte des informations permet d'obtenir la performance quasi en temps réel de toutes les informations sur la vitalité du réseau sans que ce dernier altère son comportement original.

4.2.6 Surveillance du réseau de Synchyromédia

Une application par fureteur a été développée afin de consulter l'information recueillie par SNMP. Principalement programmé en code HTML et PHP (Williams et Lane, 2004), l'application *Surveillance Réseau Synchromédia* (SRS) fait la cueillette d'information selon un menu de sélection d'éléments comme les troncs communs des commutateurs, les troncs communs des routeurs, les ports des commutateurs, les ports des routeurs, les routes, les charges des UTC, le délai, la qualité de service (*Voir* Figure 4.3), ou bien par une sélection individuelle des différents éléments (*Voir* Figure 4.4). Toute consultation se fait selon une sélection d'un espace de temps déterminé par la date et l'heure souhaitées afin d'interroger la base de données sur MySQL.

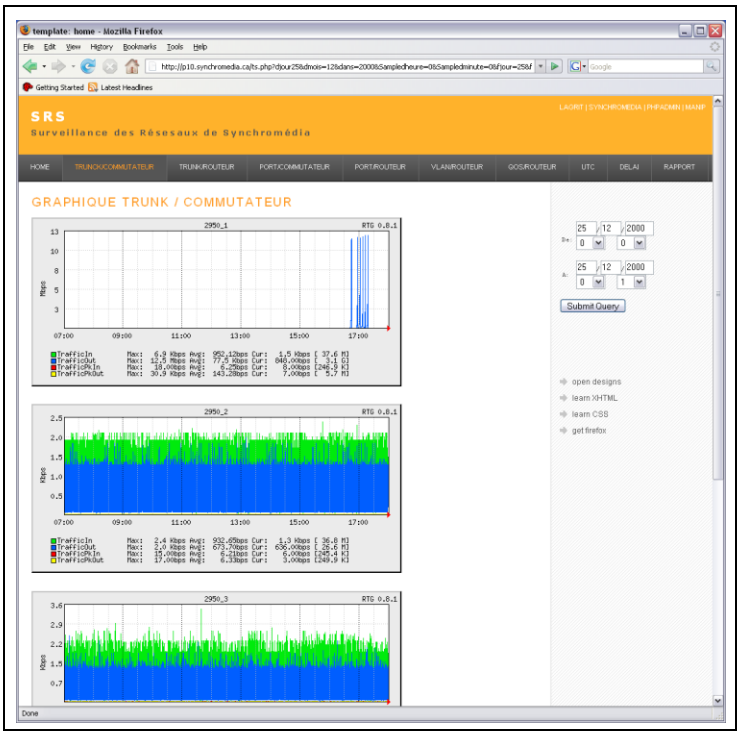


Figure 4.3 Sélection des troncs des commutateurs sur SRS.

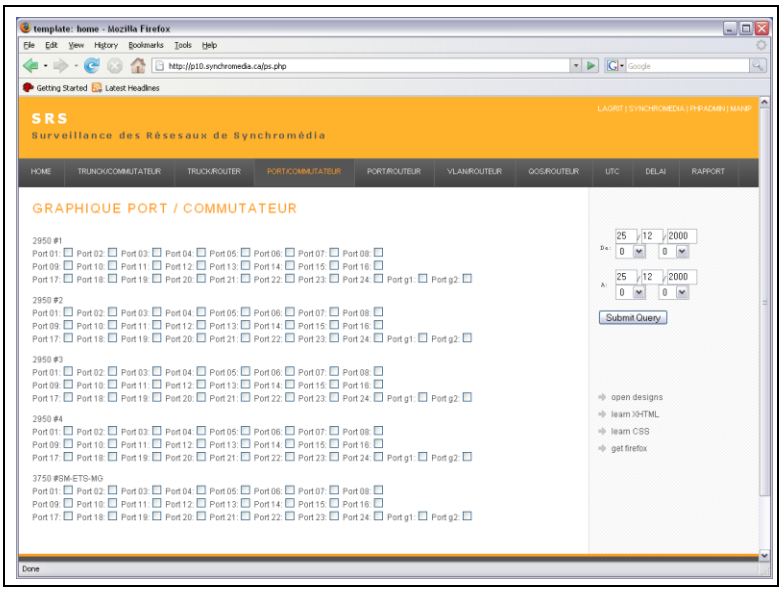


Figure 4.4 Sélection unitaire des éléments aux commutateurs sus SRS.

4.3 Modèles et méthodologie des essais

Un des objectifs pour résoudre la problématique de la perturbation est de découvrir les paramètres opérationnels du banc d'essai ainsi que le degré de perturbation des applications via une série de modèles d'essais basés sur l'encombrement des liens de communication, le délai, la gigue, la fragmentation et la perte des paquets. Ces essais sont effectués selon une liste de paramètres pour laquelle différents résultats sont obtenus. La méthode des essais et son cheminement sont en partie guidés par la méthodologie de tests d'évaluation de la performance (Bradner et McQuaid, IETF 1999). Les modèles sont décrits à la section 4.4

4.3.1 Le cadre de gestion des requêtes SNMP

Le cadre de gestion pour les essais utilise une série de variables SNMP qui sont présentes dans tous les équipements. Les variables pour une seule interface qu'elle soit physique ou logique sont lus à un intervalle régulier à chaque seconde. La liste des variables récupérées sont :

- ifInOctets
- ifOutOctets
- ifInUcastPkts
- ifOutCastPkts

D'autres variables SNMP ont été identifiées afin de fournir une information additionnelle au système d'information sur l'interface ou l'équipement :

- ifInDiscards
- ifOutDiscards
- ifInError
- ifOutError
- ifInUnknownProtos
- IcmpError

- UdpError
- cpmCPUTotal5sec
- 1.3.6.1.4.1.9999.1 (variable de délai)

Pour la surveillance de la QdS des variables SNMP spécifiques sont identifiées dans la MIB ciscoCBQQosMIBObjects. Un inventaire est présenté en annexe 2

4.3.2 Le plan d'adressage du banc d'essai

Le plan d'adressage du banc d'essai est décrit au tableau 4.1

Tableau 4.1 Adresses IP de routage

Routeur #1		Routeur #2		Routeur #3		Routeur #4		Routeur #5	
rés.	adresse IP	rés.	adresse IP	rés.	adresse IP	rés.	adresse IP	rés.	adresse IP
11	192.168.11.0 /24	101	10.10.101.0 /30	14	192.168.14.0 /24	12	192.168.12.0 /24	13	192.168.13.0 /24
21	192.168.21.0 /24	102	10.10.102.0 /30	24	192.168.24.0 /24	22	192.168.22.0 /24	23	192.168.23.0 /24
31	192.168.31.0 /24	104	10.10.104.0 /30	31	192.168.34.0 /24	32	192.168.32.0 /24	33	192.168.33.0 /24
101	10.10.101.0 /30	105	10.10.105.0 /30	102	10.10.102.0 /30	103	10.10.103.0 /30	105	10.10.105.0 /30
103	10.10.103.0 /30			106	10.10.106.0 /30	104	10.10.104.0 /30	106	10.10.106.0 /30
						107	10.10.107.0 /30	107	10.10.107.0 /30

4.3.3 Le plan d'adressage de gestion

Le plan d'adressage de gestion SNMP du banc d'essai est décrit au tableau 4.2

Tableau 4.2 Adresse IP de gestion SNMP

Matériel	Adresse IP	Matériel	Adresse IP	Matériel	Adresse IP
Commutateur #1	192.168.1.1 /24	Routeur #1	192.168.1.11 /24	Delai #11	192.168.1.103 /24
Commutateur #2	192.198.1.2 /24	Routeur #2	192.168.1.12 /24	Delai #12	192.168.1.105 /24
Commutateur #3	192.168.1.3 /24	Routeur #3	192.168.1.13 /24	Delai #13	192.168.1.108 /24
Commutateur #4	192.168.1.4 /24	Routeur #4	192.168.1.14 /24	Delai #14	192.168.1.109 /24
		Routeur #5	192.168.1.15 /24		

4.3.4 Les types de paquets

Deux catégories de trafic ont été utilisées dans les différents scénarios de test effectués sur le banc d'essai. La catégorie de trafic d'encombrement généré par le FLuke Optiview est un paquet TCP/IP UDP Echo. La catégorie de trafic usuel typique à la plateforme de travail collaboratif Synchromédia et généré par divers outils logiciels. Le logiciel couramment employé pour simuler avec précision le trafic usuel de Synchromédia est Iperf version 2. Cependant pour les expériences sur la voix sur IP, celles-ci ont été faites avec un système de téléphonie Cisco.

4.3.5 La taille des paquets

Les paquets de test doivent idéalement être distribués selon différentes tailles afin d'obtenir des résultats sur le débit théorique du média, le traitement des files d'attente et de la mémoire tampon. Ces tests incluent les tailles irréalistes afin de caractériser pour chaque taille le traitement supplémentaire des équipements. Selon le guide, la taille des paquets à utiliser pour un lien Ethernet sont : 64, 128, 256, 512, 1024, 1280, 1518. Pour les expériences de test, la liste suivante a été employée : 64, 70, 80, 96, 128, 192, 256, 320, 448, 512, 1024, 1518.

4.3.6 Le rapport des résultats

Les éléments de performance, caractéristiques de RTG avec SRS fournissent une interface pour générer des rapports et des graphiques complets ou adapter sur mesure selon un intervalle de temps sous la minute. Le rapport des résultats est un résumé de tout le contenu des informations qui comprennent les éléments suivants :

- Le nombre maximum de paquets par seconde
- La grosseur des paquets
- Le maximum théorique du média
- Le type de protocole

- La latence
- La gigue
- La perte de paquets

4.4 Modèles et paramètres des essais

Les scénarios d'essais proposés démontrent un à un les modèles contraignants de la communication réseau. Chaque condition contraignante fait l'objet de test dans trois cheminements typiques de l'utilisation des réseaux et de l'Internet. Les modèles contraignants sont l'encombrement, la perturbation et le nivelage des flux. On recherche les résultats afin de mettre en perspective la notion d'une surveillance accrue pour permettre de paramétrer des seuils quantitatifs. Ces seuils peuvent générer des alarmes et des actions préventives aux conditions contraignantes avant d'avoir un effet sur la communication.

4.4.1 L'encombrement

L'encombrement du réseau est l'effet d'un afflux soutenu de paquets qui excède la limite de traitement normal de la ressource. L'encombrement s'établit par la saturation des files d'attente et cause la perte de paquets et augmente la latence du réseau, ce qui augmente les échanges de messages de gestion et contribue à la dégradation de la performance du réseau. Lorsque l'encombrement est important, l'unité de traitement centrale de l'équipement devient saturée. L'équipement devient non opérationnel et le risque d'effondrement du réseau est quasi instantané jusqu'au moment où l'encombrement est revenu à un niveau que le système peut traiter normalement.

Pour ce test, l'Optiview est utilisé. L'équipement transmet en mode unicast un type de paquet à une taille configuré à un débit qui dans la grande majorité des tests est incrémenté au taux moyen de 0.45% par seconde. Le débit maximum du médium est 100 Mbps.

4.4.2 La perturbation

La perturbation crée un effet irrégulier dans le fonctionnement de la communication du réseau Internet. Les expériences du délai, de la gigue et de la fragmentation sont générées via le PS sur la route 101.

4.4.3 Le nivelage des flux

Le nivelage des flux est une opération sur les métriques de performance de débit et temps de réponse sur la totalité du trafic total ou sur une classe en particulier. Ces opérations sur le banc d'essai sont accomplies par la qualité de service.

CHAPITRE 5

SCÉNARIOS DE TEST ET RÉSULTAT

5.1 Élément de mesure

Pour les premiers essais, tous les éléments de mesure totalisent 707 requêtes d'information effectuées toutes les secondes et réparties comme indiqué au tableau 5.1 La grande somme de requêtes exercent un accroissement de la charge de traitement des UTC d'environ 3% sur les routeurs du banc d'essai comme le démontre la figure 5.1 On précise que la charge des UTC concerne seulement les routeurs. La mesure du taux de charge des UTC des commutateurs soumis aux différents scénarios préliminaires d'essais demeurait constamment dans un état d'occupation de 75% à 80% lorsque soumis aux différents modèles de test. Sur ce fait seul, les UTC des routeurs ont été retenues comme élément d'information. Le taux de trafic engendré par le trafic des requêtes SNMP est de 39.2 Kbps pour les commutateurs et de 32.7 Kbps pour les routeurs.

Tableau 5.1 Nombre *Object IDentifier* SNMP répertorié par équipements et fonctions

Nom	OID	Nom	OID	Nom	OID
Commutateur #1	107	Routeur #1	41	Délai #1	12
Commutateur #2	107	Routeur #2	41	Délai #2	12
Commutateur #3	107	Routeur #3	41	Délai #3	12
Commutateur #4	107	Routeur #4	49	Délai #4	12
		Routeur #5	49	Charge UTC	10

On remarque à la figure 5.1 que l'indicateur de la mesure du temps n'est pas présent sur l'axe horizontal. En fait, l'application affiche les informations à chaque seconde, mais le marquage visible sur l'axe s'accomplit lorsque la période de temps est supérieure à 30 minutes (1800 secondes). Cette contrainte affecte la grande majorité des affichages subséquents effectués avec RTG car la plupart des scénarios ont été faits sur une période moyenne de 224 secondes donc affichés sur 4 minutes sauf indication contraire.

