PROTOCOLE IP

1 - Définition et rôle du protocole IP

Internet Protocol (IP) est un protocole, ou un ensemble de règles, appliqué au routage et à l'adressage des paquets de données afin qu'ils puissent traverser les réseaux et arriver à la bonne destination. Les données traversant Internet sont divisées en morceaux plus petits, appelés paquets. Des informations IP sont attachées à chaque paquet, et ces informations permettent aux routeurs d'envoyer des paquets au bon endroit. Chaque appareil ou domaine qui se connecte à Internet se voit attribuer une adresse IP. Les paquets étant dirigés vers l'adresse IP qui leur est associée, les données arrivent là où elles sont nécessaires.

Une fois que les paquets arrivent à destination, ils sont traités différemment en fonction du protocole de transport utilisé en combinaison avec IP. Les protocoles de transport les plus courants sont TCP et UDP.

Il est l' un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à 3 champs :

- Le champ adresse IP : adresse de la machine
- Le champ masque de sous-réseau : un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau
- Le champ passerelle par défaut : Permet au protocole Internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local

2 - Fiabilité du protocole IP

Les protocoles IP assurent l'acheminement au mieux des paquets. Ils ne se préoccupent pas du contenu des paquets, mais fournissent une méthode pour les mener à destination. Ils sont considérés comme « non fiables ». Cela ne signifie pas qu'ils n'envoient pas correctement les données sur le réseau, mais qu'ils n'offrent aucune garantie pour les paquets envoyés concernant les points suivants :

- Corruption de données.
- Ordre d'arrivée des paquets (un paquet A peut être envoyé avant un paquet B, mais le paquet B peut arriver avant le paquet A)
- Perte ou destruction de paquets
- Duplication des paquets

En termes de fiabilité, le seul service offert par un protocole IP est de s'assurer que les en-têtes de paquets transmis ne comportent pas d'erreurs grâce à l'utilisation de somme de contrôle (*checksum*). Si l'en-tête d'un paquet comprend une erreur, sa

somme de contrôle ne sera pas valide et le paquet sera détruit sans être transmis. En cas de destruction d'un paquet, aucune notification n'est envoyée à l'expéditeur.

Les garanties non offertes par un protocole IP sont déléguées aux protocoles de niveau supérieur. La raison principale de cette absence de gestion de la fiabilité est la volonté de réduire le niveau de complexité des routeurs et ainsi de leur permettre de disposer d'une plus grande rapidité.

3 - La composition de l'en-tête IP d'un datagramme

Comme nous l'avons déjà mentionné, le protocole IP garantit que chaque paquet de données soit précédé des propriétés structurelles importantes dans l'en-tête et assigné au protocole de transport approprié (généralement TCP). La zone des données d'en-tête a été fondamentalement révisée pour la version 6, c'est pourquoi il est important de spécifier et différencier les en-têtes l'IPv4 et IPv6.

Structure de l'en-tête IPv4

Bits	0–3	4–7	8–11		12–15	16–18	19–23	24–27	28–31
0	Version	Longueur de l'en-tête		Type de service (ToS)		Longueur totale (Paquet)			
32		Identifcateur				Flag (drap.)	Espace fragment (Fragment offset)		
64	Durée de vie (TTL)			Protocole		Somme de contrôle de l'en-tête (checksum header)			
96		Adresse de la source							
128		Adresse de la destination							
160		Options							

Ainsi chaque en-tête IP commence toujours par une spécification de 4 bits du numéro de version du protocole Internet, IPv4 ou IPv6. Il y a ensuite 4 autres bits supplémentaires, qui contiennent des informations sur la longueur de l'en-tête **IP** (*IP header lenght*), car celle-ci ne reste pas toujours constante.
La longueur totale de l'en-tête est toujours calculée à partir de cette valeur multipliée par 32 bits. Ainsi, la valeur la plus petite possible est 5 et correspond donc à une longueur d'en-tête de 160 bits (correspond à 20 octets) quand aucune option n'est ajoutée.
Le maximum est la valeur 15, pour 480 bits (ce qui correspond à 60 octets). Les bits 8 à 15 (*Type of Service*) peuvent contenir des instructions pour le traitement et la priorisation du datagramme. Par exemple, l'hôte peut spécifier les points importants tels que notamment la fiabilité, le débit et le délai de transmission des données**.**

