Opdop présente ...

Le GIX Local HowTo

Pourquoi comment monter un point d'échange et d'accès local

par Sylvain Vallerot

mise à jour du 6 août 2014

Sommaire
Table des matières

1 Introduction

Ce guide s'adresse à tous ceux qui s'intéressent à l'opportunité de créer une infrastructure d'échange publique afin de proposer aux entreprises, prestataires et opérateurs du secteur des TIC de s'ancrer et se développer localement.

Il intéresse ces acteurs privés du secteur TIC mais aussi ceux qui développent des infrastructures comme les centres de réseau (netcenter) et/ou de données (datacenter). Il s'adresse aussi aux acteurs publics : collectivités, réseaux d'initiative publique, régulateurs, élus locaux ou en charge du développement des territoires.

Alors que les réseaux privés des grands opérateurs se sont d'abord orientés de manière à conduire efficacement les flux vers des points précis sur lesquels se sont concentrés les investissements, bien des régions sont restées en marge, en souffrance d'infrastructures locales pour enraciner une activité TIC.

Les points d'échange et d'accès au réseau constituent une solution simple pour recréer des centre d'intérêt et de développement local. Peu coûteuses et faciles à mettre en place, ils sont un moyen pour une région (au sens large) de redevenir actrice d'internet et non plus seulement consommatrice de services qui créent de la richesse ailleurs.

2 Points d'échange et d'accès au réseau

2.1 Définitions

Un point d'échange (*GIX pour « Global Internet eXchange »*, ou *IXP pour « Internet eXchange Point »*) est une plate-forme qui permettent l'interconnexion directe d'opérateurs IP, au moyen d'un équipement mutualisé qui ne s'occupe que de commuter le trafic qu'ils s'échangent. Cette plate-forme évite aux opérateurs d'avoir à établir des liens directs entre eux, un seul raccordement au point d'échange permettant à chacun d'échanger du trafic avec tous les autres opérateurs présents.

Les opérateurs raccordés concluent de gré à gré et de pair à pair, un accord d'échange (appelé «peering agreement») par lequel ils s'accordent pour s'envoyer et recevoir mutuellement du trafic. On a donc, en principe pour chaque opérateur :

- une liaison et une plate-forme qui sont mutualisées ;
- des accords de peering qui ne sont pas mutualisés (à priori).

2.1.1 Peering

Le *peering* consiste à échanger du trafic qui a son origine sur le réseau de l'un des opérateurs (ou de ses clients) et aboutit sur le réseau de l'autre (ou de l'un de ses clients) et ne fait généralement pas l'objet d'une facturation de l'un à l'autre.

2.1.2 Point d'accès au réseau (NAP)

Un point d'accès au réseau (*NAP pour « Network Access Point »*) est une plate-forme aux principes de fonctionnement similaires, mais qui autorise des échanges de trafic qui

trouvent leur source ou leur destination au-delà des réseaux des opérateurs directement connectés, et qui donnent en général lieu à des accords d'échange de trafic non gratuits. L'opérateur connecté à la plate-forme qui fait «transiter» le trafic vers des opérateurs distants est un «opérateur de transit» (ou «fournit un transit»).

2.1.3 Commutation

La base du service qu'offre le GIX est le service de commutation : les opérateurs ont chacun une adresse IP dans le VLAN de peering, et s'en servent pour établir des session pair à pair.

Le schéma de principe est donc simple :

- au niveau physique, chaque opérateur est raccordé à l'un des commutateurs constitutifs du GIX,
- au niveau 2 (ethernet), tous les opérateurs membres sont raccordés dans le même VLAN de peering,
- au niveau 3 (internet), le routeur de chaque membre a une IP dans la même zone de broadcast que les autres, ils peuvent se joindre sans intermédiaire.

Les GIX peuvent aussi proposer des services de mise en relation, appelé route-serveurs ou route-réflecteurs. Ces services facilitent l'établissement systématique de relations de peering mais n'interfèrent pas dans les relations de pair à pair.

Les GIX sont parfois des GIX exclusivement, mais ici je vous parlerai plus volontiers de GIX / NAP (même si parfois j'escamote le « NAP » pour faire court, parce que selon l'objectif de développer des infrastructures d'interconnexion, et dans le cas où elles sont indépendantes et donc auto-financées, il n'y a pas de raison (a priori, mais ça peut se produire parfois) de restreindre leur usage à la seule fonction de GIX, en excluant celle de NAP.

2.2 Utilité technique

Les GIX permettent que des opérateurs internet (qui *par définition* disposent d'un AS, de routeurs, et sont capables de mettre en œuvre le protocole BGP) puissent échanger au plus court, au plus direct et au moins cher du trafic du réseau de l'un vers l'autre. Il va leur permettre d'échanger localement des données entre eux, ce qui sera toujours plus avantageux en coût et en qualité par rapport au trafic qu'ils auraient autrement été obligés de faire passer par des liaisons de transit.

Pour un opérateur régional par exemple, le trafic destiné à des opérateurs qui sont voisins (géographiquement parlant) peut passer directement de l'un à l'autre via un GIX local, afin de ne pas faire inutilement l'aller-retour jusqu'au prochain lieu où leurs opérateurs de transit, eux, peerent ensemble.

Les NAPs ajoutent la possibilité de livrer des services payants sans démultiplier les interfaces et liaisons de livraison.

2.3 Utilité sociale

Le GIX est aussi un outil de développement local, car en permettant des interconnexions

locales plus efficaces et moins coûteuses, il permet d'encourager et de sécuriser des services locaux. Par exemple peuvent plus facilement se développer des services de haute disponibilité, des sites Web, des serveurs de jeux, des projets de PRA (*Plan de Reprise d'Activité)* pour les entreprises locales, etc.)

Mais il y a plus : en agissant comme un point de rendez-vous, le GIX agit aussi comme un pot de miel, un concentrateur de richesses, de services, de besoins, de créativité, d'activité liée à internet. Cette concentration agit qui attirant les prestataires de services, les fournisseurs de services, vendeurs de transit. Plus le GIX se développe, plus il va avoir tendance à attirer ceux qui voudront faire des offres. C'est là qu'entre en jeu la dimension de NAP : permettre la livraison de services venus de loin aux opérateurs locaux, c'est permettre aux services de venir aux opérateurs.

Pour résumer, développer un GIX / NAP local, c'est

- favoriser les échanges et le développement local
- économiser et améliorer le trafic local et régional
- rompre l'isolement des petits opérateurs locaux
- rendre le local attractif

C'est faire venir le réseau en région, au lieu de continuer à faire converger les petits opérateurs vers la capitale.

Globalement donc, c'est favoriser le maillage d'internet sur le territoire, au lieu de le faire se développer en étoile vers un seul point de concentration au seul profit des opérateurs dominants.

2.4 Pour qui ?

Les principaux bénéficiaires sont les opérateurs qui ne sont pas en situation de se débrouiller facilement tout seuls. Ces opérateurs sont souvent petits, voire embryonnaires, pas très riches, et isolés (parfois dans une région qui souffre d'une connectivité faible ou rare vers le reste du monde). Et dans ces cas-là, ils sont surtout isolés en terme de rapport de poids, par rapport à d'autres opérateurs, rares, et dominants, avec en plus parfois des pratiques un peu anti-concurrentielles. Donc, vulnérables.

