

NFA083 – Réseau et Administration Web

TCP/IP

Sami Taktak

sami.taktak@cnam.fr

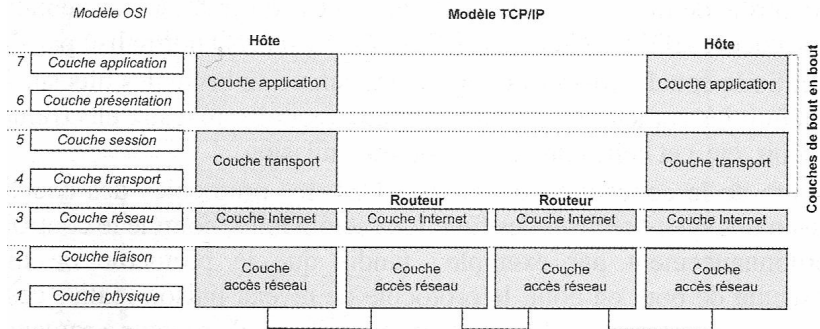
Centre d'Étude et De Recherche en Informatique et Communications
Conservatoire National des Arts et Métiers



le **cnam**

- Initialement conçu pour ARPANET
- Définit l'architecture des réseaux de l'Internet
- Normalisé par l'IETF
- TCP/IP :
 - TCP : *Transport Control Protocol*
 - IP : *Internet Protocol*
- Constitué de 4 couches

Modèle TCP/IP



Dénomination des unités de données :

- Bit au niveau physique
- Trame au niveau liaison
- Paquet ou datagramme au niveau réseau
- Segment au niveau transport
- Information au niveau application

- N'est pas normalisée par IETF
- Normalisée par d'autres organismes : IEEE, ISO, UIT, ...
- Réseaux locaux :
 - Ethernet (IEEE 802.3)
 - WiFi (IEEE 802.11)
- Réseaux d'opérateurs :
 - X25 (UIT)
 - ATM (UIT)

- Protocole IP :
 - En charge de l'adressage et du routage des paquets
 - Fonctionne en mode non connecté et non fiable
- Protocole TCP :
 - Mode connecté et fiable
 - Retransmission de paquets en cas de perte
 - Garantit la réception des paquets dans l'ordre
 - Contrôle de flux
 - Contrôle de congestion
- Protocole UDP (*User Datagram Protocol*) :
 - Mode non connecté
 - Non fiable

- Protocole TCP :
 - Adapté aux applications n'ayant pas de contrainte de temps mais exigeant des données intègres
 - Exemple :
 - Protocole de transfert de fichiers, FTP
 - Protocole de messagerie, SMTP, POP, IMAP
 - Consultation de page web, HTTP
- Protocole UDP :
 - Adapté aux applications temps réel
 - Téléphonie sur IP
 - Vidéo-conférences

Protocole IP

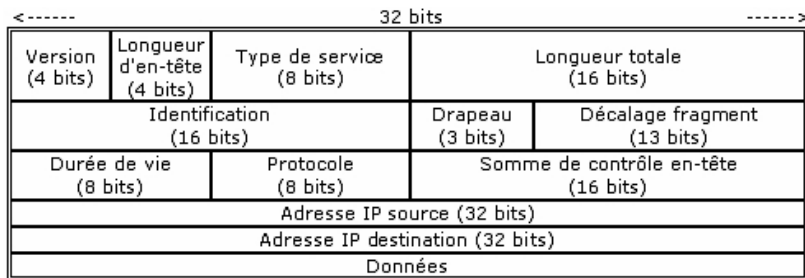
- Fournir une méthode d'*adressage* unique et universelle des machines sur Internet : l'adresse IP
- Assurer une fonction de *routage* des paquets sur le réseau à partir de l'adresse IP
- Assurer l'interface entre les couches hautes et basses, notamment par la fragmentation et le réassemblage des données

Protocoles niveau réseau complémentaires

- ICMP (*Internet Control Message Protocol*) : assure la gestion du réseau en fournissant des messages concernant les erreurs et les demandes d'information
- IGMP (*Internet Group Message Protocol*) : protocole assurant le routage de groupe ou multicast
- ARP (*Adresse Resolution Protocol*) : protocole prenant en charge la résolution d'une adresse IP en adresse MAC

