TCP/IP

MODULE 03
COUCHE RÉSEAU

Plan de la séance

Couche Réseau

- IPv4 ;
- Masque de sous-réseau ;
- IPv6 ;
- CIDR ;
- Protocole ARP ;
- Protocole ICMP ;
- Multidiffusion ;
- Protocole IGMP.

Couche Réseau

Couche Réseau

Définition

La couche réseau construit une voie de communication de **bout à bout à partir de voies de communication** avec ses voisins directs.
Ses apports fonctionnels principaux sont donc …

- le **routage**
  Détermination d'un chemin permettant de relier les 2 hôtes distants ;
- le **relayage**
  Retransmission d'un PDU (*Protocol Data Unit* ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale.

Couche Réseau

Définition

C'est aussi la dernière couche supportée par tous les hôtes du réseau pour le transport des données utilisateur : les couches **supérieures sont réalisées uniquement dans les hôtes d'extrémité**.

Le PDU de cette couche est appelé **paquet ou datagramme**. La fonction de relayage (terme OSI) est parfois appelée acheminement.

Voici les principaux protocoles de la couche Réseau …

- **Protocoles IP** (v4 et v6) ;
- **Protocole ARP** ;
- **Protocole ICMP** ;
- **Protocole IGMP**.

Couche Réseau

Protocole IP (v4 et v6)

Les protocoles TCP/IP se situent dans un modèle souvent nommé famille de protocoles TCP/IP.
Les **protocoles TCP et IP ne sont que deux des membres** de la suite de protocoles IP.

Le protocole IP (*Internet Protocol*) est un protocole qui se **charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP**.
Il fournit un **système de remise de données optimisé sans connexion**.
Le terme optimisé souligne le fait qu'il **ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi**.

Couche Réseau

Protocole IP (v4 et v6)

La fonctionnalité de **somme de contrôle du protocole ne confirme que l'intégrité de l'entête IP**.
Ainsi, seuls les **protocoles de niveau supérieur sont responsables des données contenues** dans les paquets IP (et de leur ordre de réception).

Le protocole **IP travaille en mode non connecté**, c'est-à-dire que les paquets émis par le niveau 3 sont acheminés de **manière autonome** (datagrammes), **sans garantie de livraison**.

Couche Réseau

Principes guidant IP

Dès l'origine **deux principes de base** ont guidés les concepteurs d'Internet pour la création du protocole de transport
(en occurrence IP).
Ces deux principes sont les suivants …

- **Communication de bout en bout**
  Une **communication se fait entre deux partenaires et ce sont ces derniers qui en gèrent les modalités**.
  On sait que la commutation des paquets implique la présence de **plusieurs intervenants intermédiaires et que ces intermédiaires sont transparents** et ne participent pas dans la communication (en fait ils ne sont que des relais).
  Les **nœuds d'extrémités sont considérés comme intelligents**, permettant ainsi le déploiement d'applications client/serveur à l'aide du réseau.

Couche Réseau

Principes guidant IP

Ces deux principes sont les suivants …

- **Livraison au meilleur effort**
  Ce principe implique que tous les éléments intermédiaires (aiguilleurs) de la connexion n'offre aucune garantie quant au transport des paquets entre les nœuds d'extrémités. Ils font de leur mieux pour rendre les paquets à destination. **IP n'est donc pas selon ce principe un protocole fiable**.
  Seulement les nœuds d'extrémités vont utiliser un protocole de la couche Transport du modèle OSI pour garantir cette livraison (ce qui n'est pas le cas des nœuds intermédiaires).
  C'est pourquoi le protocole **TCP est implicitement lié au protocole IP**.

Couche Réseau

Configuration IP

Toute configuration IP doit comporter les données suivantes …

- l'**adresse IP**
  (unique à l'hôte) ;
- le **masque de sous-réseau** ;
- l'**adresse de la passerelle par défaut**
  (un aiguilleur est traditionnellement appelé ainsi pour le réseau Internet).
  La passerelle est la porte d'entrée sur le réseau Internet ;
- l'**adresse d'un serveur DNS**
  Le serveur DNS est l'intermédiaire qui résout un nom convivial comme www.profsavard.info en une adresse valide de destination comme 206.167.36.22.

Couche Réseau

Configuration IP

Toute configuration IP valide doit obligatoirement **comporter les deux premiers éléments.**
Sans ces informations il sera **impossible pour un hôte de communiquer avec un hôte distant** (qu'il soit dans son propre réseau ou sur le réseau Internet).
Quant au **troisième il est essentiel si un hôte veut communiquer avec un hôte distant hors de son propre réseau local**.
Enfin, sans le **quatrième élément, l'utilisateur devra toujours connaître l'adresse exacte pour rejoindre un hôte en dehors de son réseau local**.

Couche Réseau

Adresses IPv4

Pour pouvoir établir une communication avec un autre hôte branché au réseau Internet un hôte (ou nœud) doit **obligatoirement posséder une adresse IP unique**.

Cette adresse peut être caractérisée comme étant statique ou dynamique.

- Une **adresse statique est généralement attribuée manuellement** par un administrateur réseau.
  Certains nœuds du réseau Internet nécessitent une adresse qui ne sera pas modifiée (ce qui est le cas de la plupart des serveurs).
- Une **adresse dynamique est une adresse qui sera attribuée de manière automatique** lors de l'ouverture d'un hôte.
  Cette adresse est généralement attribuée par un serveur DHCP.

Couche Réseau

Adresses IPv4

Plusieurs avantages liés à la présence d'un serveur DHCP …

- **Attribution automatique de la configuration IP** à un hôte;
- **Résolution du problème d'un réseau** qui possède plus d'hôtes que d'adresses disponibles.

DHCP (*Dynamic Hosts Configuration Protocol*) est un protocole de la couche Applications.

