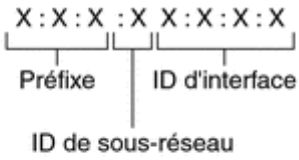
EVALUATION SEMESTRE 2 – BLOC 2

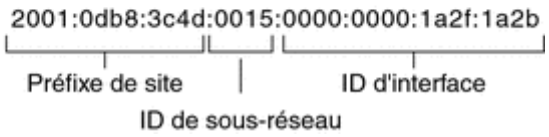
1. IP V6

1.1 Taille d'une adresse IP V6

- Une adresse IPV6 est composée de 128 bits, soit 16 octets. Elle est représentée en notation hexadécimale avec des séparateurs de deux points (:),
- Exemple : 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Cette taille est beaucoup plus grande que celle d'une adresse IPV4 qui est composée de 32 bits (4 octets).



Exemple :



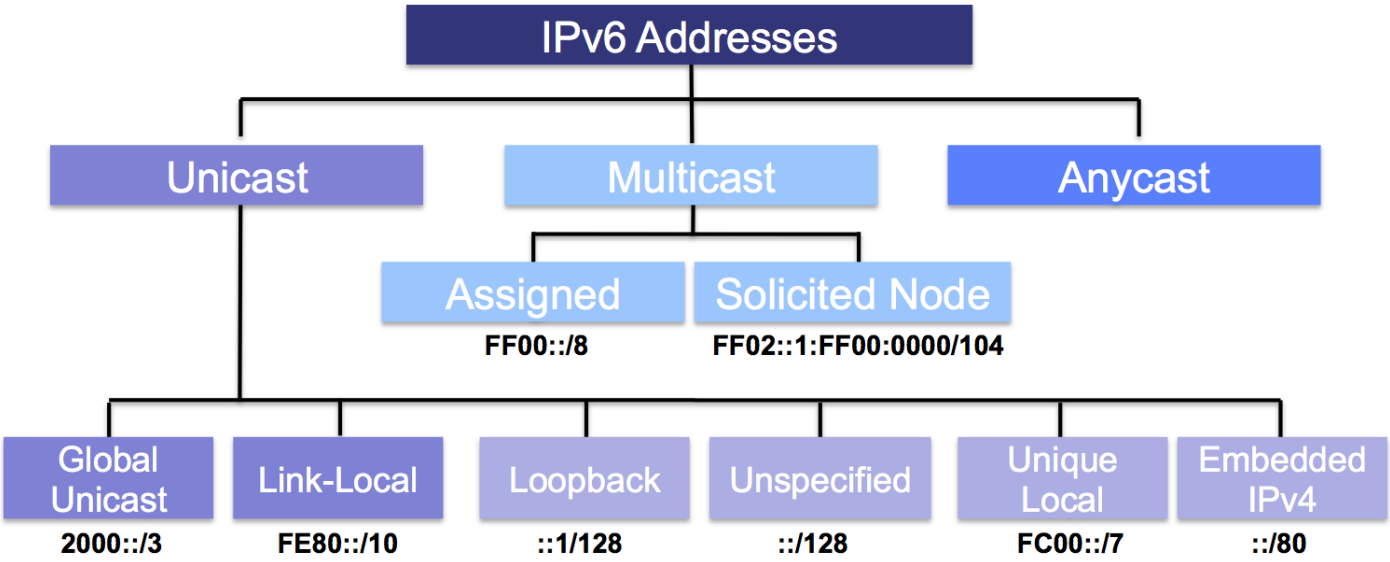
1.2. Dans quelle partie de l'adresse peut-on mettre les sous réseaux

- Dans une adresse IPV6, les sous-réseaux sont identifiés par un préfixe de sous-réseau qui est placé dans les bits les plus significatifs de l'adresse. Le préfixe de sous-réseau est utilisé pour diviser le réseau en sous-réseaux plus petits et pour identifier les adresses de chaque sous-réseau.
- Le préfixe de sous-réseau est représenté sous la forme d'une notation CIDR (Classless Inter-Domain Routing), qui indique le nombre de bits utilisés pour identifier le sous-réseau. Par exemple, si un préfixe de sous-réseau de 64 bits est utilisé, les 64 premiers bits de l'adresse sont réservés pour identifier le réseau et les 64 bits restants sont utilisés pour identifier les adresses de chaque hôte dans le sous-réseau.
- Le préfixe de sous-réseau peut être écrit directement après l'adresse IP, séparé par un slash (/). Par exemple, l'adresse IP suivante identifie un réseau avec un préfixe de sous-réseau de 64 bits : 2001:0db8:85a3:0000:0000:8a2e:0370:7334/64

<table>
<tr><td colspan="2">Préfixe de routage</td><td>Identifiant d'interface (Interface ID)</td></tr>
<tr><td>2001:0620:0000</td><td>:0000</td><td rowspan="3">:0211:24FF:FE80:C12C</td></tr>
<tr><td>Préfixe de réseau / Topologie publique</td><td>Préfixe sous-réseau / Topologie du site</td></tr>
<tr><td>48 bits</td><td>16 bits</td></tr>
<tr><td colspan="2">64 bits</td><td>64 bits</td></tr>
<tr><td colspan="2">Le préfixe caractérise le réseau ou sous-réseau</td><td>L'ID d'interface caractérise un appareil donné avec une carte réseau au sein d'un réseau.</td></tr>
</table>

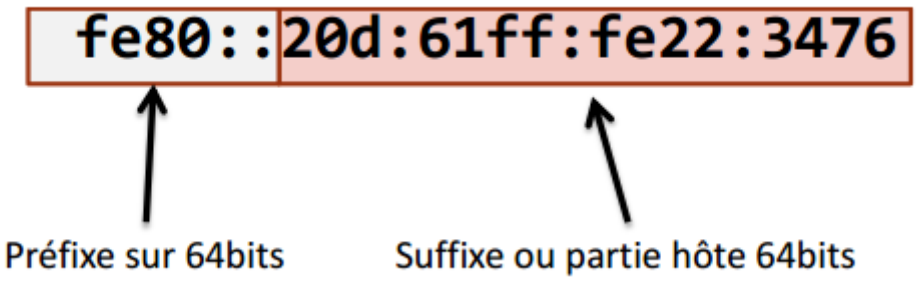
1.3. Que représente les 3 1ers bits

- Dans une adresse IPV6, les trois premiers bits représentent le type d'adresse. Ces trois bits sont appelés les "flags de format" (ou Format Prefix en anglais) et indiquent le format et le type d'adresse. Il existe trois types d'adresses IPV6 :
- Les adresses unicast : elles identifient une interface unique sur le réseau. Les trois premiers bits d'une adresse unicast sont 001.
- Les adresses multicast : elles identifient un groupe d'interfaces sur le réseau. Les trois premiers bits d'une adresse multicast sont 111.
- Les adresses anycast : elles identifient un groupe d'interfaces, mais les paquets envoyés à cette adresse sont livrés à l'interface la plus proche ou la plus appropriée du groupe. Les trois premiers bits d'une adresse anycast sont 011.
- Ainsi, en analysant les trois premiers bits d'une adresse IPV6, on peut déterminer le type d'adresse et savoir si elle identifie une interface unique, un groupe d'interfaces ou une adresse anycast.