- IP (*Internet Protocol*) : initialement décrit dans la RCF 791 en 1981
- 2 versions du protocole cohabitent sur Internet : IPv4 et IPv6
- Protocole exécuté sur les hôtes et les routeurs
- Protocole sans connexion
- Non fiable (pas d'acquittement), pas de contrôle de flux, pas de contrôle de congestion
- Prend en charge le routage, l'adressage, la fragmentation et le réassemblage des paquets IP appelés *datagrammes IP*

Format du Datagramme IP



Format du Datagramme IP

- *Version* (4 bits) : indique la version du protocole IP utilisée (4 pour IPv4, 6 pour IPv6)
- *Longueur d'en-tête* (4 bits) : indique la longueur de l'en-tête en multiple de mots de 4 octets
- *Type de service* (8 bits) : champ ayant beaucoup évolué depuis 1981 ; prévu pour le routage avec qualité de service
- *Longueur total* (16 bits) : longueur totale en octets de datagramme
- *Identification* (16 bits) : numéro identifiant le datagramme
- *Drapeau* (3 bits) : Indique si la fragmentation est autorisée et, le cas échéant, si le paquet est le dernier de la fragmentation

Format du Datagramme IP

- *Décalage de fragment* (13 bits) : numéro de fragment
- *Durée de vie* (TTL : *Time to live*) (8 bits) : décrémentée à chaque saut ; datagramme détruit si TTL = 0
- *Protocole* (8 bits) : numéro identifiant le protocole encapsulé dans le datagramme IP normalisé par l'IANA ; protocoles courants : ICMP :1, IGMP :2 ; IP :4 ; TCP :6 ; UDP :17 ; IPv6 :41
- *Somme de contrôle* (16 bits) : calculée sur les mots de 16 bits formant l'en-tête
- Adresse IP source (32 bits) : adresse IP de l'équipement source du datagramme
- Adresse IP destination (32 bits) : adresse IP de l'équipement destination du datagramme

Structure des Adresses IPv4

- Adresses codées sur 4 octets (32 bits)
- Écrite en notation décimale pointée : valeur décimale de chaque octet séparée par un point (192.168.0.1)
- Adresse découpée en 2 parties :
 - Première partie identifiant le réseau, généralement appelée « *préfixe réseau* » ; notée *Net-id* dans la suite
 - Deuxième partie identifiant l'équipement dans le réseau ; notée *Host-id* dans la suite

Soit N le nombre de bits alloués au *Net-id* et H le nombre de bits alloués au *Host-id* :

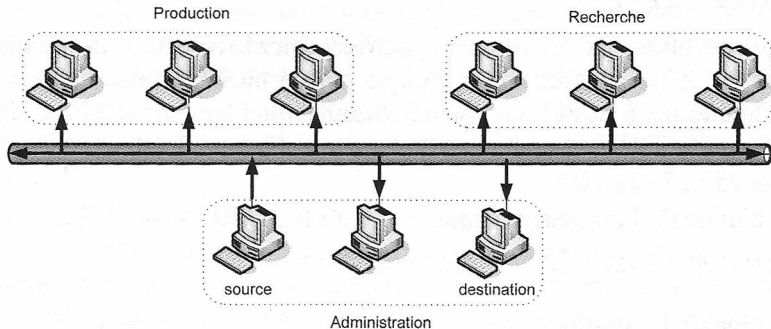
- Nombre de réseaux différents pouvant être créés : 2^N
- Nombre d'adresses disponibles pour les équipements : $2^H - 2$

