RFC 6740 : ILNP Architectural Description

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 novembre 2012

Date de publication du RFC : Novembre 2012

https://www.bortzmeyer.org/6740.html

Le protocole ILNP vient d'être spécifié dans une série de neuf RFC, dont ce RFC 6740 [1] est le point de départ, décrivant l'architecture générale d'ILNP. ILNP appartient à la famille des protocoles à séparation de l'identificateur et du localisateur <https://www.bortzmeyer.org/separation-identificateur-localisate
html>. Ces protocoles visent à résoudre une limite fondamentale de l'Internet : l'adresse IP est utilisée à la fois comme **identificateur** (nommer une machine, par exemple pendant la durée d'une session TCP) et comme localisateur (indiquer son point d'attachement au réseau). Cette confusion rend certaines configurations, notamment le "*multi-homing*" et la mobilité, très difficiles.

Ce n'est pas qu'ILNP soit le premier protocole à vouloir séparer ces deux fonctions. Avant de donner le feu vert à la publication de ces RFC, l'IESG a notamment examiné HIP <https://www.bortzmeyer.org/hip-resume.html> et LISP <https://www.bortzmeyer.org/lisp-wg.html>, avant de conclure qu'ILNP avait des caractéristiques suffisamment originales pour qu'il soit intéressant qu'il soit décrit dans des RFC.

ILNP avait été choisi par les présidents du groupe de recherche Routage de l'IRTF comme étant la base des futurs travaux sur une meilleure architecture pour l'Internet (travaux décrits dans le RFC 6115). S'il faut le résumer en cinq points :

— ILNP est défini comme une architecture abstraite, avec plusieurs concrétisations possibles. Celle décrite dans ces RFC est compatible avec l'Internet actuel (une autre, plus « table rase », serait possible).
— ILNP fonctionne entièrement dans les machines terminales, les routeurs ne sont pas changés.
— Chaque machine ILNP a au moins un Identificateur et au moins un Localisateur. En IPv6, ils sont indiqués dans chaque paquet (ILNP peut aussi tourner au-dessus d'IPv4 mais c'est plus complexe.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6740.txt

— Pour trouver le Localisateur d'une machine qu'on veut contacter, la méthode standard est d'utiliser le DNS (ILNP repose nettement plus sur le DNS que ses concurrents).
— Les changements de localisateur en cours de session sont faits par un nouveau message ICMP, "*Locator Update*". Ces derniers sont sécurisés par un **numnique <https://www.bortzmeyer.org/nonce.html>**, nombre imprévisible envoyé au début de la session.

Bon, après cette introduction rapide, voyons tout en détail. D'abord, pourquoi veut-on à tout prix séparer identificateur et localisateur ? Le mieux est de relire le RFC 4984 pour avoir tous les détails. Disons que l'actuelle confusion de l'identificateur et du localisateur est pénible pour :

— La croissance des tables de routage : pour avoir des adresss IP stables, certains réservent du PI et l'annoncent dans la table de routage globale.
— Le "*multi-homing*" : sans adresses PI, pas de moyen facile de gérer les adresses de ses fournisseurs d'accès.
— La mobilité : changer d'endroit ou de fournisseur casse les connexions TCP en cours.

Face à ces problèmes, des tas de propositions pour améliorer les mécanismes d'adressage et de nommage dans l'Internet ont été faites : RFC 814, RFC 1498, RFC 2101, RFC 2956 et bien d'autres. La conclusion était souvent la même : le mélange de fonctions d'identification d'une machine et de sa localisation dans le réseau est une mauvaise idée. Ces fonctions devraient être séparées.