Couche Réseau

Anatomie d'une adresse IPv4

Une adresse IP se divise en deux parties …

- La **première représente la partie réseau**.
  Il est important de préciser ici qu'un réseau est un regroupement logique de plusieurs hôtes.
  Cette partie réseau est attribuée par un responsable fournisseur et est unique pour le réseau Internet
- La **seconde partie d'une adresse IPv4 est l'identifiant unique** pour un hôte de ce réseau.
  Cette **partie est gérée localement par les responsables du réseau interne**.
  C'est cette partie qui est attribuée dynamiquement ou statiquement.
  Cette partie identifiant doit être obligatoirement unique au réseau interne.

Couche Réseau

Anatomie d'une adresse IPv4

Une adresse IP peut être **publique ou privée** …

- Une **adresse publique est une adresse que doit posséder tout hôte qui veut établir une communication sur le réseau Internet**.
  Ceci permet d'établir une session sans intermédiaire interne (comme un serveur proxy).
- Une **adresse privée est une adresse qui permet aux hôtes d'un même réseau de communiquer entre eux sans toutefois pouvoir ouvrir une session avec un hôte sur le réseau Internet**.
  Par défaut, les **aiguilleurs (la porte de sortie sur le réseau Internet) sont configurés pour ne pas laisser passer les paquets provenant d'un hôte possédant une adresse privée**.

Couche Réseau

Anatomie d'une adresse IPv4

Le **protocole NAT permet de faire le lien entre un hôte possédant une adresse privée et un serveur proxy possédant une adresse publique**.
Ce serveur proxy devient à la fois traducteur entre adresses privées et adresses publiques et aiguilleur.

Deux fournisseurs pour l'attribution des adresses réseau IPv4 …

- **ICANN** ou *Internet Corporation for Assigned Names and Numbers* et
- **RIR** ou *Regional Internet Registries*.

Couche Réseau

Méthode d'attribution des identificateurs IPv4

- **Prévoir l'avenir**
  Tenir compte de la croissance future du réseau
  (surtout dans la planification des sous-réseaux)
- **Assurer l'unicité**
  Bien identifier les sous-réseaux
- **Éviter les adresses à accès limité**
  Adresses de réseau, diffusion, bouclage, …

Couche Réseau

Dispositifs de réseau	Étendues d'adresses
Aiguilleurs	192.168.0.1 à 192.168.0.5
Stations de travail	192.168.0.6 à 192.168.0.245
Stations serveurs	192.168.0.246 à 192.168.0.254

Couche Réseau

Méthode d'attribution des identificateurs IPv4

Une adresse IPv4 est **composée de 32 bits** dont une partie sert à identifier le réseau et une partie pour identifier les hôtes composant ce réseau.

La partie de ces 32 bits attribuée à chacune des parties varie selon la classe.

Couche Réseau

Classe A **0RRR RRRR HHHH HHHH HHHH HHHH HHHH HHHH***
• 7 bits pour l'identification réseau ou 2^7 ➔128 réseaux
• **Réseaux possibles**: **1**.0.0.0 à **126**.0.0.0 donc 126 réseaux **Exclusions**: les réseaux 0.0.0.0 (utilisé dans les tables d'aiguillage) et 127.0.0.0 (réservé pour l'adresse de bouclage) **Adresses privées**: le réseau 10.0.0.0
• 24 bits disponibles pour l'hôte ou 2^{24} ➔16 777 216 - 2 (numéro de réseau et adresse de diffusion générale)

Couche Réseau

Classe B **10RR RRRR RRRR RRRR HHHH HHHH HHHH HHHH***
• 14 bits pour identifier les réseaux ou 2^{14} ➔16 384 réseaux
• **Réseaux possibles**: 128.0.0.0 à 191.255.0.0 **Adresses privées**: le réseau 172.16.0.0
• 16 bits disponibles pour l'hôte ou 2^{16} ➔ 65 536 - 2 (numéro de réseau et adresse de diffusion générale)

Couche Réseau

Classe C 110R RRRR RRRR RRRR RRRR RRRR HHHH HHHH*
• 21 bits pour identifier les réseaux ou 2^{21} → 2 097 152 réseaux possibles
• **Réseaux possibles:** 192.0.0.0 à 223.255.255.0 **Adresses privées:** les réseaux 192.168.0.0 à 192.168.255.0
• 8 bits disponibles pour l'hôte ou 2^{8} → 256 - 2 (numéro de réseau et adresse de diffusion générale)

Couche Réseau

Classe D 1110 RRRR RRRR RRRR RRRR RRRR HHHH HHHH*
• **Adresses possibles:** 224.0.0.0 à 239.255.255.255

Couche Réseau

Classe E 1111 0RRR RRRR RRRR RRRR RRRR HHHH HHHH*
• Adresses possibles: 240.0.0.0 et plus

