Cours 3 : Protocoles IP et protocoles associés

Module R4 : Technologie IP

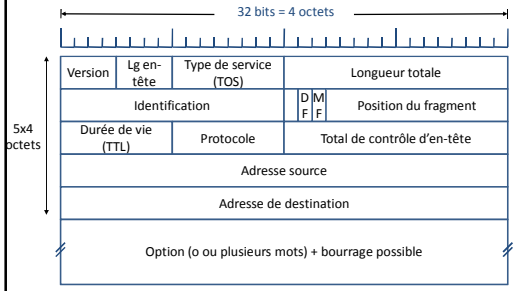
IUT R&T 1ère année

David Mercier

Plan

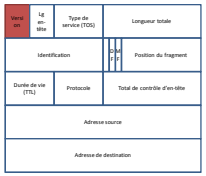
- Protocole IPv4
  - Format des datagrammes
  - Fragmentation IP
  - ICMP : protocole de messages de contrôle de l'Internet
  - ARP : protocole de résolution d'adresses
  - RARP / BOOTP / DHCP
- Protocole IPv6

Format de l'en-tête IPv4



Datagramme IPv4

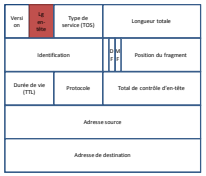
Champ Version



- Sur **4 bits** (représenté par 1 chiffre hexadécimal)
- Indique la version du protocole ip utilisé
  - Est égal à 4 (ipv4) ou 6 (ipv6)

Datagramme IPv4

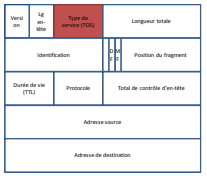
Champ Longueur en-tête (IHL)



- Sur **4 bits** (représenté par 1 chiffre hexadécimal)
- **Longueur de l'en-tête en mots de 32 bits**
- En-tête minimal = 20 octets correspond à un champ longueur d'en-tête égal à 5.
- Valeur maximale 15 (soit un en-tête de 60 octets).

Datagramme IPv4

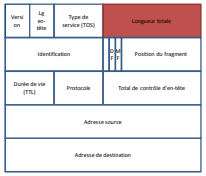
Champ Type de service (TOS)



- Sur **1 octet** (représenté par 2 chiffres hexadécimaux)
- Sert à distinguer **différentes classes de service** (différentes combinaisons de **fiabilités** et **débits** possibles)
- Dans la pratique, les routeurs actuels l'**ignorent**.

Datagramme IPv4

Champ Longueur totale (TL)

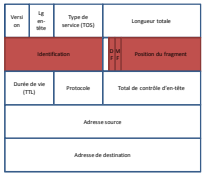


- Sur **2 octets** (représenté par 4 chiffres hexadécimaux)
- Indique la **longueur du datagramme** (en-tête et données comprises)
- Valeur maximale :
  2^16-1 = 65535 octets
- Suffisant actuellement, mais les réseaux gigabits futurs nécessitent des datagrammes plus longs.

7

Datagramme IPv4

La fragmentation

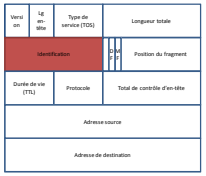


- Concernent la fragmentation d'un paquet IP
- **MTU** (Maximum Transmission Unit) = **taille maximale** (en octets) du **paquet** pouvant être transmis en une seul fois.
- Ex : MTU sur Ethernet = 1500 octets

8

Datagramme IPv4

Champ Identification

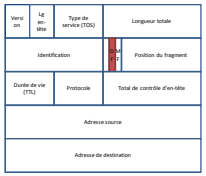


- Sur **2 octets** (représenté par 4 chiffres hexadécimaux)
- Permet à l'hôte destinataire de **déterminer** à quel **datagramme** appartient un fragment reçu.
- Tous les fragments d'un datagramme contiennent la même valeur d'identification.

9

Datagramme IPv4

Bit DF

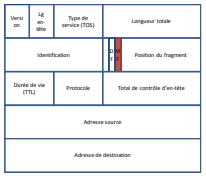


- Bit DF : *don't fragment*
- L'émetteur du datagramme ordonne que le paquet ne soit pas fragmenté

10

Datagramme IPv4

Bit MF

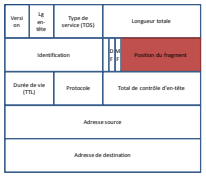


- Bit MF : more *fragment*
- Est activé dans tous les fragments d'un datagramme excepté le dernier.