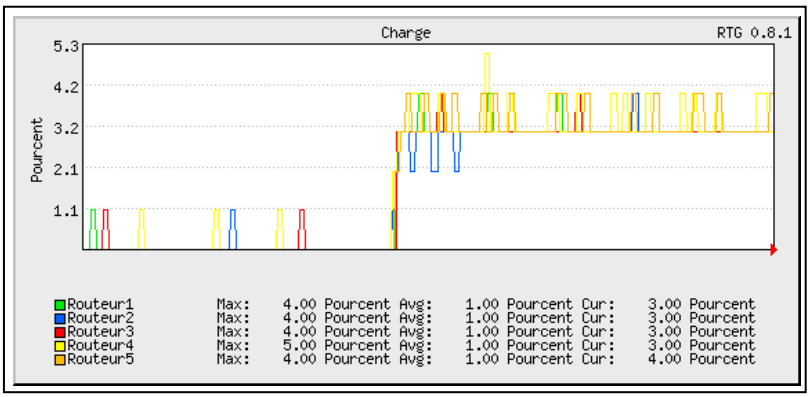


Figure 5.1 Affiche le taux d'occupation des UTC à gauche sans requêtes SNMP et à droite avec requêtes SNMP.

5.1.1 Précision des éléments de mesure

La fidélité des données observées n'est pas entièrement conforme aux attentes. Dans certains cas, lorsque l'analyse s'effectue à la plus petite échelle offerte par SRS, soit la minute, on observe parfois des éléments qui ne suivent pas la logique normale des flux et des paquets. Un exemple sur le trafic SNMP illustre ce phénomène. On observe à la figure 5.2 et 5.3 des différences entre les données du flux de trafic et des paquets. Les graphiques sont fidèles aux données recueillies par RTG.

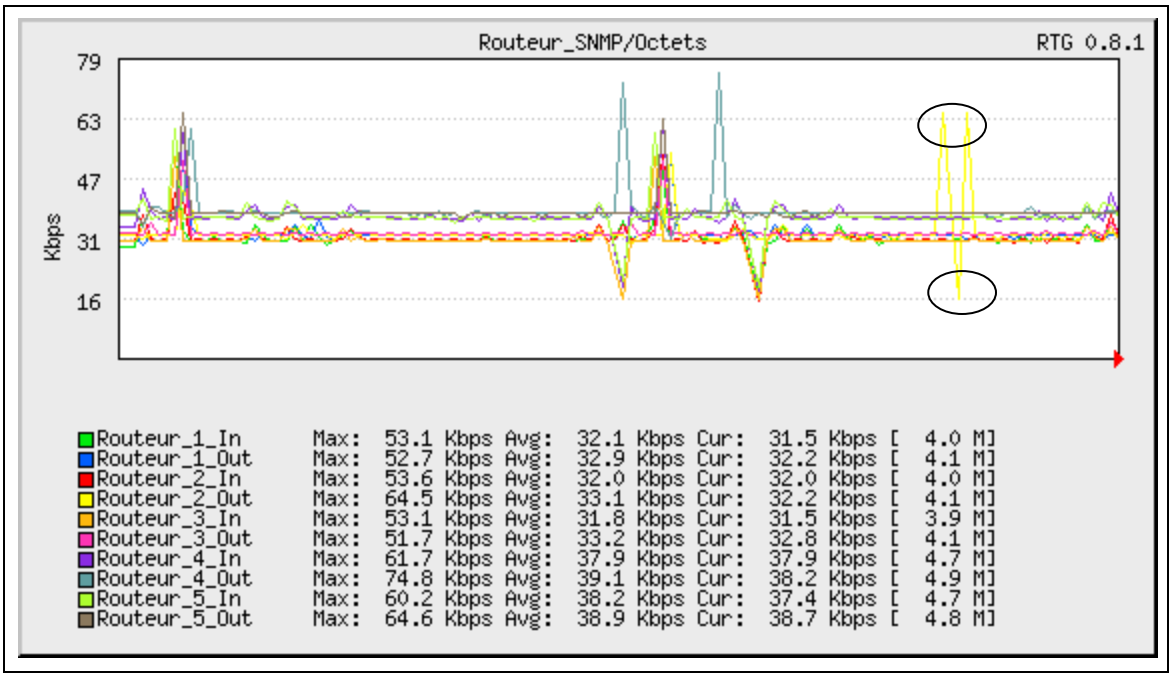


Figure 5.2 Trafic SNMP des cinq routeurs (bits / seconde)
les inconsistances obtenues sont encerclées.

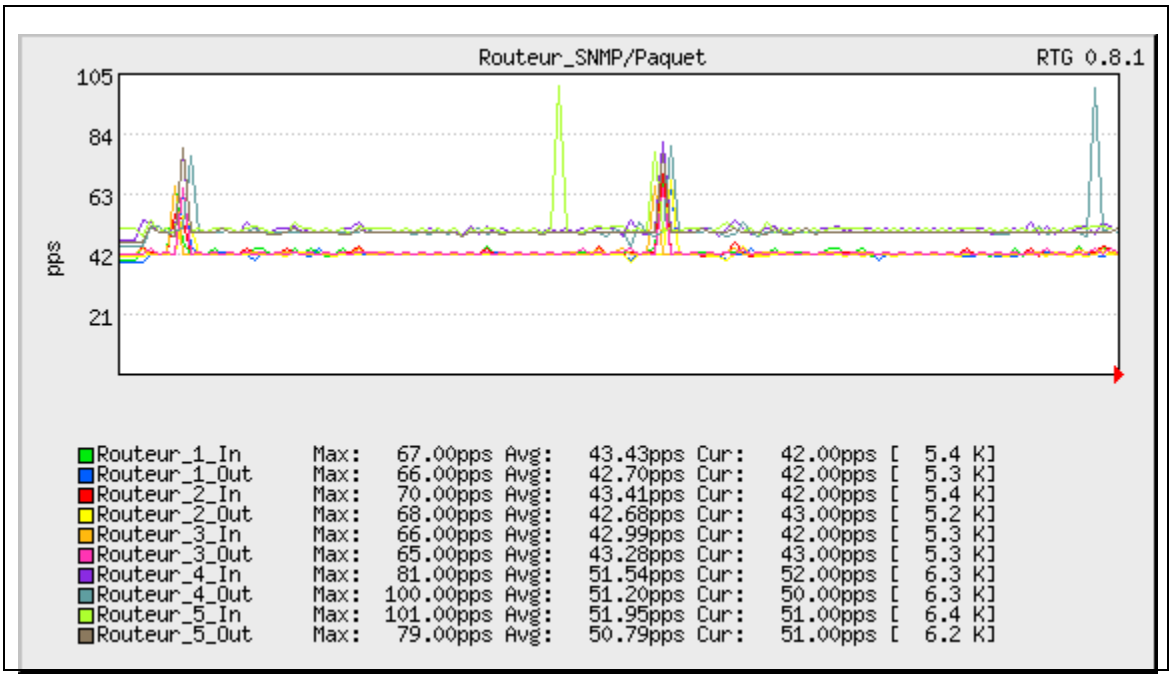


Figure 5.3 Trafic SNMP des cinq routeurs (paquets / seconde).

Les deux cercles sur la figure 5.2 mettre en relief le phénomène de l'incohérence des lectures faites par RTG via SNMP. Les indicateurs des interfaces SNMP des routeurs en mode d'opération normal doivent être linéaires ou constants ce qui démontre la régularité de la saisie des informations, soit de 33.1 kbps sur l'interface de sortie de SNMP du routeur #2. Cette linéarité est validée par les données graphiques de la figure 5.3 qui indique le nombre de paquets par seconde sur la même interface au même moment. Dans le cas des variations anormales présentées à la figure 5.2, on observe au même instant sur la figure 5.3, l'absence d'irrégularité. On conclut que l'information saisie est constante pour cette interface. La cause probable de ce phénomène est erreurs lors de la saisie d'information SNMP avec l'application. Les données démontrent que la valeur de l'information SNMP du routeur #2 en sortie est, au départ le double de la valeur moyenne et qu'à un autre moment elle est absente, donc aucune donnée n'a été enregistrée à cet instant. La mesure de la perturbation sera par contre à vérifier avec d'autres données.

5.2 Scénario de l'encombrement

L'encombrement du réseau est effectué selon les scénarios suivants :

- Les premiers scénarios de l'encombrement sont exécutés selon les paramètres définis à la section 4.3. Ces scénarios sont exécutés sans autre source de trafic. Le but est d'obtenir des repères de nivellement de la charge et de la capacité des équipements de communication.
- La seconde série de scénarios est exécutée toujours selon les paramètres initiaux, mais en plus avec du trafic usuel natif à la plateforme de Synchromédia. Celle-ci comprend du trafic TCP, du trafic de voix sur IP et du trafic vidéo en UDP.
- La troisième série de scénarios est exécutée avec un contrôle plus précis du trafic d'encombrement qui inclut les classes de services pour tout type de trafic. Le but est d'effectuer la mesure des différentes classes en préparation du traitement de la qualité de service.

- La quatrième série de scénarios est la mesure de l'effet du traitement de la qualité de service au scénario ultérieure.

5.2.1 Encombrement du réseau

Le taux moyen d'incrémentation du trafic d'encombrement est 0.5% par seconde. Tous les graphiques suivants ont une durée de 240 secondes. On note que la taille du paquet concerne seulement les données et n'inclut pas l'en-tête du paquet. Tous les paquets d'encombrement ont été générés avec un en-tête IP de 20 octets. La source du trafic d'encombrement est transmise dans le banc d'essai via le commutateur #1 et a comme destination le poste sur la route #34.

5.2.2 Encombrement de paquets de 64 octets

On observe le comportement des routeurs (*Voir* Figure 5.4) soumis à une charge transmise dans le réseau avec des paquets de taille de 64 octets. Le générateur de trafic a généré plus de 148,817 paquets par seconde, pour un débit de 100 Mbps ce qui a pour effet de saturer à 99% l'unité de traitement du router #1. On observe que les routeurs #2 et #3 n'atteignent que 81% et 83% de la limite de l'UTC. Les routeurs #4 et #5 n'étant pas sollicités par le test de l'encombrement, ils ont une charge de 3% à 4%. On indique l'espace de temps ou la perte d'information survient, cet phase affecte grandement la limite opérationnelle de la gestion des routeurs et par la même occasion la mesure de la perturbation. Une première mesure de la perturbation du trafic est sans contredit le niveau de charge anormalement élevé des routeurs. Rare sont les conditions d'opération qui peuvent générer un niveau de traitement au delà de la barrière du 90%.

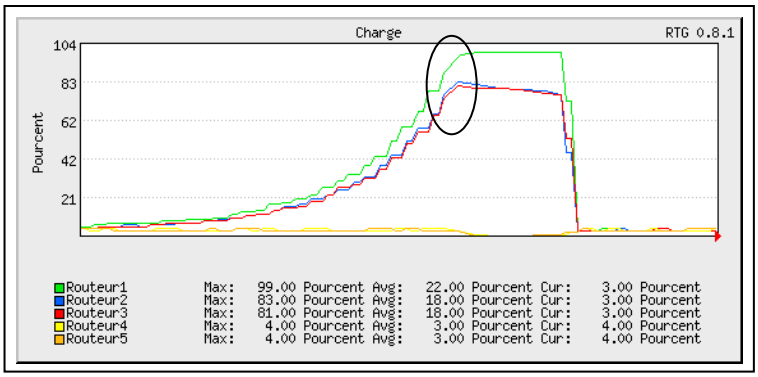


Figure 5.4 Charge des UTC pour trafic de paquets à 64 octets. On indique le moment ou la saturation est atteinte.

Le trafic d'encombrement a atteint un maximum mesuré de 36 Mbps au port d'entrée du commutateur#1 pour un débit d'environ 49,300 paquets par seconde. Les données observées sur les ports des routeurs démontrent que le trafic d'encombrement a atteint un débit moyen de 33.6 Mbps soit 2.4 Mbps de moins que le trafic au port du commutateur. Ici aucune mesure n'est faite pour les paquets perdus. Cet encombrement a comme effet de limiter le taux de saisie des informations SNMP et donne des graphiques irréalistes (*Voir* Figure 5.5). A cet instant le niveau de charge des UTC est de 88% pour le routeur #1 ce qui correspond à un débit d'entrée de 47,078 paquets par seconde et 24.72 Mbps. À cette étape, les données des OID sont obtenues en moyenne toutes les 10 secondes donc une diminution de 90% de la cadence d'échantillonnages par rapport au mode normal d'opération. Aucune gestion n'est possible dans un délai normal. On indique à la figure 5.5 et la figure 5.6 le niveau maximum de donnée auquel le routeur et l'environnement de gestion SRS peuvent fonctionner pour la capacité du lien et la taille des paquets. Dépassé ce seuil, aucune information valide n'est recueillie par RTG.

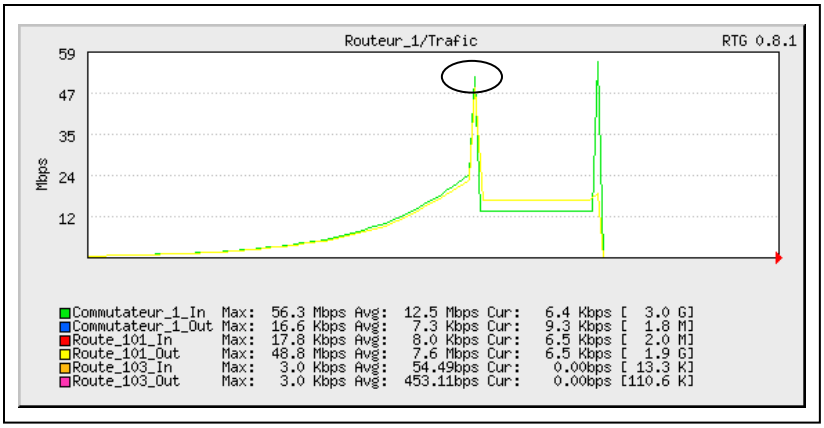


Figure 5.5 Nombre d'octets des ports du routeur #1 pour des paquets de trafic à 64 octets. On indique le moment ou la perte d'information survient.