Pour un opérateur ainsi vulnérable, un GIX permet de rompre l'isolement. Un opérateur petit en région face à des mastodontes commercialement très agressifs (voire prédateurs) est confronté à un double problème. En effet il a souvent peu de choix en ce qui concerne ses solutions de connectivité vers le reste du monde, car les rares gros opérateurs présents sur place ne disposent pas toujours des services ou de la capillarité de réseau utiles, ou bien sont aussi des concurrents.

Au-delà des idées générales ci-dessus, voyons un peu plus en détail quels opérateurs seront intéressés par un GIX local.

2.4.1 Petits, micro et pas-opérateurs

Les premiers seront les opérateurs locaux, qui ne comprendront pourtant pas forcément les avantages d'un GIX de prime abord, parce qu'ils n'ont pas forcément conscience de ce qu'est un opérateur IP en termes techniques et stratégiques, ni donc de ce que ça implique pour

eux.

Il faudra donc peut-être le leur expliquer, pour ne pas dire : les former. Puis les accompagner dans cette transition, et faire de leur réseau passif un réseau actif d'opérateur (avec des routeurs BGP), avec un numéro de système autonome (un numéro d'AS), avec des adresses IP autant que possible indépendantes, éventuellement, et s'appuyer pour cela sur un LIR qui sache conseiller et accompagner avec neutralité.

Car souvent les sociétés locales sont clientes d'un opérateur national dominant ou d'une multinationale, qui les tiennent captives sur des adresses IP ne leur appartenant pas, liées à un contrat de fourniture d'autres services (transit, hébergement, liaison, collecte) et bien entendu, n'ont pas été leur expliquer l'intérêt de devenir des systèmes autonomes pour pouvoir s'affranchir de leur unique fournisseur. Sous couvert de conseil, de support, ou d'infogérance les opérateurs dépossèdent souvent leurs clients de toute liberté, ne serait-ce que de choix.

Mais ce sont les petites structures les plus dynamiques, même si avec des statuts différents (associatifs ou sociétés) elles peuvent avoir des visions très différentes, elles ont en commun le besoin de se développer localement et de voir la diversité et les opportunités se développer là où elles sont. Beaucoup plus souples, elles peuvent aussi s'adapter plus facilement : les décisions se prennent plus vite, plus efficacement, les strates administratives et organisationnelles ne sont pas un barrage. Elles ont donc tout à fait la capacité d'accéder aux compétences utiles pour devenir des opérateurs et tirer parti des points d'échange locaux.

2.4.2 Opérateurs moyens

C'est en fait une classe assez dépeuplée, en France les opérateurs moyens sont des grosses entreprises qui n'ont pas fait leur business sur des activités IP, ou bien elles l'auraient fait à Paris.

Leur activité est industrielle ou tertiaire, et leur usage de réseaux est essentiellement interne, avec de grosses contraintes (de gros enjeux) parce que la totalité de leur activité repose sur le fonctionnement de ces réseaux, qui ne sont pas leur activité, mais qui leur sont vitaux. Elles sont donc prêtes à y mettre les moyens, et l'ont déjà fait. Elle sont clients de solutions clé en main, auprès des opérateurs dominants, elles sous-traitent bien souvent la compétence (et donc les vraies décisions) en ce domaine.

En plus de ça, leur trafic externe est minime car leur business n'a rien à voir avec internet : ce ne sont pas des fournisseurs de contenus, ni des fournisseurs d'accès en général, et donc l'échange de trafic avec des tiers n'est pas un enjeu majeur pour elles, et encore moins un enjeu qui justifie qu'elles remettent en cause une seule seconde leur réseau mal ficelé, leur contrat gold leurs infra gérée par telle société de service, etc.

Bon courage pour les attirer sur un point d'échange donc, qui sera vu comme peu fiable, inutile pour leur besoin, voire un risque pour leur stabilité et leur sécurité. Leurs prestataires qui tiennent à les garder captifs leur déconseilleront catégoriquement pour préserver leur poule aux œufs d'or. Les banques, les gros distributeurs, les industriels sont dans celle classe d'opérateurs moyens, mais pour ainsi dire hors du net.

Il existe tout de même quelques sociétés qui se sont développés dans le domaine de d'accès à internet souvent, ou de l'hébergement, avec une spécialité de terrain (comme l'accès Wifi

ou en courant porteur). Celles-là auront des exigences assez fortes, mais aussi de l'expertise à apporter. Difficile de se tenir à la bonne distance, car la nécessité de se rassurer les poussera souvent à vouloir tout contrôler. Leur bonne volonté, leur compétence et leur capacité de financement pourra être très utile dans les phases de conception technique, pour financer le superflu (mais surtout pas le nécessaire) ce qui leur permettra aussi de se rassurer, pour prendre part aux astreintes du support, pour avoir un peu plus de trésorerie en fonds de roulement, etc.

2.4.3 Les gros opérateurs

Les gros opérateurs ne sont pas tout à fait ravis qu'un point d'échange local se monte, parce que ce service est clairement en train de piétiner leurs plates-bandes et de permettre à n'importe qui de faire les yeux doux à leurs clients. Il ne faut donc pas s'attendre à une réaction constructive d'un opérateur historique, qui y verrait une formidable occasion d'échanger son trafic local avec un autre opérateur dominant dans l'intérêt du consommateur.

N'y comptez pas. Une autre raison est que leur trafic est leur business. Il est donc risqué de faire passer leurs interconnexions avec d'autres opérateurs sur des infrastructures qu'ils ne maîtrisent pas. Les interconnexions importantes seront gérées via des peerings privés (donc via des liaisons privées) bien mieux maîtrisées dans leur discours (il suffit de surveiller un peu le trafic entre certains gros opérateurs pour voir à quel point de prétexte peut facilement passer derrière certains enjeux financiers, les consommateurs étant alors pris en otage).

Ensuite si peerer avec d'autres gros, c'est pour eux une affaire privée (donc pas sur un GIX public), peerer avec les petits, ça ne vaut pas le coup. C'est même un non-sens. Parce que maintenir des centaines de sessions de peering avec des centaines d'opérateurs microscopiques, c'est de la perte de temps d'ingénieur réseau. La bonne manière de faire, sera donc de leur refuser le peering, et de leur proposer soit d'acheter du transit, soit d'acheter du peering privé. Un peer refusé, c'est un petit opérateur qui devra payer pour son trafic (donc un client potentiel) ne l'oublions pas, un gros opérateur est avant tout un opérateur commercial.

Donc autant s'y faire tout de suite : les gros opérateurs sont très difficiles à faire peerer. Ils peuvent éventuellement être présents sur des GIX, pour des raisons politiques notamment. Mais leur présence n'aidera pas les petits opérateurs. Bien sûr il y a des contre-exemples pour faire mentir cette règle et il faut la relativiser en fonction du modèle économique du dit opérateur, les enjeux qui font les rapports de force peuvent varier de l'un à l'autre.

2.4.4 La contrainte

Enfin si on peut être tenté de les forcer, il faut garder en tête d'obliger un opérateur à se raccorder ne l'oblige pas à monter des peerings avec les autres. Et que monter des peerings avec les autres n'oblige pas à y faire circuler du trafic. La contrainte est donc difficile à mettre en place, encore plus à surveiller et faire respecter. Mais il faut se souvenir que la raison d'être d'un opérateur c'est d'avoir l'autonomie et la liberté de choisir ses interconnexions, et donc quelle justification pour contraindre un opérateur ?

