MINISTERE DE L'ENSEIGNEMENT SUPERIEURET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DEL'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master en Électronique
Option : Réseaux et Télécommunications

Thème:

Monitoring des performances et des incidents d'un réseau IP d'un opérateur mobile

Proposé par :
M^r^ SAGHIR Moncef

Réalisé par :
Mr HAMOUNI Sofiane
Melle BOUDJELI Farida

Dirigé par:
M^me^ HEMDANI Naima

2013/2014

Remerciements

Nous tenons à exprimer nos reconnaissancesà Madame. HEMDANI,pour son encouragement et encadrement. Nous tenons aussi à remercier infiniment M.MONCEF SAGHIR qui a accepté de diriger nous travaux tout au long de notre stage à WATANIYA TELECOM ALGERIE(Ooredoo), et qui nous ont toujourssoutenu et fourni l'aide nécessaire afin de pouvoir réaliser nos objectifs dans les meilleures conditions.

Nous souhaitons par ailleurs souligner la contribution importante de l'équipe du département Data Netwoking, particulièrementMr. HASSANI, Mr. KORAICHI, et Mr. MONCHINI , Mr AMROUCHE et Mr AOUCHICHEet chef de serviceTechnologie , l'expertise de cette équipe a toujours été d'un précieux recours.

Noustenonsà remercier également nos familles et nos amis qui nous ont soutenus, et particulièrement HAMOUNI. M et SALAH. S ettous ceux qui nous ont aidé de près ou de loin à réaliser ce modeste travail.

Merci.

DEDiCACES

Nous dédions ce modeste travail :

A Nos très chers parents et grands-parents qui nous ont soutenus tout au long de nos études et qui ont contribué à notre réussite, que dieu les garde et leur donne une longue vie afin que nous puissions leurs faire du bien à notre tour, et les rendre fières.

A Nos grands parents, et à toutes notre famille.

A Nos Frères et sœurs, et à toutes notre famille

A tous nos amis : H.Said, B.Chabane,T.Hayet,H.Mohammed,B.Naima,B.Said et H.Djouher.

CHAPITRE 1

Organisme d'accueil

CHAPITRE 2

Etudes des composants du réseau : Juniper, Ericsson, Cisco et Extreme

CHAPITRE 3

Topologie d'un réseau à superviser

CHAPITRE 4

Simple Network Management Protocol (SNMP)

CHAPITRE 5

Manager SNMP

(Applications de supervision)

Annexe A

Annexe B

Introduction générale

Conclusion générale

Sommaire

Bibliographie

Listes des figures et des tableaux

Liste des figures :

Liste des tableaux :

Sommaire

Introduction générale

Introduction générale

Le réseau informatique est devenu une ressource indispensable voir vitale au bon fonctionnement d'une organisation, ou bien d'une entreprise. Toute entreprise, même modeste possède son propre réseau informatique avec plus ou moins de machines.

Une machine informatique, quelle que soit sa fonction, a généralement beaucoup de tâches à réaliser. Elle le fait le plus souvent discrètement que peu de ses utilisateurs le savent, sauf lorsqu'elle se plante ou devienne extrêmement lente. Bien que la plupart du temps, elle nous communique des informations comme la température du processeur, l'état des disques qu'elle enregistre dans des fichiers log, ….

Les administrateurs sont vraiment les seuls à s'intéresser à ces informations, pourtant cruciales au bon fonctionnement de certain logiciels et système d'exploitation. Et comme les parcs informatiques sont composés d'un grand nombre de machine, l'administrateur n'a pas le temps de vérifier chacune des machines pour consulter ces informations. Il serait donc agréable pour l'administrateur de récupérer ces informations à distance et de pouvoir modifier certains paramètres à distance. D'où l'appellation de la supervision réseaux.

Le département NETWORKING de l'entreprise WATANIYA TELECOM ALGERIE souhaiterait superviser ses réseaux via une interface graphique sécurisée. Aucun intrus ne doit pouvoir y'accéder à cette interface, elle devra donc être protégée par un mot de passe. L'interface devra donc comporter une cartographie du réseau, présentant les différents équipements (les serveurs, les routeurs et les switchs). Cette cartographie devra explicitement décrire l'état de ces équipements et permettre d'identifier l'état des ports des commutateurs de ses machines. Des renseignements supplémentaires sur les différentes machines (charge CPU, espace disque, mémoire disponible, etc.) pourront être renseignés. Enfin, lorsque des problèmes surviendront, l'administrateur devra être notifié par un courriel dont le contenu indiquera le service et/ou la machine défectueuse.

C'est donc le but de notre projet, de trouver une solution optimale et facile à utiliser spécialement pour la gestion des serveurs, routeurs, switch et le monitoring de ses équipements en premier lieu. Et, offrir la possibilité de devenir proactif face aux problèmes rencontres en un second lieu, le plus important est de pouvoir détecter et interpréter en un

simple coup d'œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.

Nous avons scindé ce travail en cinq chapitres ; dont

- Dans le premier chapitre nous avons présentés l' organisme d'accueil et l'architecture du réseau de cette entreprise, en nous basant plus sur notre champ d'études qu'est le département NETWORKING ou le fait de se constituer un réseau de relations et de savoir en tirer parti, notamment dans un but professionnel, d'où nous extrayons le problème de notre projet.
- Dans le second chapitre on a effectués une étude des composants du réseau

(Juniper, Ericsson, Cisco et Extreme) qui constitue le réseau Wataniya Telecom Algérie.

- Dans le troisième chapitre on a démontres la Topologie employé dans le réseau a supervisé et de présenter le principe général d'administration réseau.
- Dans le quatrième chapitre nous avons vue l'importance du protocole SNMP, qui est ainsi le standard incontournable dans le domaine de l'administration de réseaux
- Dans le cinquième et dernier chapitre, nous avons présentés les spécifications de notre solution, l'étude conceptuelle de cette application, ainsi que la description de l'implémentation et les tests de notre application sur une plateforme.

En fin, nous terminerons par une conclusion générale et quelques perspectives.

CHAPITRE 1

Organisme d'accueil

CHAPITRE I. ORGANISME D'ACCUEIL

Historique :

WATANIYA TELECOM ALGERIE (WTA) a été mise en place par la société koweïtienne Wataniya Telecom, à laquelle s'est jointe United Gulf Bank (UGB). Dotée d'une licence d'une durée de 15 ans, WTA a adopté un programme d'investissements accéléré comportant des projets de 1 milliard de dollars US sur trois ans. Grâce à ces investissements, Nedjma se taille la place de leader de l'innovation et de la plus-value : elle rend la technologie multimédia accessible à tous et facile à utiliser.

Wataniya Telecom, l'opérateur de référence WTA, a été fondée en 1999 au Koweït. Il fait partie des sociétés de KoweIt Projects COmpany (KIPCO), la plus importante entreprise privée du Koweït avec un actif de plus de 10 milliards USD. Wataniya Telecom a connu une croissance fulgurante dans l'univers des télécommunications sans fil au Moyen-Orient et en Afrique du Nord. En mars 2007, Qtel devient actionnaire majoritaire (51%) de Wataniya Telecom Kuweit et détient par conséquent 80% de Nedjma.

C'est lors d'une conférence de presse organisée, le mardi 12 novembre 2013 à l'hôtel Sheraton du Club des Pins que le directeur général de Nedjma, Joseph Ged a annoncé le changement officiel de son identité commerciale et visuelle en adoptant le nouveau nom Ooredoo (le nom de la marque traduit de l'arabe signifie «je veux»). Il a également indiqué que le transfert de la marque de Nedjma vers Ooredoo s'effectuera dans la continuité sous le slogan de « Dima Maakoum » et que le lancement de la nouvelle marque coïncide avec la mise en service de la 3G.

I. Présentation de Wataniya Télécom Algérie :

Les investissements de l'opérateur de téléphonie mobile (Ooredoo) en Algérie ont atteint 485,5 millions de dollars US en 2013, contre 226 millions de dollars US en 2012, selon un bilan rendu public par la filiale algérienne du groupe qatari.
Ce volume représente 19% des investissements globaux de la maison mère qatarie Ooredoo, selon un communiqué de l'opérateur de téléphonie mobile.

Le bénéfice net de la filiale algérienne s'est chiffré à 201,4 millions de dollars US en 2013, contre 98,7 millions de dollars l'année précédente, soit une progression de plus que le double, selon la même source.

En 2013, les revenus d'Ooredoo ont atteint 1,06 milliard de dollars, contre 955,4 millions de dollars en 2012, soit une augmentation de 15%. Le nombre d'abonnés de l'opérateur s'est établi au 4ème trimestre 2013 à 9,5 millions, en hausse de 200.000 abonnés par rapport au 3ème trimestre.

Elle détient 32% des parts de marché de la téléphonie mobile en Algérie, selon la même source.
Ooredoo est le premier investisseur dans le secteur des télécommunications en Algérie pour la quatrième année consécutive, selon le communiqué.

Ooredoo, détenu principalement par le qatari Qtel, avait obtenu une licence d'exploitation de la téléphonie mobile en Algérie en décembre 2003 suite à une offre de 421 millions de dollars. Mais, ce n'est qu'en août 2004 qu'elle avait procédé au lancement commercial de sa marque,

ces numéros téléphoniques commencent par l'indicatif 05 xx xx xx xx ce qui donne un numéro de téléphone à 10 chiffres.

Logo de 2004 à 2009

Logo de 2010 à 2013

Logo actuel

II. Qualité de service :

Ooredoo offre aux utilisateurs algériens un nouveau monde en matière de télécommunications mobiles. En effet, Ooredoo met au service de la clientèle algérienne non seulement des produits et services innovateurs, mais aussi une haute qualité de transmission grâce à des équipements issus des technologies les plus récentes, un service à la clientèle basé sur les standards les plus élevés et une politique de prix hautement concurrentielle.

III. Réseau :

Le réseau Ooredoo a été déployé dans des délais record pour offrir aux consommateurs algériens des communications de qualité exceptionnelle en émission et en réception.

Ooredoo utilise le réseau GSM sur les fréquences 900/1800 et le réseau GPRS/EDGE pour les applications de données. D'après l'autorité de régulation de la poste et des télécommunications(ARPT), le réseau Ooredoo couvre 99% des chefs-lieux des wilayas, et plus de 95% des agglomérations et routes nationales.

Au 15 décembre, Nedjma devenue Ooredoo procède au lancement commercial de son réseau 3G HSPA+ après autorisation de l'ARPT, sous le label 3G++ et simultanément avec l'opérateur national Mobilis couvrant ainsi 10 wilayas au premier jour de lancement, en l'occurrence, Alger, Oran, Ouargla, Constantine, Sétif, Djelfa et en exclusivité à Béjaïa, Chlef, Bouira et Ghardaïa.

Le déploiement se poursuivra plus tard à Boumerdès, Blida, Tipasa, Tlemcen, Sidi Bel Abbès, Aïn Defla et Biskra et El Oued et en exclusivité Médéa. L'opérateur envisage de couvrir d'ici la fin 2014, 25 wilayas représentant 80% de la population.

IV. Espaces Ooredoo :

Ooredoo vise à être plus près de ses clients grâce à ses espaces commerciaux, où ces derniers peuvent configurer leurs mobiles, régler leurs factures ainsi que tout problème avec leurs lignes, l'Espace propose également des packs et des mobiles. L'opérateur totalise aujourd'hui près de 308 Espaces Ooredoo opérationnels à travers le territoire national.

V. Organigramme :

L'environnement interne de Wataniya est composé de différentes directions qui se schématisent dans l'organigramme suivant :

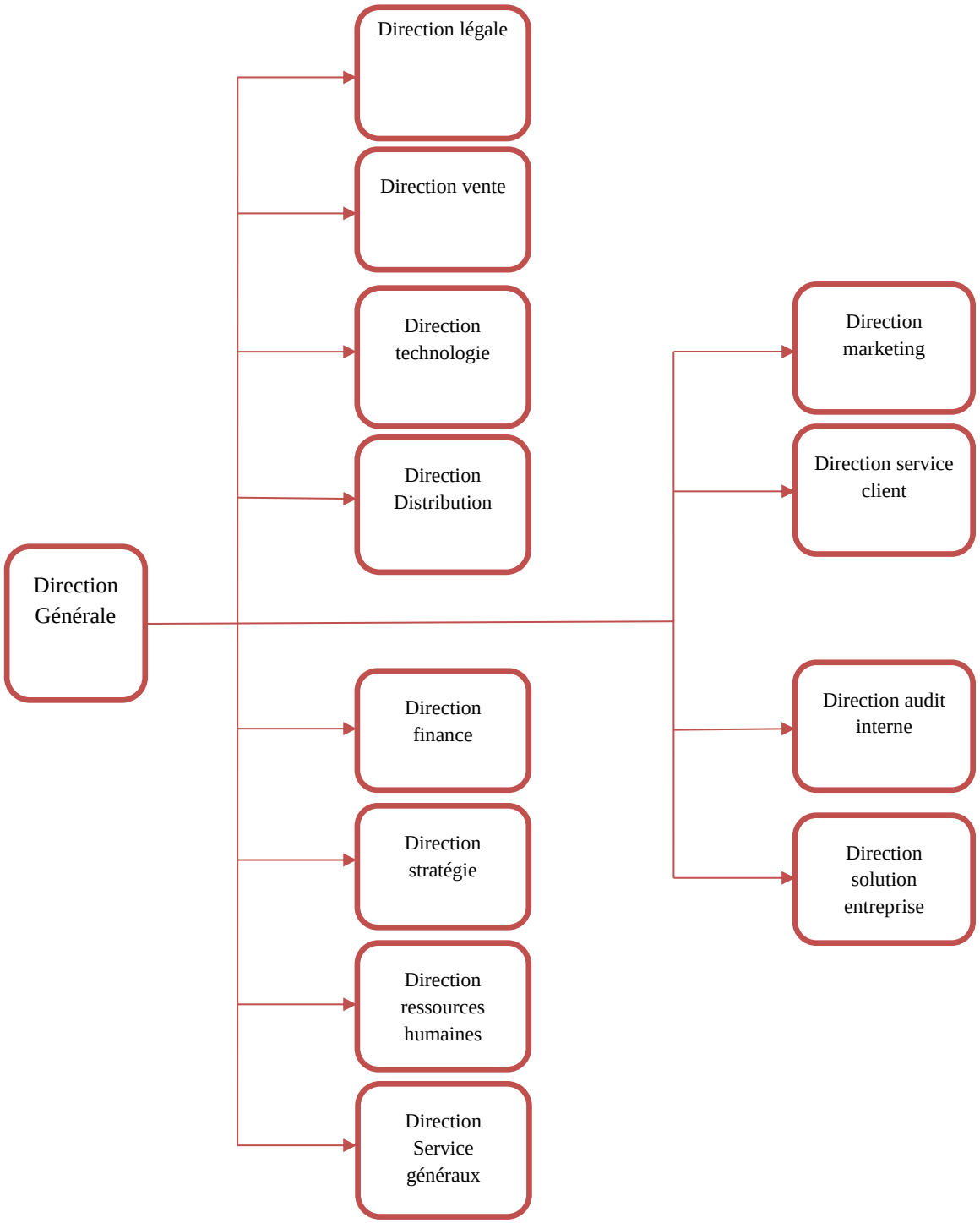


Figure I.1 : Organigramme Wataniya Telecom Algérie

Nous avons effectuées notre stage dans la direction technologie qui se compose de :

- **OSS** (Operations Support System) c'est l'ensemble des composants opérationnels où les systèmes informatiques utilisés par un opérateur de télécommunications. Elle est synonyme de maintenance opérationnelle dans le domaine des télécommunications.

  Le terme OSS est habituellement synonyme de systèmes de réseaux informatiques qui comprennent : le réseau de télécommunications lui-même et le maintien des processus tels que la maintenance du réseau.
- **NMS:** (Network Management Station) est une machine de management d'un réseau informatique**.**
- **NSS** (Network Switching Subsyste) une partie du système de réseau GSM.
- **GPRS**(General Packet Radio Service) est une norme pour la téléphonie mobile dérivée du GSM et complémentaire de celui-ci, permettant un débit de données plus élevé. On le qualifie souvent de 2,5G. Le G est l'abréviation de génération et le 2,5 indique que c'est une technologie à mi-chemin entre le GSM (2è^{me} génération) et l'UMTS (3ème génération).
- **TRANSMISSION**: Le terme transmission s'applique à toute émission radioélectrique permettant l'acheminement d'un message d'un émetteur à un récepteur.
- **NETWORKING:** le fait de se constituer un réseau de relations et de savoir en tirer parti, notamment dans un but professionnel.

  Parfois traduit par le néologisme réseautage.
- **BSS** (Base Station Subsystem) partie radio du réseau de téléphonie mobile GSM.
- **ENV:** En informatique, un environnement, désigne pour une application, l'ensemble des matériels et des logiciels système, dont le système d'exploitation, sur lesquels sont exécutés les programmes de l'application.

Conclusion :

Ooredoo est une compagnie internationale leader des télécommunications qui fournit les services de téléphonie mobile, fixe et l'Internet haut débit et les services Entreprise adaptés aux besoins des particuliers et des entreprises.

CHAPITRE 2

Etudes des composants du réseau : Juniper, Ericsson, Cisco et Extreme

CHAPITRE II.

Etudes des composants du réseau :Juniper, Ericsson, Cisco et Extreme

Introduction :

Afin de rependre aux concordances des nouvelles technologies réseaux et satisfaire leurs besoins propres en informatique, les entreprises mettent en œuvre au sein de leurs établissements des réseaux de très hautes performances afin d'offrir une qualité de service optimal pour les abonnés.

Dans notre étude, on s'est focalisé sur la partie qui compose les équipements des nodes MPLS (Multi Protocol Label Switching) du réseau Ooredoo.

Ce dernier compose de trois parties qui sont : La partie Core, partie Primary et la partie Secondary. Chaque partie du réseau a ces propres régions, locations, devise name (nomination exacte) et constructeur d'équipement, comme représenter dans le tableau suivant :

Kind of the Site	*Region*	*Location*	*Device Name*	*Equipement*	*Vendors*
Core	Alger	BabEzzouar	BEZP1	SSR8020	Ericsson
			BEZP2	SSR 8020	Ericsson
	Alger	Birkhadem	BKHP1	SSR 8020	Ericsson
			BKHP2	SSR 8020	Ericsson
Primary	Alger	BabEzzouar	BEZSR1	M120	Juniper
			BEZSR2	M120	Juniper
			BEZSR3	MX960	Juniper
			BEZSR4	MX960	Juniper
			BEZSW1	BD 8806	Extreme
			BEZSW2	BD 8806	Extreme
			BEZFW1	ISG2000	Juniper
			BEZFW2	ISG2000	Juniper
	Alger	Birbkhadem	BKHSR1	M120	Juniper
			BKHSR2	M120	Juniper
			BKHSR3	MX960	Juniper

			BKHSR4	MX960	Juniper
			BKHSW1	BD 8806	Extreme
			BKHSW2	BD 8806	Extreme
			BKHFW1	SSG520	Juniper
			BKHFW2	SSG520	Juniper
	Constantine	Constantine	CONSR1	M120	Juniper
			CONSR2	M120	Juniper
			CONSW1	BD 8806	Extreme
			CONSW2	BD 8806	Extreme
			CONFW1	SSG520	Juniper
			CONFW2	SSG520	Juniper
	Oran	Oran	ORASR1	M120	Juniper
			ORASR2	M120	Juniper
			ORASW1	BD 8806	Extreme
			ORASW2	BD 8806	Extreme
			ORAFW1	SSG520	Juniper
			ORAFW2	SSG520	Juniper
	TiziOuzou	TiziOuzou	TIZISR1	SE600	Ericsson
			TIZISR2	SE600	Ericsson
			TIZISW1	BD 8806	Extreme
			TIZISW2	BD 8806	Extreme
Secondary	Annaba	Annaba	ANNSR1	SE600	Ericsson
			ANNSR2	SE600	Ericsson
			ANNSW1	SummitX460	Extreme
			ANNSW2	SummitX460	Extreme
	Blida	Blida	BLISR1	SE600	Ericsson
			BLISR2	SE600	Ericsson
			BLISW1	SummitX460	Extreme
			BLISW2	SummitX460	Extreme
	Alger	Baraki	BRKSR1	SE600	Ericsson
			BRKSR2	SE600	Ericsson
			BRKSW1	SummitX460	Extreme
			BRKSW2	SummitX460	Extreme
	Alger	Bouzareah	BZHSR1	SE600	Ericsson
			BZHSR2	SE600	Ericsson
			BZHSW1	SummitX460	Extreme
			BZHSW2	SummitX460	Extreme
	Alger	Ouled fayet	OULSR1	SE600	Ericsson
			OULSR2	SE600	Ericsson
			OULSW1	SummitX460	Ericsson
			OULSW2	SummitX460	Extreme
	Alger	Rouiba	RBASR1	SE600	Ericsson

			RBASR2	SE600	Ericsson
			RBASW1	SummitX460	Extreme
			RBASW2	SummitX460	Extreme
	Boumerdès	Boumerdès	BMDSR1	SE600	Ericsson
			BMDSR2	SE600	Ericsson
			BMDSW1	SummitX460	Extreme
			BMDSW2	SummitX460	Extreme
	Setif	Setif	SETSR1	SE600	Ericsson
			SETSR2	SE600	Ericsson
			SETSW1	SummitX460	Extreme
			SETSW2	SummitX460	Extreme
	Alger	Zeralda	ZERSR1	SE600	Ericsson
			ZERSR2	SE600	Ericsson
			ZERSW1	SummitX460	Extreme
			ZERSW2	SummitX460	Extreme
	Tlemcen	Tlemcen	TLMSR1	7606	Cisco
			TLMSR2	7606	Cisco
	Chlef	Chlef	CHLSR1	7606	Cisco
			CHLSR2	7606	Cisco

Tableau II.1 : Tableau représentant les nodes MPLS

Commençons par la première partie qui est :

- Partie Core : elle est constituée de quatre routeurs Ericsson SSR8020 qui sont reparties dans deux locations différentes qui sont : BabEzzouar (2 routeurs) et Birkhadem (2 routeurs) qui sont dans la région d'Alger.
- Partie Primary : la partie primary se compose de seize routeurs, dix Switch et six Firewall de marque d'équipements différentes (Ericsson, Juniper et Extreme) qui sont reparties dans des régions différentes qui sont à leurs tour départagés dans des locations différentes (BabEzzouar, Birkhadem, Tizi_Ouzou, Constantine et Oran).

- Partie Secondary : la partie Secondary se constitue de vingt-deux routeurs et dix-huit switch de marque d'équipements différentes (Ericsson , Cisco et Extreme) qui sont reparties dans des régions différentes qui sont à leurs tour départagés dans des location différentes (Annaba, Blida, Alger Boumerdes , Stif, Chlef et Tlemcen).

→ Voici la représentation du tableau ci-dessus en topologie :

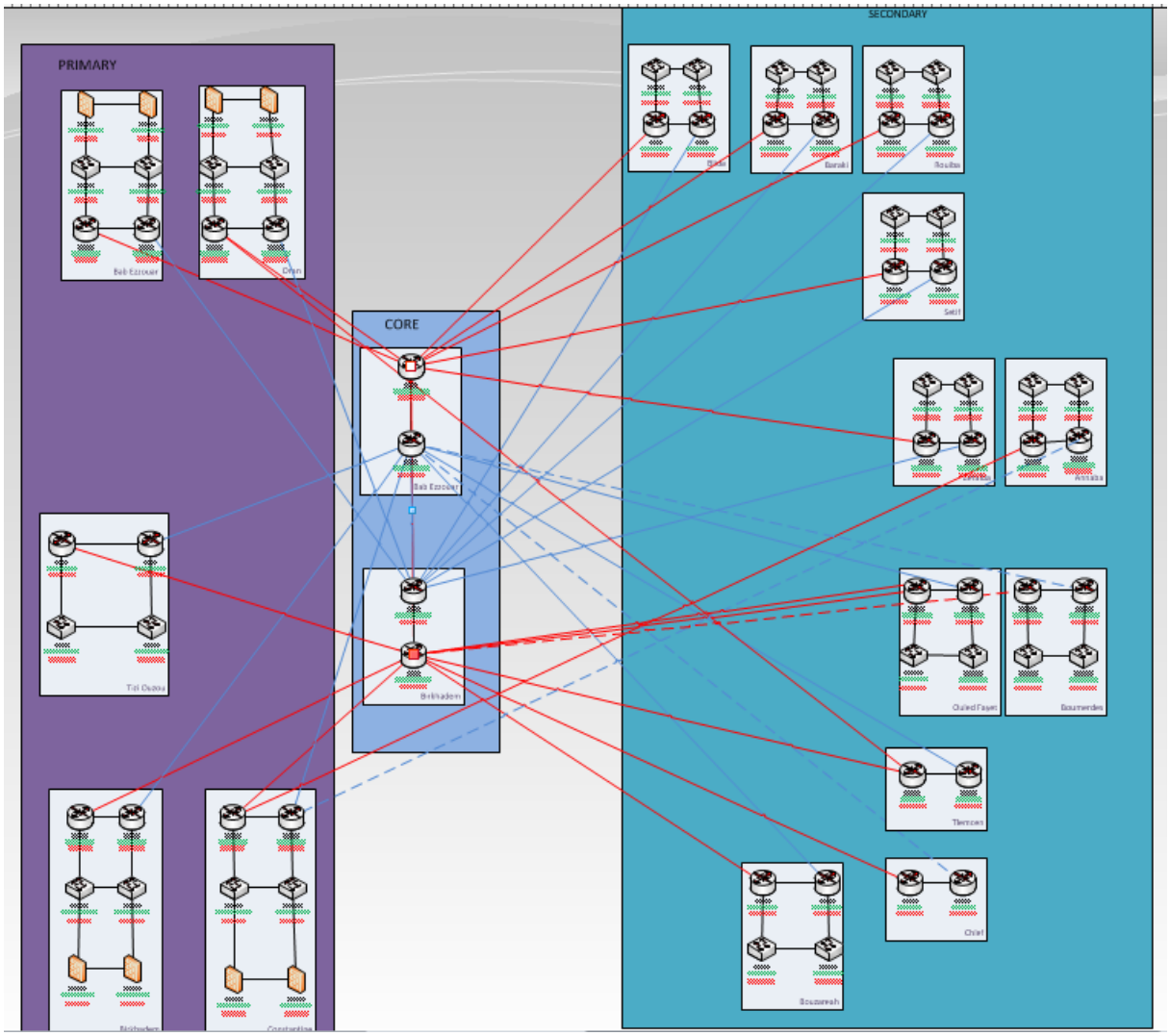


Figure II.1 : Topologie des nodes MPLS.

Voici un zoom sur une partie du site Core et une partie du site Primary :

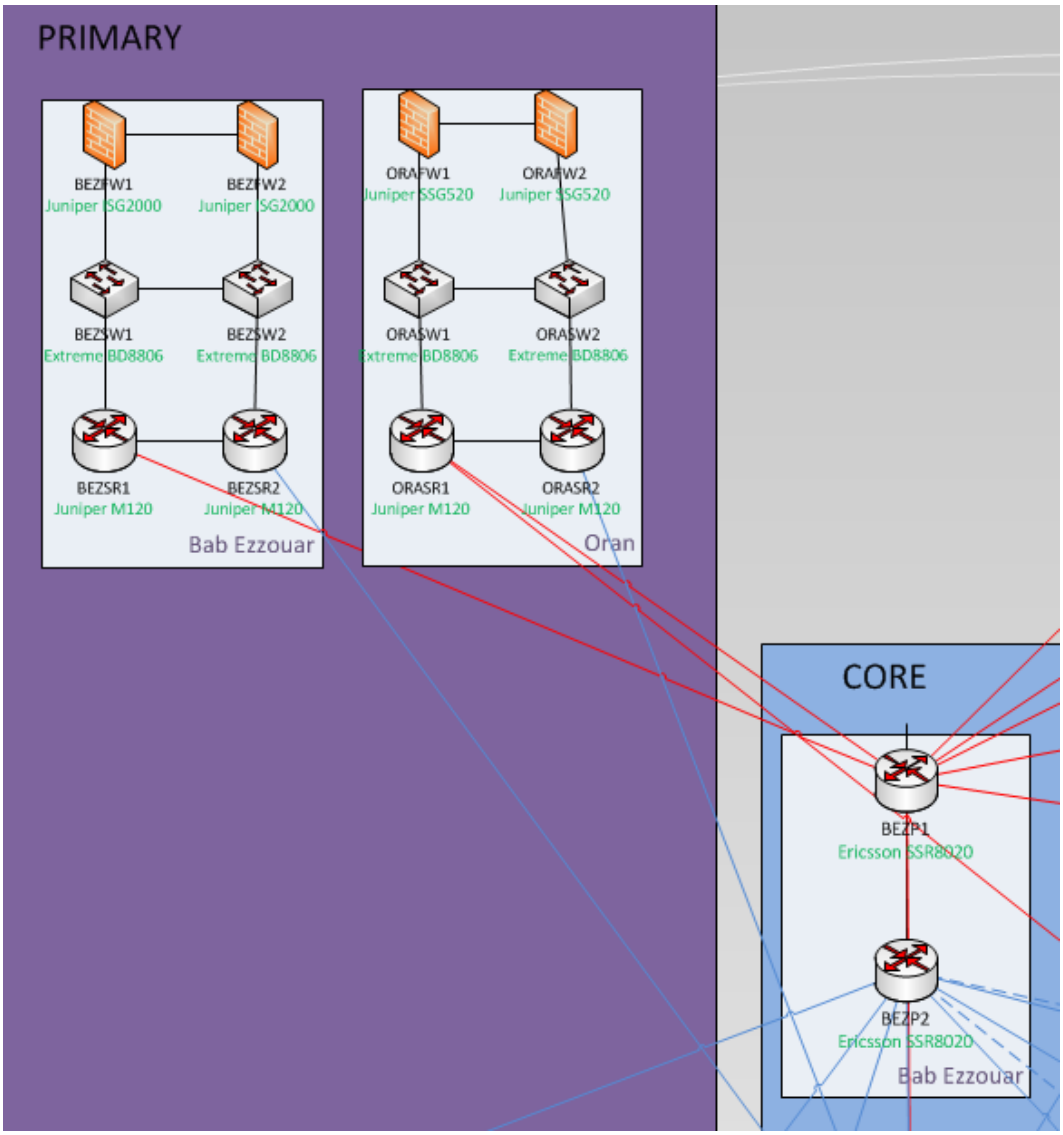


Figure II.2 :Zoom sur une partie des Nodes MPLS.

→ Cette topologie utilise des liaisons à fibre optique.

→ On remarque sur la topologie du réseau les sites (Birkhadem, Constantine, Oran et Bab Ezzouar) ont tous des Firewalls (pare feux) de marque d'équipements de noms et d'adresses IP différentes.

→ La topologie employée utilise la redondance pour minimiser le taux de panne.

→ On a deux sites les plus importants de ce réseau qui se situent dans la partie Core qui sont : Bab Ezzouar et BirKhadem

Les composants du réseau que nous allons étudiés sont les suivants:

II.1.Les routeurs :

Alors, c'est quoi un routeur ? Comment ça marche ?

II.1.1.Définition :

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Lorsqu'un utilisateur appelle une URL, le client Web (navigateur) interroge le server de noms, qui lui indique en routeur l'adresse IP de la machine visée. Son poste de travail envoie la requête au routeur le plus proche, c'est-à-dire à la passerelle par défaut du réseau sur lequel il se trouve. Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.
Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche. En plus de leur fonction de routage, les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre. Or, dans la mesure où les réseaux n'ont pas les mêmes capacités en termes de taille de paquets de données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.
C'est un équipement de couche 3 par rapport au modèle OSI. Il ne doit pas être confondu avec un commutateur qui est de couche 2.

II.1.2. Aspect d'un routeur :

Les premiers routeurs étaient de simples ordinateurs ayant plusieurs cartes réseau, dont chacune était reliée à un réseau différent. Les routeurs actuels, destinés aux PME, sont pour la plupart des matériels dédiés à la tâche de routage.

Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Un routeur possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté.

II.1.3. Fonctionnement d'un routeur :

Si le routeur reçoit des paquets en provenance du réseau A, il va tout simplement diriger les paquets sur le réseau B...

Toutefois, sur Internet le schéma est beaucoup plus compliqué pour les raisons suivantes, le nombre de réseaux auquel un routeur est connecté est généralement important, et les réseaux auquel le routeur est relié peuvent être reliés à d'autres réseaux que le routeur ne connaît pas directement.

Les routeurs fonctionnent donc grâce à des tables de routage et des protocoles de routage.

- ✓ **Sa fonction** :

*Contrairement aux ponts, les routeurs doivent être configurés.

*Ils doivent connaitre les adresses des routeurs ou des stations vers lesquels ils envoient les paquets.

II.1.4. Protocoles routés / de routage :

- Les protocoles routés (routables) sont des protocoles prenant en charge les fonctions de la couche réseau (IP, IPX, AppleTalk).

- Les protocoles de routages fournissent les mécanismes de partage et de gestion des tables de routage entre les routeurs (RIP, IGRP, EIGRP, OSPF).

II.1.5. La table de routage :

Pour afficher la table de routage d'une station ou d'un routeur, on utilise la plate-forme dotée d'un système Windows.

L'accès au server, se fait en lançant l'invite de commande (Démarrer->Exécuter->cmd) et ensuite de taper *root print*.