11

Datagramme IPv4

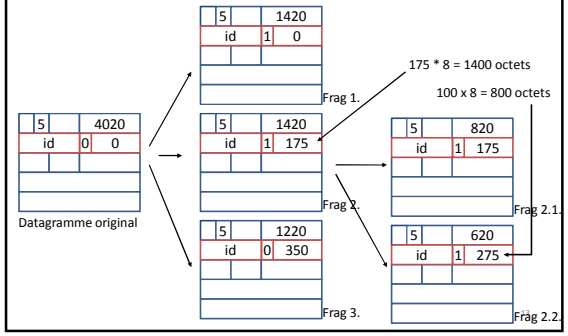
Champ Position du fragment



- Sur **13 bits** (il faut regarder 2 chiffres hexadécimaux)
- Indique la **position du fragment** dans le datagramme IP.
- Tous les **fragments** d'un datagramme, à l'exception du dernier, doivent être un **multiple de 8 octets**, l'unité élémentaire.

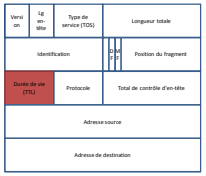
12

Exemple de fragmentation



Datagramme IPv4

Champ Durée de vie (TTL)

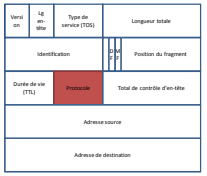


- Sur **1 octet** (représenté par 2 chiffres hexadécimaux)
- Supposé compter le temps en seconde
- Il doit être décrémenté de 1 à chaque saut et plusieurs fois si temps d'attente dans une file.
- En pratique, il **compte seulement le nombre de saut**.
- Lorsqu'il atteint 0, le datagramme est éliminé.
- Nombre de saut maximum : 255

14

Datagramme IPv4

Champ Protocole

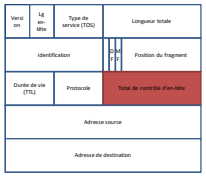


- Spécifie le protocole encapsulé
- Ex :
  - 1 = 0x01 : ICMP
  - 2 = 0x02 : IGMP
  - 6 = 0x06 : TCP
  - 17 = 0x11 : UDP
  - 89 = 0x59 : OSPF

15

Datagramme IPv4

Champ Total de contrôle d'en-tête

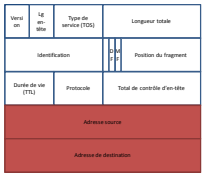


- Sur 2 octets (représenté par 4 chiffres hexadécimaux)
- Sert à vérifier l'en-tête uniquement.

16

Datagramme IPv4

Champs adresses



- Chaque adresse est sur **4 octets** (représenté par 8 chiffres hexadécimaux)
- Spécifient l'**adresse IP source** et l'**adresse IP de destination** du datagramme
- Voir cours 1 pour rappel sur les adresses IP.

17

Datagramme IPv4

Champ options

- Prévu pour ajouter des informations
- Longueur des options variables
- Rarement exploitées
- Liste complète des options : www.iana.org/assignments/ip-parameters.

18

Datagramme IPv4

Certaines options IP

Option	Description
Sécurité	Indique le degré de confidentialité du datagramme
Routage strict par la source	Décrit le chemin complet à suivre
Routage lâche par la source	Donne une liste de routeurs incontournables
Enregistrement de route	Oblige chaque routeur à ajouter son adresse IP au datagramme
Horodatage	Oblige chaque routeur à ajouter son adresse IP au datagramme et une horodate au datagramme

19

Protocoles de contrôle de l'Internet

- IP sert à la transmission des données
- Plusieurs protocoles de contrôle exécutés dans la couche réseau tels que :
  - ICMP
  - ARP
  - RARP
  - BOOTP
  - DHCP

20

ICMP (RFC 792)
Internet Control Message Protocol

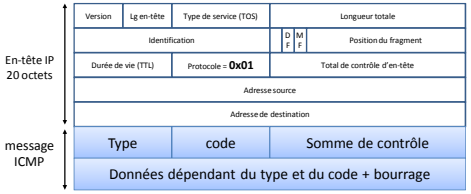
- IP non fiable…
- Permet d'envoyer des messages de contrôle (**erreurs**, **congestions**..)
- Si un routeur détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour **informer l'émetteur initial**
- Une erreur engendrée par un message ICMP ne peut pas donner naissance à un autre message ICMP (pas d'effets cumulatifs)
- Utilisé par des utilitaires (*ping*, *traceroute*, …)

21

ICMP

Datagramme

- Encapsulé dans un paquet IP



- Liste complète des types de messages ICMP : www.iana.org/assignments/icmp-parameters.