Si toutefois le contexte politique ou économique d'une région le nécessite, on peut voir

l'obligation de peerer comme un outil indispensable à faire coopérer un minimum des opérateurs concurrents dans le sens de l'intérêt public. En pareil cas la neutralité du GIX devra être particulièrement soignée. Et le recours à un service de *route-server* obligatoire (voir plus bas) permettra au gestionnaire du GIX d'avoir la visibilité utile.

2.5 Comment faire

La première chose pour créer un GIX / NAP est de rassembler quelques bonnes volontés pour se lancer dans l'aventure.

Comme on le verra plus loin, le budget d'un GIX n'est pas forcément monstrueux. Inutile de s'en faire une montagne, de chercher des financements gigantesques et cinquante participants avant de démarrer. Peerer, ça demande d'être deux, et un matériel très raisonnable.

Ce qui est nécessaire dès le début, c'est de définir les règles de fonctionnement et la politique du GIX.

2.5.1 Politiques

Le GIX est un outil commun, que vont utiliser des membres. Il doit leur offrir un service qui autant que possible sera clair et bien délimité. La première chose est donc de définir quelle entité sera en charge de sa gestion, quelles seront ses missions, et quelles missions ne seront pas les siennes.

C'est le moment de résumer la fonction de GIX, et de choisir de l'ouvrir ou non aux échanges de nature commerciale entre les participants (donc d'en faire aussi un NAP).

C'est le moment de réfléchir à créer une association qui sera en charge de ce GIX, de décider comment on en deviendra membre, comment les membres contribueront, décideront de tout ce qui a trait au fonctionnement de la structure légale, mais aussi de la vie de la structure technique.

2.5.2 Indépendance

L'indépendance est un enjeu fort sur un GIX. Les expériences du FreeIX et du Panap à Paris, ont démontré que un opérateur IP qui monte un GIX pour satisfaire à ses propres intérêts peut très bien cesser de s'en occuper plus ou moins franchement, et finalement le liquider seulement quelques années après. L'initiative du Pouix de Gitoyen, malgré ses airs anti-commerciaux, n'a pas démenti l'importance de cet enjeu. Les autres opérateurs ne doivent pas dépendre de telles lubies, ni des intérêts de l'un d'entre eux en particulier. L'Equinix Exchange est un autre exemple français de GIX mal indépendant, car cette activité du groupe est conçue comme un instrument commercial (destiné à accroître l'intérêt du datacenter qui le maintient) et non pas comme ayant une réelle finalité de service.

Ces projets non (ou mal) indépendants se reconnaissent facilement : ils sont gratuits pour les membres, et les membres n'y décident rien.

Ces exemples sont donc à éviter pour construire un GIX pérenne, et une structure simple, légère, spécialisée, avec des règles simples et claires apportera beaucoup plus de stabilité dans le temps.

Une conséquence est que le GIX doit être capable de s'auto-financer en trouvant le bon équilibre entre qualité de service et coût. Le GIX étant toutefois un service utile et motivant, et à la fois d'une grande simplicité, cette équation est à priori soluble.

2.5.3 Neutralité

Il s'agit ici de la neutralité vis-à-vis des opérateurs IP qui vont participer au GIX.

Les attentes à la neutralité peuvent sembler assez rares sur un GIX. Mais on peut citer les problématiques de neutralité du réseau (priorisation, etc.) mais aussi de confidentialité, respect des libertés individuelles, etc. Il est donc souhaitable pour la tranquillité de tous que la transparence soit de mise, et notamment que l'équipement du GIX ne soit pas «prêté» ou partagé par l'un des opérateurs membres, mais dédié au projet.

S'agissant d'un NAP, puisque des enjeux financiers interviennent, le besoin de neutralité se trouve accru.

En tout état de cause, la neutralité du GIX / NAP doit faire partie des objectifs du projet, et il n'est pas concevable de faire confiance à un opérateur IP pour rendre le services à ceux qui sont tantôt ses partenaires, tantôt ses clients, tantôt ses concurrents.

2.5.4 Le prix

Le prix dépendra des coûts engagés. Pour répondre aux objectifs d'indépendance et de neutralité (que je qualifierais de prioritaires), il faut les répartir équitablement, et de manière à couvrir les coûts de fonctionnement (évidemment).

Tout est imaginable, et on peut répartir les prix à loisir :

- cotisation en tant que membre
- frais d'installation et frais récurrents en fonction de la taille du port souscrit
- mesure précise de l'utilisation du réseau
- tarification en fonction de la taille du CA de l'opérateur
- un mélange de tout ça…

Évidement plus la proposition tarifaire est complexe, plus la facturation le sera aussi, avec en plus des risques de rendre plus difficiles des développement ultérieurs, par exemple

- une implantation sur un autre site, avec donc une infra plus complexe et plus coûteuse
- une interconnexion avec un autre GIX
- lors d'un recours à des équipements plus gros (et coûteux)

Quelques notions qui peuvent jouer :

- être adhérent, payer une cotisation annuelle, c'est à la portée de tout le monde et ça peut correspondre aux frais de fonctionnement immuables et invariables de la structure (banque, assurance, papeterie, correspondance, assemblées)
- pour un petit opérateur qui utilise 10 Mbps, payer 100 ou 1000 ne fait pas forcément sens
- un port 1000 Mbps cuivre peut servir comme port de 100 Mbps mais pas l'inverse, mais cela peut revenir plus cher d'avoir les deux types de ports

- le prix du transit tend à diminuer (pas forcément en province), les prix du peering n'ont pas forcément besoin de faire la même chose, car l'aspect financier n'est pas le seul à entrer en jeu

2.6 Le besoin technique

Le GIX / NAP est un élément simple d'interconnexion en comparaison aux réseaux IP des opérateurs qui en sont membres. Il n'en est pas pour autant une infrastructure dont il faut sous-estimer l'importance, car elle est le point névralgique d'interconnexion de ces réseaux.

2.6.1 Composition fonctionnelle

On trouve les éléments suivants dans le fonctionnement du GIX :

- une infrastructure de commutation
- un système d'information qui prend en compte tous les acteurs (opérateurs membres, administrateurs, public)
- un NOC (centre des opérations) disponible et réactif
- une infrastructure propre pour l'exploitation du point d'échange, qui permet de gérer les opérations du NOC, héberger le système d'information et les services

2.6.2 Constitution physique

La mission est simple et donc les éléments constitutifs le sont aussi. On a besoin :

- d'un lieu sur lequel les opérateurs puissent faire arriver une extrémité de leur réseau, pour se raccorder (en général, un datacenter—ou un netcentre—relativement neutre, *i.e.* qui ne viendra pas interférer)
- sur ce lieu, d'un rack, qui permettre essentiellement
    - d'accueillir les différents équipements,
    - de faire arriver les liaisons des futurs membres du GIX
    - d'avoir un peu de place pour brasser, ranger des accessoires : un tournevis, un dBmètre, des optiques ou quelques câbles, etc.
    - quelques tiroirs fibre (à vous de voir selon les modalités de brassage propres au site) et/ou panneaux de brassage cuivre
- le commutateur de production
- un commutateur de spare
- deux serveurs rackables pour les services

2.6.3 Le système d'information

Infrastructure essentielle, le point d'échange doit avoir une gestion impeccable, autant par souci de la stabilité du réseau que par le besoin de crédibilité et de pérennité du service.