1.4. De quelle taille est la partie hôte

- Dans une adresse IPv6, la partie hôte est généralement de taille 64 bits. Les adresses IPv6 sont composées de 128 bits au total, dont les 64 premiers bits représentent l'identificateur de préfixe de réseau et les 64 derniers bits représentent l'identificateur d'interface, qui est la partie hôte. Cela permet à chaque interface d'un réseau IPv6 d'avoir une adresse unique et permanente. Cependant, il est important de noter que certaines adresses IPv6 peuvent avoir une partie hôte de taille différente en fonction de la configuration de l'adresse.



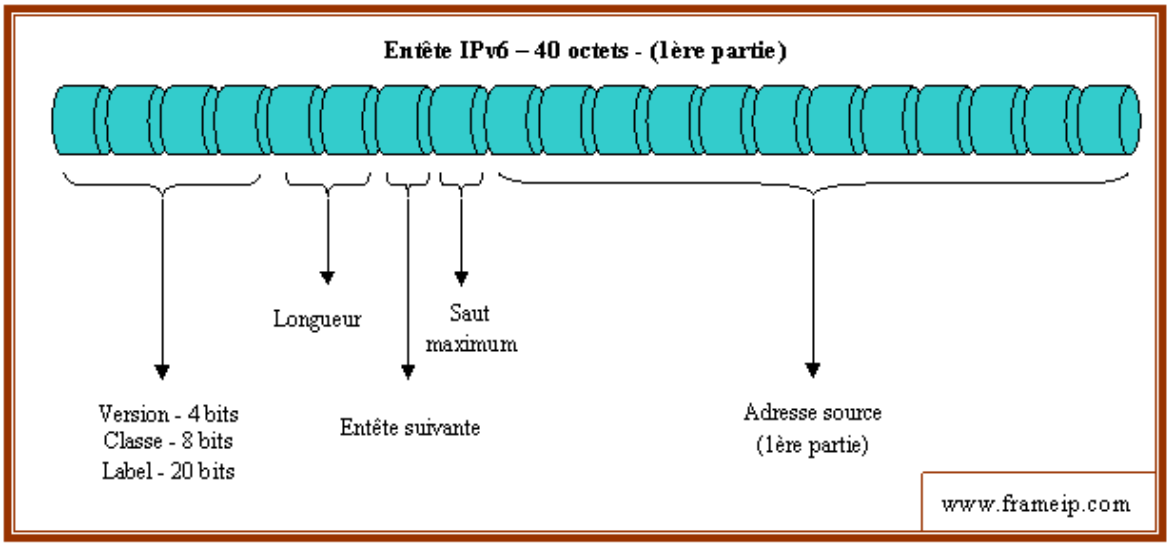
1.5. Est-ce un adressage plat ou hiérarchique ?

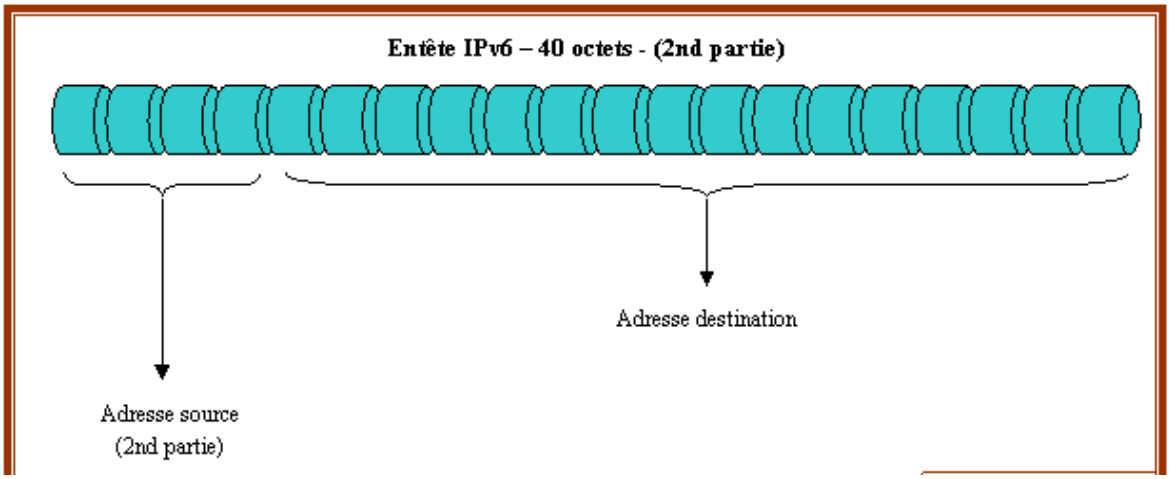
- Une adresse IPv6 est un adressage hiérarchique. Elle utilise une structure de préfixe de réseau qui permet de diviser l'espace d'adressage IPv6 en plusieurs sous-réseaux plus petits. Le préfixe de réseau est généralement fourni par un fournisseur d'accès Internet (FAI) ou une autre organisation qui contrôle une partie de l'espace d'adressage IPv6.
- L'adressage IPv6 hiérarchique permet une meilleure gestion et allocation des adresses IPv6, ainsi qu'une meilleure routabilité des paquets sur Internet. En effet, cette structure permet de router les paquets de manière efficace en les envoyant uniquement aux routeurs qui sont sur le chemin le plus court vers la destination, plutôt que de les envoyer à tous les routeurs sur Internet.

1.6. La taille de l'en tete est-elle variable ?

- Oui, la taille de l'en-tête IPv6 est fixe à 40 octets. Contrairement à IPv4 qui peut avoir une taille d'en-tête variable, IPv6 a une taille d'en-tête fixe pour simplifier le traitement et l'acheminement des paquets IPv6.
- Cependant, IPv6 utilise des extensions d'en-tête optionnelles qui peuvent être ajoutées après l'en-tête de base de 40 octets pour fournir des fonctionnalités supplémentaires telles que le routage, la fragmentation, la sécurité, etc. Ces extensions d'en-tête optionnelles peuvent être ajoutées ou supprimées en fonction des besoins, ce qui peut augmenter la taille totale de l'en-tête IPv6.