Adresses Particulières

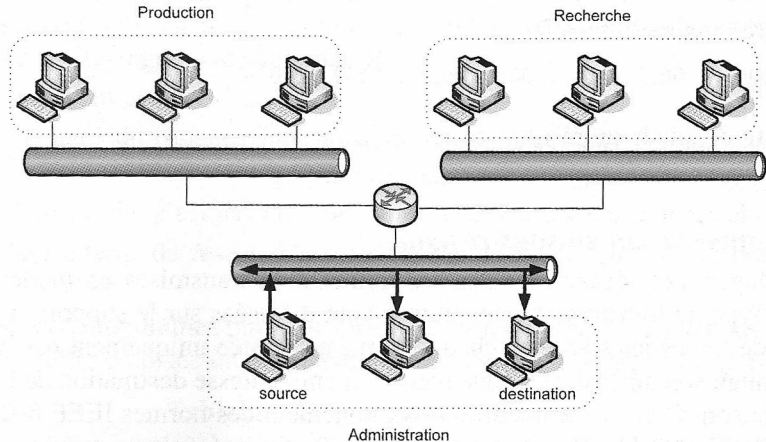
- Notation CIDR (*Classless Inter Domain Routing*)
- 0.0.0.0 : adresse utilisée pour indiquer n'importe quelle adresse
- Net-id, Host-id=0 : adresse du réseau (Host-id = 0), ex. 192.168.0.0/24
- Net-id, Host-id avec tous les bits à 1 : adresse de diffusion dans le réseau Net-id, ex. 192.168.255.255
- 255.255.255.255 : broadcast local (non relayé par les routeurs)
- Net-id=127, Host-id \neq 0 : adresse locale (*loopback* ou *loaclhost*)
- Adresses privées :
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16



Exemple de Segmentation en Sous-Réseaux



Exemple de Segmentation en Sous-Réseaux



Segmentation du réseau d'adresse 193.55.44.0/24 en 3 sous-réseaux

- Segmentation réalisée en partageant les bits de Host-id en deux parties : une identifiant les sous-réseaux (bits de poids fort), l'autre les hôtes du sous-réseaux
- 2 bits de Host-id nécessaires pour créer 3 sous-réseaux
- Valeurs possibles pour le 4^e octet :
 - Valeur binaire : 0000 0000, valeur décimale : 0
 - Valeur binaire : 0100 0000, valeur décimale : 64
 - Valeur binaire : 1000 0000, valeur décimale : 128
 - Valeur binaire : 1100 0000, valeur décimale : 192



Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	
193.55.44.64/26		
193.55.44.128/26		
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26		
193.55.44.128/26		
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	
193.55.44.128/26		
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	255.255.255.192
193.55.44.128/26		
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	255.255.255.192
193.55.44.128/26	193.55.44.191	
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	255.255.255.192
193.55.44.128/26	193.55.44.191	255.255.255.192
193.55.44.192/26		

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	255.255.255.192
193.55.44.128/26	193.55.44.191	255.255.255.192
193.55.44.192/26	193.55.44.255	

Exemple de Segmentation en Sous-Réseaux

- 4 adresses de sous-réseaux possibles :
 - Adresse réseau : 193.55.44.0/26
 - Adresse réseau : 193.55.44.64/26
 - Adresse réseau : 193.55.44.128/26
 - Adresse réseau : 193.55.44.192/26
- Adresse de diffusion et masques des sous-réseaux :

Sous-réseau	Adresse de diffusion	masque
193.55.44.0/26	193.55.44.63	255.255.255.192
193.55.44.64/26	193.55.44.127	255.255.255.192
193.55.44.128/26	193.55.44.191	255.255.255.192
193.55.44.192/26	193.55.44.255	255.255.255.192

Émission d'un datagramme

Lors de l'émission, le protocole IP réalise les opérations suivantes :

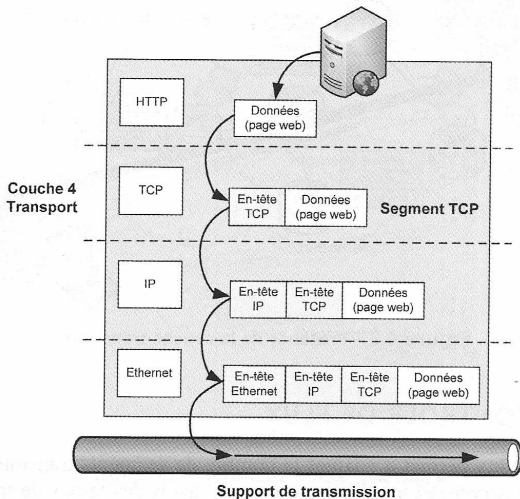
- Complète tous les champs de l'en-tête
- Détermine le prochain saut pour le datagramme : c'est l'opération de routage
- Vérifie le type d'adresse : unicast ou broadcast
- Procède à la fragmentation du paquet si nécessaire
- Transmet le datagramme à la couche liaison