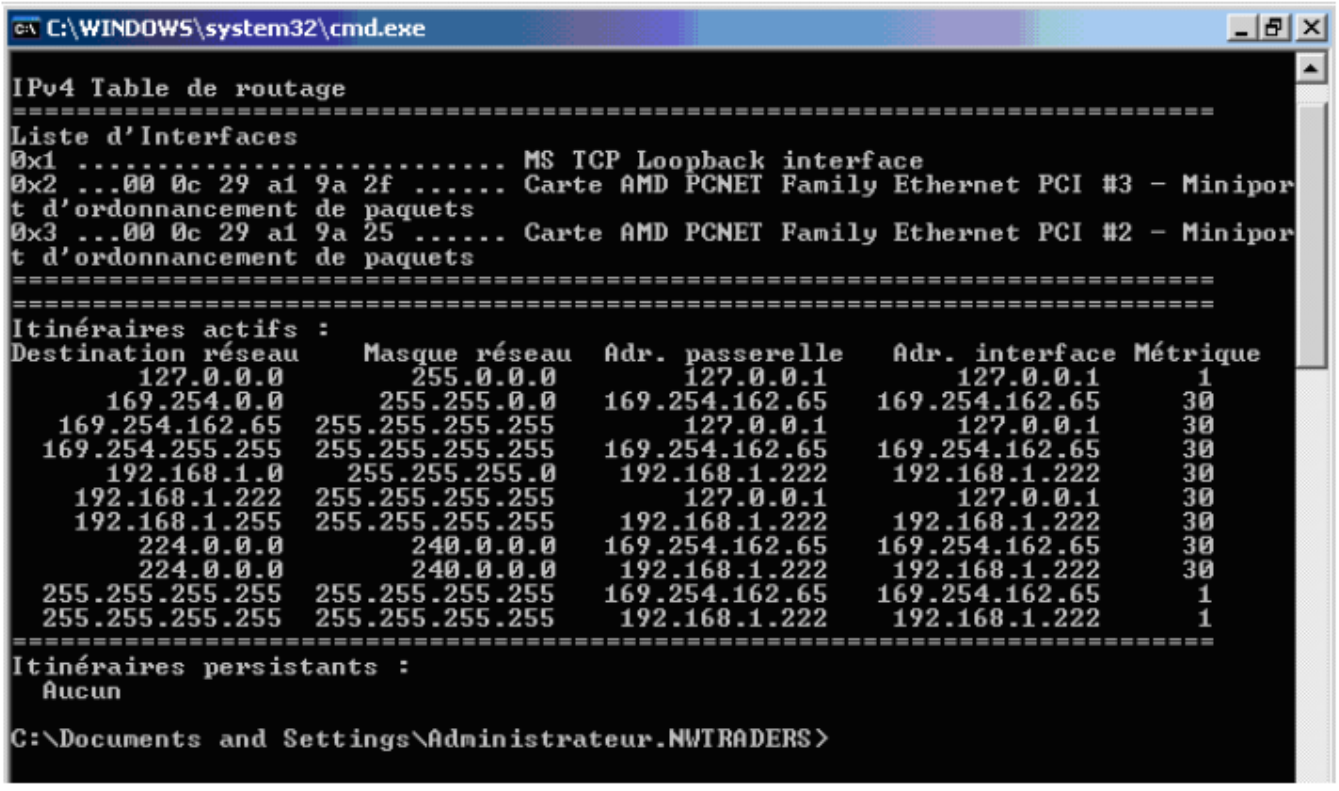


Figure II.3 : Table de routage

La table de routage regroupe trois types d'entrées :

- ✓ Itinéraire réseau : Il s'agit d'un chemin indiquant l'interface réseau, c'est-à-dire, le dispositif permettant l'acheminement des paquets, afin de joindre un autre réseau.
- ✓ Itinéraire hôte : C'est un chemin personnalisé (dispositif administrable à distance, comme un serveur par exemple) permettant de contrôler et optimiser le trafic réseau.
- ✓ Itinéraire par défaut : Il s'agit du chemin définit pour l'acheminement par défaut des paquets d'informations, notamment lorsque ces derniers n'arrivent pas à emprunter un chemin donné.

On observe qu'au sein de la table de routage, plusieurs informations apparaissent, notamment cinq colonnes qui affichent les informations sur les entrées par défaut de la table :

*Destination réseau : Affiche l'adresse IP des réseaux de destination.

*Masque réseau : Indique le masque de sous réseau utilisé sur le réseau de destination et associé à ce dernier.

*Adresse passerelle : Représente l'adresse de l'élément arbitraire le plus proche, c'est-à-dire, l'adresse de routeur qui sera traversée par le paquet avant d'atteindre sa destination. Il s'agit là d'une adresse qui doit nécessairement être accessible par le routeur.

*Métrique : Représente en quelque sorte, une échelle de mesure. En effet, il s'agira de l'élément qui permettra au routeur de « décider » de choisir une route plutôt qu'une autre. Plus cet indice est faible, plus la route semblera fiable pour le routeur.

Il semble nécessaire de préciser que l'espace de stockage de la table de routage est une mémoire de type RAM (Random Access Memory), c'est-à-dire, une mémoire qui est vidée à chaque redémarrage du système.

II.2. Les différents constructeurs de l’équipement Routeur :

Nous allons étudier trois différent modèle de Router de marque déférentes.

II.2.1. Le constructeur Ericsson SSR (Smart Service Router) :

La figure ci-dessous nous presente le modele du constructeur Ericsson :

Figure II.4 :Routeur Ericsson

II.2.1. 1.Le routeur Ericsson SSR 8000 :

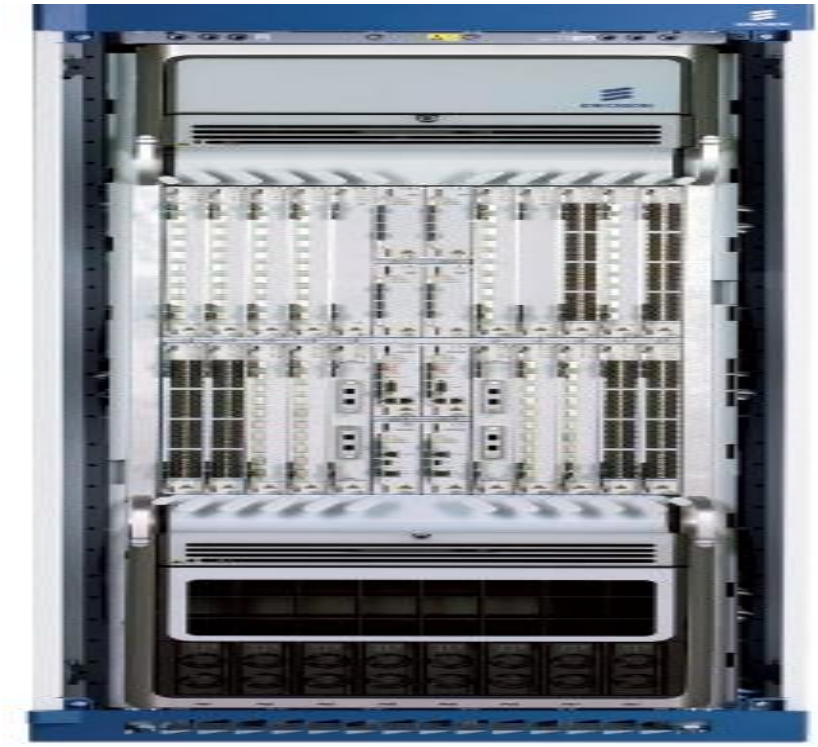


Figure II.5 : Routeur Ericsson SSR8000

Les routeurs Ericsson SSR 8000 est une famille de Routeurs de Services Intelligents, fournit aux opérateurs une plate-forme fortement évolutive, consolidée qui offre des services pour l'infrastructure de réseau tant fixe que mobile. Il offre des services comme le cheminement de bord IP/MPLS et des fonctionnalités de Passerelle de Paquet Développées. Le Routeur de Services Intelligent permet la convergence de réseau complète donc les abonnés peuvent avoir accès aux services de dispositifs ou emplacements.

Actionné par le Processeur de Réseau Intelligent 4000 (SNP 4000), le premier processeur C-programmable de l'industrie exécutant Linux inchangé, le Routeur de Services Intelligent est

une vraie plate-forme multi-application qui livre la Couche 2 à la Couche 7 services avec la performance prévisible.

II.2.1.2.Description :

Avec une capacité de carte mère de 16 TByte/S et un non-blocage commutant le tissu, un Routeur de Services Intelligent peut peser aux besoins de bande passante (de largeur de bande) de même les demandes (applications) les plus exigeantes, en protégeant la bande passante basse (la largeur de bande basse), des demandes de latence basse de devenir évincé. L'État de l'art signalant des capacités d'adresses au contrôle croissant au-dessus qui vient avec un nombre toujours croissant de dispositifs d'utilisateur final connectés. Une variété de fonctions de réseau, la gestion d'abonné s'étendant d'un contrôle de politique et le support de mobilité permet une introduction rapide et simple de nouveaux services d'utilisateur final, l'expérience d'utilisateur final maximale et l'utilisation optimale de ressources de réseau. La disponibilité sophistiquée et des capacités de résistance (d'élasticité), englobant tant le matériel (la quincaillerie) que le logiciel, minimisent la probabilité et le potentiel.

II.2.1. 3.Des fondations solides :

Pour le routeur c'est la croissance des services intelligents qui est donc le moyen approprié pour les opérateurs de réseaux pour lutter contre un trafic de plus en plus volumineux, et une diversité sans cesse croissante des applications et dispositifs d'utilisateur final. Il s'adapte aux sans précédents le débit et les capacités de signalisation. Il a les Smartphones (intelligents) afin d'optimiser l'expérience de l'utilisateur final compte tenu des ressources limitées.

Il simplifie la gestion du réseau pour minimiser les dépenses de fonctionnement. Et il fournit la résilience qui garantit un fonctionnement robuste dans toutes circonstances.

- nous s'intéresserons plus précisément au plus récent produit de cette famille qui est :

→ Le routeur Ericsson SSR8020 :

Le SSR 8020 fournit vingt fentes pour des cartes de ligne et Cartes de Services Intelligentes et huit fentes pour cartes de tissu d'échange.

*Les cartes de tissu d'échange pour le Routeur de Services Intelligent supportent :

*La commutation de tissu avec 500 Gbps plein-duplex.

*Les cartes de ligne viennent jusqu'à 40 ports chacune.

*Les cartes de Services sont disponibles avec un portefeuille complet de fonctions de réseau.

* la Mobilité supportent, y compris :

- Ericsson leader mondial 3G et des technologies de réseau d'évolution à long terme.

- la gestion des abonnés, fourniture du haut débit fonctions de passerelle de réseau telles que l'authentification, autorisation et de compatibilité, le contrôle d'admission; et l'hôte et la configuration d'adresse.

- Contrôle de la politique basée sur le célèbre service de contrôle-Aware d'Ericsson et de la solution de charge, ce qui permet la définition des politiques souples et politique fiable.

* l'application par le biais de haute performance deep packet l'inspection.

- Les services voix et multimédia sur la base des IP Multimedia sous-système, y compris une capacité de transcode contenu pour la livraison adapté au dispositif de l'utilisateur final.

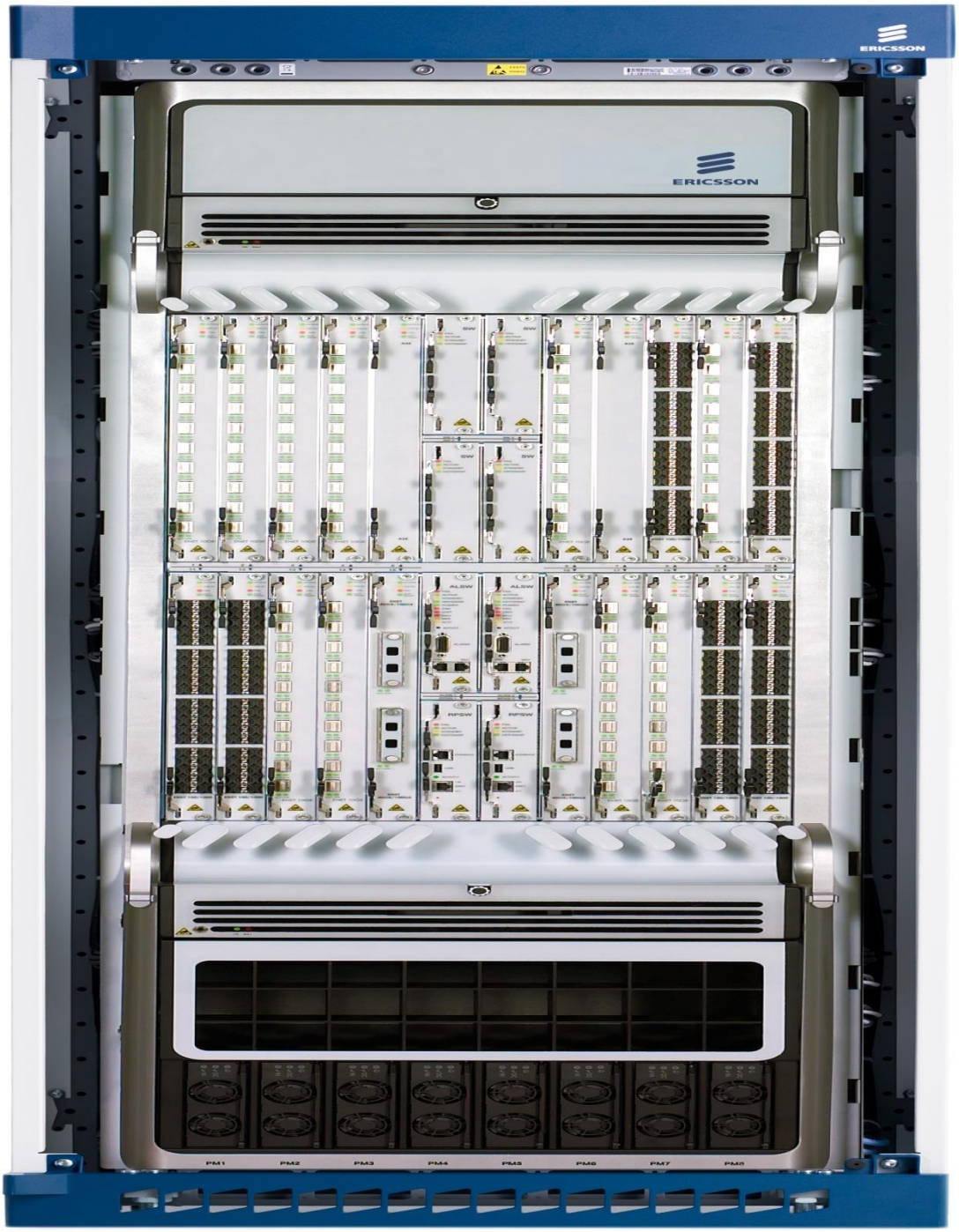


Figure II.6 : Routeur Ericsson SSR8020

II.2.2.La famille des routeurs Ericsson SE :

Le SmartEdge Multi-Service bord Router (MSER) famille primée unifie plusieurs ensembles de fonctionnalités dans une plate-forme unique multi-fonctionnel qui comprend routage de périphérie, l'agrégation Ethernet, gestion des abonnés, et des services de pointe. Ces services sont offerts avec une fiabilité de classe opérateur, d'évolutivité et de performance. La famille MSER de produits a également l'alimentation électrique minimale.

Certaines des principales caractéristiques comprennent:

*Soutien à une gamme complète de protocoles de passerelle de routage intérieurs, extérieurs et de haute performance de routage multicast avec une performance prévisible et durable. Convient pour déploiement en scrutant, applications bord agrégation et services de routage où le routage IP à haute performance est une exigence absolue.

*Rend la gestion avancée du trafic avec une qualité de service hiérarchique.

*le lissage du trafic global, et la gestion des abonnés Peut être relié directement à une couche d'accès au réseau, par exemple un DSLAM (Digital Subscriber Line Access Multiplexer). Ceci élimine les couches du réseau inutiles et réduit la complexité.

*Prise en charge de 256 000 abonnés par périphérique physique à l'aide de toutes les méthodes de l'abonné encapsulation pour les clients DHCP ou IP d'accès.

Figure II.7 : Famille des routeurs Ericsson SE

-Nous nous intéresserons plus précisément au plus récent produit de cette famille qui est le routeur Ericsson SE600.

➢ II.2.2.1.Le routeur Ericsson SE600 :

Figure II.8 : Le routeur Ericsson SE600

Le SmartEdge 600 (MSER) consolide et simplifie la périphérie du réseau, permettant aux opérateurs de s'adapter plus à la bande passante, le trafic et les abonnés ; il est idéal pour le déploiement des réseaux d'accès à grand débit.

Et d'autres services avancés et sur une seule plateforme compacte.

* Il intègre jusqu'à six applications réseau sur un seul routeur.

* Il est hautement évolutive encore utilise seulement 1/ 6 d'un rack 7 pi.

* Il peut doubler la capacité de support de nouvelles mises à jour vidéo, étendre les services multi-play aux réseaux mobiles à large bande.

* Il prend en charge plus de 1,2 millions d'abonnés dans un rack pour faciliter l'acheminement de l'IPTV (Internet Protocol TéléVision), HDTV (High-Définition TéléVision), le haut débit et la mobilité de mégabits.

Ce nouveau produit repose sur un système d'exploitation très résistant, utilisé dans toutes les plateformes SmartEdge. Il est capable de redémarrage sans à-coups et assure la compatibilité ascendante avec les modèles précédents, ce qui entraîne l'interopérabilité garantie, mise à niveau facile et la réutilisation des ressources actuelles. La plate-forme utilise également les dernières technologies ASIC (Application-Specific Integrated Circuit) conçu en interne par Ericsson pour fournir jusqu'à quatre interfaces 10G par carte de ligne. L'architecture primée élimine point de défaillance unique et prévoit une empreinte beaucoup plus petite par rapport aux plates-formes concurrentes de la même capacité.

Le routeur SE600 Ericsson ouvre la voie à la convergence fixe / mobile en fournissant un point d'IP très fiable de présence pour tous les utilisateurs, indépendamment de la mobilité au sein ou entre les technologies d'accès, permettant un monde où n'importe quel réseau peut fournir un service de n'importe quel appareil connecté.

II.2.3.La famille des routeurs Juniper :

Les M-series sont des routeurs multiservice de bord de réseau (Multiservice Router). Les séries M utilisent des ASIC (Application Specific Integrated Circuit) pour la commutation de paquets. Ils peuvent ainsi servir de terminaux pour de multiples fibres optiques.

Figure II.9 :Routeur Juniper.

- ✓ **La gamme des routeurs M** :

L'historique des routeurs dans la gamme M :

- M40 septembre 1998,
- M20 novembre 1999,
- M160 mars 2000,
- M7i novembre 2003,

En 2007, cette gamme vise les applications suivantes :

- M5 : petit point de présence, gros bureaux,
- M7i : idem et CPE managé,
- M10 : pour des points de présence plus importante, la version M10i offre une redondance des cartes CPU et d'alimentations,
- M20 et M40e : points de présence importants ;

- M120 : Grande performance allant jusqu'à 120 Gb/s et supportant les nouveaux services IP convergés ;
- M160 et M320 : cœurs de réseau internet, ce dernier supportant 320 Gb/s au total.

Tous ces routeurs utilisent le même système d'exploitation (JunOS), ainsi les fonctionnalités sont identiques dans toute la gamme, les services proposés homogènes et les coûts d'exploitation réduits. La différence, réside dans la capacité du fond de panier et du nombre de cartes enfichables.

	RE-400	**RE-850**
CPU	CELERON 400MHz	CELERON 850MHz
Mémoire	256, 512, 768 Mo	1536 Mo
Carte flash	256 Mo (option)	256 Mo (série)
Disque Dur	20/30 Go	20 Go

Tableau II.2 : Tableau représentant les spécifications des cartes enfichables.

Ces cartes peuvent aussi avoir un slot PCMCIA (pour Personal Computer Memory Card International Association), qui ont comme option le Flash.

Nous utiliserons dans notre travail le routeur Juniper M120 :

➢ II.2.3.1.Le routeur Juniper M120 :

Le routeur Juniper M120 Multiservice Edge Router est une plate-forme de 120 Gbits/s à haute redondance, idéale pour la prise en charge d'applications de routage d'extrémités convergentes à large bande passante. Cette plate-forme est conçue pour permettre l'agrégation de services pour les besoins de multi-services des fournisseurs de services et

des utilisateurs dans les entreprises.

Figure II.10 :Le routeur Juniper M120

✓ Les caractéristiques du routeur Juniper M120 :

-Débit semi-duplex avec agrégation : 120 Gbit/s

-Emplacements FPC et débit duplex intégral par emplacement : 4 emplacements FPC, 10Gbits/s

-PIC par châssis : 16

-Châssis par rack : 4

-Redondance : Oui

-Dimensions : * 52,7 x 44,5 x 65,3 cm

*20,75" x 17,5" x 25,7"

-Poids maximal: 104,3kg / 230 lb

-Montage : Façade ou central

-Options d'alimentation :

*Alimentation DC (à pleine charge) : 45 A à - 48 VDC ; 2 150 watts.

*Nb de blocs d'alimentation nécessaires (non redondant/redondant): ½.

*Alimentation en entrée système AC (entièrement chargé): 28 à 14 A ; 100 à 240 VAC ; 47 à 63 Hz ; 2 200 Watts.

*Nb de blocs d'alimentation nécessaires (non redondant/redondant): 1.

II.2.4.La famille routeur Cisco 7600:

La gamme Cisco 7600 est le premier routeur de périphérie de classe opérateur de l'industrie à offrir, la commutation Ethernet à haute densité, de classe transporteur routage IP / MPLS, et des interfaces 10 Gbps intégrés.

Déployer une haute performance IP / MPLS,qui offre ainsi des services IP personnalisées évolutives à la périphérie du réseau, l'amélioration de l'efficacité opérationnelle et optimiser le retour sur des investissements de réseau.

- **Caractéristiques importantes:**

*Haute performance, avec un maximum de 720 Gbps dans un seul châssis, ou 40 Gbps de capacité par fente.

*Un choix de facteurs de forme spécialement conçue pour la haute disponibilité.

*Suite évolutive et extensible de capacités matérielles et logicielles pour permettre aux services Carrier Ethernet intelligents.

* Appel vidéo intégrée de contrôle d'admission à la qualité visuelle innovante de l'expérience à la fois pour la diffusion.

* Services Gateway intelligent, qui propose abonné évolutive et la sensibilisation de l'application avec des capacités d'identité multidimensionnelle et des contrôles de politique.

*Le contrôle des frontières sessions intégrées de la qualité de l'expérience à la fois dans le

Protocole Session Initiated (SIP) et les applications non-SIP.

➢ Applications:

*Carrier Ethernet: Agrégation des consommateurs et des entreprises de service.

*Bord des services Ethernet: services IP personnalisés.

*Convergence des réseaux maillés sans fil et la mobilité de service.

* IP / MPLS bord de prestataire de routage.

*Agrégation Enterprise WAN.

* Siège central de routage.

Figure II.11 :La famille des routeurs Cisco 7600

➢ II.2.4.1.Routeur Cisco 7606S :

Le routeur Cisco 7606 - S est un routeur compact, haute performance conçu dans un 6 -slot facteur de forme pour le déploiement à la périphérie du réseau, où la performance robuste et IP / MPLS de services sont nécessaires pour répondre aux exigences des entreprises et les prestataires de services.

Il permet aux fournisseurs de services Carrier Ethernet pour le déploiement d'une infrastructure de réseau de pointe qui prend en charge une gamme de vidéo IP et le triple-play (voix , vidéo et données) des applications du système dans les marchés des services résidentiels et d'affaires, comme il offre également le WAN ainsi que des solutions de mise en réseau métropolitain régional (MAN) à la périphérie de l'entreprise.

Avec une puissante combinaison de vitesse et de services dans un facteur de forme compact, la gamme Cisco 7606 - S est un excellent choix pour de multiples applications, il répond aussi aux exigences de redondance, de haute disponibilité avec un taux de transfert jusqu'à 240 Mbits distribués et 480 Gbps total.

Le routeur Cisco 7606 – S offre des performances et de la fiabilité avec des options pour les processeurs de route redondantes et des alimentations.

Dans le cadre de la gamme Cisco 7600, le 7606 - S routeur Cisco est une amélioration sur le châssis 6 - slot très réussie (Cisco 7606).

Figure II.12 :Routeur Cisco 7606S

II.3.Les Switch:

II.3.1.Définition:

Le Switch est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique ou de télécommunication et qui permet de créer des circuits virtuels.

II.3.2.Fonctionnement :

Le commutateur établit et met à jour une table. Dans le cas du commutateur pour réseau Ethernet, c'est la table d'adresses MAC qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port. Le commutateur construit donc dynamiquement une table qui associe des adresses MAC avec les ports correspondants.

Lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, le commutateur

renvoie la trame sur le port correspondant. Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise. Si l'adresse du destinataire est inconnue dans la table, alors la trame est traitée comme un broadcast, c'est-à-dire qu'elle est transmise à tous les ports du commutateur à l'exception du port de réception.

Un commutateur de niveau 2 est similaire à un concentrateur dans le sens où il fournit un seul domaine de diffusion. En revanche, chaque port a son propre domaine de collision. Le commutateur utilise la micro-segmentation pour diviser les domaines de collision, un par segment connecté. Ainsi, seules les interfaces réseaux directement connectées par un lien point à point sollicitent le medium. Si le commutateur auquel il est connecté prend en charge le full-duplex, le domaine de collision est éliminé.

II.3.3.Méthodes de transmission :

La transmission des paquets peut s'opérer selon quatre méthodes :

*Mode direct (cut through) : le commutateur lit juste l'adresse du matériel et la transmet telle quelle. Aucune détection d'erreur n'est réalisée avec cette méthode.

*Mode différé (store and forward) : le commutateur met en tampon, et le plus souvent, réalise une opération de somme de contrôle sur chaque trame avant de l'envoyer.

*Fragment free : les paquets sont passés à un débit fixé, permettant de réaliser une détection d'erreur simplifiée. C'est un compromis entre les précédentes méthodes.

*Adaptive switching : est un mode automatique. En fonction des erreurs constatées, le commutateur utilise un des trois modes précédents.

II.4.les différents constructeurs de l’équipement Switch :

II.4.1.Introduction aux switchs Extreme :

Les Switchs Extreme sont conçus par la firme Extreme Networks, qui offrent des technologies Ethernet best-in-class;qui optimise la qualité de l'expérience utilisateur en reconnaissant les utilisateurs, leurs appareils et des machines virtuelles; c’est aussi un modulaire de bout en bout, extensible, et toujours en marche du système d'exploitation qui ajoute à l'intelligence du réseau.

II.4.1.1. Le Switch Extreme BD8800:

BlackDiamond commutateurs de la série 8000 offrent disponibilité voix-classe, de puissance à haute densité sur Ethernet Gigabit Ethernet et 10 Gigabit Ethernet partout où il est nécessaire. Ils servent ainsi un noyau d'entreprises de haute performance. Les ports non bloquants interconnectés des milliers de serveurs de haute performance pour l'informatique en grappe et les applications de centre de données. Une gamme complète de couches 2 - 4 caractéristiques pour IPv4 et IPv6 permet l'agrégation des connexions à haute vitesse, ce qui élimine les goulots d'étranglement entre la bordure et le noyau.

Le BlackDiamond 8000 correspond bien au bord des entreprises les plus exigeantes de commutation de voix sur IP (VoIP), vidéo, sans fil, et le trafic de données.

- **Ses avantages:**

  - ✓ **Connectivité de haute performance à faible puissance :**

* Gigabit haute densité et 10 commutateurs Ethernet Gigabit.

*Grande capacité de commutation et de la densité de ports élevée

*Connectivité de convergence prête avec Voice-over-IP provisionnement automatique.

*Des options de connectivité flexibles pour des applications multiples

*Faible consommation d'énergie pour les coûts d'énergie réduite et de refroidissement

  - ✓ **Haute disponibilité :**

* Conception de système redondant.

*Système modulaire Extreme XOS ® d'exploitation (OS) pour les opérations non-stop.

*Protection automatique Ethernet Switching (EAPS) du protocole de résilience.

✓ La sécurité globale assurer la défense en profondeur

* Le port Universal profil de sécurité dynamique pour fournir des stratégies de sécurité à grains fins.

*La détection des menaces et de la réponse des instruments de réagir aux intrusions réseau avec CLEAR-débit sécurité Moteur de règles.

*Infrastructure de réseau durci.

*Critères communs EAL3 + certifié.

Figure II.13 : Switch Extreme 8800

II.4.1.2.Le Switch Extreme X460:

La série X460 Sommet est basée sur Extreme Networks et Extreme XOS révolutionnaires, un OS très résistant qui offre une disponibilité continue, la gestion et l'efficacité opérationnelle. Chaque commutateur offre la même haute performance, la technologie du matériel non-blocage, dans la tradition Extreme Networks de simplifier les déploiements de réseau grâce à l'utilisation de matériel et de logiciel commun à travers le réseau. Les commutateurs X460 sommet sont des commutateurs campus de pointe efficaces avec IEEE 802.3 at PoE plus et peuvent également servir de commutateurs d'agrégation pour les réseaux d'entreprise

traditionnels.

La série Summit X460 est également une option pour DSLAM (Digital Subscriber Line Multiplixeur) [c'est un équipement situé sur le réseau de l'operateur local qui a pour fonction d'acheminer et de transmettre les données à destination d'abonnés] ou agrégation CMTS (Cable Modem Termination System), ou pour l'accès Ethernet actif. Le Sommet X460 peut également être utilisé comme un commutateur top - of-rack (c'est des commutateurs qui tissent sur le même réseau, des liens LAN contrôlés de bout en bout) pour de nombreux environnements de centres de données avec des fonctionnalités telles que Gigabit Ethernet haute de densité pour les environnements de centres de données concentrées ; améliorant ainsi les performances.

- **Avantages:**

*Haute performance et de commutation et de routage hautement évolutif.

*Sommet X460 offre un noyau classe, une commutation intelligente et un routage avec une densité de port exceptionnel.

*Haute densité.

*Option de connectivité Ethernet pour 10 Gigabit pour six ports dans un système et 32 ports dans un système.

*Haute disponibilité et simplicité.

*Soutien AVB (Sommet X460 prend en charge les normes IEEE Audio Video Bridging (AVB) que les transmissions audio et vidéo en temps réel fiables sur Ethernet, pour la haute définition et le temps sensible flux multimédia avec la qualité assigné de service QoS.

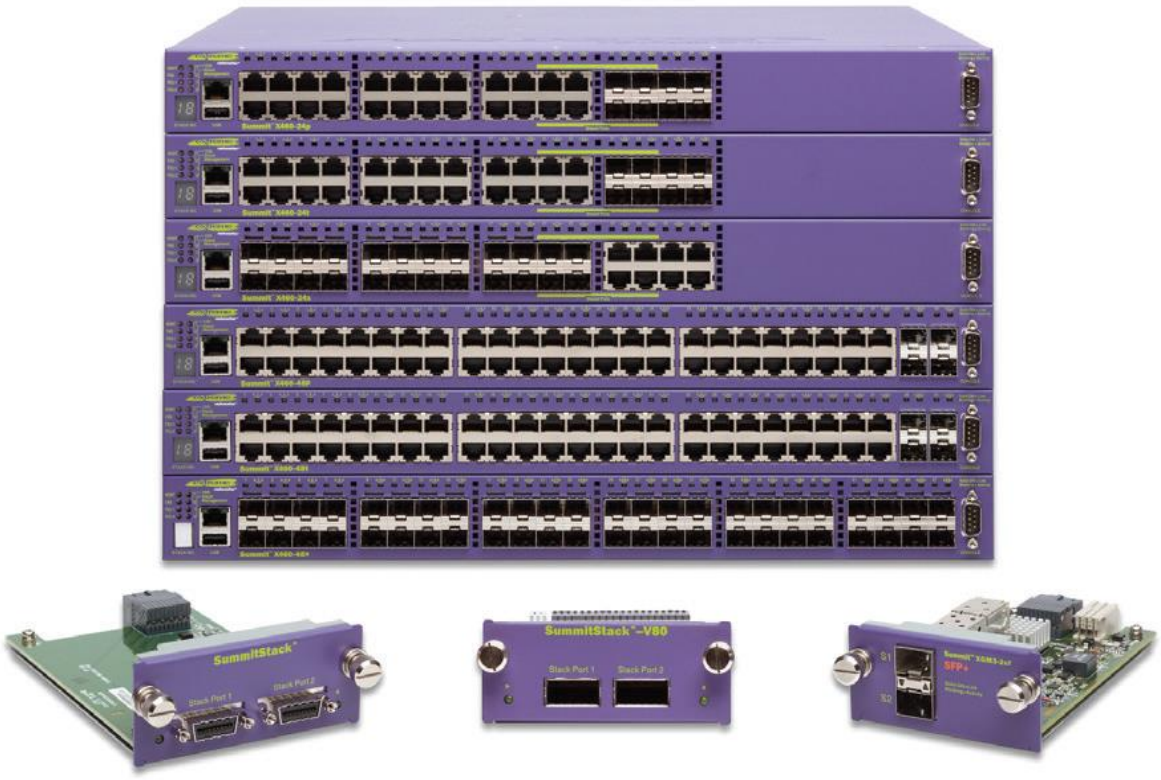


Figure II.14 : Le Switch Extreme X460

II.5.les différents constructeurs de l'équipement Firewall:

II.5.1.Définition:

Un firewall (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

Figure II.15 : Exemple d'un Firewall

II.5.2. Firewall Juniper SSG520:

Avant de parler sur le SSG520 on va d'abord évoquer la série se SSG500 ou le firewall SSG520fait partie (est inclus dedans) :

Juniper Networks Sécurisation Services Gateway 500 (SSG 500) se compose d'appareils spécialement conçus pour la sécurité qui offre un mélange parfait de performances, de sécurité, de routage et de connectivité LAN / WAN pour les grandes directions régionales et de taille moyenne, les entreprises autonomes. La fluidité du trafic dans et hors du bureau ou de l'entreprise régionale est protégée contre les vers, les logiciels espions, chevaux de Troie et les logiciels malveillants par un ensemble complet de gestion unifiée des menaces (UTM) Les caractéristiques de sécurité, y compris pare-feu dynamique, VPN IPSec, IPS,…

Figure II.16 : Firewall Juniper SSG520

Le Firewall SSG520 est Conçu pour gérer la sécurité, de routage et de réseau local (LAN) / besoins Area Network (WAN) de connectivité large de succursales régionales et moyennes entreprises, la passerelle Juniper Secure Services (SSG) 520 offre des performances et une disponibilité exceptionnelle. Une partie de la haute disponibilité (HA) fonctionnalités offertes par Juniper SSG520 réseau privé virtuel (VPN) de la plate-forme de sécurité comprennent le basculement de session pour acheminer le changement, la détection de défaillance de la liaison, le chiffrement du trafic HA, l'authentification de nouveaux membres HA, et la détection de défaillance de l'appareil. Comme l'un des modèles proposés dans la gamme de produits Juniper SSG500, la plate-forme de sécurité SSG520M VPN est très modulaire et sert à protéger votre environnement informatique unique, contre les attaques internes et externes. Juniper SSG520 services sécurisés passerelles protègent également les centres de données des accès non autorisés et veiller à la conformité réglementaire. En fait, les versions du système Network Equipment Building (NEEF) conformes de la SSG520 sont même disponibles.