La longueur totale indique la taille totale du paquet de données, en d'autres termes, la taille des données utiles est ajoutée à la longueur de l'en-tête. Le champ ayant une longueur de 16 bits, la limite maximale est de **65 635 octets.** Le RFC 791 spécifie également que chaque hôte doit pouvoir traiter au moins 576 octets. Un datagramme IP peut être fragmenté arbitrairement sur son chemin de l'hôte vers les routeurs ou autres périphériques, mais les fragments ne doivent pas être plus petits que les 576 octets mentionnés. Les autres champs de l'en-tête IPv4 ont la signification suivante :

- **Identification :** tous les fragments d'un datagramme ont le même numéro d'identification que celui qu'ils reçoivent de l'expéditeur. En associant ce champ de 16 bits, l'hôte cible peut assigner des fragments individuels à un datagramme spécifique.

- **Flag (drapeau)** : chaque en-tête IP contient 3 bits *flag* qui contiennent des informations et des directives pour la fragmentation. Le premier bit est réservé et a toujours la valeur 0, le second bit appelé « Don't Fragment » indique si le paquet peut être fragmenté (0) ou non (1). Le dernier bit, appelé « *More Fragments* » indique si d'autres fragments suivent (1) ou si le paquet est complet ou s'il se termine par le fragment actuel (0).

- **Position du fragment** : ce champ indique à l'hôte cible de l'endroit où se trouve un seul fragment, ce qui permet facilement de compiler à nouveau l'ensemble du datagramme. La longueur de 13 bits signifie qu'un datagramme peut être divisé en un maximum de 8192 fragments.

- **Durée de vie** (*Time to Live, TTL*) : pour s'assurer qu'un paquet ne migre pas d'un nœud à un autre dans le réseau indéfiniment, il est envoyé avec une durée de vie maximale (*Time to Live*). La norme RFC spécifie l'unité en secondes pour ce champ de 8 bits, a noter que la durée de vie maximale est de 255 secondes. Pour chaque nœud de réseau passé, le TTL est réduit d'au moins 1. Si la valeur 0 est atteinte, le paquet de données est automatiquement rejeté.

- **Protocole** : le champ de protocole (8 bits) affecte le protocole de transport correspondant au paquet de données, par exemple, la valeur 6 représente TCP ou la valeur 17 pour le protocole UDP.

- **Somme de contrôle de l'en-tête** : le champ « Checksum » de 16 bits contient la somme de contrôle de l'en-tête. En raison de la diminution du TTL par arrêt intermédiaire, il faut le recalculer pour chaque nœud de réseau. L'exactitude des données de l'utilisateur n'est pas vérifiée pour des raisons d'efficacité.

- **Adresse de la source et adresse de destination** : chaque 32 bits, soit 4 octets, sont réservés à l'adresse IP assignée de l'hôte source et cible. Ces adresses IP sont généralement écrites sous la forme de 4 nombres décimaux séparés par des points. L'adresse la plus basse est 0.0.0.0, la plus haute est 255.255.255.255.

- **Options** : le champ « options » étend le protocole IP avec des informations supplémentaires qui ne sont pas fournies dans la conception standard. Comme il ne s'agit que d'ajouts facultatifs, le champ a une longueur variable, qui n'est limitée que par la longueur maximale de l'en-tête. Les options possibles sont, par exemple, « Security » (indique la confidentialité d'un datagramme), « Record Route » (affiche tous les nœuds réseau passés, leur adresse IP pour tracer l'itinéraire du paquet) et « Time Stamp » (ajoute l'heure à laquelle un nœud en particulier a été passé).

