Capgemini France
Outsourcing Services
Réseaux & Sécurité
Tour Anjou
Puteaux
33, quai de Dion Bouton
92814 Puteaux cedex

+33(0)1 41 26 51 00
+33(0)1 41 26 51 01

Etude d'outils de filtrage sur les réseaux à haut débit

Rapport de Mission

SNEP

Type :	Rapport de mission
Usage :	Confidentiel
Version :	3.0
Date :	01/07/2004
Statut :	Approuvé
Auteur :	Capgemini France
Référence :	CAP/OS/RM02070

APPROBATION DU DOCUMENT			
Organisme ou entreprise	**Nom**	**Date**	**Visa**
SNEP	M.GOLDSMITH		
CAPGEMINI	M.FRESNEL	01/07/2004	

DIFFUSION				
Destinataire	**Organisme ou entreprise**	**Nombre**	**Pour action**	**Pour info**
M. GOLDSMITH	SNEP	1	X	
M.FRESNEL	Capgemini France	1	X	

MISES A JOUR			
Version	**Date**	**Auteur**	**Motifs**
V1.0	29/06/2004	Capgemini France	Création
V2.0	30/06/2004	Capgemini France	Modification
V3.0	01/07/2004	Capgemini France	Modification

SOMMAIRE

1. RAPPEL DU CONTEXTE DE LA MISSION

1.1 OBJECTIFS DE LA MISSION

Une société tierce a réalisé pour le compte du SNEP une étude de faisabilité technique des outils de filtrage sur haut débit, ayant pour objectifs :

- Etudier les solutions de filtrage sur les réseaux haut débit.
- Tester un système de filtrage dans le cadre d'une démonstration de faisabilité.
- Proposer des recommandations.

Cette société sera désignée la société « VALERIE » dans le reste du document.

Capgemini a répondu aux besoins suivants exprimés par le SNEP :

1. *Valider la méthodologie des tests réalisés par la société VALERIE*
2. *Valider les tests réalisés par la société VALERIE.*
3. *Valider la faisabilité de l'implémentation de la solution retenue.*
4. *Mettre à plat les besoins de service continus de cette architecture pour en assurer la pérennité et le bon fonctionnement.*
5. *Réaliser une présentation écrite et orale de l'étude.*

1.2 DEMARCHE ADOPTEE

La démarche adoptée au cours de cette mission répond à un double objectif, tout d'abord satisfaire les attentes précédemment citées et enfin garantir le bon déroulement de la mission quant à son organisation et à la formalisation des résultats attendus de la part du SNEP.

La démarche adoptée se compose de six phases distinctes :

1. *Lancement.*
2. *Etude de l'existant.*
3. *Approfondissement.*
4. *Tests.*
5. *Etude d'impacts*
6. *Rédaction du rapport de mission.*

Remarque importante :

Les phases 3 et 4 ont été rendues nécessaires pour paliers aux insuffisances constatées lors des phase 1 et 2.

Capgemini en corrélation avec le SNEP a pris l'initiative de rajouter des volets techniques et méthodologiques au sein de l'étude de « VALERIE ».

Les tableaux suivants détaillent ces phases.

Phase 1 - Lancement	
Objectifs	Durant cette brève étape de démarrage, Capgemini établit l'organisation pour la la mission en sa totalité, en incluant la définition de l'équipe projet et la définition des rôles et des responsabilités.
Détails des activités	Capgemini conduit aussi une réunion de lancement avec le SNEP et avec la participation d'un représentant de la société « VALERIE ». Sa finalité est d'introduire l'équipe projet avec la méthodologie de Capgemini et de définir les étapes initiales de la mission. Le compte rendu de la réunion de lancement documente le périmètre, les objectifs, l'approche, les livrables et le planning du projet.
Livrables	Fourniture par Capgemini du document suivant : • Compte rendu de la réunion de lancement.

Phase 2 - Etude l'existant	
Objectifs	Cette seconde phase consiste en l'analyse de la documentation et des travaux effectués par la société « VALERIE ».
Détails des activités	Une présentation succincte des travaux réalisés par « VALERIE » au démarrage de la phase a été réalisée au démarrage de la phase. La prise en compte des aspects fonctionnels, techniques et organisationnels s'effectue au travers de réunions de travail avec les interlocuteurs de la société « VALERIE ». NOTA : • Il n'existe pas à proprement parler d'un document d'expression des besoins. • La société « VALERIE » a mis à disposition de Capgemini la première version de la documentation une semaine après le démarrage de la mission. • Les documents de test n'existent pas.
Livrables	Fourniture par la société « VALERIE » d'une première version de la documentation : • Réseaux P2P. • Modes de filtrage & solutions du marché. « VALERIE s'est appuyé sur la documentation accessible (« datasheets » des constructeurs) en ligne sur les sites Internet associés. • Protocole expérimental.

Phase 3 - Approfondissement	
Objectifs	Cette troisième phase vise à approfondir avec la société « VALERIE » l'étude principalement sur les axes suivants : • Méthodologie : définir des critères permettant d'identifier et de classer les différentes solutions susceptibles de répondre au besoin de filtrage sur haut débit. • Architectures : prendre en compte les différentes architectures de collecte haut débit. • Tests : définir les scénarii de test et les résultats attendus. • Economie : donner une estimation du coût d'acquisition de la solution. Cette phase est conclue par la sélection d'une solution de filtrage qui sera testée dans la phase suivante.
Détails des activités	La prise en compte des aspects fonctionnels, techniques et organisationnels s'effectue au travers de réunions de travail avec les interlocuteurs de la société « VALERIE ».
Livrables	Fourniture par la société « VALERIE » d'un complément d'étude : • Synthèse des solutions de filtrage suivant les critères définis • Topologies ADSL et câbles • Protocole de test

Phase 4 - Tests	
Objectifs	Cette quatrième phase vise à tester et valider la solution sélectionnée précédemment dans un environnement de test. L'accent sera mis sur les aspects suivants : • Architecture réseau. • Protocoles. • Charges. • Administration.
Détails des activités	Les principales activités réalisées durant cette phase sont les suivantes : • Préparation de l'environnement de test. • Finalisation des tests à effectuer. • Réalisation des tests. • Réalisation d'un bilan des tests. NOTA : Les tests sont réalisés en présence de Capgemini et de « VALERIE ».
Livrables	Production par Capgemini du document : • Bilan des tests.

Phase 5 – Etude d'impacts	
Objectifs	Cette cinquième phase vise à présente une étude d'impact. Seulement les impacts techniques sont considérés dans cette phase.
Détails des activités	Les principales activités réalisées durant cette phase sont les suivantes : • Réalisation d'une étude d'impact.
Livrables	Le résultat de cette étude d'impact figure dans le rapport de la mission.

Phase 6 – Rédaction du rapport de mission	
Objectifs	Cette dernière phase vise à présenter au SNEP un rapport de mission.
Détails des activités	Les principales activités réalisées durant cette phase sont les suivantes : • Rédaction du rapport de mission. • Séminaire de restitution.
Livrables	Fourniture par Capgemini de la documentation suivante : • Rapport de mission accompagné d'une présentation de synthèse.

1.3 DEROULEMENT DE LA MISSION

Afin de réaliser la mission, Capgemini dispose d'un délai de 25 jours ouvrés, exploité de la façon suivante :

- Entretiens avec les interlocuteurs techniques et fonctionnels.
- Prise en compte des objectifs, enjeux et contraintes du SNEP.
- Validation et approfondissement.
- Rédaction et présentation du rapport de mission.

Les entretiens avec les interlocuteurs techniques de la société « VALERIE » ont porté essentiellement sur les thèmes suivants :

- Identification et classification des réseaux d'échange.
- Identification et classification des solutions de filtrage.
- Prise en compte des architectures des réseaux haut débit en France (DSL, câbles).
- Définition d'hypothèses pour le déploiement et chiffrage d'un déploiement.

Nous tenons à remercier l'ensemble de nos interlocuteurs pour leur disponibilité et leur parfaite collaboration, qui nous a permis d'atteindre nos objectifs dans les meilleures conditions d'efficacité.

2. PRESENTATION DU DOCUMENT

Conformément aux objectifs de la mission ainsi qu'au déroulement de cette dernière, le présent document formalise les différentes réflexions sur la base des différentes études réalisées par la société « VALERIE » pour les solutions de filtrage sur les réseaux à haut débit.

Ce document doit permettre au SNEP d'obtenir une visibilité globale sur la faisabilité technique des solutions possibles aujourd'hui en ce qui concerne le filtrage sur les réseaux haut débit. Les options envisageables sont matérialisées et argumentées. Une maquette est également décrite.

Les diverses réflexions menées lors de cette mission tiennent compte dans la mesure du possible des facteurs environnementaux suivants :

- Architectures de collecte à haut débit des FAIs.
- Implémentation.
- Pérennité des solutions de filtrage.
- Prix des solutions.

La conduite de cette mission doit s'appuyer sur une connaissance précise du contexte et des objectifs du SNEP ainsi que des contraintes associées. Le caractère confidentiel de la mission a été également pris en compte.

La première partie du document permet d'obtenir une certaine visibilité quant à ce contexte, en prenant en compte les aspects techniques, fonctionnels et organisationnels.

La seconde partie identifie un ensemble de critères clés permettant de caractériser les solutions de filtrage. Ces critères servent également de point de comparaison entre les différentes solutions. Une indication sur le prix d'acquisition est donnée.

La troisième partie identifie la solution retenue pour maquettage à l'issue de l'étude comparative.

La quatrième partie présente la maquette réalisée pour valider la solution retenue dans un environnement de test.

Enfin, dans une dernière partie, nous présenterons les impacts en regard de notre compréhension du contexte, des objectifs et attentes du SNEP.

Nota

Nous tenons à rappeler que l'objectif de cette mission est l'étude de faisabilité d'une solution de filtrage. Il ne constitue pas un document de spécifications pour un FAI.

3. SYNTHESE GENERALE

3.1 ANALYSE DE L'EXISTANT

Le parc d'abonnement à Internet haut débit a plus que doublé en 2003, passant de 1,6 à 3,5 millions d'abonnés. Les Fournisseurs d'Accès Internet (FAI) offrent un service de bande passante sur Internet à ses abonnés. Ce service est assuré par une architecture de type ADSL ou Câble.

Ces réseaux ont favorisé le développement de réseaux d'échanges de fichiers de différents formats (musique, films…).

Nous pouvons comme exemple de réseaux P2P : WPNP, FastTrack, eDonkey2K, Overnet, BitTorrent, SoulSeek, MP2P, Direct Connect, Gnutella, Earthstation 5, Filetopia, Mediaseek, Freenet, JXTA.

3.2 FILTRAGE DES FLUX

3.2.1 Objectifs

Nous entendons par filtrage la capacité à limiter un type de flux (préalablement identifié). Le blocage est de fait un niveau de filtrage maximum.

Différents modes de filtrage existent :

- Filtrage URL ou adresse IP : Ce moyen est adapté pour interdire l'accès à des sites qui proposent des contenus illégaux mais ne répond pas aux impératifs de neutralisation du P2P

- Filtrage des Ports : C'est un moyen basique pour filtrer certains ports qui sont spécifiques aux réseaux P2P, mais des moyens de contournements existent qui rendraient très rapidement inopérante cette solution si elle constituait l'unique filtrage mis en place.

- Filtrage des Protocoles : C'est, de loin, le moyen le plus efficace, et celui qui présente les plus grandes garanties de pouvoir être adapté à l'évolution des technologies P2P

- Filtrage des Contenus : C'est, sur le papier une bonne solution, mais il est en l'état impossible d'envisager sa mise en œuvre à grande échelle. Les ressources nécessaires aux processus d'identification des contenus sont lourdes. L'encryptage utilisé sur certains protocoles P2P rend difficile, voir inefficace ce type de filtrage.