Il est donc indispensable de ne pas sous-estimer la composante essentielle au pilotage et à la qualité des services qu'est son système d'information.

Les fonctions du système d'information

La première fonction du système d'information est de proposer des interfaces aux différents acteurs qui entrent en contact avec l'infrastructure. On peut distinguer essentiellement quatre profils d'usager différents.

- Le public, qui consulte les outils mis à sa disposition pour observer le trafic échangé sur le GIX / NAP, sa fréquentation par les opérateurs, ou bien encore pour utiliser le Looking-Glass, point d'observation du réseau déporté sur le GIX.
- Les opérateurs qui bénéficient d'une interface sécurisée pour suivre leurs statistiques de trafic et positionner des alertes, produire des requêtes à l'intention des administrateurs du GIX / NAP, suivre des tickets d'incidents ou bien rechercher de nouveaux peers avec lesquels échanger du trafic
- Les administrateurs techniques de l'infrastructure, qui suivent les tickets et les demandes des opérateurs, suivent l'usage du réseau et gèrent l'utilisation des ressources, assurent la maintenance au quotidien.
- Les gestionnaires du GIX / NAP qui bénéficient d'accès privilégiés pour extraire des statistiques sur les usages des diverses fonctionnalités, réaliser la facturation, ou pour suivre de plus près des tickets qui retiennent leur attention.

Le système d'information a également un aspect fonctionnel essentiel du point de vue de la normalisation et de la qualité, puisque en centralisant les informations il permet à la fois de réaliser l'inventaire des utilisations et des ressources disponibles, mais aussi de générer de manière reproductible, cohérente et fiable les configurations à mettre en œuvre pour les filtres automatiques, pour les configurations initiales des seuils d'alertes, pour la gestion de la topologie ou encore pour les route-serveurs.

Les interfaces

Il est souhaitable que le système d'information propose aux différents acteurs des interfaces qui répondent à leurs besoins. Généralement des interfaces Web apportent un confort et une évolutivité satisfaisants.

Des fonctionnalités souhaitables sont proposées ci-dessous :

1. Une interface destinée aux opérateurs membres, qui leur permet de :
    - modifier les informations relatives à leur entité et à leur système ;
    - commander un nouveau port ;
    - suivre le trafic sur leur interface ;
    - positionner des seuils d'alertes pour différents types de trafic, entrant ou sortant ;
    - mettre les filtres des route-serveurs à jour lorsque leurs annonces changent ;
    - consulter la liste des membres connectés ;
    - consulter le looking-glass des route-serveurs.
2. Une interface dédiée aux administrateurs, qui leur permet de :

- valider l'inscription des opérateurs ;
- réaliser la livraison des ports demandés par les opérateurs ;
- gérer l'affectation des ressources (adresses IP, VLANs, numéros de ports, types d'interfaces) sans risque ;
- notifier les opérateurs des configurations techniques à mettre en place, ou les leur rappeler ;
- changer le mot de passe d'accès au site des membres pour un opérateur, et le lui envoyer ;
- générer les filtres et les configurations pour les équipements et les route-serveurs ;
- trouver rapidement les informations dont ils ont besoin pour le support.

3. Une interface consultative pour les gestionnaires. Pour ce qui est de la facturation, une interface Web peut être utile à titre consultatif, mais pour la génération de documents comptables il est préférable que le système soit automatisé et qu'une protocole permette de faire interroger le système d'information par les outils de facturation. Une API suffisante est donc recommandée.

Un site Web présentant le GIX / NAP et les principales informations au public.

2.6.4 Le commutateur

Le cœur du GIX est son infrastructure de commutation, par laquelle vont échanger les opérateurs (membres) raccordés. Chacun depuis sont routeur (couche 3) avec une adresse IP que le GIX leur aura attribuée, et tous dans une même zone de broadcast (un même réseau), ils vont échanger deux à deux, en toute liberté.

Cette zone d'échange c'est donc, à proprement parler, le GIX. Son travail essentiel est donc de gérer les couches inférieures sans faute ; je veux parler des couches 1 (physique) et 2 (liaison), de maîtriser impeccablement la topologie du réseau, de s'assurer de la sécurité des lieux (détecter les boucles, contrôler les adresses, filtrer les paquets techniquement nuisibles).

Mais la principale qualité du GIX est de se faire oublier : qu'il soit simple ou complexe un bon GIX est transparent, et depuis internet (la couche 3, au-dessus) il est quasiment invisible.

Dimensionnement

Le dimensionnement du commutateur est à votre convenance, il est bien clair qu'on a pas besoin d'un châssis de 10u qui requiert 2 kVA pour commuter des trafics comme on en verra sur un GIX local au début de son existence. Tous les commutateures un peu modernes, tant qu'on ne leur demande que de commuter des paquets (ce qui sera le cas sur un GIX) feront ça très correctement, en hardware. Autant se diriger vers des équipements « top-of-rack » car leur vocation n'est pas non plus d'allumer des fibres pour faire de la longue distance.

Ceci permettra de rester dans un budget, un encombrement physique, et un besoin de puissance raisonnables.

Fonctionnalités

Pour creuser un peu la question du commutateur, on peut tout de même évoquer les aspects suivants.

- ce doit être un commutateur gigabit, adapté au site notamment pour ce qui est de ses interfaces : inutile de mettre un 24 ports cuivre + 4 sfp sur un site dans lequel tous les raccordements se font en fibre
- s'il est prévu d'avoir des membres raccordés en FastEthernet, le cuivre pourra être requis, car les interfaces SFP ou GBIC ne le supportent pas toujours, une solution relativement simple peut alors être de prévoir un second commutateur, avec des ports cuivre, et un uplink vers le commutateur principal qui lui, sera full gigabit
- le réseau d'un petit GIX a beau être simple, il faut maîtriser la topologie, les MAC et les risques liés aux boucles et aux broadcast, ça veut dire filtrer correctement les BPDU en entrée/sortie, filtrer les MAC par port, envisager d'activer la détection de boucle, le port security, réfléchir à fixer des seuils pour bloquer les orages
- le support du 802.1q ne fait plus tellement question sur les commutateures professionnels
- les fonctionnalités comme RMON et SNMP bien pratiques pour lever des alertes, surveiller des seuils, relever des compteurs
- si votre GIX comprend plusieurs équipements, la gestion de la topologie va se révéler une problématique cruciale et des protocoles plus efficaces et réactifs que spanning-tree s'inviteront rapidement, idéalement des protocoles plus rapides (ERP, MRP).

Les règles techniques

Plutôt que de faire doublons je vous renvoie vers la traduction des « Best Current Operational Pratices » (Bonne pratiques) pour la gestions des points d'échange publics, que j'ai traduite et placée en partie 2 de ce HOWTO.

2.6.5 Le route-server

Afin de faciliter le montage de sessions entre les *n* membres, vous pouvez éviter qu'ils aient à configurer n-1 sessions en mettant à disposition un service de route-server (RS).

Le RS est l'équivalent du route-reflector (RR) qui, au sein d'un AS, permet d'éviter de devoir mettre tous les routeurs en full mesh à cause du fonctionnement de iBGP. La problématique est certes un peu différente puisque sur un GIX on travaille en eBGP, mais le but est le même : simplifier le nombre de sessions à monter.