22

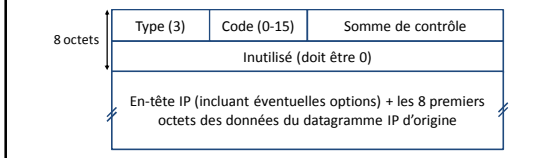
ICMP

Principaux types de messages ICMP

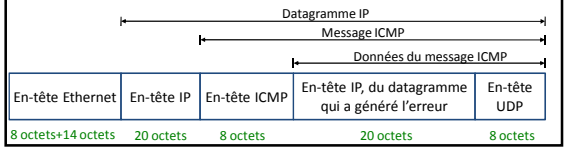
Type de message	Description
Type = 3, Code : 0 à 15 Destination inaccessible	Paquet n'a pu être livré (Ex : destination non localisable, pb bit DF)
Type = 11, Code : 0 à 1 Délai expiré	TTL = 0
Type = 12, Code : 0 En-tête erroné	Champ d'en-tête invalide
Type = 4, Code : 0 Ralentissement de la source	Paquet de rétention (servait initialement à contenir les hôtes envoyant trop de paquets). Le contrôle de congestion est maintenant assuré par la couche transport (cours 4)
Type = 5, Code : 0 à 3 Redirection	Indication d'une meilleure route
Type = 8, Code = 0 Demande d'écho	Demande à une machine si elle est active
Type = 0, Code = 0 Envoi d'écho	La machine distante est active

Exemple

Message ICMP « inaccessible »



Exemple message ICMP retourné du fait d'un **port UDP inaccessible** :



ICMP

Quelques failles ICMP connues

- Les messages ICMP de type 3 pour les codes 2 ou 3 (voire 4) peuvent clore une connexion TCP
- Un envoi répété de message ICMP de type 4 (code 0) ralentit grandement le débit d'une connexion
- Le message ICMP de type 3 pour le code 4 ralentit une connexion en passant le MTU au minimum (68 octets) puis en l'augmentant progressivement

Commande ping

- Envoi d'un paquet ICMP demande d'écho (type 8 echo-request), attente de réponse, mesure du temps aller-retour.
- **Exécution** de la commande
  - Linux :

    ping [-c nbre_de_ping_voulu] @IP ou nom d'hôte

  - Windows :

```
C:\>ping -n 1 cache-etu.univ-artois.fr

Envoi d'une requête 'ping' sur cache-etu.univ-artois.fr [193.49.62.52] avec 32 octets de données :

Délai d'attente de la demande dépassé.

Statistiques Ping pour 193.49.62.52:
    Paquets : envoyés = 1, reçus = 0, perdus = 1 (perte 100%),
```


Commande traceroute

- Principe :
  - Envoie de paquets ICMP echo-request type 8 avec un TTL de plus en plus grand (en commençant à 1).
  - Chaque routeur recevant un paquet IP en décrémente le TTL. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur (type 11, code 1).
  - Traceroute découvre ainsi les routeurs de proche en proche.
  - Il existe des variantes avec l'emploi de paquets UDP ou TCP.
- Sous Windows : commande équivalente tracert
- Il existe de nombreux outils graphiques d'analyse réseau :
  - Etherape, The Dude, NetPerf, Cheops

Tracert www.u-tokyo.ac.jp

```
Détermination de l'itinéraire vers www.u-tokyo.ac.jp [133.11.114.194]
avec un maximum de 30 sauts :

  1   41 ms   40 ms   40 ms  88.160.34.254
  2   41 ms   40 ms   46 ms  lille-6k-1-a5.routers.proxad.net [213.228.12.190]
  3   44 ms    *       *     cbv-6k-2-v800.intf.routers.proxad.net [212.27.50.117]
  4   49 ms   44 ms   45 ms  th2-crs16-1-be1003.intf.routers.proxad.net [212.27.58.1]
  5   46 ms   46 ms   45 ms  xe-11-1-0.edge3.Paris1.Level3.net [212.73.207.13]
  6   46 ms   55 ms   51 ms  ae-31-53.ebr1.Paris1.Level3.net [4.68.109.94]
  7   59 ms   52 ms   54 ms  ae-2.ebr1.London2.Level3.net [4.69.133.94]
  8   64 ms   55 ms   51 ms  ae-45-105.ebr2.London2.Level3.net [4.69.141.118]
  9   66 ms   52 ms   54 ms  ae-2.ebr1.London1.Level3.net [4.69.132.146]
 10   56 ms   54 ms   54 ms  ae-1-100.ebr2.London1.Level3.net [4.69.132.118]
 11  119 ms  119 ms  120 ms  ae-41-41.ebr1.NewYork1.Level3.net [4.69.137.66]
 12  122 ms  126 ms  125 ms  ae-71-71.csw2.NewYork1.Level3.net [4.69.134.70]
 13  123 ms  120 ms  121 ms  ae-2-79.edge1.NewYork1.Level3.net [4.68.16.78]
 14  120 ms  120 ms  125 ms  JAPAN-TELEC.edge1.NewYork1.Level3.net [4.78.132.18]
 15  298 ms  296 ms  301 ms  tokyo1-dc-RM-P-2-3-0-11.sinet.ad.jp [150.99.203.57]
 16  298 ms  299 ms  298 ms  UTnet-1.gw.sinet.ad.jp [150.99.190.102]
 17  299 ms  300 ms  299 ms  ra3a-gi1-0-0.nc.u-tokyo.ac.jp [133.11.206.146]
 18  309 ms  310 ms  309 ms  ra39-vlan336.nc.u-tokyo.ac.jp [133.11.206.153]
 19  295 ms  298 ms  299 ms  ra35.nc.u-tokyo.ac.jp [133.11.127.41]
 20  297 ms  297 ms  297 ms  www.u-tokyo.ac.jp [133.11.114.194]

Itinéraire déterminé.
```

