Rapport

Technologies de gestion du trafic des FSI : État des connaissances

Préparé par

Graham Finnie
Analyste en chef, *Heavy Reading*

www.heavyreading.com

Pour le compte du

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)

Janvier 2009

No. du Catalogue BC92-68/2009F-PDF

ISBN # 978-1-100-90832-8

TABLE DES MATIÈRES

SOMMAIRE 3

SOMMAIRE 3

I. L'ÉVOLUTION DE LA GESTION DU TRAFIC 5

II. TECHNOLOGIES ACTUELLES : L'ÉMERGENCE DE L'IAP ET DU CONTRÔLE FONDÉ SUR LES RÈGLES 8

2.1 Inspection approfondie des paquets 8
2.2 Techniques d'inspection approfondie du flux et techniques connexes 11
2.3 Contrôle et gestion fondés sur les règles 12

III. L'AVENIR DES TECHNOLOGIES DE GESTION DU TRAFIC 16

LISTE DES FIGURES

SECTION I

Figure 1 : Quelques fournisseurs dans le secteur de l'IAP 10
Figure 2 : Principaux organismes de normalisation et normes 13
Figure 3 : Quelques fournisseurs dans le secteur du contrôle fondé sur les règles 14
Figure 4 : Vision de la future fourniture des services 17

Sommaire

Depuis quelques années, la capacité des fournisseurs de services Internet, entreprises de télécommunication, câblodistributeurs et autres à gérer le trafic Internet passant par leurs réseaux s'est rapidement améliorée. Ils peuvent maintenant gérer le trafic de telle façon que certaines applications, services ou abonnés d'Internet bénéficient d'un accès préférentiel à la bande passante, alors que d'autres n'obtiennent qu'un accès limité ou rien du tout. Ils peuvent également gérer la façon dont le trafic circule à destination et en provenance d'adresses ou d'abonnés Internet, en se servant, au besoin, des applications que les abonnés utilisent.

Ce rapport a pour objet de brosser un tableau de l'état de la gestion du trafic, en se penchant plus particulièrement sur les techniques actuelles et émergentes et leur potentiel d'amélioration de la capacité des FSI à gérer le trafic Internet.

À la Section I, nous revenons brièvement sur l'historique de la gestion du trafic, qui prend sa source dans les efforts des fournisseurs de services d'améliorer la performance des applications du Protocole Internet (IP) sur les grands réseaux d'entreprise et commerciaux des FSI. Nous définissons et expliquons également quelques concepts fondamentaux comme le « surapprovisionnement » et les techniques largement utilisées comme le DiffServ et le MPLS et expliquons pourquoi certains fournisseurs de services estiment qu'elles ne sont plus adéquates à elles seules pour gérer le volume de trafic. Dans cette section, nous définissions également certains concepts fondamentaux de la gestion du trafic comme le blocage et le lissage du trafic ainsi que la restriction de la bande passante.

À la Section II, nous revenons sur l'évolution des principaux concepts et technologies de la gestion du trafic, en insistant sur les inspections approfondies des paquets (IAP) et le contrôle fondé sur les règles. Nous identifions les principaux fournisseurs dans ces domaines, examinons les liens entre ces diverses technologies et identifions les importantes normes techniques et en analysons les utilisations.

Finalement, à la Section III, nous examinons brièvement l'avenir de ces technologies et leur évolution et identifions d'importantes tendances susceptibles d'influencer l'avenir. Ces tendances sont notamment la gestion du trafic centrée sur l'abonné et celle contrée sur le mobile, les nouvelles normes possibles et l'intégration des outils existants entre eux et dans l'équipement de télécommunication.

Voici les plus importantes conclusions de ce rapport :

- **Les technologies de gestion du trafic deviennent de plus en plus intelligentes** et permettent une discrimination relativement pointue entre les applications acheminées sur les réseaux IP; elles permettent également aux fournisseurs de services, s'ils le souhaitent, de gérer le trafic au niveau de l'abonné.

- **La technologie actuelle la plus importante en gestion du trafic est l'inspection approfondie des paquets (IAP).** L'IAP est en train d'être largement déployée, parce qu'elle permet aux FSI d'identifier avec plus d'exactitude les applications et qu'elle présente un large potentiel d'applications, y compris le traitement des menaces pour la sécurité.

- **Par rapport à d'autres aspects des télécommunications, il existe peu de normes industrielles pour l'IAP.** Il est donc difficile de juger de ce qui est possible dans ce domaine, mais également de créer un environnement compétitif dynamique où la gamme des options et des capacités offertes aux fournisseurs de services augmente.

- **Bien qu'ils ne soient pas encore largement déployés, il existe un intérêt croissant pour les serveurs et les architectures de gestion, notamment entre les entreprises de télécommunication de premier niveau.** Ces serveurs peuvent traiter un plus large éventail de tâches de gestion avec plus de flexibilité que l'IAP et font surtout partie d'une architecture reconnue et normalisée à l'échelle internationale. Ces serveurs tendent à cibler davantage l'abonné que l'application.

- **L'application actuelle la plus importante pour ces technologies est la gestion poste à poste (P2P) du trafic et des applications.** De plus, ces technologies sont également souvent utilisées pour accorder un traitement préférentiel aux propres applications ou abonnés privilégiés d'un FSI, pour gérer la diversité croissante des menaces pour la sécurité ou pour surveiller et analyser le trafic.

- **Le développement des technologies et la demande du marché va dans le sens d'une gestion des abonnés plutôt que des applications.** La gestion au niveau de l'abonné donne davantage d'options aux fournisseurs de services et est associée à de nouveaux concepts comme la gestion de l'identité.

- **Sur le plan du développement, l'évolution va également dans le sens d'une réponse aux besoins des fournisseurs de services mobiles.** À mesure que les exploitants de réseaux cellulaires lancent des services mobiles à large bande moyennant des forfaits, ils ont besoin d'aide pour gérer le trafic, les applications et les abonnés, et les fournisseurs répondent à ce besoin.

- **Les technologies continuent d'évoluer à mesure que s'ajoutent de nouvelles idées comme l'inspection approfondie du flux.** Bon nombre de ces nouvelles technologies visent soit à améliorer la capacité de reconnaître des applications soit à améliorer la capacité de s'adapter aux nouveaux comportements des abonnés.

I. L'évolution de la gestion du trafic

Les fournisseurs des technologies de gestion du trafic décrivent souvent Internet comme un réseau du « meilleur possible », car il n'existe aucune garantie absolue que les paquets transférés sur un réseau IP arriveront de façon à ce que l'application sous-jacente (par exemple, navigation sur le Web ou lecture de vidéo en transit) soit toujours bonne ou acceptable. Le Protocole de contrôle de la transmission (TCP) comprend cependant des techniques de contrôle de la congestion, définies dans la norme de l'Internet Engineering Task Force (IETF), RFC2581[i], qui peuvent être considérées comme une forme de gestion du trafic.