En principe le RS est transparent dans le routage : il ne fait que relayer les annonces NLRI émises par les membres connectés, sans modifier l'AS-PATH (chemin) ni le next-hop (adresse du routeur auquel envoyer les paquets pour joindre la destination). Et en conséquence le trafic IP ne passe pas par le RS, il continue d'aller directement d'un routeur d'un membre au routeur d'un autre membre, en niveau L2 (commutation), sans intermédiaire ni passage par le niveau 3 (IP) donc sans routage.

Avantages

Chaque opérateur qui le souhaite peut, en établissant une simple session BGP avec le route-server, récupérer les annonces des autres membres qui y sont déjà raccordés, et s'en servir pour envoyer ses propres annonces.

Pour le gestionnaire du point d'échange, le RS présente l'avantage de pouvoir observer les routes annoncées par les membres. Sur un GIX dans lequel l'utilisation du RS serait la règle, il serait possible d'observer le comportement des membres en étudiant leurs annonces faites au route-serveur.

Enfin le RS est l'équipement idéal pour mettre en place un service de *looking-glass* qui permet d'avoir une vue d'internet depuis le point d'échange. Une vue nécessairement partielle, mais qui donne une idée utile de l'impact du GIX sur le réseau. Ce service de *looking-glass* peut, si le RS n'est pas obligatoire à utiliser, également être mis en oeuvre sur un simple collecteur de routes avec lequel les membres seraient obligés de peerer.

Inconvénients

En utilisant le RS, un opérateur perd un peu de la finesse qu'il aurait en établissant une session avec chaque peer. Or du fait de l'existance du RS, certains opérateurs risquent de ne plus vouloir établir de sessions directes.

Un autre inconvénient est la (re)centralisation qui fait du RS un équipement relativement critique, mais on peut regagner en sécurité en mettant plusieurs RS à disposition, l'arrêt de l'un d'entre eux pour maintenance (ou incident) n'ayant alors pas d'impact sur le trafic.

Enfin si le peering avec un RS n'est pas obligatoire, un *looking-glass* qui l'utilise donnera qu'une image faussée du peering sur le GIX.

Précisions sur le RS

Attention on ne peut pas utiliser un route-server pour interconnecter deux GIX, contrairement à ce qui se dit ça et là. En effet le RS, comme le RR, ne prend pas en charge le trafic IP, il ne fait que relayer les annonces BGP.

Les points d'échange qui utilisent des plages d'adresses différentes et disent s'interconnecter avec un route-server font un abus de langage trompeur : ils utilisent en réalité un routeur, et par conséquent on ne peut plus parler de peering. Ceci sort donc complètement du cadre de ce document.

Outils

Les RS ayant seulement la fonction de gérer des sessions BGP et de les propager, ils ne nécessitent pas des équipements dotés d'une fond de panier puissant pour faire passer le trafic. Autrement dit les RS sont des purs *routing engines*, à l'exclusion de la fonction de *forwarding engine*. En cela ils sont parfaitement complémentaires du commutateur du GIX lui-même, qui est un pur *forwarding engine*.

Il est conrant que les gestionnaires de points d'échangent tirent profit de cette caractéristique du RS, en confiant cette fonction à un simple serveur, type PC industriel rackable, doté d'un logiciel de routage, en général en logiciel libre, tel que *quagga*,

openbgpd ou *bird*. Il existe sur internet des exemples divers de configurations de RS avec ces logiciels. Leur déploiement et leur maintenance s'en trouvent considérablement facilités, outre les économies ainsi réalisées.

2.7 Les besoins humains

Il y a très peu de travail à faire sur un GIX, une fois la mise en place faite. Mais le GIX reste une infrastructure réseau essentielle, un concentrateur de trafic, et donc aussi un point de vulnérabilité important. Il est important qu'au moins un technicien soit à même d'intervenir sur place dans un délai raisonnable, et à ce niveau tout est permis, y compris la sous-traitance de la maintenance d'urgence à l'un des membres.

Pour ce qui est de la mise en place, les tâches sont assez variables et peuvent se répartir.

2.7.1 Administratif

Créer, déclarer la structure. Obtenir des ressources IP du Ripe ou d'un LIR (ce ne sont pas des ressources critiques, elles n'ont pas forcément besoin d'être annoncées sur internet, et il sera un peu pénible mais faisable de re-numéroter en cas de besoin).

Gérer le secrétariat.

2.7.2 Financier

Ouvrir un compte en banque, gérer la facturation (les prélèvements, les relances) la comptabilité.

2.7.3 Technique

Les installations techniques physiques sont peu complexes, l'affaire d'un ou deux jours au maximum pour installer les équipements et accessoires.

Le développement d'une base informatisée pour la gestion des membres, des statistiques d'utilisation si besoin, de l'assignation des ports et des adresses, et les interfaces de commande, listing des membres, outils de gestion, monitoring, alertes, looking-glass… Tout ça peut prendre beaucoup plus de temps, mais aussi se faire sur la durée.

Il est aussi possible de s'appuyer sur des développements qui ont déjà été faits par d'autres, comme le FR-IX.

2.8 Se lancer

Comme dit plus haut, il n'est pas utile d'attendre de réunir tout le monde pour démarrer le projet. L'expérience montre que le plus difficile est de se lancer, à force de vouloir faire trop bien ou en accord avec tout le monde.

Le consensus s'acquiert plus vite en petit comité et un projet modeste, simple a plus de facilités à se mettre en place. D'autres participants pourront se joindre au projet une fois qu'il est lancé, d'autant c'est un des principes du GIX d'agir comme pot de miel.

Dans cette optique il convient de veiller à ce que le projet initial soit compatible avec les

besoins futurs et avec des extensions potentielles futures. Il doit être pensé pour un maximum d'ouverture, avec une évolutivité des matériels, des interconnexions et la venue de nouveaux opérateurs en tête.

Compte tenu que les investissements utiles ne sont pas nécessairement très importants, une manière efficace de (au moins) démarrer le projet est de monter une association dite « loi de 1901 ».

2.8.1 Fixer les règles

Dans une association il faut parfois bien réfléchir aux nécessités un peu opposées de se garantir contre la survenue massive de nouveaux adhérents pas forcément en phase avec la visée initiale (entrisme), et la trop grande rigueur qui rend le collectif inaccessible.

Le premier risque peut être limité grâce à l'esprit du contrat associatif : c'est une convention entre les parties, donc un contrat, en vue de poursuivre un objectif précis. Celui-ci doit être bien cadré dans les statuts. On peut aussi faire appel à une charte, qui définira les usages admis et ceux qui ne le sont pas. Ce sera l'occasion rêvée pour bannir le spam, les protocoles bizarres, les équipements qui fonctionnent mal et vont poser des problèmes à tout le monde, interdire le forçage de routes, etc.

A titre d'exemple vous pouvez trouver ici la convention proposée par FR-IX.

Cette réflexion sur le projet pourra amener ses fondateurs à voir beaucoup plus loin que le besoin local, et à envisager des partenaires plus lointains.

2.8.2 Le peering distant

Le peering à distant (remote peering) consiste à avoir recours à des liaisons de transport de niveau 2 pour se raccorder à des GIX distants, au lieu de liaisons locales (donc physiques, dites « layer-1 »).