Il y a un petit problème terminologique ici : les architectures où ces fonctions sont séparées sont parfois toutes appelées « séparation de l'identificateur et du localisateur ». Mais notre RFC adopte un vocabulaire plus strict. Il réserve ce terme de « séparation de l'identificateur et du localisateur » aux architectures (comme ILNP) où la séparation est faite dès le début (dans les machines terminales) et utilise le terme de « "*map and encapsulate*" » (qu'on trouve souvent abrégé en "*map-and-encap*") aux architectures qui utilisent un tunnel pour transporter les paquets entre deux machines ne connaissant pas la séparation Identificateur/Localisateur. Selon cette terminologie, LISP `<https://www.bortzmeyer.org/lisp-wg.html>`, dont le nom veut dire "*Locator/Identifier Separation Protocol*", n'est donc pas un « vrai » système « à séparation de l'identificateur et du localisateur ».

Ce RFC, le premier à lire lorsqu'on veut comprendre ILNP, est d'abord la description d'une architecture. On n'y trouvera pas de protocole, de format des paquets, etc. Les protocoles concrets viennent après, dans d'autres RFC. Deux protocoles qui mettent en œuvre l'architecture ILNP ont été définis, ILNPv4 pour IPv4 et ILNPv6 pour IPv6. Je parlerai surtout d'ILNPv6, qui est plus simple à exposer (le faible espace d'adressage d'IPv4 a nécessité quelques astuces qui rendent ILNPv4 plus difficile à comprendre).

Comme indiqué plus haut, d'autres incarnations de l'architecture ILNP peuvent être imaginées, notamment en choisissant une approche « table rase » qui ferait tourner cette architecture sur un nouveau protocole, sans relation avec IP. Mais, pour l'instant, ces hypothétiques incarnations n'ont pas été définies.

Les autres RFC à lire, une fois celui-ci achevé, sont :

— RFC 6741, « "*ILNP Engineering and Implementation Considerations*" », qui décrit les questions concrètes communes à ILNPv4 et ILNPv6,
— RFC 6742, « "*DNS Resource Records for ILNP*" », qui explique les enregistrements DNS nécessaires pour ILNP,
— RFC 6743, « "*ICMPv6 Locator Update message*" », définit le nouveau message ICMP "*Locator Update*",
— RFC 6744, « "*IPv6 Nonce Destination Option for ILNPv6*" », normalise la nouvelle option IPv6 permettant d'indiquer le numnique de la connexion,
— RFC 6745, « "*ICMPv4 Locator Update message*" », définit le nouveau message ICMP "*Locator Update*" pour IPv4,
— RFC 6746, « "*IPv4 Options for ILNP*" », normalise deux nouvelles options IPv4, une pour indiquer le numnique de la connexion, une pour indiquer l'identificateur (pour IPv6, il tient dans l'adresse et cette option n'est pas nécessaire),

— RFC 6747, « "*ARP Extension for ILNPv4*" », qui décrit comment adapter le vieux protocole ARP à ILNP,
— RFC 6748, « "*Optional Advanced Deployment Scenarios for ILNP*" », explore des fonctions plus avancées d'ILNP et des perspectives plus lointaines.

Les section 2 et 3 détaillent cette architecture. Parmi les propriétés importantes de l'Identificateur, le fait qu'une machine puisse en avoir plusieurs, par exemple à des fins de protection de la vie privée : avoir le même Identificateur tout le temps permettrait la traque d'une machine à travers ses déplacements, un problème analogue à celui qui a mené au RFC 8981. Une machine peut donc utiliser plusieurs identificateurs (mais, évidemment, pas au sein d'une même session).

Si l'application ne se sert que de noms de domaine pour contacter son pair, elle est dite « bien élevée » et fonctionnera sans problèmes avec ILNP. Ce comportement est celui recommandé par le RFC 1958. Si, par contre, l'application utilise explicitement des adresses IP (le RFC cite les fichiers de configuration d'Apache), elle pourra avoir des ennuis avec ILNP, où ces adresses ont une sémantique différente.

Les connexions des protocoles de transport, comme TCP, utilisent uniquement l'identificateur, résistant ainsi aux changements de localisateurs. Une machine d'un site "*multi-homé*" peut ainsi basculer d'un FAI à l'autre sans casser ses connexions TCP (cf. section 3.4).