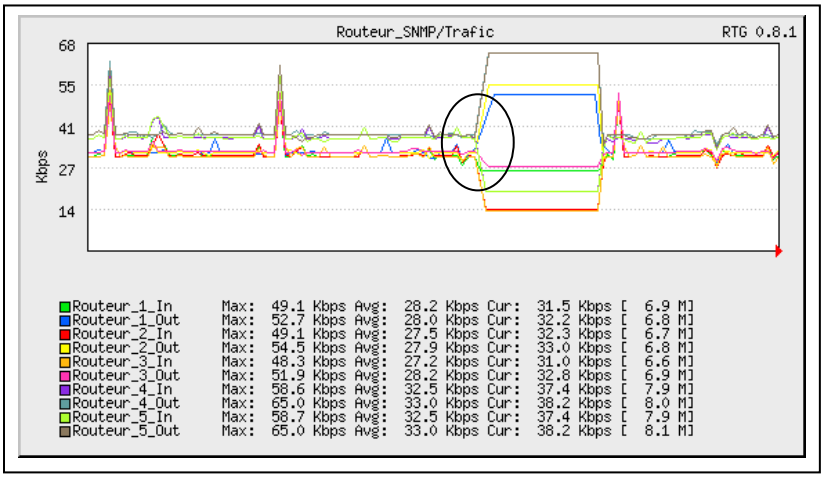


Figure 5.6 Nombre d'octets SNMP des routeurs pour des paquets de trafic à 64 octets. On observe l'impact soudain de l'effet de l'encombrement sur le réseau de surveillance.

Un autre effet de l'encombrement observé sur le réseau est la latence de la communication qui est mesurée de bout en bout pour différente route. Le niveau des délais augmente (*Voir* Figure 5.7) au moment où le nombre de paquets sature l'unité de traitement centrale par un débit mesuré de 47,000 paquets par seconde.

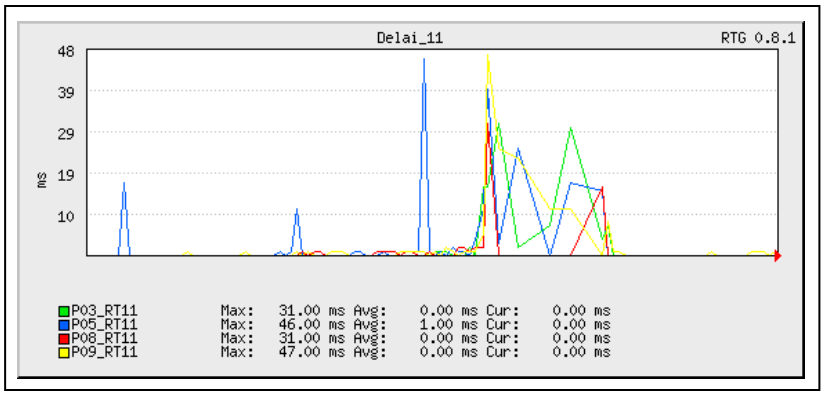


Figure 5.7 Délai observé pour le réseau #11.

5.2.3 Encombrement avec des paquets de 70,80 et 96 octets

L'encombrement de trafic selon la taille des paquets de 70, 80 et 96 octets démontre qu'il y a peu de changement sur la charge des *unités de traitement central* (UTC) des routeurs par rapport à l'encombrement précédent. On mesure toujours un écart de 18% en moyenne entre le routeur #1 et les routeurs #2 et #3. Ici on n'observe que la taille des paquets à une influence proportionnelle au niveau de saturation des UTC. On note une augmentation du débit réel en mégabits au port des routeurs. Avec un encombrement de paquets dont la taille est de 70 octets, on mesure un débit moyen de 33.6 Mpbs. Le débit atteint 44.8 Mbps avec des paquets de taille de 96 octets au port d'entrée du routeur #1. Au port de sortie du routeur, le débit est inférieur de 3.2 Mbps. Le routeur rejette 3,500 paquets par seconde. On constate toujours une saturation des enregistrements (*Voir* Figure 5.8) des informations SNMP pour tous les routeurs incluant les routeurs exclus de l'encombrement.

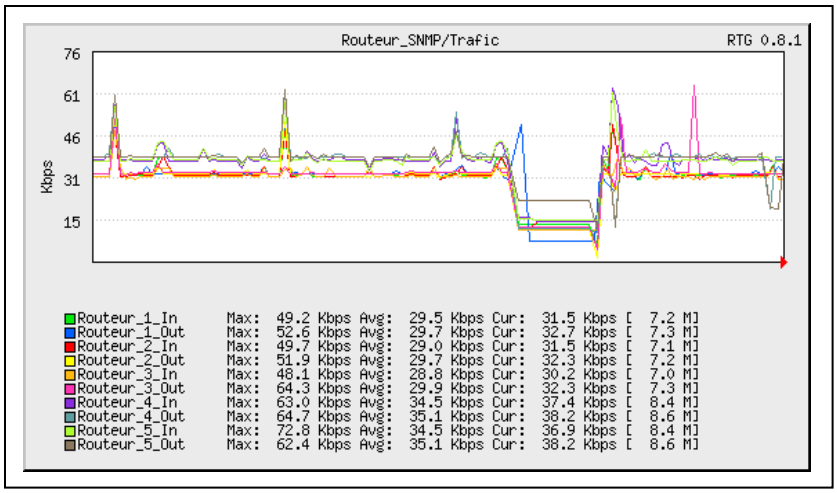


Figure 5.8 Nombre d'octets SNMP des routeurs pour des paquets de trafic 96 octets.

On note un délai de 28.9 millisecondes en moyenne pour l'encombrement des paquets de tailles de 70 à 96 octets soit 10 millisecondes inférieures à la mesure de délai avec un encombrement de trafic avec des paquets de 64 octets. On remarque le délai à partir d'un encombrement de 10,000 paquets par secondes (*Voir* Figure 5.9) au port d'entrée du routeur #1 et s'accroît rapidement lorsque le trafic d'encombrement atteint la barre de 43,000 paquets par seconde mesurée sur un port d'entrée du routeur. Une analyse des données démontre aussi que la variation dans le délai est deux fois plus importante pour les routes mesurées via les postes P_05 et P_09 du banc d'essai. On constante par le schéma du banc d'essai que les postes P_05 et P_09 ont deux routeurs de plus par lesquels les paquets sont acheminés, ce qui perturbe cette mesure.

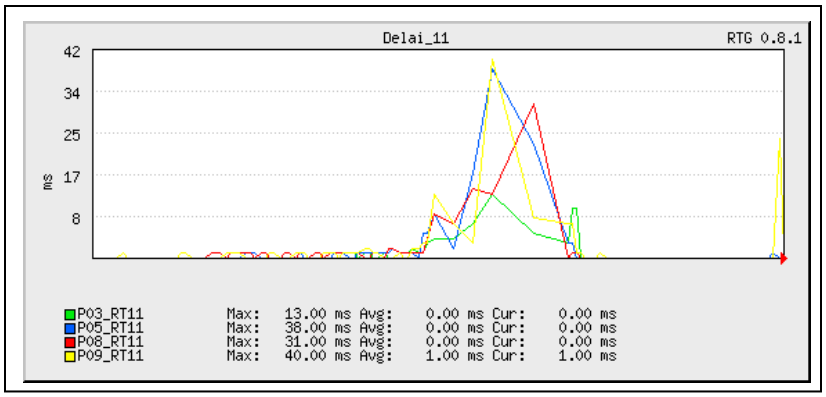


Figure 5.9 Délai observé pour le réseau 11 pour du trafic de 80 octets / 120 secondes.

5.2.4 Encombrement de paquets de 128 à 384 octets

L'encombrement de trafic des paquets de taille de 128, 192, 256, 320, et 384 octets permet de suivre une progression de la diminution de l'effet de l'encombrement sur les charges des unités de traitement centrales des routeurs et une augmentation du débit transporté de bout en bout sur le réseau. On observe une diminution de la charge de l'UTC lorsque la taille des paquets du trafic d'encombrement atteint 256 octets. À cette taille (*Voir* Figure 5.10) la charge de l'UTC du routeur #1 atteint 94%.

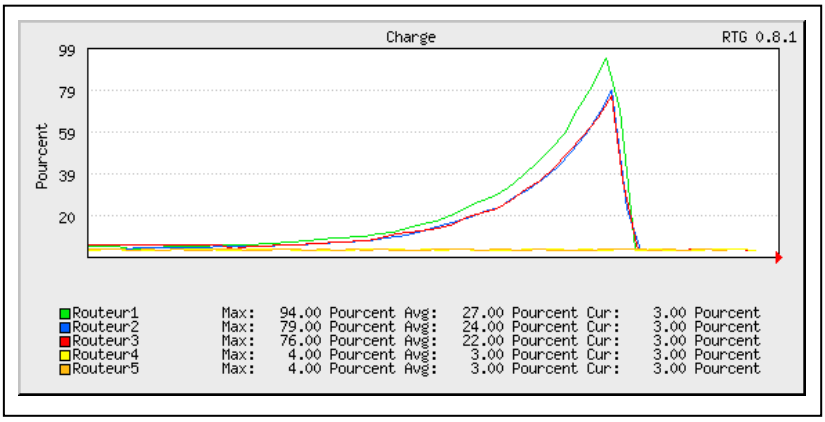


Figure 5.10 Charges de l'UTC des routeurs pour du trafic de paquets de 256 octets.

On observe une augmentation des réponses aux requêtes SNMP lorsque la taille des paquets grossit. Avec des paquets de taille de 256 octets (*Voir* Figure 5.11), on note une perturbation à un moment précis dont la durée à moins d'impact sur la quantité de données SNMP reçue. On précise le laps de temps où la perturbation est la plus intense, mais qui a peu d'impact sur le fonctionnement de l'ensemble des équipements. Ainsi toute perturbation pourra être observé. Avec des paquets d'encombrement de 384 octets, le taux de réponse est nominal.

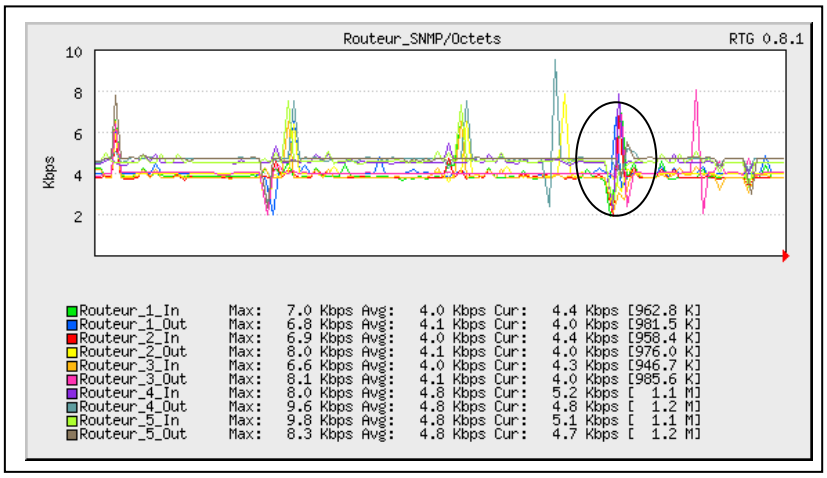


Figure 5.11 Nombre d'octets SNMP des routeurs pour des paquets de trafic de 256 octets On observe l'effet sur le réseau au moment de saturation anticipé.

L'impact de la taille des paquets d'encombrement a un effet direct sur la quantité d'information transportée de bout en bout. L'analyse comparative des débits maximum mesurés pour le trafic d'encombrement démontre un taux maximum de 6.3 méga-octets pour des paquets de 128 octets, de 9.4 méga-octets pour des paquets de 192 octets et de 10.3 méga-octets pour des paquets de 256 octets. L'encombrement subséquent, dont la taille des paquets est supérieure à 256 octets, n'accentue pas le débit qui passe que de 11.3 à 12 méga-octets.

5.2.5 Caractérisation du réseau de l'encombrement à vide

La caractéristique du réseau est décrite par le graphique de la figure 5.12 et la figure 5.13. Il affiche les frontières de l'encombrement fonctionnel du réseau selon la taille des paquets pour le banc d'essai. Le débit maximum à l'interface est limité par le nombre de paquet que le routeur peut traiter par seconde. Le nombre maximum de paquet par seconde est de 48,000.

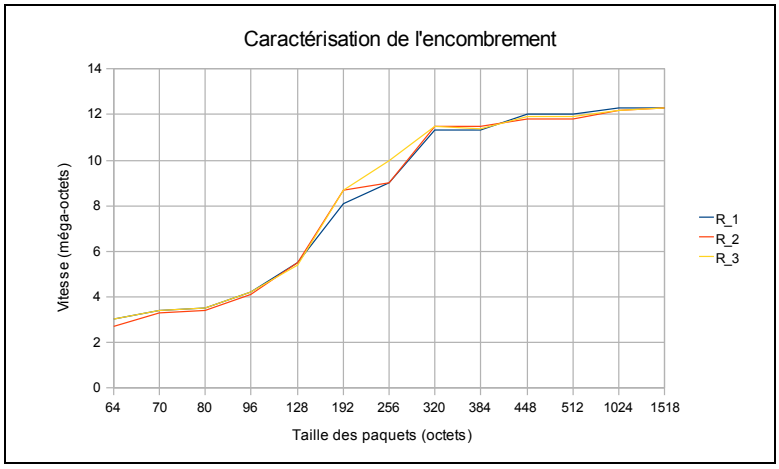


Figure 5.12 Débit maximal selon la taille des paquets de 64 à 1518 octets.

