IPv8 : Qu'est-ce que c'est et pourquoi l'IETF veut-il ressusciter IPv4 ?

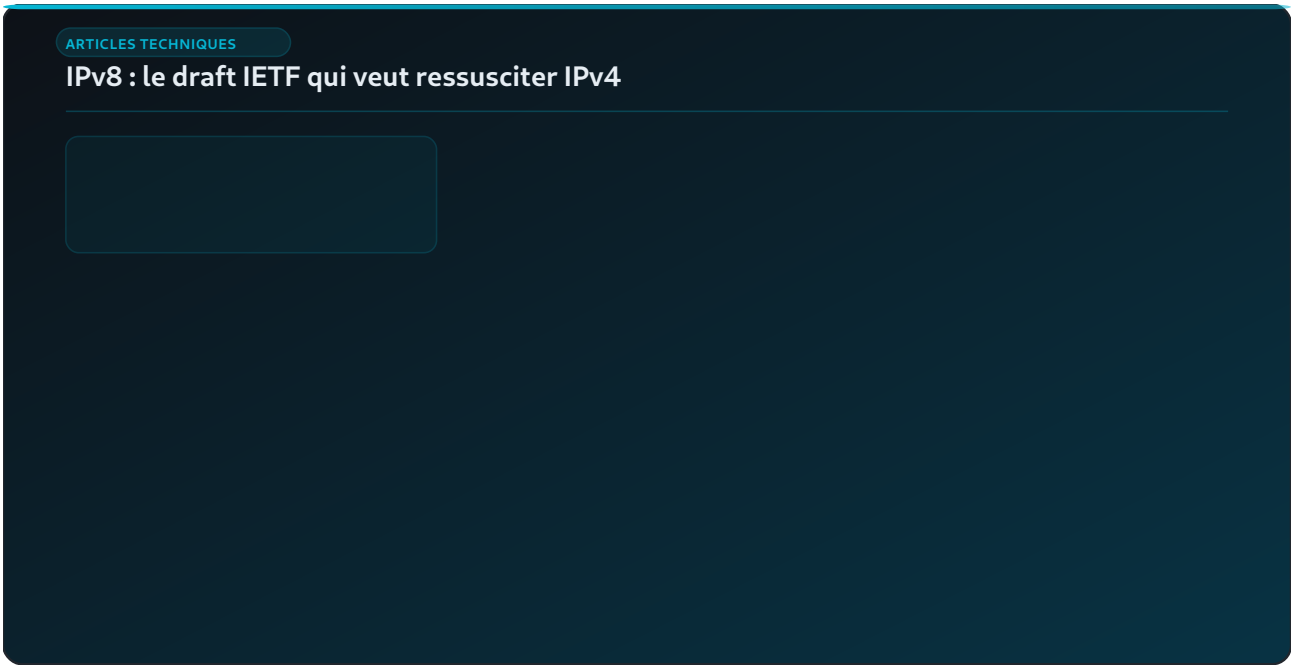
IPv8 est un draft IETF proposant une extension 64 bits d'IPv4 pour simplifier la transition réseau. Analyse technique, enjeux sécurité et impact pour les...

IPv8 n'est pas encore dans les manuels scolaires, ni dans les certifications Cisco ou les formations de l'ANSSI — et pourtant, ce draft soumis à l'IETF en avril 2026 fait parler de lui dans les cercles d'ingénierie réseau. À l'heure où IPv6, déployé depuis plus de vingt ans, peine encore à dépasser 45 % d'adoption mondiale selon les chiffres APNIC, un ingénieur nommé James Thain a eu l'audace de proposer une troisième voie. IPv8 se présente comme une extension 64 bits d'IPv4, rétrocompatible avec l'existant, sans dual-stack imposé, sans renumérotation massive, et avec une infrastructure réseau centralisée qui absorbe DHCP, DNS, NTP et authentification Zero Trust en un seul bloc. L'idée est provocatrice, controversée, peut-être satirique selon certains membres de la communauté IETF — mais elle met le doigt sur une réalité inconfortable que beaucoup d'équipes réseau vivent au quotidien : la migration vers IPv6 est douloureuse, coûteuse, et loin d'être achevée. Dans cet article, nous décortiquons IPv8 sous toutes ses coutures : ce qu'il est techniquement, comment il se positionne face à IPv6, pourquoi il suscite autant de scepticisme, et ce que les responsables de la sécurité réseau en France devraient en retenir dans le contexte NIS 2 et des recommandations ANSSI.