Ce mode de raccordement permet à beaucoup plus de participants de rejoindre le point d'échange sans avoir à faire des investissements lourds pour étendre leur réseau jusqu'au pied du GIX pour s'y relier. C'est donc un levier intéressant pour développer la fréquentation du GIX et donc au bénéfice de tout le monde sur cet aspect.

Il y a pourtant de nombreux inconvénients, qui ne sont pas sans impact sur la qualité et la stabilité du GIX, et ceci explique que les raccordements de ce type ne sont pas toujours autorisés.

Parmi ces désagréments on trouve en particulier : les risques d'instabilités accrus du fait d'un lien L2 (actif), la plus longue durée requise pour repérer la chute d'une liaison en L2 par rapport au L1 et donc l'impact de cette durée sur la quantité de trafic perdu, les risques d'interférence de la topologie L2 du commutateur par le L2 qui sert à transporter le participant distant. Tous ces risques sont proportionnels au nombre de participants ainsi raccordés et dégradent globalement la qualité du GIX.

Il convient bien évidement de considérer aussi l'accroissement de la latence qui vient en directe contradiction avec la qualité résultant d'une proximité physique que viennent chercher les membres locaux.

Autoriser ou non le remote peering est donc un compromis à faire entre la qualité et la

volonté d'ouvrir le GIX à davantage d'opérateurs. On peut aussi envisager des solutions comme le recours à des VLANs différents : l'un autorisé et l'autre non au remote peering, avec des route serveurs différents, des mécanismes de sécurité différents. Les membres peuvent ainsi choisir.

Une alternative à laquelle il convient de réfléchir, est de développer un autre GIX qui sera plus proche des nouveaux membres, et d'interconnecter ce nouveau GIX avec le premier. L'interconnexion est ainsi mutualisée, plus facilement meilleure, et on obtient une meilleure qualité.

2.9 Raccorder des GIX

Monter un GIX local c'est bien. Mais on peut pousser le raisonnement en développant des GIX et en développant entre eux des interconnexions. Raccorder des GIX voisins permettra en effet d'augmenter virtuellement les effectifs de chaque GIX tout en conservant la plupart des avantages d'un GIX local (trajet court, bas coût, efficacité) tout en augmentant les possibilités de développement des opérateurs participants.

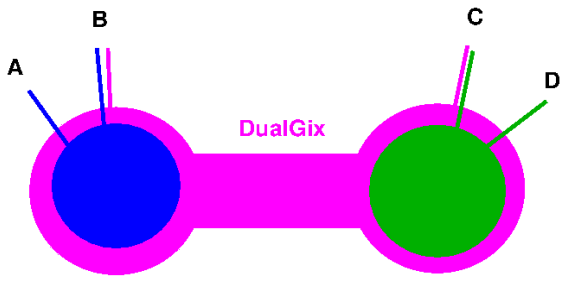
Il est important d'envisager dès le départ de telles possibilités d'extension afin de veiller à ne pas faire des choix (techniques, politiques, financiers) qui se révéleraient par la suite incompatibles. Pour cela on peut par exemple veiller à rester cohérent avec un schéma comme celui du DualGix.

2.9.1 Le modèle DualGix

Afin d'encourager davantage encore le dynamisme autour des points d'échange, Opdop a créé le concept de DualGix qui consiste à rapprocher deux GIX / NAPs comme des domino, pour en constituer un troisième, en sur-couche.

Fonctionnement

Ce nouveau GIX en sur-couche est opéré grâce à un nouveau VLAN qui est propagé jusqu'aux interfaces des membres participants sur les deux GIX interconnectés. Il suffit que les interfaces soient taguées dans ce nouveau VLAN pour que les membres puissent y accéder, et établir des sessions de peering.



Dans la figure ci-contre on a un GIX *bleu* sur lequel peerent les opérateurs A et B. Et un autre GIX *vert* sur lequel sont raccordés C et D.

Le VLAN dessiné en *mauve* constitue un nouveau GIX qui permet à B et C d'établir une session BGP pour peerer ensemble.

Il est tout à fait possible de mettre les services habituels à dispositon sur ce nouveau GIX, comme par exemple un route-server.

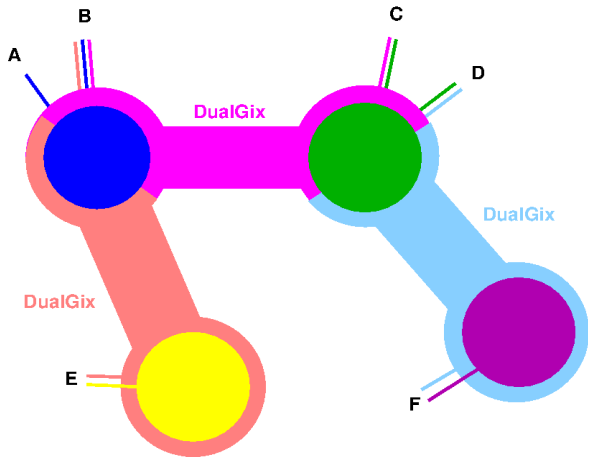
Gestion

Ce troisième service est géré exactement comme un GIX / NAP classique, en collaboration

par les deux GIX fondateurs. Le sur-coût de l'interconnexion est intégré dans une nouvelle offre, optionnelle, proposée aux membres qui veulent pouvoir peerer « plus loin ». Et il est partagé à 50% par les deux GIX puisque leur trafic respectif sur cette interconnexion est, par définition, strictement identique en volume.

Modularité

Ce modèle s'applique facilement et peut être traité comme une brique de base dans des schémas plus complets. Par exemple le GIX A peut établir un DualGix avec le GIX B, et un autre avec le GIX C, sans qu'il y ait interférence. L'usage de VLANs d'interconnexion différents permet facilement d'isoler ces trafics, et c'est nécessaire car le GIX A ne doit pas devenir un simple intermédiaire de B et C.



Or cet intermédiaire agirait nécessairement au niveau IP (routage), ce que le GIX A s'interdit. Si B et C veulent échanger directement du trafic, ils peuvent à leur tour créer un DualGix.

Sur l'image ci-contre on peut voir quatre GIX (représentés par les ronds bleu, vert, jaune et violet) qui sont interconnectés par des DualGIX (mauve, rose et cyan).

Par exemple l'opérateur B, présent initialement sur le GIX bleu, peut peerer avec A qui est sur le même GIX. Mais comme B a un accès dans le DualGIX mauve, il peut aussi peerer avec C qui est sur le GIX vert. Et avec E, grâce à son raccordement au DualGIX rose.

2.9.2 L'interconnexion avec routeur

Tordons ici le cou à l'idée trop répdandue qu'on peut utiliser un route-serveur pour interconnecter des GIX. Un route-serveur ne fait que propager les annonces des routes, mais ne transporte par le trafic. Pour transporter le trafic d'un GIX à l'autre et donc en général d'un subnet IP à un autre (les deux GIX n'ayant pas le même plan de numérotation), c'est d'un routeur qu'il est question : le trafic est géré par un équipement de niveau 3 l'implication évidente que, par définition, il ne s'agit plus de peering mais de transit.