Outre le TCP, la technique la plus répandue pour alléger la congestion du trafic est le surapprovisionnement, c'est-à-dire que les liaisons sont calculées pour que la bande passante disponible dépasse d'une certaine marge le maximum ou le volume moyen de trafic attendu. Le ratio de surapprovisionnement et la façon dont il est calculé varient largement et dépendent d'un grand nombre de facteurs dont la topologie ou l'architecture du réseau, le volume ou le flux de trafic, le nombre d'utilisateurs qui l'utilisent, le genre d'utilisateurs, la combinaison des applications utilisées, l'historique et les variations prévues du volume de trafic, la technologie du propriétaire de la liaison et le marketing.

Dans une enquête auprès des entreprises de télécommunication et autres fournisseurs de services réalisée en 2007[ii], Heavy Reading a constaté que le surapprovisionnement est de loin la technique la plus employée pour en arriver à une qualité de service (QS) acceptable sur les réseaux IP, mais qu'elle est progressivement supplantée par d'autres techniques de gestion du trafic qui pourraient finir par prendre sa place. En fait, notre enquête a montré également que la majorité des fournisseurs de services estiment que le surapprovisionnement n'est pas à lui seul une solution adéquate à long terme.

On voit en effet arriver des applications Internet qui possèdent des caractéristiques particulièrement gourmandes—en particulier, la voix (et audio, p. ex, la musique), et la vidéo (y compris les propres services IPTV du fournisseur de services, la vidéo « over the top » (OTT) de sites comme YouTube et le téléchargement de gros fichiers vidéo, en utilisant souvent des logiciels poste à poste).

Les applications en temps réel comme la téléphonie supportent mal l'instabilité (retard variable), la latence (retard) ou la perte de paquets (ce qui arrive fréquemment sur les réseaux congestionnés qui utilisent des technologies Internet traditionnelles pour contrôler la congestion). Pour leur part, les applications poste à poste peuvent entraîner une très forte augmentation de la demande de bande passante et perturber la planification du réseau fondée sur le surapprovisionnement.

Par conséquent, le ratio de surapprovisionnement pourrait aboutir à des coûts de bande passante trop élevés et rendre d'autres approches plus rentables. De plus, en raison de la multiplication sans fin des nouvelles applications Internet, il devient de plus en plus difficile pour les ingénieurs de réseau de planifier utilement sans une certaine capacité de contrôle (ou tout au moins de connaissance) du comportement des applications et des abonnés. Et de nouveaux problèmes surgissent. Par exemple, certains programmes poste à poste créent apparemment un problème particulier en ce sens qu'ils consomment autant de bande passante que possible. De plus le surapprovisionnement n'est pas aussi efficace pour les réseaux d'accès qui posent de plus en plus problèmes en raison des gros volumes téléchargés par les utilisateurs vers le réseau.

---

[i] Voir http://www.ietf.org/rfc/rfc2581.txt

[ii] Sondage privé de 100 entreprises de télécommunication sans fil et filaires et d'ESM par câble, mars 2007

Dans ces conditions, on commence à envisager la gestion du trafic au niveau de l'application ou de l'abonné, ce qui est le principal sujet de ce rapport. Les efforts concomitants pour améliorer l'efficacité de la bande passante par la restructuration du trafic se poursuivent, mais ne sont pas étudiés plus avant dans ce rapport.

Outre le TCP et le surapprovisionnement, il existe déjà plusieurs techniques largement utilisées pour gérer le trafic au niveau des applications. L'évolution d'Internet, qui d'un réseau purement universitaire est devenu un réseau commercial utilisé par des entreprises et autres pour fournir des services avec les besoins techniques critiques que cela implique, a conduit, par exemple, (à la suite d'un certain nombre d'étapes) à l'élaboration de deux normes de l'IETF appelées DiffServ et Multiprotocol Label Switching (MPLS) (commutation d'étiquette multiprotocole).

Le DiffServ est un mécanisme relativement simple de classification du trafic en petit nombre de classes de services ou d'applications afin d'accorder différents types de priorité au trafic. Une classification DiffServ typique établit une distinction entre la voix sur IP (VoIP), le trafic axé sur les transactions à durée de vie critique et le trafic sans garantie (p. ex. courriel).

Le DiffServ est souvent utilisé en association avec le MPLS, qui ajoute une étiquette aux paquets qui traversent un réseau IP. Cela permet notamment d'attribuer différentes classes de services (CS) à différentes applications, de sorte que certaines applications (comme la voix sur IP) seront prioritaires si une liaison est congestionnée.

Tant le DiffServ que le MPLS ont été créés il y a environ dix ans et sont maintenant largement répandus parmi les entreprises dans les réseaux privés qui utilisent le Protocole Internet et par certains FSI pour contrôler la qualité de certains services. Il existe des variantes comme le MPLS-TE (contrôle du trafic), et T-MPLS, conçu spécialement pour acheminer les services IP comme la téléphonie.

Pendant ce temps, toute une gamme de techniques plus générales sont nées et sont appliquées à divers points du réseau, ordinateur de l'utilisateur final, appareil ou passerelle jusqu'au réseau central.

Voici quelques-unes des techniques typiques

- **Le plafonnement,** qui mesure et limite la capacité en amont ou en aval qu'un utilisateur peut consommer pendant une période donnée (un mois, par exemple).
- **Le blocage**, qui s'applique normalement au trafic jugé indésirable, comme les pourriels, ou à des applications dont on estime qu'elles utilisent trop de bande passante
- **La restriction,** qui limite le montant de trafic acheminé sur un réseau pendant une période donnée, par mise en tampon (mémorisation) des paquets ou, au besoin, en éliminant des paquets
- **Le lissage**, un ensemble de techniques plus complexes qui permettent de contrôler le volume de trafic, le rythme d'acheminement, etc.

La capacité d'appliquer ces contrôles en fonction d'applications particulières existe déjà depuis plusieurs années à l'aide de technologies comme DiffServ, mais les techniques se sont beaucoup affinées.

Des techniques comme l'inspection approfondie des paquets (IAP) notamment améliorent la capacité de reconnaître les applications et les protocoles, alors que la gestion fondée sur les règles crée un cadre structuré pour appliquer un large éventail de règles aux abonnés, aux applications et aux cheminements des réseaux.

Autrement dit, les fournisseurs de services peuvent contrôler le trafic de trois façons différentes :

- **Dans le réseau** : par exemple, par une restriction de la bande passante lorsque le trafic atteint un certain volume, sans référence à l'application sous-jacente, à la source/destination ou à l'abonné
- **Au niveau du service ou de l'application :** par exemple, identifier et bloquer une application ou donner la priorité à certaines applications au détriment d'autres, en particulier pendant les périodes de congestion du réseau
- **Au niveau de l'abonné** : par exemple, limiter l'utilisation que peut faire un abonné de la bande passante, quelles que soient les applications en cause.

Comme le montre cette description, la gestion du trafic peut dépendre **ou** ne pas dépendre de l'application utilisée ou de l'abonné qui l'utilise. De plus, l'équipement d'assez haute technicité actuel permet de combiner ces capacités auparavant séparées, de sorte que l'on peut contrôler l'usage d'une application par un abonné en fonction du type d'abonnement, du niveau ou autre information.