Nécessaire lorsqu'un datagramme doit traverser un réseau dont la taille maximum des trames (MTU, *Maximum Transmission Unit*) est inférieure à la taille du datagramme

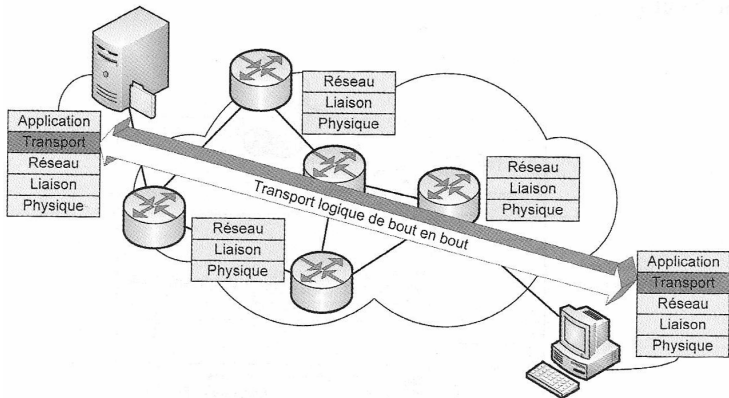
Exemple :

- MTU d'un réseau Ethernet : 1500
- MTU d'un lien PPPoE : 1492
- Souvent, Ethernet utilisé sur le réseau local, PPPoE utilisé sur les liens ADSL \Rightarrow Fragmentation obligatoire

Couche Transport



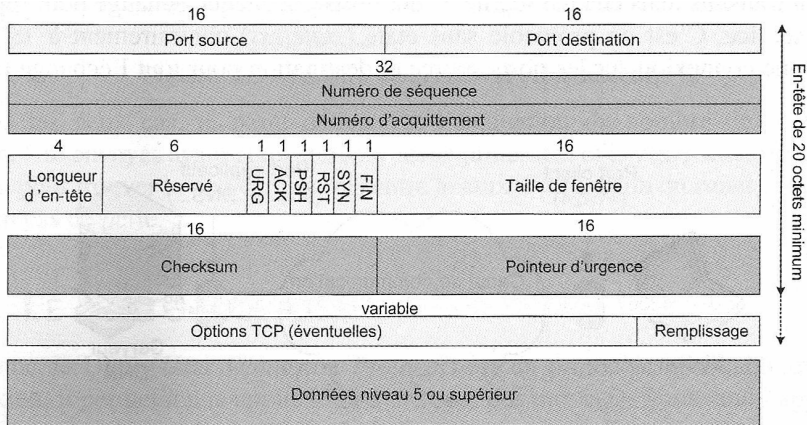
Couche Transport



TCP : *Transmission Control Protocol*

- Établissement et fermeture de la connexion virtuelle
- Segmentation et réassemblage des données
- Acquiescement des datagrammes reçus et retransmission sur absence d'acquiescement
- Reséquencement des datagrammes s'ils ne sont pas délivrés dans l'ordre
- Contrôle de flux
- Multiplexage des données issues de plusieurs processus hôtes en un même segment

TCP : Transmission Control Protocol



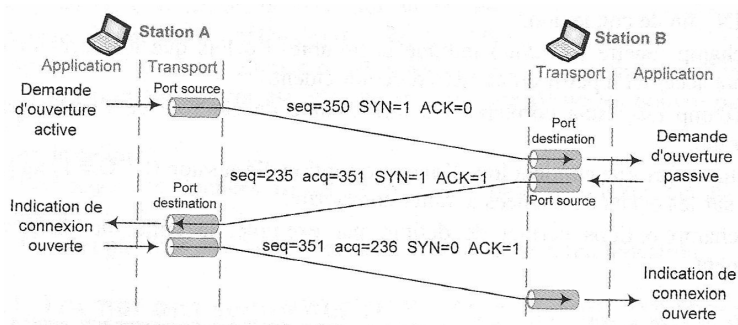
TCP : *Transmission Control Protocol*

- Numéro de port : permet d'identifier le service concerné (source ou destination)
- Numéro de séquence : indique le numéro du premier octet transmis dans le segment
- Numéro d'acquittement : numéro de séquence du prochain octet attendu par l'émetteur
- Longueur de l'en-tête (4 octets) : nombre de mots de 32bits constituant l'en-tête
- Champ fenêtre (16 bits) : nombre de d'octets pouvant encore être émis à partir du dernier acquittement reçu
- Champ *checksum* : somme contrôle de l'en-tête et du message
- Champ priorité (16 bits) : lors d'un interruption, pointeur sur les octets à traiter en priorité