Voici la structure de l'entête IPv6 basé sur 40 octets.

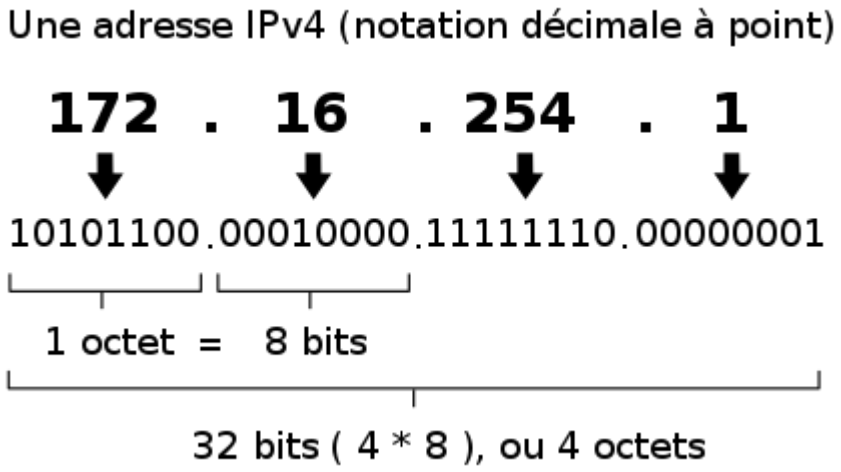




2. Idem pour IP V4

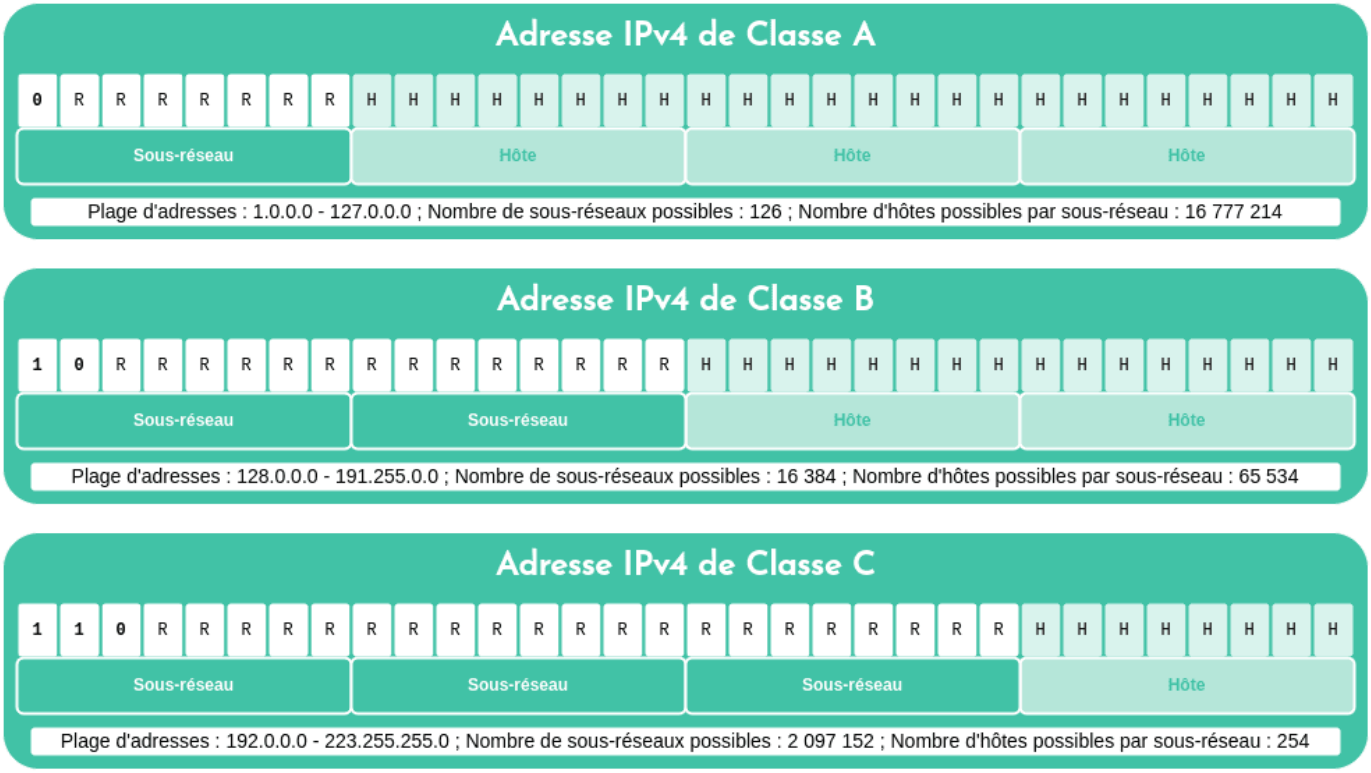
2.1. Taille d'une adresse IPV4

- Une adresse IPv4 est composée de 32 bits, soit 4 octets. Elle est généralement représentée sous forme de quatre nombres décimaux séparés par des points, chacun des nombres étant compris entre 0 et 255. Par exemple, 192.168.0.1 est une adresse IPv4 couramment utilisée pour les réseaux locaux.
- Avec 32 bits, l'espace d'adressage IPv4 est limité à 2^32 adresses, soit un peu plus de 4 milliards d'adresses uniques. Cela signifie que l'espace d'adressage IPv4 est presque épuisé, et c'est pourquoi une nouvelle version du protocole, IPv6, a été développée pour offrir un espace d'adressage plus grand et répondre aux besoins croissants de l'Internet.