3.2.2 Solutions envisagées

Il existe trois types de solutions de filtrage :

- Les outils d'optimisation de réseaux : Les outils de QoS (Qualité de service) gèrent les priorités des flux. Ils peuvent ainsi limiter ou bloquer le débit pour un type de flux donné, et garantir de la sorte une qualité de service pour les flux de données critiques.

- Les sondes IDS/IDP : Ces sondes permettent la détection et la prévention des attaques Internet, en analysant chaque paquet afin d'y trouver soit un comportement soit une signature connue.

- Les flow-based switch : Ces commutateurs agissent par classification des flux. On différencie ainsi le trafic interactif du trafic non interactif qui est typiquement un trafic P2P.

Nous avons shortlisté pour la présente étude trois solutions du marché : ALLOT, Packeteer et Ellacoya. Nous avons étudié ces solutions sur la base de critères : reconnaissance du filtrage, actions de filtrage, performances, administration et implémentation.

A l'issue de cette étude, une nouvelle shortlist a été définie avec les deux solutions ALLOT et Ellacoya. Ces deux solutions semblent en mesure de pouvoir répondre à la problématique de filtrage sur haut débit.

3.3 SOLUTION MAQUETTEE

Une maquette avec la solution ALLOT a été réalisée. Elle a permis d'adresser favorablement les deux objectifs suivants :

- Tests quantitatifs : Limitation des flux P2P et capacité à traiter un trafic Gigabit.
- Tests qualitatifs : Identification et blocage des flux P2P.

3.4 IMPACTS

Les impacts sont d'ordre technique (exemples : sécurité, intégration dans les architectures FAI, performances, supervision) ou liés à la pérennité des solutions de filtrage (veille technologique, maintenance

4. RAPPORT

4.1 EXPRESSION DU BESOIN

4.1.1 Définitions

Filtrage

Nous entendons par filtrage la capacité à limiter un type de flux (préalablement identifié). Le blocage est de fait un cas particulier du filtrage.

Réseaux à haut débit

Les réseaux haut débit existent depuis une dizaine d'années et ont tout d'abord été développés pour recevoir la télévision par le réseau téléphonique classique sans occuper une ligne téléphonique. Le rapide développement des technologies de l'information a fait apparaître de nouveaux services consommateurs de capacité de transmission. L'accès rapide à Internet, la visioconférence, l'interconnexion des réseaux P2P, le télétravail, la distribution de programmes TV et la VoIP (voix sur IP avec les offres de Free et de France Telecom) sont des exemples de ces nouveaux services multimédia que l'usager désire obtenir à domicile ou au bureau.

Un accès Internet est caractérisé par la bande passante allouée à un internaute par son fournisseur d'accès Internet.

Nous parlons de haut débit lorsque qu'un FAI offre un service d'accès permanent d'au moins 128 Kbit/s.

Réseaux ADSL

Le système ADSL[1] (*Asymmetric Digital Subscriber Line*) permet de faire coexister sur une même ligne un canal descendant (*downstream*) de haut débit, un canal montant (*upstream*) moyen débit ainsi qu'un canal de téléphonie.

Le standard ADSL, finalisé en 1995, prévoit :

- Un canal téléphonique avec raccordement analogique.
- Un canal montant avec une capacité maximale de 800 Kbit/s.
- Un canal descendant avec un débit maximal de 8192 Kbit/s.

Comme pour toutes les technologies DSL, la distance de boucle entre le central (*DSLAM*) et l'utilisateur ne doit pas dépasser certaines limites afin de garantir un bon débit des données. Le tableau suivant précise les débits en fonction de la distance et du diamètre du câble

[1] Dans les pays francophones, le terme ADSL est parfois remplacé par LNPA qui signifie « Ligne Numérique à Paire Asymétrique ».

Downstream [Kbit/s]	Upstream [Kbit/s]	diamètre du fil [Mm]	Distance [km]
2048	160	0.4	3.6
2048	160	0.5	4.9
4096	384	0.4	3.3
4096	384	0.5	4.3
6144	640	0.4	3.0
6144	640	0.5	4.0
8192	800	0.4	2.4
8192	800	0.5	3.3

Pour dépasser ces limites, les équipementiers travaillent aujourd'hui sur deux évolutions majeures :

- L'ADSL2+, qui sera expérimenté par France Telecom en septembre et par Free dès le printemps, permettra d'augmenter le débit maximal théorique d'une ligne jusqu'à près de 16 Mbits/s.
- Le Rich Extended ADSL, prévu pour l'année 2005, permettra pour sa part d'atteindre 8 Mbits/s à une distance de 3,5 km du DSLAM.

Réseaux câblés

A l'origine distributeur de services audiovisuels, le câble est depuis 1999 permet également l'accès Internet.

Les capacités du câble prévoient :

- Un canal montant avec une capacité maximale de 320Kb/s à 10Mb/s.
- Un canal descendant avec un débit maximal de 27 à 36 Mb/s.

La norme DOCSIS[2] assure une meilleure qualité dans la gestion des débits.

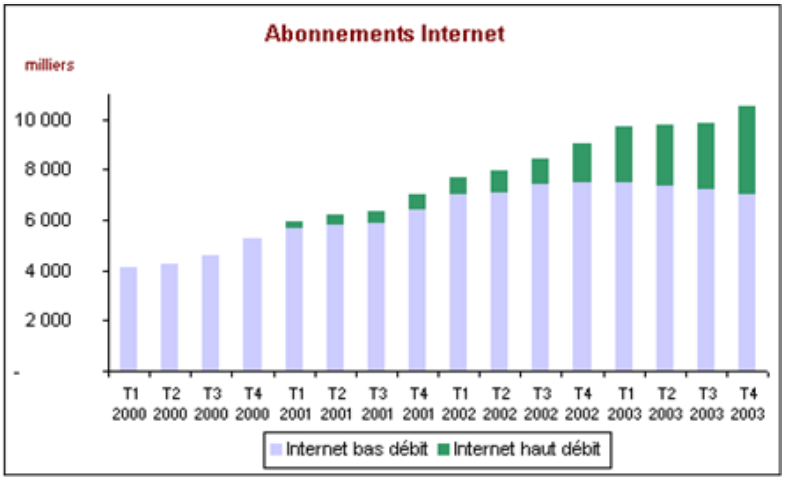
Les fournisseurs d'accès Internet via le câble proposent aujourd'hui des offres allant de 160Kb/s à 2560Kb/s de bande passante. La liaison est de type permanente, avec attribution d'une adresse IP fixe.

[2] DOCSIS : *Data Over Cable Service Interface Specification*. La norme a été créée en 1997

4.1.2 Contexte

4.1.2.1 Evolution des abonnements Internet haut débit en France

Le parc d'abonnements à Internet haut débit a plus que doublé en 2003, passant de 1,6 million à 3,5 millions d'abonnés. Sur le seul quatrième trimestre 2003, plus de 700 000 nouveaux abonnements ont été enregistrés. Le parc d'abonnements à des accès bas débit (< à 128 kbit/s), qui n'a pas fait l'objet d'une publication par l'AFA[3], est estimé à 7 millions à fin 2003.



Afin de mieux rendre compte de l'évolution de l'Internet à haut débit, l'observatoire des marchés de l'ART restitue non seulement le nombre des abonnements auprès des opérateurs déclarés, mais aussi le nombre d'abonnements vendus par ces opérateurs déclarés aux FAIs non déclarés, qui les revendent au client final.

Abonnements Internet (unités)	4ème trim 2002	1er trim 2003	2ème trim 2003	3ème trim 2003	4ème trim 2003	Variation 4T03/4T 02
Abonnements Internet bas débit [4]	7 469 000	7 490 000	7 338 000	7 215 000	7 000 000	-6,3%
Abonnements Internet haut débit (câble, xdsl, BLR) [5]	1 590 975	2 236 245	2 450 019	2 790 270	3 524 338	+121,5%
Total des abonnements Internet	9 059 975	9 726 245	9 788 019	10 005 270	10 524 338	+16,2%

[3] AFA : Association des Fournisseurs d'Accès et de Services Internet (*http://www.afa-france.com*). L'AFA rassemble les données des opérateurs suivants : AOL France, 9 Online, Aricia, Cario, Club-Internet, Free (RTC uniquement), Inter PC, NC Numéricâble, Noos, Tiscali France, UPC France, Wanadoo.

[4] Source : données de l'AFA jusqu'au troisième trimestre 2003, estimation de l'observatoire des marchés au quatrième trimestre 2003. Selon la définition de l'AFA, sont comptabilisés : les comptes d'accès gratuits ou facturés à l'usage qui font l'objet d'au moins une connexion dans les 40 derniers jours, et tous les comptes payants sur une base forfaitaire mensuelle (incluant ou non un forfait téléphonique, particuliers et professionnels).

[5] Source : données de l'AFA jusqu'au troisième trimestre 2002, données de l'observatoire des marchés de l'ART à partir du quatrième trimestre 2002.

Les abonnements Internet haut débit (unités)	4ème trim 2002	1er trim 2003	2ème trim 2003	3ème trim 2003	4ème trim 2003	Variation 4T03/4T 02
Abonnements Internet par le câble (source AFORM) [6]	*282 992*	*312 707*	*336 668*	*348 295*	*393 854*	*+39,2%*
Abonnements Internet par ligne ADSL (source France Telecom)	*1 361 377*	*1 905 463*	*2 041 180*	*2 346 120*	*2 967 434*	*+118,0%*

Nota

Les donnés publiques de l'AFORM pour le câble et de France Telecom pour l'ADSL sont données à titre indicatif. Le total des deux lignes du tableau ci-dessus n'est pas strictement égal aux chiffres de la rubrique " abonnés à Internet haut débit " du tableau précédent.

4.1.2.2 Architecture DSL

Une Fournisseur d'accès Internet (FAI) offre un service de bande passante sur Internet à des abonnés. Ce service est assuré par une architecture qui se décline sous 3 options, transparentes pour l'utilisateur.

Option 1 – Mise à disposition directe de la paire cuivre de l'abonné par France Telecom à ses concurrents.

Cette mise à disposition peut être opérée sous deux formes possibles :

- Dégroupage total : Intégralité des bandes de fréquence de la paire de cuivre
- Dégroupage partiel : fréquence haute de la paire de cuivre seulement, utilisable pour les données.

Le FAI dispose d'une infrastructure dégroupée jusqu'au nœud de raccordement des abonnés (NRA).

Nous pouvons citer, par exemple, Free et 9Telecom.

Option 3 – Les FAIs achètent à un opérateur alternatif une prestation globale d'accès, de collecte et de transport du trafic.

La prestation de collecte du trafic DSL au niveau régional est réalisée par France Telecom. Le FAI possède son propre réseau de transport IP et s'appuie sur France Telecom pour le transport ATM.

Nous pouvons citer, par exemple, Tiscali.

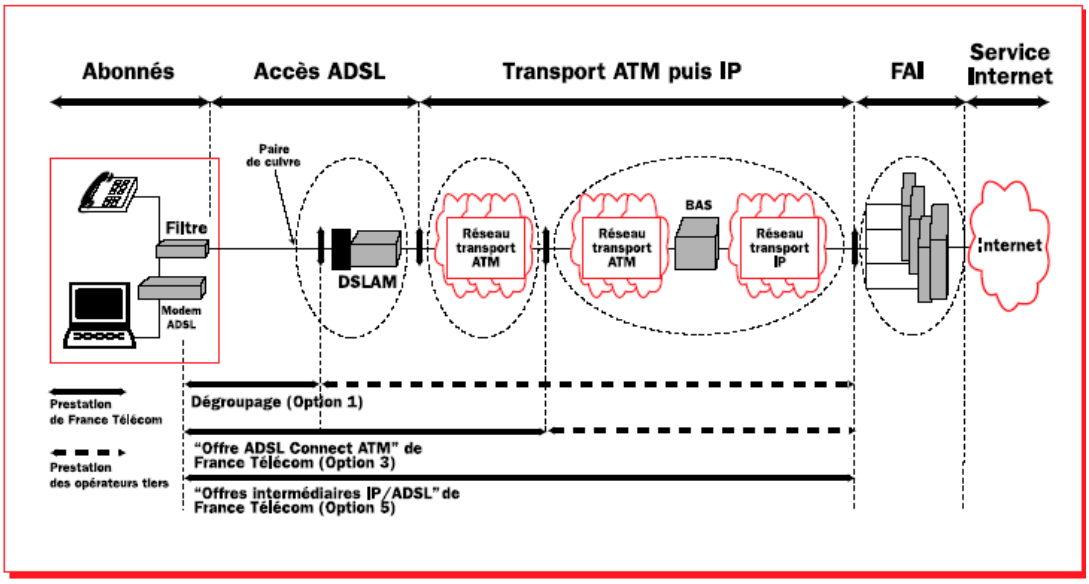
[6] Source : Association Française des Opérateurs de Réseaux Multiservices (*http://www.aform.org*)

Option 5 – Revente, sous marque propre du FAI

Les offres d'accès sont conçues et gérées par l'opérateur historique (France Telecom).