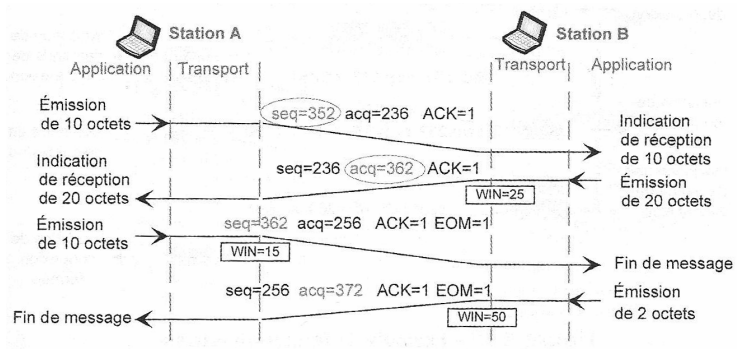
TCP : *Transmission Control Protocol*

- Champ option : définit par exemple la taille maximum d'un segment
- Bits de contrôle : permettent de définir la fonction des messages ainsi que la validité de certains champs
 - URG=1 : si champ des priorités est utilisé (pour demande d'interruption d'émission par exemple)
 - ACK=1 : si la valeur du champ acquittement est significative
 - EOM ou PSH : indique une fin de message (*End Of Message*), les données doivent être transmises (*pushsed*) à la couche supérieure
 - RST (*Reset*) : demande de réinitialisation de la connexion
 - SYN : demande d'ouverture de connexion
 - FIN : fin de connexion

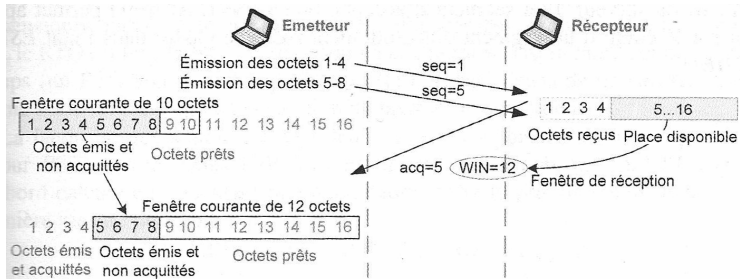
TCP : Établissement d'une Connexion



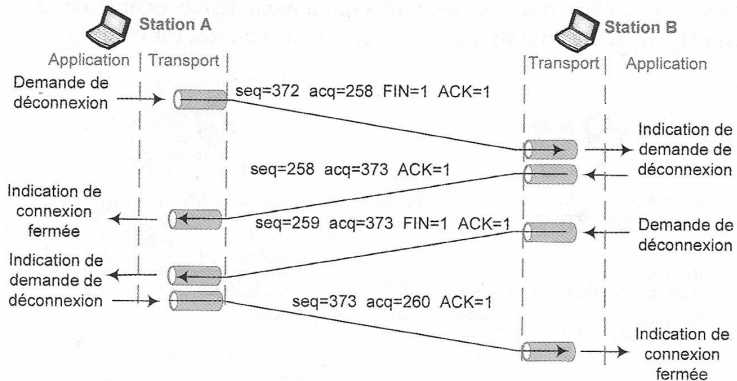
TCP : Échange TCP



TCP : Gestion de la Fenêtre d'Émission



TCP : Fermeture d'une Connexion

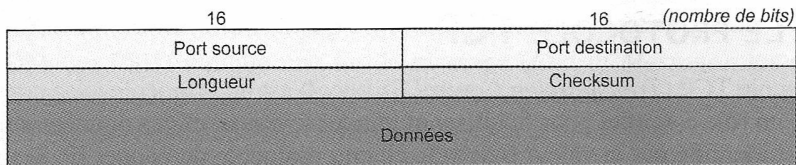


UDP : *User Datagram Protocol*

- Protocole non fiable
- Sans connexion
- Pas de contrôle de flux
- Fonctionnalité simple : permet d'envoyer un message d'une application à une autre sans garantie
- Permet de désigner les ports source et destination
- Protocole sans état (*stateless*)