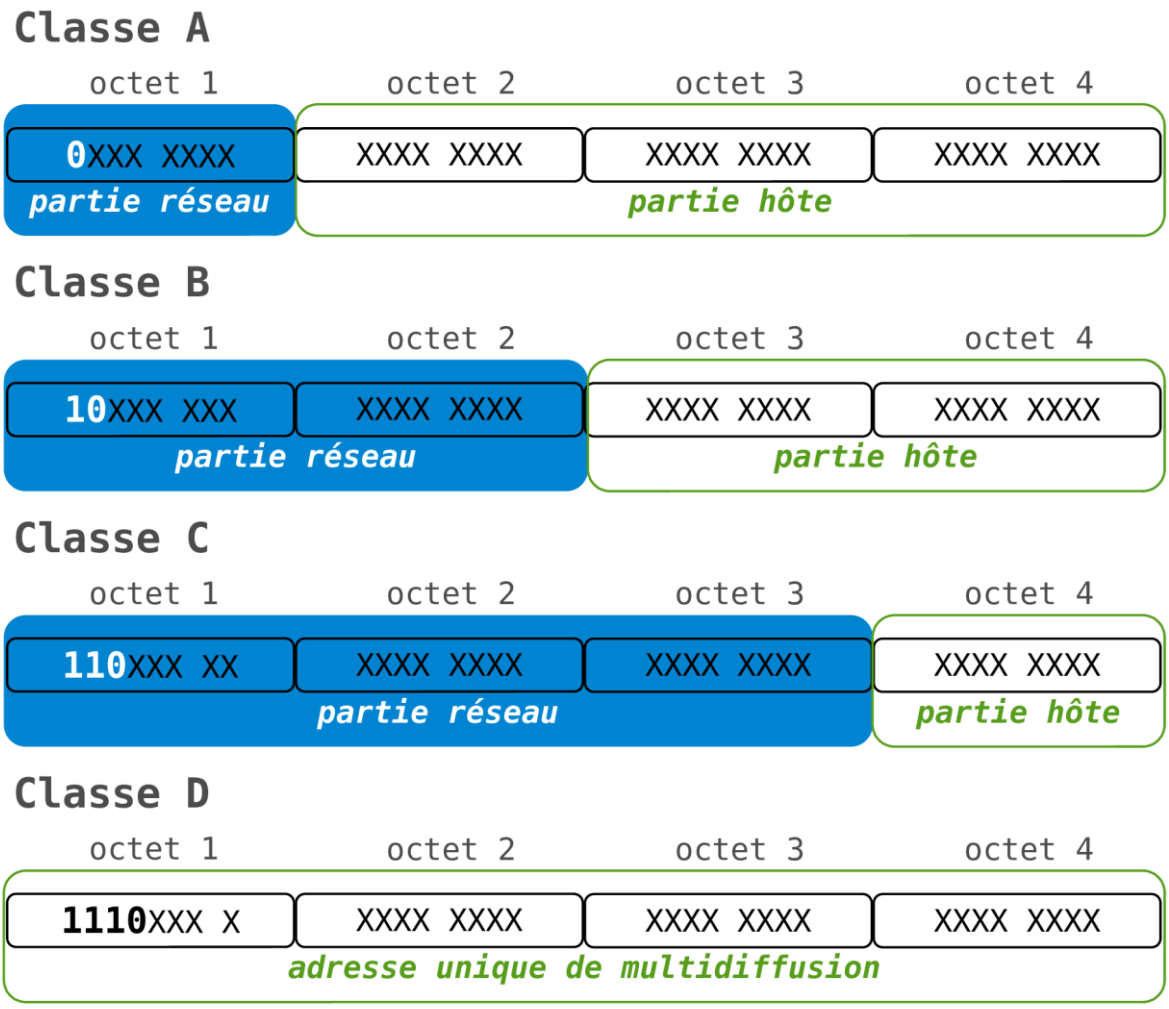
2.2. Dans quelle partie de l'adresse peut-on mettre les sous réseaux

- Dans une adresse IPv4, les sous-réseaux sont identifiés en utilisant des bits de l'adresse IP qui sont réservés à cet effet. Les bits qui identifient les sous-réseaux sont situés dans la partie de l'adresse IP appelée "masque de sous-réseau".
- Le masque de sous-réseau est une valeur binaire qui indique quelles parties de l'adresse IP sont réservées pour identifier le sous-réseau et quelles parties sont réservées pour identifier l'hôte. Le masque de sous-réseau est souvent représenté sous forme de notation décimale avec un préfixe CIDR (Classless Inter-Domain Routing), qui indique le nombre de bits réservés pour le sous-réseau. Par exemple, un masque de sous-réseau /24 indique que les 24 premiers bits sont réservés pour identifier le sous-réseau, tandis que les 8 derniers bits sont réservés pour identifier l'hôte.
- En résumé, les sous-réseaux dans une adresse IPv4 sont identifiés en utilisant des bits réservés dans le masque de sous-réseau, qui permettent de diviser l'espace d'adressage IPv4 en plusieurs sous-réseaux plus petits.



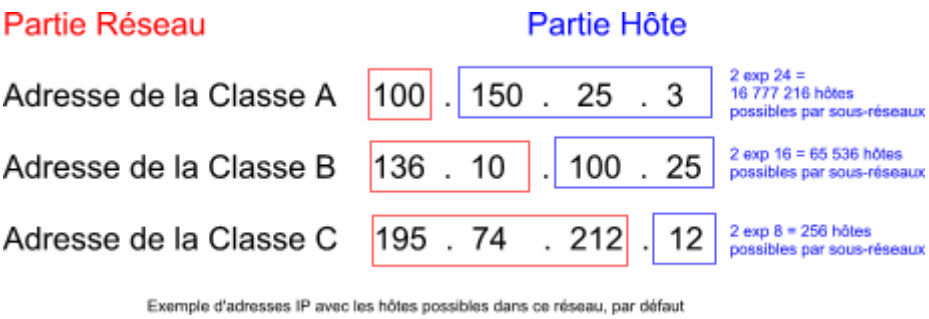
2.3. Que représente les 3 1ers bits

- Dans une adresse IPv4, les trois premiers bits sont utilisés pour identifier la classe de l'adresse IP. Il existe cinq classes d'adresses IPv4, identifiées par les trois premiers bits de l'adresse IP :
- Classe A : Les adresses IP de classe A ont un premier bit à 0. Les 7 bits suivants identifient le réseau, et les 24 bits restants identifient l'hôte. Les adresses de classe A vont de 0.0.0.0 à 127.255.255.255, ce qui donne un total de 128 réseaux de classe A.
- Classe B : Les adresses IP de classe B ont les deux premiers bits à 10. Les 14 bits suivants identifient le réseau, et les 16 bits restants identifient l'hôte. Les adresses de classe B vont de 128.0.0.0 à 191.255.255.255, ce qui donne un total de 16 384 réseaux de classe B.
- Classe C : Les adresses IP de classe C ont les trois premiers bits à 110. Les 21 bits suivants identifient le réseau, et les 8 bits restants identifient l'hôte. Les adresses de classe C vont de 192.0.0.0 à 223.255.255.255, ce qui donne un total de 2 097 152 réseaux de classe C.
- Classe D : Les adresses IP de classe D, ont les quatre premiers bits à 1110. Elles sont réservées pour la diffusion multicast, c'est-à-dire pour envoyer un paquet à un groupe de destinataires.
- Classe E : Les adresses IP de classe E ont les quatre premiers bits à 1111. Elles sont réservées pour des usages expérimentaux et ne sont pas utilisées en production.
- Il est important de noter que la classification des adresses IP par classe n'est plus utilisée aujourd'hui. Le système de notation CIDR (Classless Inter-Domain Routing) est maintenant utilisé pour permettre une gestion plus flexible de l'espace d'adressage IPv4.