Ceci permet de définir des critères et amorces pour différents niveaux d'alarmes afin de prévenir tout dysfonctionnement du contrôle des équipements et du flux de trafic. Un premier critère pour les routeurs est le niveau de charge des UTC lorsqu'ils atteignent un niveau de 92% à 95% aucune mesure utile ne parvient à SRS donc aucune gestion n'est possible sur les équipements afin de poser des actions dans le but de rétablir le contrôle. Un second critère est le flux par rapport à la taille des paquets (*Voir* Figure 5.13), surtout les paquets de petite taille. SRS démontre les seuils établis pour les différentes tailles des paquets pour les routeurs comme paramètres d'amorçage des alarmes toujours dans le but de maintenir le fonctionnement des équipements.

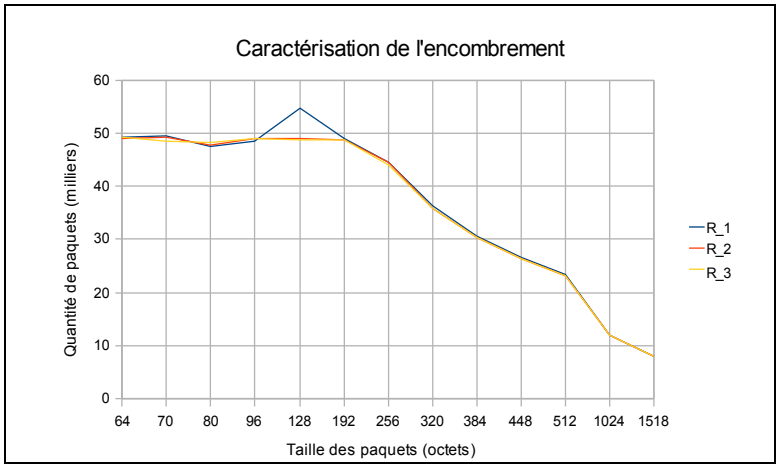


Figure 5.13 Débit maximal selon la quantité des paquets de 64 à 1518 octets.

5.3 Encombrement sur trafic TCP

L'observation de l'impact de l'encombrement du trafic TCP a pour but de déterminer la limite de fonctionnement des équipements et des échanges afin d'obtenir une référence de comportement lorsqu'une communication TCP est soumise à une perturbation. Le protocole *File Transport Protocol* (FTP) est utilisé comme générateur de trafic TCP via un poste serveur P_01 et un poste client P_04. Dans cette expérience, on reproduit l'encombrement selon la même sélection de tailles de paquets d'encombrement que dans l'expérience précédente. Le trafic d'encombrement est généré selon un taux variable d'incrémentation de 0.5% de paquets par seconde.

5.3.1 Trafic FTP sans encombrement

Le trafic FTP sans encombrement est caractérisé par l'observation de la charge des UTC de des routeurs (*Voir* Figure 5.14). On observe une caractéristique du trafic TCP sur le niveau de charge des routeurs. On note un écart de charge entre l'UTC du routeur #1 et les UTC des routeurs #2 et #3. Autre que le fait que le routeur #1 est le premier routeur par lequel se propage le trafic, aucun élément obtenu par RTG n'explique le graphique de charges

observées pour du trafic FTP. On observe (*Voir* Figure 5.15) les caractéristiques suivantes : la vitesse moyenne est de 9 méga-octets, la taille moyenne du paquet FTP incluant l'en-tête est de 1324 octets. Selon la caractérisation du réseau, le trafic atteint un débit maximum de 11.9 méga-octets, 88% du temps. Il occasionne un délai moyen pour l'accès de 3 millisecondes.

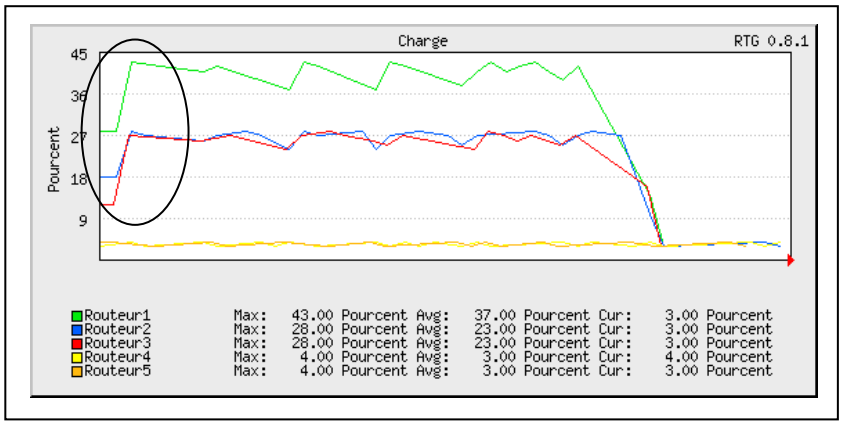


Figure 5.14 Charges est UTC des routeurs pour du trafic FTP. On distingue la différence de charge UTC entre les routeurs.

On observe clairement (*Voir* Figure 5.16) le transfert de données à 9,000 paquets par seconde, ainsi que les donnés associées au contrôle des échanges à 4,500 paquets par seconde pour un débit moyen de 232 kilo-octets.

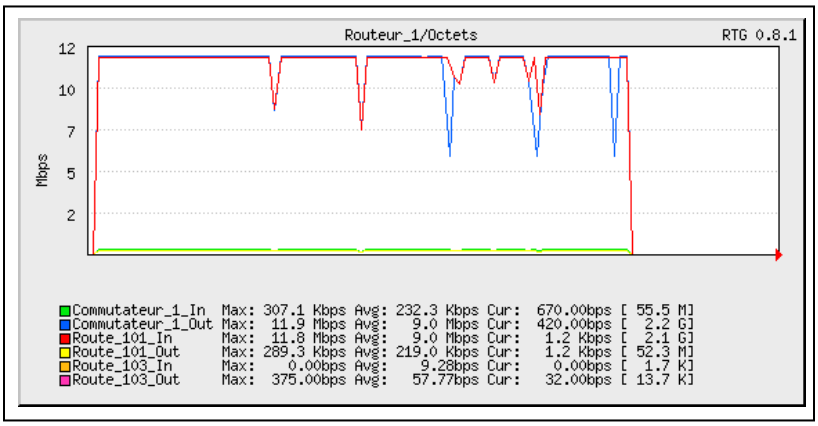


Figure 5.15 Débit en méga-octets pour du trafic FTP.

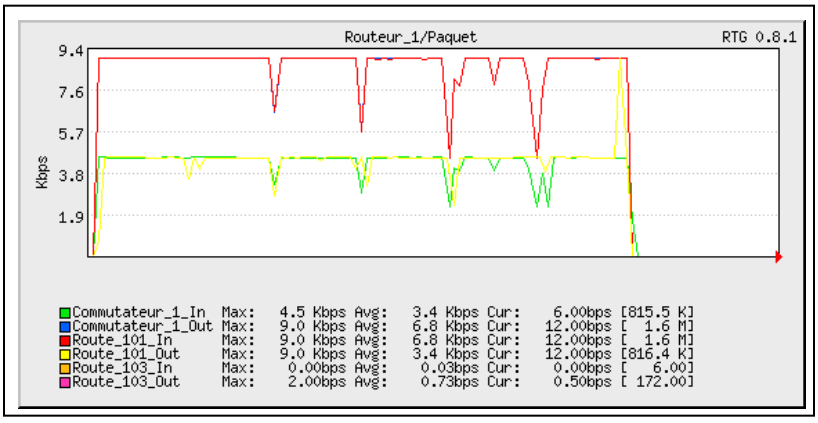


Figure 5.16 Débit en paquets pour du trafic FTP.

5.3.2 Trafic FTP avec encombrement de paquets de 64 octets

Le scénario où l'impact est le plus significatif sur les équipements de communication est celui de l'encombrement avec des paquets de petite taille. On observe que la durée du transfert FTP s'est accrue de 40 secondes par rapport au transfert sans aucun trafic d'encombrement. Celle-ci engendre une dégradation jusqu'à 22.4% lorsque le trafic d'encombrement atteint 35,300 paquets par seconde ce qui représente une charge de l'UTC du routeur #1 à 92,8%, mais seulement de 55.4% pour les routeurs #2 et #3. Au-delà de ce seuil, (*Voir* Figure 5.17) les échanges FTP se dégradent rapidement à moins de 1 méga-octet par seconde. Le trafic d'encombrement atteint un maximum mesuré à 47,000 paquets par seconde pour un débit de 2.26 méga-octets par seconde (*Voir* Figure 5.18). On indique le moment précis ou le débit d'encombrement surcharge l'UTC du routeur.

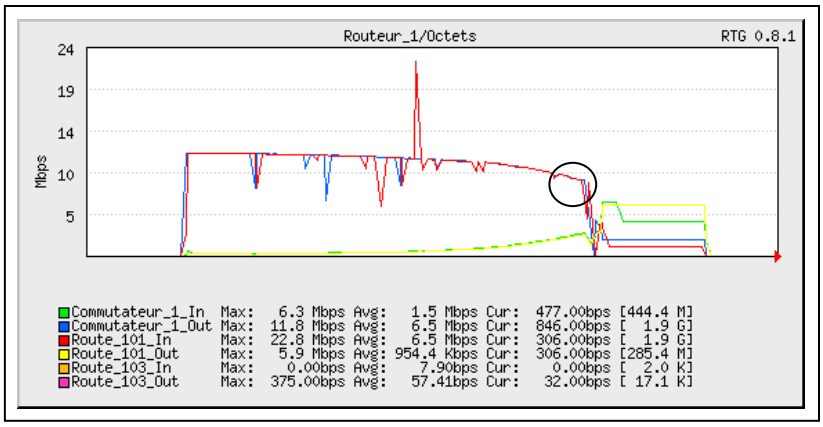


Figure 5.17 Mesure en octets du trafic FTP avec encombrement de 64 octets aux ports de routeur. On indique le moment ou TCP cesse de fonctionner convenablement.

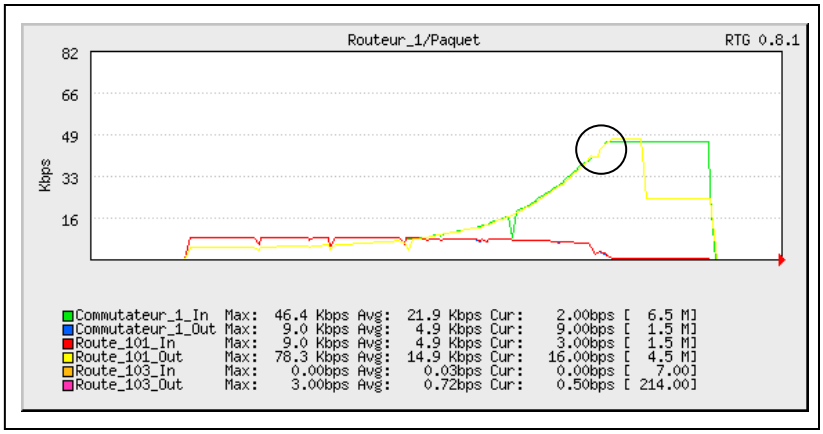


Figure 5.18 Mesure en paquets du trafic FTP avec encombrement de 64 octets aux ports de routeur. On indique moment ou le niveau d'encombrement surcharge le routeur.

Le délai est en moyenne de 5.25 millisecondes, mais s'est accru à 34.5 millisecondes dès que le trafic d'encombrement atteint le cap des 33,000 paquets par seconde ou 2.11 méga-octets soit 7% sous le débit de saturation de l'équipement. L'élément important à retenir pour cette expérience est que la quantité de donné recueillie par RTG est affectée lorsque le niveau d'encombrement sature l'interface ou les UTC. Ceci est surtout visible par la quantité de paquet à l'interface du routeur et commutateur.

5.3.3 Trafic FTP avec encombrement variable de 128 à 1518 octets

L'observation de l'encombrement selon différentes tailles des paquets et du débit sur le trafic FTP permet d'établir les points suivants :

- Lorsque la taille des paquets du trafic d'encombrement dépasse 256 octets. On indique le moment précis où les équipements réseau atteignent le maximum du débit de l'équipement de 96 Mb/s (Voir Figure 5.19). Les équipements réseau atteignent ce maximum sans égard de la nature du trafic. L'élément de perturbation étant moins dévastateur pour l'environnement de mesure, ici on réussi à distinguer les éléments de perturbations.
- Aucune coupure de communication FTP n'a été détectée pour tous les scénarios d'encombrement.
- Le temps de transfert entre le serveur FTP et le client est en moyenne 30% de plus par rapport à l'absence de trafic d'encombrement.
- La charge des UTC reste stable à 40% avec des paquets d'encombrement de 1518 octets. Pour les autres tailles, la charge décroît du sommet de 95% pour des paquets de taille de 64 octets à 62% pour des paquets de taille de 1024 octets.
- Le trafic SNMP n'est plus perturbé par le trafic d'encombrement lorsque les paquets sont de 320 octets et plus.