Points clés à retenir

- La virtualisation avec Proxmox VE offre un rapport performance/coût imbattable
- Le hardening de l'hyperviseur est un prérequis à tout déploiement en production

• Les snapshots et sauvegardes immutables constituent le filet de sécurité essentiel



Pour comprendre pourquoi IPv8 fait autant de bruit, il faut d'abord revenir sur l'échec relatif — ou du moins la lenteur spectaculaire — de la transition vers IPv6. RFC 2460 a défini IPv6 en décembre 1998. Près de trois décennies plus tard, le constat est sévère : l'adoption mondiale reste fragmentée et géographiquement inégale.

⚡ **Retour terrain**

Dans les projets techniques complexes, j'ai appris à toujours commencer par auditer la documentation existante plutôt que l'infrastructure elle-même. Dans 80 % des cas, le delta entre la documentation et la réalité est la source première de risques. Une infrastructure

bien documentée qui ne correspond pas à la réalité est plus dangereuse qu'une infrastructure sans documentation — parce qu'elle induit une fausse confiance.

Selon les données APNIC (Asia-Pacific Network Information Centre) de mai 2026, environ 45 % du trafic mondial est acheminé via IPv6 — mais ce chiffre masque des disparités énormes. L'Inde dépasse les 70 % d'adoption grâce aux déploiements massifs de Jio, les États-Unis oscillent autour de 55 %, tandis que la France plafonne aux environs de 38 %. Les chiffres RIPE NCC pour l'Europe indiquent que seulement 30 % des Autonomous Systems (AS) européens annoncent des préfixes IPv6 actifs. Du côté de l'ARIN (pour l'Amérique du Nord), l'épuisement des blocs IPv4 a été officiellement déclaré en 2015, mais le marché secondaire des adresses IPv4 continue de prospérer — une adresse IPv4 se négocie encore entre 40 et 60 dollars l'unité en 2026.

Pourquoi IPv6 peine-t-il autant à s'imposer ? Plusieurs facteurs structurels expliquent cette résistance :

La rétrocompatibilité nulle : IPv6 n'est pas rétrocompatible avec IPv4. Les deux protocoles ne peuvent pas communiquer directement, ce qui force le déploiement en dual-stack (faire tourner les deux simultanément), consommateur de ressources et complexe à gérer.

Le confort du NAT : La traduction d'adresses réseau (NAT) a permis de prolonger artificiellement la vie d'IPv4 en permettant à des milliers d'équipements de partager une seule adresse publique. Les équipes réseau se sont adaptées à cette réalité, et beaucoup ne voient pas d'urgence à migrer.

Le coût de la renumérotation : Migrer un parc d'équipements vers IPv6 impose une renumérotation complète, la mise à jour des règles de firewall, des ACL, des configurations BGP, des politiques de routage et des outils de supervision. Pour une grande entreprise ou un opérateur télécom, le coût peut atteindre plusieurs millions d'euros.

La formation des équipes : Les ingénieurs réseau formés sur IPv4 doivent réapprendre une syntaxe d'adressage radicalement différente (128 bits en hexadécimal), de nouveaux protocoles de découverte (NDP en remplacement d'ARP), et des mécanismes de configuration automatique (SLAAC) peu intuitifs.

C'est précisément dans cette impasse que James Thain a introduit son draft le 14 avril 2026 : `draft-thain-ipv8-00`. La promesse ? Garder ce qui fonctionne dans IPv4, étendre l'espace d'adressage sans tout casser, et intégrer nativement la sécurité Zero Trust.

Qu'est-ce qu'IPv8 exactement ? Le draft IETF décrypté

IPv8 est un Internet-Draft soumis à l'IETF (Internet Engineering Task Force) par l'ingénieur James Thain le 14 avril 2026. Le document porte la référence `draft-thain-ipv8-00`. À ce stade, il ne s'agit que d'un working draft — une proposition de travail, pas un RFC (Request for Comments) officiel, et encore moins un standard adopté.

L'IETF publie régulièrement des Internet-Drafts qui peuvent être le point de départ d'un futur standard ou simplement rester sans suite. La majorité des drafts n'atteignent jamais le statut de RFC. Cela dit, même les proposals rejetées ou controversées jouent un rôle utile : elles ouvrent des débats, documentent des problèmes, et parfois influencent les standards futurs de manière indirecte.