La plate-forme de sécurité Juniper SSG520 VPN est équipée de nombreuses fonctionnalités de sécurité et de performances impressionnantes. Par exemple, le Juniper SSG520M offre jusqu'à 650 mégabits par seconde (Mbps) de la performance du pare-feu dynamique, jusqu'à 300Mbps de performances IPsec VPN, et 300 000 paquets par seconde (PPS) de pare-feu capacité de transmission de paquets. Capable de supporter un montant illimité d'utilisateurs, des plates-formes Juniper VPN SSG520 également 4 slots d'extension PIM, 2 EPIM slots d'extension, 4 ports 10/100/1000 E/S fixes, 128 000 sessions simultanées, 10.000 nouvelles sessions par seconde, et jusqu'à 125 réseaux locaux virtuels. En plus des caractéristiques de performance et les spécifications de la Juniper SSG520, ses nombreuses fonctionnalités de sécurité comprennent : l'usurpation d'identité par zone IP, protection de paquet mal formé, réseau joindre détection, anti-virus, filtrage de l'URL externe, anti-spam, la force brutale attaque atténuation, la sécurité VoIP et beaucoup plus.

Conclusion :

Dans ce chapitre, nous avons effectué une étude sur les composants utilisés dans les architectures réseaux et mit en évidence les performances des équipements constituant le réseau de l'entreprise Wataniya Télécom Algérie, et avec la supervision de ses équipements qui fera l'objet d'étude du chapitre suivant, offrent une meilleure qualité de service.

CHAPITRE 3

Topologie d'un réseau à superviser

CHAPITRE III.

Topologie d'un réseau à superviser

Introduction

Toute entreprise a besoin d'information lui permettant de comprendre l'état de la sécurité et de l'intégrité de son réseau, et d'identifier les problèmes potentiels avant qu'ils ne se déclarent. En effet, les meilleurs dispositifs de sécurité ne peuvent pas protéger de façon optimale un réseau s'ils ne sont pas correctement supervisés. Ainsi, la sécurité d'un réseau repose d'une part sur l'architecture et son adéquation aux besoins des composants qui le constituent, mais aussi sur l'administration et la supervision au jour le jour de ces équipements.

III.1.Administration de réseaux :

C'est tous les moyens mis en œuvre (connaissances, techniques, outils) qui permettent de superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût et de qualité, mais aussi assurer la réactivité face aux besoins de changement et d'évolution. Il est souhaitable d'appuyer autant que possible son administration de réseaux sur des standards: le protocole SNMP est actuellement la technologie de base qui permet d'administrer un réseau TCP/IP.

III.1.1.Les activités d'administration de réseaux :

L'ISO (International Standard Organization) a regroupé les activités d'administration de réseaux en cinq domaines fonctionnels :

- La gestion des anomalies : détecte les problèmes réseaux (logiciels ou matériels) et les archives accompagnés d'une solution dans une base de données.
- La gestion des comptabilités : permet d'établir des coûts d'utilisation des ressources (la consommation réseau) voir même une facturation.
- La gestion des performances : analyse de manière continue les performances du réseau afin de le maintenir dans un état de performance acceptable. Pour ce faire :
  - → des variables contenant des informations significatives quant aux performances sont récupérées (exemple : le temps de réponse d'une station, ou le taux d'utilisation d'un segment réseau…)
  - → les variables sont analysées.
  - → si elles dépassent un seuil de performance fixé préalablement, une alarme est envoyée à l'administrateur.
- La gestion des configurations: effectue un suivi des différentes configurations sur le réseau. De ce fait, elle permet une identification et un contrôle des systèmes et une collecte d'informations.
- La gestion de la sécurité : contrôle l'accès aux ressources en fonction des politiques de sécurité (met en application les politiques de sécurité).

Ces activités sont communément classées selon la façon suivante :

- Supervision : consiste à surveiller, et collecter toutes sortes d'informations.
- Gestion : consiste à gérer le réseau (gestion configurations, ressources, sécurité, dysfonctionnement, les remontées d'alarmes et leurs rapports...)
- Exploitation : consiste à traiter les problèmes opérationnels sur le réseau (maintenance, assistance technique…)

III.2.La supervision :

Ensembles de moyens consistant à surveiller les systèmes et à récupérer des informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes.

III.2.1.Objectifs de la supervision :

Les différentes orientations de la supervision réseau doivent être décrites afin d'effectuer les choix de paramétrages adéquats :

- Prévention des pannes : grâce aux Statistiques de la qualité de service et aux Collectes et mesures de performances.
- Diagnostic et résolution rapide de problèmes (la reprise sur incidents).
- Détection d'intrusion.

III.2.2.Les modules de la supervision :

Autour de la supervision, plusieurs modules coexistent :

- La supervision réseau : s'occupe de composants matériel tels que serveur, imprimante, pare-feu …
- La supervision système : s'occupe des applications et logiciels.
- La notification : permet l'envoi d'alertes par email, par sms, par téléphone, par avertissement sonore, …
- L'exécution de commandes : permet de relancer une application qui fait défaut.
- La retranscription d'état du système : permet de voir à tout moment l'état de tous les composants et applications supervisés sous forme d'un graphique, d'une carte ou d'un tableau. Son but est de rendre les résultats plus lisibles.
- La cartographie : visualise le réseau supervisé par l'intermédiaire de carte, de graphique, de tableau, …
- Le reporting : consiste en un historique complet de la supervision.

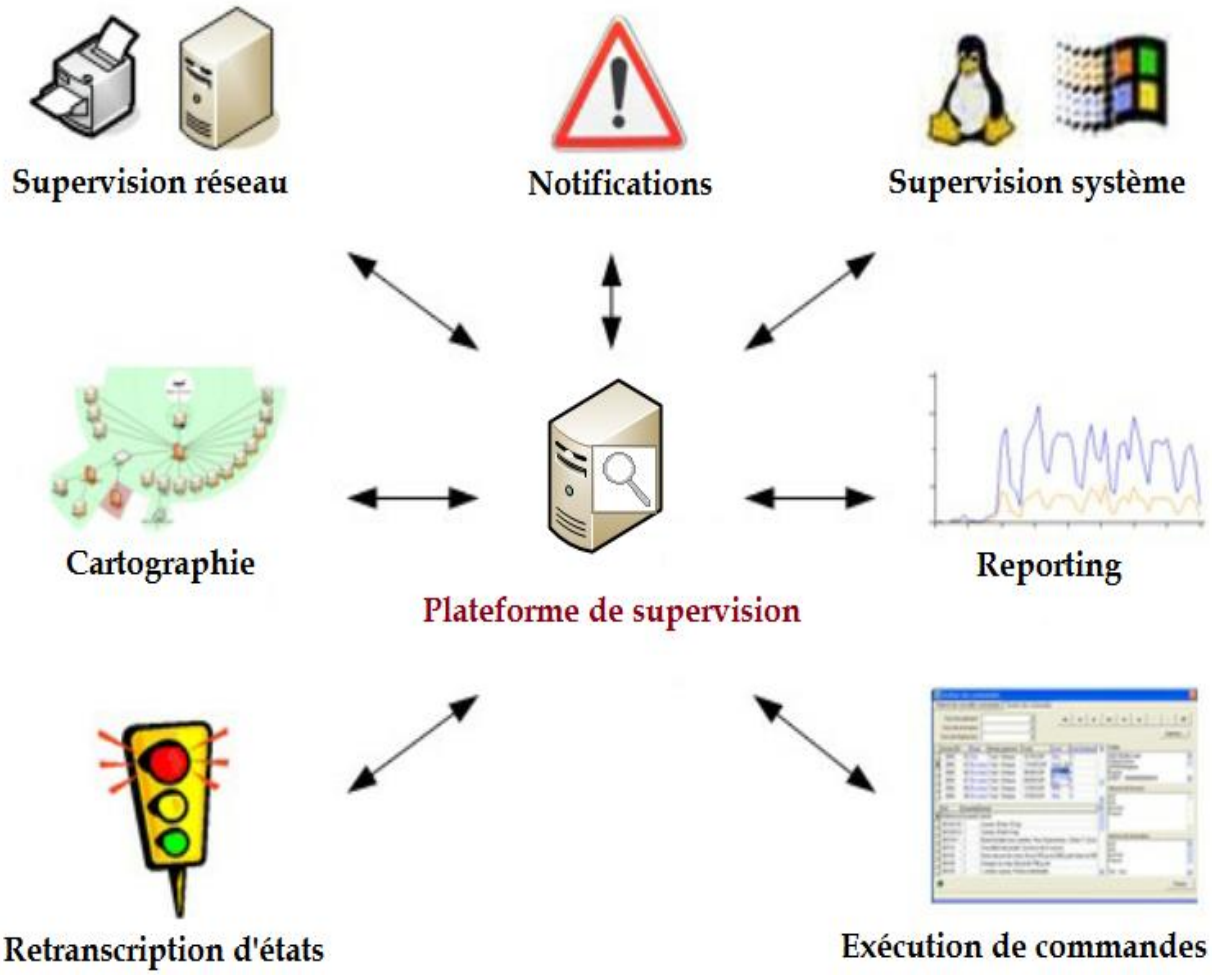


Figure III.1 :Les modules coexistant autour de la supervision

III.2.3.Les événements et les indicateurs à superviser :

Il est important de choisir les événements correspondants aux besoins du service ou du métier ainsi que les informations d'état à superviser, le plus souvent :

- Table ARP.
- Tables de session.
- L'équipement est-il opérationnel ?
- Quelle est la charge CPU ?
- Quelle est la charge réseau ?
- Quel est le temps de réponse ?
- Les disques sont-ils proches de la saturation ?
- La connectivité est-elle toujours assurée ?
- Y'a-t-il des activités suspectes ?
- …

III.2.4.Architectures de supervision :

On distingue deux architectures de supervision :

- Architecture centralisée : la surveillance se fait par un serveur de supervision global, et les remontées d'informations et d'alarmes se transmettent directement vers ce serveur.
- Architecture décentralisée : les remontées d'information se transmettent dans un premier temps vers les serveurs de supervision locaux, puis de ces derniers vers le serveur global.

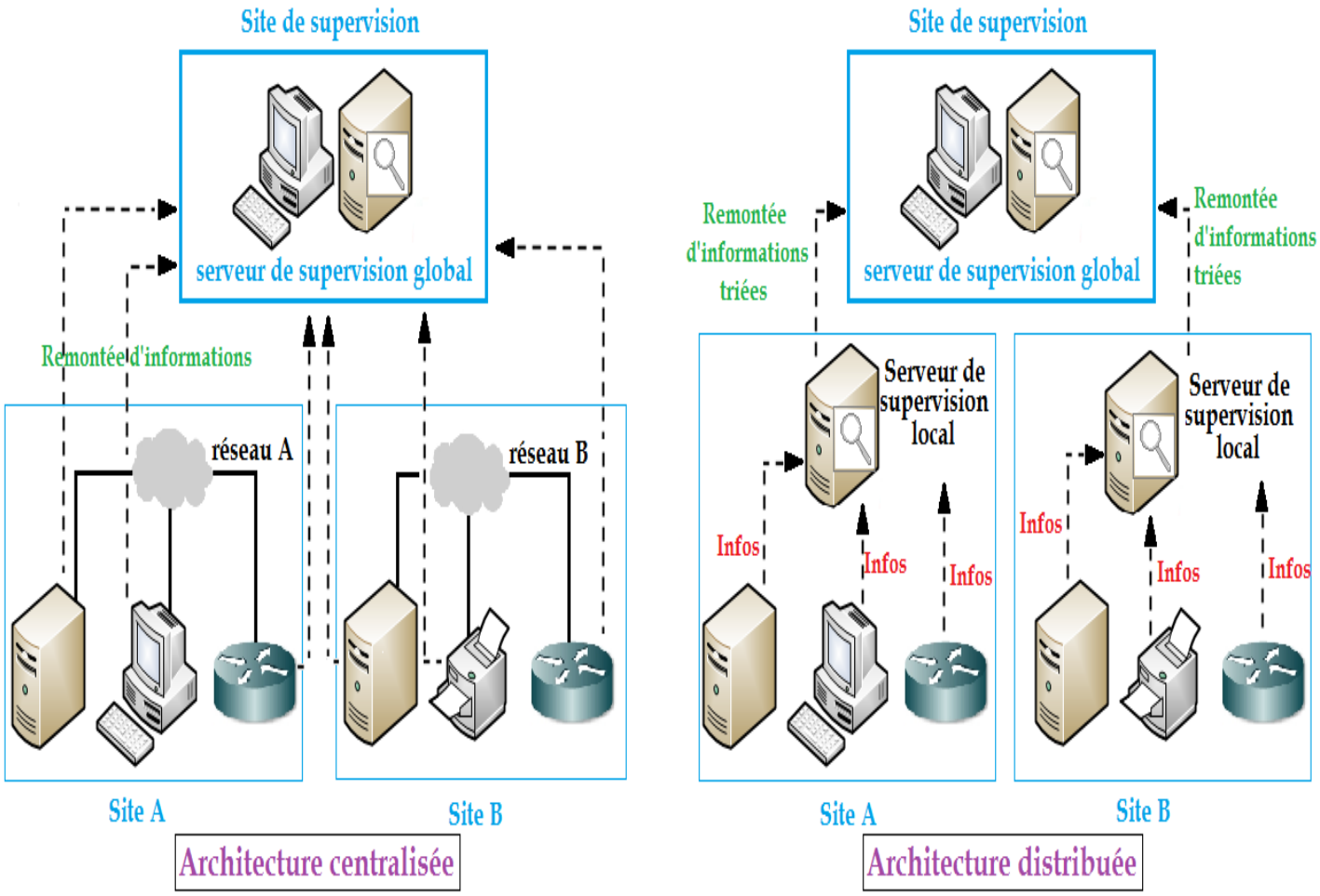


Figure III.2 : Les architectures de supervision

III.2.5. Les méthodes de supervision :

Les principales méthodes de supervision sont les suivantes :

- Analyser les fichiers log (fichiers journaux) en consultation ou avec remontée.
- Récupérer des résultats de commandes et de scripts locaux ou distants.
- Utiliser le protocole SNMP (Simple Network Management Protocol).

Pour ce faire deux modes sont utilisés, le temps réel et le temps différé.

III.2.5.1. Supervision en temps réel :

Ce mode de supervision est utilisé selon les événements et les indicateurs à superviser et selon leur criticité, les outils les plus souvent utilisés sont :

- Tripwire : outil de scellement de configuration. Selon une fonction de hachage, le fichier de configuration est haché puis signé, et on vérifie l'intégrité en comparant à ce haché.
- MBSA (Microsoft Baseline Security Analyzer) : outil fourni par Microsoft pour vérifier le niveau de sécurité des machines Windows à distance ou en local.
- Sonde IDS : système servant à détecter des attaques.
- Antivirus : programmes pour surveiller et lutter contre les virus.
- SMS (System Management Server) : utilisé pour gérer des machines Windows.

III.2.5.2. Supervision en temps différé :

Une supervision en temps différé s'effectue en parallèle avec la supervision en temps réel, elle constitue le plus souvent une analyse manuelle, mais lorsque le volume des données est important, des outils de traitement de logs sont utilisés. En pratique, tous les équipements génèrent pour chaque événement important des lignes de log, ces fichiers journaux sont archivés et centralisés sur des serveurs afin de les analyser à posteriori pour :

- Évolution à long terme.
- Détection des tendances et anomalies à suivre sur le réseau.
- Suivi de la qualité de service.
- Intervention sur des incidents de sécurité à posteriori.

On peut citer :

- **Analyse d'attaques :**

L'analyse des fichiers log permet de récolter des compléments d'information lors du traitement d'un événement de sécurité (action non autorisée détectée par l'analyse). Afin d'identifier et diagnostiquer cet événement et lancer les procédures de sécurité adéquates.

Remarque : un événement de sécurité peut être une mauvaise manipulation, une préparation d'attaque ou même une attaque. Par exemple une ligne de logs signalant une tentative échouée de connexion d'un utilisateur pour erreur de mot de passe, cela est traduit par une mauvaise manipulation. Cet événement est plus grave si cette ligne de code est répétée plusieurs fois.

Afin d'obtenir des informations sur l'origine d'une attaque, on utilise :

- Traceroute : utilitaire permettant d'afficher la route suivie par les paquets IP depuis le point d'émission jusqu'à la destination, en donnant la liste de tous les équipements traversés.
- Whois : un outil qui permet de lister la plage d'adresses IP à laquelle appartient une adresse IP entrée ainsi que des informations (nom, coordonnées postales et téléphoniques) sur le propriétaire de cette plage.
- dig, host, Nslookup : des outils qui permettent d'effectuer des requêtes DNS.

➢ Tableau de bord de sécurité :

Permet d'avoir une vue d'ensemble de la sécurité opérationnelle d'une plateforme ou d'un réseau (détection des anomalies, des attaques et des évolutions à mener sur le périmètre considéré pour effectuer une prévention des pannes et des attaques). Dans un tableau de bord, figure les éléments qui suivent :

- ✧ Information sur les événements marquants survenus dans la période de référence.
- ✧ État d'avancement des mécanismes de sécurité du domaine sécurité.
- ✧ Synthèse des événements de sécurité que subit le réseau accompagnés de leurs niveaux de sévérité, qui peuvent être :
    - ✦ le nombre de machines impactées, nature de l'impact (visant la disponibilité, l'intégrité...), sévérité de l'impact.
    - ✦ L'origine de l'attaque (son adresse source).
    - ✦ La caractérisation de l'événement (virus, DoS…).
    - ✦ la réaction face à l'incident.

Remarque : dès qu'il est question de tâches de plus langue haleine, l'emploi de tableaux de bord devient fastidieux. Pour cette raison, les fichiers log sont traités par des outils tel que les produits de type ESM (Entreprise Security Management), ou des outils de supervision libres.

III.2.6.Formats de données de la supervision :

Il s'agit des fichiers de journalisation :

III.2.6.1.Syslog :

C'est un standard pour tout ce qui concerne les messages de notification d'événements définissant à la fois le format de ces données et le mécanisme de transport de ces messages.

Pour tout événement survenant sur un système peut être logé, pour ce faire, un message est généré, ne dépassant pas 1024 octets par message, comme par exemple, une erreur d'authentification, un message du noyau ou d'une application, ou une connexion à un service.

Remarque : deux propriétés caractérisent un message, sa facilité et sa sévérité, qui peuvent être présentées par des entiers. La facilité permet de distinguer quel est le processus ou démon tournant sur le système à l'origine du message. La sévérité concerne le coté critique (urgence, erreur, avertissement, information, alerte...

III.2.6.2.Netflow :

Technologie conçue par Cisco, elle permet de collecter des données sur le trafic traversant des équipements réseau, et de ce fait effectuer des mesures de ce trafic dans un cadre de supervision ou de facturation.

Un flux IP est caractérisé par les adresses IP, le protocole utilisé, les ports, les interfaces d'entrée et de sortie ainsi que le champ TOS(…). Au premier passage d'un paquet, le routeur consulte ses tables afin de déterminer vers quel nœud le routeur l'achemine. Cependant, les paquets qui suivent bénéficient du cache Netflow lors de leur entrée sur le routeur, cela permet à celui-ci d'accéder à l'information de routage plus rapidement.

Quand le routeur libère son cache Netflow d'une entrée, un datagramme peut être envoyé à un superviseur en incluant les informations de routage. Ces données sont rassemblées par un collecteur générique qui effectue souvent des prétraitements basiques permettant l'émission de rapports. Les données qui peuvent être pertinentes pour la supervision de la sécurité sont les données de comptage (Netflow accounting). Leur analyse est judicieuse dans de nombreux cas, comme par exemple dans la détection d'attaques, cela grâce aux regroupements des logs, qui permettent d'observer des comportements et d'expliquer des événements de sécurité.

Conclusion :

Ce chapitre nous a permis de présenter le principe général d'administration réseau et la topologie employé dans le réseau a supervisé .Le chapitre suivant sera consacré à la spécification d'un protocole qui va nous permettre de mettre en œuvre ce qui était dit précédemment.

CHAPITRE 4

Simple Network Management Protocol (SNMP)

CHAPITRE IV.

Simple Network Manager Protocol (SNMP)

Introduction :

SNMP est l'acronyme de Simple Network Management Protocol. On peut le traduire par Protocol simple de gestion de réseaux. Chaque machine, indépendamment de son système d'exploitation possède de nombreuse informations capitales pour l'administrateur réseaux.si jamais celui-ci arrive à saturation. Le SNMP emploi le Protocol UDP en tant que protocole de couche transport.

SNMP est un protocole de communication qui a été créé pour être une couche utilisant TCP/IP à un niveau supérieur. Il opère en accord avec UDP et IP, et permet de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance. C'est l'un des protocoles les plus utilisés pour la gestion (management, monitoring) des réseaux.

Ces informations peuvent être :

- La quantité de RAM disponible.
- La charge CPU.
- L'état du disque dur.

Concrètement, dans le cadre d'un réseau, SNMP est utilisé pour:

- administrer les équipements.
- surveiller le comportement des équipements.
- modifier le paramétrage de certains composants.

Comme son nom l'indique, il est relativement simple tout en étant très complet. En effet, sa simplicité ne lui empêche pas de pouvoir gérer des réseaux hétérogènes complexes.

Son utilisation est basée sur trois éléments. Les voici :

- Les agents, placés sur les éléments actifs du réseau.
- Les managers.
- La MIB.

Nous expliquerons chacun des éléments ci-dessus ultérieurement.

Les éléments actifs peuvent être un:

- ordinateur.
- serveur.
- routeur.
- switch.

Nous allons maintenant étudier les différents éléments constituant cette gestion de réseaux.

IV.1. Les éléments constituants :

IV.1.1. Les agents :

Comme dit précédemment, nous allons installer ces agents dans les entités que nous voulons gérer. Celles-ci peuvent être des routeurs, des machines, des serveurs…

Cet agent, installé dans un élément va donc avoir le rôle de serveur. Cet agent « écoute » le port 161 les requêtes provenant d'un manager et lui renvoie sa réponse. Ces requêtes sont en fait des demandes d'informations sur le matériel ou sur un service et l'agent renvoie cette information.

Mais, cet agent peut aussi avoir d'autre fonction. Par exemple, en fonction de sa configuration, il peut envoyer, sans requête préalable certaines alertes. Ces alertes peuvent être la charge CPU qui est anormalement haute, le débit du réseau qui devient critique …

Par ailleurs, l'agent peut aussi agir directement sur le matériel, c'est-à-dire modifier certains paramètres et même prendre le contrôle à distance.

IV.1.2. Les managers :

Le manager est celui qui veut connaître certaines informations (l'administrateur). Pour cela il envoie des requêtes aux différents agents implantés dans les éléments actifs et ces derniers répondent avec les informations demandées.

IV.1.3. La MIB :

La MIB (Management Information Base) est une base de données contenant toutes les informations que le manager serait susceptible de savoir.

Chaque MIB est propre à l'agent. Il y a donc une MIB pour chaque équipement supervisé. Cette MIB contient des:

- informations à consulter.
- paramètres à modifier.
- alarmes à émettre.

La MIB est organisé hiérarchiquement avec une structure arborescente, de la même façon que les domaines d'Internet.

Chaque nœud d'un arbre représente un objet. Cet objet est définit avec un OID (Object Identifier). Cet identifiant est constitué d'une suite de chiffre séparé par des points.

Pour qu'un client accède à ces objets, il faut qu'il en connaisse l'existence. Une MIB contient un ensemble d'informations standards ; c'est la MIB standard.

Or pour la plupart des éléments réseaux, on rajoute un certain nombre d'objets propre à un agent pour en exploiter les possibilités : c'est la MIB privée. Par exemple, dans la MIB standard, nous retrouvons certains compteurs, notamment ceux mesurant la performance réseau.

La MIB est un fichier texte écrit en langage ASN 1(Abstract Syntax Notation 1). Il contient la spécification de différents OID. Pour chaque OID, cette spécification comprend :

* Un OID unique, dans l'arbre des OID ; par exemple 1.3.6.1.2.1.1.3.

* Un nom générique ; par exemple sysUpTime.

* Une description de cet OID;

* Son type ; par exemple TimeTicks. Il existe différents types possibles de données qui permettent de couvrir tous les besoins ;

* Son statut ; par exemple mandatory. Les différents statuts possibles sont "mandatory", "optional", "obsolete".

* Son mode d'accès ; par exemple read-only. Les differents accès sont: "read-only", "read-write", "write-only", "not-accessible".

IV.1. 3.1.Quelques difficultés courantes avec les MIB :

- → **Disponibilité du fichier MIB :** S'il n'est pas nécessaire de disposer de la MIB d'un équipement pour le superviser, il est parfois difficile voire impossible de comprendre le rôle des OID de cet agent ou de deviner à la suite de quel événement va être envoyé un message "Trap" au superviseur. La seule référence reste le fichier MIB de l'équipement et ce fichier est parfois difficile à trouver.
- → **Erreur de syntaxe:** Il est très courant de trouver des fichiers MIB comportant des erreurs de syntaxe.la ligne suivante tirée du fichier d'un équipementier réseau qui faisait planter le compilateur de MIB. Il y avait un double commentaire (le double caractère '-'), et la norme ASN.1 est très claire à ce sujet : un commentaire commence avec le double caractère '-' et se termine à la fin de la ligne ou alors au double caractère '-' suivant présent sur la même ligne. En conclusion, il n'est pas exclu de trouver des erreurs de syntaxe dans un fichier MIB (même écrit par un équipementier réseau renommé).
- → **Complétude du fichier MIB :** Parfois aussi, on trouve des MIB dont la description textuelle des OID est vide, ce qui n'aide pas beaucoup à leur compréhension. De même, il est souvent impossible de connaître de manière fiable la liste des OID (on

parle des varbinds) portés par un message "Trap". Il faut alors avoir recours à un analyseur de protocole pour connaître cette liste.

Voici un exemple d'objet :

ifDescr est décrite par :

```
ifDescr OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..255))
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
            "A textual string containing information about the
```

Le fichier fournit toutes les informations relatives à la propriété « sysName » :

- Syntaxe : il s'agit d'une chaîne de caractères de taille variant entre 0 et 255.
- Accès : l'accès à cette variable se fait en lecture ou en écriture.
- Etat : cette variable existe et est toujours utilisable.
- Description : il s'agit du nom complet du nœud.
- Sa place dans l'arborescence : 5ème propriété de l'objet « system » : On en déduit que cette variable a pour clé la valeur 1.3.6.1.2.1.1.5.

Ainsi, nous avons la description de toutes les variables, leurs méthodes d'accès et la clé que nous devons utiliser pour lire ou écrire sa valeur. La majorité des constructeurs fournit des fichiers MIBs contenant des informations sur les variables propres à leur matériel, ne faisant pas partie des informations standards. Il existe un grand nombre d'outils permettant de visualiser l'arbre des MIBs et de rechercher une variable au sein de celui-ci.

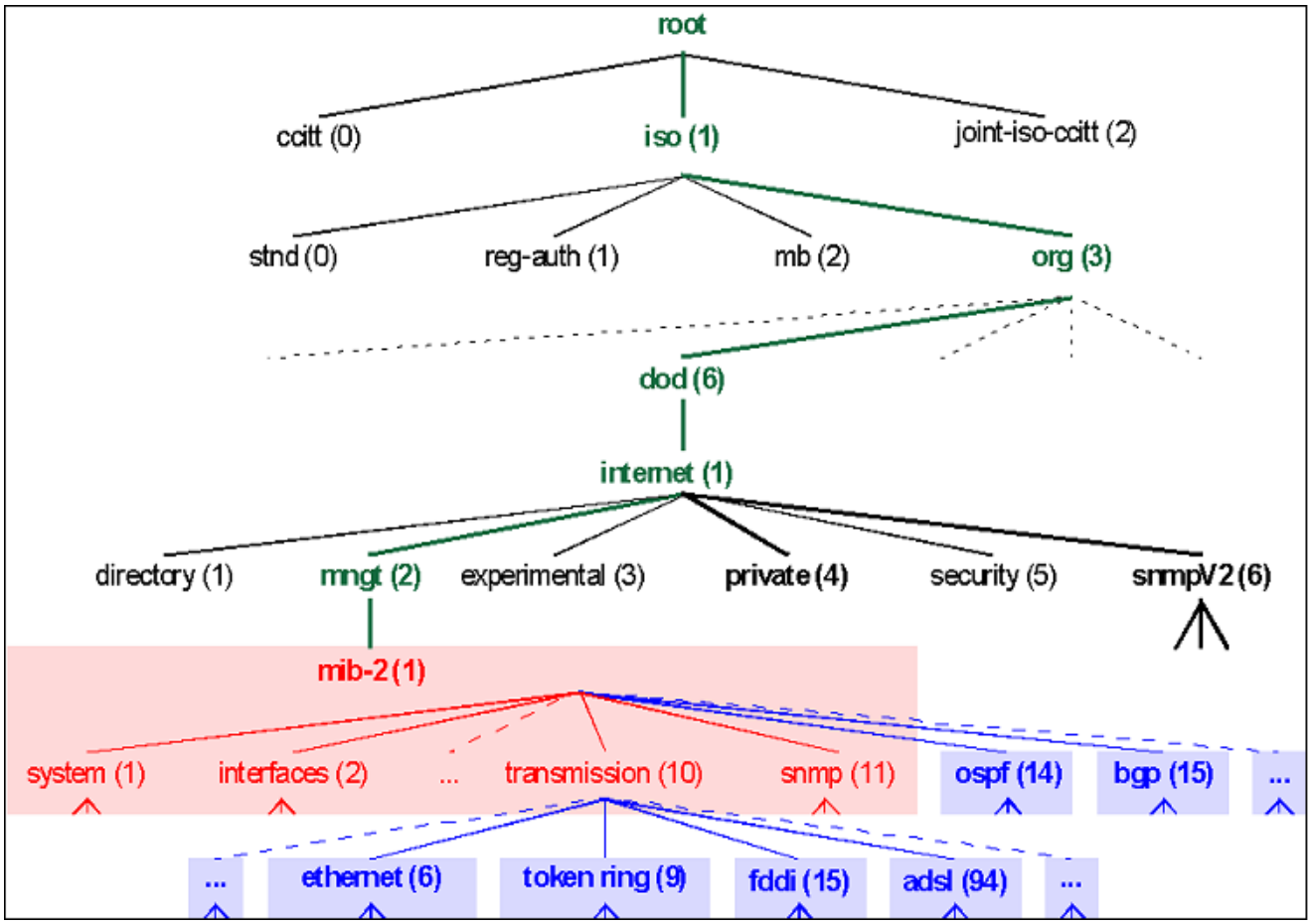


Figure IV.1 : L'arborescence des OIDs en SNMP

La figure présente l'arborescence des OIDs, constituant les MIBs. En SNMP, on utilise communément deux branches :

• iso.org.dod.internet.mngt.mib-2 (1.3.6.1.2.1) : il s'agit de la branche contenant tous les objets standards, définis précisément dans les RFC. Ainsi, tout agent SNMP doit pouvoir reconnaître cette branche et les variables qui y sont définies.

• iso.org.dod.internet.private.enterprises (1.3.6.1.4.1) : cette branche est l'origine de tous les objets propres au matériel et définies par le constructeur. Ainsi, chaque constructeur se voit attribué un identifiant (VendorID), qui lui fournit un espace de données au sein de l'arbre des MIBs. Si nous prenons l'exemple de Cisco, dont l'identifiant est 9, toutes les variables propres à Cisco ont une clé débutant par 1.3.6.1.4.1.9.

IV.2.L'architecture du protocole :

IV.2.1.Modèle :

Le protocole SNMP est bâti au-dessus du protocole UDP/IP. Voici le modèle :

	Modèle *OSI*	Modèle *TCP/IP* (protocole)
7	Application	***SNMP***
6	Présentation	
5	Session	
4	Transport	*UDP*
3	Réseau	*IP*
2	Liaison	Interface réseau
1	Physique	

Tableau IV.1 :SNMP bâti au-dessus de l'UDP/IP.

- ✓ **Localisation de SNMP dans le modèle TCP/IP :**

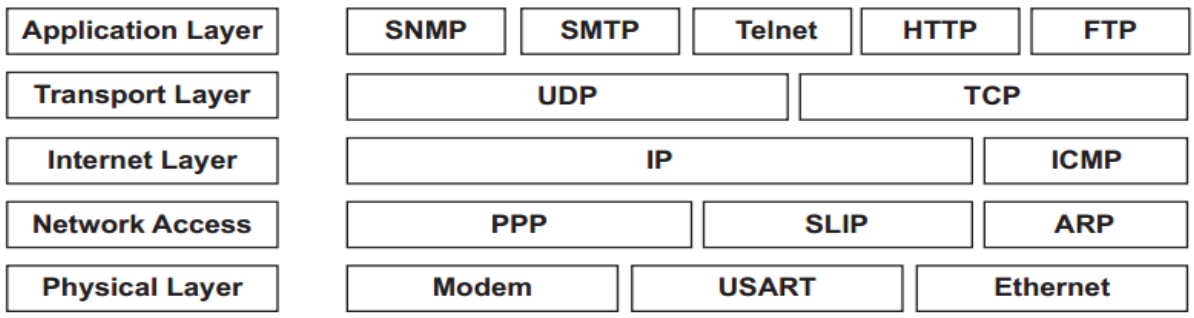


Figure IV.2 :Localisation de SNMP dans le modèle TCP/IP.

Le protocole SNMP utilise le protocole UDP et le port 161 pour la partie agent. Ce port servira à recevoir les requêtes de la station de gestion. Le port 162 quant à lui est réservé au manage pour recevoir les réponses ou les alertes des différents agents.