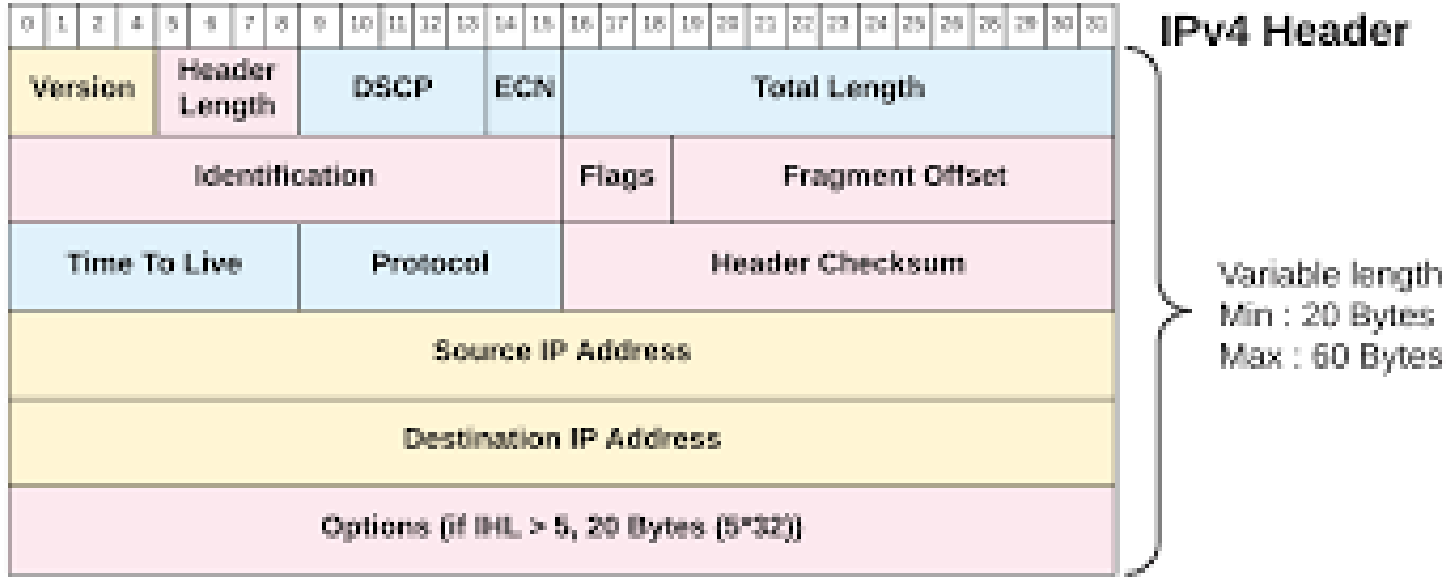
Couche Réseau

En-tête IPv4

Dans un réseau TCP/IP, on assigne généralement **une adresse IP à chaque hôte**.
Le terme d'hôte est pris dans son sens large, c'est à dire un **nœud de réseau**.
Une imprimante, un aiguilleur (*router*), un serveur, un poste de travail sont des nœuds qui peuvent avoir également un nom d'hôte, s'ils ont une adresse IP.

Le datagramme correspond au format de paquet défini par le protocole Internet.
Les cinq ou six (sixième facultatif) premier **mots de 32 bits** représentent les **informations de contrôle appelées entête**.

Couche Réseau



Couche Réseau

En-tête IPv4

Voici en quoi consistent les différents champs d'une entête IP …

- **Version** -- 4 bits
- **Longueur de l'en-tête ou IHL (*Internet Header Length*)** -- 4 bits
- **Type de service ou ToS (pour Type of Service)** -- 8 bits
- **Longueur totale en octets ou Total Length** -- 16 bits
- **Identification** -- 16 bits
- **Indicateurs ou drapeaux (*flags*)** -- 3 bits
- **Décalage du segment (*Fragment offset*)** -- 13 bits
- **Durée de vie ou TTL (*Time To Live*)** -- 8 bits
- **Protocole (*Protocol*)** -- 8 bits
- **Somme de contrôle de l'en-tête (*Header Checksum*)** -- 16 bits
- **Adresse source (*Source address*)** -- 32 bits
- **Adresse de destination (*destination address*)** -- 32 bits
- **Options** -- 0 à 40 octets par mots de 4 octets
- **Remplissage (*padding*)**

Couche Réseau

Fragmentation et assemblage IP

Lorsqu'un un **datagramme est fragmenté**, il n'est **réassemblé que par la couche IP destinatrice finale**.
Cela implique trois remarques …

- La **taille des datagrammes reçus** par le destinataire final est directement **dépendante du plus petit MTU rencontré** sur le réseau
- Les **fragments deviennent des datagrammes** à part entière.
- Rien ne s'oppose à ce qu'un **fragment soit à nouveau fragmenté**.

Couche Réseau

Masque de sous-réseau (IPv4)

Le masque de sous réseau est un **élément essentiel à toute configuration IP**.
Il complète et caractérise l'adresse IP.

Fonctions
Les deux fonctions du masque de sous-réseau sont les suivantes ...

- **Première fonction**
  Déterminer si un hôte distant est un hôte attaché à son réseau local ou encore est un hôte extérieur, connecté sur Internet.
- **Seconde fonction**
  Permettre à l'administrateur local de **séparer un réseau en sous-entités**. Cette option permet de gérer plus facilement des grands réseaux.

Couche Réseau

Masque de sous-réseau (IPv4)

Avantages

Les avantages d'utiliser des sous-réseaux sont les suivants ...

- **Utilisation optimisée de l'espace d'adressage**
- **Administration simplifiée**
  Permet d'administrer les sous-réseaux de manière indépendante et efficace. Permet de gérer plus efficacement des parties du réseau qui ont des exigences contradictoires
- **Possibilité de structurer un réseau interne sans affecter les réseaux externes**
  Seul l'aiguilleur du réseau destination doit connaître la présence des sous-réseaux
- **Sécurité améliorée**
  La structure du sous-réseau est invisible à l'externe donc la sécrité est améliorée indirectement

Couche Réseau

Masque de sous-réseau (IPv4)

Méthode 1

Détermination du nombre de bits

- **Écrire en binaire le nombre de sous-réseaux** souhaités
- **Compter le nombre de bits nécessaire**
  (ne pas oublier de soustraire 2)
- **Définition du masque de sous-réseau**

Couche Réseau

Masque de sous-réseau (IPv4)

Méthode 1
Détermination du nombre de bits

Pour établir le masque de sous-réseau, il faut emprunter des bits à la portion identificateur d'hôte.
Additionner au masque de sous-réseau par défaut le nombre de bits nécessaire.