2.4. De quelle taille est la partie hôte

- Dans une adresse IPv4, la partie hôte est déterminée par la classe d'adresse IP à laquelle elle appartient. La partie hôte est la partie de l'adresse IP qui identifie un périphérique spécifique sur un réseau donné.
- Voici la taille de la partie hôte pour chaque classe d'adresse IPv4 :
- Classe A : La partie hôte est composée de 24 bits, ce qui permet d'identifier jusqu'à 16 777 214 hôtes sur un réseau donné.
- Classe B : La partie hôte est composée de 16 bits, ce qui permet d'identifier jusqu'à 65 534 hôtes sur un réseau donné.
- Classe C : La partie hôte est composée de 8 bits, ce qui permet d'identifier jusqu'à 254 hôtes sur un réseau donné.
- Classes D et E : Les adresses IP de classe D et E sont réservées à des usages spécifiques et n'ont pas de partie hôte.
- Cependant, il est important de noter que ces classes d'adresses ne sont plus utilisées dans la gestion actuelle de l'espace d'adressage IPv4. Le système de notation CIDR (Classless Inter-Domain Routing) est maintenant utilisé pour permettre une gestion plus flexible de l'espace d'adressage IPv4, et la taille de la partie hôte peut varier en fonction du masque de sous-réseau utilisé.



2.5. Est-ce une adresse hiérarchique ou plat ?

- L'adresse IPv4 est divisée en classes d'adresses, qui déterminent la taille de l'adresse du réseau et la taille de l'adresse de l'hôte. Les classes d'adresses permettent également de déterminer le nombre maximal de sous-réseaux et d'hôtes qu'un réseau peut avoir.
- En outre, le système de notation CIDR (Classless Inter-Domain Routing) permet une gestion plus flexible de l'espace d'adressage IPv4. CIDR permet de diviser un réseau en plusieurs sous-réseaux, en utilisant un masque de sous-réseau pour déterminer la taille de l'adresse du réseau et la taille de l'adresse de l'hôte.
- En conclusion, l'adressage IPv4 est hiérarchique, ce qui permet une gestion efficace des adresses IP et une organisation logique du réseau.

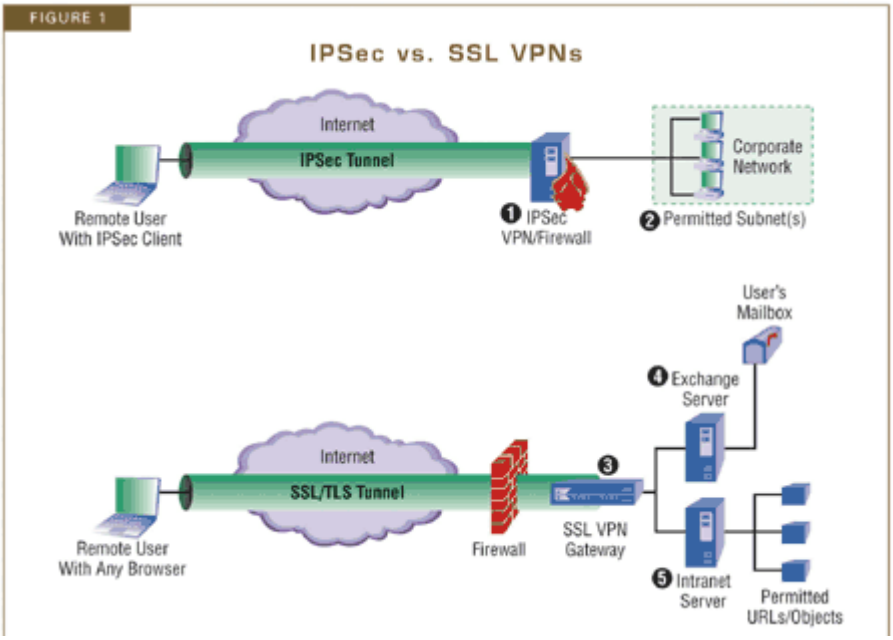
2.6. La taille de l'en tête est-elle variable ?

- La taille de l'en-tête d'un paquet IPv4 est fixe et a une taille de 20 octets, sauf dans certains cas où des options sont ajoutées à l'en-tête. Dans ce cas, la taille totale de l'en-tête peut être variable, allant jusqu'à un maximum de 60 octets.
- L'en-tête IPv4 contient des informations importantes telles que l'adresse source et l'adresse de destination, ainsi que des informations sur le type de protocole utilisé, la longueur du paquet, le nombre de sauts (time-to-live), et des options éventuelles.
- La taille de l'en-tête IPv4 fixe de 20 octets est composée de différentes parties telles que le champ Version, le champ Header Length, le champ Type of Service, le champ Total Length, le champ Identification, le champ Flags, le champ Fragment Offset, le champ Time to Live, le champ Protocol, le champ Header Checksum, l'adresse IP source, l'adresse IP de destination, et éventuellement des options.
- En résumé, la taille de l'en-tête IPv4 est généralement fixe à 20 octets, sauf si des options sont ajoutées, auquel cas la taille totale de l'en-tête peut varier jusqu'à un maximum de 60 octets.

3. VPN

3.1. Différence IP Sec et SSL ?

- IPsec (Internet Protocol Security) et SSL (Secure Sockets Layer) sont deux protocoles différents utilisés pour fournir des connexions sécurisées sur Internet. Bien qu'ils offrent tous les deux des fonctionnalités de sécurité pour les connexions en ligne, ils diffèrent sur plusieurs points.
- Voici les principales différences entre les protocoles VPN IPsec et SSL :
- Type de sécurité : IPsec utilise une sécurité de niveau réseau, tandis que SSL utilise une sécurité de niveau application.
- Mode de fonctionnement : IPsec peut fonctionner en mode transport et tunnel, tandis que SSL ne fonctionne qu'en mode tunnel.
- Configuration : IPsec nécessite une configuration plus complexe, tandis que SSL est plus facile à configurer.
- Performance : IPsec peut être plus rapide en raison de sa nature de niveau réseau, tandis que SSL peut ralentir les performances en raison de sa nature de niveau application.
- Compatibilité : IPsec est généralement pris en charge sur les routeurs et les pare-feux, tandis que SSL est souvent pris en charge par les navigateurs web et les applications de bureau.
- Utilisation : IPsec est souvent utilisé pour les connexions VPN entre les réseaux d'entreprise, tandis que SSL est souvent utilisé pour les connexions de site à site et les connexions de clients à serveur.
- En résumé, IPsec et SSL sont deux protocoles différents utilisés pour sécuriser les connexions en ligne. IPsec utilise une sécurité de niveau réseau, est plus complexe à configurer et est souvent utilisé pour les connexions VPN entre les réseaux d'entreprise, tandis que SSL utilise une sécurité de niveau application, est plus facile à configurer et est souvent utilisé pour les connexions de site à site et les connexions de clients à serveur.