Conséquences

Les implications sont majeures. La première est que le gestionnaire de l'équipement intermédiaire devient un transitaire (par définition du transit), et met en jeu sa neutralité puisque son routeur agit sur les annonces BGP des membres, ce qui est susceptible d'être mal reçu. La seconde est qu'il s'intercale entre les membres des deux GIX ainsi reliés, et prend la responsabilité d'acheminer leur trafic, et donc la part de risque que cette responsabilité implique. La troisième est que les membres d'un GIX n'ont plus la même latitude de choix et de maîtrise de leur trafic, donc l'intérêt est moindre. Enfin techniquement, la latence induite par un routeur est généralement supérieure, et le chemin en BGP sera rallongé donc de moindre qualité.

Pour toutes ces raisons une interconnexion maîtrisée en couche 2 est préférable, même si les deux modèles ne sont pas exclusifs l'un de l'autre.

3 Bonnes pratiques pour la spécification d'un point d'échange public

- Source : http://www.ipbcop.org/
- Auteurs : Michaël Smith, Florian Hibler
- Date : 8 octobre 2011
- Statut : draft
- Titre original : Public Peering Exchange Configuration best current operations practices
- Traduction : Sylvain Vallerot

Résumé

Ce document passe en revue les différentes composantes qui tendent à instaurer de bonnes pratiques pour la gestion et le raccordement à des points d'échanges. Il indique des principes de configuration et de paramétrage, mais pas d'information liée à des équipements en particulier.

3.1 Contexte

Il y a une multitude de points d'échanges dans le monde, qui sont utilisés pour fournir à des opérateurs une infrastructure mutualisée afin de leur permettre de s'interconnecter et d'échanger du trafic. Bien qu'il puisse y avoir des spécificités propres à chaque point d'échange, il y a aussi des éléments de configuration communs qui, s'ils sont mis en œuvre, contribueront à la stabilité du service.

Ce document décrit les grandes lignes qui devraient s'appliquer dans la plupart des situations, proposant ainsi une base pour les spécifications de points d'échanges mais ne prévalant pas sur elles. Les règles spécifiques à chaque point d'échange doivent être respectées même lorsqu'elles sont contraires aux recommandations faites ici.

3.2 Bonnes pratiques

Ce document est divisé en quatre sections.

- recommandations physiques
- recommandations pour les couches OSI 1 et 2
- recommandations pour la couche transport
- autres recommandations

Ce document utilise les définitions ou conventions de nommage suivantes.

- GIX - terme générique utilisé pour désigner un point d'échange, un point d'accès au réseau (NAP), etc.
- participant(s) - terme générique utilisé pour désigner une ou des entités se raccordant à un GIX

3.3 Couche physique

3.3.1 connexion directe

Autant que possible chaque participant devrait se raccorder sur l'équipement de commutation du GIX au moyen d'une interface de niveau 3.

Une connexion directe permet de minimiser les risques d'apparition de trames de broadcast inattendues ou de tout autre type de trafic indésirable et provenant d'un autre réseau de niveau 2.

En particulier, les connexions de commutateur à commutateur entre GIX et participant devraient être évitées. Le risque de problèmes pouvant avoir un impact sur l'ensemble de l'infrastructure de commutation et sur les participants est considérablement plus élevé du fait de problèmes liés au niveau 2 qu'avec des connexions directes.

3.3.2 connexion à distance

Dans cette situation, le participant ne se raccorde pas physiquement directement au GIX, car il n'a pas d'équipement sur place ou à proximité. Ce choix est généralement motivé par une recherche d'économie. Le transport s'effectue en général par MPLS via des opérateurs agréés par le GIX. Ces opérateurs de transport doivent s'assurer de leur compatibilité avec le réseau du GIX (la plupart des pré-requis sont indiqués dans la section 2).

Revendeurs

Certains GIX prévoient des ports pour les revendeurs (avec des offres de peering à distance). Un opérateur de transport agréé se raccorde alors au GIX et revend des connexions en utilisant ce raccordement. La revente permet à des participants de devenir membres du GIX au travers de l'opérateur de transport, sans avoir besoin de payer directement pour un raccordement sur le GIX.

Par exemple si le transporteur se raccorde au GIX avec un port 10G, il peut revendre 10 fois 1G, ou 100 fois 100 Mbps, ou 1000 fois 10 Mbps à des participants potentiels. Toutefois le port 10G ne doit pas être sur-souscrit.

3.3.3 Qualifier le raccordement

Lors de la première connexion à un GIX, il est recommandé de prendre note des caractéristiques observées afin de pouvoir s'y référer si plus tard des problèmes apparaissent. En particulier la qualité du lien devrait être vérifiée et consignée.

Liaison optique

Les puissances d'émissions et de réception devraient être relevées au moyen d'un puissance mètre optique, et consignées. Toute mesure suspecte devrait donner lieu à des réparations avant que du trafic soit envoyé sur cette liaison.

Liaison cuivre

Des tests de continuité devraient être conduits et leurs résultats consignés. Comme pour la fibre, toute mesure suspecte devrait donner lieu à des réparations avant que du trafic soit envoyé sur cette liaison.

Liaison optique ou cuivre

Une fois le raccordement fait, les compteurs devraient être consultés pour repérer d'éventuelles anomalies. En particulier on ne devrait pas observer d'erreurs (CRC, Framing, Input, Ouput, Drops, etc.) sans quoi des mesures curatives devraient être mises en œuvre avant d'utiliser la liaison.

3.3.4 Étiquetage

Tous les éléments de connectique devraient être étiquetés pour une identification aisée, en utilisant des règles de nommage standardisées. Ceci concerne les câbles fibre et cuivre, les patch panels, les interfaces et les équipements raccordés.

3.3.5 Documentation

Une bonne documentation des configurations sera d'une valeur inestimable en cas de problème ou pour une transmission de compétence. Elle devrait inclure :

- une définition segment par segment de chaque circuit : chaque point de raccordement entre une interface et le GIX devrait être répertoriée avec les identifications utilisées sur l'étiquetage
- une liste des prestataires, intervenants ou fournisseurs impliqués dans la couche physique : avec au strict minimum un contact ou une liste de contacts doit figurer dans la documentation, si plusieurs opérateurs fournissent des services au GIX ces informations doivent apparaître pour chacun et être associées aux éléments qu'ils fournissent dans l'infrastructure.

3.4 Couches data et réseau

3.4.1 Configuration des IP

Il convient de veiller à ce que les bons masques de réseau soient utilisés sur les interfaces. Il n'est pas sûr de supposer que tous les GIX utilisent des préfixes de taille identique.

3.4.2 Ethertypes

Les trames échangées sur les GIX ont habituellement les types suivants.

- 0x0800 - IPv4
- 0x0806 - ARP
- 0x86dd – Ipv6

3.4.3 Broadcast et non-IP

Les protocoles fonctionnant en broadcast ou pas en IP doivent être désactivés sur les interfaces raccordées au GIX, ou filtrées d'une manière ou d'une autres lorsque la désactivation n'est pas possible. Ceci concerne (mais sans se réduire à cette liste) les trames DHCP, MOP, Ethernet Keepalive, NetBIOS et les annonces RA IPv6.

3.4.4 Protocoles propriétaires

Tous les protocoles dynamiques d'exploration (CDP, FDP, etc.) doivent être désactivés sur les interfaces raccordées au GIX.

3.4.5 IP redirect

Les redirections doivent être inhibées sur les interfaces reliées au GIX.

3.4.6 IP Directed Broadcast

Doit être également désactivé sur les interfaces reliées au GIX.

3.4.7 Proxying

Les protocoles de proxy, tels que Proxy ARP et IPV6 Proxy Neighbor Discovery, doivent être désactivés.