Ex. Classe B

1111 1111 1111 1111 0000 0000 0000 0000
0000 0000 0000 0000 1111 0000 0000 0000
1111 1111 1111 1111 1111 0000 0000 0000

Si l'on désire obtenir 12 sous-réseaux :

1. Il faut 4 bits ou 2^4
2. Un masque de sous-réseau ne doit pas contenir que des 0 ou des 1 -- donc 16 – 2 = 14
3. Il reste 12 bits pour les hôtes -- 2^{12} ou 4 094 – 2 hôtes

Couche Réseau

Tableau synthèse Masque de sous-réseaux, ID de sous-réseaux et nombre de sous-réseaux pour une classe B							
Poids binaire	64	32	16	8	4	2	1
Bits supplémentaires	2	3	4	5	6	7	8
SR possibles	(2^2-2) 2	(2^3-2) 6	(2^4-2) 14	(2^5-2) 30	(2^6-2) 62	(2^7-2) 126	(2^8-2) 254
Masque de SR	128 + 64 192	192 + 32 224	224 + 16 240	240 + 8 248	248 + 4 252	252 + 2 254	254 + 1 255
Bits ID hôtes	6 + 8 14	5 + 8 13	4 + 8 12	3 + 8 11	2 + 8 10	1 + 8 9	0 + 8 8

Couche Réseau

Masque de sous-réseau (IPv4)

Méthode 2
ID des hôtes

Les adresses pour chaque sous-réseau correspondent à toutes les combinaisons binaires possibles comprises entre l'adresse du sous-réseau et son adresse de diffusion.

Étapes …

1. Trouver l'ID du sous-réseau suivant :
   ex. 255.255.240.0 (4 bits sont utilisés donc 16 comme valeur incrémentée)
   160.16.32.0 + 16 = 160.16.48.0
2. Déterminer l'adresse du premier hôte :
   160.16.32.1
3. Déterminer l'adresse de diffusion :
   160.16.47.255
4. Déterminer l'adresse du dernier hôte :
   160.16.47.254

Couche Réseau

Internet Protocol version 6 (IPv6)

Au début des années 90, l'évolution du réseau Internet semblait compromise à court terme car le protocole IP (Internet Protocol) **limitait le nombre d'équipements qui pouvaient s'y connecter**.

À sa création, ce **réseau ne devait servir qu'à relier une centaine d'hôtes** mais de nombreuses catégories d'utilisateur sont très vite venues s'y joindre. On y trouvait les scientifiques, les universitaires, puis en 1992, le réseau fut ouvert aux activités commerciales ainsi qu'aux particuliers.
Depuis, le **nombre d'équipements connectés ne cesse d'augmenter et on approche de la saturation du réseau**.

Elle porte notamment sur …

- l'**auto configuration** ;
- la **mobilité** ;
- la **diffusion multipoints**
  et
- la **sécurité**.

Couche Réseau

Internet Protocol version 6 (IPv6)

IPv6 est le protocole de la prochaine génération d'Internet et c'est pour cela qu'on l'appelle aussi **IPng**, initiales de ***Internet Protocol Next Generation***.
On s'attend à ce que **IPv6 remplace graduellement IPv4**, avec une période de transition de plusieurs années de coexistence.

Couche Réseau

Avantages d'IPv6

- **Échelonnement**
  IPv6 possède des adresses de **128 bits** face aux adresses de 32 bits de Ipv4 ;
- **Sécurité**
  IPv6 assure la sécurité dans ses spécifications en utilisant le chiffrement de l'information et l'authentification de l'expéditeur de ladite information ;
- **Applications en temps réel**
  Afin d'offrir un meilleur support pour le trafic en temps réel (par exemple, vidéoconférence), IPv6 comprend l'étiquetage de flux dans ses spécifications.

Couche Réseau

Assignation des adresses IPv6

Avec IPv6, le client recevra une sous classe comme la suivante …
2001:0ba0:1c01::/48

Ce même client pourra également concevoir dans ses installations 65 535 sous réseaux différents, résultant des combinaisons créées en utilisant w,x,y,z dans le groupe ...
2001:0ba0:01b0:wxyz::/64

Chacun de ces **65 535 sous réseaux** qu'un client pourra créer, aura à son tour plus de **18 trillions d'adresses IP distinctes** qui peuvent être d'**assignation automatique** (plug and play) ou manuelle de la part du client.
À l'heure actuelle,l'ipv6 n'est pas utilisé dans la majorité des réseaux informatiques.
Les **entreprises boudent l'ipv6 car le déploiement de ce protocole engendre des frais** de mise en place non justifiés à leurs yeux.

Couche Réseau

Adressage IPv6

La taille d'une adresse IPv6 est de **16 octets (128 bits)**. Cette taille, suffisamment importante, permet d'établir un **plan d'adressage hiérarchisé en trois niveaux**.

- **Topologie publique utilisant 48 bits** ;
- **Topologie de site sur 16 bits** ;
- **Topologie d'interface sur 64 bits**.

Une adresse IPv6 est donc longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4.
La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une **écriture hexadécimale**, où les **8 groupes de 2 octets (16 bits par groupe)** sont séparés par un signe deux-points …
2001:0db8:0000:85a3:0000:0000:ac1f:8001
2A01:E35:2421:4BE0:CDBC:C04E:A7AB:ECF3

Couche Réseau

Adressage IPv6

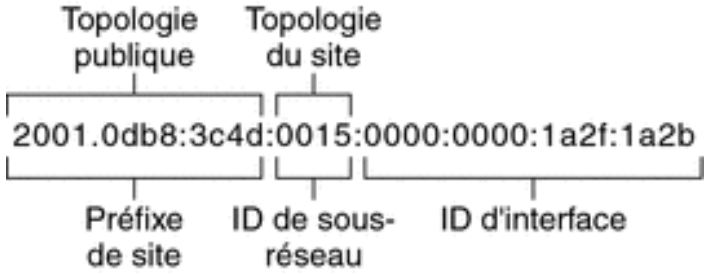
Il est permis d'**omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux**. Ainsi, l'adresse IPv6 ci-dessus est équivalente à:
2001:db8:0:85a3:0:0:ac1f:8001