Il y a lieu de noter également que les questions liées à la gestion du trafic, et ses solutions, sont en partie déterminées par le réseau sous-jacent et ses caractéristiques. Les grandes entreprises de télécommunication, les exploitants de réseaux cellulaires, les FSI à large bande et les télédistributeurs ne font pas tous face aux mêmes problèmes. Malgré des points communs dans les solutions, la mesure dans laquelle elles sont déployées et la façon dont elles le sont varient.

Par exemple, le secteur de la télédistribution a largement recours à des techniques plus complexes comme l'IAP et les serveurs de règles. La majorité des câblodistributeurs sont devenus des exploitants de systèmes multiples, ou ESM, qui offrent l'accès Internet, la téléphonie et la télévision. Étant donné que les réseaux par câble avaient été conçus au départ pour des signaux de télévision unilatéraux, il a fallu procéder à une importante restructuration des réseaux, mais l'architecture de base d'un réseau de télévision câblé, souvent appelée « arborescente », reste différente des architectures utilisées dans les réseaux des entreprises de télécommunication de sorte que la gestion du trafic est prioritaire pour les câblodistributeurs. Dans les réseaux câblés, il y a partage d'une plus grande partie de la bande passante du réseau d'accès que dans un réseau d'entreprise de télécommunication. Les câblodistributeurs ont donc besoin de contrôler l'accès à la bande passante.

Les FSI qui utilisent les réseaux DSL des entreprises de télécommunication font également une forte utilisation de l'IAP.

Depuis quelque temps l'attention se porte sur les exploitants de réseaux cellulaires mobiles, surtout parce que ces compagnies sont confrontées aux mêmes difficultés que les ESM (liaisons à capacité partagée ou limitée) et en partie parce que la plupart des réseaux cellulaires mobiles sont mis à niveau pour pouvoir offrir des services à large bande à haut débit, notamment l'accès Internet. De nombreux équipementiers dont il est question dans ce rapport estiment que cela représente leur meilleur débouché pour l'avenir.

Malgré l'intérêt que suscitent ces technologies, elles ne sont pas déployées par tous. Selon un sondage de 2007[i] de Heavy Reading, environ 25 % des répondants de quelque 100 compagnies filaires, sans fil et par câble utilisaient l'IAP, alors qu'une petite proportion seulement avait recours aux serveurs de règles—mais dans les deux cas, ils avaient fortement l'intention de déployer cet équipement, et son utilisation s'est probablement répandue depuis lors.

[i] Sondage auprès de 100 entreprises de télécommunication sans fil & filaires et EMS par câble, mars 2007

II. Technologies actuelles : L'émergence de l'IAP et du contrôle fondé sur les règles

Dans cette section, nous étudions l'évolution de plusieurs concepts et technologies de gestion du trafic, plus particulièrement l'IAP et le contrôle fondé sur les règles. Nous identifions les principaux fournisseurs dans ces domaines, examinons les liens entre les diverses technologies, décrivons les principales normes techniques et analysons les utilisations de ces technologies.

2.1 Inspection approfondie des paquets

Le trafic Internet prend la forme de paquets discrets de données qui contiennent non seulement du contenu (p. ex. voix, courriel, etc.), mais également d'autres informations qui indiquent notamment d'où vient le paquet et où il va.

L'idée de l'IAP est née vers 2000, mais du fait qu'il ne s'agit pas d'une technique normalisée, sa définition est quelque peu élastique. D'une part, on peut dire que l'inspection de paquets est « approfondie » si elle atteint l'objectif de reconnaître l'application sous-jacente que le paquet transporte. Sa façon de le faire est normalement propriétaire et souvent confidentielle et est une source fondamentale de la différentiation entre fournisseurs. Mais le terme IAP est souvent associé également au modèle d'Interconnexion de systèmes ouverts (OSI) pour les communications, qui divise la tâche d'interconnexion des systèmes informatiques en sept niveaux.

Selon cette définition, l'inspection « superficielle » des données ne s'intéresse qu'à l'information facile à examiner comme les adresses de source et de destination des en-têtes de niveau 3. L'inspection approfondie des paquets s'intéresse aux en-têtes des niveaux 4 à 7, ainsi qu'à toute information pertinente dans les données utiles du paquet elles-mêmes et examine souvent une séquence de paquets connexes pour avoir une vue d'ensemble. Il est ainsi possible de mieux identifier l'application sous-jacente. En fait, l'IAP est souvent appelée la technologie du niveau 7 car ce niveau est celui de « l'application » dans le modèle OSI.

En résumé, l'équipement IAP inspecte le contenu des paquets qui circulent sur un réseau IP. Il peut identifier plus ou moins bien l'application ou le protocole utilisé en examinant l'adresse IP de source et de destination, le numéro de port et les données utiles des paquets. Les numéros de port sont un des moyens les plus simples d'identifier les applications; par exemple, les courriels qui utilisent le protocole de transfert de courrier simple (SMTP) utilisent le port 25. Les en-têtes de paquet contiennent cette information, ainsi que l'adresse de source et de destination et d'autres, en particulier l'information de classe DiffServ, le cas échéant. On peut examiner les données utiles du paquet elles-mêmes (p. ex., une partie de page Web) pour voir les chaînes du protocole qui l'identifient (p. ex. « kazaa », qui apparaît dans des champs utilisés pour traiter les demandes de Kazaa). L'équipement peut également inspecter les signes indicateurs d'une application, comme la longueur des données utiles du paquet.

En regroupant cette information, l'équipement IAP identifie les applications à différents niveaux d'exactitude. L'IAP a un côté aléatoire où des faux positifs et des faux négatifs sont inévitables, mais où les avantages l'emportent malgré tout sur les inconvénients pour de nombreux acheteurs.

L'IAP a d'abord servi surtout à surveiller et planifier le trafic hors ligne dans un but d'analyse du trafic pour aider les fournisseurs de services à comprendre quelles étaient les applications qui consommaient la bande passante et comment la situation évoluait. Il s'agissait de la principale application, par exemple, de l'équipement fourni par les pionniers comme P-Cube (faisant maintenant partie de Cisco) et Sandvine.

Mais aujourd'hui, l'IAP sert surtout à identifier et à contrôler la bande passante disponible pour certaines applications—autrement dit, pour une gestion du trafic en temps réel. Elle sert en parti-

culier à identifier les protocoles poste à poste (P2P) comme Bit Torrent, pour procéder éventuellement à un blocage, une restriction ou un lissage.

Mais ce n'est pas la seule application de l'IAP. Il y en a d'autres comme l'identification et le blocage d'applications malveillantes et de menaces à la sécurité, l'amélioration de la performance d'applications « critiques », privilégiées ou payées, l'application de contrôles parentaux par abonné, la fourniture de services à différents niveaux, la publicité personnalisée, etc. Et certains équipements viennent avec un environnement de développement d'applications avec lequel les acheteurs peuvent développer leurs propres applications.