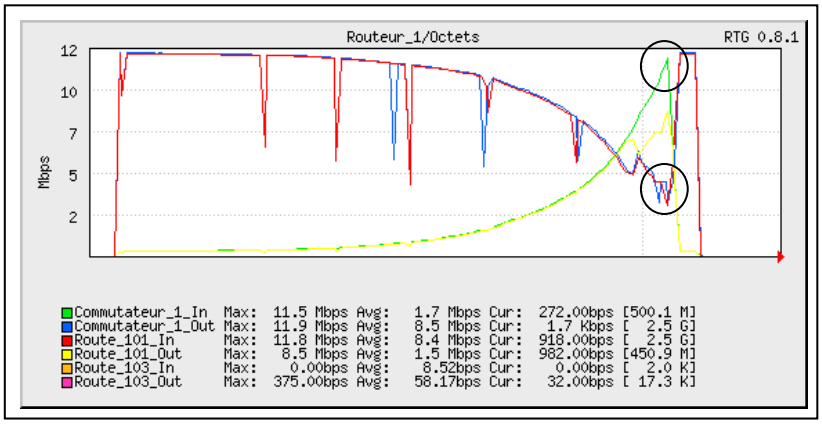


Figure 5.19 Mesure du trafic FTP avec encombrement de 256 octets aux ports des routeurs. On indique le moment ou TCP cesse de fonctionner convenablement.

5.3.4 Caractérisation du réseau de l'encombrement sur TCP

Le trafic en TCP est sensible à l'encombrement des paquets de petite taille inférieure à 256 octets et à la charge des UTC des routeurs. Il est concevable d'avoir deux critères de sélection afin d'amorcer un avertissement ou une alarme pour le trafic TCP. Le premier critère une quantité définie de paquets pour des paquets dont la taille varie entre 64 à 256 octets. Le second est le niveau de charge des UTC des routeurs.

5.4 Le trafic de la voix sur IP

La voix sur IP est conçue avec un mécanisme de compression afin de limiter l'encombrement du trafic sur l'infrastructure de communication. Malgré ce mécanisme, ce scénario a pour but de démontrer quel serait l'impact qu'un encombrement procure lors d'une communication entre deux interlocuteurs. La présente est l'essai de l'encombrement sur une communication entre deux postes de téléphone IP. La source d'encombrement est la même que celle utilisée lors des expériences précédentes. On retrouve la charge des UTC (*Voir* Figure 5.24) en moyenne de 3% avec un comportement réseau (*Voir* Figure 5.20 et 5.21) lors

de la communication de référence. L'encodage est G.711µ de 64Kbps. Le niveau du trafic des paquets RTP est d'environ 95 Kbps. Tous les paquets transmis sont de taille fixe à 172 octets. On observe du poste qui effectue l'appel, la transmission de treize paquets au gestionnaire d'appel pour établir la communication. Aucun message n'est transmis au gestionnaire par la suite.

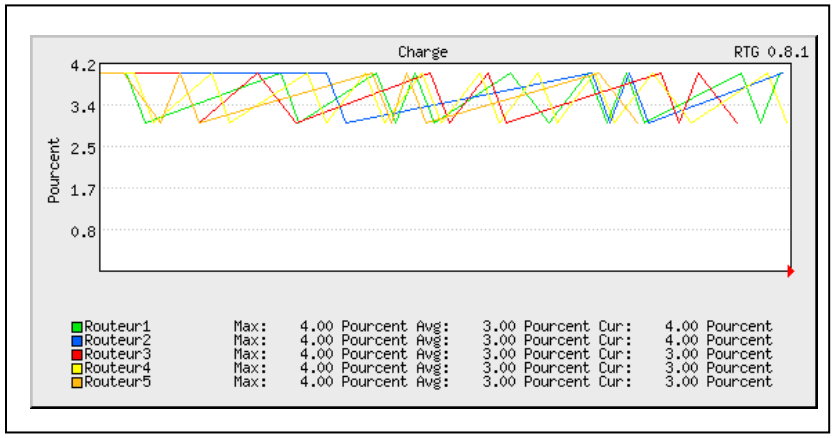


Figure 5.20 Charge UTC des routeurs pour de la VoIP sans encombrement.

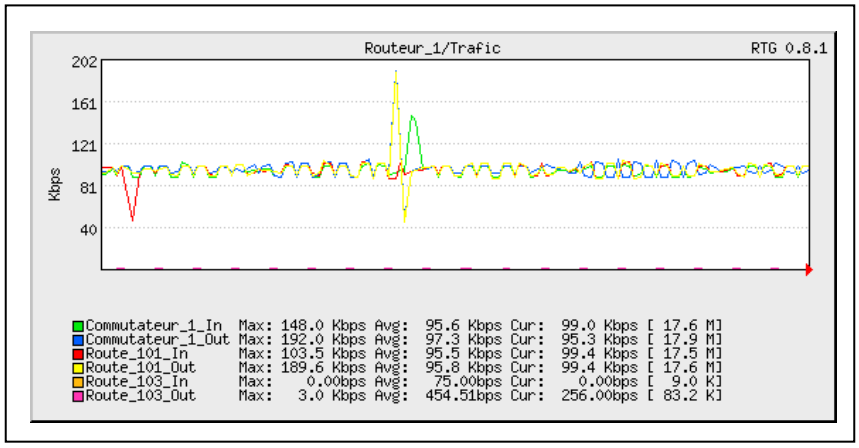


Figure 5.21 Mesure en octets du trafic de VoIP.

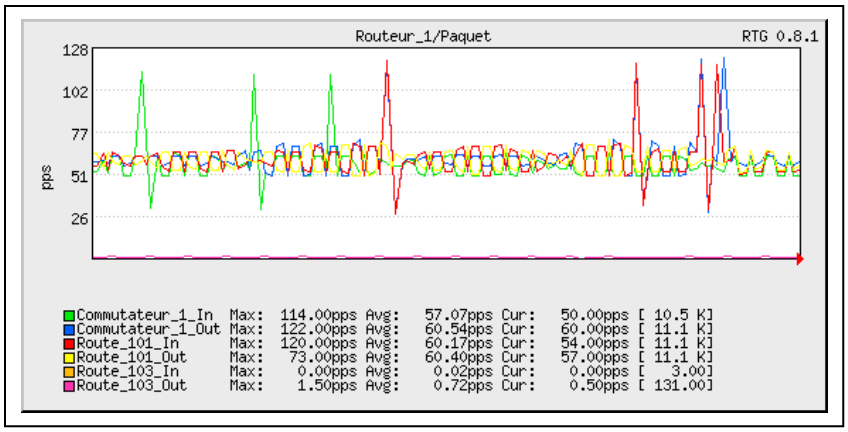


Figure 5.22 Mesure en paquet du trafic de VoIP.

5.4.1 Encombrement à 64 octets sur trafic de voix sur IP

Pour la voix sur IP, on observe le même impact de l'encombrement de paquets de 64 octets sur les équipements de réseaux. La charge des routeurs ainsi que la saisie des informations SNMP sont quasi nulles lorsque le débit d'encombrement atteint 3.11 méga-octets au routeur #1. L'effet de l'encombrement ne dure que 32 secondes durant lesquelles, sept résultats de requêtes SNMP soit 23% de l'échantillonnage ont été enregistrés. Comme tous les autres expériences précédentes, on observe (*Voir* Figure 5.23) la lecture du trafic de la VoIP directement aux ports des commutateurs auxquels les postes téléphoniques sont connectés. On indique le moment où l'information du trafic de la voix sur IP ainsi que la durée ne parviennent plus à SRS. Lorsque le trafic d'encombrement a cessé d'être transmis, on observe la reprise des échanges de trafic de conversation entre les deux interlocuteurs. La durée de l'effet perturbateur n'a pas permis de rompre définitivement le lien. On note l'espace de temps où SNMP devrait rapporter une diminution notable du trafic de la VOIP tel qu'obtenu via TShark et par la mesure de la qualité de la voix sur IP via MOS. Avec la saturation des routeurs, le réseau SNMP ne recueille aucune information utile qui permettrait de mesurer l'impact de cet encombrement.

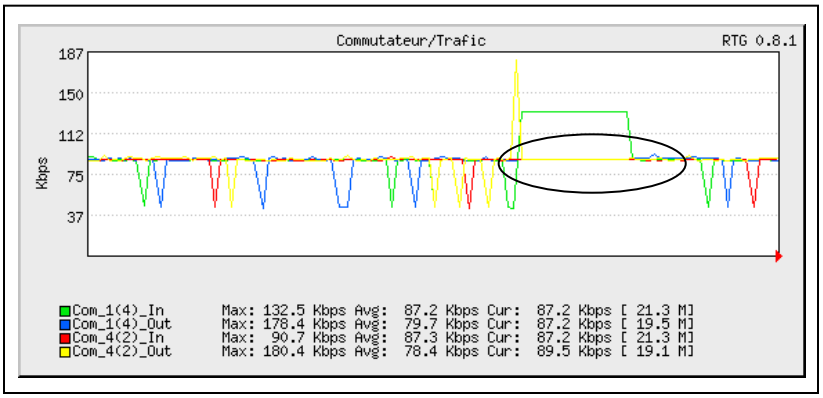


Figure 5.23 Mesure de la VoIP avec l'encombrement à 64 octets au commutateur. On indique le moment ou aucune information ne parvient au poste de téléphone.

Le trafic d'encombrement emprunte la même route que le trafic de voix sur IP sans encombrer directement tous les échanges entre les postes téléphoniques IP. Le gestionnaire des appels est connecté sur le commutateur #3 et l'observation du trafic démontre des échanges normaux. Aucun trafic n'est échangé entre le gestionnaire d'appel et les postes de téléphone à la suite de la présence de l'encombrement. Il semble que le gestionnaire d'appel n'a aucun mécanisme d'intervention pour prendre action pour contrer l'effet de la latence et des pertes de paquets entre les postes téléphoniques. Le délai et la gigue sont quasi inexistant jusqu'au moment où le trafic d'encombrement atteint 2.1 méga-octets. SRS rapporte en moyenne 22 millisecondes de latence sur la route encombrée ce qui est dans les tolérances de selon la norme de la voix sur IP (International Telecommunication Union. Telecommunication Standardization Sector., 2003). Cependant par l'emploi de la méthode d'analyse de performance de la VoIP *Mean Opinion Score* (MOS) (International Telecommunication Union. Telecommunication Standardization Sector., 2006) balisée par un classement de 1 qui est la plus basse valeur et 5 étant la meilleure, l'expérience reçoit un score de 2. On ne remarque (*Voir* Figure 5.23) aucune diminution du débit du trafic de la VoIP ou perte de paquet. Cependant, avec l'analyse des échantillons obtenus par l'application Tshak valide le résultat de MOS. Sur la période de l'encombrement saturé de routeur #1 on observe sur la figure 5.24 que le délai moyen est de 330 millisecondes soit le double de la limite acceptable de la VOIP. On note également une diminution de 50% des paquets reçus.

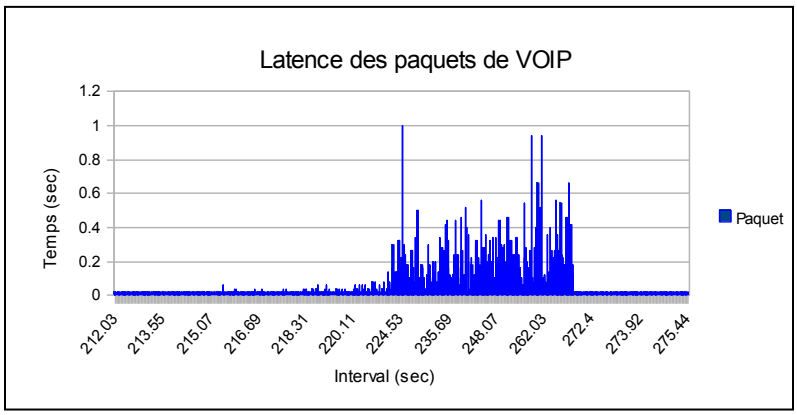


Figure 5.24 Latence de la VoIP.

5.4.2 Encombrement variable de 128 à 1518 octets sur trafic de voix sur IP

L'effet mesuré de l'encombrement procure un effet perturbateur dont la durée varie de 20 secondes pour des paquets de 128 octets à 5 secondes pour des paquets de 448 octets sur les échanges entre les points de communication. On indique le moment où la perturbation pourrait avoir un effet contraignant (*Voir* Figure 5.25). On note qu'à la différence de l'encombrement de trafic avec des paquets de 64 octets, ici l'application RTG recueille l'information du trafic de la voix sur IP. La période d'encombrement la plus intense est encerclée. Ceci démontre la viabilité de l'information lorsque le réseau est optimal. À la suite des résultats, l'amorce de la latence et de la perte de paquets RTP intervient lorsque l'UTC d'un routeur atteint 100%.