De plus, une **unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise**, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points (::).
Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en:
2001:db8:0:85a3::ac1f:8001

Couche Réseau

Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques
fe80::/10	Adresses locales lien (auto-configuration)
ff00::/8	Adresses multicast
::1/128	Adresse de bouclage (semblable à 127.0.0.1 en IPv4)
0:0:0:0:0:0:0:0 ou encore notée ::	Adresse utilisée pendant l'initialisation de l'adresse IPv6 d'une machine. Cela est une phase transitoire

Couche Réseau

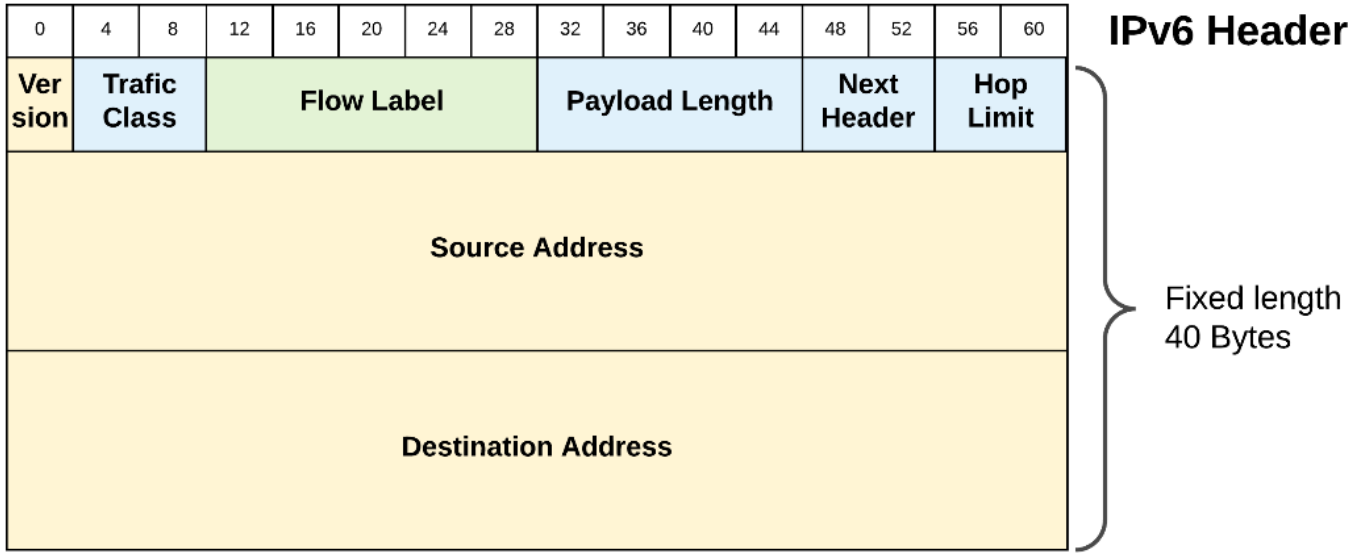


Couche Réseau

Entête IPv6

L'en-tête du paquet IPv6 est de **taille fixe à 40 octets**, tandis qu'en IPv4 la taille minimale est de 20 octets, des **options pouvant la porter jusqu'à 60 octets**, ces **options demeurant rares** en pratique.

Couche Réseau



Couche Réseau

Entête IPv6

La signification des champs est la suivante :

- **Version *(Version)*** -- 4 bits
- **Classe de trafic (*Traffic Class*)** -- 8 bits
- **Étiquette de flux (*Flow Label*)** -- 20 bits
- **Longueur de la charge utilse (*Payload length*)** -- 16 bits
- **Prochain entête (Next Header)** -- 8 bits
- **Nombre de sauts (Hop Limit)** -- 8 bits
- **Adresse source (*Source Address*)** -- 128 bits
- **Adresse de destination (*Destination Address*)** -- 128 bits

Il est possible qu'un ou plusieurs en-têtes d'extension suivent l'en-tête IPv6.
L'en-tête de routage permet par exemple à la source de spécifier un chemin déterminé à suivre.

Couche Réseau

Comparaison avec IPv4

- La **taille de l'en-tête est fixe**, le champ IHL (*IP Header Length*) est donc inutile.
- Le **champ *Time to Live*** (TTL) est **renommé en *Hop Limit***, reflétant la pratique (la RFC 791 prévoyait en effet que le champ TTL reflétait le temps en secondes).
- Il n'y a **pas de somme de contrôle sur l'en-tête**.
  Avec IPv4, cette somme de contrôle inclut le champ TTL et oblige les routeurs à le recalculer dans la mesure où le TTL est décrémenté.
  Ceci simplifie le traitement des paquets par les routeurs.
- Le **champ *Payload length* n'inclut pas la taille de l'en-tête** standard (ni des en-têtes optionnels qui suivent), contrairement au champ *Total length* d'IPv4.
- Les **éventuelles informations relatives à la fragmentation sont repoussées dans un en-tête qui suit**.

Couche Réseau

CIDR (*Classless Inter-Domain Routing*)

Le routage inter-domaine sans classe est une **méthode d'allocation d'adresses IP et de routage IP**.
L'*Internet Engineering Task Force* (IEEE) a introduit le CIDR en 1993 afin de **remplacer l'ancienne architecture d'adressage réseau** de classe sur Internet. Son objectif était de **ralentir la croissance des tables de routage** sur les routeurs sur Internet et d'aider à ralentir l'épuisement rapide des adresses IPv4.

Le CIDR englobe plusieurs concepts.
Il est basé sur le **masquage de sous-réseau de longueur variable** (*Variable Length Subnet Mask*) qui permet de spécifier des préfixes de longueur arbitraire. Le CIDR a introduit une **nouvelle méthode de représentation des adresses IP**, désormais connue sous le nom de notation CIDR, dans laquelle une adresse ou un préfixe de routage est écrit avec un **suffixe indiquant le nombre de bits du préfixe**, comme **192.0.2.0/24** pour IPv4, et **2001:db8::/32 pour IPv6**.