3.1.1. En termes de protocole de chiffrement

- Les protocoles VPN IPsec et SSL utilisent des méthodes de chiffrement différentes pour assurer la sécurité des données lorsqu'elles sont transmises sur Internet.
- Le protocole IPsec utilise des algorithmes de chiffrement tels que AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) et SHA (Secure Hash Algorithm) pour assurer la confidentialité, l'intégrité et l'authenticité des données. Il peut également utiliser des protocoles de clé publique tels que IKE (Internet Key Exchange) pour établir des connexions VPN sécurisées.

- Le protocole SSL utilise également des algorithmes de chiffrement tels que AES et RSA (Rivest–Shamir–Adleman) pour assurer la sécurité des données. SSL est généralement utilisé pour sécuriser les connexions de site à site et les connexions de clients à serveur, telles que les connexions HTTPS (HyperText Transfer Protocol Secure) utilisées pour sécuriser les transactions bancaires en ligne, les connexions de messagerie électronique sécurisées, etc.
- En termes de sécurité, IPsec est considéré comme plus sûr que SSL car il utilise une sécurité de niveau réseau, tandis que SSL utilise une sécurité de niveau application. Cependant, SSL est souvent plus facile à configurer et à utiliser que IPsec.
- En fin de compte, le choix entre IPsec et SSL dépendra des besoins spécifiques de l'utilisateur en termes de sécurité, de performance et de compatibilité avec les équipements réseau existants.

3.1.2. De type d'utilisation

- Les VPN (Virtual Private Networks) utilisent des protocoles de sécurité tels que IPsec et SSL pour créer des connexions sécurisées entre des appareils distants via Internet.
- Le VPN IPsec est souvent utilisé pour créer des connexions VPN site à site ou client à site entre des réseaux d'entreprise. Cela permet aux employés distants de se connecter au réseau de l'entreprise depuis n'importe où dans le monde, tout en bénéficiant d'une sécurité renforcée pour leurs communications. IPsec peut également être utilisé pour connecter des réseaux de succursales entre eux, créant ainsi un réseau privé virtuel étendu.
- Le VPN SSL est souvent utilisé pour créer des connexions VPN de type client à site. Cela permet aux utilisateurs individuels de se connecter à un réseau distant depuis n'importe quel appareil avec un navigateur web, sans nécessiter de logiciel supplémentaire. Les connexions SSL sont souvent utilisées pour accéder à des ressources distantes, telles que des applications web, des fichiers partagés et des bases de données.
- En résumé, IPsec est souvent utilisé pour les connexions VPN site à site ou client à site entre des réseaux d'entreprise, tandis que SSL est souvent utilisé pour les connexions VPN de type client à site pour permettre aux utilisateurs individuels d'accéder à des ressources distantes. Le choix entre IPsec et SSL dépendra des besoins spécifiques de l'utilisateur en termes de sécurité, de performance et de compatibilité avec les équipements réseau existants.