Notez bien que l'identificateur identifie une machine, pas une interface réseau. Sa sémantique est donc très différente de celle des adresses IPv4, IPv6, ou des "*Interface Identifier*" d'IPv6 (RFC 4219).

Cela ne signifie pas que l'identificateur puisse être utilisé directement par les applications clientes. Comme indiqué plus haut, il est plutôt recommandé de se servir du nom de domaine.

Dans cette architecture, qu'est-ce qui est le plus proche d'une adresse IP ? Probablement le couple {Identificateur, Localisateur}, I-LV (pour "*Identifier - Locator Vector*", cf. section 3.3). Ce couple désigne une liaison, notée (I, L), entre un identificateur et un localisateur.

Bref, un paquet ILNP contiendra un I-LV source et un I-LV destination. Notez que la sémantique d'un I-LV est proche de celle d'une adresse IP mais pas identique (l'I-LV se sépare en deux, I et L, l'adresse IP est structurée différemment, avec plusieurs préfixes hiérarchiquement emboîtés, etc). Le RFC 6741 indique comment ces IL-V sont représentés dans un paquet IP.

Dans les fichiers ou entre discussions entre humains, les identificateurs ont le format d'un "*Interface Identifier*" IPv6 (section 3.1.2). Ce format, normalisé dans le RFC 4291 est fondé sur le format EUI-64 par exemple `3a59:f9ff:fe7d:b647`. Si le bit « global » est mis à 1, l'identificateur est supposé être unique au niveau mondial.

Le localisateur a une syntaxe analogue (par exemple, `2001:db8:43a:c19`). Une machine peut aussi avoir plusieurs localisateurs (par exemple parce qu'elle a plusieurs connexions réseau). Le routage sera fait sur la base des localisateurs, comme avec IP Classique aujourd'hui (ce n'est donc pas par hasard que le localisateur ressemble à un préfixe IPv6). Le localisateur peut être modifié en route (cas du NAT). Contrairement à l'identificateur, relativement stable (en tout cas pendant la durée d'une connexion), le localisateur peut changer souvent (par exemple en situation de mobilité). Lorsque cela se produit, la machine avertit ses correspondants (CN pour "*Correspondent Nodes*") avec un message ICMP "*Locator Update*". Si elle veut être contactée (si c'est un serveur), elle doit aussi mettre à jour le DNS. Ces deux mécanismes sont décrits en détail dans le RFC 6741.

Ces identificateurs et localisateurs sont publiés dans le DNS (cf. RFC 6742). Une application qui veut contacter `www.example.com` aujourd'hui utilise le DNS pour connaître l'adresse IP correspondante. Demain, elle utilisera ILNP pour connaître identificateur et localisateur. (Pour des raisons de sécurité, DNSSEC est recommandé.)

Il est aussi précisé que l'un des buts d'ILNP est de pouvoir l'incarner dans des protocoles qui sont compatibles avec l'existant (pour permettre à ILNP et IP Classique de coexister) et déployables de manière incrémentale (ne pas exiger que tout le monde passe à ILNP d'un coup).

La section 4 explique ensuite comment se fait le routage. Alice et Bob connaissent ILNP et veulent se parler, avec, entre eux, plusieurs routeurs traditionnels ne connaissant rien à ILNP. (En terminologie ILNP, Bob est le CN - "*Correspondent Node*".) Dans le cas le plus courant, Bob a mis son (ou ses) Identificateurs et son (ou ses) Localisateurs dans le DNS (notez que les serveurs DNS utilisés n'ont pas **besoin** de connaître ILNP, mais cela optimise le temps de réponse DNS s'ils le gèrent). Cela a pu être fait manuellement ou, mieux, automatiquement via les mises à jour dynamiques (de préférence sécurisées, cf. RFC 3007). Alice va faire une requête DNS (cf. RFC 6742) et récupérer ainsi Identificateur et Localisateur de Bob (notez qu'ILNP n'a pas pour l'instant de mécanisme pour récupérer un Localisateur à partir d'un Identificateur).