Nous pouvons citer, par exemple, Club Internet et La Poste.

Le schéma ce dessous représente les 3 options précédemment introduites.



DSLAM (Digital Subscriber Line Access Multiplexer)

Situé sur le réseau de l'opérateur local, au niveau du répartiteur, il fait parti des équipements utilisés pour transformer une ligne téléphonique classique en ligne ADSL permettant la transmission de données, et en particulier l'accès à Internet, à haut débit. La fonction du DSLAM est de regrouper plusieurs lignes ADSL sur un seul support, qui achemine les données en provenance et à destination de ces lignes.

BAS (Broadband Access Server)

Equipement dont la fonction est de gérer le transport de données en mode ATM dans le cadre des offres d'accès à Internet par ADSL. Sur le réseau de France Telecom, chaque BAS regroupe le trafic ATM issu d'une dizaine de DSLAM. Un BAS gère donc le trafic de l'ensemble des lignes ADSL situées dans les zones couvertes par les DSLAM qui lui sont connectés. La zone ainsi couverte par un BAS est appelée "plaque" par France Telecom. Il est établi un circuit ATM "montant" et un circuit ATM "descendant" entre chaque client connecté et le BAS auquel il est raccordé.

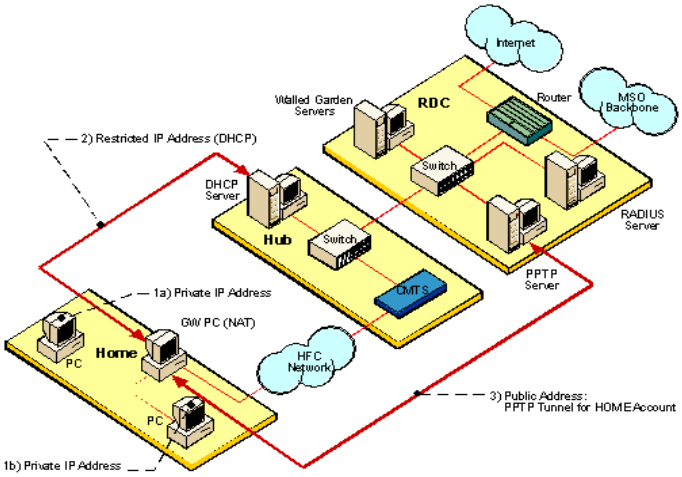
4.1.2.3 Architectures câble

À l'origine, les réseaux câblés étaient basés sur l'utilisation du câble coaxial. Avec les progrès dans les technologies de transmission grâce à l'utilisation de la fibre optique, les opérateurs de câble utilisent des réseaux hybrides composés de liens en fibre optique et de câble coaxial HFC (*Hybrid Fiber Coaxial*), via le réseau téléphonique utilisant la paire torsadée.

Un câblo-opérateur est propriétaire et exploitant de son architecture câble. Il existe deux principaux fournisseurs d'accès Internet en France via le câble : Noos et NC Numéricable.

L'architecture se compose de CMTS (*Cable Modem Termination System*), équivalent au DSLAM pour l'ADSL, lesquelles sont reliées à différents routeurs en France. Chaque utilisateur se connecte au CMTS via le réseau HFC.

Il y a création d'un tunnel pour l'authentification de la liaison point à point entre l'abonné et un serveur PPTP ou un LNS. Le LNS est généralement le routeur d'accès au backbone IP, qui termine le tunnel pour ensuite aboutir sur un réseau IP (Regional Network sur le schéma).



4.1.3 Moyens d'échange de contenu "P2P"

Les éléments constituant un réseau P2P peuvent être de nature hétérogène : PC, PDA ou téléphone portable. Ils forment un réseau virtuel, à travers un protocole de communication, s'appuyant sur une infrastructure existante.

Les réseaux P2P peuvent être utilisés de manières licites, pour partager des fichiers distribués (plus rapide que le ftp) ou effectuer du travail collaboratif (messages instantanés, calcul intensif, applications partagés, jeux). Une utilisation illicite existe, avec le téléchargement de musique (format mp3…), d'applications ou de films piratés.

Le réseau virtuel se défini suivant différents modèles et différentes topologies P2P.

Nota

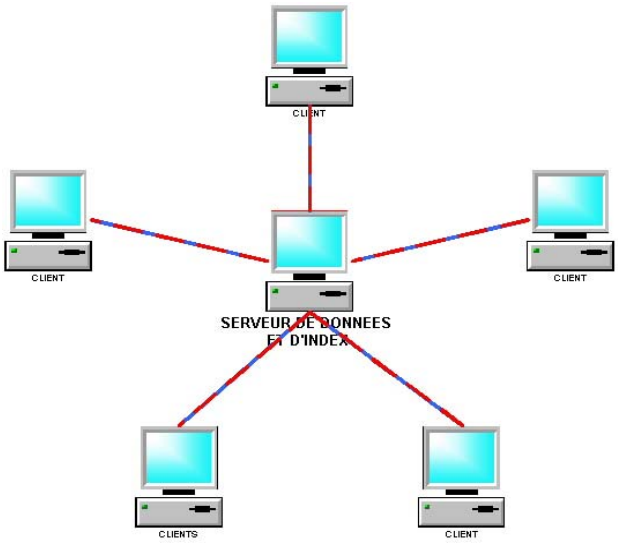
Dans les schémas suivants, les traits bleus représentent le trafic de transfert de données et les traits rouges, les requêtes de recherches de fichiers :

Architecture type I : Système centralisé

Dans cette architecture, chaque client se connecte à un serveur central.

Les avantages de cette solution résident dans une configuration statique, un management centralisé et une asymétrie du réseau.

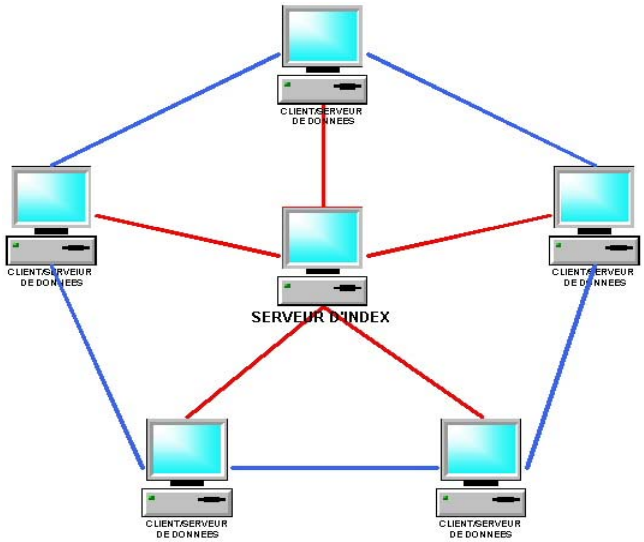
Cependant, ce système n'est plus utilisé actuellement à cause de la simplicité de reconnaissance et de la limitation de la bande passante (point de convergence). Pour rappel, le plus connu était Napster, arrêté en septembre 2001 après des poursuites judiciaires.



Architecture type II : Système décentralisé (ou distribués) à index centralisé

Dans cette architecture, les clients sont en même temps serveurs de fichiers. Seulement l'indexation des fichiers est centralisée.

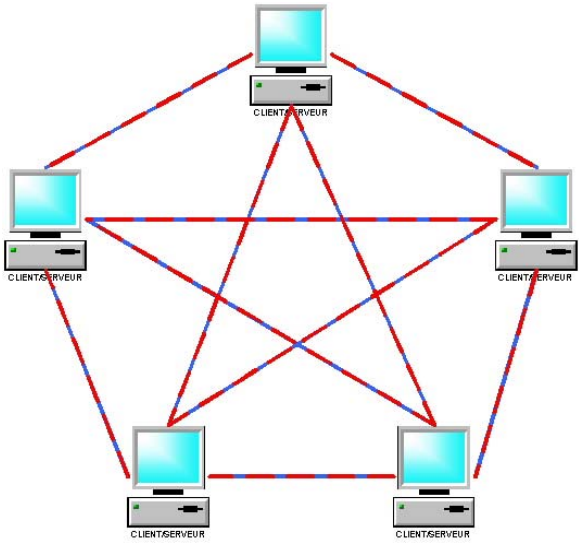
Les avantages de cette solution sont l'auto organisation, la simplicité de découverte des « peers », l'évolution dynamique et la symétrie du réseau.



Architecture type III : Système décentralisé (ou distribué) à index décentralisé

Avec la notion de réseau décentralisé apparaît la notion d'index décentralisé. Sur un réseau de type décentralisé, certains clients agissent comme un serveur d'index pour l'ensemble des clients. Ces serveurs d'index, appelés *ultrapeer*, sont élus notamment en fonction de leurs connectivités et de leurs disponibilités. Chaque requête est soumise au réseau, ensuite traitée itérativement par les *ultrapeers*. Chaque *ultrapeer* agit à la manière d'un proxy pour les autres *ultrapeer* du réseau. La requête est retournée dès lors qu'elle contient un nombre d'objets suffisants.

L'algorithme de recherche *Ultrapeer GUESS* fut un des premiers à être utilisé sur le réseau *Gnutella2*. Depuis, d'autres algorithmes ont été développés notamment par *Kazaa*.



Les échanges Peer-to-Peer (P2P)

Le P2P est un échange direct de ressources et services entre ordinateurs. Chaque ordinateur est responsable du partage de ses propres ressources. Les architectures P2P sont articulées autour de trois composants :

- Un Protocole de communication (ou « réseau P2P ») : il détermine les règles d'échange (adresses, comportements).
- Des clients : ils implémentent les fonctions respectant les règles du protocole ainsi qu'une interface ergonomique.
- Un ou plusieurs serveurs.

Le tableau suivant ventile les différents réseaux P2P connus aujourd'hui suivant les types d'architecture (types I, II, III).