Structure de l'en-tête IPv6

<table>
<tr><td>Bits</td><td>0–3</td><td>4–7</td><td>8–11</td><td>12–15</td><td>16–18</td><td>19–23</td><td>24–27</td><td>28–31</td></tr>
<tr><td>0</td><td>Version</td><td colspan="3">Classe de traffic</td><td colspan="5">Identificateur de flux</td></tr>
<tr><td>32</td><td colspan="4">Longueur des données</td><td colspan="2">En-tête suivant</td><td colspan="2">Hop-Limit (nombre de sauts)</td></tr>
<tr><td>64</td><td colspan="8" rowspan="2">Adresse de la source</td></tr>
<tr><td>128</td></tr>
<tr><td>192</td><td colspan="8" rowspan="2">Adresse de destination</td></tr>
<tr><td>256</td></tr>
</table>

L'en-tête du protocole IPv6, contrairement à l'en-tête de son prédécesseur, a une **taille fixe de 320 bits** (40 octets). Des informations supplémentaires moins fréquemment utilisées peuvent être ajoutées séparément entre l'en-tête standard et les données utilisateur. **Ces en-têtes d'extension** (*Extension Header*) doivent être comparés avec le champ « options » du protocole IPv4 et peuvent être ajustés à tout moment sans avoir à modifier l'en-tête actuel. Cela vous permet notamment de déterminer les chemins des paquets, de spécifier des informations de fragmentation ou d'initier une communication cryptée via IPsec. Une somme de contrôle d'en-tête n'existe pas, au profit notamment de la performance.

Comme pour IPv4, l'en-tête IP actuel commence par le numéro de version long de 4 bits de l'Internet Protocol. Le champ suivant « Classe de trafic » est équivalent à l'entrée « Type of Service » dans l'ancienne variante de protocole. Ces 8 bits informent l'hôte cible sur le traitement qualitatif du datagramme, comme dans la version précédente, ce qui permet d'appliquer les mêmes règles. La nouveauté d'IPv6 est le *FlowLabel* ou identificateur de flux (20 bits), qui permet d'identifier les flux de données à partir de paquets de données en continu. Ceci permet de réserver la bande passante et d'optimiser le routage.

La liste suivante explique les informations d'en-tête supplémentaires du protocole IP amélioré :

- **Taille des données utilisateur** : IPv6 transmet une valeur pour la taille des données utilisateur transportées, y compris l'en-tête de l'extension (16 bits au total). Dans la version précédente, cette valeur devait être séparément calculée en prenant la longueur totale moins la longueur de la ligne d'en-tête.

- **En-tête suivant** : le champ « Next Header » de 8 bits est l'équivalent de la spécification du protocole dans IPv4 et en tant que tel a repris sa fonction qui est l'affectation du protocole de transport souhaité.

- **Nombre de sauts** : le Hop Limit (8 Bit) définit le nombre maximum de stations intermédiaires qu'un paquet peut traverser avant d'être rejeté. Comme pour TTL dans IPv4, la valeur est réduite d'au moins 1 pour chaque nœud.

- **Adresse de la source et adresse de destination** : la majorité des en-têtes Ipv6 contiennent les adresses de l'expéditeur et du destinataire. Comme mentionnée précédemment, ceux-ci ont une longueur de 128 bits (quatre fois la longueur des adresses IPv4). Il existe aussi des différences significatives dans la notation standard. La version la plus récente d'Internet Protocol utilise des nombres hexadécimaux et les divise en 8 blocs de 16 bits chacun. Les deux points sont utilisés au lieu des simples points pour la séparation. Une adresse IPv6 complète ressemble à ceci : 2001:0db8:85a3:08d3:1319:8a2e:0370:7344.