Le nom "IPv8" peut sembler étrange — pourquoi sauter de 4 à 8, et que sont devenus IPv5, IPv6 et IPv7 ? En réalité :

IPv5 : c'était le Stream Protocol (ST-II), un protocole expérimental des années 1990 pour la transmission de flux en temps réel, jamais standardisé publiquement.

IPv6 : le successeur officiel d'IPv4, adopté par le RFC 2460 en 1998.

IPv7 : un numéro réservé pour des usages internes IETF, jamais attribué à un protocole public.

IPv8 : le numéro choisi par Thain pour sa proposition, sans lien formel avec les versions précédentes.

Le principe fondateur d'IPv8 tient en une phrase clé du draft : *"IPv4 is a subset of IPv8. An IPv8 address with the routing prefix field set to zero is an IPv4 address."* Cette assertion est la clé de voûte de toute l'architecture proposée.

Comment IPv8 fonctionne-t-il techniquement ?

L'architecture d'adressage IPv8 repose sur une extension 64 bits structurée en deux champs de 32 bits :

```
 +------------------+------------------+
|  Routing Prefix  |   Host Address   |
|   (32 bits)      |   (32 bits)      |
+------------------+------------------+
  = Numéro d'AS       = Adresse IPv4
```

Le champ **Routing Prefix** (32 bits) correspond au numéro d'Autonomous System (AS). Les AS sont les blocs de routage fondamentaux d'internet — chaque opérateur télécom, chaque grande entreprise dispose d'un ou plusieurs numéros d'AS attribués par les RIR (Regional Internet Registries : RIPE NCC, ARIN, APNIC, etc.). En utilisant le numéro d'AS comme préfixe de routage, IPv8 crée un espace d'adressage de 2^64 adresses — soit environ 18,4 quintillions d'adresses, contre 4,3 milliards pour IPv4 et 340 undécillions pour IPv6.

Le champ **Host Address** (32 bits) conserve intégralement la syntaxe des adresses IPv4 actuelles. C'est là que réside la promesse de rétrocompatibilité : un équipement IPv4 standard, avec son adresse 192.168.1.10, peut être représenté dans IPv8 comme `0:192.168.1.10` (préfixe AS à zéro). Un équipement pleinement IPv8 dans l'AS 12345 et avec l'adresse hôte 10.0.0.1 aurait l'adresse `12345:10.0.0.1`.

Le Zone Server : un service réseau centralisé

L'un des aspects les plus audacieux — et les plus controversés — d'IPv8 est la proposition du **Zone Server**. Plutôt que de maintenir des services réseau distincts (DHCP, DNS, NTP, authentification), le Zone Server consolide tout en un seul composant déployé en cluster actif/actif :

DHCP8 : attribution dynamique d'adresses IPv8

DNS8 : résolution de noms adaptée aux adresses 64 bits

NTP8 : synchronisation temporelle intégrée

NetLog8 : journalisation réseau native

OAuth8 : authentification Zero Trust basée sur JWT

XLATE8 : translation entre IPv4 et IPv8 pour la compatibilité

L'authentification Zero Trust via OAuth8 mérite une attention particulière. Le draft propose une validation locale des tokens JWT, sans dépendance vis-à-vis d'un Identity Provider (IdP) externe. Concrètement, chaque connexion réseau serait authentifiée cryptographiquement au niveau de la couche réseau elle-même — une intégration native de ce que des solutions comme Zero Trust Network cherchent à accomplir par des couches applicatives superposées.

Le mécanisme de translation XLATE8

Pour la transition, IPv8 propose XLATE8 : un mécanisme de translation d'adresses permettant à des équipements IPv4 existants de communiquer avec des équipements IPv8 sans modification. XLATE8 fonctionne au niveau des passerelles réseau, de manière analogue au NAT64 utilisé aujourd'hui pour faire cohabiter IPv4 et IPv6 — mais avec une compatibilité binaire directe puisque l'adresse IPv4 est littéralement intégrée dans l'adresse IPv8.