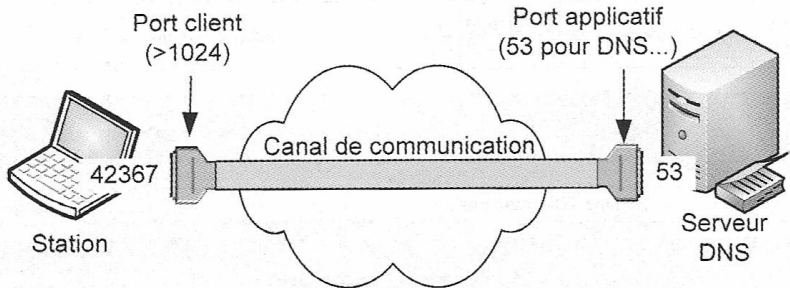


Format du Datagramme UDP



- Port sources et Port destination (16 bits chacun) : permettent de désigner les applications sources et destinations du message
- Longueur (16 bits) : longueur totale du message (données et entête) en octets
- Checksum (16 bits) : somme de contrôle
- Données : de taille variable

Format du Datagramme UDP

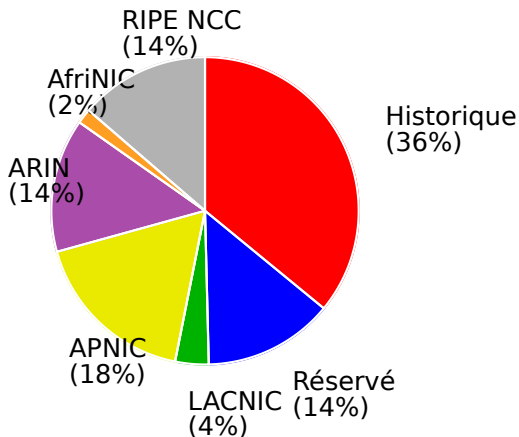


- IPv4 définit une plage d'adressage de 4 milliards d'adresses
- Semblait largement suffisant au début d'Internet (années 1970)
- Une partie des adresses non utilisables :
 - Utilisation privée
 - Multicast (adresse entre 224.0.0.0 et 239.255.255.255)
 - Adresses réservées (entre 240.0.0.0 et 255.255.255.255)
 - Adresses particulière (adresse de réseaux, de broadcast...)
 - Mais aussi pour raison historique : mauvaise attributions des ressources (allocation de réseau de classe A)

5 classes d'adresses IP :

- utilisé jusque dans les années 1990
- Classe A, 1 octet pour le Net-id :
 - $2^{24} - 2$ adresses \approx 16 millions d'adresses
 - exemple : 10.0.0.0/8
- Classe B, 2 octets pour le Net-id :
 - $2^{16} - 2$ adresses = 65 534 adresses
 - exemple : 172.16.0.0/16
- Classe C, 3 octets pour le Net-id :
 - $2^8 - 2$ adresses = 254 adresses
 - exemple : 192.168.1.0/24
- Réseaux de classe A entiers distribués à des entreprises et des organisations

Allocation des blocs IPv4



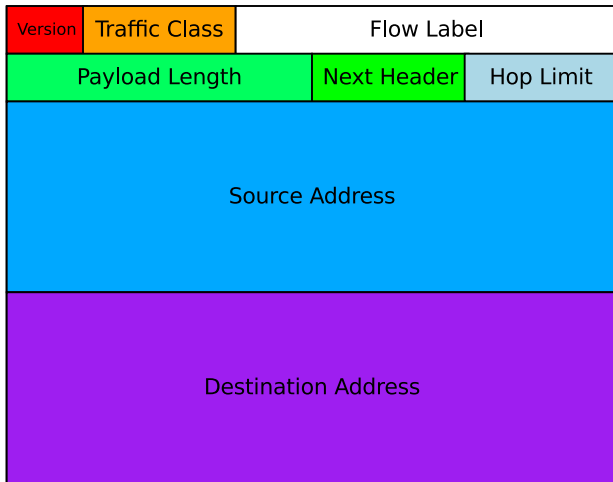
- 3 février 2011 : annonce par l'IANA de la distribution des 5 derniers blocs d'adresses
- 15 avril 2011 : annonce par l'APNIC qu'il ne dispose plus que d'1 bloc /8
- 14 septembre 2012 : annonce par le RIPE NCC qu'il ne dispose plus que d'1 bloc /8
- Épuisement prévu entre 2013 et 2015 pour les autres registres régionaux (RIR)