IV.2.2.Les messages :

Il existe six types de messages : quatre types de messages pour les requêtes, un message répo nse et un message "trap». Voici leurs fonctions :

- **GetRequest :** Le Manager SNMP demande une information à un agent SNMP.

• **GetNextRequest :** Le Manager SNMP demande l'information suivante à l'agent SNMP.

• **GetBulk :** Permet la recherche d'un ensemble de variables regroupées. Cette commande apparaît dans la version 2 de SNMP.

• **SetRequest :** Le Manager SNMP met à jour une information sur un agent SNMP.

• **GetResponse :** L'agent SNMP répond à un GetRequest ou à un SetRequest.

• **Trap :** Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont: Warm Start, Link Down, Link Up, Authentification Failure, Cold Start.

Voici un exemple d'échange de messages entre le manager et l'agent.

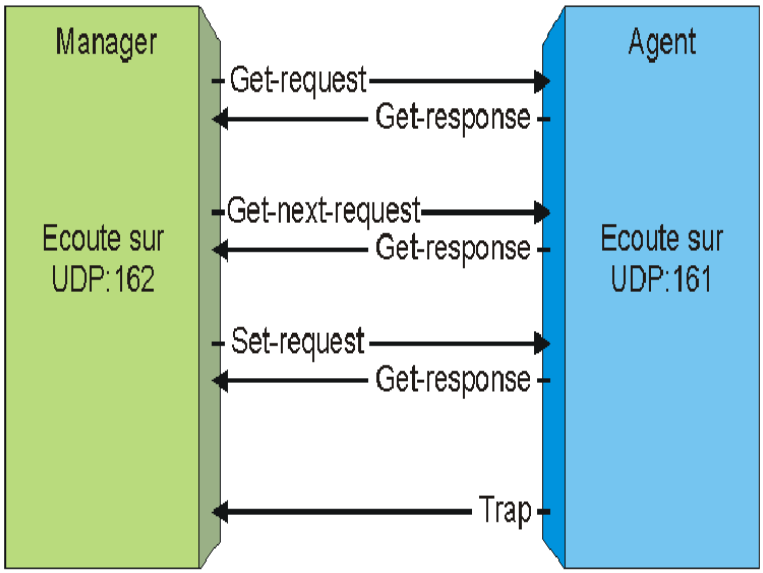


Figure IV.3. Échange entre Manager et Agent.

IV.2.3.Trame SNMP et TRAPU :

Voici la trame SNMP :

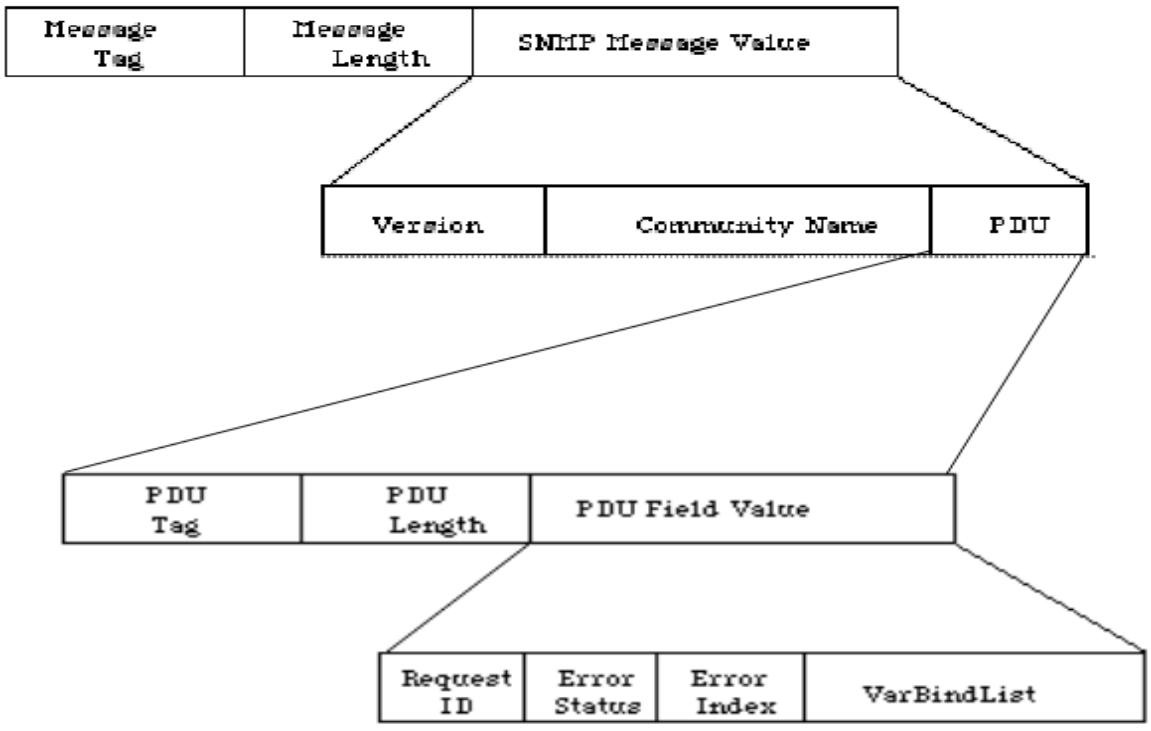


Figure IV.4 : Les messages d'une Trame SNMP.

IV.2.3.1.Les différents champs :

• **Version :** Ce champ indique la version du protocole utilisé. 0 pour la V1 et 3 pour la V3.

• **Community Name :** Sert à faire de l'authentification. En effet, on peut définir plusieurs groupes qui auront des droits différents sur les objets de la MIB (lecture seule, lecture/écriture). Cette authentification est la seule option de sécurité observée dans SNMPv1. Malheureusement, la chaîne de caractère correspondante transite en clair sur le réseau.

• **PDU Tag :** Type de requête : GetRequest, GetNextrRequest. Voici le tableau correspondant :

Type de PDU	Nom
0	Get-request
1	Get next-request
2	Set-request
3	Get response
4	Trap

Tableau IV.2 : Tableau des Différents type de PDU.

• **Request ID :** Identifiant du message. Il sert à faire correspondre la réponse avec la requête.

• **Error Status :** Indicateur d'erreur.

• **Error Index :** Pointeur sur l'erreur.

• **VarBindList :** Valeur des différentes variables.

La trame du « Trap » est légèrement différente d'une trame SNMP. Elle est représentée dans la figure ci-dessous:

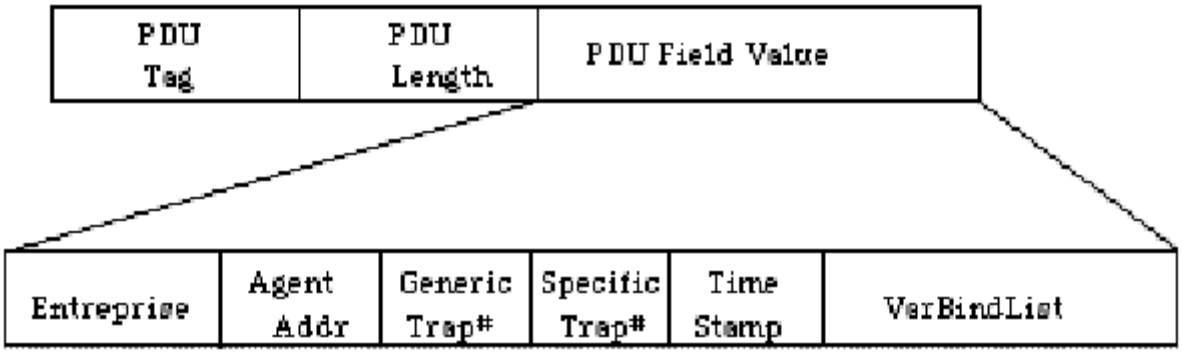


Figure IV.5 :Trame du Trap

Notons de plus près les différents champs :

- **Entreprise :** Valeur de l'objet sysobjectid de la MIB de l'agent.
- **Agent Addr :** Adresse IP de l'agent.
- **Generic Trap :** Valeur des trap.
- **Specific Trap :** trap spécifique à l'agent donc non standardisé.
- **Time Stamp :** Valeur de l'objet sysUpTime de la MIB de l'agent lorsque l'événement s'est produit.
- **VarBindList :** Liste de variables contenant des informations sur le Trap.

Voici la liste des « Trap » (les alarmes envoyées par l'agent) :

Nom	**Numero SNMP**	**Signification**
coldStart	0	L'agent se réinitialise et les objets peuvent changer (changement de configuration).
warmStart	1	L'agent se réinitialise, mais les objets ne sont pas modifiés (pas de changement de configuration).
linkDown	2	Une des interfaces de l'agent est non opérationnelle (la première variable dans la liste variable bindings identifie l'interface).
linkUp	3	Une des interfaces de l'agent est à nouveau opérationnelle (la première variable dans la liste variable bindings identifie l'interfaces).

authenticationFailure	4	Un message SNMP a été reçu d'une entité SNMP et il y a eu un problème d'authentification en fonction du nom de communauté et des droits d'accès qui sont accordés.
egpNeighborLoss	5	Un EGP peer (EGP=Exterior Gatway Protocol) est tombé (la première variable dans la liste variable-bindings contient l'adresse IP).
entrepriseSpecific	6	certains évènements dépendant de l'agent et ne sont donc pas standardisés, Dans ce cas le numéro du trap est donné dans le champ specific-trap.

Tableau IV.3 : la liste des « Trap » envoyé par l'agent.

De plus, en examinant la trame, nous pouvons remarquer que le seul processus d'identification est le champ « Community Name » mais, malheureusement transite en clair sur le réseau. De ce fait, il est évident que le protocole SNMP n'est pas sécurisé donc une attaque serait envisageable. En effet, une tierce personne pourrait prendre facilement le contrôle d'une machine et dégrader le matériel voir pire.

C'est pourquoi, l'IETF a voulu mettre en place une nouvelle version du protocole: SNMP V2. Mais, les différents collaborateurs n'ont pas pu s'entendre sur un mécanisme homogène de sécurité et ont donc décidé de développer chacun leur version 2 du protocole SNMP la version SNMPV2u et SNMPV2*.

Mais, comme il ne peut y avoir deux versions officielles du protocole, aucune de ces deux versions n'a été adoptée.

IV.3.Les différentes versions et la sécurité :

IV.3.1.Version 1 :

La version 1 du protocole SNMP qui est la plus utilisée par les administrateurs réseaux ne comporte aucun processus d'authentification et de sécurité hormis le champ « Community Name » qui passe malheureusement en clair sur le réseau.

IV.3.2.Version 2 :

Il existe plusieurs variantes de la version 2, mais aucune d'entre elles n'a été officialisée. Cette version reste principalement expérimentale et rajoute notamment de la sécurité avec SNMPsec. Cette version a laissé place à la version 3 de SNMP.

IV.3.3.Version 3 :

Propose une nouvelle terminologie, on ne parle plus de manager, d'agent mais d'entité. Constitue une transition vers une architecture p2p et modulaire, une entité est composée d'un engin de base et d'applications.

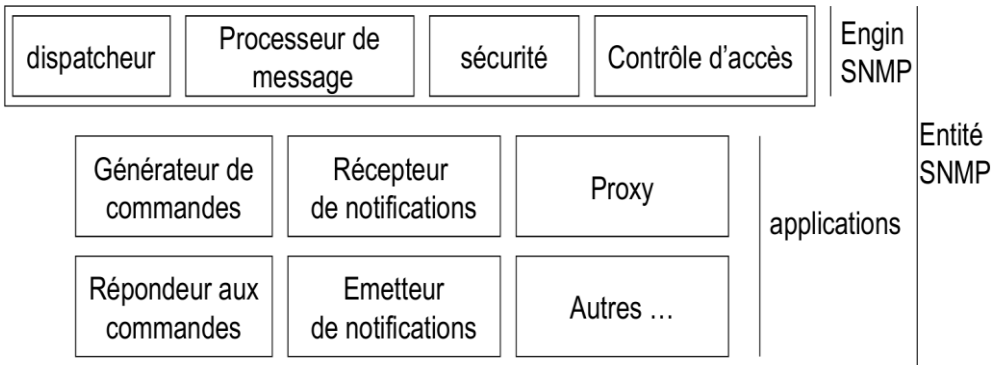


Figure IV.6 : Entité SNMP

✓ SNMP Engine :

Comme son nom l'indique, le moteur assure toute la partie technique du travail.

Le dispatcher aiguille les messages qui arrivent du réseau vers le bloc de traitement de messages qui sera capable de le traiter (par exemple le sous-système SNMPv1 ou SNMPv3 du module message processing). Inversement, il redirige les messages en provenance de ce module vers le réseau, encapsulé dans le protocole adéquat (par exemple, UDP/IP ou IPX).

Le message processing s'occupe du décodage et de l'assemblage des messages. Des sous-systèmes gèrent les différents types de messages utilisables par l'entité (SNMPv1, SNMPv2C, SNMPv3).

Le module security traite de la sécurité des échanges, si elle est nécessaire : c'est lui qui est chargé de traiter la confidentialité des communications et l'authentification du correspondant.

Plusieurs protocoles sont définis et utilisables et l'architecture SNMPv3 est extensible de manière à permettre l'utilisation d'autres modèles de sécurité que ceux prévus d'origine.

Le changement majeur de cette version est l'introduction d'authentification et de sécurité dans le protocole SNMP. En effet, avec cette version, les messages échangés ne peuvent plus être lu par tout le monde sur le réseau.

Cette sécurité est basée sur 2 concepts :

• USM (User-based Security Model).

• VACM (View Access Control Model).

Cette partie de sécurité assure plusieurs fonctions. Ces fonctions ont pour but d'empêcher tous types d'attaques qui peuvent être de :

• authentification ;

• cryptage ;

• estampillage de temps.

✓ L'authentification :

L'authentification permet de s'assurer que le paquet n'a pas subi de modification et que le mot de passe fournit par le manager est correct. Le mot de passe est partagé, c'est-à-dire qu'il doit être connu uniquement des entités qui s'envoient les messages.

L'authentification est effectuée grâce à des fonctions de hachage :

• HMAC-MD5-96.

• HMAC-SHA-96.

Les algorithmes de hachage MD5 et Secure Hash (SHA) sont utilisés pour calculer des hashs.

Le mécanisme d'authentification est représenté ci-dessous:

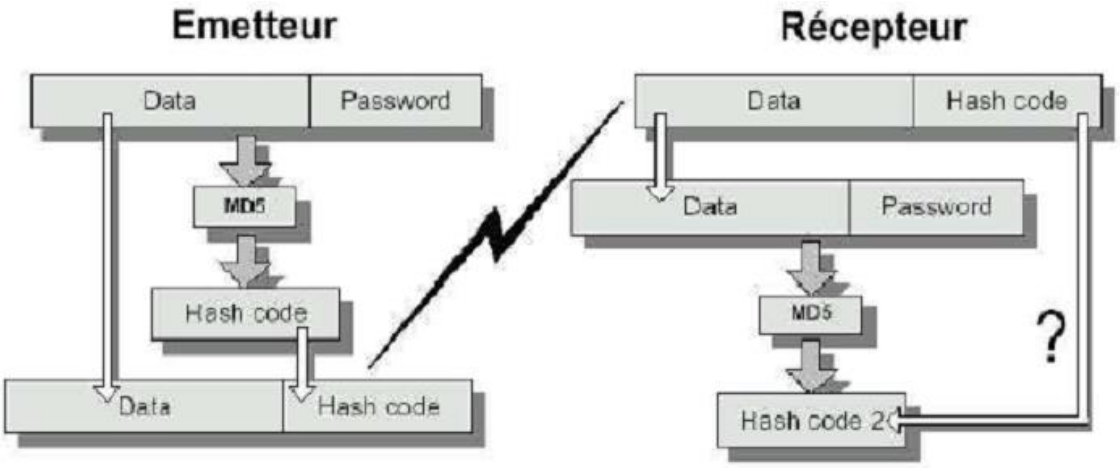


Figure IV.7 : Mécanisme d'authentification.

Les étapes d'authentification sont les suivantes :

- L'émetteur regroupe des informations à transmettre avec le mot de passe.
- On applique la fonction de hachage.
- Les données et le code de hachage sont ensuite transmis sur le réseau.
- Le récepteur prend le bloc des données, et y ajoute le mot de passe.
- On applique la fonction de hachage.
- Si le code de hachage est identique à celui transmis, le transmetteur est authentifié.

Lors de cette étape, le mot de passe n'est pas passé sur le réseau. Cette technique ne cache pas le contenu du paquet et ne crypte pas. De ce fait, une tierce personne pourrait regarder le contenu du paquet mais, ne pourrait le modifier sans connaître le mot de passe. Lors de cette étape, toute la trame est authentifiée.

✓ Le cryptage :

Comme dit précédemment, cette partie de la sécurité permet de crypter le message SNMP. Ainsi, si une tierce personne « écoute » le réseau, elle ne pourra voir le contenu du paquet car celui-ci sera crypter.

Le cryptage se fait grâce au DES (Data Encryption Standard) avec des clés de 64 bits.

Voici le schéma de la phase de cryptage :

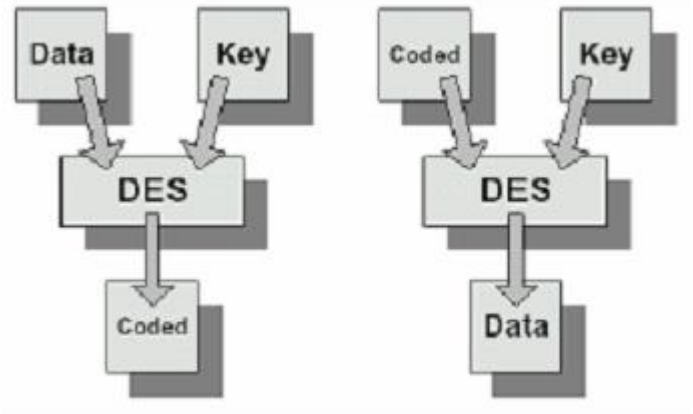


Figure IV.8 : Phase de cryptage.

Le mot de passe utilisé lors de la phase de cryptage est évidemment différent de celui utilisé pour l'authentification. Ceci permet l'indépendance des deux systèmes. Lors de cette phase, seul le « PDU » est crypté.

- **L'estampillage de temps :**

  Si une requête est transmise, les mécanismes d'authentification et de cryptage n'empêchent pas quelqu'un de saisir un paquet SNMPv3 validé du réseau et de tenter de le réutiliser plus tard, sans modification.

  Par exemple, si l'administrateur effectue l'opération de mise à jour d'un équipement, quelqu'un peut saisir ce paquet et tenter de le retransmettre à l'équipement à chaque fois que cette personne désire faire une mise à jour illicite de l'équipement. Même si la personne n'a pas l'autorisation nécessaire, elle envoie un paquet, authentifié et encrypté correctement pour l'administration de l'équipement.

On appelle ce type d'attaques le « Replay Attack ». Pour éviter ceci, le temps est estampillé sur chaque paquet. Quand on reçoit un paquet SNMPv3, on compare le temps actuel avec le temps dans le paquet. Si la différence est plus que supérieur à 150 secondes, le paquet est ignoré. SNMPv3 n'utilise pas l'heure normale. On utilise plutôt une horloge différente dans chaque agent. Ceux-ci gardent en mémoire le nombre de secondes écoulées depuis que l'agent a été mis en circuit.

✓ VACM :

Le VACM permet de contrôler tous les accès à la MIB. Il est alors possible de restreindre l'accès en fonction de l'utilisateur ou d'un groupe d'utilisateur.

✓ La trame V3 :

La trame V3 est très différente de la trame V1 mais reste codée dans le même langage pour assurer la compatibilité.

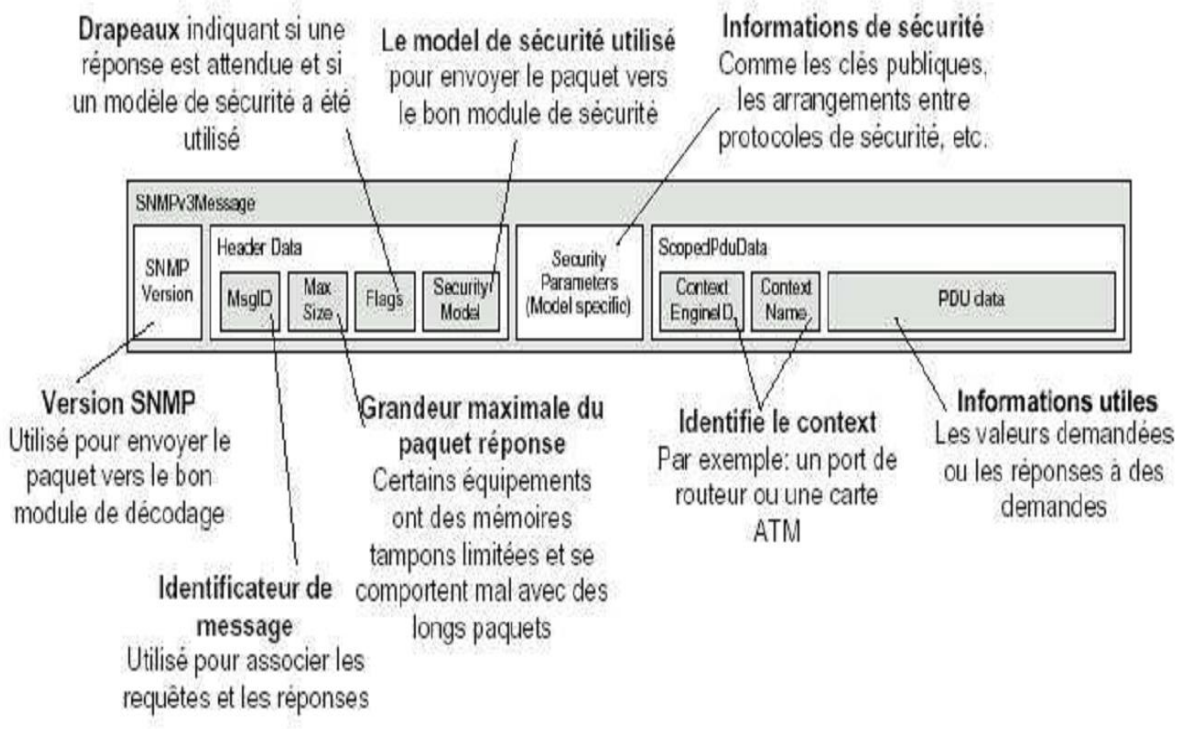


Figure IV.9 : Trame SNMP

IV.4.Avantages et inconvénients du protocole SNMP :

IV.4.1. Avantages :

L'avantage majeur d'utiliser SNMP est, qu'il est de conception simple. Il est donc aisé de l'implémenter sur un réseau, puisqu'il ne nécessite pas une longue configuration et qu'il est de petite taille. Le résultat le plus important de cette simplicité est une administration simplifié du réseau et une implémentation rapide.

Un autre avantage de SNMP est qu'il est très répandu aujourd'hui. Presque tous les grands constructeurs de matériel réseau implémentent dans leurs produits le support SNMP.

L'expansion est un autre avantage de SNMP. De par sa simplicité de conception, il est facile à mettre à jour pour qu'il réponde aux besoins des utilisateurs futurs. Il est également modulable.

Enfin, SNMP est, en général, basé sur le protocole de transport UDP, ce qui nécessite moins de ressources et de connexions simultanées comparativement à TCP. Notamment, il demande peu de ressource réseaux et aussi est une solution peu coûteuse.

IV.4.2. Inconvénients :

Le premier défaut de SNMPv1 est qu'il contient quelques gros trous de sécurité à travers lesquels des intrus peuvent accéder aux informations transitant sur le réseau. La solution à ce problème est apportée dans les versions suivantes qui implémentent des mécanismes de sécurité en ce qui concerne le caractère privé des données ainsi qu'une authentification et un contrôle d'accès.

Il n'y a pas de contrôle de transmission des données, vu que SNMP travaille avec UDP. L'interrogation régulière des agents par la station d'administration provoque une surcharge du trafic sur le réseau. Cette surcharge n'est pas trop gênante sur un réseau local mais devient embarrassante via Internet.

IV.5. Le SNMP et d'autres protocoles :

➢ ICMP (Internet Control Message Protocol) :

ICMP est un protocole de couche réseau (couche 3 du modèle OSI) qui vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol). C'est l'un des protocoles fondamentaux constituant la suite de protocole internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreurs. Les paquets ICMP sont encapsulés dans des paquets IP (malgré qu'ils soient au même niveau OSI), et peuvent contenir des bouts de paquets IP pour citer celui ayant généré l'erreur. Afin de catégoriser les erreurs, celles-ci sont divisées en types eux-mêmes parfois divisés en codes.

C'est un protocole très simple, qui n'a pas pour fonction directe la supervision d'un réseau mais, qui est utilisé comme source d'information sur la qualité du réseau ou sur la présence d'une machine.

Conclusion :

Dans ce chapitre nous avons démontrés l'importance du protocole SNMP,il est ainsi le standard incontournable dans le domaine de l'administration de réseaux d'entreprise. Son utilisation s'est étendue au-delà, dans le monde du système et des applications.

Les limitations des versions 1 et 2 sont comblées avec la version 3. Ce dernier standard demande toutefois plus de travail d'implémentation et de mise en œuvre.

Dans tous les cas, établir une administration de réseau efficace demande un travail non négligeable en termes de choix et de mise en place d'outils, d'organisation et de monitoring qui sera mit en place dans le prochain chapitre.

CHAPITRE 5

Manager SNMP (Applications de supervision)

CHAPITRE V.

Manager SNMP (Applications de supervision)

Introduction :

A l'issu d'une étude préalable du réseau informatique de Wataniya Algérie Telecom, nous avons pu dégager les insuffisances auxquelles nous devions apporter une solution, qui consiste à la supervision des performances et des incidents d'un réseau IP.

Présentation du projet :

Notre stage s'est déroulé au sein de l'équipe Data Networking. Ce service a pour objectif de résoudre les problématiques liées aux réseaux.

Durant notre stage, notre travail consiste à mettre en place :

- ⇨ Une station de supervision qui comporte le monitoring des équipements des nodes MPLS (Manager Protocol Label Switching).
- ⇨ Une étude sur un système de supervision récemment installé (**InfoVista**).
- ⇨ Réalisation d'une application qui a pour objectif de développer un outil qui facilite la supervision et la maintenance des composants du réseau.

- ➢ **Étapes de conception pour** le projet de supervision :

  - Implémentation du système de supervision sous SNMP et installation des outils de supervision.

  -Activation du service SNMP et des paramètres dans chacun des équipements du réseau à superviser (Routeurs, Switch et Firewall).

V.1. Mise en œuvre de plateforme de test :

- Conception de maquettes virtuelles en se servant d'outils de simulation, émulation et de virtualisation permettant de tester et d'illustrer les configurations avec les logiciels (Oracle VM Virtual Box et GNS3).

-Réalisation de test sur la supervision avec l'aide du PRTG (Paessler Router Traffic Grapher) et INFOVISTA.

V.1.1. Conception d'une maquette virtuelle utilisant le logiciel Oracle VM Virtual Box :

Le Virtual Box est un logiciel de virtualisation qui permet de créer des machines virtuelles qui seront utilisées par le logiciel GNS3 comme station de supervision.

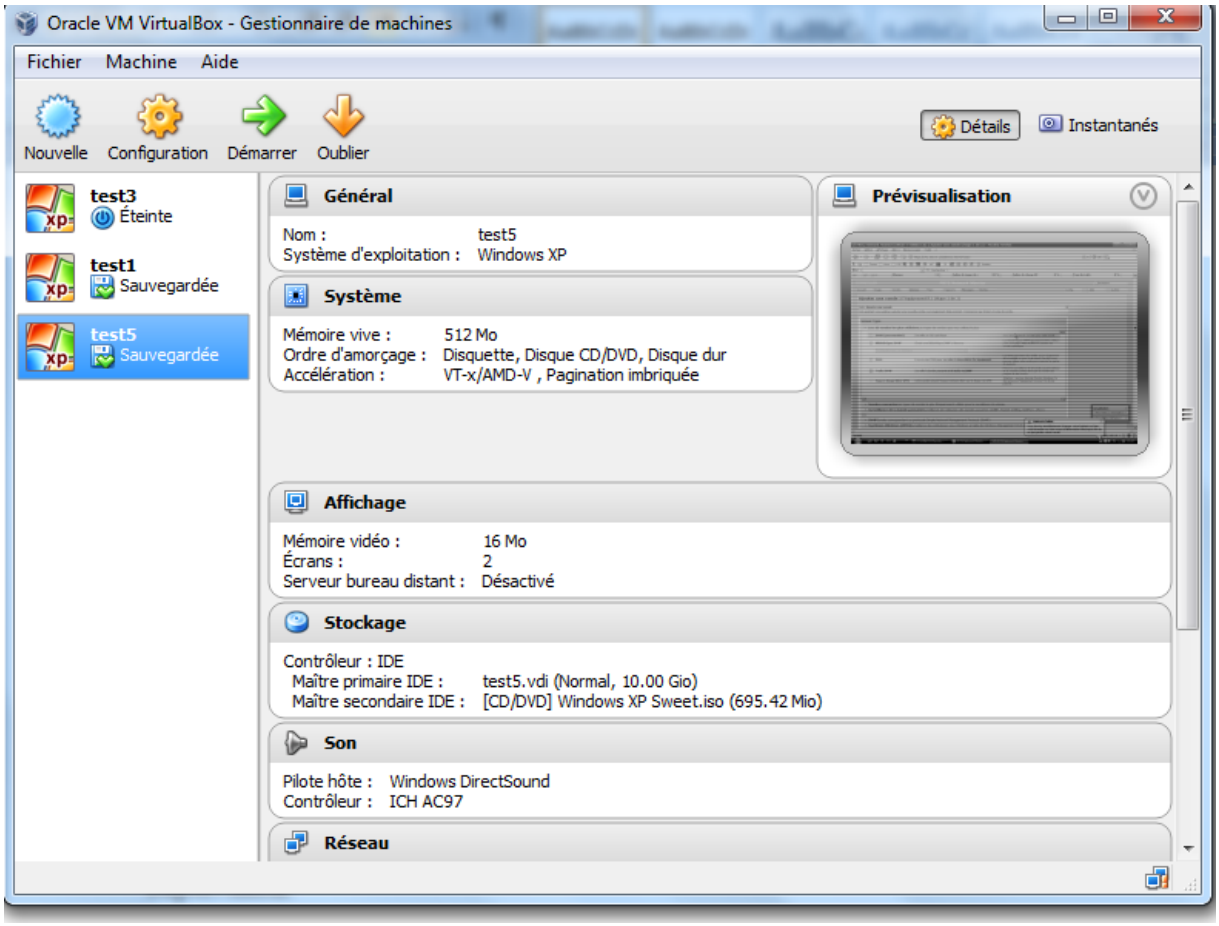


Figure V.1 : l'interface de création des machines virtuelles

V.1.2. Conception d'un réseau virtuel à superviser avec le logiciel GNS3 :

Le logiciel GNS3 est un logiciel de simulation réseaux qui permet de créer des topologies réseaux souhaitées.