IPv8 vs IPv6 : comparaison technique

Voici une comparaison synthétique des deux protocoles sur les critères les plus importants pour les équipes réseau et sécurité :

Critère	IPv6	IPv8 (proposé)
Longueur d'adresse	128 bits	64 bits
Espace d'adressage	~3,4 × 10^38	~1,8 × 10^19
Rétrocompatibilité IPv4	Non (dual-stack requis)	Oui (IPv4 = cas particulier)
Migration	Renumérotation complète	Extension progressive
Dual-stack obligatoire	Oui (phase de transition)	Non
Sécurité native (IPsec)	Oui (obligatoire en RFC 6434)	JWT/OAuth8 (proposition)
Configuration automatique	SLAAC / DHCPv6	DHCP8 (via Zone Server)
Résolution de noms	DNS avec enregistrements AAAA	DNS8 (intégré Zone Server)
Statut standardisation	RFC 8200 (2017)	Draft-00 (2026, non officiel)
Adoption réelle	~45 % trafic mondial	0 % (expérimental)
Support équipements	Natif sur tous OS modernes	Aucun à ce jour
NAT nécessaire	Non (en théorie)	Non (en théorie)

Ce tableau illustre le paradoxe d'IPv8 : sur le papier, certains avantages sont réels (rétrocompatibilité, migration douce), mais l'absence totale d'implémentation et le statut embryonnaire du draft le placent à des années-lumière d'IPv6 en termes de maturité opérationnelle.

Les arguments pour IPv8 : ce que la proposition a de séduisant

Malgré les critiques, IPv8 soulève des arguments qui méritent d'être pris au sérieux, au moins comme exercice intellectuel sur les limites d'IPv6.

La rétrocompatibilité comme avantage majeur

L'argument le plus solide d'IPv8 est sa rétrocompatibilité structurelle avec IPv4. En intégrant l'adresse IPv4 comme champ de 32 bits dans la structure même de l'adresse IPv8, la migration n'implique pas de renumérotation. Un équipement IPv4 existant reste addressable sans

modification — son adresse est simplement préfixée de zéro dans le nouveau schéma. Pour les grandes organisations disposant de centaines de milliers d'équipements documentés et inventoriés, l'absence de renumérotation représente une économie considérable.

Pas de dual-stack imposé

Le dual-stack IPv4/IPv6 est l'une des principales sources de complexité dans les déploiements actuels. Faire fonctionner deux piles réseau simultanément double la surface d'attaque, multiplie les configurations à maintenir, et crée des problèmes de performance (happy eyeballs, fallback automatique). IPv8, en étant nativement compatible IPv4, évite cette phase de transition douloureuse.

Un espace d'adressage suffisant

Avec 2^64 adresses, IPv8 offre un espace théoriquement suffisant pour l'internet des objets prévisible. L'argument selon lequel IPv6 avec ses 128 bits est "trop grand" est certes discutable, mais la gestion d'adresses 64 bits reste plus simple humainement que 128 bits — les numéros d'AS actuels sont familiers aux ingénieurs réseau, et les adresses IPv4 hôtes le sont encore davantage.

L'intégration Zero Trust native

L'authentification OAuth8 basée sur JWT au niveau de la couche réseau est conceptuellement intéressante. Aujourd'hui, le Zero Trust est principalement implémenté en surcouche applicative (ZTNA, Cloudflare Access, etc.). Une intégration native dans la couche réseau pourrait simplifier l'architecture de sécurité, réduire les dépendances et améliorer les performances. Sur ce point, IPv8 anticipe une tendance réelle.

Les arguments contre IPv8 et le scepticisme de la communauté IETF

Les critiques sont nombreuses, et certaines sont fondamentales. La communauté IETF n'a pas accueilli le draft avec enthousiasme, plusieurs membres ayant qualifié le document de non-sérieux sur les listes de diffusion.

Un espace d'adressage insuffisant à long terme

2^64 adresses, c'est beaucoup — mais c'est aussi potentiellement insuffisant à très long terme. Avec l'explosion de l'IoT (on parle de 75 à 100 milliards d'objets connectés d'ici 2030 selon Ericsson et IDC), les prévisions les plus conservatrices indiquent que même 2^64 adresses pourraient être épuisées dans les décennies à venir si chaque objet nécessite une adresse routeable publique. IPv6 avec 2^128 adresses élimine ce problème pour des siècles.