- IPv6 (*Internet Protocol version 6*) : protocole réseau sans connexion de la couche 3 du modèle OSI (*Open Systems Interconnection*)
- Développé au cours des années 1990 sein de l'IETF
- Ses spécifications finalisées dans la RFC 2460 en décembre 1998
- Augmentation de 2^{32} à 2^{128} du nombre d'adresse soit 667 millions de milliards d'adresses IP par mm^2 de la surface de la Terre
- Mécanisme de configuration et de renumérotation automatique
- Mécanisme de sécurisation des communications, de qualité de service et de multicast
- Simplification des en-têtes de paquets pour faciliter le routage



- Adresse 128 bits au lieu de 32 bits
- Mécanismes d'attribution automatique des adresses
- IPsec fait partie des spécifications de base du protocole
- En-tête du paquet IPv6 simplifié
- Adresses locales facilitant l'interconnexion de réseaux privés

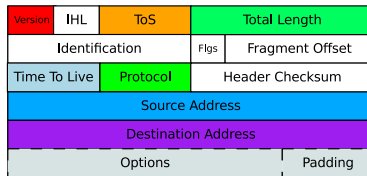
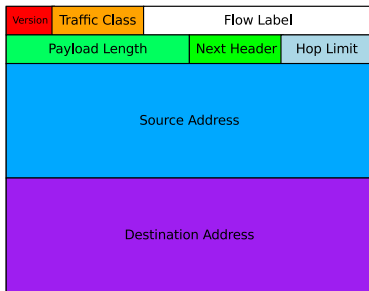
En-tête IPv6



- *Version* (4 bits) : fixé à la valeur du numéro de protocole Internet, 6
- *Traffic Class* (8 bits) : utilisé pour la qualité de service
- *Payload length* (16 bits) : taille des données en octets
- *Next Header* (8 bits) : spécifie le type d'en-tête suivant (en-têtes d'extension additionnels optionnels)
- *Hop Limit* : nombre maximum de sauts
- Adresse source et adresse destination

⇒ En-tête simplifié par rapport à l'en-tête IPv4

Comparaison des En-têtes IPv6 et IPv4



- Adresse sur 128 bits \Rightarrow 16 octets
- Notation hexadécimale : 8 groupes de 2 octets séparés par « : »
 - 2001:0db8:0000:85a3:0000:0000:ac1f:8001
 - 2001:db8:0:85a3::ac1f:8001
- Utilise la notation CIDR :
 - 2001:db8:1f89::/48 représente le bloc d'adresse commençant à 2001:db8:1f89:0:0:0:0:0 et finissant à 2001:db8:1f89:ffff:ffff:ffff:ffff:ffff.

Découpage de l'Espace d'Adressage IPv6

Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fe80::/10	Adresses locales lien
ff00::/8	Adresses multicast

source : RFC 4291 – IP Version 6 Addressing Architecture

Structure des Adresses Unicast Globales

Champ	préfixe	sous-réseau	interface
Bits	48	16	64

- Préfixe : représente la partie réseau vue de l'extérieur du site (*topologie publique*)
- sous-réseau : représente la segmentation en sous-réseau connue qu'à l'intérieur du site (*topologie privée*)
- Interface : partie identifiant une machine dans le réseau (Host-id)

Adresse IPv6 Spécifiques

- `::/128` est l'adresse non spécifiée, équivalent à `0.0.0.0` en IPv4
- `::1/128` est l'adresse localhost, équivalent à `127.0.0.1` en IPv4
- Adresses ouvertes à la réservation depuis 1999 :
`2001::/16`
- Adresses 6to4 `2002::/16` permettant d'acheminer du trafic IPv6 via des réseaux IPv4
- Adresses multicast `ff00::/8`
- Adresses lien local : `fe80::/10`