Couche Réseau

CIDR (Classless Inter-Domain Routing)

Le CIDR a été mis au point afin (principalement) de **diminuer la taille de la table de routage** contenue dans les routeurs, Il permet d'agréger plusieurs entrées de cette table en une seule.
Cette technique a permis d'**agréger des réseaux par région géographique et fournisseurs d'accès**.
Elle permet ainsi une agrégation maximum des sous-réseaux qui sont routés ensembles avec la même politique

Couche Réseau

Notation CIDR

La notation CIDR est une représen**tation compacte d'une adresse IP et de son préfixe de routage associé**. La notation est construite à partir d'une **adresse IP, d'une barre oblique (/) et d'un nombre décimal**.
Le nombre final est le **nombre de bits 1 dans le masque de routage**, traditionnellement appelé masque de sous-réseau.

Couche Réseau

Notation CIDR

Par exemple …

- **192.168.100.14/24** représente l'**adresse IPv4 192.168.100.14 et son préfixe de routage associé 192.168.100.0**, ou de manière équivalente, son **masque de sous-réseau 255.255.255.0**, qui a 24 bits de début 1 ;
- le **bloc IPv4 192.168.100.0/22 représente les 1024 adresses** IPv4 de 192.168.100.0 à 192.168.103.255 ;
- le **bloc IPv6 2001:db8::/48 représente le bloc d'adresses IPv6 de 2001: db8:0:0:0:0 0:0 à 2001:db8:0:ffff:ffff:ffff:ffff:ffff** ;
- **:1/128 représente l'adresse de bouclage IPv6**.
  Sa longueur de préfixe est 128, qui est le nombre de bits dans l'adresse.

Couche Réseau

Notation CIDR

Pour IPv4, la notation CIDR est une **alternative à l'ancien système de représentation des réseaux** par leur adresse de départ et le masque de sous-réseau, tous deux écrits en notation décimale par points.
192.168.100.0/24 est équivalent à 192.168.100.0/255.255.255.0.

Le nombre d'adresses d'un sous-réseau peut être calculé comme $2^{\text{longueurs d'adresse} - \text{longueur de préfixe}}$,
où la longueur de l'adresse est de **128 pour IPv6** et
de **32 pour IPv4**.

Couche Réseau

Protocole ARP

Une **station ne lit le contenu d'une trame qu'à la condition qu'elle lui soit adressée**.

Or le **paquet IP est justement placé dans la trame**. Lorsqu'une couche haute transmet des données à une autre hôte, elle **communique à la couche IP, l'adresse IP de destination**.

IP formate ensuite un paquet avec une entête IP. Celle-ci comportent l'**adresse de destination**, transmise par la couche supérieure, et l'**adresse IP source de l'émetteur**.
Cette dernière est connue par IP car il a été initialisé lors de l'installation de l’hôte.

Couche Réseau

Protocole ARP

IP communique ce paquet à la couche 2 (ici la sous-couche MAC) pour l'**encapsuler dans une trame MAC** avant émission sur le support.
Mais il doit également **communiquer l'adresse MAC de destination de la trame**, pour que la couche 2 puisse formater correctement la trame.

ARP (*Address Resolution Protocol*) prend en charge, comme son nom l'indique, la **résolution d'adresse entre le niveau 2 et le niveau 3**.
Il a pour rôle de **trouver l'adresse MAC correspondant à une adresse IP donnée**.

Lorsqu'il a découvert cette adresse, il **met à jour une table ARP**.

Couche Réseau

Protocole ARP

Le protocole **ARP est nécessaire au fonctionnement d'IPv4** utilisé au-dessus d'un réseau de type Ethernet.

En **IPv6, les fonctions de ARP sont reprises par le *Neighbor Discovery Protocol* (NDP)**.