Réseaux P2P	Type d'architecture			Clients
	Type I	Type II	Type III	
WPNP			X	WINMX
FastTrack			X	Kazaa, Kazaa lite, Morpheus, imesh, Grokster
eDonkey2K		X		eDonkey, emule, Shareaza
Overnet			X	eDonkey, Overnet, kDrive
BitTorrent			X	BitTorrent, The Shadow, Experimental, BT, bitTornado, Azureus
SoulSeek			X	SoulSeek
MP2P			X	Piolet, Blubster, RockiNet

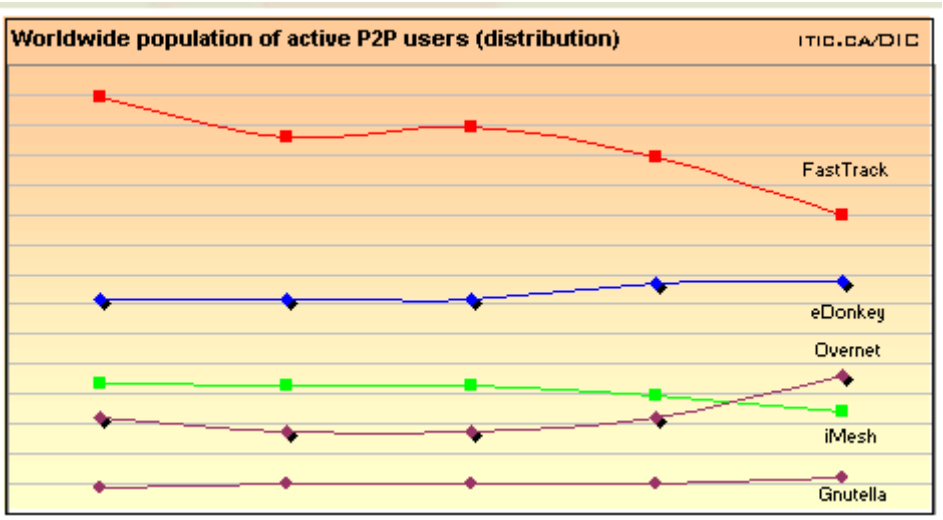
Direct Connect			X	Direct Connect, DC++
Gnutella			X	Gnutella, Shareaza, Gnicleus, LimeWire, BearShare, XoloX, Morpheux
Earthstation 5			X	Earthstation 5
Filetopia			X	Filetopia
Mediaseek		X		Medaiseek.pl
Freenet			X	FCP
JXTA			X	WINMX

Nous pouvons constater que la majorité des réseaux P2P d'aujourd'hui ont une architecture de type III (c'est-à-dire, des système décentralisés à index décentralisé)

Nota

Les réseaux *Freenet* et *JXTA* sont deux réseaux P2P sont au stade du projet. Ils ne pourront être testés dans le cadre de la mission.

Le graphe suivant donne une classification pdes réseaux P2P par nombre d'utilisateurs[7].



[7] Source : Canada : http://www.itic.ca/DIC/News/archive.fr.html daté du 03/06/04.

4.1.4 Identification des flux P2P

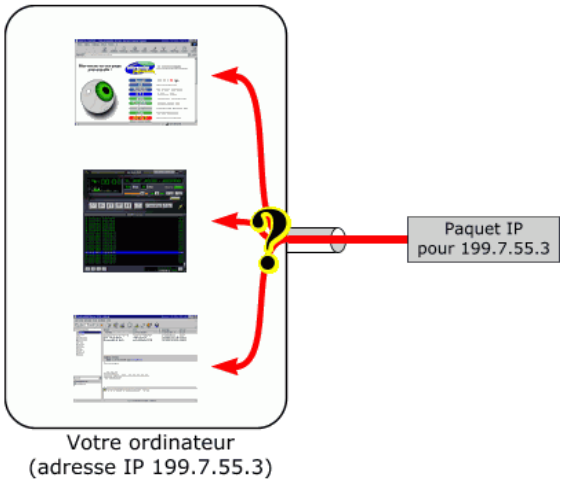
Les clients obéissent aux règles et comportement définis par les réseaux P2P.

Adresses

Sur le réseau Internet, le protocole de communication est IP (*Internet protocol*). Chaque machine sur le réseau possède, pour communiquer avec les autres, une adresse IP.

Ports

Lorsqu'on utilise un ordinateur, connecté en réseau à Internet ou à intranet, il est possible d'effectuer plusieurs taches en parallèle (exemple : naviguer sur Internet et recevoir un nouveau courrier). Ceci implique que l'ordinateur doit être capable d'identifier et de différencier différentes sources d'informations. Chacune de ces applications source d'information se voit donc attribuer une adresse unique sur la machine : un port TCP (ou UDP). Ainsi, une application donnée utilisant un port donné n'interférera pas avec une autre application utilisant un autre port sur la même machine. Cette combinaison, adresse IP plus port TCP (ou UDP), est forcément unique par application.



Les deux tableaux suivants listent les ports les plus connus (ports TCP et ports utilisés pour les échanges P2P)

Port	Application ou service	Description
21	FTP (File Transfert protocol)	Transfert de fichier
23	Telnet	Prise de main à distance
25	SMTP (Simple Mail Transfert Protocol)	Messagerie
53	DNS (Domain name Server)	Résolution de nom
80	HTTP (Hyper Text Transfert ptotocol)	WEB

Exemples de ports utilisés par le P2P :

Application ou service	Port
WPNP	TCP 6669 UDP 6257
FastTrack	TCP 1214 UDP 1214
eDonkey2K	TCP 4661 TCP 4662 UDP 4672 UDP 4665
Overnet	TCP 4661 TCP 4662 UDP 4672 UDP 4665
SoulSeek	TCP 2240 TCP 2834

Signature

Les réseaux P2P ont évolué, ils peuvent aujourd'hui emprunter un port dédié à une autre application (courante comme celle citées précédemment). La méthode consistant à différencier les flux selon le numéro de port utilisé est donc nécessaire mais non suffisante pour pouvoir différencier les flux P2P du reste du trafic. Il est donc nécessaire d'utiliser un système de détection de signatures qui consiste à rechercher un comportement ou une chaîne alphanumérique dans les paquets IP afin d'y retrouver un élément unique particulier d'une session P2P. Par exemple, le terme *Kazaa* se retrouve dans les paquets des flux *Kazaa*.

Exemples de signatures :

Application ou service	Signature
WPNP	Recherche de WinMX
FastTrack	Recherche de FastTrack ou Kazaa
BitTorrent	En début de connexion, les paquets laissent apparaître les clés « .torrent »
MP2P	L'analyse des paquets sur un port aléatoire laisse apparaître la réponse « SIZ<file size in bytes »
Gnutella	L'analyse des paquets laisse apparaître « GNUTELLA CONNECT » lors de l'établissement de la connexion.
Earthstation 5	L'analyse des paquets laisse apparaître un dialogue client serveur spécifique.

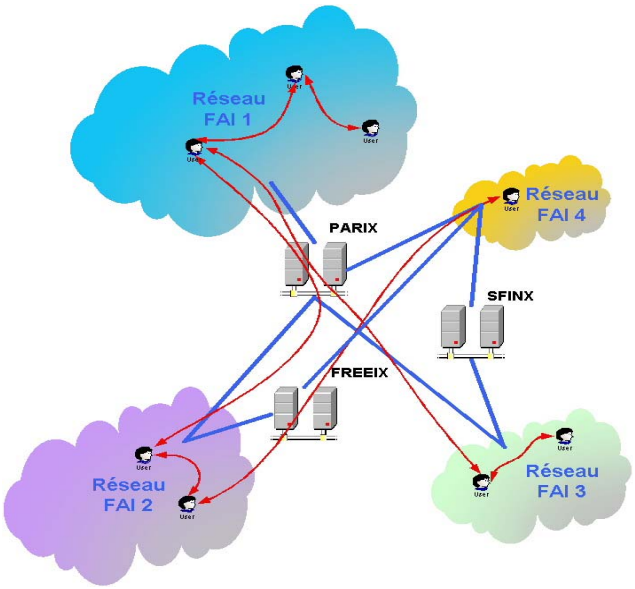
4.1.5 Types d'architectures et localisation

Cette section apporte des précisions sur la localisation potentielle des boîtiers de filtrage pour les différentes architectures haut débit.

Les boîtiers de filtrage peuvent être placés soit entre les FAIs, soit entre l'abonné et le FAI.

Dans la première option, les boîtiers sont placés sur les points de peering ou sur les points d'interconnexion de réseaux. Ce cas permet un filtrage entre FAI mais n'autorise pas le filtrage au sein même du FAI.

La seconde option semble la plus appropriée. Elle est étudiée dans la suite de la présente section sur la base des différentes architectures haut débit.



Peering

Mode de partage des ressources Internet dans lequel deux ou plusieurs fournisseurs locaux acceptent d'interconnecter leurs réseaux

DSL Options 1 et 3

Nous pouvons regrouper ces deux options pour ne traiter qu'un seul cas car leurs architectures sont similaires. Les équipements *BAS* servent à concentrer de 1 à 25 *DSLAM*.

Pour pouvoir filtrer le trafic intra et extra FAI, **les boîtiers de filtrage sont à placer entre les BAS et le réseau « IP core ».**

Les interfaces physiques entre le *BAS* et l'*IP Core* Network sont à priori en *GigaEthernet*. Cependant, il est possible que le niveau liaison ne soit pas en GigaEthernet (en POS : Packet over SDH par exemple).

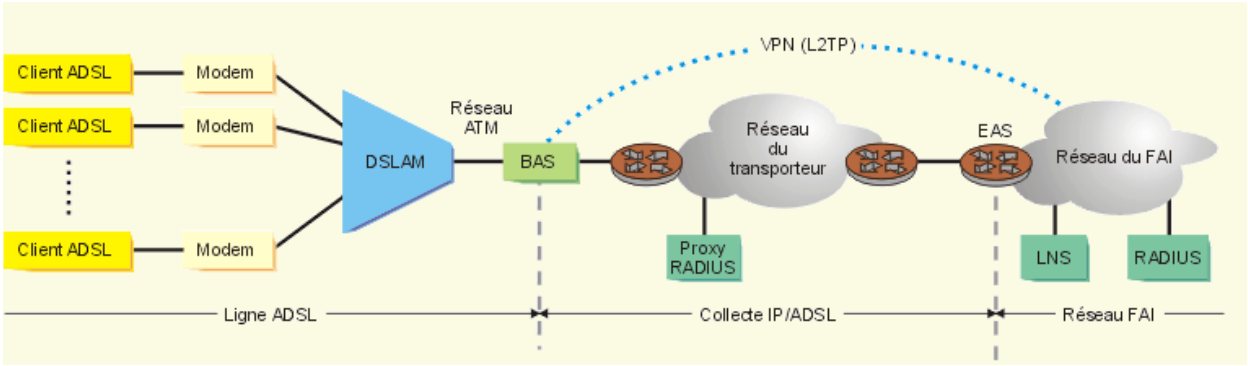
DSL Option 5

Cette architecture est plus complexe.

Il s'agit du FAI qui ne dispose pas d'une infrastructure de transport.

- RADIUS : serveur servant à l'authentification et à l'accounting.

- EAS : Equipement d'Accès au Service (Equipement fourni et géré par le transporteur pour la connexion à son réseau).
- L2TP : Layer 2 Tunneling Protocol donne l'illusion d'une connexion directe entre le FAI et le BAS.



Les spécifications[8] d'accès au Service (EAS) par France Telecom sont très claires. Les niveaux des débits sont les suivants :

- Raccordement 10, 30, 60, 100, 300 et 600 Mbit/s
- Raccordement supérieur ou égal à 1Gbit/s : débit Ethernet (pour les raccordements de débit supérieur à 1 Gbit/s, plusieurs raccordements 1 Gbit/s seront déployés en attendant une solution d'interface unique)

Le tableau suivant donne les principales caractéristiques de l'EAS.

Type de raccordement	Interface	Support	Connecteur	Standard
10 et 30 Mbit/s	Fast Ethernet	100 base T	RJ45	IEEE 802.3u
60, 100, 300, 600 Mbits/s et 1 Gbit/s	Giga Ethernet	1000 Base SX (FO multimode)	SC/PC	IEEE 802.3z

Il y a établissement d'un Tunnel L2TP persistant pour chaque abonné du FAI. L2TP s'établit depuis le BAS (qui joue le rôle de LAC : L2TP Access Concentrator) jusqu'au LNS (L2TP Network Server) du FAI. Après le LNS, le trafic est IP.

En conséquence, le boîtier de filtrage est à placer juste après le LNS qui concentre les abonnés du FAI.