En gros, l'utilisation de l'IAP évolue de la façon suivante :

- Outil hors ligne pour analyser le trafic réseau
- Identification et blocage ou lissage du trafic P2P
- Traitement des menaces pour la sécurité ou des nuisances comme les attaques de déni de service distribué (DDoS)
- Étagement du service et contrôle des services privilégiés
- Contrôle parental et filtrage des URL
- Publicité personnalisée, offres de services ciblées, etc.
- Gestion de service par un tiers

L'IAP est un domaine technologique dynamique où la gamme des équipements et des capacités est très large. Heavy Reading a récemment identifié 12 fournisseurs vendant de l'équipement IAP auto-développé à des fournisseurs de services et entreprises de télécommunication (il y en a d'autres qui vendent seulement aux entreprises qui construisent leurs propres réseaux). La Figure 1 montre certains des principaux fournisseurs et le fait que, pour le moment, les petits spécialistes dominent le secteur.

Un rapport de Light Reading publié en 2008 évaluait le marché mondial de l'IAP à environ 450 millions de dollars cette année-là et prévoyait qu'Il serait de plus de 1 milliard de dollars en 2012.[i] Il affirmait qu'une bonne partie de la croissance serait attribuable à l'utilisation de l'IAP par les exploitants de réseaux cellulaires mobiles.

Les fournisseurs d'équipement IAP sont en concurrence selon un certain nombre de paramètres, notamment :

- Le nombre de signatures d'application ou de protocole qu'ils ont compilées—normalement des centaines dans une « bibliothèque » typique de signatures. Ils se font également concurrence en ce qui concerne leur capacité à reconnaître les protocoles qui ont été délibérément déguisés par des sites Web ou des applications—nous y reviendrons plus en détail dans la section suivante sur la DFI— ainsi que la vitesse à laquelle ils actualisent les bibliothèques en fonction des nouvelles applications et modèles de trafic. De nombreux fournisseurs offrent un service d'actualisation en continu fondé sur les nouvelles versions de logiciels, comme ce qui est offert aux utilisateurs de logiciels de détection de sécurité ou de virus.

- Le fait d'installer ou non un équipement incorporé, un outil plus utile pour la gestion du trafic en temps réel. L'équipement IAP incorporé est déployé directement dans le flux binaire et il agit immédiatement pour bloquer ou restreindre les applications en temps réel– plutôt que hors ligne, où le dispositif sort les données hors ligne, les examine, les nettoie au besoin ou les modifie et les réinjecte dans le flux binaire. L'IAP en ligne est

[i] Voir http://www.lightreading.com/insider/

plus difficile, mais éventuellement plus efficace lorsque la vitesse et le faible taux de latence sont des facteurs essentiels.

- La taille des liaisons ou le nombre d'abonnés ou de flux en cause, certains fournisseurs affirmant qu'ils peuvent traiter le trafic sur des liaisons de 80Gbit/s ou plus et gérer des réseaux ayant des millions de clients.

- La puissance de traitement des ordinateurs, qui influe sur la vitesse à laquelle l'équipement IAP identifie l'information et agit sur elle. Certains fournisseurs appliquent des technologies informatiques de pointe comme le traitement multiprocessus et le traitement parallèle.

- La capacité de traiter les menaces pour la sécurité comme les attaques de déni de service distribué (DDoS).

Figure 1 : Quelques fournisseurs dans le domaine de l'IAP

FOURNISSEUR	OBSERVATIONS
Allot Communications	Famille relativement large de produits IAP comprenant un produit de type serveur centralisé et des dispositifs d'application de bordure répartis; comprend aussi maintenant des appareils de sécurité. Les clients sont surtout des petits FSI qui les utilisent pour la gestion du trafic, mais également quelques grands exploitants de mobiles.
Arbor Networks	Spécialisé au départ dans le traitement des menaces pour la sécurité pour les entreprises de télécommunication, s'est diversifié avec l'acquisition du fournisseur d'IAP, Ellacoya, en 2008. Se spécialisant dans les dispositifs incorporés, Ellacoya est un des spécialistes les mieux établis et les plus importants de l'IAP.
Bivio Networks	Petit fournisseur d'IAP qui a commencé récemment à cibler les entreprises de télécommunication; utilise le traitement informatique réparti haut débit comme principale plateforme technologique, ainsi que la programmabilité des appareils.
Cisco Systems	Le produit IAP, appelé SCE, a été développé par P-Cube, que Cisco a acquis en 2004. Utilisé surtout pour la surveillance, mais aussi maintenant par certains pour la gestion du trafic en temps réel. La nouvelle version traite des liaisons de 10Gbit/s; est intégré aux routeurs de Cisco.
Cloudshield	Petit spécialiste d'IAP qui privilégie le développement d'applications ouvertes, en particulier dans le secteur de la sécurité, basé sur son propre OS et langage; disponible en lame dans le LameCenter d'IBM. A quelques clients de niveau 1 qui utilisent un équipement destiné essentiellement à la gestion du trafic et la sécurité.
Procera Networks	Spécialiste de l'IAP/DFI qui a récemment commencé à cibler les entreprises de télécommunication de niveau 1; langue de reconnaissance auto-développée avec plus de 800 signatures actuellement revendiquées. Les clients sont surtout des petits FSI et des entreprises de télécommunication municipales qui utilisent l'équipement pour la gestion d'une utilisation équitable.

Radware	Spécialiste de l'IAP et de la sécurité relativement important et bien établi qui utilise à la fois l'IAP et la DFI; se spécialise dans le contrôle de la qualité des services des entreprises de télécommunication et le contrôle des applications OTT, mais a récemment ajouté le contrôle « comportemental ». Prétend avoir de nombreux clients de niveau 1.
Sandvine	Grand spécialiste de l'IAP qui élargit sa gamme de produits et de technologies qui se limitait jusqu'à maintenant à la surveillance de base des applications et au contrôle du trafic P2Pr la clientèle était au début composée des EMS par câble nord-américains, mais comprend maintenant davantage d'entreprises de télécommunication filaire et sans fil, et d'autres régions.

Initialement, l'équipement d'IAP était déployé principalement dans les principaux points d'agrégation et d'homologage, mais est maintenant plus largement distribué et plus proche du client, ce qui améliore la capacité d'appliquer les contrôles par abonné ou par service.

L'autre grande tendance potentielle dans l'IAP est l'intégration de ses capacités dans des dispositifs existants comme les routeurs de bordure. Certains fournisseurs d'équipement de télécommunication, comme Starent et Zeugma Systems, se vantent que leur équipement possède des capacités IAP depuis le début; Starent a réussi à établir une gamme de plateformes de réseau central et de passerelle pour les exploitants de mobile qui comprend l'IAP, alors que la nouvelle entreprise Zeugma fait un routeur de bordure pour les exploitants de réseau qui comprend l'IAP.