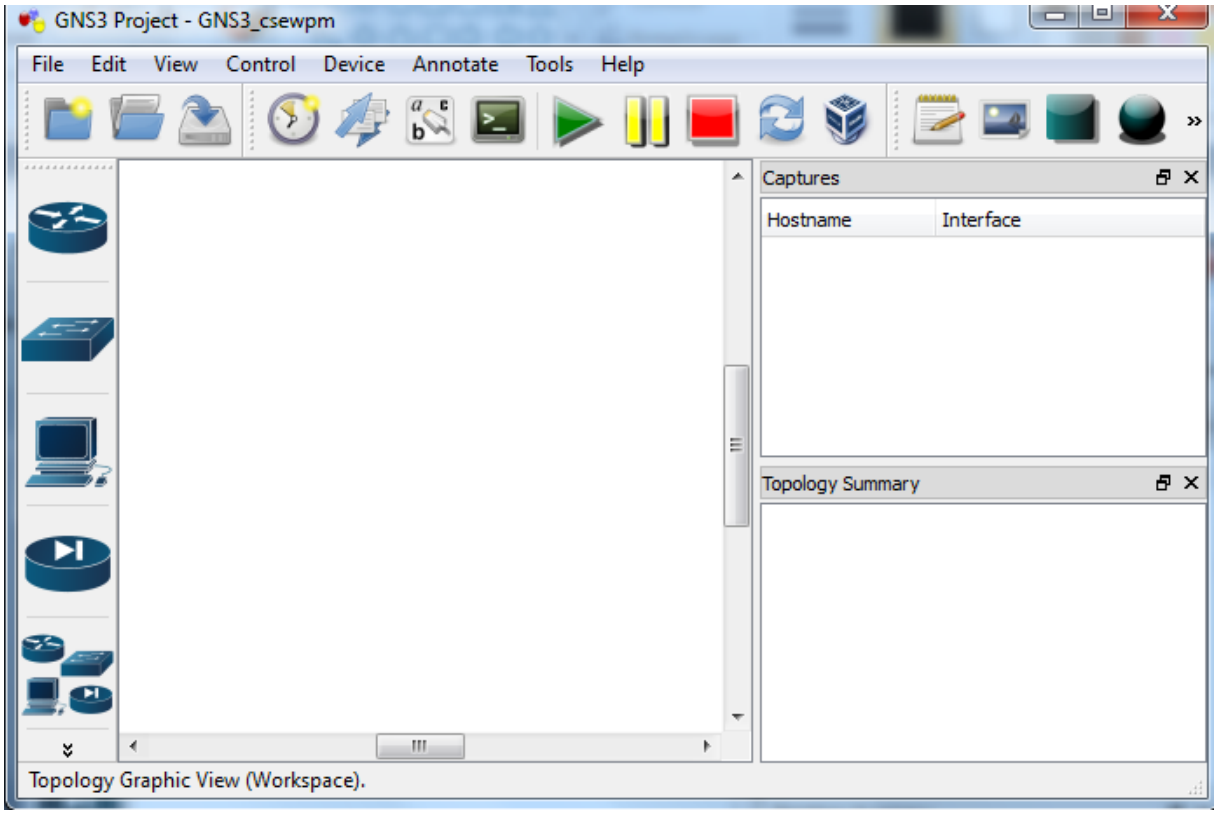


Figure V.2 : L'interface de création de topologie

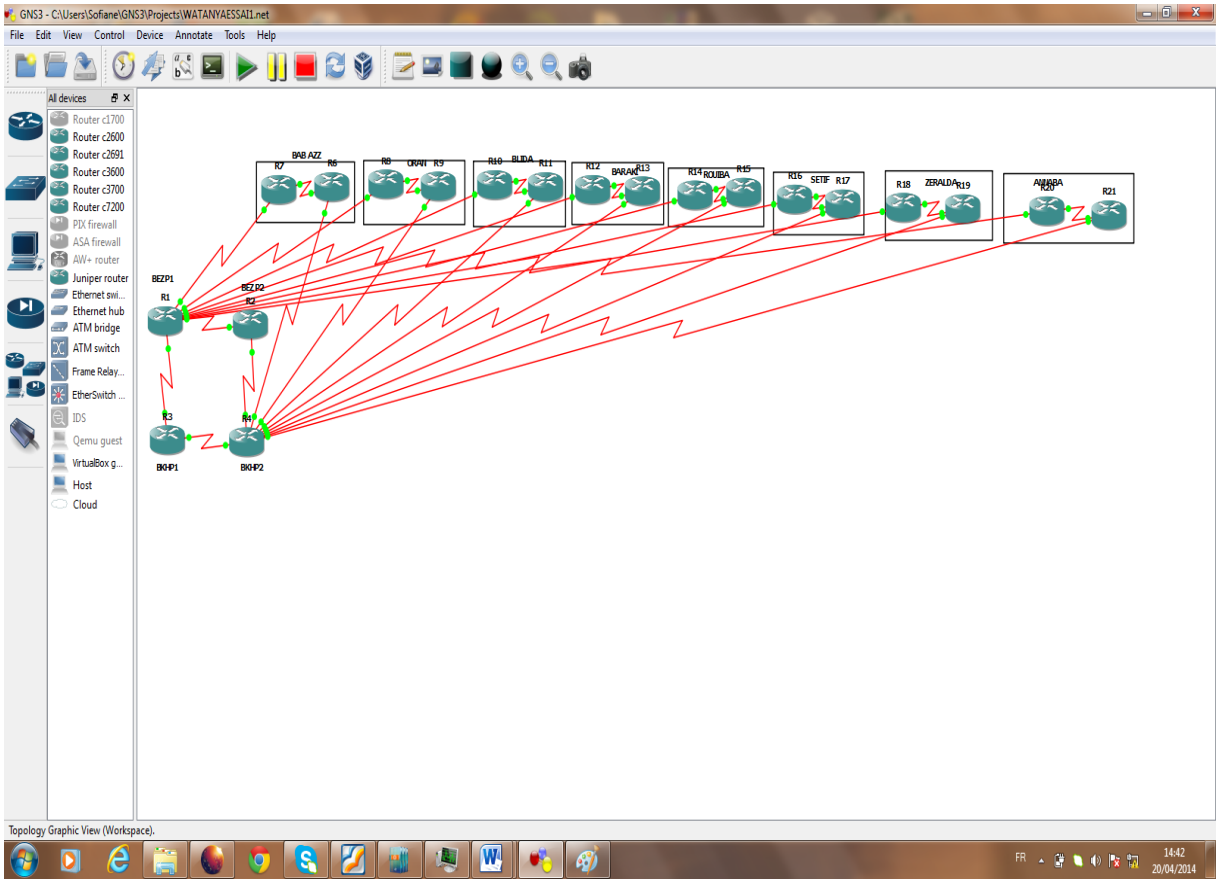
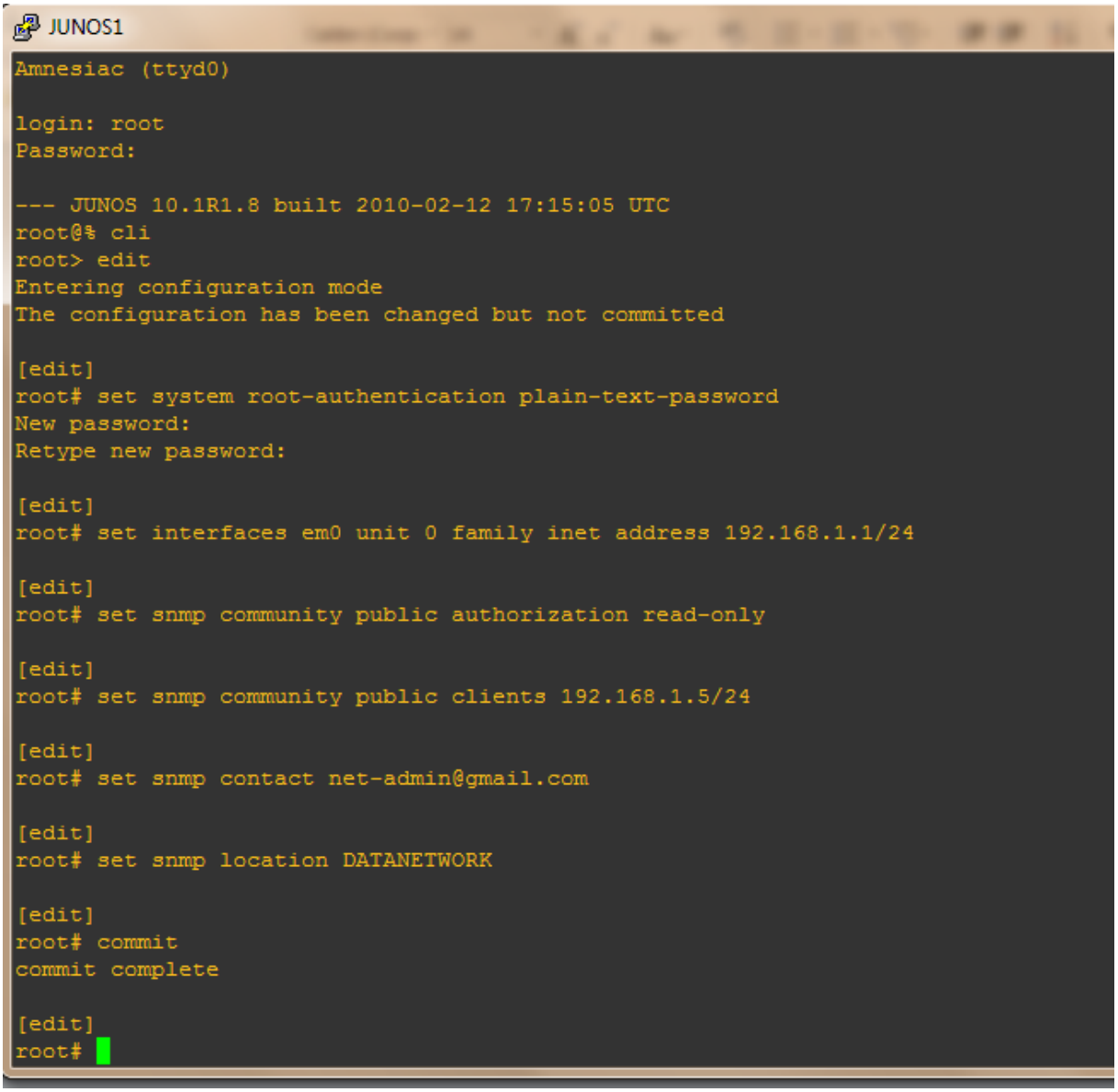


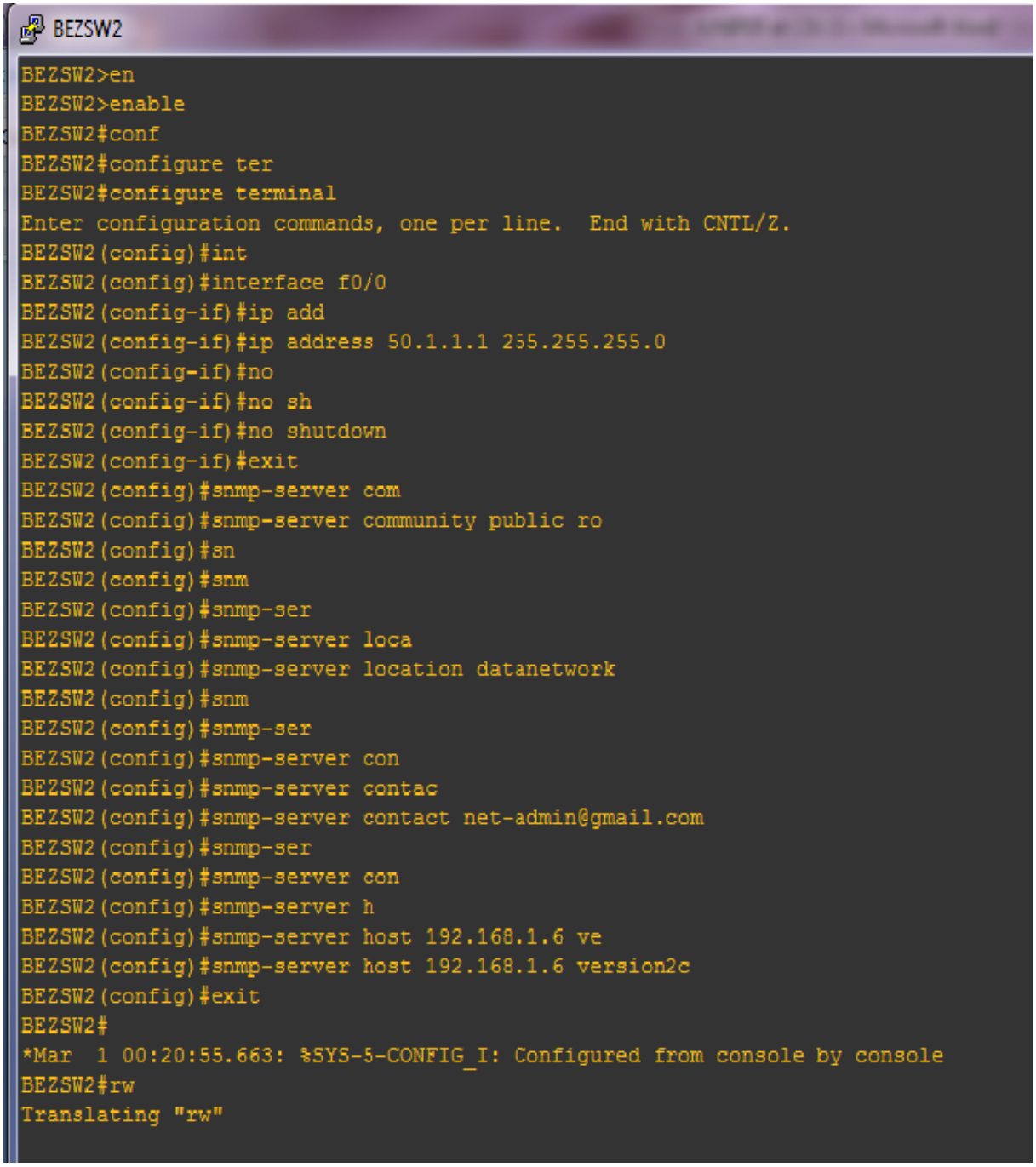
Figure V.3 : La topologie crée

La configuration de l'adresse IP d'une interface et le protocole SNMP sur les équipements suivants:

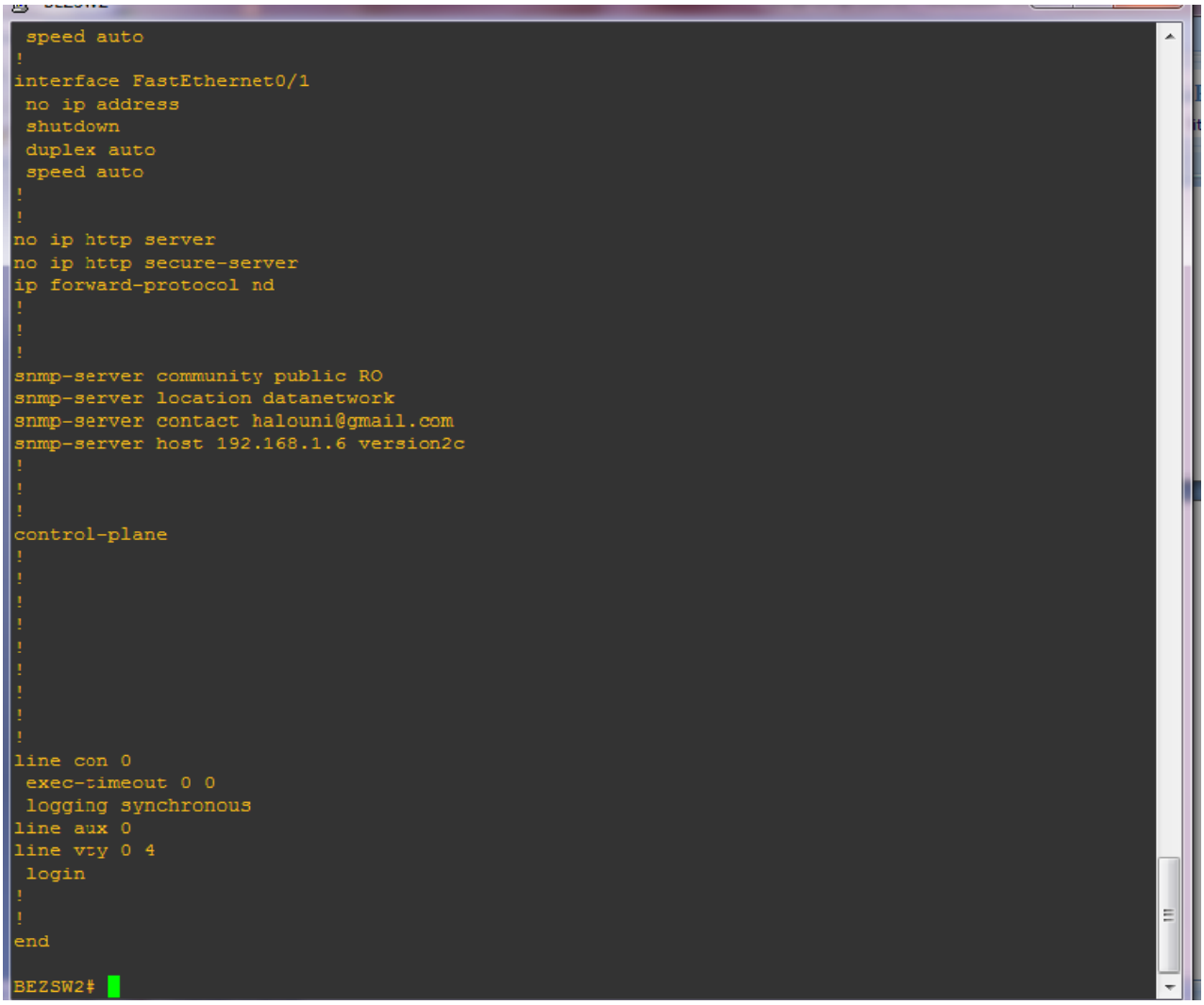
- ✓ **Routeur Juniper :**



- ✓ **Routeur Cisco :**



⇨ Les résultats après configuration du **Routeur Cisco** :



```
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
!
!
snmp-server community public RO
snmp-server location datanetwork
snmp-server contact halouni@gmail.com
snmp-server host 192.168.1.6 version2c
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end

BEZSW2#
```

Après avoir effectué la configuration des différents équipements (routeurs et switchs), nous allons rajoutés une machine virtuelle déjà créé pour faire la supervision de cette topologie en la connectant à l'un des équipements sachant que cette machine doit avoir l'adresse IP configurée dans le protocole SNMP .

A savoir que le logiciel de monitoring (PRTG) sera installé sur cette machine virtuelle.

V .2. Tests de supervision avec l'aide du PRTG :

C'est la première solution de monitoring que nous allons proposer.

V .2. 1. Définition :

Le PRTG (Paessler Router Traffic Grapher) est un logiciel qui supervise l'utilisation de la bande passante, et d'autres paramètres réseau, géré via SNMP. Les informations sont présentées sous forme graphique via une interface Web permettant de visualiser le volume de trafic en fonction du temps, ce qui permet d'identifier les points de charge. PRTG tourne sur une machine Windows dans notre réseau et permet d'enregistrer constamment les paramètres de l'usage du réseau. Les données enregistrées sont par la suite sauvegardées dans une base de données interne pour être consultées ultérieurement. PRTG utilise SNMP pour enregistrer les données de trafic, de charge ou toute autre valeur accessible via SNMP afin de les présenter sous forme graphique dans le temps sur des périodes plus ou moins longues.

Le PRTG est une solution de supervision de réseau en temps réel basé sur le protocole SNMP. Il permet au service informatique d'avoir une remonté d'information quasi instantané lors d'un problème. Malgré un système basé sur le SNMP, PRTG utilise d'autres protocoles ou ressources systèmes pour obtenir un maximum d'information sur les différents éléments du réseau.

V.2.2. Son utilisation :

La gestion de PRTG se fait via une interface WEB avec une adresse IP : 10.54.3.98 (l'adresse du serveur web) avec un port spécifié qui est : 8081 et le serveur PRTG est installé sur un hôte local d'adresse 127.0.0.1, ce qui signifie (pas d'agent distant). Donc pour se connecter en un clic sur «login par défaut », cela nous amène à la page d'accueil qui recense tous les périphériques déjà ajouté.

V.2.3. Ses références :

*PRTG Network Monitor V7

* 1996-2009 Paessler AG

*Burgschmietstrasse 10

*D-90419 Nuernberg, German

⇨ Versions installées:

-Server Service: V7.2.5.5114

-Probe Service: V7.2.5.5114

-Server Administration Tool: V7.2.5.5114

-Probe Administration Tool: V7.2.5.5114

-Import Tool: V7.2.5.5114

V.2.4. Son Interface:

⇨ L'interface WEB principale du PRTG est donnée ci-dessous.

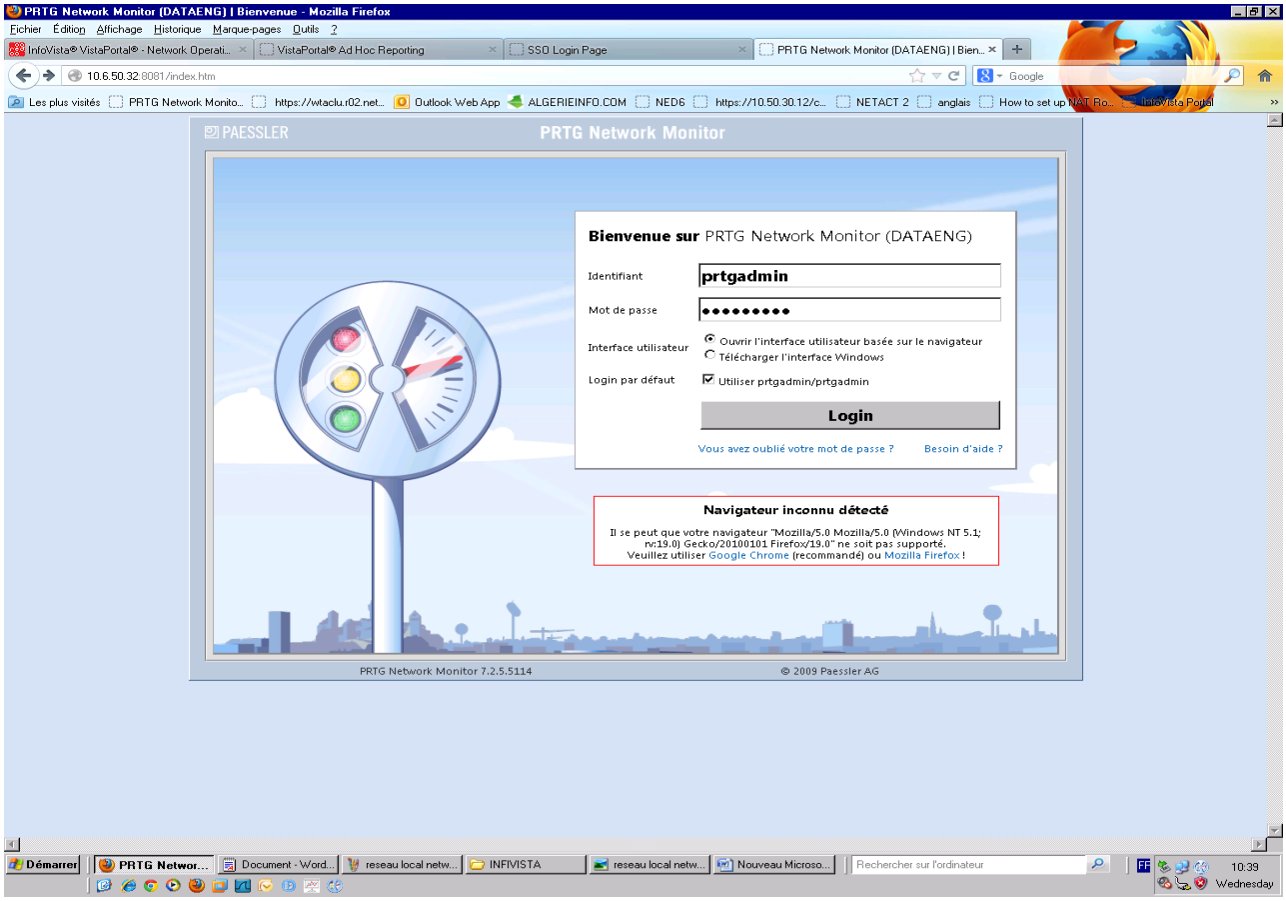


Figure V.4 : L'interface WEB principale du PRTG

⇨ L’interface WEB principale du PRTG: Accès au plan de travail désiré.

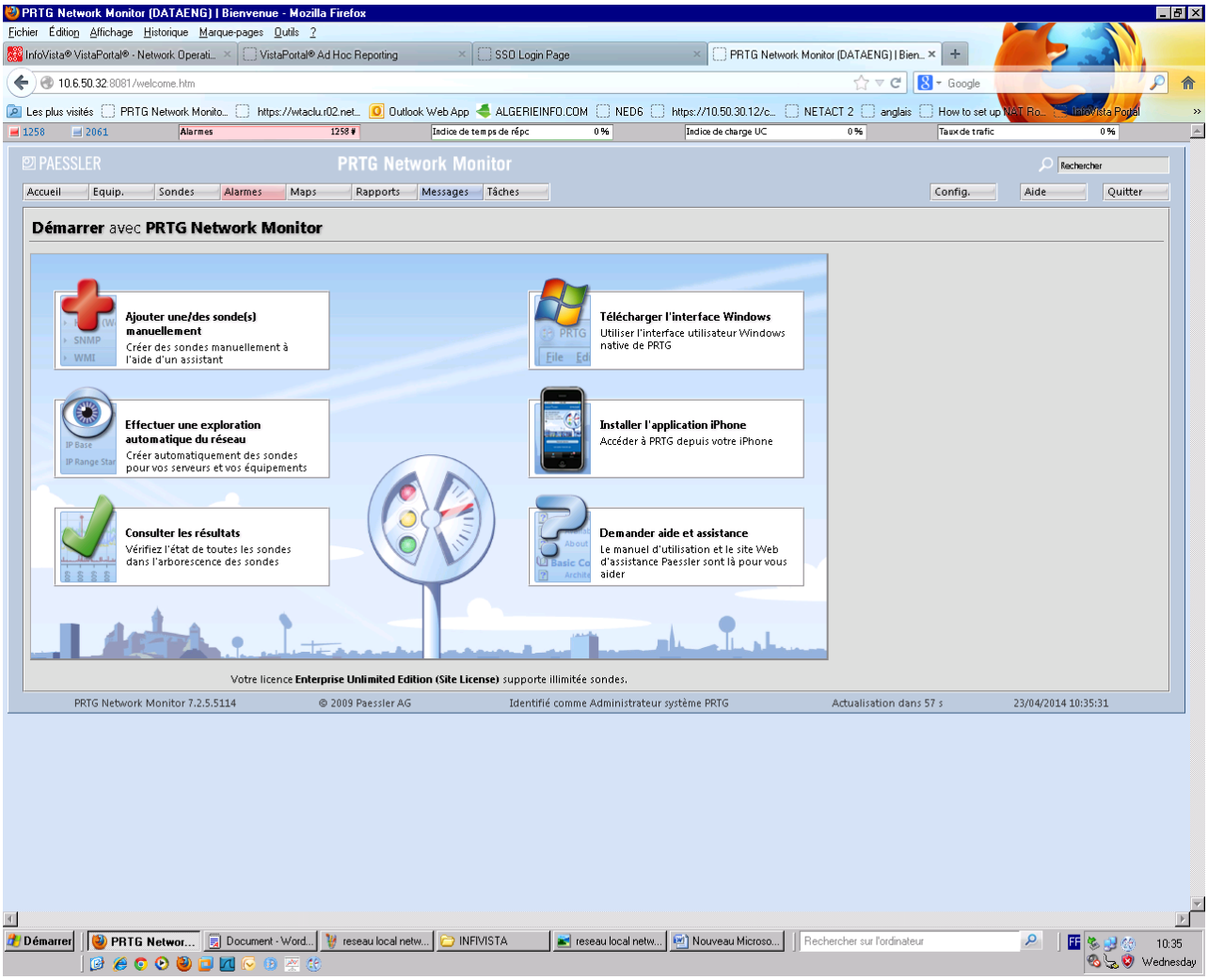


Figure V.5 : Accès au plan de travail de l’interface WEB principale du PRTG

⇨ interface du groupe principale qui contient tous les équipements recensés dans la topologie.

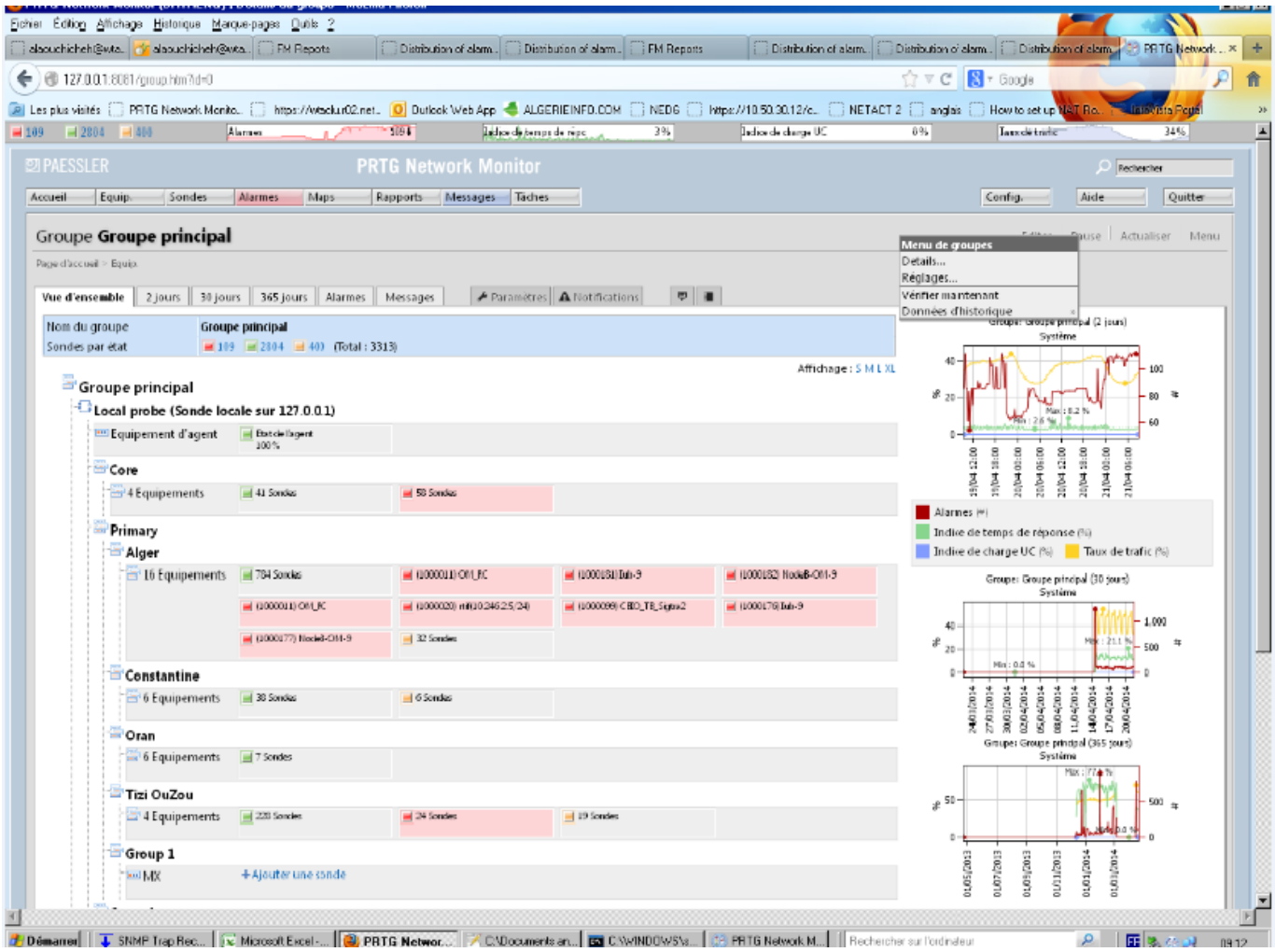


Figure V.6 : Les équipements recensés dans la topologie

- ✓ C'est l'ensemble principal incluant le serveur de supervision.
- ✓ C'est un sous-groupe représentant la supervision de tout le réseau « élevé ».
- ✓ C'est un sous-sous-groupe pour les imprimantes du réseau « élevé ».
- ✓ C'est un capteur ayant pour fonction un simple Ping pour vérifier les connectivités de l'équipement surveillé. C'est un capteur obligatoire et duquel dépends tous les autres capteurs de l'équipement.
- ✓ C'est un récapitulatif de l'état de tous les capteurs.

V.2.5. Sa configuration :

Pour la configuration, on peut rajouter un équipement pour avoir une vue de groupe, ajouter un groupe, ajouter un groupe automatique, trier les groupes, trier les groupes et les équipements.

V.2.5.1.Ajout d'un équipement:

Pour surveiller un périphérique sur certains points, il faut d'abord l'ajouter dans l'interface PRTG :

Sur la page d'accueil, on survole les Périphériques puis on clique sur Ajouter un équipement , on choisit dans quel groupe l'ajouter puis on clique sur poursuivre, puis on rajoute les informations sur l'équipement :

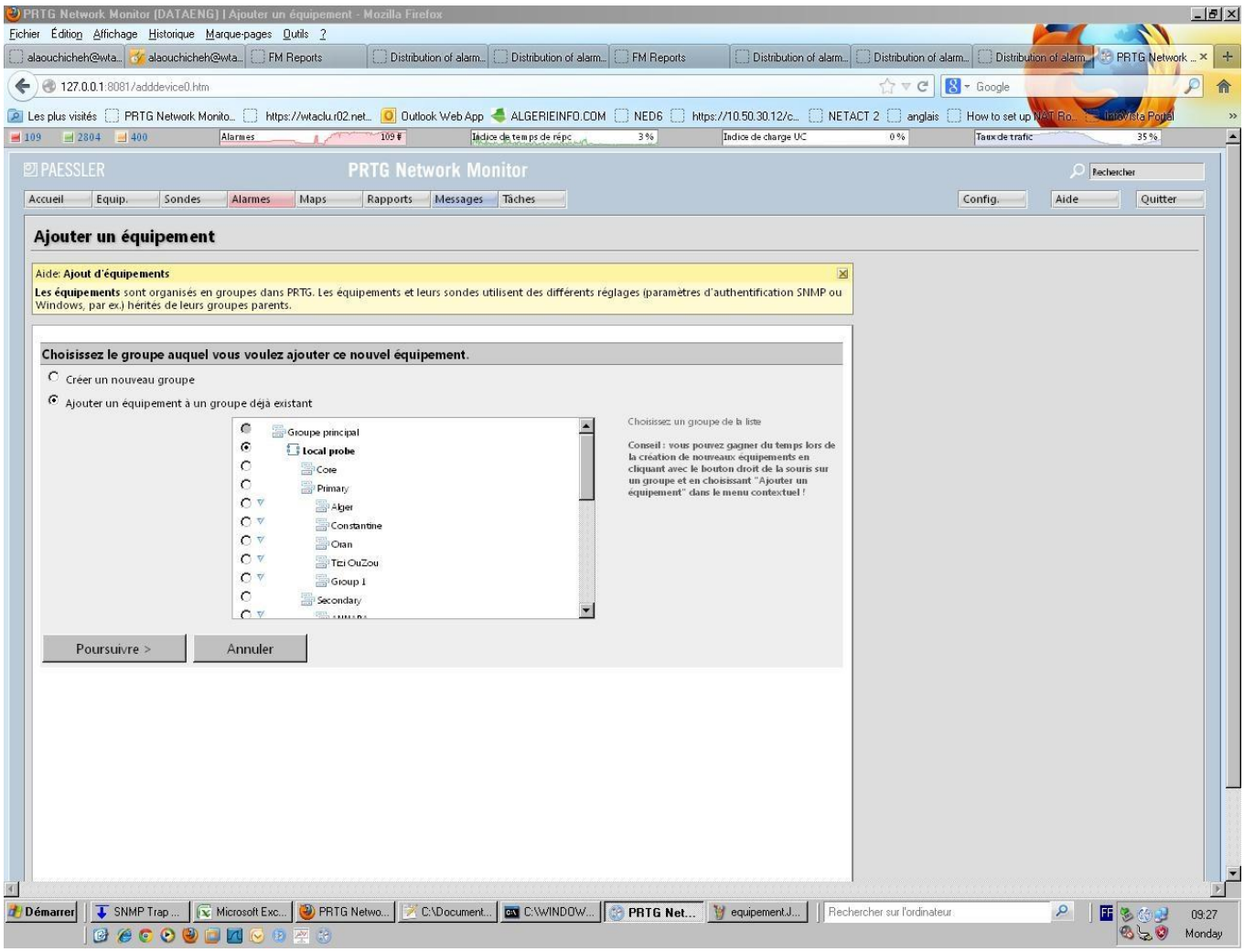


Figure V.7 : Ajout d'un équipement dans un groupe choisi

V.2.5.2. Ajout d'un capteur (sonde):

➢ Configuration de l'agent :

L'agent SNMP qui sera supervisé doit être configuré en fonction du protocole SNMP, c'est-à-dire qu'il doit être ajouté à la même communauté que le superviseur et on doit connaitre son adresse IP.