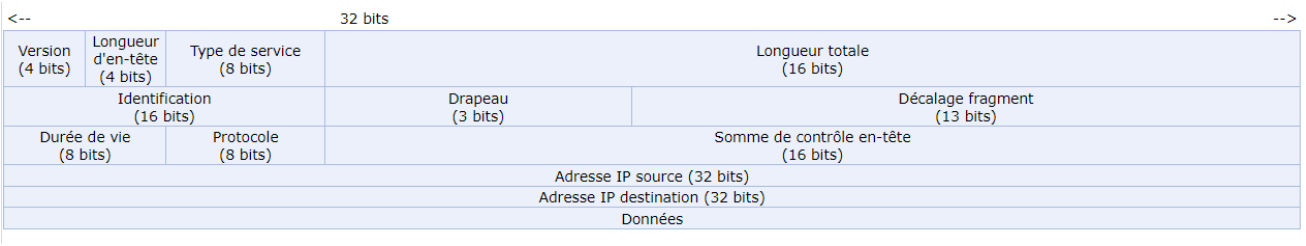
4- Les datagrammes

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).

La taille maximale d'un datagramme est de 65536 octets. Mais, cette valeur est rarement atteinte, car les réseaux ont une capacité moindre par rapport à une telle dimension. De plus, les réseaux utilisés pour propager de l'information sur Internet, sont adossés à différentes technologies, si bien que la taille maximale d'un datagramme peut également varier selon le type de réseau sous-jacent

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Voici ce à quoi ressemble un datagramme :



Voici la signification des différents champs :

- **Version** (4 bits) : il s'agit de la version du protocole IP que l'on utilise (Ici on utilise la version 4 *IPv4*) afin de vérifier la validité du datagramme. Elle est codée sur 4 bits.
- **Longueur d'en-tête**, ou *IHL* pour *Internet Header Length* (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête (nota : la valeur minimale est 5). Ce champ est codé sur 4 bits.
- **Type de service** (8 bits) : il indique la façon selon laquelle le datagramme doit être traité.
- **Longueur totale** (16 bits): il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.
- **Identification, drapeaux (flags) et déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes, ils sont expliqués plus bas.
- **Durée de vie** appelée aussi **TTL**, pour *Time To Live* (8 bits) : ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.
- **Protocole** (8 bits) : ce champ, en notation décimale permet de savoir de quel protocole est issu le datagramme
    - ICMP : 1
    - IGMP : 2
    - TCP : 6
    - UDP : 17
- **Somme de contrôle de l'en-tête, ou en anglais *header checksum* (16 bits)** : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête (champ *somme de contrôle* exclu). Celle-ci est en fait telle que lorsque l'on fait la somme des champs de l'en-tête (somme de contrôle incluse), on obtient un nombre avec tous les bits positionnés à 1
- **Adresse IP source** (32 bits) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre
- **Adresse IP destination** (32 bits) : adresse du destinataire du message

5- La fragmentation des datagrammes

Comme nous l'avons vu précédemment, la taille d'un datagramme maximale est de 65536 octets. Toutefois cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets. De plus, les réseaux sur Internet utilisent différentes technologies, si bien que la taille maximale d'un datagramme varie suivant le type de réseau.
La taille maximale d'une trame est appelée *MTU* (Maximum Transfer Unit), elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible. Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter, c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets.

Le routeur va ensuite envoyer ces fragments de manière indépendante et les réencapsuler (ajouter un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment. De plus, le routeur ajoute des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre. Rien ne dit toutefois que les fragments arriveront dans le bon ordre, étant donné qu'ils sont acheminés indépendamment les uns des autres.

Pour tenir compte de la fragmentation, chaque datagramme possède plusieurs champs permettant leur réassemblage :

- **champ déplacement de fragment** (13 bits) : champ permettant de connaître la position du début du fragment dans le datagramme initial. L'unité de mesure de ce champ est de 8 octets (le premier fragment ayant une valeur de zéro).
- **champ identification** (16 bits) : numéro attribué à chaque fragment afin de permettre leur réassemblage.
- **champ longueur totale** (16 bits) : il est recalculé pour chaque fragment.
- **champ drapeau** (3 bits) : il est composé de trois bits :
    - Le premier n'est pas utilisé, doit être nul