Alice et Bob vont avoir besoin dans leurs systèmes d'une nouvelle structure de données, l'ILCC ("*I-L Communication Cache*", section 4.2 et RFC 6741) qui permet de se souvenir des Localisateurs actuellement en service pour un CN donné. Au début, on y met les localisateurs récupérés via le DNS.

Ensuite, en IPv6, tout est simple. Alice fabrique un paquet IPv6, contenant l'option "*Nonce*" (numnique) du RFC 6744, et dont la source est la concaténation de son Localisateur et de son Identificateur (avec les valeurs données plus haut à titre d'exemple, ce sera `2001:db8:43a:c19:3a59:f9ff:fe7d:b647`). La destination est formée en concaténant Localisateur et Identificateur de Bob. Les deux adresses ainsi fabriquées sont des adresses IPv6 tout à fait normales et les routeurs entre Alice et Bob suivent la méthode de routage, et de résolution d'adresses en local (NDP) traditionnelles.

En IPv4, cela sera toutefois plus complexe (on ne peut pas mettre Identificateur et Localisateur dans les 32 bits d'une adresse IPv4, et ARP ne permet pas de résoudre un Identificateur, trop gros pour lui). Voir les RFC 6746 et RFC 6747 pour les solutions adoptées.

Comment est-ce que cela résout le problème du "*multi-homing*", déjà cité plusieurs fois ? Comme l'explique la section 5, ILNP traite le "*Muti-homing*" en fournissant un Identificateur par machine et au moins un Localisateur par FAI. Alice utilise un des localisateurs pour le paquet initial, puis prévient Bob par un message ICMP "*Locator Update*" pour annoncer les autres. En cas de panne ou de ralentissement d'un des FAI, Bob pourra envoyer ses paquets via les autres localisateurs (l'identificateur restant inchangé).

Pour les connexions entrantes (si Alice est un serveur Web), on publiera dans le DNS tous les localisateurs et le client les essaiera tous.

"*Multi-homing*" est en fait un terme très large. Il y a plusieurs cas :

— "*Host multi-homing*" où une machine a plusieurs connexions à l'Internet. C'est relativement rare mais cela peut être, par exemple, un "*smartphone*" connecté en Wi-Fi et 3G en même temps. ILNP permet à cette machine d'utiliser les deux localisateurs, chacun issu des deux connexions possibles.

— "*Site multi-homing*" où c'est un site entier qui est connecté à plusieurs opérateurs. Le RFC cite le cas où le site a des adresses PI et les annonce en BGP (ce qui charge la table de routage globale) mais il oublie le cas où les routeurs de sortie du site font simplement du NAT vers les adresses des FAI (ce qui ne permet ni la redondance des connexions entrantes, ni la continuité des connexions TCP). Dans le scénario typique de "*site multi-homing*" avec ILNP, les routeurs du site annoncent sur le réseau local avec RA ("*Router Advertisement*") les N préfixes des N opérateurs utilisés, et les machines les utilisent comme localisateurs. Dans ce cas, les routeurs du site n'ont **pas** besoin de connaître ILNP, les machines terminales font tout le travail (enregistrer les localisateurs, les abandonner s'ils ne sont plus annoncés, etc).

Dans ILNP, la mobilité est traitée quasiment comme le "*multi-homing*" (section 6). Elle est donc très différente du "*Mobile IP*" du RFC 6275. Dans les deux cas, l'identificateur reste constant pendant que le localisateur actuellement utilisé peut changer. La principale différence est le délai : en cas de mobilité rapide, les mécanismes d'ILNP peuvent être trop lents pour assurer la transition (point que le RFC oublie de mentionner).