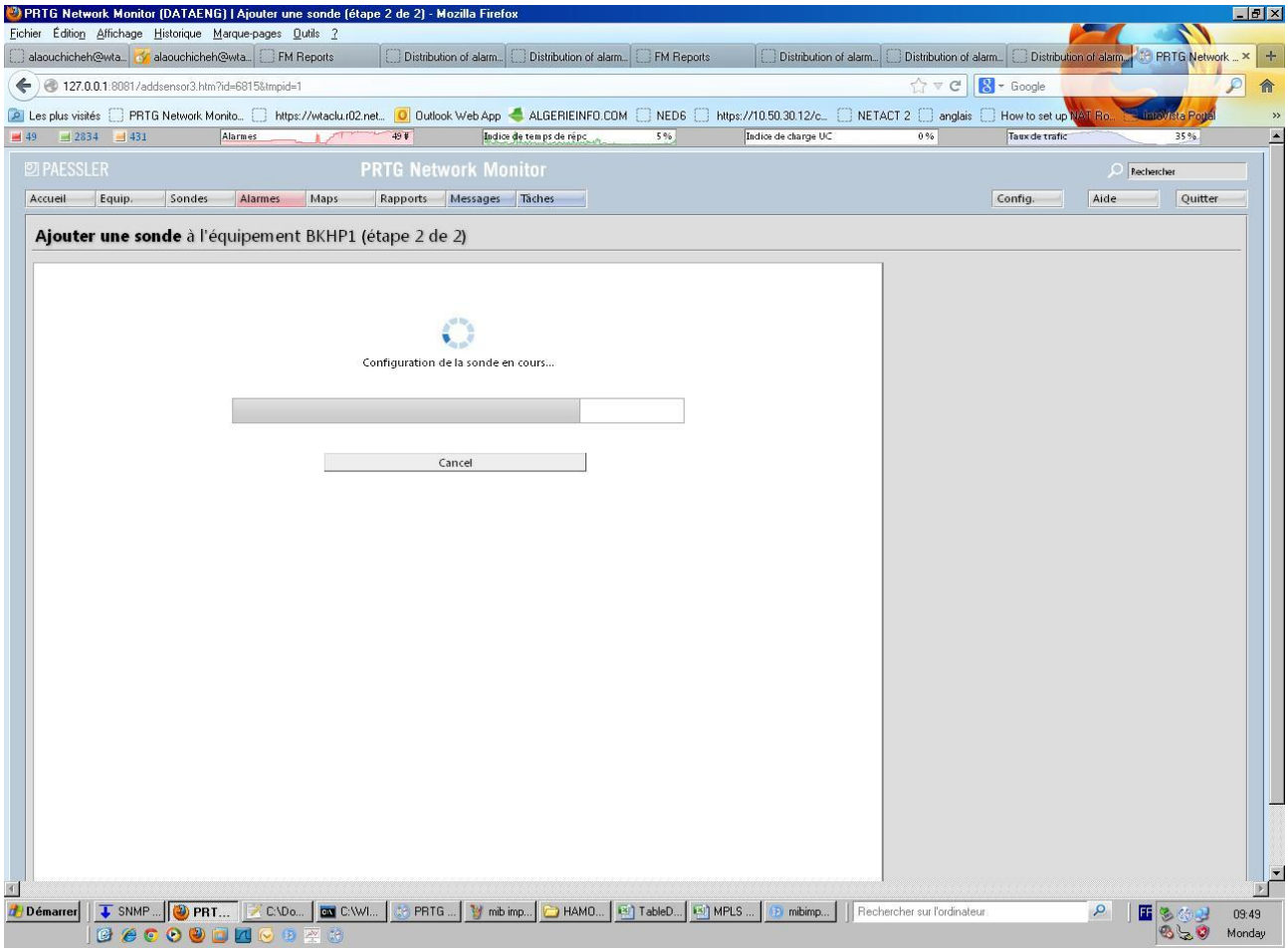


Figure V.8 : Ajout d'une sonde à un équipement

V.2.5.3.Création du capteur :

Les capteurs peuvent être créés de deux façons différentes :

➢ 1ere méthode :

Soit par l'exploration automatique, avec des fichiers MIB (Management Information Base) déjà implémenté dans la solution PRTG, ou par vérification d'informations qu'on pourra

récupérer de l'agent. Le PRTG renvoie une liste de capteurs automatiques dont laquelle il faut sélectionner les capteurs voulus.

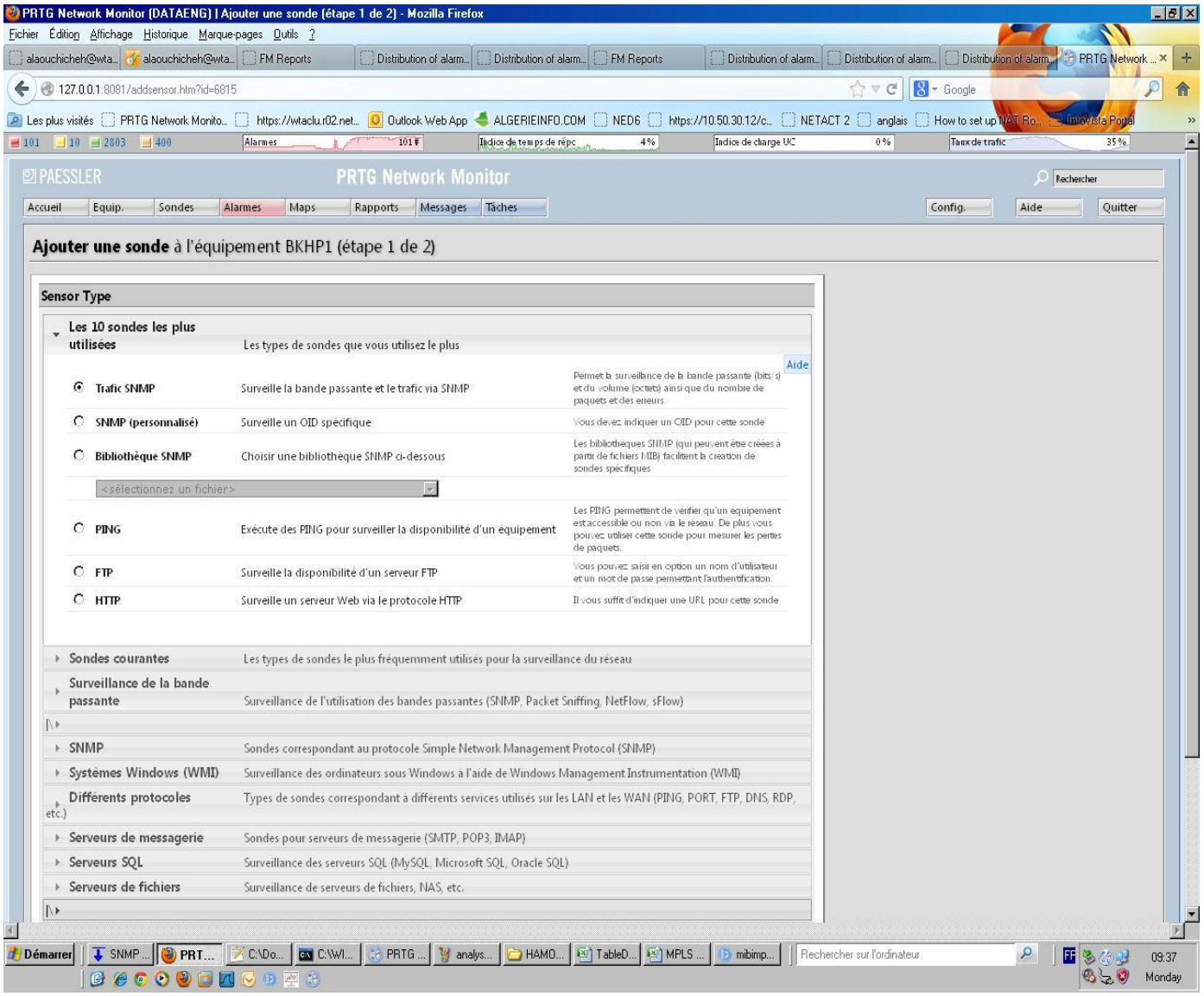
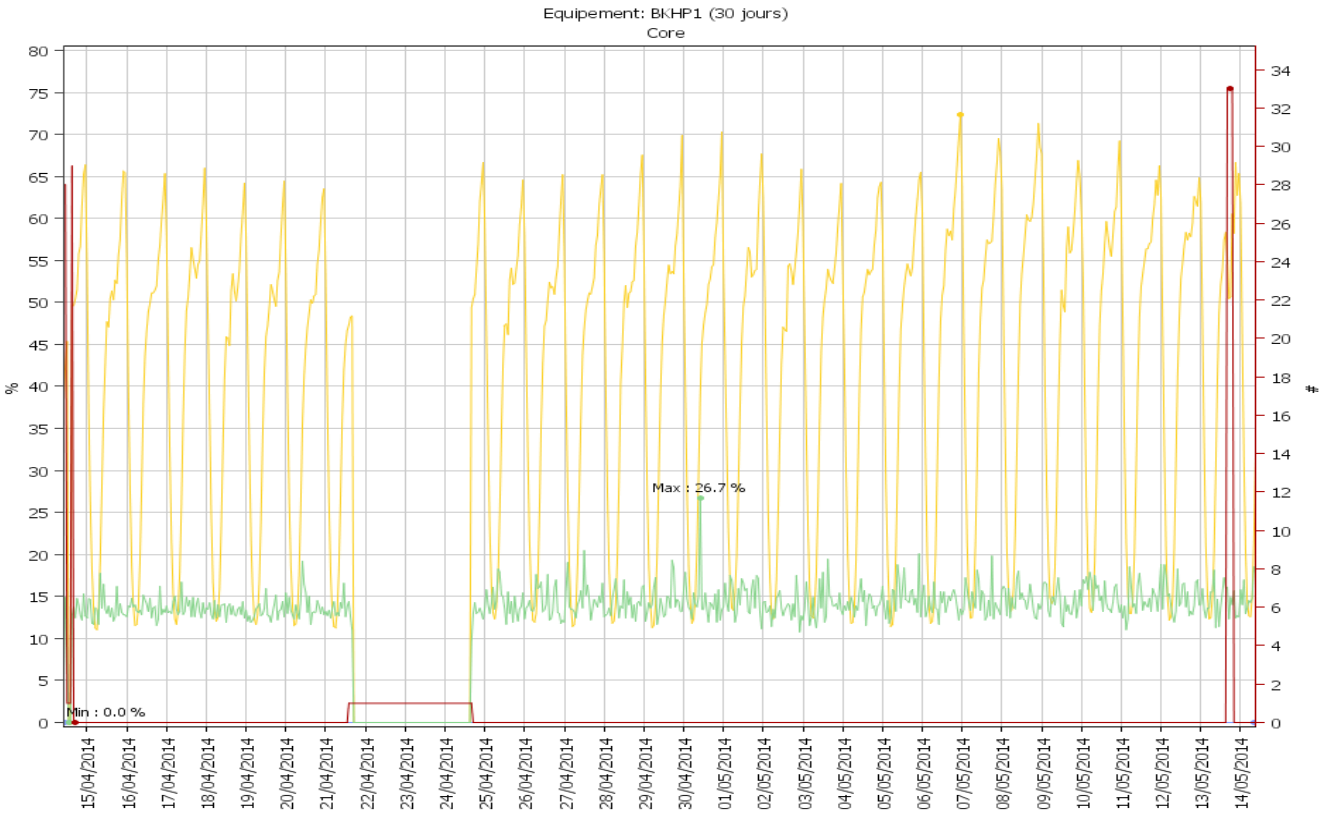


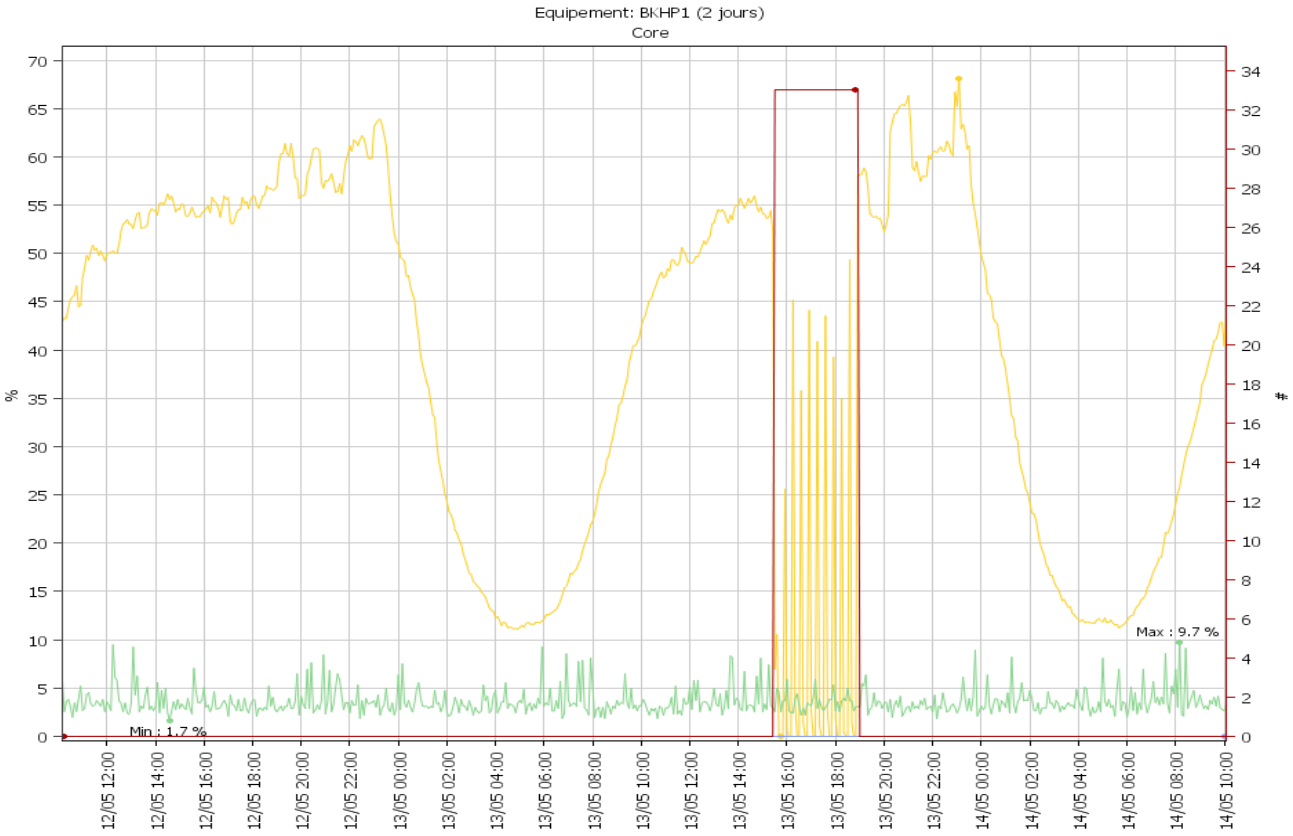
Figure V.9 : Sélection des sondes à rajouter à un équipement

Les résultats de la supervision d'une sonde :

- Données (BKDP1) sur 30jours



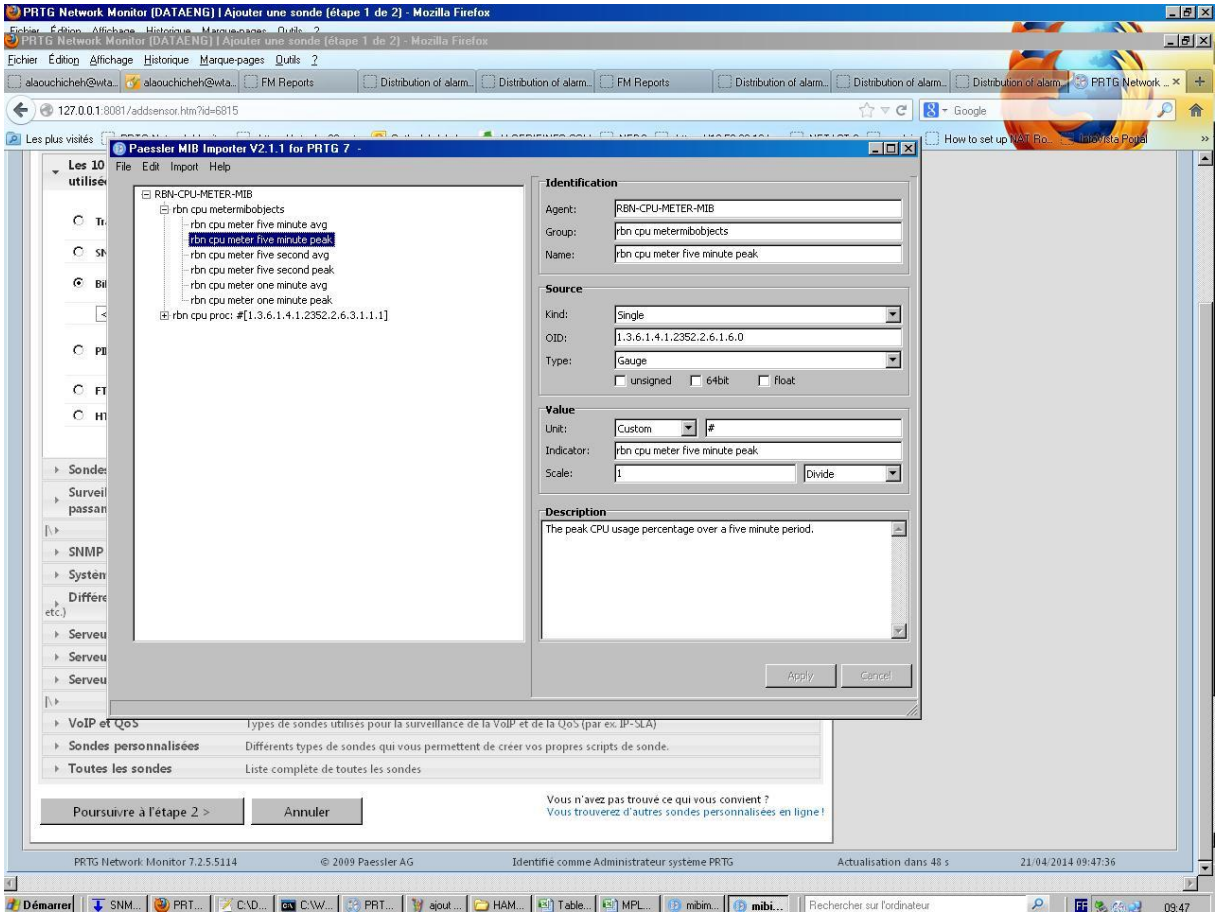
- Données (BKDP1) sur 2jours

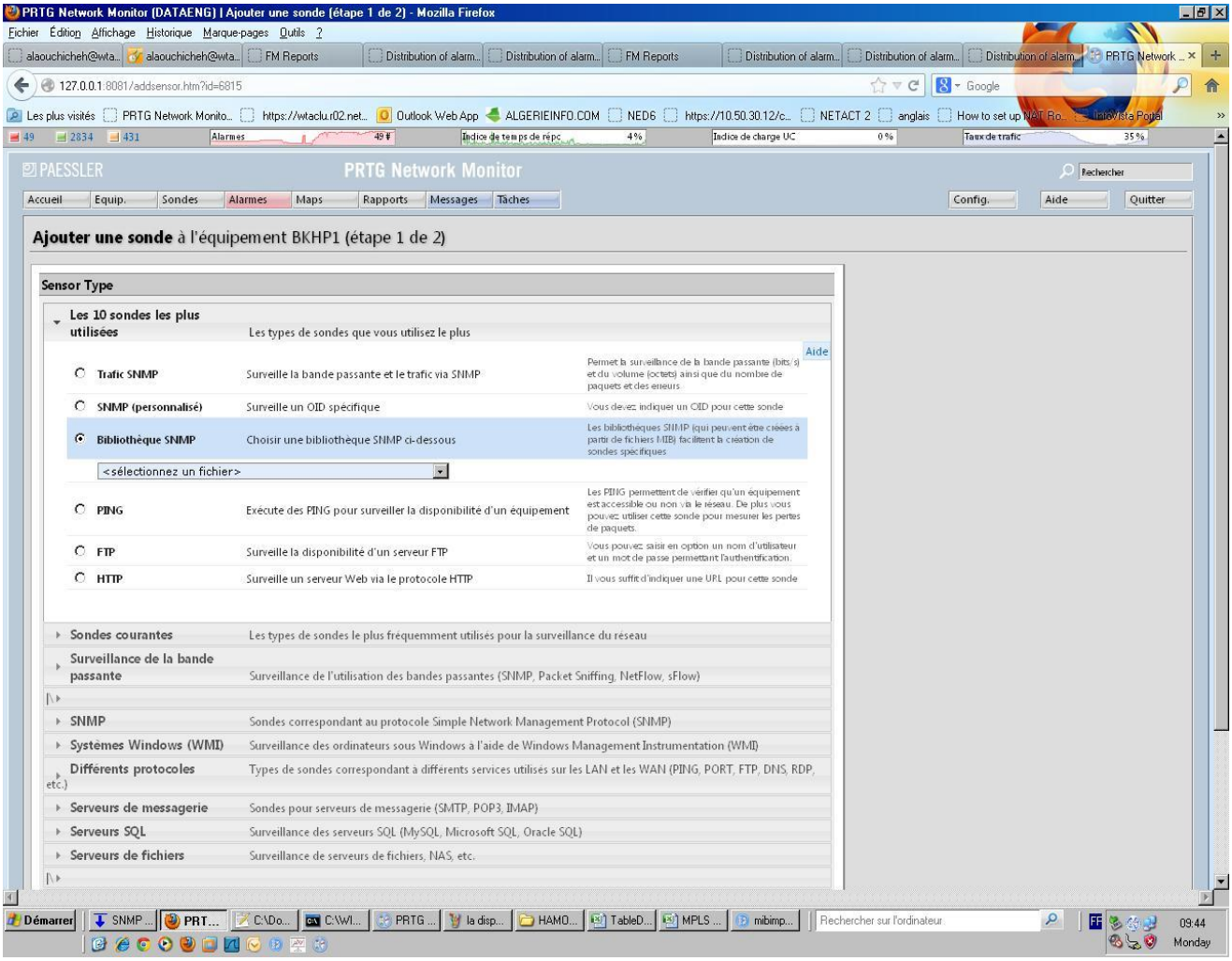


- **2eme méthode :**

Cette méthode consiste à spécifier les sondes qu'on va créer via le protocole SNMP.

- Création de bibliothèque SNMP en utilisons Paessler MIB Importer V2.





Figures V.10 : Importé une MIB pour la bibliothèque SNMP (SSR 8020 Ericsson)

A partir de cette bibliothèque, on utilise les MIB importés pour créer des sondes bien spécifiées comme le CPU d'un équipement, sa RAM et le trafic qui passe dans une interface.

On peut paramétrer une sonde pour quelle renvoie des notifications dans les cas suivants :

- **déclanchement d'état :** s'active lorsqu'une sonde passe à l'état non fonctionnel, cela constitue le cas le plus fréquent d'envoi d'une notification

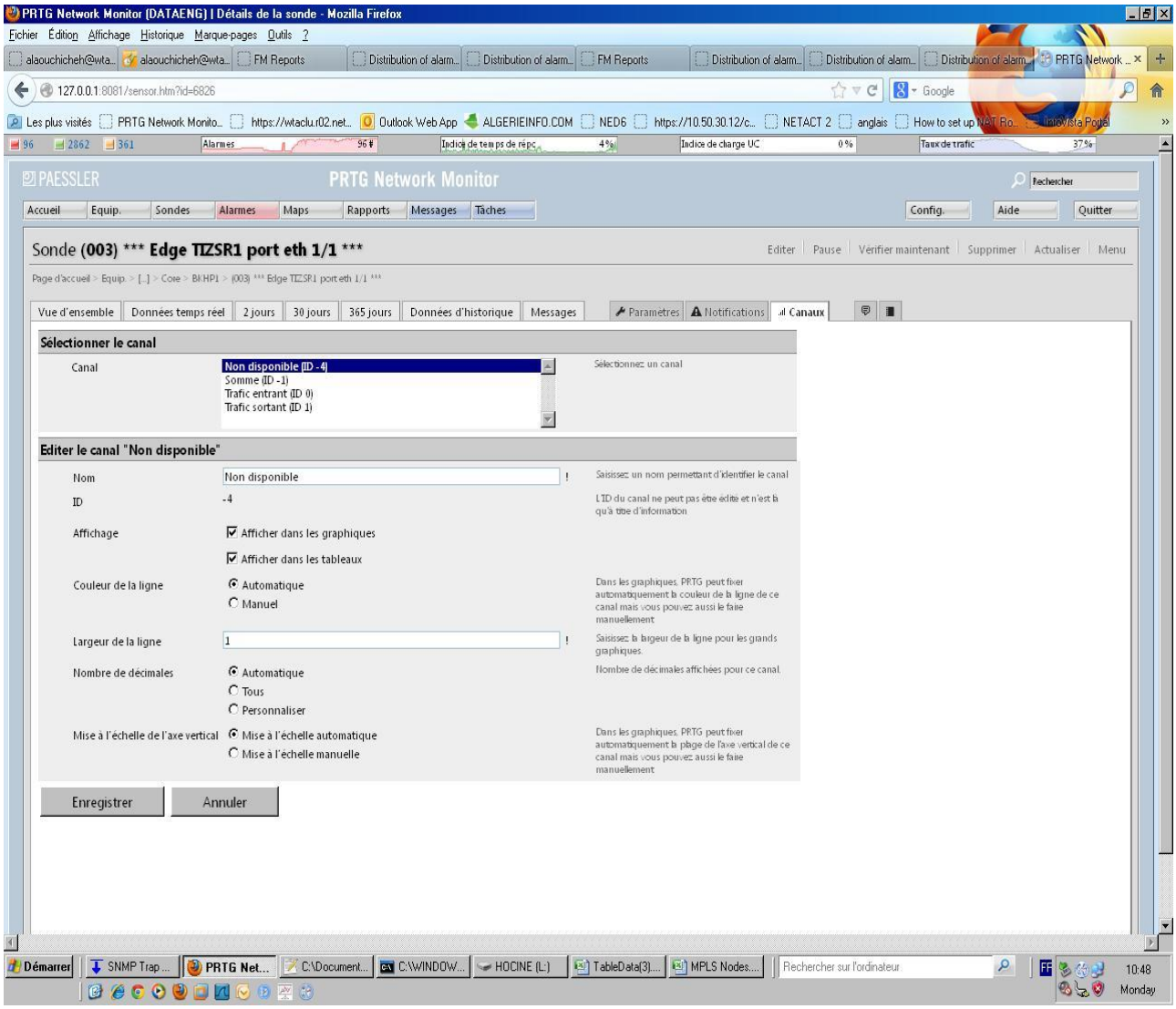
- **déclanchements de débit :** qui nous permet d'envoyer des notifications lorsqu'une sonde de trafic a franchi un seuil de bande passante prédéfini pendant un temps donné.

-**déclenchement(s) de volume :** Les déclenchements de volume vous permettent d'envoyer des notifications lorsqu'une sonde de trafic a franchi un seuil de volume prédéfini pendant un temps donné.

-déclenchement(s) de seuil : Avec les déclenchements de seuil, vous disposez d'une solution souple qui vous permet d'envoyer des notifications lorsqu'une sonde a mesuré certainesvaleurs. Ce type de déclenchement n'est pas disponible pour la sonde actuelle.

-déclenchement(s) de modification : ils sont activés par certaines sondes (par ex. les sondes de fichier ou les sondes de journal des événements) dès lors que le contenu d'un fichier ou du journal des événements a changé.

- **Les Canaux :**



Voici les résultats obtenus en supervisant l'équipement qui se trouve dans la partie Core (BKHP1) :

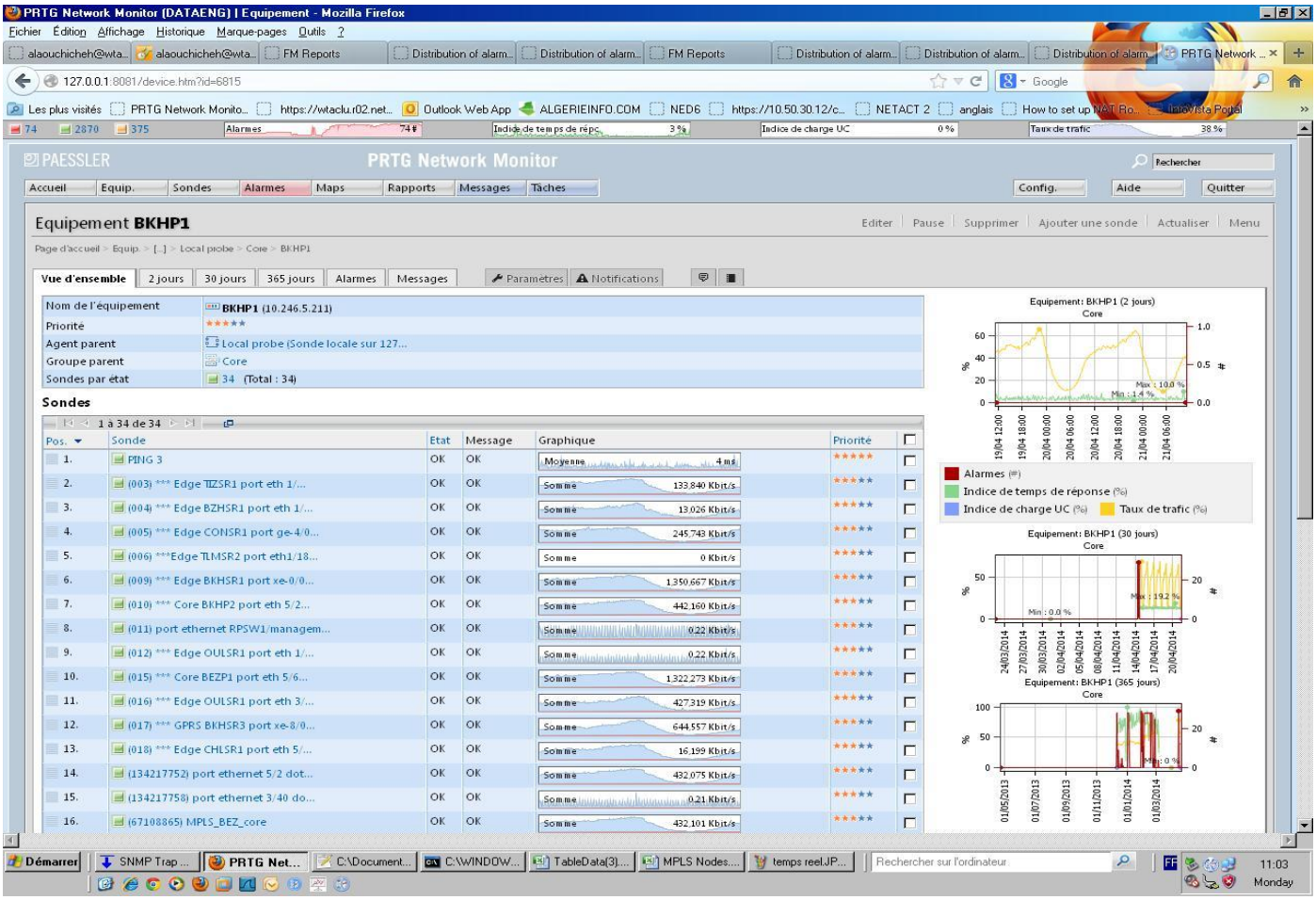


Figure V.11 : Supervision d'équipement de la partie Core (BKHP1)

V.3. Tests de supervision à l'aide du logiciel InfoVista :

C'est la deuxième solution de monitoring que nous allons proposer..

Introduction:

Le management des services et des applications de réseaux nécessitent une assurance d'apporter des solutions et d'avoir une visibilité sur les différentes performances du réseau.

Figure V.12 : Sigle de VistaPortal

Les besoins de l'entreprise Wataniya Telecom Algerie :

- Intégration d'équipement Extreme Sommet X460.
- Intégration d'équipements Ericsson SSR.

V.3.1.Mise en marche :

Le serveur InfoVista est l'un des principaux composants de la Fondation Vista.
Dans cette section, nous allons expliquer brièvement comment un serveur InfoVista interagit avec d'autres composants.
Il est entièrement géré par VistaMart qui assure la centralisation et l'approvisionnement en fournissant :

- ✓ Des Informations sur la topologie, qui indiquent les ressources qui doivent être surveillés.
- ✓ Les mesures, que fait Infovista sur le réseau sont regroupées dans une bibliothèque.
- ✓ Règles d'activation, qui définissent les rapports et les données à recueillir.

Une fois VistaMart a synchronisé ses informations avec un serveur InfoVista sur le modèle de topologie, le serveur InfoVista peut commencer le sondage de données sur les ressources du réseau (dispositifs, les interfaces, les applications, etc…), et pousser les données vers le

référentiel VistaMart. Il agrège ensuite les données conformément à un modèle d'information et met à la disposition des applications possibles VistaPortal et Vista360 (client Web).

Le diagramme au-dessous résume les flux de données au sein de la l'architecture centrale InfoVista.