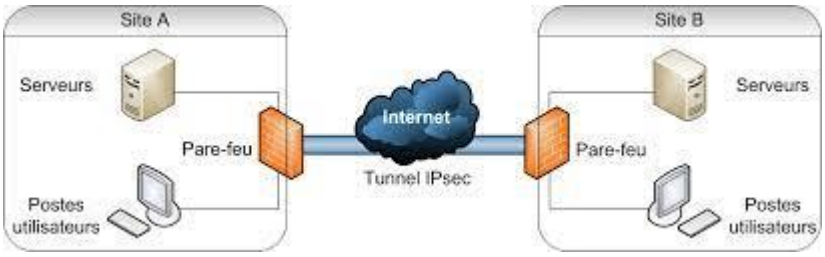


Figure 1: VPN IPSEC

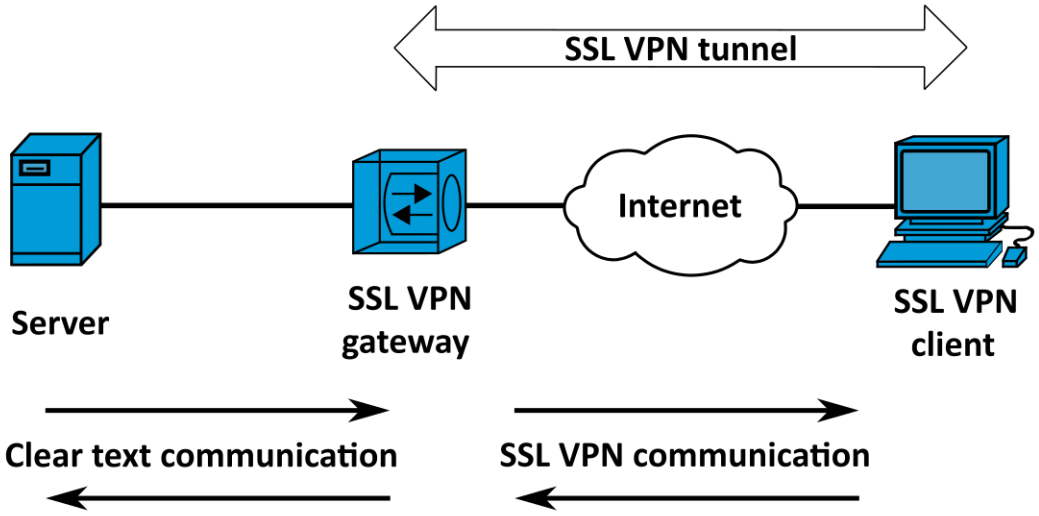


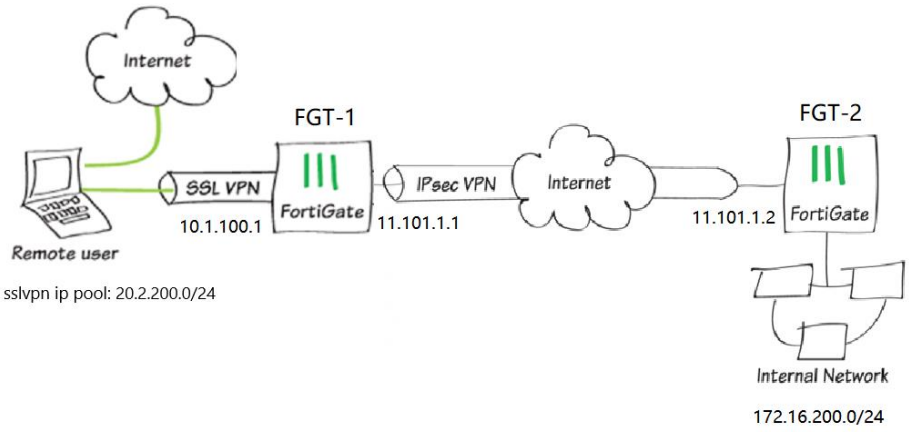
Figure 2: VPN SSL

3.2. De facilité de mise en œuvre

- En termes de facilité de mise en œuvre, SSL est généralement considéré comme plus facile à configurer et à utiliser que IPsec.
- Le protocole SSL est intégré dans la plupart des navigateurs web modernes, ce qui signifie que les utilisateurs peuvent se connecter à un réseau distant via une interface web sans avoir besoin de télécharger ou d'installer de logiciel supplémentaire. Cela rend les connexions SSL très faciles à utiliser pour les utilisateurs finaux.
- Le protocole IPsec, en revanche, peut-être plus complexe à configurer et à déployer, en particulier pour les connexions site à site qui nécessitent une configuration et une gestion plus avancées. Cependant, de nombreuses solutions VPN commerciales proposent des options de configuration et de gestion simplifiées pour faciliter la mise en œuvre de VPN IPsec.
- En fin de compte, la facilité de mise en œuvre dépendra des besoins spécifiques de l'utilisateur et des solutions VPN choisies. Cependant, dans l'ensemble, SSL est généralement considéré comme plus facile à configurer et à utiliser que IPsec.

3.3. Peut-on mettre les 2 en même temps

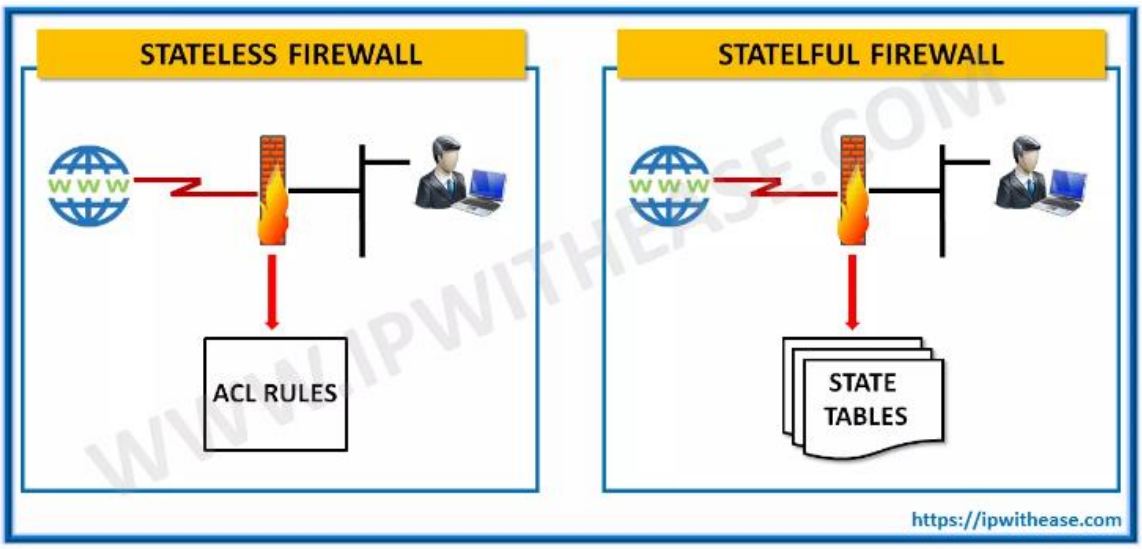
- Oui, il est possible de mettre en place une architecture VPN qui utilise à la fois IPsec et SSL.
- Cela peut être réalisé en utilisant une solution de passerelle de sécurité qui prend en charge les deux protocoles. Par exemple, une passerelle de sécurité peut être configurée pour accepter les connexions VPN SSL entrantes et sortantes, tout en offrant également la possibilité de créer des tunnels VPN IPsec pour les connexions site à site ou client à site.
- L'utilisation de plusieurs protocoles VPN peut offrir des avantages en termes de flexibilité et de sécurité. Par exemple, les connexions VPN SSL peuvent être utilisées pour offrir une accessibilité facile et rapide aux ressources distantes via un navigateur web, tandis que les connexions VPN IPsec peuvent offrir une sécurité renforcée pour les connexions site à site ou client à site qui nécessitent une protection supplémentaire.
- Cependant, l'utilisation de plusieurs protocoles VPN peut également être plus complexe à gérer et à configurer, en particulier pour les entreprises ayant des besoins de sécurité élevés. Il est donc important de bien comprendre les besoins spécifiques de l'entreprise et de choisir les protocoles VPN appropriés en fonction de ces besoins.



4. Infra

4.1. Qu'est-ce qu'un pare feu Statefull

- Un pare-feu statefull, également appelé pare-feu de couche 4, est un type de pare-feu qui surveille l'état des connexions réseau en gardant une trace des sessions de connexion actives.
- Contrairement aux pare-feu de couche 3 qui se concentrent uniquement sur l'adresse IP et le port, un pare-feu statefull est capable de surveiller le trafic de la couche 4 (transport) du modèle OSI, qui inclut des informations telles que les numéros de séquence et d'acquittement TCP, les identificateurs de session UDP et d'autres informations de contrôle de connexion.
- Cela permet au pare-feu statefull de vérifier si les paquets entrants ou sortants font partie d'une session de connexion établie ou autorisée, ce qui permet de mieux protéger le réseau contre les attaques malveillantes telles que les attaques par déni de service (DoS) et les attaques par rebond.
- En outre, les pare-feux stateful sont également capables de bloquer les paquets qui ne sont pas conformes aux règles de sécurité définies pour une session de connexion, tout en autorisant le trafic légitime à travers le pare-feu.
- En somme, un pare-feu statefull offre une sécurité renforcée pour les connexions réseau en surveillant l'état des connexions et en appliquant des règles de sécurité spécifiques pour chaque session de connexion.



4.2. Qu'est-ce qu'OSPF

- OSPF (Open Shortest Path First) est un protocole de routage de type Link-State utiliser pour acheminer des paquets dans un réseau de plusieurs routeurs.