Comme pour le "*multi-homing*", il peut y avoir mobilité d'une machine (le "*smartphone*" cité précédemment qui, maintenant, se déplace) ou d'un réseau entier (cas d'un bateau en déplacement, par exemple, où il faudra que les machines à bord connaissent ILNP). ILNP obtient le maintien de la connectivité grâce à des localisateurs qui changent dynamiquement (même en cours de session), une mise à jour de la liste que connait le CN, grâce aux messages ICMP "*Locator Update*" et enfin les mises à jour dynamiques du DNS (RFC 2136) pour continuer à recevoir de nouvelles sessions même après déplacement.

Avec IP Classic, si le téléphone se déplace et perd la Wi-Fi, les connexions TCP en cours sont coupées. Avec ILNP, le téléphone pourra simplement utiliser le(s) localisateur(s) restant(s) (ici, celui de la 3G) et garder ses connexions.

On a vu qu'ILNP était un truc assez ambitieux, promettant de résoudre plein de problèmes. Mais, comme l'ont montré les malheurs de plusieurs protocoles, **être meilleur ne suffit pas**. L'inertie de la base installée est forte. Il faut donc absolument, pour qu'un nouveau protocole ait la moindre chance de réussir, des mécanismes de compatibilité avec l'existant et de déploiement incrémental (on ne peut pas exiger que tout le monde migre au même moment). La section 8 discute en détail ces points. D'abord, un paquet ILNPv6 ne se distingue en rien d'un paquet IPv6 actuel (c'est un peu plus compliqué avec ILNPv4, pour lequel le traditionnel ARP ne suffit pas, cf. RFC 6747). Cela veut dire que les routeurs, de la petite "*box*" au gros routeur du cœur de l'Internet n'auront besoin d'aucun changement. Le routeur ne sait même pas que le paquet est de l'ILNPv6 (voir le RFC 6741 sur les détails concrets des paquets ILNP). On est donc dans un cas très différent de celui d'IPv6 où il fallait modifier tous les routeurs situés sur le trajet.

Côté DNS, il faudra des nouveaux types d'enregistrement (RFC 6742). Cela ne nécessite pas de modifications des résolveurs/caches. Sur les serveurs faisant autorité, il faudra légèrement modifier le code pour permettre le chargement de ces nouveaux types.

Il serait tout de même souhaitable que les serveurs DNS, lorsqu'ils reçoivent une requête pour des noms qui ont des enregistrements ILNP, envoient tous ces enregistrements dans la réponse. Ce n'est pas nécessaire (le client pourra toujours les demander après) mais cela diminuera le temps total de traitement. (Les requêtes de type `ANY`, « donne-moi tous les enregistrements que tu as », ne renvoient pas forcément le résultat attendu, un cache n'ayant pas forcément tous les enregistrements correspondant à un nom.)

Si Alice et Bob connaissent tous les deux ILNP et qu'Alice initie une session avec Bob, tout se passera bien. Alice demandera l'enregistrement DNS de type `NID`, le serveur lui renverra l'identificateur de Bob, les localisateurs seront ajoutés par le serveur DNS (s'il connait ILNP) ou demandés explicitement par

Alice par la suite. Alice générera le numnique, et l'enverra à Bob avec sa demande de connexion (RFC 6744). Mais, dans une optique de déploiement incrémental, il faut prévoir le cas où Alice aura ILNP et pas Bob, ou bien l'inverse. Que se passera-t-il alors ?

Si Alice connait ILNP et pas Bob, il n'y aura pas d'enregistrement `NID` dans le DNS pour Bob. Alice devra alors reessayer avec de l'IP classique. Si un enregistrement NID était présent à tort, Alice tentera en ILNP et enverra le numnique. Bob, en recevant cette option inconnue, rejettera le paquet en envoyant un message ICMP indiquant à Alice ce qui s'est passé.

Si Alice ne connait pas ILNP alors que Bob le connait, Alice ne demandera pas le `NID` et ne tentera rien en ILNP. Si Bob accepte l'IP Classic, la connexion marchera, sans ILNP.