Le numéro d'AS comme préfixe de routage : une fausse bonne idée

L'utilisation du numéro d'AS comme préfixe de routage soulève de sérieuses questions d'ingénierie. Les numéros d'AS ne sont pas hiérarchiques — ils sont attribués par les RIR de manière pseudo-aléatoire selon la disponibilité, sans logique géographique ou topologique. Une structure d'adressage basée sur les AS serait donc aussi peu agrégeable que les préfixes IPv4 actuels, avec un risque de croissance incontrôlée des tables de routage BGP. Or, l'une des promesses d'IPv6 est justement une meilleure agrégabilité des préfixes.

Zéro implémentation, zéro adoption

Un protocole réseau n'existe que s'il est implémenté. À ce jour, aucun système d'exploitation, aucun équipement réseau, aucun chipset ne supporte IPv8. Créer un écosystème complet (noyaux OS, drivers, firmware, outils de diagnostic, sondes de supervision, règles de firewall) prend des années et mobilise des ressources colossales. IPv6 a nécessité 20 ans pour atteindre 45 % d'adoption — et il bénéficiait du soutien des grands constructeurs dès le départ.

La nature potentiellement satirique du draft

Plusieurs membres influents de la communauté IETF ont mis en doute le sérieux du draft sur les listes de diffusion. La proposition du Zone Server — un super-service centralisant DHCP, DNS, NTP, journalisation et authentification — va à l'encontre des principes fondateurs d'internet, qui reposent sur la décentralisation et la séparation des responsabilités. Cette centralisation crée un point de défaillance unique (SPOF) massif, incompatible avec la résilience requise pour une infrastructure critique.

IPv6 résout déjà les problèmes qu'IPv8 prétend résoudre

Les mécanismes de transition NAT64, 464XLAT, et les tunnels 6to4 permettent déjà à des équipements IPv4 de communiquer dans un réseau IPv6. Ce n'est pas parfait, mais c'est opérationnel et déployé à grande échelle. L'argument de la rétrocompatibilité d'IPv8 perd donc de sa substance face à la réalité des outils de transition IPv6 existants.

Enjeux pour la sécurité réseau : NAT, firewalls et surface d'attaque

Pour les RSSI et les équipes sécurité, IPv8 — ou plus généralement tout changement de protocole réseau fondamental — soulève des questions critiques qui méritent une analyse rigoureuse.

La disparition du NAT : une arme à double tranchant

IPv8, comme IPv6, supprime en théorie le besoin du NAT. Si cela simplifie la connectivité de bout en bout et élimine les problèmes de translation, cela expose aussi directement chaque équipement sur internet. Le NAT, bien qu'il ne soit pas un mécanisme de sécurité au sens strict, a toujours joué un rôle de filtre implicite — un équipement derrière NAT n'est pas directement routable depuis l'extérieur. Dans un monde IPv8 sans NAT, chaque objet connecté aurait une

adresse globalement unique et potentiellement routable, ce qui augmente mécaniquement la surface d'attaque.

Les bonnes pratiques de sécurité DNS et réseau deviennent d'autant plus critiques dans ce contexte : la sécurisation périmétrique par filtrage d'adresses ne suffit plus, et les architectures Zero Trust deviennent incontournables.

Reconfiguration des firewalls et ACL

L'adoption d'IPv8 (si elle devait se produire) imposerait une refonte complète des règles de firewall. Les règles basées sur des plages d'adresses IPv4 deviendraient obsolètes. Les ACL sur les routeurs, les règles iptables/nftables sur les serveurs Linux, les politiques de sécurité sur les firewalls NGF (Next-Generation Firewall) — tout devrait être repensé pour intégrer la nouvelle structure d'adressage 64 bits. Sur Linux, cela impliquerait par exemple des modifications au niveau du noyau et des outils réseau :

```
 # Exemple hypothétique de configuration IPv8 sous Linux
# (non implémenté - à titre illustratif)
ip addr add 12345:192.168.1.10 dev eth0
ip route add 12345:10.0.0.0/8 via 12345:192.168.1.1

# Vérification du protocole actif
sysctl net.ipv4.conf.all.forwarding
sysctl net.ipv6.conf.all.forwarding
# Un futur : sysctl net.ipv8.conf.all.forwarding
```

Impact sur les outils de supervision et SIEM

Les outils de détection d'intrusion (IDS/IPS), les SIEM, et les sondes réseau sont tous conçus pour analyser des flux IPv4 ou IPv6. L'introduction d'un nouveau protocole de couche 3 imposerait une mise à jour complète des signatures, des parsers de logs, et des règles de corrélation. Pour les équipes SOC, la période de transition serait une fenêtre de vulnérabilité significative — les attaquants qui maîtriseraient le nouveau protocole avant que les outils défensifs ne soient mis à jour auraient un avantage tactique réel.