- Il fonctionne en créant une base de données topologique du réseau et en calculant le chemin le plus court pour atteindre une destination à partir de chaque nœud. Contrairement aux protocoles de routage à vecteur de distance comme RIP (Routing Information Protocol), OSPF échange des informations topologiques entre les routeurs en utilisant des paquets Link-State Advertisement (LSA).
- Les routeurs OSPF communiquent en utilisant un identifiant de routeur unique (Router ID) et forment des adjacences avec les autres routeurs du réseau. Les adjacences sont établies en échangeant des paquets Hello, qui permettent de découvrir les routeurs voisins, et en synchronisant les bases de données topologiques.
- Une fois que les routeurs ont créé une carte topologique du réseau, OSPF calcule le chemin le plus court pour atteindre une destination en utilisant l'algorithme SPF (Shortest Path First). L'algorithme SPF est utilisé pour calculer la distance entre les routeurs en fonction du coût des liens, puis pour déterminer le chemin le plus court pour atteindre chaque destination.
- En résumé, OSPF est un protocole de routage Link-State qui permet aux routeurs de construire une carte topologique du réseau et de calculer le chemin le plus court pour atteindre une destination à partir de chaque nœud.

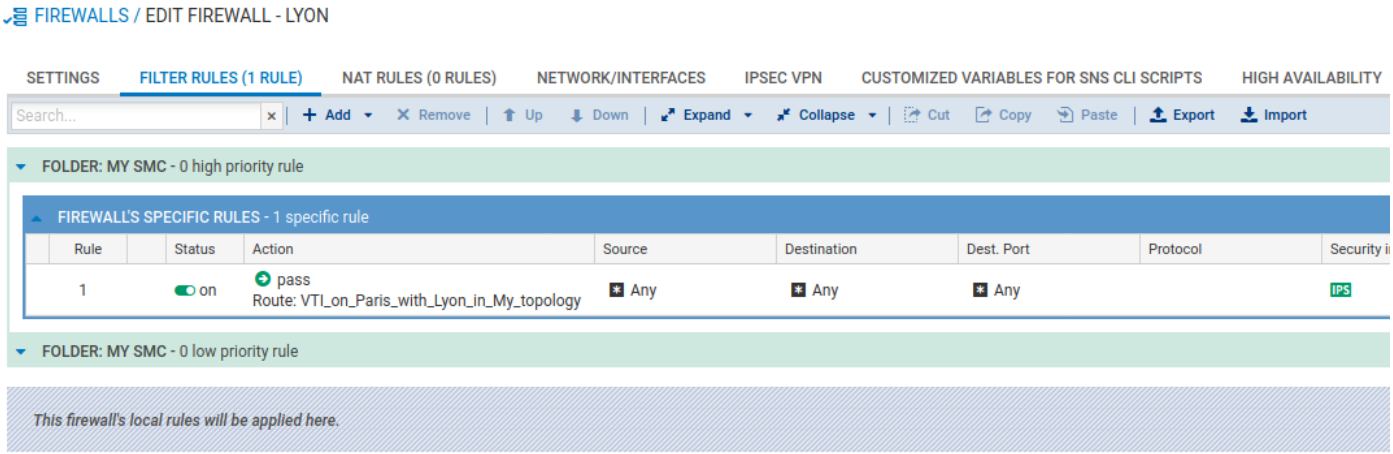
4.3. Quelle est la différence avec RIP

- La principale différence entre OSPF et RIP est la façon dont ils calculent les chemins de routage.
- RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance qui utilise le nombre de sauts (nombre de routeurs intermédiaires) pour déterminer le chemin optimal entre deux destinations. RIP n'utilise qu'une seule métrique pour déterminer la distance entre les routeurs, qui est le nombre de sauts, et ne prend pas en compte d'autres facteurs tels que la bande passante ou la charge du lien.
- En revanche, OSPF est un protocole de routage Link-State qui utilise une base de données topologique pour calculer le chemin le plus court entre deux destinations. OSPF prend en compte plusieurs facteurs pour calculer la distance entre les routeurs, y compris la bande passante, la charge du lien, le coût de la liaison, etc.
- Une autre différence importante entre les deux protocoles est leur gestion des mises à jour de routage. RIP envoie des mises à jour de routage périodiques à tous les routeurs du réseau, même si rien n'a changé dans la topologie du réseau. En revanche, OSPF n'envoie des mises à jour de routage que lorsqu'il y a un changement dans la topologie du réseau, ce qui réduit le trafic de routage et améliore l'efficacité du réseau.
- En somme, la principale différence entre OSPF et RIP est que OSPF utilise une approche Link-State plus sophistiquée pour calculer les chemins de routage, tandis que RIP utilise une approche à vecteur de distance plus simple. De plus, OSPF a une gestion plus efficace des mises à jour de routage que RIP.

4.4. Qu’est-ce qu’une politique par routage ?

- Une politique de routage est un ensemble de règles et de procédures qui déterminent comment le trafic réseau doit être acheminé à travers le réseau en fonction de critères tels que la destination, l'origine, le type de service, la bande passante, la sécurité, etc.
- Les politiques de routage peuvent être utilisées pour optimiser les performances du réseau, garantir la qualité de service, améliorer la sécurité, contrôler le flux de trafic et réduire les coûts de connectivité.
- Par exemple, une entreprise peut avoir une politique de routage qui spécifie que tout le trafic de données doit être acheminé par un VPN pour des raisons de sécurité. Une autre entreprise peut avoir une politique de routage qui privilégie l'utilisation de certaines connexions réseau pour des applications critiques qui nécessitent une bande passante élevée.
- Les politiques de routage peuvent être mises en œuvre à différents niveaux dans le réseau, y compris au niveau de l'ensemble du réseau, des sous-réseaux ou des routeurs individuels. Elles peuvent être configurées manuellement ou automatiquement à l'aide de logiciels de gestion de réseau.

- En somme, une politique de routage est un ensemble de règles qui déterminent comment le trafic réseau doit être acheminé à travers le réseau en fonction de critères spécifiques, et qui permettent d'optimiser les performances du réseau, de garantir la qualité de service et de contrôler le flux de trafic.



4.5. Quelle fonctionnalité doit-on activer pour limiter les attaques d'un DHCP Rogue ?

- Pour limiter les attaques de type DHCP Rogue, il est recommandé d'activer la fonctionnalité "DHCP Snooping" sur les commutateurs du réseau.
- Le DHCP Snooping est une fonctionnalité de sécurité des commutateurs réseau qui permet de limiter les risques d'attaques de type DHCP Rogue en bloquant les messages DHCP provenant de sources non autorisées.
- Lorsque DHCP Snooping est activé sur un commutateur, celui-ci examine tous les messages DHCP échangés sur le réseau et vérifie si le message provient d'une source autorisée, telle que le serveur DHCP. Si le message est considéré comme non autorisé, le commutateur peut le bloquer ou le rediriger vers un port d'isolement, empêchant ainsi l'attaque de se propager dans le réseau.
- En activant DHCP Snooping, les administrateurs réseau peuvent donc limiter les risques d'attaques de type DHCP Rogue et renforcer la sécurité du réseau DHCP.