Il existe des liens assez étroits entre la sécurité et l'IAP qui valent également la peine d'être mentionnés. Une grande partie de l'équipement IAP possède certaines capacités pour le traitement de menaces pour la sécurité, et certains fournisseurs sont des spécialistes dans ce domaine. Par exemple, Arbor Networks, le principal fournisseur de dispositifs d'inspection du flux aux entreprises de télécommunication pour détecter les menaces pour la sécurité, a acheté un important fournisseur d'IAP, Ellacoya, afin d'intégrer plus efficacement les deux aspects. Un autre, Adaptive Mobile, spécialisé dans le règlement des problèmes de pourriels, virus et autres pour les entreprises de télécommunication, peut maintenant traiter les menaces « combinées » qui consomment les ressources réseau de façon imprévisible. D'autres, comme Allot Communications, ont pris une direction opposée : ancien spécialiste de l'IAP, Allot a acheté un spécialiste de la sécurité, Esphion, en 2008 afin d'améliorer sa capacité à répondre aux besoins de sécurité des compagnies de télécommunication.

2.2 Techniques d'inspection approfondie du flux et techniques connexes

L'IAP traditionnelle présente certaines lacunes importantes dans sa capacité à reconnaître les applications, ce qui a conduit les fournisseurs, existants et nouveaux, à chercher des moyens de renforcer l'IAP par de nouvelles approches plus exactes. Celles-ci portent des noms divers, mais par souci de simplicité, nous les appellerons inspection approfondie du flux ou DFI.

On peut considérer la DFI comme une technique qui vient compléter l'IAP en identifiant avec plus d'exactitude les applications et les protocoles. La DFI infère l'application (ou la menace) à partir du comportement du flux de paquets, plutôt que par la surveillance des signatures de protocole ou de l'utilisation des ports dans le paquet lui-même. C'est un point important, car le trafic est de plus en plus souvent chiffré ou tunnellisé à travers le réseau et de plus en plus d'applications se déguisent en utilisant, par exemple, le « mauvais » port, ce qui complique la tâche d'identification du trafic par l'IAP traditionnelle. Certaines applications ont ce que l'on appelle une agilité de port et ne sont pas associées à un numéro de port particulier; il existe d'autres déguisements comme le trafic de protocole de transfert hypertexte (HTTP) (port 80), mais qui sont en réalité (par exem-

ple) de la voix sur IP. Le trafic P2P est de plus en plus souvent chiffré et il devient donc difficile d'utiliser l'IAP traditionnelle.

Contrairement à l'IAP, la DFI n'est pas un terme normalisé et il existe un ensemble de techniques apparentées appelées analyse comportementale, analyse heuristique, reconnaissance de tendances et ainsi de suite. Mais le principe est généralement le même : inférer l'identité des applications que l'on ne peut pas détecter autrement par l'IAP car elles sont déguisées. On peut, par exemple, examiner l'histogramme de la longueur d'un paquet et la comparer à une bibliothèque d'histogrammes de longueur de paquets : les paquets de couche de contrôle P2P sont plus courts que les purs paquets HTTP.

Presque tous les fournisseurs cherchent à ajouter ces techniques s'ils ne l'ont pas déjà fait. Les fournisseurs qui ajoutent et renforcent ces capacités sont actuellement Allot, Anagran, Ericsson, Nokia Siemens Networks, Procera et Radware.

Anagran, un spécialiste dans ce domaine, qualifie son approche de « gestion comportementale du trafic ». Anagran s'intéresse aux caractéristiques, à la forme et à la taille du flux, ainsi qu'au nombre de ports, aux adresses de source/destination et au protocole pour améliorer l'identification.

Mais la plupart des fournisseurs d'IAP orthodoxes ajoutent également ce genre de technologie. Par exemple, Radware intègre les capacités IAP et DFI à son produit Network Delivery Controller.

2.3 Contrôle et gestion fondés sur les règles

Le contrôle basé sur les règles est en principe un ensemble de techniques plus étendu que l'IAP qui contrôle le flux du trafic Internet (notamment) dans une architecture structurée et normalisée. Il suscite un grand intérêt parmi les grandes entreprises de télécommunication et les fournisseurs de services, mais n'est pas encore aussi largement répandu que l'IAP.

Ces outils sont d'une certaine façon en concurrence avec l'équipement d'IAP, mais aussi complémentaires. On peut utiliser les serveurs de règles avec l'IAP, et c'est souvent le cas pour les grands équipementiers. Parallèlement, certains fournisseurs d'IAP, comme Allot et Sandvine, ajoutent de nouvelles capacités, parfois par acquisition, et se positionnement comme fournisseurs de ces outils pour séduire la clientèle.

Le contrôle basé sur les règles est forcément un concept général, car il se fonde normalement sur l'utilisation d'un moteur de règles automatisé pour appliquer des règles logiques simples qui, une fois concaténées, peuvent déclencher des politiques relativement complexes en réponse à de l'information reçue de réseaux, de clients et d'applications. Par exemple: *« Si le client A est abonné au forfait. Or, et si c'est la fin de semaine, il peut télécharger un nombre illimité de vidéos de musique ».* Cet ensemble de conditions peut facilement être élargi en ajoutant simplement d'autres modalités– par exemple, l'information sur l'âge du client ou sur le volume qu'il a déjà téléchargé. Et on peut ajouter de l'information dynamique (p. ex., où se trouve le client, quel appareil il utilise ou les conditions du réseau à ce moment-là) aux règles invoquées dans un cas particulier.

Comme cette description l'implique, un élément important de la plupart des outils fondés sur les règles est qu'ils ont (ou peuvent avoir) des liens vers les bases de données sur les abonnés et la facturation. Cet équipement pourrait donc devenir un moyen très intéressant d'offrir des services plus personnalisés aux clients. Cela veut dire également que les règles sont plus souvent liées aux abonnés qu'aux applications, ce qui fait dire à un spécialiste dans ce domaine, Camiant, dans la description de son outil de « gestion d'une utilisation équitable » qu'il est « indépendant des applications » et conçu pour être utilisé au niveau de l'abonné.

Plusieurs organismes internationaux importants de normalisation des télécommunications ont normalisé les architectures de règles au cours des 3 à 4 dernières années. Il s'agit notamment de 3GPP et 3GPP2, qui créent des normes pour les exploitants de réseaux cellulaires mobiles; ETSI, qui a créé une architecture pour les entreprises de télécommunication filaires dans le cadre de son architecture TFSIAN pour les réseaux des entreprises de télécommunication de la prochaine génération et CableLabs, qui a créé une architecture de règles pour les exploitants de systèmes multiples par câble (ESM par câble).