Nota

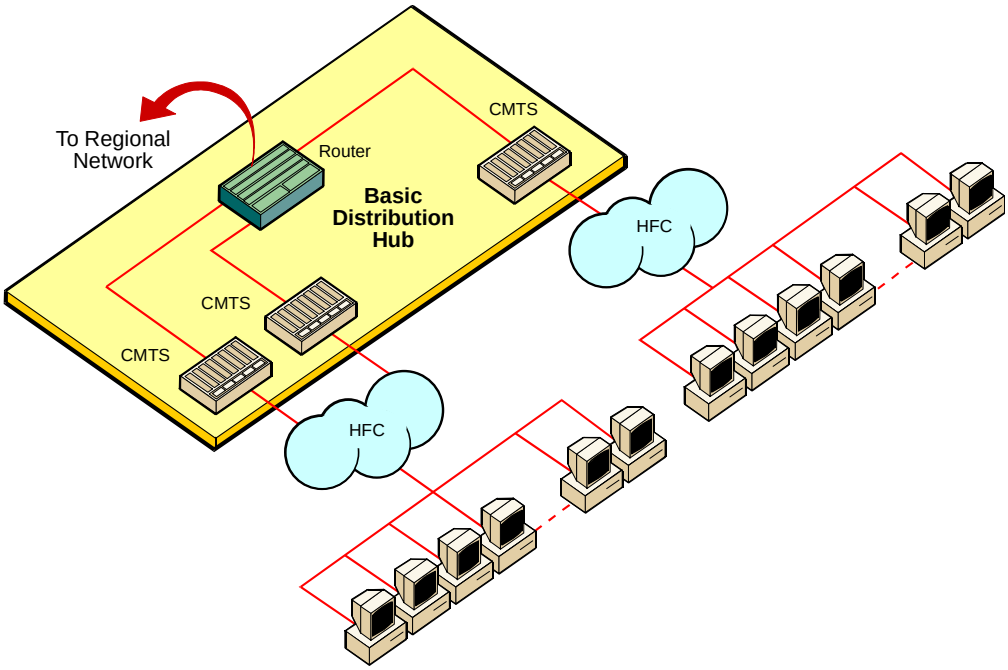
[8] Sur le site de France Telecom, les spécifications de la collecte IP/ADSL sont données, et notamment les interfaces physiques. Voir http://www.francetelecom.com/fr/entreprises/grandes_entreprises/solutions/acces/internet/att00012854/STAS_CIPA.pdf

Avec le DSL Option 5, il n'est pas rare d'avoir chez les FAIs plusieurs LNS (une dizaine par exemple chez NERIM) pour des questions de capacité, de redondance. Dans ce cas, autant de boîtiers de filtrage que de LNS sont à prévoir.

Architectures câbles

L'authentification de l'internaute sur le réseau câblé se réalise via le PPTP server ou le LNS (généralement le routeur d'accès au backbone IP, représenté en haut sur le schéma suivant, qui termine le tunnel pour ensuite aboutir sur un réseau IP).

Il y a création d'un tunnel virtuel de la liaison point à point.



En conséquence, le boîtier de filtrage est à placer derrière le LNS (comme pour le cas de le DSL Option 5).

4.2 CHOIX DE SOLUTION

4.2.1 Solutions du marché

4.2.1.1 Typologie des solutions

Les outils d'optimisations de réseaux (QoS)

Les outils de QoS (Qualité de Service) sont des *Appliances* (solution packagées : matériel /logiciel) permettant la gestion des priorités des flux.

Ils ont été conçus à l'origine pour classer les flux Internet afin de leur donner une priorité destinée à gérer la bande passante d'un réseau. Ils peuvent ainsi limiter (le blocage étant un cas particulier de limitation) le débit pour un type de flux, et garantir ainsi une qualité de service pour les flux de données critiques.

L'implémentation de la QoS est systématiquement en « coupure », c'est à dire que le trafic à analyser doit passer au travers de *l'appliance* afin d'être traité.

Les IDS/IDP (Intrusion Detection and prevention)

Les IDS/IDP sont des *Appliances* qui permettent de détecter et/ou de prévenir une attaque Internet. Ces outils ne possèdent pas la faculté de trier les différentes sessions par flux ; ils se contentent d'analyser chaque paquet afin d'y retrouver soit un comportement, soit une signature connue.

Il est possible de placer ce type d'appliance soit en « coupure » (comme pour la QoS), soit en « port mirroring » (redirection du trafic pour analyse).

Les Flow-Based Switch

Les « flow based » switch sont des commutateurs qui n'agissent plus par reconnaissance exacte du trafic mais par classification par flux. Il est en effet possible de catégoriser les flux générés par le trafic Internet en fonction du type de trafic. On différencie ainsi le trafic interactif du trafic non interactif qui est typiquement un trafic P2P. Cependant, la plupart de ces *Appliances* n'intervenant pas au niveau applicatif, il est difficile de ne pas impacter d'autres trafics comme le FTP Passif.

4.2.1.2 Différents acteurs

Le tableau suivant liste les principales solutions de filtrage du marché. Le choix de solution est réalisé parmi ces solutions

Types de solutions	Principales acteurs du marché
Solutions orientées « QoS »	ALLOT - Netenforcer KAC1020 Packeteer - PS 8500 ISP Sandvine - PPE8200 IPANEMA
Solutions orientées « Flow based switch »	Ellacoya 1600 - E12TX - E2GIG - AC Caspian Networks - Apeiro P-Cube
Solutions orientées filtrage réseaux	Routeurs Firewall (Cisco, Checkpoint, …)
Solutions orientées IDS/IDP	Netscreen IDP1000
Solutions orientées filtrage de contenu	Audible Magic

Afin de pouvoir constituer une shortlist, nous avions procédé dès le début à l'élimination de solutions sur la base de certains critères.

Les solutions écartées ont été les suivantes :

- Une solution à base de reconnaissance d'œuvre (par fingerprint) comme Audible Magic. Aucune information précise sur son fonctionnement, ses capacités, etc. Sa capacité à traiter à la volée un flux important paraît incertaine. La reconnaissance par œuvre implique de référencer chaque œuvre et impose donc une grande réactivité et une administration lourde. Dans le cas de réseaux P2P avec chiffrement du contenu, ce type de solution sera certainement aveugle.
- Les solutions de types Firewall (PIX Cisco, Checkpoint FW-1, …). Comme nous l'avons vu précédemment (et tester lors de la maquette), les filtrages sur adresses IP et sur les ports ne sont pas suffisants.
- Les solutions dont les informations disponibles en ligne étaient insuffisantes pour une première évaluation comparative.

    - *Ipanema technologies – Ipanema.(QoS)*

      Cette société n'a pas souhaité répondre à la demande d'information quant à son aptitude à filtrer les trafics P2P.

    - *Sandvine – PPE8500 ISP (QoS)*

      Cette *appliance* ne permet que 7500 connexions concurrentes, ce qui est trop faible rapporté au débit. Il existe un nombre important de protocoles. Cependant l'acquisition des licences se fait par protocole.

    - *Netscreen - IDP 1000 (IDS/IDP)*

Cette appliance se présente sous la forme d'un logiciel et d'un serveur DELL 1750.Ce serveur possède une interface Gigabit sur port cuivre, qui du fait de la limitation du bus PCI ne semble pas être à même de traiter plus de 250 Mbit/s. le logiciel de gestion de l'IDP 1000 permet de créer des signatures pour toutes sortes de protocole. Mais il n'existe pas de signatures déjà existantes pour l'ensemble des protocoles P2P de façon native. Pour compléter les fonctionnalités, il faut en faire la demande spécifique à Netscreen. Sur ce point la réactivité de l'éditeur n'est pas certaine. Il s'agit avant tout d'un produit orienté sécurité.

- *Caspian Networks – Apeiro (Flow Based Switch)*

  Solution qui a été envisagée car seule solution avec Switch ATM. Trop peu d'informations. Pas d'analyse applicative formelle permettant une classification des protocoles P2P au niveau application (impact sur les applications avec port dynamique telle que FTP passif)

- *P-Cube (Flow Based Switch)*

  Sa solution Flow-based semble intéressante. Cependant aucune documentation précise n'est disponible en ligne[9].

La shortlist retenue dans le cadre de l'étude est la suivante. Trois solutions constituent cette shortlist.

Types de solutions	Shortlist (solutions retenues pour l'étude comparative)
Solutions orientées « QoS »	ALLOT - Netenforcer KAC1020 Packeteer - PS 8500 ISP
Solutions orientées « Flow based switch »	Ellacoya 1600 - E12TX - E2GIG - AC
Solutions orientées filtrage réseaux	Néant
Solutions orientées IDS/IDP	Néant
Solutions orientées filtrage de contenu	Néant

[9] La société n'est pas représentée en France

4.2.2 Grille de critères pondérés

Une grille de critères a été élaborée pour évaluer les différentes solutions de filtrage retenues.Les différentes catégories de critères sont :

- Reconnaissance du filtrage.
- Actions de filtrage.
- Performances.
- Administration.
- Implémentation.

Nota

Il n'a pas été pris en compte les éléments financiers.

Les critères seront notés selon le barème suivant :

Note	Explication
0	Fonction non supportée
1	Faible
2	Normale
3	Fort

A chaque critère est affecté un coefficient permettant de déterminer son niveau d'importance dans le contexte du SNEP. Le tableau suivant en présente les différentes valeurs possibles.

Pondération	Explication
1	Peu important
2	Important
3	Très important

Le mode d'évaluation définit le score de chaque critère de la façon suivante :

[Score $_{critère}$ = Note * Coefficient contextuel]

La grille de critères est détaillée ci-dessous.

Critère	Coefficient contextuel
Reconnaissance du filtrage	
Classification par signature	3
Classification par port : • TCP, UDP • Source • Destination	2
Classification par adresse : • Source • Destination	2
Actions de filtrage	
Blocage du trafic	3
Limitation du trafic : • Entrée • Sortie	1
Nombre maximum de réseaux P2P filtrables[10]	1
Performances	
Tenu en charge (capacité à traiter la charge en environnement de production)	3
Nombre de connexions simultanées	3
Administration	
Fonctionnalités	2
Sécurité (port de management) • Séparation des interfaces d'administration et d'analyse • Journaux	3
Implémentation	
Transparence (bypass) et redondance (électrique)	3
Support	2
Interfaces physiques[11]	1

[10] Coefficient de 1, car aujourd'hui il existe peu de réseaux P2P (de l'ordre de la dizaine).

4.2.3 Grille de critères notés

La grille de critères notée se trouve ci-dessous.

Critère	Coéff contextuel	ALLOT		Ellacoya		Packeteer	
		Note	Point	Note	Point	Note	Point
Reconnaissance du filtrage							
Classification par signature	3	3	9	3	9	3	9
Classification par port	2	3	6	3	6	3	6
Classification par adresses	2	3	6	3	6	3	6
Actions de filtrage							
Blocage du trafic	3	2	6	2	6	2	6
Limitation du trafic	2	2	4	2	4	2	4
Nombre Maximum de réseaux P2P filtrables	1	3	3	3	3	3	3
Performances							
Tenue en charge	3	2	6	3	9	1	3
Nombre de connexions simultanées	3	3	9	2	6	2	6
Administration							
Fonctionnalités	2	2	4	2	4	2	4
Sécurité	3	2	6	2	6	2	6
Implémentation							
Transparence	3	2	6	2	6	2	6
Support	2	2	4	1	2	2	4
Interfaces physiques	1	2	2	2	2	2	2
TOTAL	**30**		**71**		**69**		**65**
Note ramenée sur 10			**7,9**		**7,6**		**7,2**

[11] Coefficient de 1 car des contournements sont possibles à travers l'ajout d'équipements spécialisés dans le changement de medium physique.

4.2.4 Conclusion

Les solutions ALLOT et Ellacoya semblent en mesure de pouvoir répondre favorablement à la problématique de filtrage sur haut débit.

Packeteer obtient la note de 1 dans la rubrique performance pour la tenue en charge. Pour la problématique considérée, cette note est éliminatoire. En effet cette solution ne supporte qu'au maximum un débit de 200 Mbits/s, c'est insuffisant dans un contexte opérateur.

Il est à noter que la société Ellacoya n'a pas de représentant en France (d'où la note de 1 pour la partie support)

Compte tenu des contraintes du planning de la mission et des disponibilités des matériels, nous nous sommes limités au niveau des tests à la solution ALLOT.