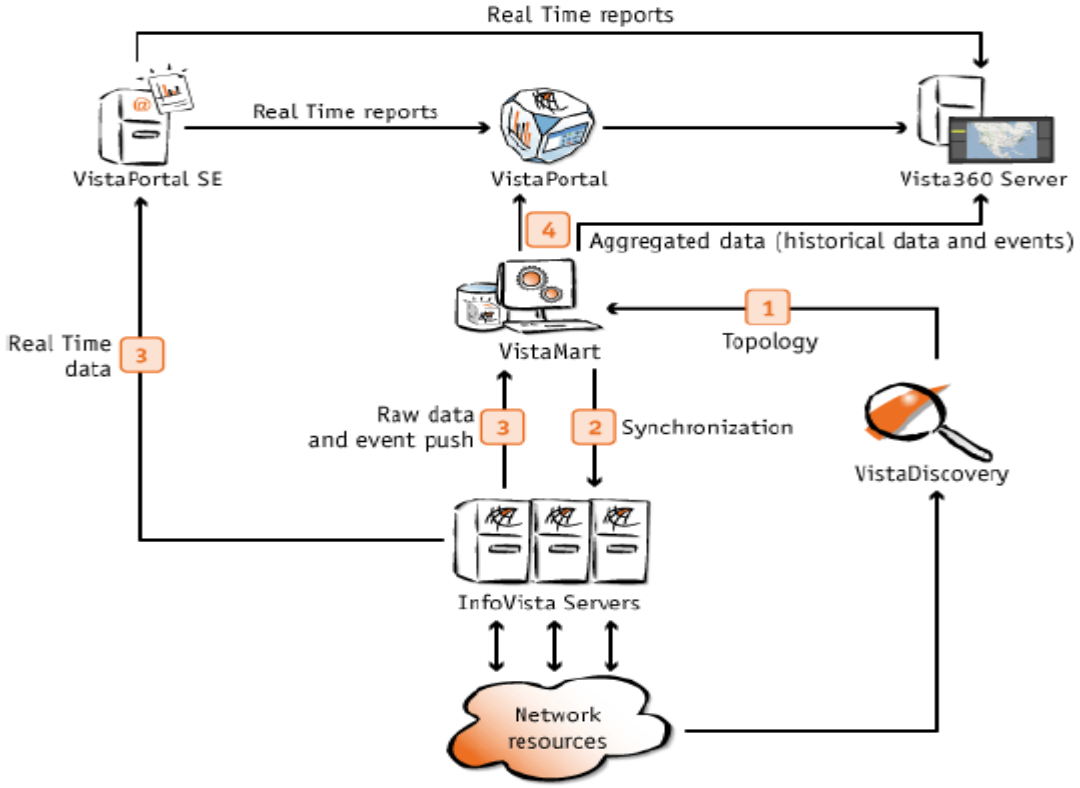


Figure V.13 : Les flux de données de l'architecture centrale d'InfoVista

VistaMart obtient des informations de topologie de Vista Discovery ou d'un appareil externe source de topologie.

VistaMart synchronise avec le serveur InfoVista les informations nécessaires sur les ressources du réseau à surveiller (topologie, modèle d'information).

InfoVista Server démarre et scrute et pousse des données brutes à VistaMart sur les ressources surveillées.

Le serveur InfoVista fait des rapports en temps réel disponibles sur la demande de VistaPortal SE à VistaPortal et Vista360.

VistaMart agrège les données reçues à partir du serveur et rend InfoVista disponible à VistaPortal et Vista360.

V.3.2. Installer un serveur InfoVista:

Le package d'installation contient le logiciel InfoVista (serveur et client) que nous pouvons installer sur différentes versions de plates-formes comme illustré dans le tableau ci-dessous :

Platform	Microsoft Windows® 64bit	Sun Solaris®	Red Hat Linux®
Release	Windows 2008	Solaris 10	Red Hat Linux 5.2

On peut installer une ou plusieurs instances du serveur d'InfoVista (ou services) sur la même plate-forme, en fonction de dimensionnement des exigences désirées.

- **Environnements virtualisés :**

VMWARE InfoVista Server prend en charge les environnements virtualisés avec VMware. Par exemple, nous pouvons installer plusieurs serveurs InfoVista sur un ordinateur de plate-forme Microsoft et sur une plate-forme Linux qui résident sur la même machine physique contrôlée par un hyperviseur VMware:

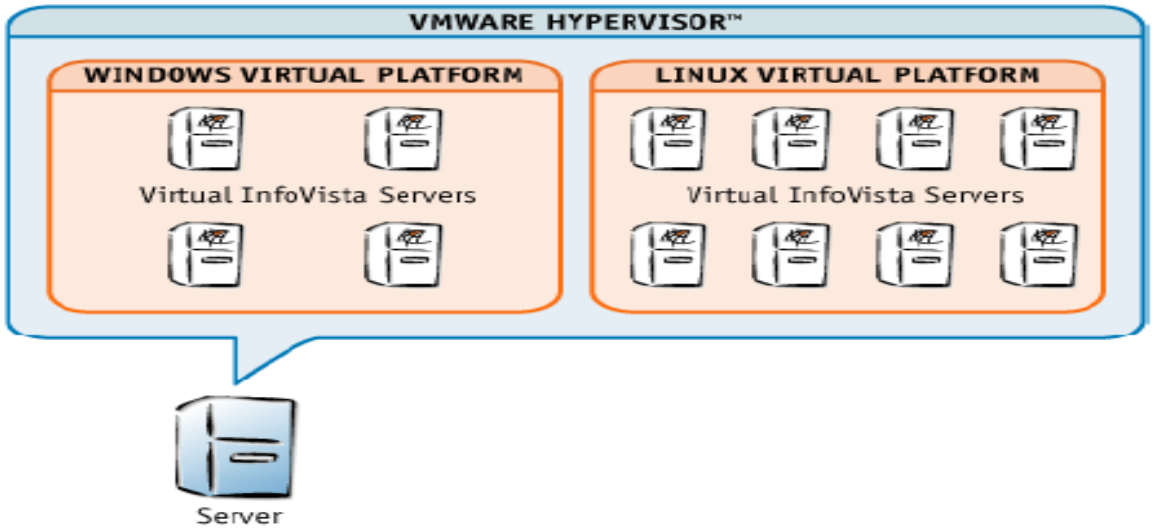


Figure V.14 : Le hyperviseur VMware

V.3.3. Fonctionnement d'InfoVista Server :

Une fois qu'on a installé et configuré le serveur InfoVista dans un environnement Fondation Vista, comme ça le service Serveur InfoVista est synchronisé avec VistaMart. On

n'a aucune tâche opérationnelle à faire, InfoVista serveur fait automatiquement les sondages de données des ressources du réseau et pousse l'information à VistaMart.

V.3.4. Dépanner un Server InfoVista :

Le Cockpit Vista est conçu pour surveiller les autres composants de la Vista Foundation. Selon les alertes Vista Cockpit soulevées sur un serveur InfoVista, nous pouvons utiliser les rapports de la bibliothèque InfoVista améliorés ainsi que des signaux et des traces observées par InfoVista Server.

V.3.5. Que peut ont faire avec InfoVista Server ?

Nous pouvons créer nos propres bibliothèques comme des ensembles d'indicateurs, des propriétés, des règles et des modèles de rapports que nous concevons à nos besoins. Pour apprendre à concevoir des bibliothèques de l'application Client InfoVista Server, on fait appel à IVReport.

Il y a un ordre spécifié d'installation et de mise à niveau des produits de la fondation Vista (dont InfoVista Server fait partie) pour qu'ils fonctionnent ensemble correctement. L'ordre de l'installation diffère de l'ordre de mise à niveau.
L'installation ou la mise à niveau des produits de la Fondation Vista selon l'ordre indiqué dans le tableau ci-dessous:

Order	Installation	Upgrade
1	VistaCockpit	VistaCockpit
2	VistaMart	VistaPortal
3	VistaDiscovery	VistaDiscovery
4	InfoVista Server	InfoVista Server
5	VistaPortal	VistaMart

- **VistaCockpit :**

Vista Cockpit, nous permet de surveiller, configurer et dépanner les différents produits InfoVista installés sur notre plate-forme.

Vista Cockpit nous aide à:

-Centraliser et planifier les tâches InfoVista.

-Surveiller la disponibilité de VistaFoundation.

-Mettre en œuvre des procédés à haute disponibilité.

-Accéder au centre de tous les produits InfoVista installés (documentations simplifiées pour le dépannage).

- **Vista Mart:**

VistaMart est la partie centrale de la VistaFoundation qui rassemble les données de serveurs InfoVista et les centralisent pour l'analyse et le stockage ultérieur dans son référentiel.

Les principales fonctions de VistaMart sont les suivantes:

• La gestion des fichiers de topologie et de synchronisation des serveurs InfoVista.

• Distribution des cas suivis sur plusieurs serveurs InfoVista.

• La centralisation et l'agrégation des données.

• La centralisation des événements de serveurs InfoVista et la génération d'événements pour l'affichage.

• Fourniture d'échantillons de données et des valeurs agrégées pour VistaPortal (rapports).

- **Vista Discovery** :

Vista Discovery est l'élément de première ligne dans l'architecture InfoVista.

⇨ Les objectifs principaux qui définissent le rôle de Vista Discovery :

- Associer les périphériques contrôlés avec InfoVista .

• D'une part nous soumettrons des adresses IP ou des fichiers de topologie existante provenant à partir d'applications tierces à Vista Discovery.

• D'autre part, nous fournirons et validerons les listes des modèles de rapport pour identifier les types de ressources.

• Vista Discovery réconcilie les deux listes et les dispositions de VistaMart avec un consolidé de liste de ressources (équipements de réseau, applications et serveurs) pour qui relèvent les modèles disponibles. Les rapports sont ensuite publiés sur Vista Portal.

- ✓ Enquête sur l'équipement spécifique en profondeur.
- ✓ VistaDiscovery fonctionne sur une connexion TCP/IP.
- ✓ VistaDiscovery Server fournit référentiel VistaMart et/ou serveurs InfoVista avec le fichier de topologie.

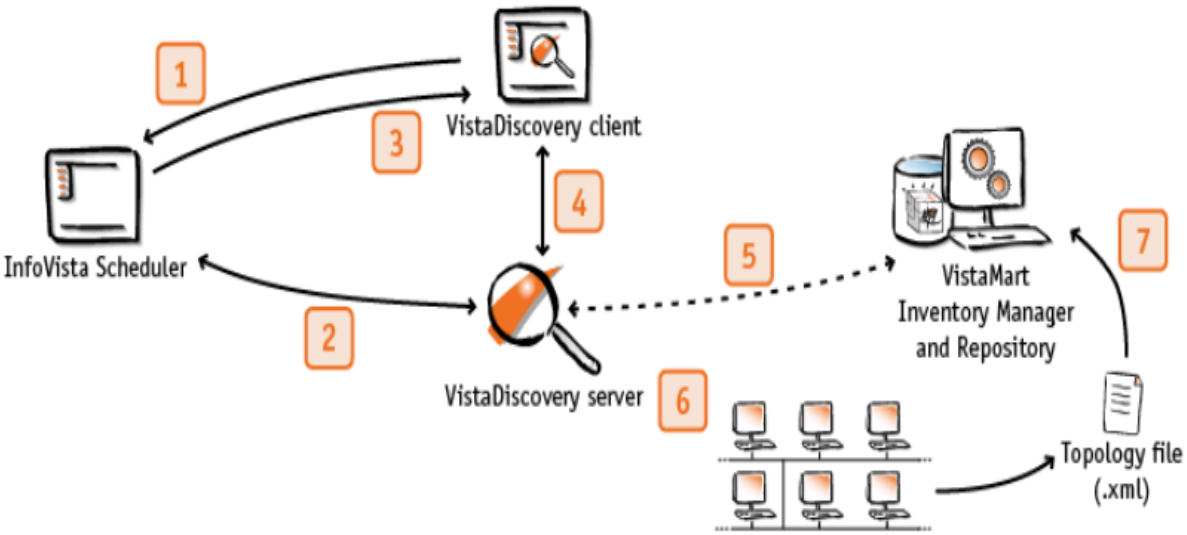


Figure V.15 :Architecture de VistaDiscovery

➢ VistaPortal:

VistaPortal et VistaPortal Standard Edition (SE) sont les deux modules de présentation de la VistaFoundation. La VistaFoundation est une collection de produits InfoVista qui travaillent ensemble, comme illustré ci-dessous, de fournir des rapports sur le rendement des infrastructures IT.

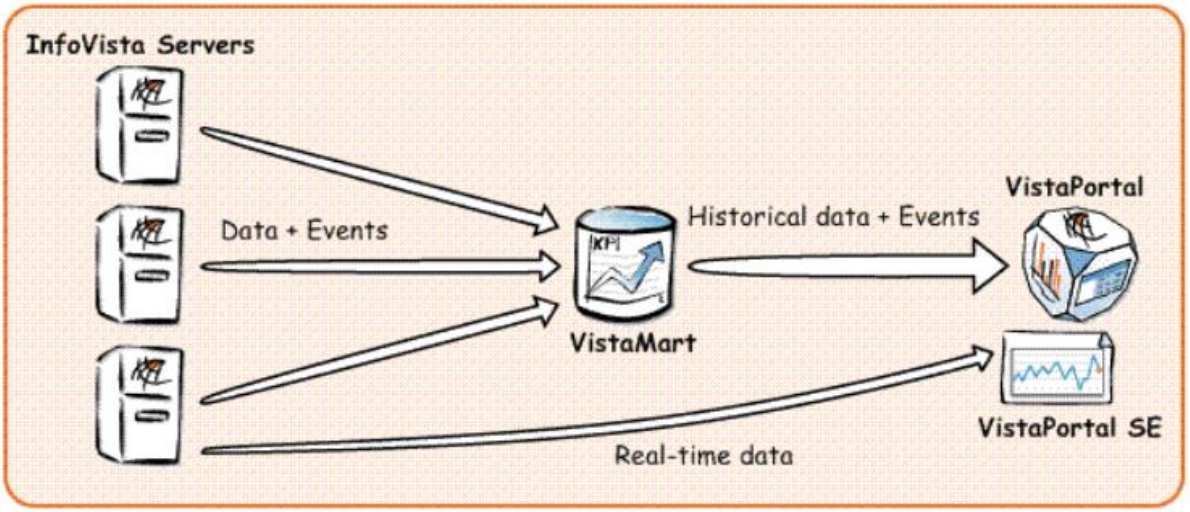


Figure V.16 : Architecture de VistaFoundation

VistaPortal récupère les données de performance historiques de VistaMart, qui traite des données recueillies à partir de serveurs InfoVista et calcule les mesures dérivées.

D'autre part, VistaPortal SE, qui est installé avec VistaPortal, récupère les données en direct en temps réel directement à partir des serveurs InfoVista.

Les deux VistaPortal et VistaPortal SE présentent les données à l'utilisateur dans les différents rapports et les formats à l'aide d'une interface Web. Ces rapports peuvent être personnalisés ou pré-emballés comme solutions de reporting.

Rapports VistaPortal SE sont appelés rapports instantanée, par opposition au rapport de VistaPortal.

- **Infovista 360:**

La gestion et l'exploitation peuvent facilement créer des tableaux de bord Ad-hoc afin de visualiser des données InfoVista en utilisant des interfaces utilisateur simple.

Exemples de profils d'utilisateurs:

• Les gestionnaires de services dans les centres d'opérations de service (SOC) qui ont besoin de prêter attention à des situations particulières client/service.

• Les gestionnaires qui veulent garder un œil sur une activité critique (clients ou services) afin d'assurer la prise de décision proactive.

• Les utilisateurs finaux qui ont besoin d'un accès fréquent aux données InfoVista pour répondre aux questions au jour le jour.

• Le personnel opérationnel qui ont besoin de fonctions de dépannage avancées et l'accès rapide aux données.

V.4 : Identification des besoins

Notre application a pour objectif de développer un outil qui facilite la supervision et la maintenance des composants du réseau. Ceci en mettant en place une plateforme de travail collaboratif qui va permettre de :

- ✓ Echanger des notifications entre les utilisateurs.
- ✓ Planifier des taches dans l'agenda.
- ✓ Gestion des Hardwares et softwares.
- ✓ Gérer la plateforme pour l'administrateur général (ajout, suppression, modification, réaffectation…).

V.4.1 : Diagramme de contexte :

Le diagramme de contexte est un modèle conceptuel qui permet d'avoir une vue globale des interactions entre le système et les liens avec l'environnement extérieur. Il permet aussi de bien délimiter le domaine d'application.

Dans notre cas le diagramme de contexte est le suivant :

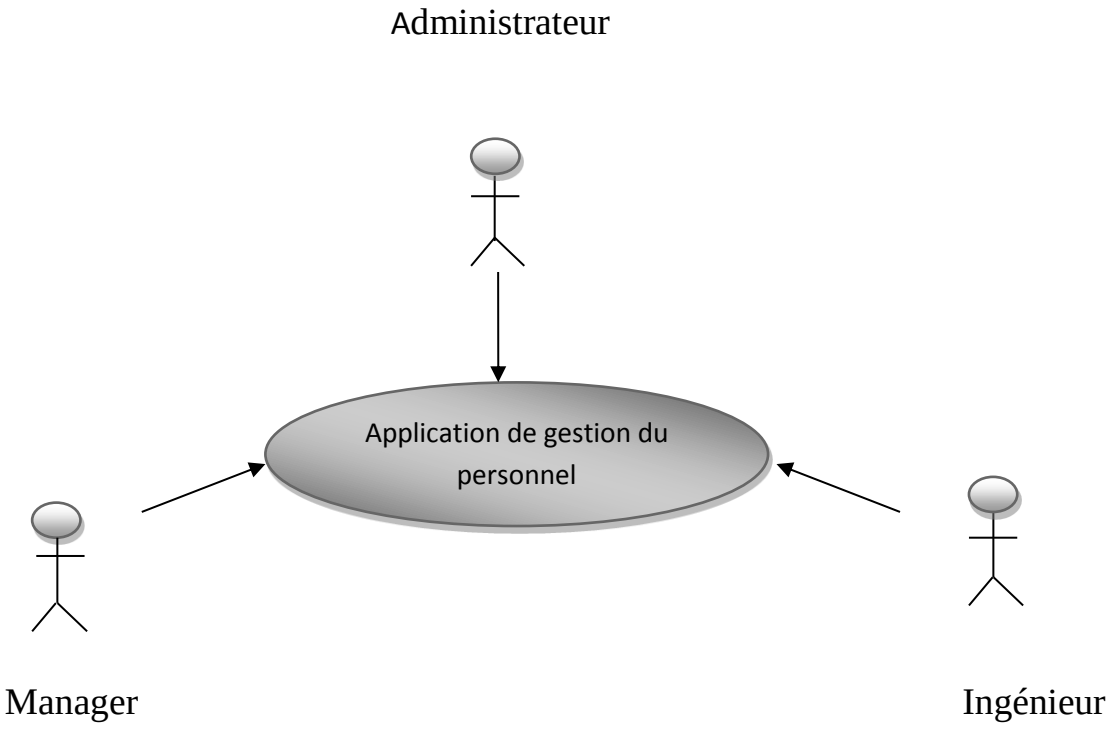


Figure V.17 : Diagramme de contexte de l'application

V.4.2 : Environnement de développement :

En matière d'environnement de développement, le marché offre un choix très large. Pour la réalisation de notre application.

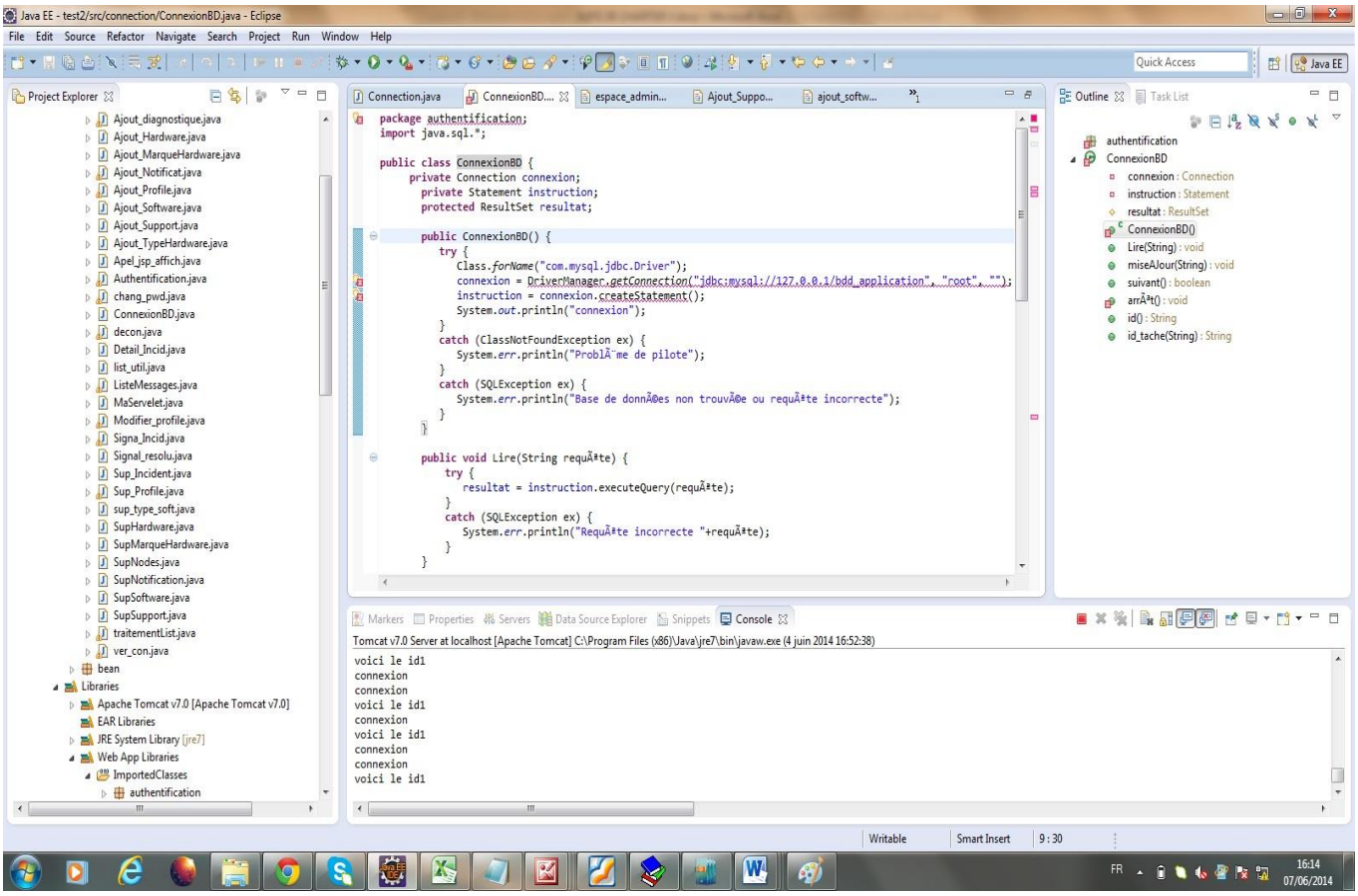
- ✓ Nous avons utilisé l'environnement de développement suivant :

V.4.2.1 : Eclipse :

Eclipse IDE est un environnement de développement intégré libre (le terme Eclipse désigne également le projet correspondant, lancé par IBM) extensible, universel et polyvalent, permettant potentiellement de créer des projets de développement mettant en œuvre n'importe quel langage de programmation. Eclipse IDE est principalement écrit en Java (à l'aide de la bibliothèque graphique SWT, d'IBM), et ce langage, grâce à des bibliothèques spécifiques, est également utilisé pour écrire des extensions.

La spécificité d'Eclipse IDE vient du fait de son architecture totalement développée autour de la notion de plug-in: toutes les fonctionnalités de cet atelier logiciel sont développées en tant que plug-in.

Eclipse a passé depuis son développement par plusieurs versions depuis la première version 1.0 en 2001 et jusqu'aujourd'hui. Dans notre travail nous avons utilisées la version 4.2 appelée Juno.



V.4.2.2 : Adobe dreamwaver CS5 :

Dreamweaver est le système professionnel par excellence pour la création de sites Web et d'applications. Sa puissante combinaison d'outils de mise en forme visuelle, de fonctions de développement d'applications et d'édition de code permet aux développeurs et aux concepteurs de créer des sites et des applications visuellement attrayants et normalisés.

Qu'il s'agisse de la prise en charge des concepts basés sur CSS ou de fonctionnalités de codage manuel, Dreamweaver fournit aux professionnels les outils dont ils ont besoin dans un environnement intégré et optimisé.

V.4.3 : Outils de développements :

V.4.3 .1 : JAVA :

Le langage de programmation que nous avons choisi pour le développement de notre application est le langage JAVA, développé par SUN Microsystems, il est disponible pour les principales plates formes du marché (LINUX, Windows ou autres) et il est totalement gratuit. JAVA possède de nombreuses caractéristiques :

- Simple du faite que sa syntaxe soit basée sur celle du C++, mais dépouillée de tous les mécanismes complexes, redondants et inutiles (pointeurs,…).
- Performant, puissant, java est une plateforme de développement comportant une bibliothèque de classes très riche et de nombreux outils d'interfaces de programmations applicatifs (API).
- Interprété, portable et indépendant des architectures matérielles : Cette caractéristique est un avantage primordiale pour java face à des applications transmises par un réseau et exécutées sur des machines hétérogènes. Un programme java est successivement compilé pour fournir un code intermédiaire indépendant de la plateforme d'exécution (le byte code) simple et rapide à traduire en langage machine.
- Riche : Un des aspects importants de l'environnement java est la richesse de ses librairies.

Java permet de développer de nombreux sortes de programmes dont :

- ✓ Des applications, sous forme de fenêtre ou de console ;
- ✓ Des applets, qui sont des programmes JAVA incorporés à des pages web ;
- ✓ Servlets et jsp pour le développement d'applications web ;

Dans notre mémoire nous avons choisi de développer en J2EE (Java 2 Entreprise Edition) : développement des applications Web en JAVA grâce aux servlets et jsp.

❖ Les Servlets :

Une servlet est un programme java qui fonctionne sur un serveur Web compatible J2EE et dont le rôle est d'apporter une réponse à une requête. Elle reçoit une requête du client, elle effectue des traitements et renvoie le résultat. La technologie des servlets n'est qu'un ensemble de classes. Pour fonctionner convenablement elles ont besoin d'une machine virtuelle JAVA et de l'ensemble des autres classes intégrées à l'API standard du langage JAVA. Une servlet est une application développée dans un contexte client-serveur.

Voici un exemple de code d'une servlet :

```
import java.io.IOException;
import java.io.PrintWriter;

import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;


public class DoIt extends HttpServlet
{

  public void doGet(HttpServletRequest request, HttpServletResponse
response)
      throws IOException, ServletException
           {

                out.println("<h1>Méthode doGet</h1>");

           }

  public void doPost(HttpServletRequest request, HttpServletResponse
response)
       throws IOException, ServletException
           {

                out.println("<h1>Méthode doPost</h1>");

           }

}
```

❖ Les jsp :

JSP « Java Server Pages » est un fichier contenant du code HTML et des fragments de code Java exécutés sur le moteur de Servlets Comparable aux langages côtés serveur de type PHP, ASP, … Les JSP permettent d'introduire du code Java dans des tags prédéfinis à l'intérieur d'une page HTML. Elles permettent donc de mélange la puissance de Java côté serveur et la facilité de mise en page d'HTML côté client. Les fichiers JSP possèdent par convention l'extension .jsp.