L'authentification JWT/OAuth8 : une promesse sous conditions

L'intégration native de l'authentification Zero Trust via JWT dans la couche réseau est séduisante sur le papier. Mais elle soulève aussi des questions de gouvernance : qui émet les certificats ? Comment gère-t-on la révocation en cas de compromission ? Quelle PKI (Public Key Infrastructure) sous-jacente ? Les tokens JWT ont une surface d'attaque connue (injection, replay attacks, algorithme none), et leur intégration dans la couche réseau elle-même nécessiterait des garanties de sécurité extrêmement robustes.

Impact sur les professionnels IT en France : NIS 2 et recommandations ANSSI

Dans le contexte réglementaire français et européen, l'émergence d'un nouveau protocole réseau — même expérimental — n'est pas sans implications pour les équipes IT et les responsables de la conformité.

NIS 2 et la gestion des protocoles réseau

La directive NIS 2 (Network and Information Security), transposée en droit français et opérationnelle depuis 2024, impose aux entités essentielles et importantes une gestion rigoureuse de leur infrastructure réseau. L'article 21 de NIS 2 exige notamment des mesures de sécurité pour la gestion des actifs, la sécurité des réseaux et des systèmes d'information, et le contrôle des accès. Dans ce cadre, tout changement de protocole réseau fondamental doit faire l'objet d'une analyse de risques formelle et d'une mise à jour du SMSI (Système de Management de la Sécurité de l'Information).

Pour les entités soumises à NIS 2 en phase opérationnelle 2026, l'émergence d'IPv8 — même à l'état de draft — est un signal qu'il faut surveiller. Les cartographies réseau, les inventaires d'actifs et les plans de gestion des changements doivent intégrer une veille sur les évolutions protocolaires.

Les recommandations ANSSI sur l'IPv6 restent d'actualité

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a publié le guide "Sécurisation des réseaux IPv6" (référence PA-022) qui détaille les bonnes pratiques pour déployer IPv6 en sécurité. À ce jour, aucune recommandation ANSSI ne porte sur IPv8 — logique pour un draft sans implémentation. Mais le guide IPv6 de l'ANSSI reste pertinent pour contextualiser les enjeux : la transition protocolaire est une période à risque qui exige une planification méticuleuse, des tests en environnement isolé, et une formation des équipes avant tout déploiement en production.

Ce que les RSSI doivent faire dès maintenant

Concrètement, pour les RSSI français en 2026, IPv8 n'impose aucune action immédiate. Mais il invite à réfléchir à plusieurs points structurels :

Auditer l'état d'avancement de la migration IPv6 : si votre organisation est encore en IPv4 pur, l'adoption d'IPv6 reste la priorité absolue, conformément aux recommandations ANSSI et aux exigences NIS 2.

Mettre en place une veille protocolaire : intégrer la surveillance des Internet-Drafts IETF dans votre veille technologique. Des proposals comme IPv8 peuvent préfigurer des évolutions importantes ou au contraire révéler des angles morts dans la communauté réseau.

Documenter les dépendances protocolaires : inventorier quels équipements, applications et services dépendent d'adresses IP codées en dur. Cette documentation sera indispensable pour toute future migration, quelle que soit la direction (IPv6 ou autre).

Évaluer les outils de sécurité sur IPv6 : avant de s'interroger sur IPv8, s'assurer que les firewalls, IDS, SIEM et outils de supervision gèrent correctement le trafic IPv6. Beaucoup d'organisations ont des angles morts IPv6 dans leurs défenses.

Conclusion et perspectives 2026-2030

IPv8, tel que proposé dans le draft `draft-thain-ipv8-00`, est une idée intellectuellement stimulante qui pointe des problèmes réels — mais qui n'est pas une réponse sérieuse à ces problèmes en l'état. La rétrocompatibilité avec IPv4 est séduisante, l'intégration Zero Trust native est visionnaire, et la critique implicite de la lenteur d'adoption d'IPv6 est légitime. Mais zéro implémentation, une communauté IETF sceptique, une centralisation problématique dans le Zone Server, et un espace d'adressage de deuxième ordre par rapport à IPv6 font d'IPv8 davantage un catalyseur de débat qu'une alternative crédible à court terme.