Vu du point de vue de Bob (qui ne connait pas les requêtes DNS qui ont été faites), la connexion est en ILNP si l'option "*Nonce*" était présente dans le paquet initial, et en IP Classic autrement.

Le RFC ne mentionne toutefois pas trois problèmes pratiques :
— Si un enregistrement DNS annonce à tort que Bob connait ILNP, Alice essaie d'abord en ILNP puis passe en IP Classic, ce qui augmentera le temps d'établissement d'une connexion.
— Plus grave, si le paquet ICMP indiquant que Bob ne connait pas ILNP est perdu ou filtré (un certain nombre de sites bloquent stupidement la totalité des messages ICMP), le délai avant qu'Alice n'essaie en IP Classic sera très long. C'est le problème connu sous le nom de « malheur des globes oculaires » (RFC 6555 et RFC 6556).
— Les options IPv6 sont très rares dans l'Internet d'aujourd'hui `<https://www.bortzmeyer.org/destination-options-ipv6.html>`. Les mauvaises expériences avec les options IPv4 `<https://www.bortzmeyer.org/options-interdites.html>` font qu'on peut être inquiet de leur viabilité.

Et la sécurité ? La section 7 couvre le cas particulier des interactions entre ILNP et IPsec (RFC 4301). La principale différence avec IP Classic est que l'association de sécurité IPsec se fait avec les identificateurs et plus avec les adresses.

Pour la sécurité d'ILNP en général, c'est la section 9 qu'il faut lire. En gros, ILNP a le même genre de risques qu'IP (on peut mentir sur son localisateur aussi facilement qu'on peut mentir sur son adresse IP) et les mêmes mesures de protection (comme IPsec).

Les "*Locator Updates*" d'ILNP, qui n'ont pas d'équivalent dans IP, sont protégés essentiellement par le numnique (RFC 6744). Sans cela, un méchant pourrait faire un faux "*Locator Update*" et rediriger tout le trafic chez lui. Avec le numnique, les attaques en aveugle sont extrêmement difficiles. Par contre, si l'attaquant peut espionner le trafic (par exemple s'il est sur le chemin de celui-ci), le numnique ne protège plus (c'est analogue au problème du numéro de séquence initial de TCP, cf. RFC 6528). Il faut alors chiffrer toute la session avec IPsec (selon le type de menaces, on peut aussi envisager SSH ou TLS). Cette situation n'est pas très différente de celle d'IP Classic.

Notez qu'il existe deux numniques par session, un dans chaque sens. Les chemins sur l'Internet étant souvent asymétriques, cela complique la tâche de l'attaquant (s'il n'est que sur un seul chemin, il ne trouvera qu'un seul numnique).

Autre attaque courante sur l'Internet (même si le RFC dit, curieusement, qu'elle existe mais n'est pas répandue), l'usurpation d'adresses. Il est facile de mentir sur son adresse IP. Peut-on mentir sur son Identificateur ou bien son Localisateur ? Disons que mentir sur son Identificateur est en effet facile et qu'on ne peut guère l'empêcher. Contrairement à HIP, ILNP n'a pas forcément de protection cryptographique de l'identificateur (cf. RFC 7343). Il est possible d'utiliser les adresses cryptographiques du RFC

3972, il reste à voir si cela sera déployé. Autre solution dans le futur, utiliser IPsec avec des clés indexées par l'identificateur (mais cela reste bien théorique).

En revanche, un mensonge sur le Localisateur est plus difficile. Il peut être protégé par les techniques du RFC 2827 et RFC 3704. Certains protocoles au-dessus, comme TCP avec ses numéros de séquence initiaux imprévisibles, ajoutent une autre protection.

Autre aspect de la sécurité, la vie privée. Comme le rappele la section 10, avoir un identificateur stable peut faciliter le suivi d'une machine (et donc de son utilisateur) même lorsqu'elle se déplace. Ce problème est connu sous le nom d'"*identity privacy*". Le problème avait déjà été mentionné avec IPv6 et la solution est la même : se servir des identificateurs temporaires du RFC 8981. (Une machine ILNP n'est **pas** forcée de n'avoir qu'un seul identificateur.)