Figure 2 : Principaux organismes de normalisation et normes

ORGANISME	PRINCIPAUX PRODUITS
3GPP	Version 7 (actuelle) de l'architecture PCRF/PCEF; version 8 en préparation
ETSI TFSIAN	Bien que TFSIAN soit maintenant intégrée à 3GPP, ETSI a d'abord développé une architecture distinctive pour les entreprises de télécommunication de niveau 1 en déployant des RPG filaires
CableLabs	Dans l'architecture PCMM, le serveur de règles est défini et le CMTS agit comme PEP
OMA	PEEM a développé et défini des mécanismes fondés sur les règles réutilisables pour des outils OMA comme la présence
Broadband Forum	Le WT-134 Policy Controller Framework est en préparation. Les spécifications d'auto-configuration TR-069 bien établies sont également pertinentes.
IETF	Principales normes AAA, en particulier Diameter; a également développé le protocole Common Open Policy Service (COPS) à l'appui du contrôle fondé sur les règles sur les protocoles de signalisation de la QS.

Ces architectures tiennent compte normalement de deux éléments—un point de décision, ou PDP, qui est normalement (mais pas toujours) un dispositif très intelligent centralisé à grand volume de calculs, normalement (mais pas toujours) associés à un moteur décisionnel, et le client de serveur de règles, ou PEP. Le travail du PDP, comme son nom l'implique, consiste à prendre des décisions à la place de dispositifs moins intelligents. Les moteurs de règles étant des entités flexibles, on peut invoquer des règles pour traiter un ensemble extrêmement vaste de conditions, déclenchées par la présence d'une application, d'un abonné, d'une URL de destination ou même de tout point de données que l'on peut identifier et sur lequel on peut agir.

Il y a moins de fournisseurs dans le domaine des serveurs de règles (PDP), mais ils comprennent quelques spécialistes importants ainsi que—et surtout— la majorité des grands fournisseurs d'équipement de télécommunication. La Figure 3 contient la liste de certains de ces fournisseurs.

Dans notre architecture générale de base, les règles sont appliquées par les PEP, qui, tout comme les PDP, sont normalement (mais pas toujours) des dispositifs répartis plus près de l'abonné. Un PEP est en fait n'importe quel équipement d'abonné capable de faire appliquer une décision – une vaste gamme d'équipements qui comprend les serveurs d'accès à distance à large bande (B-RAS), les nœuds de soutien GPRS passerelle (GGSN), les appareils IAP, les passerelles médias, les contrôleurs de session en périphérique (SBC), etc. Ces PEP diffèrent surtout dans la façon d'exécuter les décisions, du relativement simple (GGSN) au relativement complexe (IAP), mais le principe fondamental reste le même.

Comme nous l'avons vu, les normes fondées sur les règles comprennent également les interfaces d'équipement comme le Home Location Register (HLR) (registre de localisation central) ou le Home Subscriber Server (HSS) (serveur abonné central) utilisé dans les réseaux mobiles 3G. Il s'agit de répertoires de données sur les abonnés qui, en se reportant aux données sur les abonnés, permettent aux serveurs de règles de prendre des décisions qui concernent directement les utilisateurs.

Un autre domaine apparenté qui commence à converger avec les règles est l'authentification, autorisation et traçabilité (AAA), qui permet de bien identifier les abonnés qui ne reçoivent ainsi que les ressources et les services auxquels ils ont droit; ce système peut s'appliquer à la fois de façon statique et dynamique ou en association avec une disponibilité de ressource en temps réel. Il s'agit d'un aspect important pour sécuriser les réseaux et différencier entre les abonnés en fonction de leur type d'abonnement (p. ex., combien de bande passante est prévue dans leur contrat, avec quel volume ou limite de temps et autres paramètres.) plus les outils AAA sont évolués, plus il est possible de distinguer les abonnés.

En fait, le nom complet de la norme 3GPP pertinente est "Policy Charging et Rules Function" (Fonction d'imputation et de règles), qui souligne l'importance de la capacité de facturation une fois qu'une décision a été prise.

Comme cette analyse le montre bien, les outils décisionnels sont davantage axés sur les abonnés que les outils d'IAP. En fait, un des grands spécialistes du domaine, Bridgewater Systems, qualifie ses offres de « contrôle de service centré sur les abonnés », ce qui met de l'avant le fait que la compagnie a commencé dans le domaine AAA. Bridgewater se spécialise dans la capacité à comprendre l'état de l'abonné en temps réel avant de prendre une décision, notamment s'il faut lui attribuer de la bande passante. Un autre spécialiste, Broadhop, fabrique un outil de gestion fondée sur les règles, qui vise essentiellement à simplifier et automatiser la fourniture et le déploiement des services.

Il existe un autre système qui vaut la peine d'être noté, le Resource Admission Controller (RAC) (contrôle d'admission aux ressources), un concept défini dans le TFSIAN de l'ETSI. Le principal objectif est de permettre aux compagnies de téléphone qui mettent en œuvre les réseaux IP d'offrir un service téléphonique qui émule les services téléphoniques traditionnels lorsque les appels sont établis—c'est-à-dire à la réception d'une demande de faire un appel, elles peuvent refuser l'accès par un signal d'occupation si le réseau est jugé trop encombré pour prendre l'appel.

Ce principe de contrôle de l'admission pourrait bien entendu s'appliquer à un ensemble d'autres contextes et commence d'ailleurs à se généraliser.

Figure 3 : Quelques fournisseurs dans le domaine du contrôle fondé sur les règles

FOURNISSEUR	COMMENTAIRES
Bridgewater Systems	Gestion de service centrée sur les abonnés qui vise essentiellement les exploitants de réseaux mobiles et qui a pour but de faire correspondre la fonctionnalité AAA avec la compréhension de « l'état » d'un abonné ; une large gamme de fonctions sont prises en charge
Broadhop	Spécialisé dans les questions d'approvisionnement et offre une large gamme d'applications comme le contrôle parental et le VOIP prêt à l'emploi

Camiant	Fournisseur spécialisé dans les serveurs de règles centralisés qui prend en charge toutes les normes 3GPP et PacketCable pour les PDP; ses principaux clients sont les ESM par câble, mais cible aussi maintenant les entreprises de télécommunication filaires et sans fil
Ericsson	Le plus dynamique des fabricants d'équipement de télécommunication à entrer sur ce marché, avec des produits exclusifs dans les PDP et PEP; SAPC prend en charge la version 7 de 3GPP, spécifications et interfaces; produit IAP autonome et en supplément aux produits incluant les routeurs Redback
Juniper Networks	Secteur de développement hautement prioritaire pour Juniper qui intègre des équipes travaillant sur des programmes de produits centrés sur les réseaux et les abonnés; les derniers mettent fortement l'accent sur l'identité, que Juniper considère essentielle aux règles, de même que la sécurité.
Nokia Siemens Networks	Serveur de règles convergé pour les réseaux fixes et mobiles qui prend en charge la version 7 3GPP; Flexi ISN est un PEP basé sur l'IAP; Nokia Siemens vend également des produits d'identité et HSS grâce à son acquisition d'Apertio
Openet	Spécialisé dans la médiation et la facturation pour les exploitants de réseaux mobiles, en particulier la facturation du contenu; le nouveau Policy Manager justifie l'entrée dans le grand marché des serveurs de règles; basé sur la version 7 de 3GPP

III. L'avenir des technologies de gestion du trafic

Comme nous l'avons vu à la section II, la gestion fondée sur les règles en général et la gestion du trafic en particulier est un secteur dynamique qui évolue rapidement. Dans cette section, nous examinons certains plans publics de grands fournisseurs dans ce domaine et les mettons en lien avec les besoins connus des FSI pour se demander quel seraient le rôle et la forme des futures techniques.