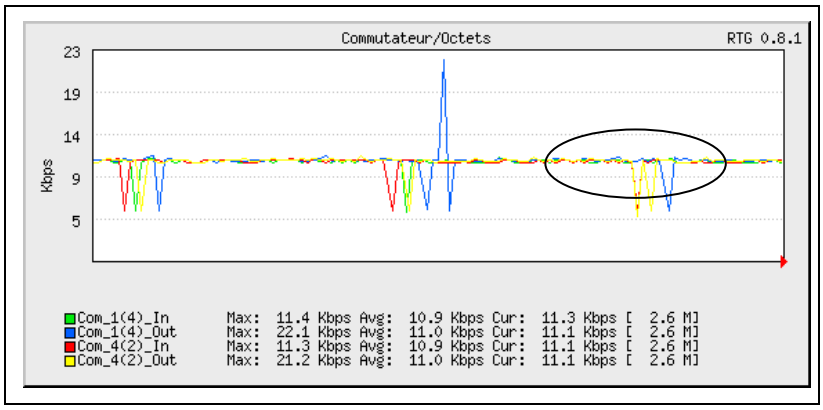


Figure 5.25 Mesure de la VoIP avec l'encombrement 256 octets. On indique le moment ou possiblement la communication pourrait être perturbée.

5.5 Le trafic de la vidéo sur IP

La vidéo sur IP retenue pour ce scénario est basée par une diffusion d'une source vers une destination unicast. Le trafic vidéo est simulé avec l'outil Iperf. La vidéo est caractérisée par une diffusion de paquets UDP dont la taille est de 1260 octets excluant l'en-tête IP. Le débit moyen est de 384 Kbps par seconde ce qui représente de 30 images à la seconde. Selon les scénarios d'essais de la diffusion entre la source et la destination sans trafic d'encombrement, le délai de propagation varie entre 0.035 et 0.061 milliseconde. Le délai est rapporté par l'application. La charge des unités de traitement centrales des routeurs est stable (*Voir* Figure 5.26) ainsi que le débit constant de 398 Kbps (*Voir* Figure 5.27). On observe cependant un comportement différent sur trafic des paquets sur les différents ports du routeur #1 (*Voir* Figure 5.28)

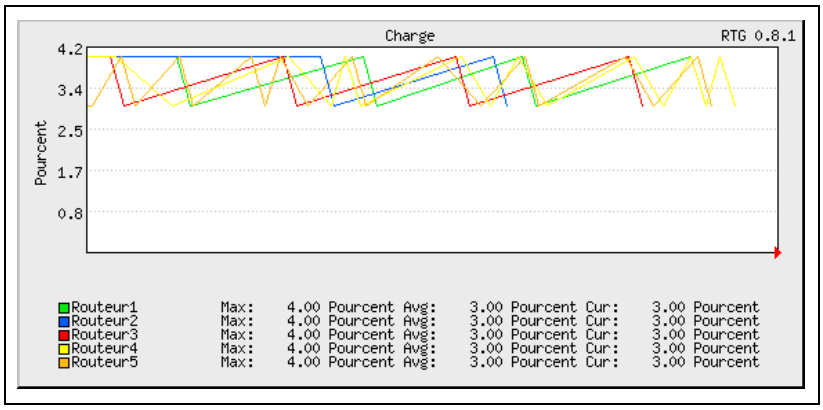


Figure 5.26 Charge UTC des routeurs pour de la Vidéo sur IP sans encombrement.

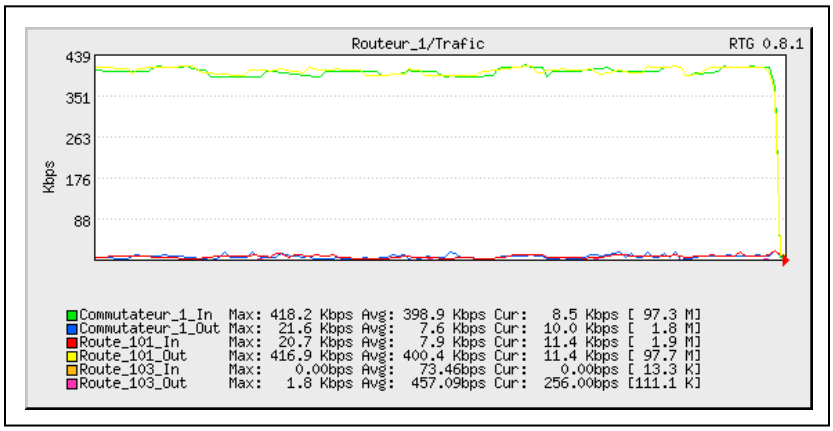


Figure 5.27 Mesure en octets aux ports du routeur #1 de la vidéo sur IP.

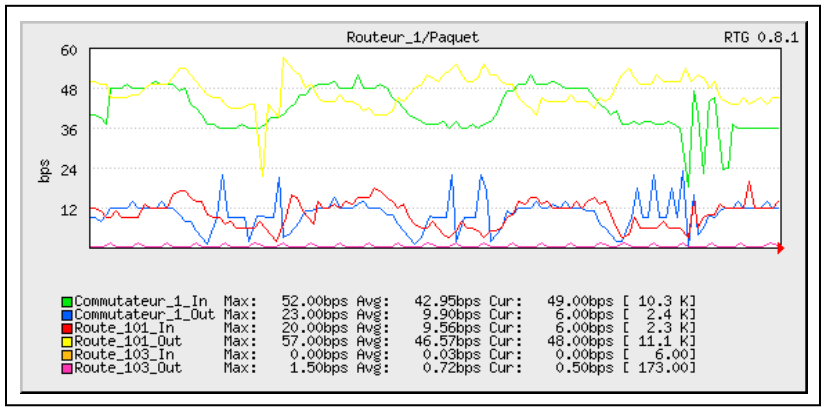


Figure 5.28 Mesure des paquets aux ports du routeur #1 de la vidéo sur IP.

5.5.1 Encombrement à 64 octets sur trafic vidéo sur IP

Comme les scénarios précédents sur l'encombrement de paquets à 64 octets, on observe le même effet de l'encombrement sur la vidéo IP. On constate la régularité de la diffusion et la réception du trafic (*Voir* Figure 5.29). C'est-à-dire on observe la constance du débit en moyenne de 30 paquets par seconde sans altération visible sous l'effet de l'encombrement exception lorsque le banc d'essai devient saturé. On indique le moment et la durée de la perturbation sur la saisie des informations SNMP. Tout comme le scénario de la voix sur IP, le même effet de l'encombrement se produit sur la saisie des informations via SNMP. Ici l'information est à toute fin pratique nulle. Le graphique n'indique pas les omissions. Cependant, les données démontrent pendant quelques secondes qu'aucune donnée n'est enregistrée par RTG dû au mode configuré qui conserve seulement des donnés différentes aux données précédentes. Ceci permet l'affichage cerné qui ne reflète pas la réalité observée avec l'application.

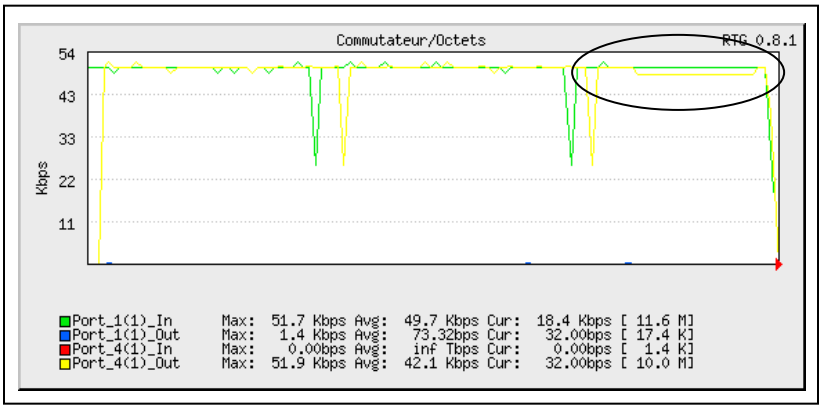


Figure 5.29 Mesure en octets de la vidéo sur IP aux commutateurs. On indique le moment où l'encombrement bloque la capture de l'information SNMP.

Avec les audits des données recueillies à la destination par l'outil Iperf, on démontre une autre réalité. L'outil maintient le débit des paquets constant, mais avec l'encombrement à 15,500 paquets par seconde et qui s'accentuent, cela engendre une latence qui atteint 0.5 milliseconde pour la vidéo, à un taux de trafic d'encombrement de 45,000 paquets par

seconde. Le débit de l'outil à ce moment est de 374 Kbps. Avec l'imprécision observée de la figure 5.29 les audits de l'application permettent d'avoir la situation réelle. La perte de paquets survient par le fait que la latence entre les paquets est plus en plus grande par rapport au niveau de tolérance de l'application étant donné que l'information du paquet n'a plus de valeur utile après un certain temps. À ce niveau, l'application accepte une perte de paquets de 50% et l'accentue selon l'accroissement du débit du trafic l'encombrement. Il en résulte une réduction de la latence pour la vidéo (*Voir* Figure 5.30 et Figure 5.31) et la perte de paquets pour Iperf qui atteint 0 Kbps lorsque le réseau devient saturé. SRS ne démontre pas cette perte de paquets au port du commutateur.

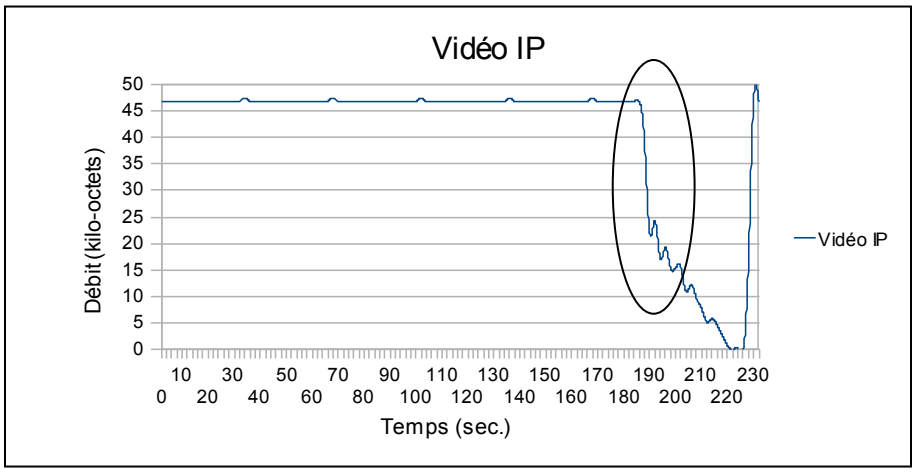


Figure 5.30 Mesure du débit reçu de la vidéo sur IP.
On indique le moment où la perte du débit se manifeste brusquement.

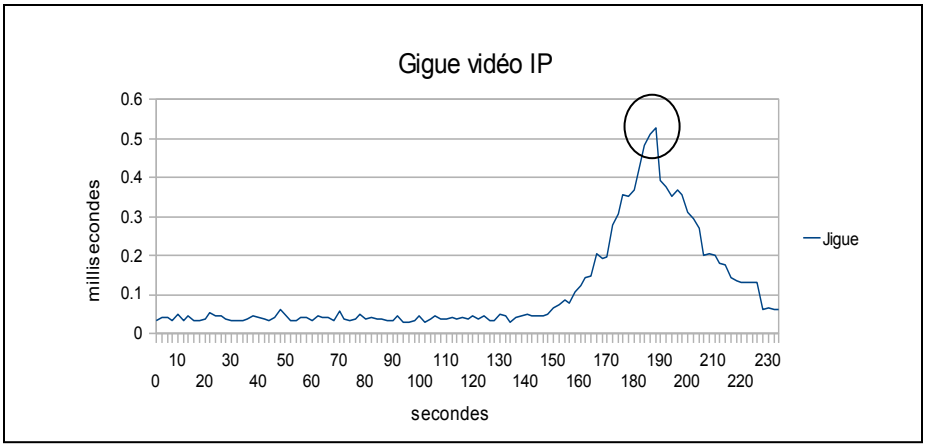


Figure 5.31 Mesure de la gigue de la vidéo sur IP. On indique le moment ou l'application rejette des paquets afin de minimiser la perte de la latence.

5.5.2 Encombrement variable de 128 à 1518 octets sur trafic de vidéo sur IP

La configuration utilisée avec Iperf, soumise un à trafic d'encombrement de 45,000 paquets par seconde occasionne toujours le même effet perturbateur. L'application agit sur le rejet de paquets qui atteint, un taux de 30.8 Kbps lorsque le réseau est saturé avec des paquets d'encombrement de 128 octets. La latence, moins importante que les scénarios de test précédent, varie de 0.1 à 0.4 milliseconde. Avec un trafic d'encombrement à 256 octets (*Voir* Figure 5.32), on observe seulement la fluctuation dans la latence. Le débit mesuré à 374.4 Kbps est constant pour ce test ainsi que pour les tests successifs d'encombrement.

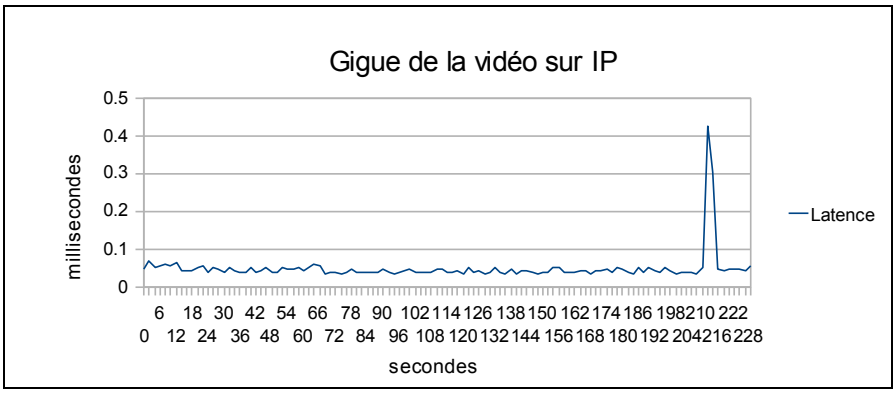


Figure 5.32 Mesure de la gigue, trafic de paquets à 256 octets.