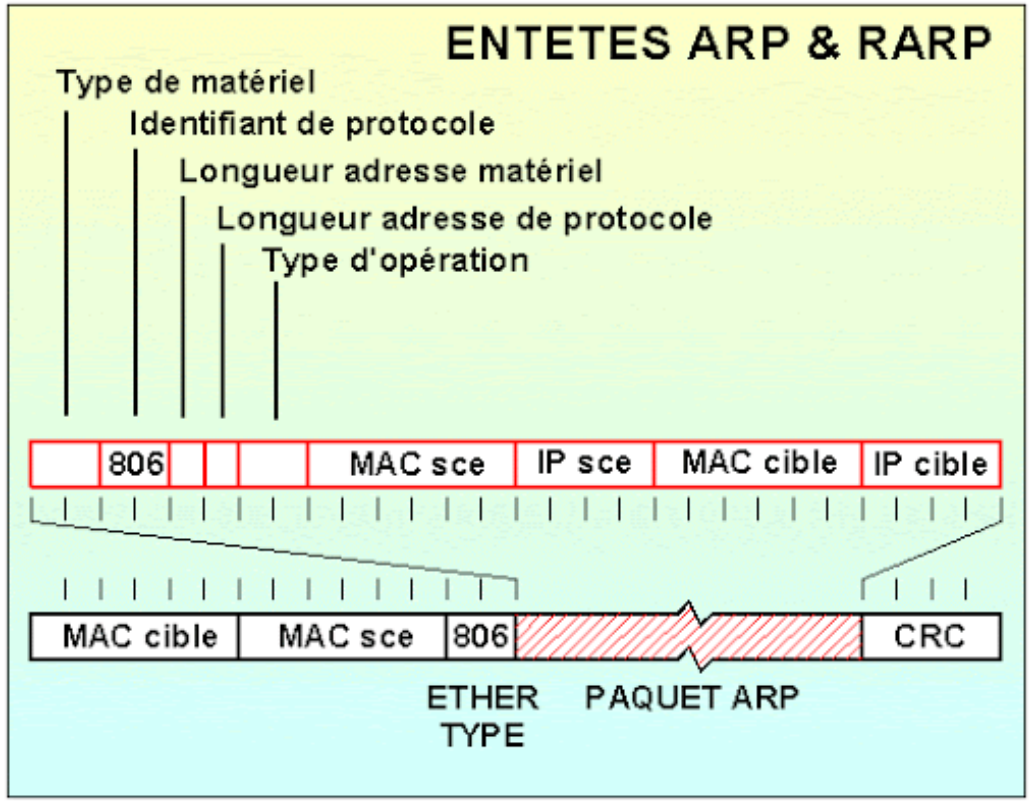
Formats des paquets ARP

ARP est encapsulé directement dans IP (il n'est pas placé dans UDP ou TCP). Il propose deux paquets …

- **ARP Request**
  La requête pour initier la recherche ;
- **ARP Reply**
  La réponse à la requête.

Couche Réseau

Protocole ARP



Couche Réseau

Protocole ARP

Voici le détail de la trame ARP ...

- **Type de matériel (*Hardware type*)**
- **Indicateur de protocole (*Hardware type*)**
- **Longueur Adresse matérielle (*Hardware Address Length*)**
- **Longueur adresse de protocole (*Protocol Address Length*)**
- **Type d'opération (*Operation type*)**
- **Adresse MAC Source (*Sender Hardware Address*)**
- **Adresse réseau de l'émetteur (Sender Prococol Address)**
- **Adresse MAC du destinataire (*Target Hardware Address*)**
- **Adresse réseau du destinataire (*Target Protocol Address*)**

Couche Réseau

Cache ARP

Le **cache ARP ou table ARP est une table de couples adresse IPv4 -- adresse MAC contenue dans la mémoire d'un hôte qui utilise le protocole ARP**, ce qui est le cas des hôtes qui sont connectés à un réseau IP sur un segment Ethernet.

Utilisation

Cette table est **utilisée par les hôtes afin de déterminer l'adresse MAC d'un autre hôte sur le même segment**.

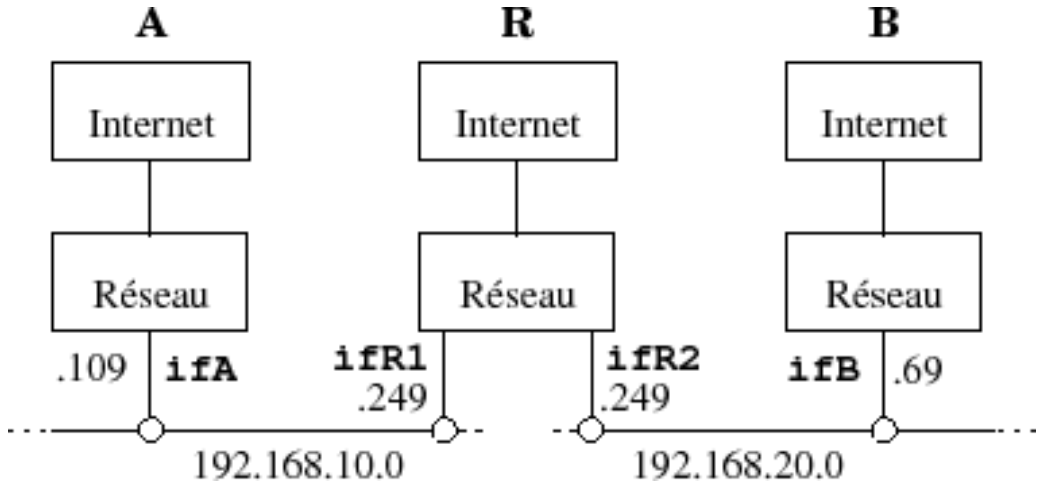
Les entrées dans cette table ont une **durée de vie limitée**, quand une entrée vient à expiration, une nouvelle requête ARP devra être initiée si besoin est.

Certains systèmes d'exploitation permettent de fixer une association dans le cache ARP de façon permanente.

Couche Réseau

ARP en pratique

Dans cet exemple, deux réseaux privés de la RFC 1918 ... **192.168.10.0 et 192.168.20.0** et l'hypothèse est que la **passerelle fonctionne comme un hôte Linux** qui ferait du **routage entre deux de ses interfaces**.



Couche Réseau

Protocole ICMP

ICMP (*Internet Control Messaging Protocol*) est le protocole de gestion de la suite TCP/IP, qui est **requis dans chaque mise en œuvre TCP/IP et autorise deux nœuds d'un réseau IP à partager des informations d'erreur ainsi que l'état IP**.
ICMP est utilisé par l'utilitaire *ping* pour déterminer l'accessibilité d'un système distant

Avec ICMP, les hôtes et les aiguilleurs (*routers*) qui utilisent la communication IP peuvent faire **état des erreurs et échanger des informations sur le contrôle limité et sur l'état**.

Couche Réseau

Protocole ICMP

Les messages ICMP sont généralement envoyés automatiquement dans l'un des cas suivants ...

- Un p**aquet (datagramme) IP ne peut pas atteindre sa destination** ;
- Un **aiguilleur IP (passerelle) ne peut pas transmettre les paquet**s et donne des informations sur l'état de la transmission ;
- Un **aiguilleur IP redirige l'hôte d'envoi pour utiliser un meilleur itinéraire** vers la destination.

Couche Réseau

Messages ICMP

Différents types de messages ICMP sont identifiés dans l'en-tête ICMP. Les **messages ICMP étant traités dans des paquets IP, ils ne sont pas fiables**.