3.4.8 Contrôle de la couche 2

Dans une configuration de commutateur à commutateur, sauf spécification inverse, les protocoles de spanning-tree doivent être désactivés sur les interfaces reliées au GIX. En cas d'impossibilité tout le trafic doit être filtré au niveau de l'interface.

3.4.9 Protocole de routage internet

Les IGP ne doivent pas apparaître sur l'interface reliée au GIX.

3.4.10 Limitation des MAC

La plupart des GIX sont très vigilants sur le nombre de MACs autorisées sur une connexion. Habituellement une seule MAC est autorisée. Si le participant a un équipement intermédiaire, il doit s'assurer que celui-ci est parfaitement silencieux et n'introduit pas de trames indésirables (comme décrit précédemment). Ceci pourrait provoquer un déclenchement du mécanisme de sécurisation du port par lequel le participant est raccordé.

3.5 Couche de transport

3.5.1 Annonce du subnet d'interconnexion

Les participants ne doivent pas annoncer le réseau qui sert pour l'interconnexion sur le GIX

en BGP.

3.5.2 Anticipation des sessions

Les participants ne doivent pas configurer à l'avance des sessions BGP avec d'autres participants, tant que tous les deux ne sont pas prêts.

3.5.3 Filtrage

Un participant devrait mettre en place des règles de maximum prefix count, ou des filtres sur les annonces de ses pairs à chaque fois que cela est possible.

3.5.4 Route serveur

Lorsqu'un GIX propose un service de Route Serveur et que le participant a une politique de peering ouverte, il devrait faire usage de ce service afin de pouvoir en récupérer le plus grand nombre d'adresses possible avec un minimum d'efforts. Il est également important si beaucoup de trafic est échangé ou si la session de peering revêt une importance particulière, d'établir des sessions de peering directes.

3.5.5 Liste de discussion

Le centre des opérations du participant devrait être conscient de l'existence d'une liste d'échange pour les participants du GIX et y être inscrit. L'adresse utilisée pour cette souscription ne peut pas être reliée à un système de gestion de ticket ni donner lieu à des réponses automatiques.

3.5.6 Déconfiguration

Si un participant quitte le GIX, les autres participants doivent déconfigurer leurs sessions avec lui au plus vite, afin de réduire le trafic ARP sur le GIX.

3.6 Autres recommandation

3.6.1 Sécurité

Il n'y a pas beaucoup de mesures disponibles pour affermir la sécurité des connexions entre les participants, compte tenu de ce que les sessions sont réalisées bi-latéralement entre eux à travers le GIX, on peut proposer mais pas forcément recommander telle ou telle méthode.

- MD5 : les participants peuvent utiliser MD5 pour authentifier leur session BGP,
- Liste d'accès MAC : un participant peut utiliser des ACL sur les adresses MAC pour vérifier que ses pairs établissent des sessions à partir de sources connues. Cependant ces ACL peuvent poser des difficultés,
- Liste d'accès sur les IP : un participant peut utiliser des ACL pour limiter les peers autorisés à établir des sessions BGP en filtrant sur leur IP,
- GSTM (Generalized TTL Security Mechanism, RFC 5082) : les participants devraient utiliser GSTM sur leurs routeurs à chaque fois que c'est possible

- les plus récents mécanismes de sécurisation de BGP ne sont pas traités dans cette version du document

3.7 Conclusion

«Soyez restrictifs dans ce que vous émettez et ouverts sur ce que vous recevez» : Eu égard à l'extrême sensibilité d'une infrastructure qui raccorde une multitude de participants sur une seule et même plate-forme de niveau 2, il serait utile de corriger cet adage en «Soyez restrictifs dans ce que vous envoyez et recevez».

Un réseau de niveau 2 est certainement la manière la moins coûteuse et la plus simple pour permettre l'interconnexion de multiples réseaux via une plate-forme commune, mais c'est aussi la plus vulnérable à des erreurs qui peuvent se produire pour ainsi dire n'importe où.

Il est dans l'intérêt de tous les participants et des opérateurs du GIX de limiter le trafic parasite sur cette plate-forme dans le but d'en améliorer la stabilité. Idéalement seules des interfaces de niveau 3 devraient être connectées à l'équipement de commutation, et les routeurs raccordés ne laisseraient jamais passer de protocoles indésirables. Mais en réalité il existe de telles disparités entre les équipements, et bien souvent même entre les versions logicielles et les fonctionnalités d'un même équipement, que chacune de présentes recommandations doit être adaptée au cas par cas.

4 À propos de Opdop

Opdop est un projet qui repose à cent pour cent sur une société fondatrice créée en 2003 et dont les activités ont considérablement évolué pour prendre en compte les préoccupations et les besoins de ses partenaires. Cette société appelée ManyOnes.COM et créée en 2003, immatriculée au registre du commerce et des sociétés de Paris sous le numéro 449 031 574, portait déjà dans son nom les marques en apparence contradictoires, mais pourtant conjuguées de la multitude et de l'unité.

De la prestation de services techniques à la gestion de réseaux d'opérateurs, du logiciel libre au routage propriétaire, et toujours **au service de ses partenaires**, ManyOnes.COM a fait **l'expérience des métiers qui sont les leurs**. Cette expérience lui permet de comprendre leurs préoccupations afin de leur apporter les nouveaux services dont ils ont besoin.

C'est dans cette optique que ManyOnes.COM s'est transformée pour se retirer des domaines qui la plaçaient en concurrence de ses partenaires et **garantir ainsi son entière neutralité** vis à vis d'eux.

Opdop signifie littéralement «OPérateur D'OPérateurs» et souligne ainsi son positionnement en-dehors du marché des services IP. Depuis janvier 2010, ManyOnes.COM s'est séparée de ses activités de services IP et a entamé sa mutation en tant que soutien au service des opérateurs IP et en tant que **support au développement numérique des territoires**.

Afin d'être complète cette démarche s'est opérée dans plusieurs directions simultanées pour couvrir le champ des besoins des opérateurs mais aussi des collectivités locales.

- La mutualisation de réseaux de transport pour rompre l'isolement des opérateurs
- Le développement de points d'échange (GIX) et d'accès au réseau (NAP) comme points d'ancrage locaux
- La formation et le conseil pour faciliter l'accession au statut d'opérateurs pour les entreprises locales ou la gestion des points d'échange et d'accès au réseau
- Les services de Local Internet Registry du Ripe pour la mise à disposition de ressources internet indispensables au fonctionnement des opérateurs

Ces nouveaux services renforcent les services proposés aux opérateurs partenaires déjà utilisateurs de la mutualisation, en accentuant l'attractivité des points d'arrivée de ces réseaux. Les GIX et NAPs sont en effet des points d'intérêts pour les autres opérateurs locaux, mais aussi des places de marché possibles pour les opérateurs distants qui vont tendre à utiliser les NAPs pour proposer leurs services aux opérateurs locaux qui s'y sont connectés.

Initialement développé sur la boucle fibre optique mutualisée et sur les six datacentres desservis, le FR-IX s'est répliqué sur les nouveaux lieux atteints ensuite par le réseau d'Opdop. Ainsi sont nés de nouveaux NAPs à Rennes, Le Mans et début 2012, à **Marseille**. Ce qui en fait le plus gros point d'échange français en termes de points de présence.