- Le second (appelé **DF** : *Don't Fragment*) indique si le datagramme peut être fragmenté ou non. Si jamais un datagramme a ce bit positionné à un et que le routeur ne peut pas l'acheminer sans le fragmenter, alors le datagramme est rejeté avec un message d'erreur ((DF)= 0 Peut fragmenter, 1 = Ne pas fragmenter.)
- Le dernier (appelé **MF** : *More Fragments*, en français *Fragments à suivre*) indique si le datagramme est un fragment de donnée (1). Si l'indicateur est à zéro, cela indique que le fragment est le dernier (donc que le routeur devrait être en possession de tous les fragments précédents) ou bien que le datagramme n'a pas fait l'objet d'une fragmentation ((MF) 0 = Dernier fragment, 1 = Plus de fragments.

Chaque fois qu'un paquet de données doit être envoyé via TCP/IP, la taille globale est automatiquement vérifiée. Si cette valeur est supérieure à l'unité de transmission maximale (MTU pour *maximum transmission unit*) de l'interface réseau respective, l'information est fragmentée, c'est-à-dire divisée en blocs de données plus petits. Cette tâche est exécutée soit par l'hôte expéditeur (IPv6) soit par un routeur intermédiaire (IPv4). Par défaut, le paquet est composé par le destinataire, qui accède aux **i**nformations de fragmentation stockées dans l'en-tête IP ou dans l'en-tête d'extension. Dans des cas exceptionnels, le réassemblage peut aussi être pris en charge par un pare-feu, si ce dernier est configuré en conséquence.

Étant donné que l'IPv6 ne prévoit généralement plus de fragmentation et ne permet plus la fragmentation du routeur, le paquet IP doit être de taille adéquate avant d'être envoyé. Si un routeur atteint un datagramme IPv6 qui dépasse l'unité de transmission maximale, il le rejette et en informe l'expéditeur sous la forme d'un message ICMPv6 de type 2 « Packet Too Big » (le paquet est trop volumineux). L'application d'envoi de données peut maintenant créer des paquets plus petits et non fragmentés ou bien initier la fragmentation. Ensuite, **l**'en-tête d'extension approprié est ajouté au paquet IP, ainsi l'hôte cible peut reconstituer les fragments individuels après réception.

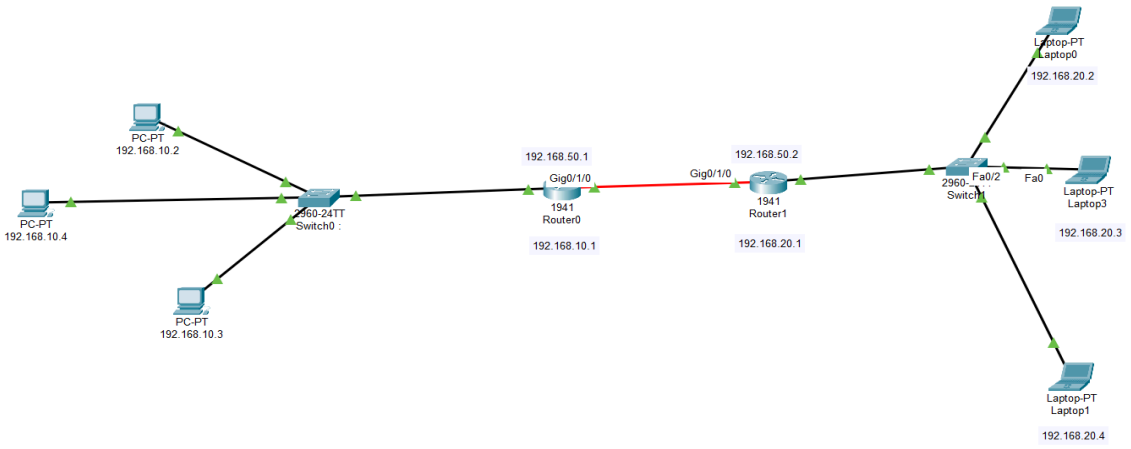


Illustration dans cisco packet Tracer