Des outils de gestion du trafic davantage centrés sur les abonnés

Une grande partie de la gestion du trafic actuelle ne porte pas sur l'information sur les abonnés eux-mêmes. Mais de façon générale, la majorité des entreprises de télécommunication et des ESM par câble ont tendance à abandonner le contrôle des applications pour privilégier le contrôle centré sur les abonnés ou les clients, en partie parce qu'il existe davantage de technologies qui permettent de le faire. Comme nous l'avons vu dans la dernière section, les outils fondés sur les règles sont plutôt centrés sur les abonnés, alors que les fournisseurs de DPS concentrent également leur travail de développement dans ce domaine.

Les fournisseurs qui s'intéressent davantage aux abonnés envisagent de les choisir en fonction d'un large éventail d'options et de personnaliser les applications pour répondre à leurs besoins particuliers – c'est-à-dire que les services peuvent devenir plus intéressants et par conséquent avoir plus de valeur. Du contrôle des coûts de la bande passante, on passe ainsi au maintien de la clientèle et à l'amélioration des services.

La plupart des fournisseurs, que ce soit de l'IAP et des outils fondés sur les règles, vont dans cette direction. Par exemple, le fournisseur d'IAP, Allot, offre une « Plateforme de gestion des abonnés », qui est censée permettre une identification en temps réel des abonnés (et non un simple aperçu ponctuel, souligne Allot), plutôt qu'une simple identification des adresses IP. D'autres comme Ellacoya (maintenant Arbor) se spécialisent dans l'intégration de l'arrière-guichet avec des systèmes de soutien opérationnels (OSS) et des systèmes de soutien fonctionnels (BSS) utilisant RADIUS, DIAMETER et autres normes AAA Internet. Cela correspondant à la conviction d'Arbor selon laquelle l'IAP et les outils fondés sur les règles s'orientent vers le contrôle par abonné.

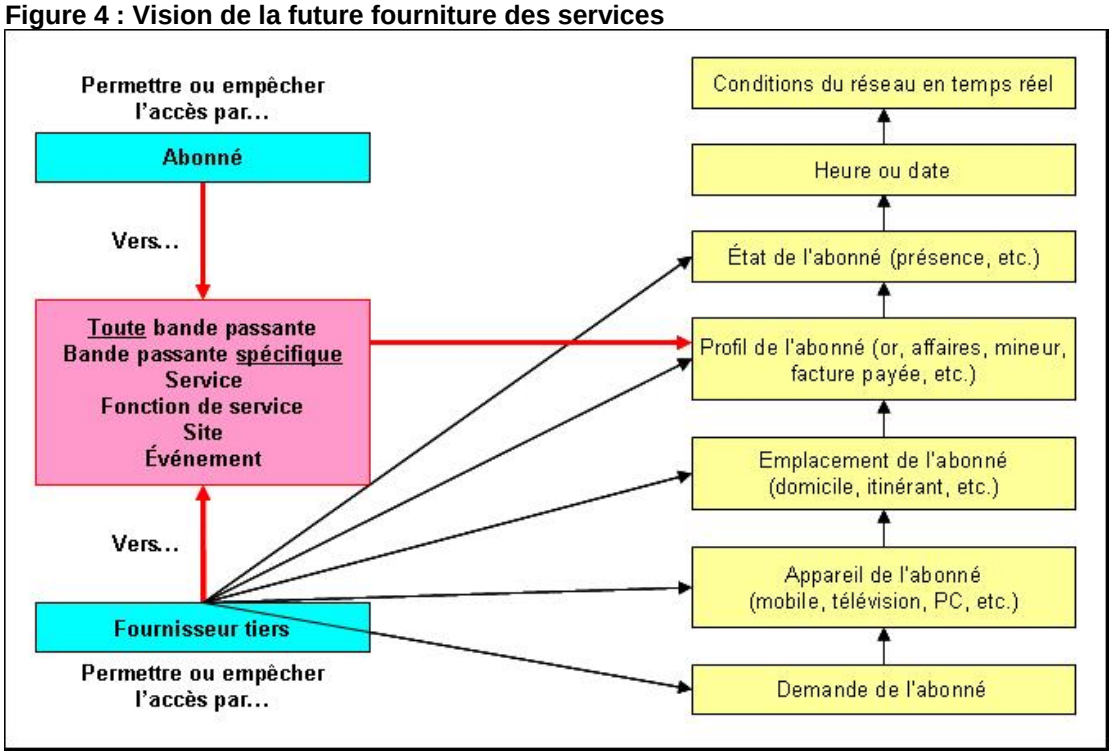
Comme nous l'avons vu dans la dernière section, les spécialistes des outils fondés sur les règles ont ciblé l'abonné dès le départ. Le principal concept de Bridgewater est une « gestion des services centrée sur l'abonné » en se fondant sur des profils statiques et de « l'état » de l'abonné, par exemple, si un abonné est hors ou en réseau, le type de réseau qu'il utilise, etc. La compagnie souligne qu'elle traite à la fois les données historiques et d'état de l'abonné sur une plateforme principale commune.

Jusqu'à un certain point, cette tendance est influencée par le travail réalisé dans un secteur apparenté, mais distinct appelé gestion de l'identité. L'idée centrale de ce nouveau domaine est que si un client a été identifié par un exploitant de réseau mobile, par exemple, comme le client A, cette information peut être partagée (dans des conditions très contrôlées) avec un tiers comme un site de cybercommerce sans que le client ait besoin de s'identifier une deuxième (ou troisième) fois. Souvent appelée « authentification unique », l'identité fédérée limite normalement la tierce partie à la seule information nécessaire dans un cas particulier pour protéger les renseignements personnels de l'utilisateur, ainsi que son identité réelle dans la plupart des cas.

Bon nombre des idées mentionnées ici ne sont pas appliquées dans les réseaux, mais donnent une idée de l'évolution possible du secteur. La Figure 4 montre la vision pour un fournisseur de l'étendue possible de ces capacités en tenant compte de la technologie actuellement disponible. Comme le montre la figure, un des aspects de cette évolution est de créer des liens plus constructifs avec des sites Web tiers et des développeurs en tant que clients de réseaux.

L'énorme croissance des services mobiles à large bande—et du trafic— est la tendance la plus manifeste dans les réseaux mobiles aujourd'hui, tendance qui conduit à une nouvelle réflexion sur les moyens de gérer le trafic.