4.3 ELEMENTS DE COUT

Il s'agit de donner une indication uniquement sur les prix d'acquisition des boîtiers de filtrage ALLOT. Les autres coûts (maintenance, infogérance…) ne sont pas intégrés à cette estimation.

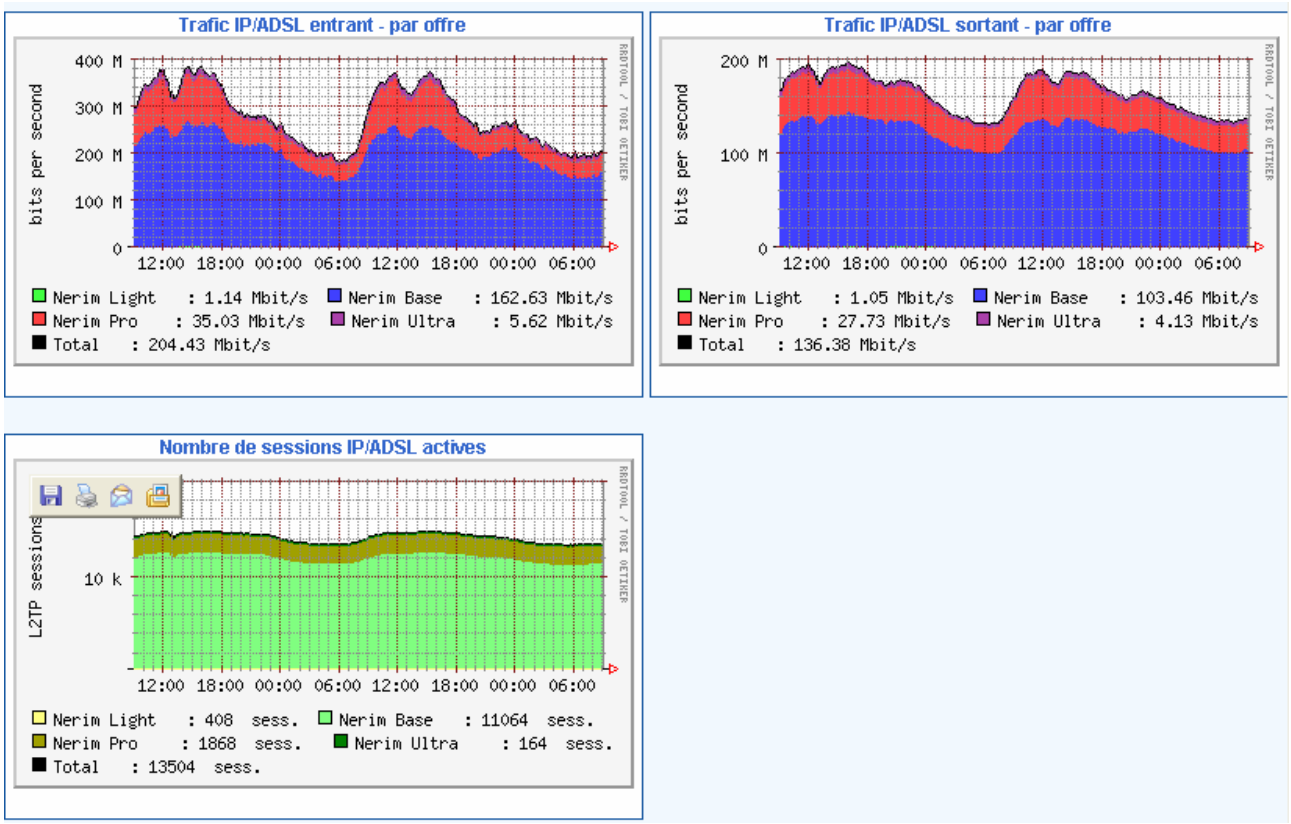
Le coût d'acquisition correspond à un investissement fait 1 fois pour filtrer définitivement un utilisateur[12].

Hypothèses

Le calcul tient compte du :

- Hypothèse de validation qu'un boîtier Gigabit ALLOT par BAS est cohérent à travers l'étude du FAI NERIM.
- Nombre d'équipements BAS chez France Telecom.
- Part de marché (nombre d'abonnés) de France Telecom sur le haut débit.

Etude du cas du FAI NERIM[13]



[12] Sous réserve de suivi du développement de nouveaux protocoles P2P.

[13] Source : NERIM fournit en ligne les statistiques sur sa collecte IP/ADSL à l'URL suivante : http://stats.nerim.net/nav/cipa/

Nous pouvons constater que 13 500 utilisateurs sont connectés de manière concurrente pour un débit de 341 Mbits/s (la moyenne du max entre trafic entrant et sortant) ; soit 26 Kbits/s en moyenne par utilisateur.

Nombre de BAS chez France Telecom

On peut consulter à l'adresse URL suivante la localisation et le nombre de BAS chez France Telecom. Aujourd'hui, ce nombre avoisine les **143 BAS**.

http://www.francetelecom.com/fr/entreprises/grandes_entreprises/solutions/acces/internet/att00012854/caracteristiques.html

Si nous prenons comme hypothèse un BAS Juniper ERX 1440 avec 64 000 connexions :

26 Kbits * 64 000 = 1,66 Gbps.

En sachant que :

- Les ERX1440 sont à priori les plus gros BAS de France Telecom..
- Il est peu probable que les ERX14000 soient configurés pour accueillir 64 000 connexions.
- Le nombre de connexions serait plutôt limité à 32 000.

L'hypothèse donc d'un boîtier de filtrage Gigabit par BAS paraît cohérente.

En sachant que :

- Le nombre d'utilisateur par BAS redback SMS1800 est : 8 000 ou 16 000
- Le nombre d'utilisateurs par BAS Juniper ERX1400 est : 32 000 ou 64 000
- Il y a 40 BAS Redback et 103 BAS Juniper[14]
- 40 * 8000 + 103 * 32 000 = 3 616 000, ce chiffre, qui représente le nombre d'abonnée ADSL que peuvent accueillir les BAS France Telecom, parait cohérent avec le nombre d'abonnés qui passent par leurs BAS : 80% des 3 millions d'abonnés ADSL, soit 2 400 000.

Part de marché France Telecom

En sachant que France Telecom/Wanadoo représente 81% du trafic Internet haut débit soit 2430 000 abonnés.

Coût d'acquisition des boîtiers ALLOT

Le modèle KAC 1010/1G-PS-I-IT Ce modèle support le Gigabit, avec 256 000 connexions.

[14] France Telecom aurait acquis en 2000 40 Bas Redback : www.dslvalley.com/news/news.php3?id=12

Cas de la collecte France Telecom

Le prix public du boîtier ALLOT est : 75 888 Euros.

Avec l'hypothèse d'une remise de 37 %, le prix est : 47 810 Euros.

Prix remisé par abonné : 47 810 * 143 / 2430 000 = 2,82 Euros.

A noter que ce cas représente 81% des abonnés ADSL (réseau France Telecom) auquel devaient s'ajouter Free et LDcom qui disposent d'architectures comparables à celle de France Telecom.

Cas FAI option 5 et câble

Ce cas représente moins d'abonnés que le précédent.

Rappel : du fait de la nécessite de créer un tunnel entre les abonnés et les LNS du FAI, l'élément de filtrage devra être intégré après le LNS. Le raisonnement économique est donc fonction du nombre de LNS et de leurs caractéristiques, notamment le débit.

Prenons une étude de cas avec NERIM

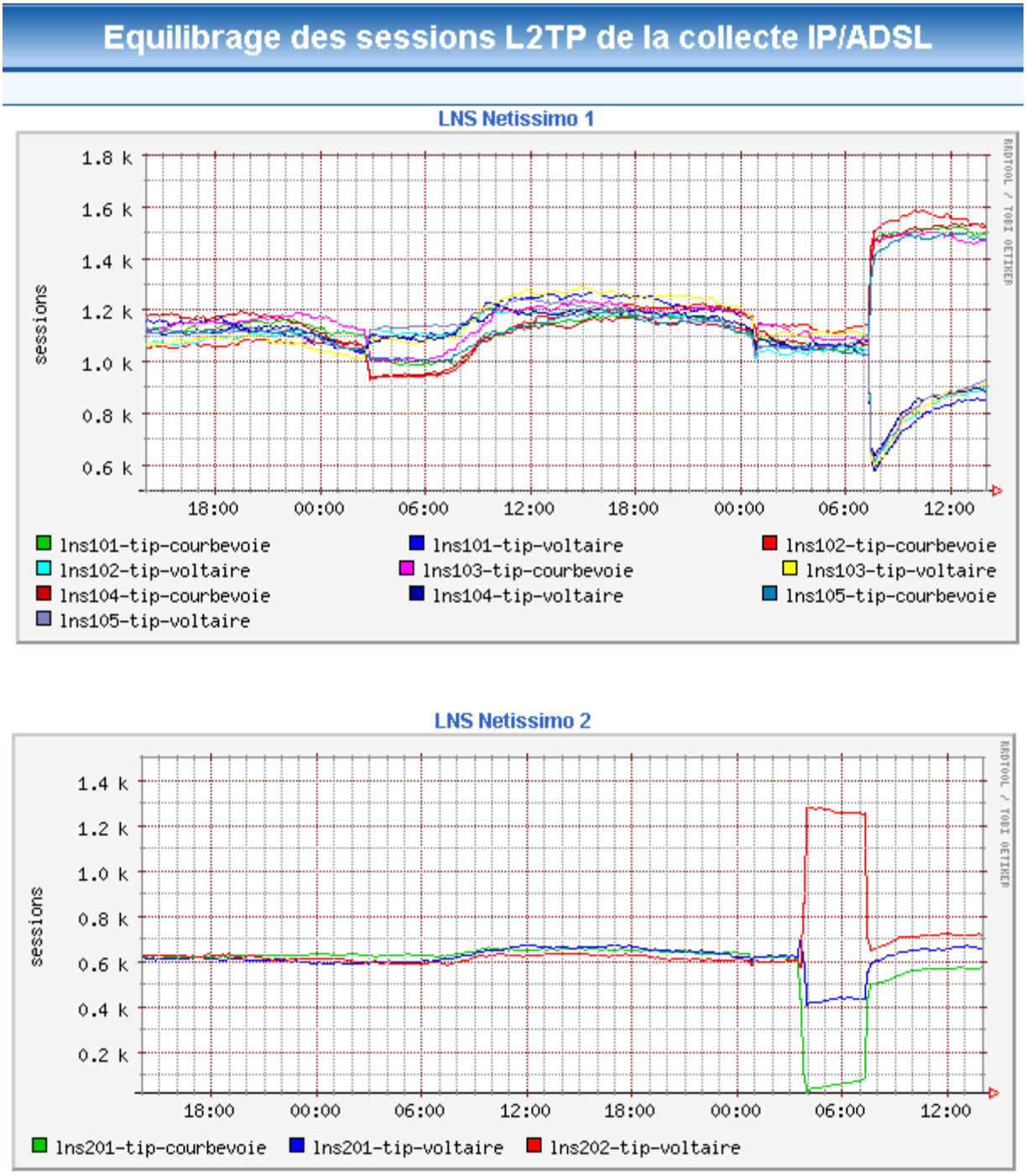
Soit 13 LNS : http://stats.nerim.net/nav/equ_sess/

Environ 15000 abonnés connectés à un instant. Hypothèse prise pour le taux de connexion : 70%.

15000 / 0,7 = 21500 abonnés au total

Soit en moyenne 1 LNS pour 1650 abonnés. Ceci semble cohérent avec les données fournies le 29 juin à 14h avec 14500 abonnés connectés.

Répartitions des sessions sur les LNS : http://stats.nerim.net/nav/equ_sess/



Les besoins en terme de performances ne seraient alors pas les mêmes que pour le cas précédent.