Message ICMP	Description
Requête d'écho (*Echo request*)	Détermine si un nœud IP (un hôte ou un aiguilleur) est disponible sur le réseau.
Réponse d'écho (*Echo reply*)	Répond à une requête d'écho ICMP.
Destination inaccessible (*Destination unreachable*)	Informe l'hôte qu'un paquet ne peut pas être livré.
Extension de source (*Source quench*)	Informe l'hôte pour réduire la vitesse à laquelle il envoie les paquets à cause de la congestion.
Redirection (*Redirect*)	Informe l'hôte d'un itinéraire préféré.
Dépassement de la temporisation (*Time exceeded*)	Indique que la durée de vie TTL (Time-to-Live) d'un paquet IP a été dépassée.

Couche Réseau

Multidiffusion

En informatique, le terme **multidiffusion (*multicast*) définit une connexion réseau multipoint**.

Définition

On entend par multidiffusion le fait de **communiquer simultanément avec un groupe d'ordinateurs identifiés par une adresse spécifique** (adresse de groupe).

Avantages

L'avantage de ce système par rapport à la classique monodiffusion (*unicast*) devient évident quand on veut diffuser de la vidéo. En **streaming on envoie une image autant de fois que l'on a de connexions simultanées**. Comme résultat ... **moins de perte de temps, de ressources du serveur et surtout de bande passante**.

En multidiffusion le **paquet n'est émis qu'une seule fois** et **sera aiguillé (routé) vers tous les hôtes du groupe de diffusion**.

Couche Réseau

Multidiffusion

Protocoles

En multidiffusion, le protocole IP utilise les **adresses de la classe d'adresses D** (**224.0.0.1 à 239.255.255.254**).
Les **adresses IP de multidiffusion 224.0.0.1 à 224.0.0.255** ont un **rôle spécifique à utilisation locale**.

Les paquets de données sont **aiguillés sur le réseau selon l'adresse des destinataires encapsulée dans la trame transmise**.
Normalement, **seuls les destinataires interceptent et décodent les paquets** qui leurs sont adressés.

Exemple d'une **adresse IP locale** pouvant servir à une communication de multidiffusion …
2**24.0.0.1** ;
Exemple d'une **adresse IP Internet** pouvant servir à une communication de multidiffusion …
239.254.254.254.

Couche Réseau

Multidiffusion

Protocoles

Un **groupe de multidiffusion se compose d'un ensemble d'hôtes**. Il est entièrement **dynamique** (**un hôte peut rejoindre ou quitter le groupe à tout moment**) et **ouvert** (**une station peut émettre un paquet dans un groupe sans en faire partie**).

Un groupe de multidiffusion est désigné par une adresse IP (de 224.0.0.1 à 239.255.255.255).
Lorsqu'un hôte veut envoyer un paquet à un groupe multidiffusion, il **envoie ce paquet à l'adresse IP identifiant ce groupe** (par ex : 224.1.2.3).
La **réception est réalisée par un aiguilleur abonné** au groupe et le **paquet est alors dupliqué et renvoyé grâce à une trame de niveau 2 Multicast**.

Le **protocole IGMP** est utilisé par le protocole IP pour l'**adhésion aux groupes de multidiffusion**.

Couche Réseau

Multidiffusion

Utilisation

L'usage de la multidiffusion sur Internet est encore **limité aux universités ou utilisé en interne par les fournisseurs d'accès Internet** (diffusion des chaînes de télévision pour certains). Certaines **radio web expérimentent un flux de multidiffusion** pour la diffusion de leurs programmes.

Couche Réseau

Protocole IGMP

IGMP (*Internet Group Management Protocol*) est historiquement défini dans l'Annexe I de la RFC 1112.
Sa **raison d'être est que les datagrammes ayant une adresse de multidiffusion sont à destination d'un groupe d'utilisateurs dont l'émetteur ne connait ni le nombre ni l'emplacement**.

L'usage de la **multidiffusion** étant par définition dédié aux applications comme la radio ou la vidéo sur le réseau Internet, donc **consommatrices de bande passante**, il est primordial que les **aiguilleurs (routers) possèdent un moyen de savoir s'il y a des utilisateurs de tel ou tel groupe sur les réseaux locaux** directement accessibles pour **ne pas encombrer la bande passante associée** avec des flux d'octets que personne n'utilise plus.

Couche Réseau

Protocole IGMP

Remarques …

- Sur un réseau local sans aiguilleur pour la multidiffusion, le seul **trafic IGMP est celui des hôtes demandant à rejoindre tel ou tel groupe** ;
- Il n'y a **pas de report pour quitter un groupe** ;
- L'étendue d'adresses multicast entre 224.0.0.0 et 224.0.0.225 est **réservée aux applications utilisant une valeur de 1 pour le champ TTL** (administration et services au niveau du réseau local) ;
- Les **aiguilleurs ne doivent pas transmettre de tels datagrammes** ;
- Il n'y a **pas de message ICMP sur les datagrammes ayant une adresse de destination du type de multidiffusion**.

Couche Réseau

Adresses IP de multidiffusion réservées

L'IANA (*Internet Assigned Numbers Authority*) est l'**organisation chargée de gérer les noms de domaine de niveau supérieur et l'adressage IP**.
Le tableau suivant présente une **liste non exhaustive d'adresses de Classe D réservées pour la multidiffusion**.

Couche Réseau

Adresses IP de multidiffusion réservées

Adresse IP multidestinataire	Description
224.0.0.0	Adresse de base réservée
224.0.0.1	Groupe multidestinataire de tous les hôtes (contient tous les systèmes du sous réseau)
224.0.0.2	Groupe multidestinataire de tous les aiguilleurs (contient tous les routeurs du sous réseau)
224.0.0.5	Aiguilleurs OSPF (open shortest path first)
224.0.0.6	Aiguilleurs OSPF désignés
224.0.0.9	Groupe RIP v2
224.0.0.12	Serveurs ou agent de relais DHCP
224.0.0.24	Adresse du groupe de serveurs WINS