D'ici 2030, plusieurs scénarios sont envisageables pour le paysage protocolaire réseau :

Scénario 1 — Victoire progressive d'IPv6 : L'adoption mondiale d'IPv6 continue sa progression (actuellement 45 %, potentiellement 70-80 % d'ici 2030 grâce aux déploiements 5G et IoT). IPv8 reste une curiosité historique.

Scénario 2 — Émergence d'une voie hybride : Des mécanismes inspirés d'IPv8 (intégration Zero Trust native, simplification de la transition) sont intégrés dans des RFC complémentaires à IPv6, sans nécessiter un nouveau protocole complet.

Scénario 3 — Fragmentation protocolaire : Des réseaux privés et des régions géographiques adoptent des protocoles propriétaires ou non-standards, fragmentant davantage l'internet. C'est un scénario pessimiste mais non impossible dans le contexte de la souveraineté numérique.

Pour les équipes réseau et sécurité françaises, le message est clair : IPv8 n'est pas une priorité opérationnelle aujourd'hui. La priorité reste la migration IPv6 et la mise en conformité NIS 2. Mais le débat qu'IPv8 suscite est une opportunité utile pour remettre à plat les choix d'architecture réseau, évaluer la maturité des outils de sécurité face aux protocoles modernes, et préparer les équipes à un paysage technologique en mutation continue.

Qu'est-ce qu'IPv8 et en quoi diffère-t-il d'IPv6 ?

IPv8 est un Internet-Draft IETF soumis en avril 2026 par James Thain, proposant un protocole réseau 64 bits qui étend IPv4 tout en conservant sa rétrocompatibilité. Contrairement à IPv6 (128 bits, incompatible avec IPv4), IPv8 intègre l'adresse IPv4 comme sous-ensemble de sa structure d'adressage. Une adresse IPv8 est composée d'un préfixe de routage (numéro d'AS, 32 bits) et d'une adresse hôte (adresse IPv4 existante, 32 bits). IPv6 reste plus mature, plus adopté et dispose d'un espace d'adressage nettement supérieur.

IPv8 va-t-il remplacer IPv6 dans les prochaines années ?

Non, pas dans un avenir prévisible. IPv8 est à ce jour un simple working draft sans implémentation dans aucun système d'exploitation ou équipement réseau. La communauté IETF a accueilli la proposition avec scepticisme. IPv6, malgré sa lenteur d'adoption, bénéficie de vingt ans de développement, d'un support natif sur tous les OS modernes, et d'une adoption croissante. Aucune organisation sérieuse ne devrait envisager de déployer IPv8 en production à court ou moyen terme.

Quels sont les risques de sécurité liés à un changement de protocole réseau ?

Tout changement de protocole réseau fondamental crée une fenêtre de vulnérabilité. Les firewalls, IDS/IPS, SIEM et outils de supervision doivent être mis à jour pour reconnaître et analyser le nouveau protocole. Pendant la transition, des angles morts peuvent exister — le trafic dans le nouveau protocole peut circuler sans être correctement filtré ni journalisé. De plus, la suppression du NAT (comme le proposent IPv6 et IPv8) expose directement chaque équipement sur internet, augmentant la surface d'attaque et rendant les architectures Zero Trust indispensables.

À RETENIR

Points clés à retenir

Contexte : la guerre IPv4 vs IPv6, vingt ans d'une transition inachevée

Qu'est-ce qu'IPv8 exactement ? Le draft IETF décrypté

Comment IPv8 fonctionne-t-il techniquement ?

IPv8 vs IPv6 : comparaison technique

Les arguments pour IPv8 : ce que la proposition a de séduisant

Comment les entreprises françaises doivent-elles se préparer aux évolutions protocolaires réseau ?

Les entreprises françaises, particulièrement celles soumises à NIS 2, doivent d'abord s'assurer que leur migration IPv6 est planifiée et en cours d'exécution, conformément aux recommandations ANSSI. Sur le plan stratégique, il est recommandé de mettre en place une veille sur les Internet-Drafts IETF, d'auditer régulièrement la couverture des outils de sécurité sur les protocoles modernes (notamment IPv6), de documenter toutes les dépendances protocolaires dans les cartographies réseau, et de former les équipes aux nouvelles architectures Zero Trust qui deviennent incontournables quelle que soit la direction protocolaire choisie.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