On peut essayer d'encadrer le prix d'acquisition d'une solution de filtrage par abonné entre le plus petit matériel potentiellement répondant à la solution et celui vu dans le cas précédent :

21 500 / 13 = 1653 abonnés en moyenne par LNS

1653 * 26 Kbps = 43 Mbps.

Il faut donc au minimum un boîtier traitant le 100 Mbps.

ALLOT KAC 402/100M-DK (2 ports 10/100, jusqu'à 100 Mbps de bande passante et 96 000 connexions simultanées)

Le prix public de ce boîtier est de : 18 360 Euros.

Avec l'hypothèse d'une remise de 37 %, le prix est de : 11 566,8 Euros.

11566,8 /1653 = 7,0 Euros par abonné

Comme pour le cas précédent, si on part sur un ALLOT devant traiter de part la structure du FAI le Gigabit, alors le prix par abonné est le suivant :

47 810 / 1653 = 28,9 Euros.

En conclusion, l'encadrement du prix d'acquisition est le suivant :

7,0 Euros < Prix par abonné < 28,9 Euros.

4.4 MAQUETTE

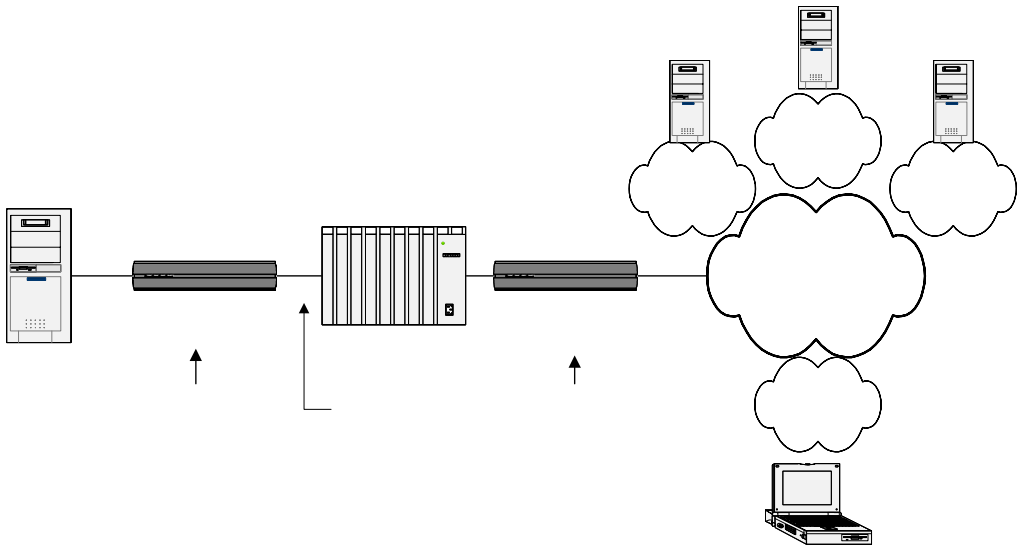
La maquette utilisée veut adresser deux objectifs :

- Tests quantitatifs : limitation des flux P2P et capacité à traiter du trafic Gigabit.
- Tests qualitatifs : identification et blocage des flux P2P.

L'architecture de la maquette qui a été utilisé est la suivante :

4.4.1 Architecture

L'architecture de la maquette qui a été utilisé est la suivante :



De gauche à droite :

- Un PC avec des clients P2P (Kazaa, eDonkey,…), pour corroborer les analyses du Boîtier ALLOT n°1 quant à sa capacité à bloquer ou limiter le trafic P2P
- Le boîtier ALLOT N°1 a pour objectif le blocage ou la limitation du trafic P2P. Il s'agit d'un AC402/100M avec une version software 5.1
- L'équipement réseau à pour but de valider les informations de charge remontées par le Boîtier ALLOT N°1 (on ne peut pas se fier uniquement aux données du boîtier si on veut le tester, il faut un tiers).
- Le boîtier ALLOT N°2 est un modèle supportant un trafic Gigabit, il est positionné entre Internet et des serveurs (non représentés sur le schéma, derrière l'équipement réseau) pour s'assurer de sa capacité à supporter un trafic proche du Gigabit par seconde. Il s'agit d'un AC1020-SP1/1G avec une version software 5.1.1.
- Un PC qui nous permettait de prendre la main sur les 4 éléments précédents.

4.4.2 Protocole test

Nous avons dans un premier temps testé chaque réseau P2P de manière séparé.. Pour chacun de ces réseaux, nous avons identifié un client propre à ce réseau, et quand cela n'a pas été possible, nous nous sommes assuré qu'il n'utilisait qu'un seul réseau (client eDonkey sur réseau Overnet)

Ensuite nous avons testé tous les réseaux en même temps.

Nota

Les résultats des tests sont présentés en annexe.

Le FAI semblent procéder à du filtrage.

Analyse réseau par réseau

Nous avons identifié 5 tests qui peuvent être exécutés dans n'importe quel ordre. On commencera chacun de ces tests en démarrant un client du réseau P2P considéré. Et on finira chaque test en stoppant le client.

Ces opérations d'arrêts / redémarrage du client sont nécessaires car le boîtier ALLOT ne perturbe pas les flux dont l'initiation était autorisée. Il faut donc les « terminer » manuellement. Ceci permet aux nouvelles connexions de se conformer aux nouvelles règles définies.

Pour chaque test nous relèverons les débits entrants et sortants sur l'ALLOT N°1 et sur le port du switch connecté à L'ALLOT N°1 (qui sert de tiers de confiance, de référentiel). Les valeurs sur le switchs étant moyennées (arithmétiquement) sur 5 minutes, chaque test durera 5 minutes.

Test	Désignation	Description
1	Recherche et transfert sans filtrage	On démarre un client P2P compatible avec le réseau P2P à tester et on lance une recherche sur un artiste, et on lance plusieurs téléchargements en parallèle pour avoir le maximum de débit en téléchargement sur plus de cinq minutes.
2	Recherche et transfert avec blocage (port et/ou signature)	On positionne un filtre sur le Boîtier ALLOT N°1 pour bloquer tout le trafic du réseau considéré peer to peer considéré. On active ce filtre. On démarre un client P2P compatible avec le réseau P2P à tester et on lance une recherche sur un artiste. Puis, si la recherche est probante, on lance plusieurs téléchargements en parallèle pour avoir le maximum de débit en téléchargement sur plus de cinq minutes Le but de cette étape est s'assurer que le trafic du réseau P2P est bien bloqué.
3	Recherche et transfert avec limitation	On positionne un filtre sur le boîtier ALLOT n°1 visant à limiter le trafic de téléchargement comme suit : • Maximum 50 Kbps téléchargement, pour le réseau P2 considéré, en In (soit de l'internet vers le client qui télécharge) • Maximum 10 Kbps téléchargement, pour le réseau P2

		considéré, en Out (soit du PC client vers l'internet). Le but de cette étape est de vérifier que le boîtier de filtrage est bien capable d'identifier le trafic du réseau P2P considéré et de limiter la bande passante qui lui ait allouée. Nous avons positionné des valeurs de limitation de trafic montant et descendant sensiblement différente pour nous assurer que la limitation est bien effective dans les deux sens. Les tests 4 et 5 par rapport à la problématique soulevée n'apportent rien, elles servent à comprendre en partie les mécanismes de recherches et transferts des réseaux P2P et s'assurer que le choix de la solution avec filtrage par signature est justifié (excluant toute solution basé uniquement sur un filtrage par ports ou adresses IP)
4	Blocage des ports	Le but de cette étape est de vérifier si un filtrage par ports (statiques) est nécessaire et suffisant. Comme pour les étapes précédents, deux fonctionnalités sont testées : la recherche des titres disponibles d'un artiste et le transferts de titres.
5	Blocage par signature	Le but de cette étape est de vérifier si un filtrage par signature est nécessaire et suffisant. Comme pour les étapes précédents, deux fonctionnalités sont testées : la recherche des titres disponibles d'un artiste et le transferts de titres.

4.4.3 Recette et commentaires

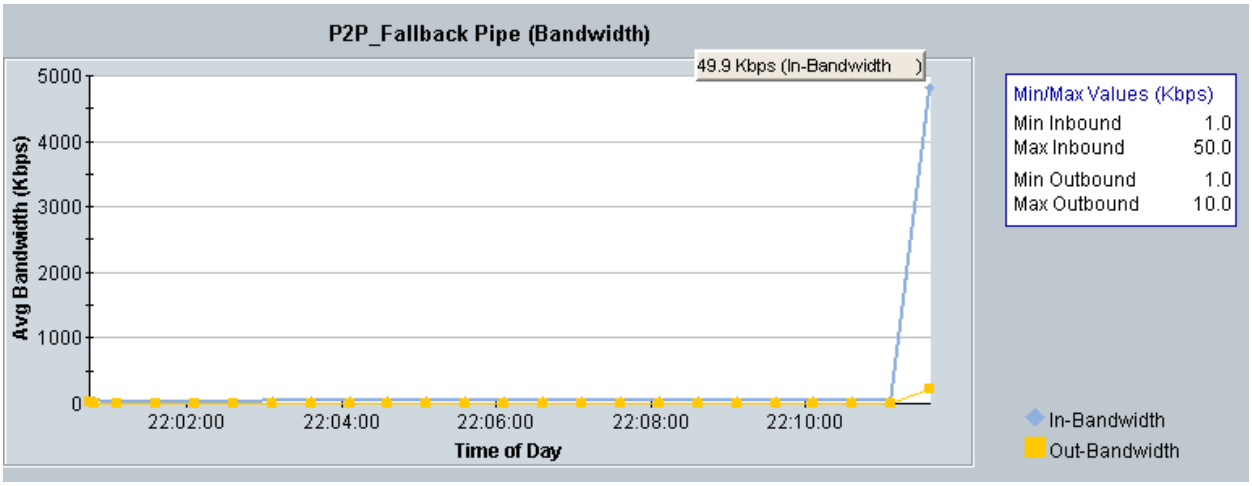
Blocage et limitation d'un réseauP2P

Réseau P2P	Client	Capacité à bloquer le trafic P2P	Capacité à limiter le trafic P2P
WPNP	WINMX v 3.31	Oui	Oui
FastTrack	Kazaa v 2.6.3	Oui	Oui
eDonkey 2000	eMule v0.42g	Oui	Oui
Overnet	eDonkey 2000 v0.53	Oui	Oui
Bit Torrent	Bit Torrent v 3.4.2	Oui	Oui
SoulSeek	SoulSekk v152	Oui	Oui
MP2P	Blubster v 2.5	Oui	Oui
Direct Connect	Direct Connect	Oui	Oui
EarthStation 5	EarthStation 5 v 2.0.11	N/A	N/A
Filetopia	Filetopia v 3.04d	Oui	Oui
Gnutella	Limeware v 4.0.6	Oui	Oui
Mediaseek	Mediaseek.pl	N/A	N/A

Nota

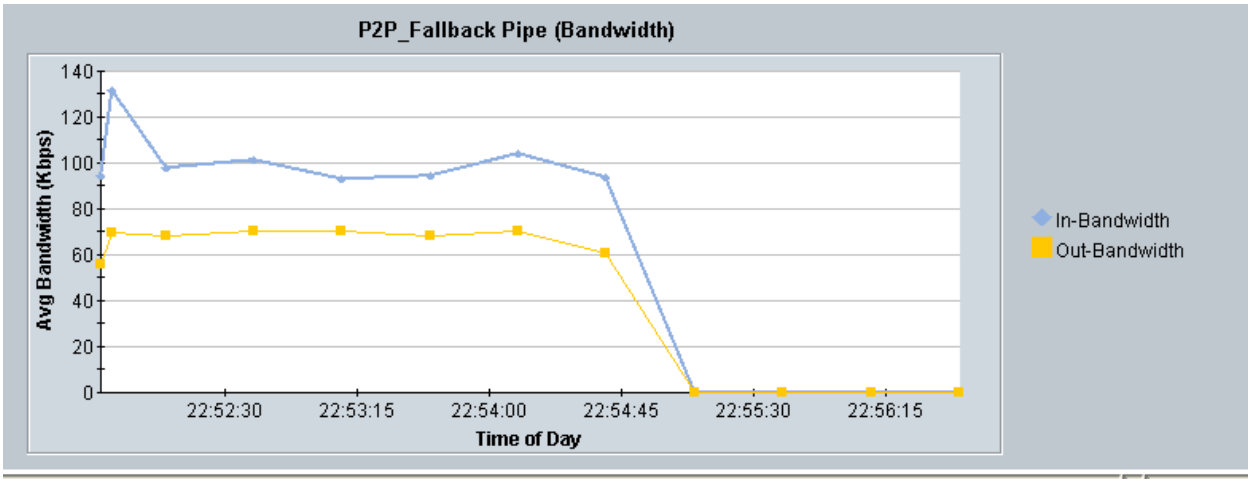
- La valeur « Oui » dans la colonne « Capacité à bloquer le trafic P2P » signifie qu'il n'a pas été possible de transférer des données.
- La valeur « Oui » dans la colonne « Capacité à limiter le trafic » signifie que la limitation de trafic obtenue est conforme aux attentes soit 50 Kbps maximum depuis Internet et 10 kbps maximum vers Internet.
- L'instabilité du client Earthstation 5 et l'impossibilité de faire fonctionner le client Mediaseek ne nous ont permis de tester les deux réseaux P2P associés.