5.6 La qualité de service

La qualité de service a été mise en place par la configuration de tous les ports des commutateurs afin d'effectuer ou de respecter le marquage des trames via le protocole 802.1 Q/p et par la transition à la frontière du réseau de niveau 2 par Diffserv (Blake et al., IETF 1998) qui fait suivre le marquage d'un paquet IP pour sa migration aux différents routeurs. Les premiers essais avec la qualité de service ont été faites selon l'algorithme LLQ / CBWFQ qui s'applique sur l'interface de l'écoulement du trafic seulement. Sur le banc d'essai, la configuration LLQ est appliquée dans un premier temps sur l'interface de sortie de la route 101 du routeur #1.

5.6.1 Classe de service

Trois classes de service ont été identifiées pour le traitement de la QdS. La classe de trafic par défaut *Differentiated Services Code Point* DSCP 0, la classe de trafic de la vidéo sur IP DSCP 24 et la classe de trafic de la voix sur IP DSCP 46.

5.6.2 Règle de services

Pour chaque classe de service, des règles de traitement ont été créées. La priorité stricte du traitement est attribuée à la classe de trafic de la voix sur IP. La largeur de bande est limitée à 256 kbps. Il est permis que le trafic de la voix sur IP occupe plus de la largeur de bande, mais la limite de garantie est fixée a 256 kbps. La politique de la vidéo sur IP permet l'utilisation jusqu'à 70 % de la largeur de bande de l'interface. La classe de trafic par défaut DSCP 0 se limite à la largeur de bande résultante des politiques précédentes.

5.6.3 Les MIBs de la qualité de service

Sur l'équipement la table MIBs associée à la qualité de service est *Cisco-class-based-qos-mib.* La sélection des objets à surveiller se fait par l'analyse des OIDs de configuration qui comprend la branche générale (Voir Figure 5.33) et la branche de l'assignation des classes (Voir Figure 5.34) afin de noter le numéro arbitraire assigné aux index de chaque objet. Pour chaque interface, dans le cas qui est la vlan 101 est associé une paire de numéros arbitraire qui identifie la politique ainsi que l'action à prendre (*Voir* Figure 5.35).

```
CISCO-CLASS-BASED-QOS-MIB::cbQosCMName.1025 = STRING: class-default
CISCO-CLASS-BASED-QOS-MIB::cbQosCMName.1029 = STRING: voip
CISCO-CLASS-BASED-QOS-MIB::cbQosCMName.1035 = STRING: video
```

Figure 5.33 Identifications des OID selon les classes de trafic configurées.

```
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtName.1027 = STRING: Match any
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtName.1033 = STRING: Match  dscp ef (46)
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtName.1039 = STRING: Match  dscp cs3 (24)
```

Figure 5.34 Assignation des OID selon les règles configurées.

```
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1193 = Gauge32: 1041
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1195 = Gauge32: 1029
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1197 = Gauge32: 1033
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1199 = Gauge32: 1043
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1201 = Gauge32: 1035
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1203 = Gauge32: 1039
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1205 = Gauge32: 1045
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1207 = Gauge32: 1025
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.1193.1209 = Gauge32: 1027
```

Figure 5.35 Configuration des OID selon les actions aux interfaces.

5.6.4 Mesure de la QdS

Pour mesurer les effets de la qualité de service, les scénarios de l'encombrement pour la voix sur IP ainsi que la vidéo décrite à la section 5.2 ont été répétés. On note que l'ajout du traitement de la QdS ainsi que quatorze objets d'information choisie pour une interface a fait augmenter le travail de l'UTC du routeur #1 de 2% pour s'établir à 5%. Les premiers résultats démontrent que la capture des informations des OID de la QdS est plus lente que les objets d'information des autres catégories de MIBs. L'information est rapportée en moyenne toutes les dix secondes. Étant donné ce facteur, il faut diviser par dix les données de la QdS afin d'obtenir des données homogènes aux autres rapports graphiques comme le démontre les figures 5.36 et 5.37.

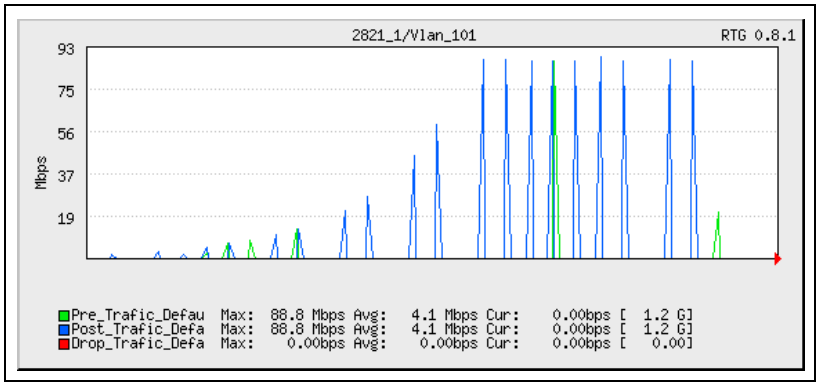


Figure 5.36 Traitement du trafic de la classe par défaut (*Best effort*) à l'interface de sortie du vlan 101.

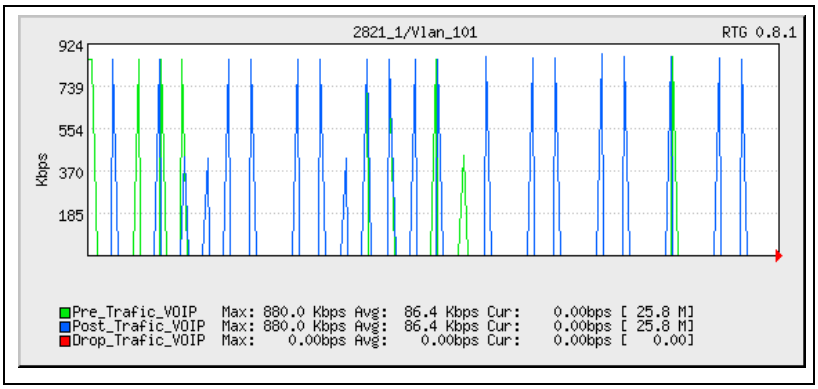


Figure 5.37 Traitement du trafic de la class de VOIP (*Expided forward*) à l'interface de sortie du vlan 101.

5.6.5 Effet de l'encombrement avec la QdS

Lors des premiers essais de l'encombrement, on observe que le traitement de l'UTC du routeur #1 où est appliqué le traitement de la qualité de service est de 40% supérieure par rapport aux autres routeurs du réseau. L'observation des résultats aux ports des équipements n'ont offert aucun changement par rapport aux résultats des expériences des sections 5.4.1 et 5.5.1. Les premières observations du traitement de la QdS sur les classes de trafic n'ont pas donné les résultats anticipés. Comme le démontre la figure 5.37, avec la QdS le trafic d'encombrement sature le lien, et la perte de paquets de la voix sur IP est de 80% tel que le d/montre la figure 5.38

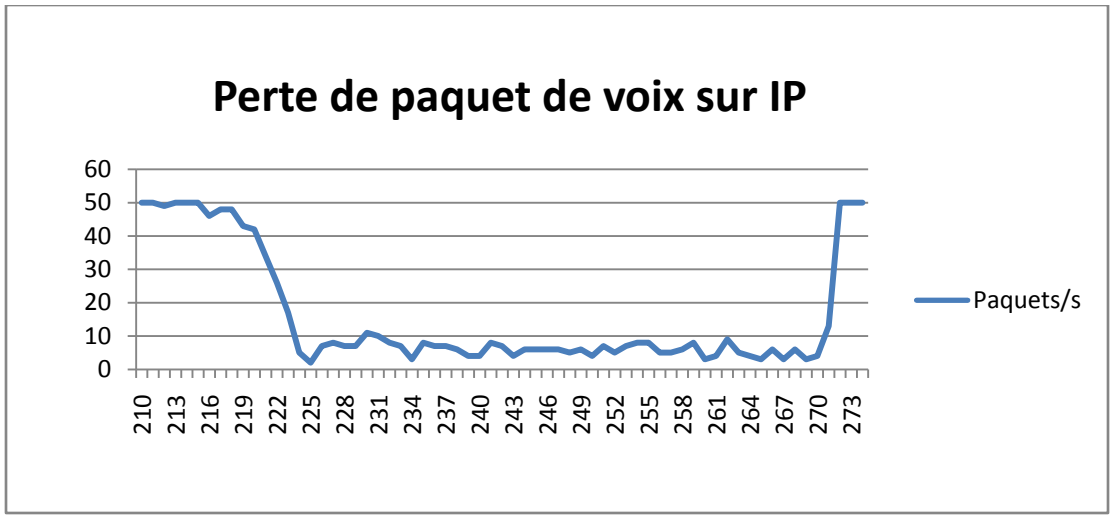


Figure 5.38 Observation du trafic de la VOIP par l'analyseur de trafic Wireshark.

La figure 5.39 montre l'absence de priorité de la classe de trafic DSCP 24 associée à la vidéo. Le trafic d'encombrement de la classe DSPC 0 engendre toujours le même effet perturbateur malgré les règles de QdS sur l'interface. Le nombre de paquets avant traitement et après traitement de la QdS est toujours identique. Le contenu des files d'attente des différentes classes de trafic n'indique aucune accumulation et aucun rejet de paquets. Tout indique que la qualité de service de l'équipement n'effectue aucun traitement. Après l'expérimentation de différents essais et configurations qui n'ont donné aucun résultat probants, on conclue cet équipement n'effectue aucun traitement de la QdS. Des recherches sur le site de la compagnie Cisco ont finalement abouti sur des éléments techniques qui confirment ce qui a été mesuré sur la QdS. Les interfaces peuvent effectuer le marquage des paquets de trafic selon une configuration qui est classée et visible via le Mibs de la QdS, mais aucun traitement n'est effectué selon ces mécanismes.

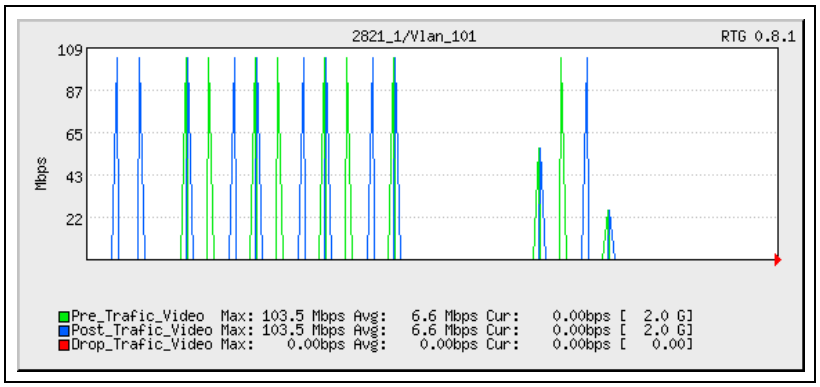


Figure 5.39 Mesure du traitement de la QdS de la classe de trafic vidéo

Aucun scénario subséquent n'a été étudié avec la QdS pour contrer l'effet de la perturbation.

CONCLUSION

Ce mémoire a été réalisé afin d'expérimenter une méthodologie sur la surveillance des réseaux en temps réel et de mesurer de façon précise les limites de fonctionnement de l'environnement de communication d'un banc d'essai réseautique pour une application de travail collaboratif dans le but de contrer la perturbation. La problématique a été définie lors de la conception du banc d'essai ou le défi était de concevoir un environnement de surveillance qui offrait des caractéristiques de précision, d'intégrité, de quantité et d'échantillonnage au niveau de la seconde afin de détecter la perturbation, lorsque la plupart des produits commerciaux offraient ces caractéristiques à l'échelle de la minute. En deuxième temps nous avons étudié la viabilité de la mesure et de la performance du protocole SNMP. Ces mesures ont été accomplies avec une partie des équipements du banc d'essai et l'environnement logiciel Net-SNMP sous Linux CentOS. Dans un troisième temps. Il y a eu la conception, le développement et la construction du banc d'essai. Dans un quatrième temps une batterie de tests a été faite avec les logiciels de surveillance populaires pour parvenir à la granularité recherchée dont MRTG et CACTI, mais l'application de surveillance retenue est RTG qui offre une très grande rapidité de l'échantillonnage et une intégrité des informations via SNMP.

Dans un cinquième temps, plusieurs scénarios de test ont permis d'explorer une grande quantité d'éléments réseau sous des conditions contrôlées sur le banc d'essai soumis aux différentes perturbations. Ceci nous a permis d'atteindre nos objectifs, d'une part obtenir les limites de fonctionnement des équipements et environnement de communication pour l'opérabilité du banc d'essai, d'autre part de déterminer la limite opérationnelle des flux de trafics ainsi que les caractéristiques générales des causes de la perturbation pour chacun d'entre eux.

Dans un dernier temps plusieurs scénarios ont été refaits sous l'influence de la qualité de service dans l'internet, notamment, l'habilité du réseau de fournir un traitement approprié

pour les différentes classes de trafic. L'objectif principal de la QdS employé est d'accorder la priorité aux classes de trafic important et sensible aux variations des flux. Il offre un mécanisme aux interfaces encombrées qui permet de prendre des décisions sur le traitement des files d'attente et le rejet des paquets. Mesurer les besoins des mécanismes existants permet de peindre un portrait du fonctionnement, même si le réseau possède des qualités acceptables qui sont loin d'être idéales. Lors des expériences sur le banc d'essai, la mesure des différents paramètres supportés par la QdS s'est avéré un exercice d'investigation démesurée et répétitif pour chaque élément de configuration des paramètres de la qualité de service des équipements. L'observation des résultats a démontré que les équipements possèdent les MIB associés aux différents types de qualité de service, mais aucun équipement matériel pour faire le traitement configuré.