Autre menace, celle sur la "*location privacy*". Non spécifique à ILNP, c'est le fait qu'on puisse connaître la localisation actuelle d'une machine via son localisateur. Le problème est très difficile à résoudre, la qualité de la connectivité étant inversement proportionnelle à la dissimulation de l'adresse. Si on force le passage par une machine relais fixe (comme le permet Mobile IP), on a une bonne protection de la vie privée... et une bonne chute des performances et de la résilience.

Si le localisateur a été publié dans le DNS, un indiscret qui veut le connaître n'a même pas besoin d'une communication avec la machine qu'il veut pister, interroger le DNS (qui est public) suffit. Si une machine veut rester discrète sur sa localisation et qu'elle n'a pas besoin d'être contactée, le mieux est qu'elle ne mette pas son localisateur dans le DNS.

Il n'existe encore aucune mise en œuvre publique d'ILNP. Un projet existe mais rien n'est encore sorti.

Pour les curieux d'histoire, la section 1.2 présente la vision des auteurs sur les différentes étapes ayant mené à ILNP. Ils remontent jusqu'en 1977 où la note IEN1 <http://www.postel.org/ien/pdf/ien001.pdf> notait déjà le problème qu'il y avait à faire dépendre les connexions d'une adresse qui pouvait changer. Cette note proposait déjà une séparation de l'identificateur et du localisateur, qui n'a pas eu lieu dans TCP/IP. Par exemple, TCP utilise dans la structure de données qui identifie une connexion les adresses IP de source et de destination. Tout changement d'une de ces adresses (par exemple parce que la machine a bougé) casse les connexions TCP en cours.

Après ce choix, et quelques années plus tard, l'idée d'une séparation de l'identificateur et du localisateur est revenue, compte-tenu de l'expérience avec TCP/IP. En 1994, une note de Bob Smart (en ligne sur https://www.bortzmeyer.org/files/bob-smart-sipp-1994.txt) repropose cette idée. Même chose en 1995 avec Dave Clark <ftp://ftp.parc.xerox.com/pub/lixia/address/ddc.address.txt>. Enfin, en 1996, Mike O'Dell propose son fameux 8+8 <http://datatracker.ietf.org/doc/draft-odell-8+8/>, qui n'atteindra jamais le statut de RFC mais reste la référence historique des propositions de séparation de l'identificateur et du localisateur. (Une grosse différence entre 8+8 et ILNP est que ce dernier n'impose pas de réécriture du localisateur en cours de route).

Depuis, plusieurs autres travaux ont été faits en ce sens, mais sans déboucher sur beaucoup de déploiements. Des « vrais » protocoles de séparation de l'identificateur et du localisateur (rappelons que les auteurs ne considèrent pas LISP <https://www.bortzmeyer.org/lisp-wg.html> comme faisant partie de cette catégorie), seul HIP <https://www.bortzmeyer.org/hip-resume.html> a connu une description dans un RFC et plusieurs mises en œuvres. ILNP offre sans doute moins de sécurité que HIP (contrairement à HIP, pas besoin d'établir une connexion avant toute communication) mais autant qu'avec l'IP actuel. Et ILNP est moins disruptif que HIP, ce qui peut être vu comme un avantage ou un inconvénient.

Quelques lectures :

— Un excellent exposé à NANOG <http://www.cs.st-andrews.ac.uk/~saleem/talks/2010/ilnp_nanog50/2010-10-03-ilnp_nanog50-v4_final.pdf>, qui explique notamment bien la différence entre localisateur et identificateur.
— Un texte plus ancien, décrivant ILNP <http://www0.cs.ucl.ac.uk/research/researchnotes/documents/RN_05_22.pdf>.
— Et bien sûr le site officiel <http://ilnp.cs.st-andrews.ac.uk/>.