Transfert de fichiers



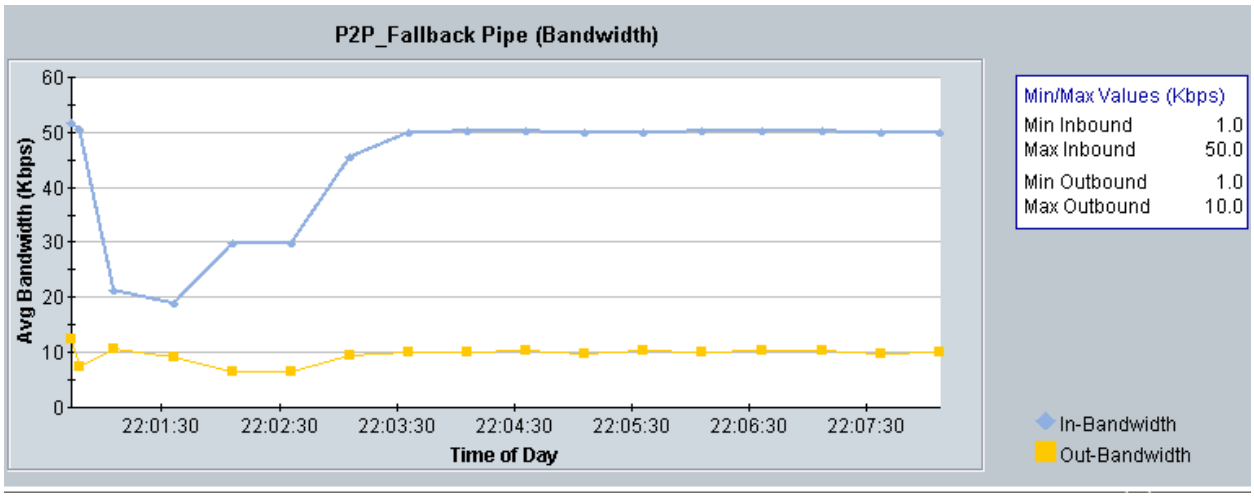
A 22 :11 :30, nous avons désactivé la limitation de trafic sur le réseau P2P WPNP. Nous pouvons voir que le téléchargement qui était bridé à 50 Kbps (la valeur indiquée en haut à droite du graphe correspond à la valeur du trafic entrant à 22 :11) passe d'un coup à 5 Mbps.

Blocage du traffic



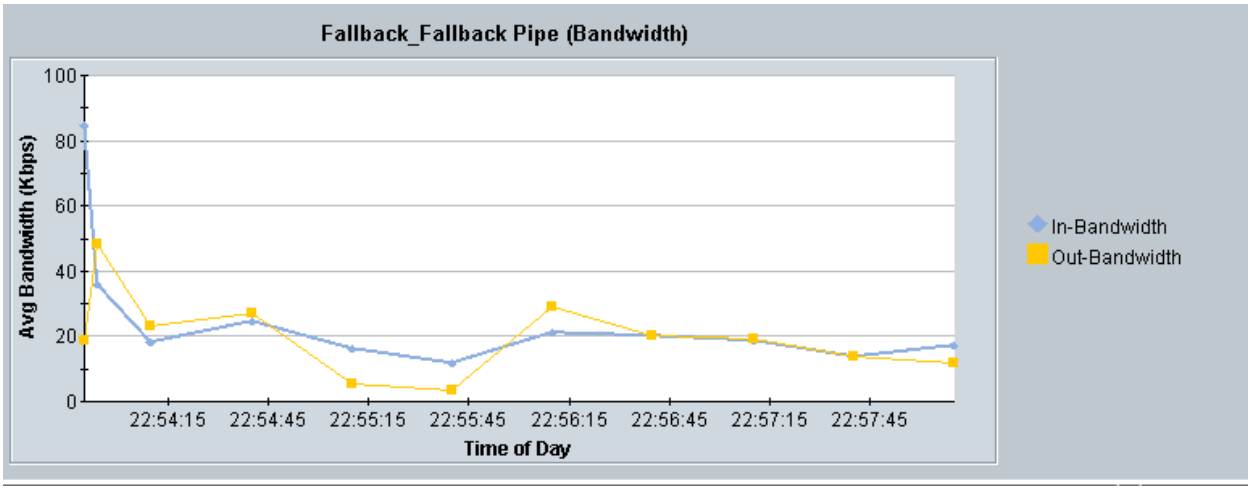
Nous pouvons constater, sur ce graphe, la mise en œuvre à 22:55 d'un filtre visant à bloquer le flux du réseau P2P WPNP

Limitation de trafic sur un réseau P2P



Il s'agit de la vérification de l'application de la limitation du trafic WPNP. Les valeurs attendues sont bien respectées. Ces valeurs sont corroborées avec celles données par le commutateur (qui fait office de tiers de confiance pour les mesures).

Trafic résiduel



Il est à noter qu'il y a un petit décalage entre les valeurs données par le boîtier ALLOT et les valeurs données par le Switch (elles sont toujours du même ordre de grandeur). Ces différences sont dues pour la plupart par le trafic d'administration (la connexion de notre PC de prise de main sur le PC client P2P, sur le Boîtier ALLOT N°1 et sur le switch L3).

Blocage d'un ensemble de réseau P2P

Nous avons regroupé des réseaux P2P : WPNP, Fasttrack, eDonket2000, Overnet, BitTorrent, SoulSeek, MP2P, Direct Connect, Filetopia, EarthStation5, Filetopia, gnutella.

Nous avons défini une règle bloquant tous ces réseaux sur l'ALLOT N°1 et nous l'avons appliqué.

Il n'a pas été possible de transférer des fichiers via ces réseaux.

Nous avons fait des tests en parallèle pour nous assurer que ces filtrages étaient bien limitées aux réseaux P2P définis dans les filtres. Avec le filtre actif sur l'ensemble des réseaux P2P, nous avons pu sans problème naviguer sur Internet et transférer un fichier par FTP (service de transfert de fichier classique).

Nota

Nous n'avons pu comme pour les tests unitaires, tester :

- EarthSation5 : Le client était très instable
- Mediaseek.pl : nous n'avons pas réussi à le faire fonctionner

Filtrage sur une adresse

De même, il est possible de filtrer ou bloquer le trafic depuis ou vers une adresse (IP ou FQDM de type www.nom.fr)

Une « black-list » avec 3 noms a été établie et appliquée. Son application entraîne l'impossibilité de se connecter aux trois sites depuis le poste de Test

Il n'a pas été mené de test de limitation de trafic vers ces sites. Cependant, à cette règle comme à celle défies pour les protocole P2P, nous pouvons appliquer la limitation de trafic.

Montée en charge

Le boîtier ALLOT n°2 (ALLOT 1020) a été utilisé sur un réseau de production pendant 1 semaine.

La somme des débits MAX (en entrée et sortie) sur la semaine est : 603 Mbps

La somme des débits moyens (en entrée et sortie) sur la semaine est : 207 Mbps

Nous constatons un fonctionnement avec 600 Mbps vers Internet sur les graphiques ci-dessus.

Le boîtier supporte correctement des flux importants (de l'ordre de Gigabit/s).

4.5 IMPACTS

Les principaux impacts des solutions de filtrage sont :

Impacts techniques

La solution doit pouvoir :

- Offrir un niveau de sécurité important pour éviter les by-pass.
- S'intégrer dans l'architecture des FAIs existantes.
- Etre apte à tenir les charges (démontrée par cette étude).
- Avoir les informations nécessaires à sa supervision.
- Avoir une interface d'administration simple.

Pérennité des solutions de filtrage

De nouveaux réseaux P2P peuvent exister à l'avenir. En conséquence, il est important que la solution assure :

- Une veille technologique.
- La maintenance des solutions de filtrage en apportant les « correctifs » utiles.

  La solution une fois en place doit être couverte par une maintenance et un support nécessaire pour minimiser les risques de pannes (même si les équipements permettent d'appliquer des by-pass en cas de chute).

  A la vue du nombre d'éléments actifs à implémenter, il est important que l'architecture soit supervisée et administrée avec les moyens adéquats :

  - Soit par une société d'infogérance réseau et sécurité :
    - Avantages :
      - Les configurations des éléments actifs resteront homogènes sur les différents FAI (contrôle de l'application).
      - L'administration restera centralisée.
      - Il sera possible d'obtenir des remises plus importantes aux vues des remises liées à l'activité.
    - Inconvénients :
      - Il risque d'y avoir des opérateurs qui refusent ce principe puisque cela donnera la vue sur les flux de leurs clients.
  - Soit directement par les opérateurs
    - Avantages :
      - Les opérateurs accepteront plus facilement la solution qui leur permettra d'augmenter les possibilités de leur réseau.
    - Inconvénients :
      - Les configurations des éléments actifs ne seront pas homogènes sur les différents FAI. Il est possible que les FAIs déconnectent le système sans en informer le SNEP.

5. CONCLUSION

La solution ALLOT nous a permis de valider la faisabilité technique du filtrage sur haut débit.

Pour plus de 80% des abonnés haut débit, le coût matériel de mise en œuvre d'une solution de filtrage est évalué à 2,82€ HT par abonné investi une fois et permettant un filtrage définitif[15].

Sachant que certains FAI semblent actuellement filtrer les flux Peer to Peer au niveau des ports, il est important d'étudier les moyens déjà mis en place chez les opérateurs et comment les réutiliser à coûts minimums.

Il sera notamment nécessaire d'évaluer l'impact des réductions de coûts sur le dimensionnement des infrastructures réseaux réalisées grâce au filtrage. De sources concordantes le trafic issu du Peer to Peer représente France plus de 50 % de la bande passante totale utilisée sur le réseau Internet national.

Le filtrage serait donc de nature à :

- désengorger les réseaux,
- permettre de substantielles réductions des investissements liés au dimensionnement des infrastructures réseaux, le filtrage libérant la capacité de transit nécessaire au développement prévisible du nombre d'abonnés.

L'objectif de cette mission est l'étude de faisabilité d'une solution de filtrage. Elle ne constitue pas un document de spécifications pour un FAI. En cas de mise en œuvre, Il sera donc nécessaire d'approfondir l'étude par un équivalent d'appel d'offres en mode confidentiel vis-à-vis de différents constructeurs nous permettant de valider les aspects techniques (applications demandés et développements spécifiques), aspects financiers (tarification des produits, coûts récurrents, retour sur investissement), la pérennité (tant des sociétés que des solutions), la réactivité, l'administration et la maintenance.

[15] Sous réserve de suivi du développement de nouveaux protocoles P2P.