RECOMMANDATIONS

Cette section propose des avenues de développement qui concerne la poursuite des essais sur d'autres environnements de réseaux ainsi que des recommandations qui concernent l'ajout d'élément de fonctionnement ainsi que l'amélioration des performances du système de surveillance de Synchromédia.

L'idée derrière le développement d'un réseau d'essais avec des outils de surveillance en temps réel a toujours été de fournir des réponses précises et complètes aux questions des développeurs pour la conception, le développement et la validation et de découvrir les irrégularités dans le fonctionnement réseau de la plateforme. Ce questionnement a donné lieu à la recherche des causes et des moyens de prévention possibles pour contrer la perturbation du fonctionnement de la plateforme de travail collaboratif de Synchromédia. Pour y arriver, plusieurs fonctionnalités ont été conçues sur SRS, afin de répondre aux nombreuses questions et problématiques. Certains de ces concepts ont été essayés sur SRS comme l'utilisation de l'application Tshark, NetFlow et même plusieurs scénarios d'essais de la QdS. Les résultats obtenus avec ces outils offrent une information beaucoup plus réelle et complète dans leurs ensembles. Cependant, l'intégration de ces informations dans un environnement uniforme de SRS, tout en conservant le but recherché de la précision et de l'intégrité des données, est une difficulté à laquelle cette recherche a été confrontée.

L'application TShark a été utilisée dans le but d'obtenir des échantillons de quelques paquets de trafic parmi une sélection de ports afin d'avoir une vue très précise sur la nature du trafic mesuré. L'application permet la saisie du trafic selon une quantité maximale de paquets ou sur une période de temps. La problématique du système est le stockage des informations qui peuvent prendre des proportions énormes par rapport aux espaces de stockage disponible pour cette recherche. Cet outil n'a donc pas été retenu pour SRS.

Netflow est un autre outil qui offre un large inventaire d'informations moins précises que l'application TShark. Comme décrit à la section 3.4.1 Netflow rapporte une vue d'ensemble selon une période de temps, en moyenne à toutes les cinq minutes (*Voir* Annexe I)
L'intégration de ces informations dans l'environnement SRS bien qu'utiles et complémentaires est un travail non essentiel pour le but recherché.

ANNEXE I

ÉCHANTILLION DE NETFLOW

Échantillions de Netflow version 9 via nfcapd et nfdump

Date flow start	Duration	Proto	Src IP Addr:Port	Input		Dst IP Addr:Port	Output	Flags	Tos	Packets	Bytes	Flows
2008-11-11 17:12:23.648	0.000	TCP	192.168.33.252:2000	19	->	192.168.11.201:52841	16	.AP...	96	1	52	1
2008-11-11 17:12:23.648	0.000	TCP	192.168.33.252:2000	19	->	192.168.11.201:52841	16	.AP...	96	1	52	1
2008-11-11 17:08:18.220	259.996	UDP	192.168.11.101:1048	16	->	192.168.14.104:5001	19	.A....	0	26417	32.4 M	1
2008-11-11 17:08:18.220	259.996	UDP	192.168.11.101:1048	16	->	192.168.14.104:5001	19	.A....	0	26417	32.4 M	1
2008-11-11 17:12:38.220	0.000	UDP	192.168.14.104:5001	19	->	192.168.11.101:1048	16	.A....	0	1	1288	1
.												
.												
2008-11-11 17:14:25.012	0.000	TCP	192.168.33.252:2000	19	->	192.168.11.201:52841	16	.AP...	96	1	52	1

Summary: total flows: 24, total bytes: 64.9 M, total packets: 52866, avg bps: 1.4 M, avg pps: 144, avg bpp: 1287

Time window: 2008-11-11 17:08:18 - 2008-11-11 17:14:25

Total flows processed: 24, skipped: 0, Bytes read: 1260

Sys: 0.001s flows/second: 12006.0 Wall: 0.000s flows/second: 24340.8

ANNEXE II

MIB DE LA QUALITÉ DE SERVICE

OID de l'information sur la nature de la configuration.

cbQosConfigIndex.Index.Index
cbQosObjectsType.Index.Index
cbQosPolicyMapName.Index

OID de l'information sur les configurations et contenu des différentes queues avant et après traitements sur les « class-map ».

cbQosCMName. Index
cbQosCMDesc. Index.Index
cbQosCMPrePolicyPkt. Index.Index
cbQosCMPrePolicyByte. Index.Index
cbQosCMPrePolicyBitRate. Index.Index
cbQosCMPostPolicyByteOverflow. Index.Index
cbQosCMDropPkt. Index.Index
cbQosCMDropByte. Index.Index
cbQosCMNoBufDropPktOverflow. Index.Index

OID de l'information sur les configurations et le contenu des différentes queues selon les unités.

cbQosQueueingCfgBandwidth. Index
cbQosQueueingCfgBandwidthUnits. Index
cbQosQueueingCfgFlowEnabled. Index
cbQosQueueingCfgPriorityEnabled. Index
cbQosQueueingCfgAggregateQSize. Index
cbQosQueueingCfgIndividualQSize. Index
cbQosQueueingCfgPrioBurstSize. Index
cbQosQueueingCurrentQDepth. Index.Index
cbQosQueueingMaxQDepth. Index.Index
cbQosQueueingDiscardByte. Index.Index
cbQosQueueingDiscardPktOverflow. Index.Index

cbQosQueueingDiscardPkt. Index.Index

OID du contenu associé aux configurations et statistiques des unités avant traitement des polices de QdS.

cbQosMatchStmtName. Index
cbQosMatchPrePolicyPkt. Index.Index
cbQosMatchPrePolicyByte. Index.Index
cbQosMatchPrePolicyBitRate. Index.Index

BIBLIOGRAPHIE

Agoulmine, Nazim, et Omar Cherkaoui. 2003. *Pratique de la gestion de réseau : solutions de contrôle et de supervision d'équipements réseau pour les entreprises et les opérateurs télécoms*. Paris: Eyrolles, xii, 275 p.

Atsushi, Kobayashi, et Toyama Katsuyasu. 2007. « Method of Measuring VoIP Traffic Fluctuation with Selective sFlow ». In *Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on*. p. 89-89.

Ben-Artzi, A., A. Chandna et U. Warrier. 1990. « Network management of TCP/IP networks: present and future ». *Network, IEEE,* vol. 4, n° 4, p. 35-43.

Beverly, Robert. 2002. « RTG: A Scalable SNMP Statistics Architecture for Service Providers ». In *Lisa Proceedings 2002: Sixteenth Systems Administration Confefence* (Philadelphia 3-8 novembre 2002). p. 8. Berkeley, CA <http://www.usenix.org/events/lisa02/tech/beverly/beverly.pdf>.

Blake, S., D. Black, M. Carlson, Davies. E., Z. Wang et W Weiss. IETF 1998. « RFC 2475: An Architecture for Differentiated Services ». <http://www.ietf.org/rfc/rfc2475.txt?number=2475>.

Bradner, S., et J. McQuaid. IETF 1999. « RFC 2544: Benchmarking Methodologue for Network Internconnect Devices ». <http://www.ietf.org/rfc/rfc2544.txt?number=2544>.

Cacti - a complete network graphing solution Aout 2008. <http://www.cacti.net/>.

Case, J., M. Fedor, M. Schoffstall et J. Davin. IETF 1990. « RFC 1157: A Simple Network Management Protocol (SNMP) ».

Case, J., K. McCloghrie, M. Rose et S. Waldbusser. IETF 1996. « RFC 1901: Introduction to Community-based SNMPv ». <http://www.ietf.org/rfc/rfc1901.txt?number=1901>.

Case, J., R. Mundy, D. Partain et B. Stewart. IETF 1999. « RFC 2570: Introduction to Version 3 of the Internet-standard Network Management Framework » <http://www.ietf.org/rfc/rfc2570.txt?number=2570>.

Cisco Systems, Inc. 2007. « Introduction to Cisco IOS NetFlow - A Technical Overview » <http://www.cisco.com/application/pdf/en/us/guest/products/ps6601/c1042/cdccont_0900aecd80311fc2.pdf>.

Deri, L, et R Carbone. 1998. *Nework Top*. <http://www.ntop.org/news.html>.

Estan, Cristian. 2003. « Internet traffic measurement: What's going on in my network? ». Ph.D., United States -- California, University of California, San Diego. <http://proquest.umi.com/pqdweb?did=764887931&Fmt=7&clientId=46962&RQT=309&VName=PQD>.

FlowScan - Network Traffic Flow Visualization and Reporting Tool <http://www.caida.org/tools/utilities/flowscan/>.

Fullmer, Mark. *flow-tools -- Tool set for working with NetFlow data* <http://www.splintered.net/sw/flow-tools/docs/flow-tools.html>.

Haag. 2007. « NFdumpd & NFcapd ». <http://nfsen.sourceforge.net/>.

Heinanen, J., F. Baker, W. Weiss et J. Wroclawski. IETF 1999. « RFC 2597: An Assured Forwarding PHB ». <http://www.ietf.org/rfc/rfc2597.txt?number=2597>.

International Telecommunication Union. Telecommunication Standardization Sector. 2003. « ITU-T G.114 One-way transmission time ». In. <http://www.itu.int/rec/T-REC/g>.

International Telecommunication Union. Telecommunication Standardization Sector. 2006. « ITU-T P.800.1 Mean Opnion Score (MOS) terminology ». In <http://www.itu.int/rec/T-REC/p>.

Jacobson, V., K. Nichols et B. Poduri. IETF 1999. « RFC 2598: An Expedited Forwarding PHB ». <http://www.ietf.org/rfc/rfc2598.txt?number=2598>.

Kadoch, Michel. 2004. *Protocoles et réseaux locaux : l'accès Internet*. Montréal: École de technologie supérieure, xvii, 529 p.

Le petit Larousse illustré 2008. 2007. Paris: Larousse, 1 cédérom p.

Liu, Bin, Chuang Lin, Donghua Ruan et Xuehai Peng. 2006. « Netflow based flow analysis and monitor ». In., p. 4146448. Coll. « International Conference on Communication Technology Proceedings, ICCT ». Guilin, China: Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ 08855-1331, United States. <http://dx.doi.org/10.1109/ICCT.2006.341847>.

Muuss, M.J. 1993. *The Story of the PING Program*. <http://ftp.arl.army.mil/~mike/ping.html>.

Muuss, Mike. 1983. *Ping Program*. <http://ftp.arl.mil/~mike/ping.html>.

Net-SNMP. mars 2007. *NET-SNMP 5.4.2*. <http://www.net-snmp.org/>.

NfSen - Netflow Sensor. <http://nfsen.sourceforge.net/>.

Odom, Wendell., et Michael J. Cavanaugh. 2004. *IP Telephony Self-Study Cisco DQOS Exam Certification Guide*. Coll. « Exam certification guide series. ». Indianapolis, Ind.: Cisco Press.

Oetiker, T. octobre 2008. *MRTG - Multi Routeur Traffic Grapher*. <http://oss.oetiker.ch/mrtg/>.

Oetiker, Tobias. 2008. *About RRDtool*. <http://oss.oetiker.ch/rrdtool/>.

Orebaugh, Angela, Syngress Media Inc. et Books24x7 Inc. 2007. *Wireshark & Ethereal network protocol analyzer toolkit, Jay Beale's open source security series*. Coll. « Jay Beale's open source security series ; [v. 1] ». Rockland, Mass.: Syngress.

Phaal, P., S. Panchen et N. McKee. IETF 2001. « RFC 3176: InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks » <http://www.ietf.org/rfc/rfc3176.txt?number=3176>.

Postel, J. IETF 1980a. « RFC 768: User Datagram Protocol » <http://www.ietf.org/rfc/rfc0768.txt?number=768>.

Postel, J. IETF 1980b. « RFC 793: Transmission Control Protocol » <http://www.ietf.org/rfc/rfc0793.txt?number=0793>.

Postel, J. IETF 1981. « RFC 792: INTERNET CONTROL MESSAGE PROTOCOL » <http://www.ietf.org/rfc/rfc0792.txt?number=792>.

Reynolds, J., et J. Postel. IETF 1980. « RFC 0961: OFFICIAL ARPA-INTERNET PROTOCOLS ». <http://www.ietf.org/rfc/rfc0961.txt?number=0961>.

Schemers, Roland. 2002. « fping ». <http://fping.sourceforge.net/index.html>.

Seagren, Eric, et Books24x7 Inc. 2007. *Secure your network for free using Nmap, Wireshark, Snort, Nessus, and MRTG*. Rockland, Mass.: Syngress.

Simoneau, Paul. 1999. *SNMP network management*. New York, N.Y.: McGraw-Hill, xvi, 447 p.

SMI Network Management Private Enterprise Codes: . Octobre 2008. <http://www.iana.org/assignments/enterprise-numbers>.

Stallings, William. 1999. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd. Reading, Mass.: Addison-Wesley, xiv, 619 p.

Welcher, Peter J. 2005. « NetFlow and IPFIX » <http://www.netcraftsmen.net/welcher/papers/netflow02.html>.

Williams, Hugh E., et David Lane. 2004. *Web database applications with PHP & MySQL*, 2nd. Sebastopol, Calif.: O'Reilly, xviii, 796 p.