Figure 4 : Vision de la future fourniture des services



Une gestion du trafic plus centrée sur le mobile

Même si les utilisations convergent, les difficultés techniques que pose la gestion du trafic dans les réseaux mobiles sont différentes de celles que posent les réseaux fixes. La plus évidente est que les abonnés du téléphone cellulaire se déplacent, ce qui crée des problèmes au niveau de l'AAA et renforce la nécessité d'avoir au moins des bases de données centralisées. L'autre grande différence est le fait que la bande passante est divisée à égalité entre un grand nombre d'utilisateurs et que la capacité de traiter un grand nombre d'abonnés est donc relativement plus importante que la taille de la liaison qui est contrôlée. Plusieurs fournisseurs indiquent d'ailleurs que l'application de contrôles fondés sur les règles aux liaisons radio exige une certaine expertise dans le domaine.

Cette réalité, ainsi que l'intérêt suscité par la convergence fixe-mobile, le réseautage neutre sur le plan de l'accès et la fourniture de services dite « à trois écrans » (télévision, PC et téléphone mobile), poussent la plupart des fournisseurs vers des solutions de convergence qui fonctionnent dans différents contextes. Mais certains mettent en garde contre le fait que le travail dans le contexte des réseaux d'accès à la radio sans fil pose des problèmes particuliers qui pourraient être préjudiciables à certains spécialistes du filaire, et les fournisseurs n'avancent pas tous dans cette direction au même rythme.

Identification plus exacte des applications

Motivé en partie par le combat permanent contre les réseaux zombies, les pourriels et autres menaces, on investit continuellement dans des technologies qui permettent d'identifier plus exactement les applications. Il s'agit d'une course classique aux armements technologiques dans laquelle il n'y a pas de « gagnant » au bout du compte, mais dans laquelle la plupart des spécialistes ainsi que les grands acteurs investissent des sommes considérables. La tendance vers des techniques comportementales et heuristiques va probablement se poursuivre de sorte que l'IAP, la DFI et autres techniques connexes vont probablement continuer d'être très utiles aux fournisseurs de services pour identifier les applications, malgré tous les efforts déployés pour éviter l'identification.

L'hostilité envers l'IAP, en particulier parmi les fournisseurs d'applications poste à poste, pourrait également conduire les chercheurs à trouver des compromis entre les intérêts des deux groupes. Par exemple, un fournisseur d'IAP allemand, Ipoque, a développé une application qui permet aux clients d'établir une « liste blanche » des fichiers et des sites de Bit Torrent jugés légitimes, et d'autres projets du même genre pourraient voir le jour.

Impact éventuel de nouvelles normes ou révisions Internet

De même, la controverse au sujet de la neutralité du réseau et du traitement du trafic poste à poste a suscité un nouvel intérêt parmi les chercheurs pour trouver des solutions qui sont approuvées par le milieu, éventuellement sous la forme d'un nouvel appel de commentaires de l'IETF. Par exemple, deux groupes de travail spéciaux de l'IETF appelés Transport for Advanced Network Applications (TANA)[i] et Application Layer Traffic Optimization (ALTO)[ii] étudient différents moyens d'améliorer la façon dont les applications poste à poste consomment la bande passante Internet.

Un autre projet, Participation proactive des fournisseurs de réseau pour le poste à poste (P4P)[iii], vise à permettre aux protocoles poste à poste de communiquer avec des systèmes de gestion de réseau. Il s'agit ici de créer une relation plus constructive entre les développeurs d'applications Web et les fournisseurs de réseau. De nombreuses grandes entreprises de télécommunication, dont AT&T, Telefonica et Verizon, ainsi que des développeurs de contenu Web dont Bit Torrent, Joost et Limewire sont favorables au P4P.

Mais il est encore trop tôt pour dire si ces tentatives et d'autres porteront fruit et influeront sur l'utilisation des outils de gestion du trafic déjà employés.

Plus grande intégration du matériel et des logiciels

Nous avons déjà vu aux sections précédentes que les frontières entre des catégories d'équipement et des types de fournisseurs auparavant distincts dans des secteurs comme les règles, l'IAP, l'AAA et l'imputation ont commencé à s'estomper. Cette tendance va probablement se poursuivre pendant une année ou deux et conduira peut-être à des outils d'une utilité plus étendue.

Il existe également une tendance connexe vers un équipement à lame plutôt que des appareils autonomes.

---

[i] Voir http://www.ietf.org/internet-drafts/draft-shalunov-tana-problem-statement-01.txt

[ii] Voir http://tools.ietf.org/html/draft-marocco-alto-problem-statement-00

[iii] Voir http://www.pandonetworks.com/p4p

Par exemple, le SCE est une conception qui repose sur un appareil, mais Cisco affirme que l'objectif à long terme est d'en arriver à une architecture en lame, les lames SCE étant ajoutées à un châssis de routeur. Selon Cisco, la performance et l'extensibilité seront améliorées et ses clients demandent à tous les fournisseurs, y compris Cisco, de réduire le nombre des boîtiers.

Par conséquent, la fonctionnalité IAP est un nouvel élément essentiel du Redback's SmartEdge Multi-Service Edge Router 1200, lance en 2007 (bien que l'IAP n'ait été commercialisée que dans la deuxième moitié de 2008). Le 1200 comporte des capacités d'IAP qui sont intégrées au boîtier et peut traiter des tâches en ligne comme le contrôle du trafic poste à poste et l'atténuation des menaces à des vitesses de 10 Gbit/s.

Certains fournisseurs affirment que d'autres classes d'équipement peuvent traiter directement de simples décisions, c'est-à-dire qu'une entreprise de télécommunication pourrait retarder le déploiement d'un serveur de règles plus moderne et plus coûteux. Par exemple, Nextpoint prétend que ses passerelles SBC et de sécurité peuvent offrir une sorte de « PDP allégé » et traiter au moins certaines décisions à la place d'un vrai PDP. Et Cisco a fait remarquer que d'importantes améliorations apportées aux semi-conducteurs et à la puissance de calcul permettaient de pousser très loin la puissance de calcul nécessaire à l'IAP et autres tâches de surveillance.

En résumé, voilà un secteur de la recherche technologique très dynamique dans lequel nous nous attendons à voir des développements rapides et éventuellement inattendus ainsi que des améliorations constantes dans la capacité des entreprises de télécommunication et des fournisseurs de services à intégrer la gestion du trafic, des applications et des abonnés.

Annexe A : Au sujet de l'auteur

GRAHAM FINNIE
ANALYSTE EN CHEF, *HEAVY READING*

Graham Finnie mène des recherches sur les télécommunications depuis plus de 20 ans. Il est entré à *Heavy Reading* en 2004 après dix ans au Yankee Group. À Heavy Reading, Finnie est notamment responsable de la rédaction d'une série de rapports sur les nouvelles technologies de contrôle, y compris l'IMS. Tout récemment, il a rédigé le rapport de Heavy Reading intitulé *Policy Controller & IAP: The New Broadband Imperative,* septembre 2008. Finnie a également écrit de nombreux textes sur la prochaine génération des technologies à large bande. Il a été nommé analyste en chef à Heavy Reading en février 2007.
Finnie habite au Royaume-Uni. On peut le rejoindre à Finnie@HeavyReading.com.