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8" />
        <title>Exemple</title>
    </head>
      <body>
        <%
```

V.4. 4 : Les serveurs déployés :

V.4. 4 .1. Le serveur Apache :

Le serveur Apache est le serveur HTTP le plus répandu avec près de 60% du marché, soit le double de son principal concurrent Microsoft-IIS. Ces principaux avantages tiennent de son mode de distribution et à son mode de licences. L'avantage principal de ce produit n'est pas la gratuité, mais ce serveur http est le plus libre, et offre une totale indépendance à l'utilisateur pour la maintenance et le développement, il est aujourd'hui le serveur web le plus utilisé au monde.

V.4. 4 .2. Le conteneur de servlets Tomcat :

Le conteneur de servlets choisi est le moteur Tomcat 7.0 développé par la fondation Apache. Le dialogue entre le moteur de servlets et le serveur web s'effectue à l'aide d'un module logiciel appelé connecteur. Tomcat peut fonctionner sur d'autres serveurs Web mais seul le couple Tomcat/ Apache a été testé. Le module Tomcat du serveur Apache a été développé à partir des sources de Sun Microsystems. Il représente une implémentation de référence pour les servlets. Tomcat peut fonctionner seul, mais cela n'est pas une solution efficace. En exploitation il est préférable d'associer Tomcat avec un serveur HTTP plus puissant, qui se chargera du contenu statique. Tomcat pourra ainsi être mis à contribution uniquement pour les requêtes mettant en œuvre des servlets, et nous opterons pour ce principe.

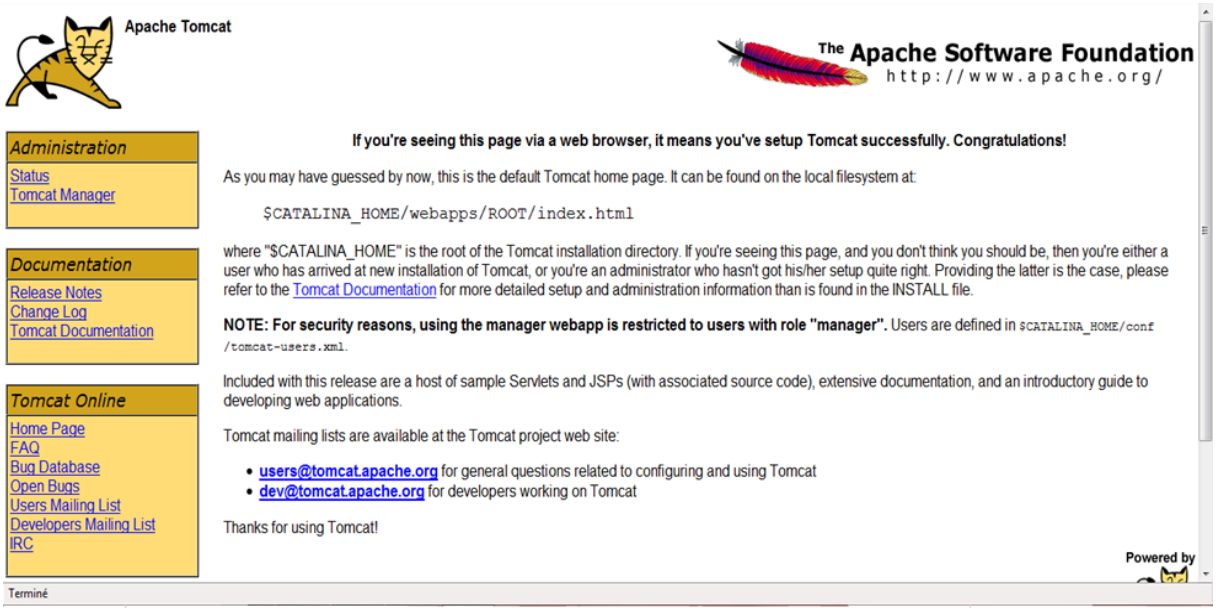


Figure V.18 : Interface d'Apache Tomcat

V.4. 4 .3. Le serveur de données :

Notre choix sur le serveur de bases de données c'est porté sur le serveur MySQL. Son fonctionnement en mode Client /Serveur, ses fonctions nombreuses et puissantes, ses possibilités de connexion, sa rapidité et sa sécurité font de lui un serveur hautement adapté à nos besoin. C'est un serveur de bases de données relationnelles, robuste, basé sur le langage de requête SQL (Structured Query Language), qui est un langage standard pour le traitement des bases de données.

V.4. 5 :Wampserver :

Wampserver est un paquetage contenant à la fois deux serveurs (Apache et MySQL), un interpréteur de script (PHP), les deux bases SQL PhpMyAdmin et SQLiteManager pour gérer plus facilement les bases de données. Il permet d'installer automatiquement et facilement une plateforme permettant l'exploitation d'un site web en PHP qui éventuellement aurait besoin d'un accès à une base de données.

V.4. 5.1. L'interface PHPmyadmin :

PhpMyAdmin est une application web qui permet de gérer un serveur de bases de données MySQL. Dans un environnement multiutilisateur, cette interface écrite en PHP permet également de donner à un utilisateur un accès à ses propres bases de données.

La figure suivante montre une copie d'écran de la page d'accueil de PHPmyadmin. L'écran est divisé en deux parties. Sur la gauche on peut afficher toutes les bases de données gérés par le serveur.la partie droite présente l'ensemble des opérations disponibles en fonction du

contexte.

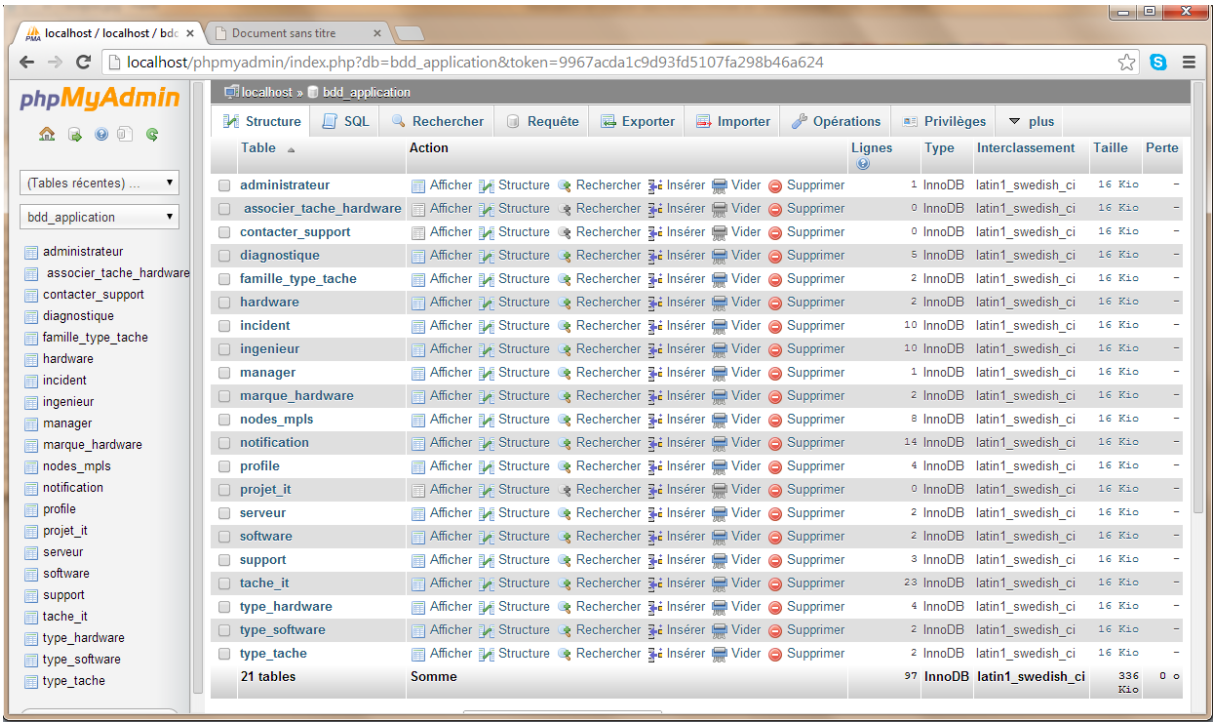


Figure V.19 : Interface phpMyAdmin

V.5 : Architecture du système :

Le principe de fonctionnement de la solution proposée est basé sur une architecture Client-Serveur trois tiers Figure V.20 , le premier niveau est le client demandeur de la ressource, le second niveau est le serveur web utilisant le conteneur de servlet (Apache Tomcat), le troisième niveau est le serveur de BD (Mysql).

Figure V.20 : Architecture applicative

V.5.1 .Partie présentation

Pour illustrer l'échange de données entre L'administrateur et les différends MANAGER et INGENIEUR, nous avons réalisé une applications

À travers les interfaces présentées ci-dessous, nous visons à donner une vue générale de notre application conçue.

V.5.2.Représentation des interfaces de l'application :

L'interface d'authentification (figure V.21) est la première fenêtre télécharger et visualisé par l'utilisateur. Il doit choisir son profil et devra taper son login, son mot de passe ainsi pour pouvoir accéder à la suite de l'application.

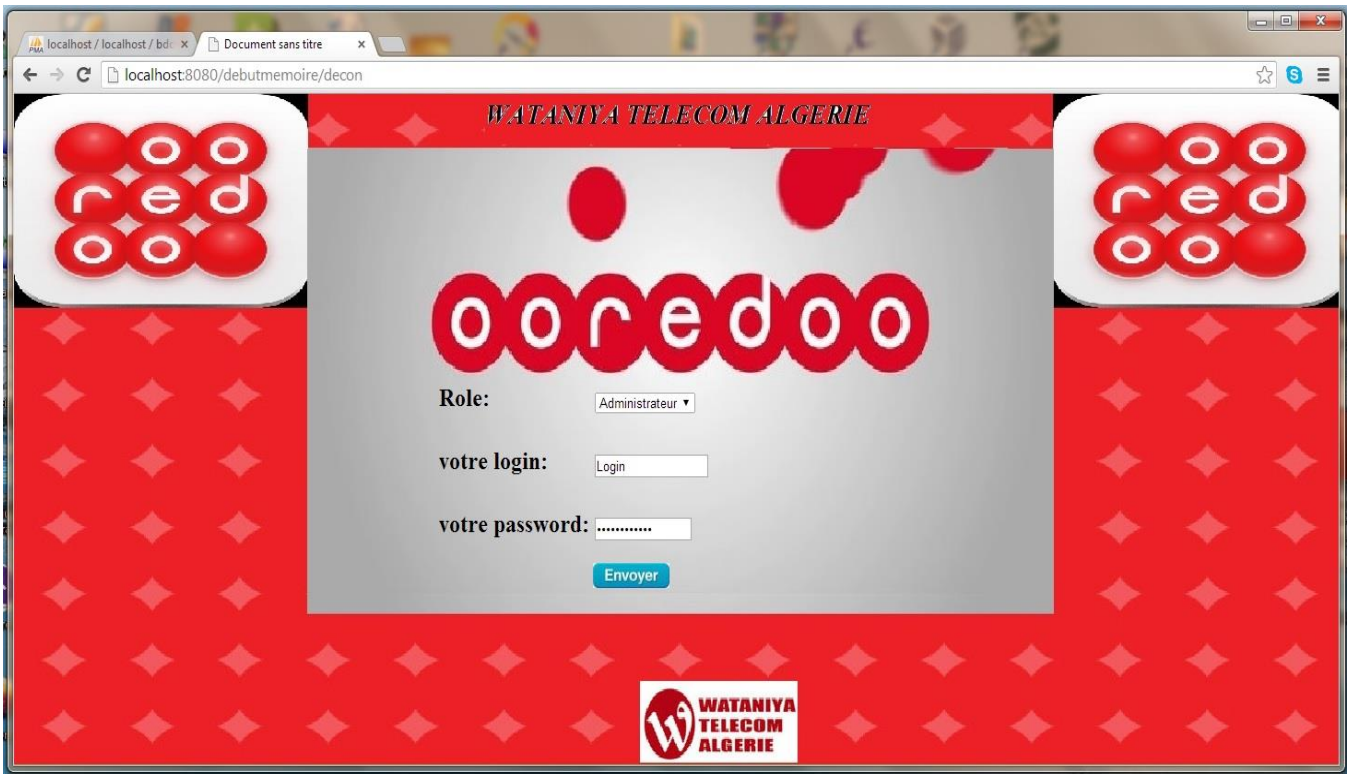


Figure V.21 : Interface Principale de l'application

Alors, si les cordonnées (Rôle, login, mot de passe) saisies par l'utilisateur sont justes, l'interface correspondante à cet utilisateur selon son profil sera téléchargée.

On distingue trois cas :

-Administrateur.

-Manager.

-Ingénieur.

Cas 1 : Si le profil de l'utilisateur est Administrateur alors la page suivante sera télécharger.

Figure V. 22 : Interface Administrateur

Conclusion :

Les performances management et les defaults management qu'offre le logiciel **PRTG** de supervision répondent en sorte aux exigences des différents services Technologie de l'entreprise Wataniya Telecom Algérie. Mais, cette dernière est toujours en quête de nouvelles technologies pour s'imposer devant ces concurrentes, d'où l'intérêt au nouveau logiciel **InfoVista,** qui permet la planification du réseau IP, l'assurance de service proactif, la gestion de la performance du réseau, la gestion des performances des applications et propose même des solutions d'optimisation des réseaux.

Conclusion générale

Conclusion générale :

L’entreprise WATANIYA TELECOM ALGERIE se soucie toujours de sa réputation et concerné par la satisfaction et le confort de ses clients. Elle veut à tout prix éviter la confrontation à des clients mécontents ; d'où éviter le risque de les perdre ; et cela en travaillant davantage pour offrir à ses clients une meilleure qualité de services, en anticipant les pannes et en évitant les arrêts de longue durée gênant les services qui peuvent causer de lourdes conséquences aussi bien financières qu'organisationnelles.

Le stage que nous avons effectué au sein de WTA, nous a permis d’approfondir nos connaissances notamment dans, les réseaux et la supervision, la programmation en java2EE, et base de donnée. Dans le plan professionnel, nous avons pu contribuer dans la réalisation de différentes tâches effectuées dans les différents services de l’organisme à savoir : l’acquisition de connaissances sur la configuration de différent constructeurs Juniper, Cisco, Ericsson, Extreme et le troubleshooting de ces derniers.

Par ce présent travail, nous avons répondus au cahier de charge qui a été proposé par l’entreprise. La conception et la réalisation que nous avons effectué, nous a permis d’aguerrir à la démarche de monitoring via des logiciels de très hautes performances, qui sont le PRTG en premier lieu et l’INFOVISTA qui est une solution récente et plus performante. Et enfin, nous clôturerons ce travail par une présentation de notre application de monitoring réalisée avec java2EE. Éventuellement, notre travail peut être amélioré par la mise en réseau de notre application afin que nous puissions récupérer le trafic pour une analyse qui va permettre de le classer selon différentes sortes de données (vidéo, audio, e-mail,...) qui seront enregistrés dans une base de données pour être utiliser ultérieurement.

Annexe A

A.1. Graphical Network Simulator

GNS3 est un simulateur graphique d'équipement réseaux qui nous permet de créer des topologies de réseaux complexes et d'en établir des simulations. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS (Internetworking Operating System) Cisco .L'IOS c'est le système d'exploitation des **routeurs** et **Switch et firewall** Cisco et **Juniper** pour entrer dans l'interface graphique de chaque éléments il faut télécharger son IOS, GNS3 est compatible avec : **Windows, Linux,…**

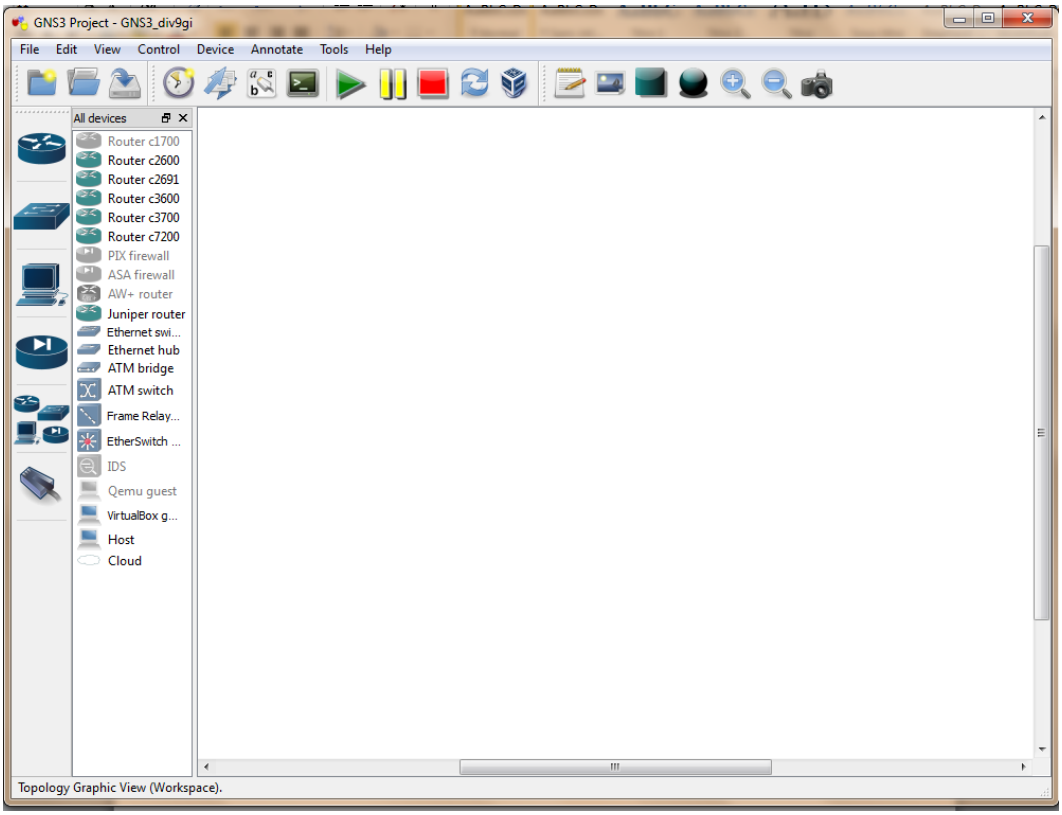


Figure.A.1. Interface graphique de GNS3

Pour ce qui concerne la configuration du système d'exploitation d'un Routeur :

→ On clique sur Edit.

→IOS images and hypervisors.

→Dans settings on sélection IOS (Internetworking Operating System) de routeur voulu.

→On met save.

A.2-Oracle VM VirtualBox :

C’est un logiciel qui permet la création de machine virtuelle, on peut utiliser crier des machine qui auront pour système d’exploitation Windows, Linux,…

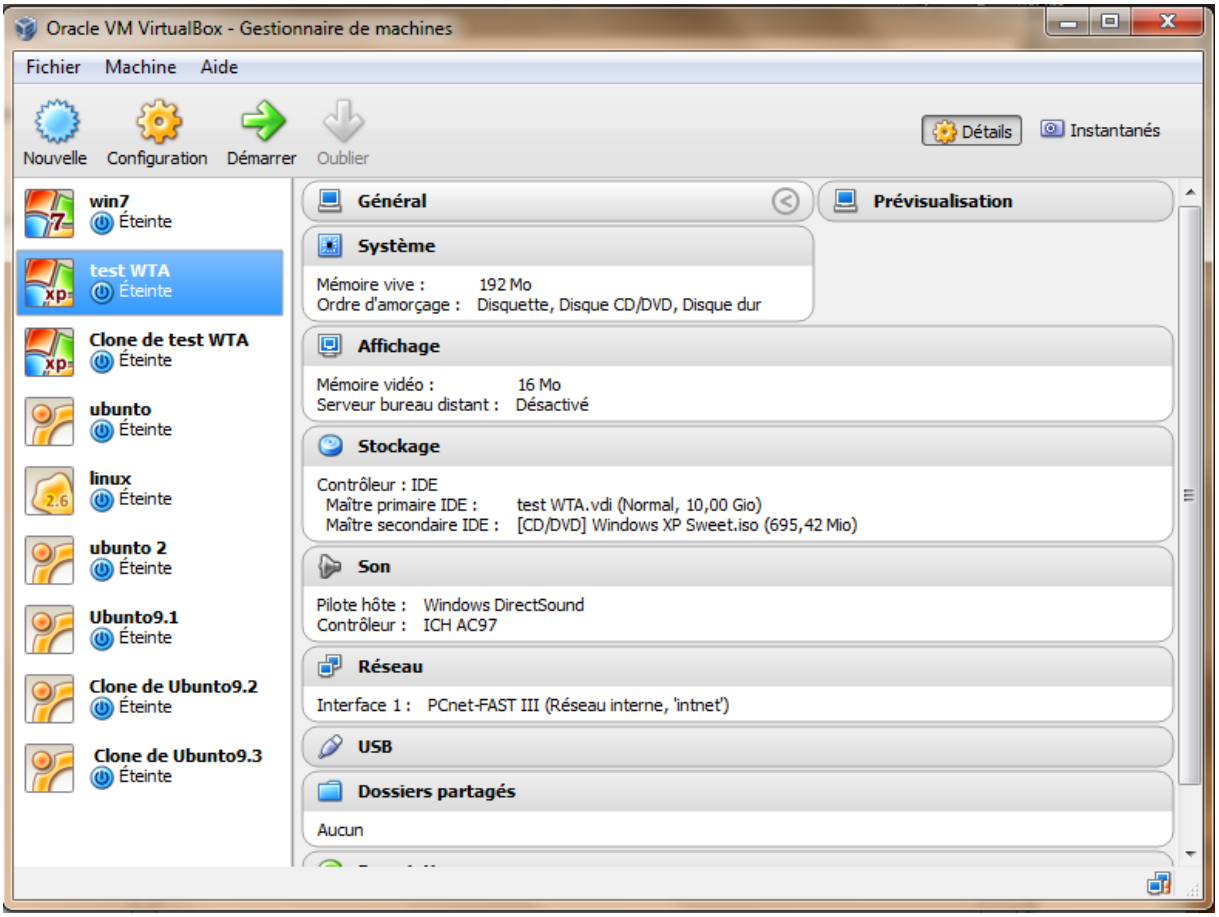


Figure.A.2. Interface graphique de VM VirtualBox.

Exemple de création d’une machine qui aura pour système Windows 7 :

→On clique sur Nouvelle.

→On met le nom de la machine (exemple : test WTA).

→On suit les étapes de configuration de ram et de disc dure…

→Dès que la machine ai étais crier, elle sera affiché sur l'interface de VM VirtualBox, on clique sur cette machine avec le bouton droit et on clique sur démarré.

→ Après avoir démarré la machine on sélectionne l'IOS de système d'exploitation voulu (Windows, Linux,…).

A.3-Connecté GNS3 à VM Virtual Box :

Pour établir une connexion entre GNS3 et VM Virtual Box.

Dans GNS3 :

On clique sur Edit →Préférences→Virtual Box→test Settings : il y aura le message suivant qui va s'affiché :

VBoxwrapper and VirtualBox API 4.2.16 have successfully started

On va dans Virtual Box Guest pour sauvegarder les machines Virtuelles déjà crier sur Virtual Box.

A.4-Création de routeur JUNIPER :

Pour crier un routeur Juniper afin de l'utiliser sur GNS3 nous avons besoin de :

→Qemu0.11 : est un « émulateur de système » : c'est un logiciel qui permet de faire tourner un ou plusieurs systèmes d'exploitation (ou seulement des processus) sur un système d'exploitation déjà installé sur la machine.

Que ce soit pour tester un système, une distribution, expérimenter la programmation noyau, faire des tests de sécurité sans mettre en péril votre environnement de travail, adapter vos développements à d'autres environnements etc.

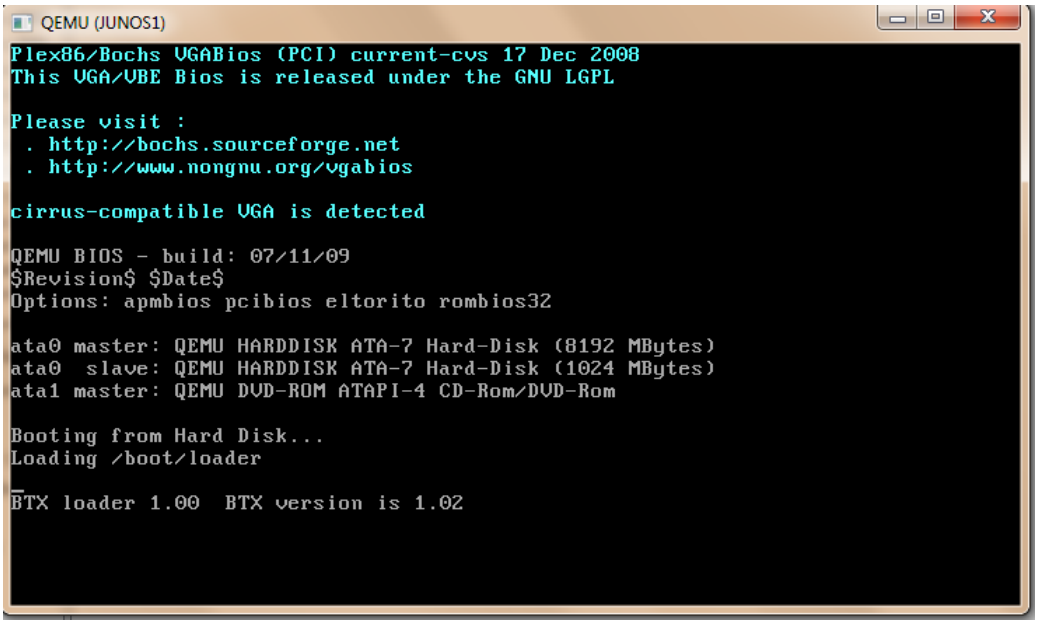


Figure.A.3.Interface Qemu.

→Jinstall-10.1R1.8-domestic-olive : c'est l'image du système qu'on veut faire tourner et ici on utilise celle de Juniper.

Apres la création de ce système on aura :

Pour pouvoir l'utiliser on va dans GNS3 :

On clique sur Edit →Préférences→Qemu→

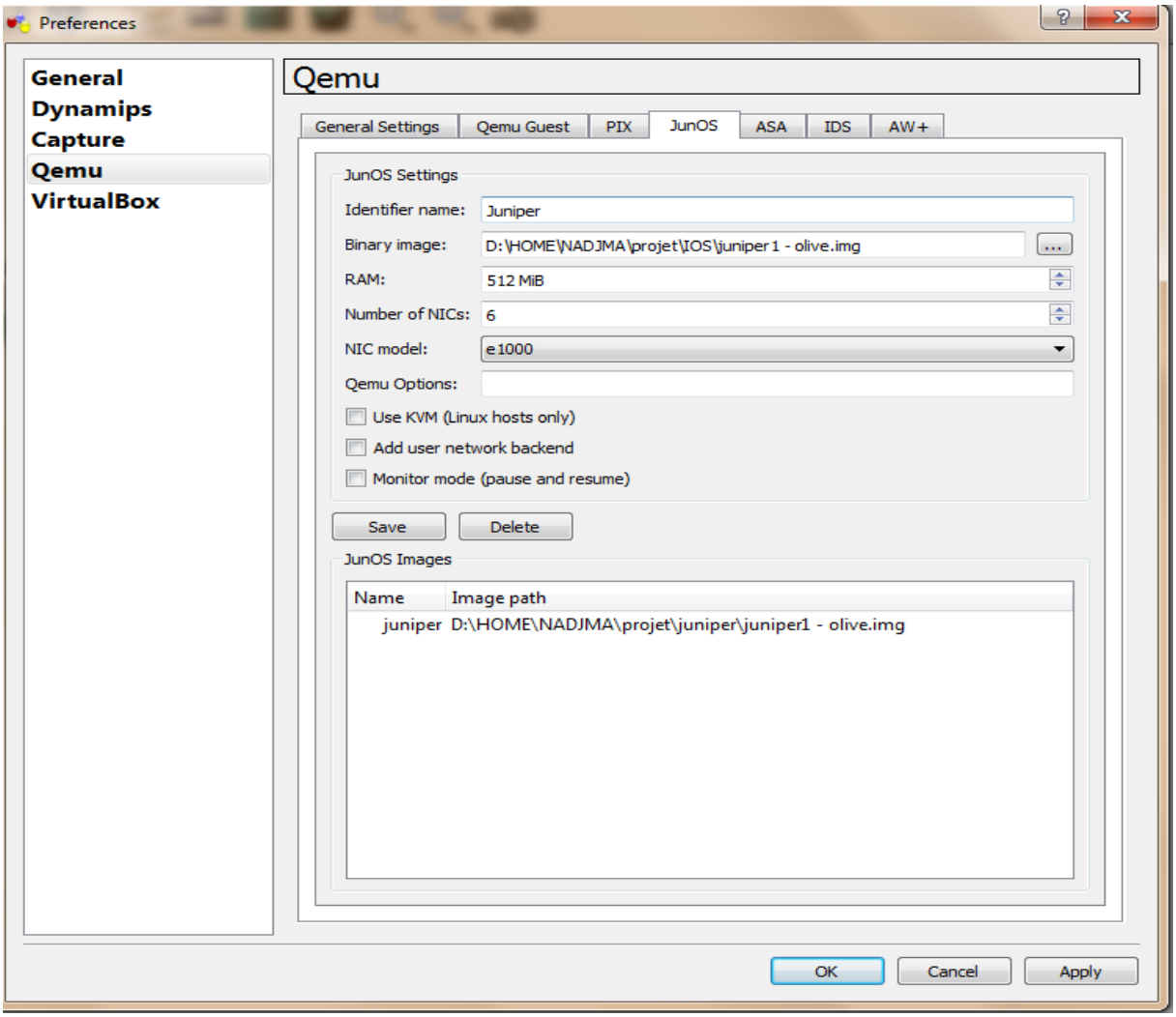


Figure.A.4. Configuration de routeur Juniper sur GNS3

On sauvegarde.

Le routeur Juniper pourra être utilisé.

A.5-JPerf :

C'est un outil utilisé pour faire les tests de performance afin de valider votre réseau.

Cette forme de test peut aider à identifier mauvaise performance ou disqualifier le port Ethernet.

Vous aurez besoin de deux machines, une machine qui sera comme server et une autre machine client.

L’outil JPerf utilise une interface graphique Java.

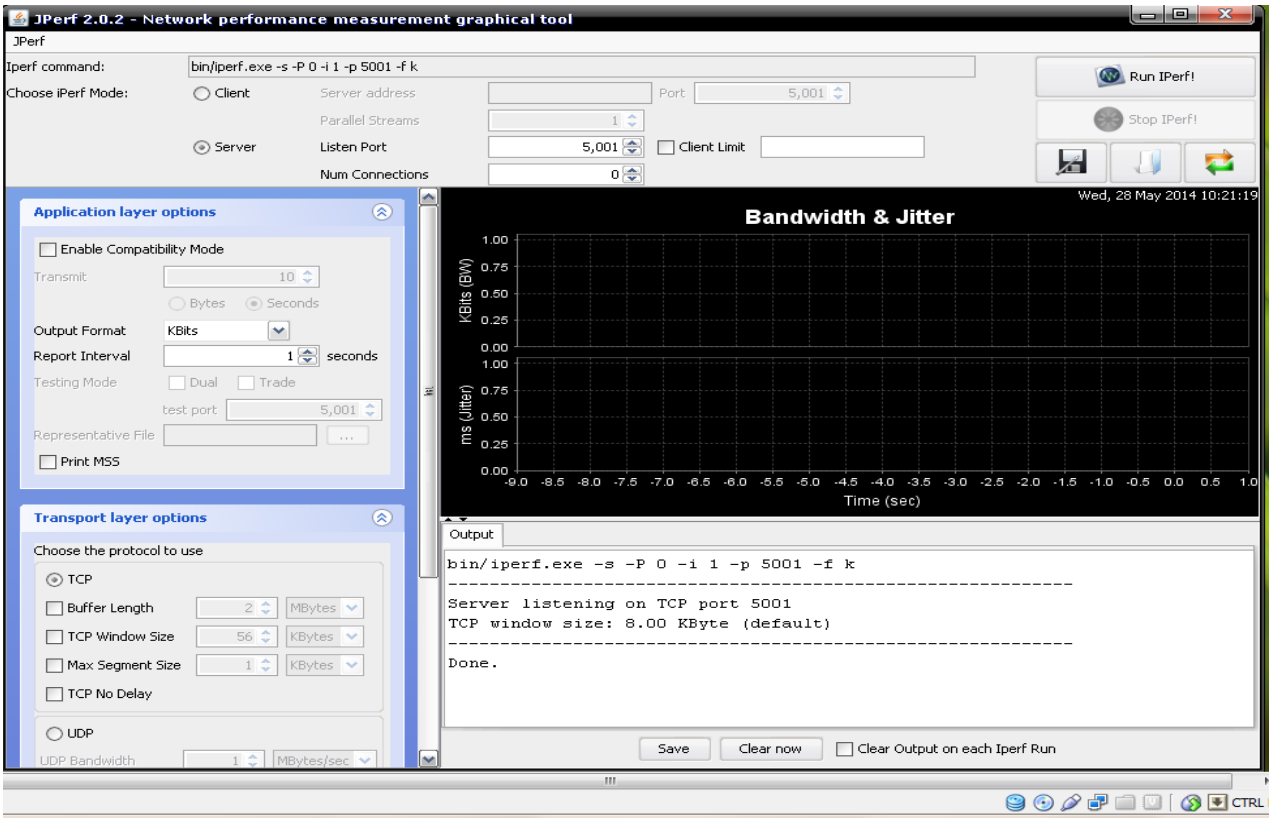


Figure.A.5. Interface JPerf

Annexe B

B.1.Présentation de J2EE :

J2EE (Java 2 Enterprise Edition) est une norme proposée par la société Sun, portée par un consortium de sociétés internationales, visant à définir un standard de développement d'applications d'entreprises multi-niveaux, basées sur des composants.

On parle généralement de «plate-forme J2EE» pour désigner l'ensemble constitué des services (API) offerts et de l'infrastructure d'exécution. J2EE comprend notamment :

- Les spécifications du serveur d'application, c'est-à-dire de l'environnement d'exécution : J2EE définit finement les rôles et les interfaces pour les applications ainsi que l'environnement dans lequel elles seront exécutées. Ces recommandations permettent ainsi à des entreprises tierces de développer des serveurs d'application conformes aux spécifications ainsi définies, sans avoir à redévelopper les principaux services.
- Des services, au travers d'API, c'est-à-dire des extensions Java indépendantes permettant d'offrir en standard un certain nombre de fonctionnalités. Sun fournit une implémentation minimale de ces API appelée J2EE SDK (J2EE Software Development Kit).

Dans la mesure où J2EE s'appuie entièrement sur le Java, il bénéficie des avantages et inconvénients de ce langage, en particulier une bonne portabilité et une maintenabilité du code.

De plus, l'architecture J2EE repose sur des composants distincts, interchangeables et distribués, ce qui signifie notamment :

- qu'il est simple d'étendre l'architecture ;
- qu'un système reposant sur J2EE peut posséder des mécanismes de haute-disponibilité, afin de garantir une bonne qualité de service ;
- que la maintenabilité des applications est facilitée.

B.2.Les API de J2EE :

Les API de J2EE peuvent se répartir en trois grandes catégories :

- Les composants. On distingue habituellement deux familles de composants :
    - Les composants web : Servlets et JSP (Java Server Pages). Il s'agit de la partie chargée de l'interface avec l'utilisateur (on parle de logique de présentation).
    - Les composants métier : EJB (Enterprise Java Beans). Il s'agit de composants spécifiques chargés des traitements des données propres à un secteur d'activité (on parle de logique métier ou de logique applicative) et de l'interfaçage avec les bases de données.
- Les services, pouvant être classés par catégories :
    - Les services d'infrastructures : il en existe un grand nombre, définis ci-dessous :
        - JDBC (Java DataBase Connectivity) est une API d'accès aux bases de données relationnelles.
        - JNDI (Java Naming and Directory Interface) est une API d'accès aux services de nommage et aux annuaires d'entreprises tels que DNS, NIS, LDAP, etc.
        - JTA/JTS (Java Transaction API/Java Transaction Services) est un API définissant des interfaces standard avec un gestionnaire de transactions.
        - JCA (J2EE Connector Architecture) est une API de connexion au système d'information de l'entreprise, notamment aux systèmes dits «Legacy» tels que les ERP.
        - JMX (Java Management Extension) fournit des extensions permettant de développer des applications web de supervision d'applications.
    - Les services de communication :
        - JAAS (Java Authentication and Authorization Service) est une API de gestion de l'authentification et des droits d'accès.
        - JavaMail est une API permettant l'envoi de courrier électronique.

- JMS (Java Message Service) fournit des fonctionnalités de communication asynchrone (appelées MOM pour Middleware Object Message) entre applications.
- RMI-IIOP est une API permettant la communication synchrone entre objets.

L'architecture J2EE permet ainsi de séparer la couche présentation, correspondant à l'interface homme-machine (IHM), la couche métier contenant l'essentiel des traitements de données en se basant dans la mesure du possible sur des API existantes, et enfin la couche de données correspondant aux informations de l'entreprise stockées dans des fichiers, dans des bases de données relationnelles ou XML, dans des annuaires d'entreprise ou encore dans des systèmes d'information complexes.

Bibliographie

❖ **Livres :**

[1] Claude SEVERIN, Préface de Jean-Pierre Arnaud, « RESEAUX & TELECOMS », 2e édition, DUNOD Informatique, 2003.

[2] Tarmo ANTTALAINEN, « introduction to Telecommunications Network Engineering », 2nd edition, Artech House, 2003.

[3] Jean-Luc MONTAGNIER, « Réseaux d'entreprises par la pratique», edition Eyrolles.

[4] Stallings W. « Network Security ». 2nd edition. Prentice Hall, 2003.

[5] Vincent REMAZEILLES, « La sécurité des réseaux avec CISCO». Edition eni.

[6] Jean-François PILLOU, Jean-Philippe BAY, « Tout sur la sécurité informatique ». 2e édition, DUNOD, 2005.

[7] Jean-Luc MONTAGNIER. « Construire son réseau d'entreprise ». Éditions Eyrolles, 2001.

[8] Cédric LIORENS, Laurent LEVIER, Denis VALOIS. « Tableaux de bord de la sécurité réseau ». 2nd edition. Editions Eyrolles, 2003.

❖ **Articles :**

[9] Cécilien CHARLOT. « Solution NAC de contrôle d'accès au réseau ». [H5845], base documentaire Attaques et mesures de protection des SI (2008). Dans le thème sécurité des systèmes d'information, et dans l'univers technologies de l'information. Edition Techniques de l'ingénieur.

[10] Olivier WILLM. « Administration de réseaux informatiques : protocole SNMP ». [H 2840], base documentaire Architecture des systèmes et réseaux (2003). Dans le thème Technologies logicielles Architectures des systèmes et dans l'univers technologies de l'information.

[11] Sarah NATAF, Vincent BEL, Franck VEYSSET. « Technique de supervision de la sécurité des réseaux IP ». [H 5820], dans le thème sécurité des systèmes d'information. Edition Techniques de l'ingénieur.

[12] Microsoft Etudes 2008. « Sécurité des réseaux informatiques ». Microsoft corporation, 2007.

❖ **Sites :**

[1] : http://www.paessler.com/prtg.

[2] : Cisco IOS, Configuration Fundamentals, Configuration Guide; http://www.cisco.com/.
[3] : GNS3: http://www.gns3.net/.
[4] : Wireshark: http://www.wireshark.org/.
[5] : VirtualBox: VirtualBoxImage.com.
[6] : Juniper : www .juniper .net.
[7] : Ericsson : http://www.ericsson.com
[8] : Routing Issues: QoS/CoS, Jean-Marc, UzéLiaison Research & Education, EMEA : juze@juniper.net.
[9] : www.siteduzero.com.
[10] : http://thumbcreator.com/olive/olive-juniper-simulator.html.
[11] : http://thumbcreator.com/prtg/prtg-mib-importer.html.

[12] www.sndl.cerist.dz

[13] www.commentcamarche.com

[14] www.Cisco.com

[15] www.develloppez.com

[16] www.dpstelecom.com

[17] www.wiki.monitoring-fr.org

[18] http://www.loriotpro.com/

Mots clés

-Juniper,Ericsson,Cisco,Extreme,MPLS,RIP, IGRP, EIGRP, OSPF,IP, IPX, AppleTalk,SNP 4000,MSER,DSLAM,HDTV,l'IPTV,EAPS,VPN, IPSec, IPS,

LAN,SSG,WAN,Juniper SSG520,HA,NEEF,URL,SNMP,TCP/IP,Table ARP,charge CPU, MBSA, DNS, Oracle VM Virtual Box , GNS3 ,PRTG ,XOS,Traffic Grapher, INFOVISTA,MIB, RAM,SSR,Extreme Summit X460,SE-