Traversée de l'Atlantique ≈ 120-54= 66ms

Traversée du Pacifique ≈301-125= 176ms

ARP (RFC 826)
Address Resolution Protocol

- Les équipements de liaison (cartes réseau ...) utilisent des adresses physiques (MAC).
- Problème : ils ne comprennent pas les adresses IP.
- Besoin d'associer @MAC et @IP.
- **ARP**, protocole de résolution d'adresses, permet la correspondance @IP -> @MAC

Illustration sur un exemple

3 réseaux de classe C - /24 - interconnectés

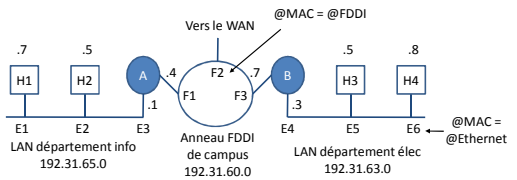


Illustration sur un exemple

Envoie d'un message de H1 vers H2

- La **1ière étape** consiste à **obtenir l'@IP** de H2 à partir de son nom (protocole **DNS** – couche application)
- Le logiciel de la couche supérieur peut alors **générer un paquet** incluant l'**@IP de H2** 192.31.65.5 dans la champ *adresse de destination*, et le passer au logiciel IP pour qu'il l'expédie.
- Ce dernier **examine l'@IP** et constate qu'elle se trouve sur **son réseau**. Il a besoin de l'**@MAC**.
- Deux solutions envisagées :
  1. Un fichier de configuration @MAC <-> @IP (problèmes : m-à-j, erreurs, bcp de temps,…)
  2. Plus efficace : protocole **ARP**. H1 envoie sur son réseau un **paquet broadcast** « À qui appartient l'adresse 192.31.65.5 ? ». Chaque hôte regarde son @IP, celui qui à cette @IP lui répond.

31

ARP

Fonctionnement

- Si la machine source et destinataire sont sur le même réseau (Ex : H1 vers H2)
  - Requête ARP : broadcast who-has @ IP?
  - Réponse ARP : destinataire a reçu le broadcast et s'est reconnu, il envoie son @MAC : @ip is-at …
  - La source peut envoyer ses données vers le destinataire (adresse MAC destination connue)
- Si elles ne sont pas sur le même réseau (Ex : H1 vers H4)
  - La **diffusion ne passe pas le routeur**
  - **Résolution de proche en proche** :
    - E1 envoie les données à 192.31.65.1 (ARP pour trouver E3),
    - le routeur info envoie les données à 192.31.60.7 (ARP pour trouver F3),
    - le routeur elec envoie les données à 4 (ARP pour E6)

32

ARP

Optimisations

- **Cache ARP** : le résultat de chaque résolution est conservé pour les émissions suivantes (**commande arp** : arp -a)
- Actualisation dynamique des correspondances (remplacement d'une carte Ethernet,…) les entrées du cache ARP doivent expirer au bout d'un certain temps
- La correspondance (@IP,@MAC) de l'émetteur sont inclus dans la requête ARP pour le récepteur, voire toutes les machines qui reçoivent le broadcast, qui mettent à jour leur cache.
- Utilisation d'un **proxy ARP** : une machine qui répond à la place du destinataire (qui ne reçoit pas le broadcast). Fait directement le lien.
- Solution nécessaire si la route (adresse de la passerelle) pour atteindre la destination n'est pas connue.

33

Datagramme ARP

- Encapsulé dans une trame Ethernet, FDDI, TR...
- ARP n'est pas limité au protocole Ethernet.

Type Mat. 2 octets	Type prot. 2 octets	Taille @Mat 1 octet	Taille @prot. 1 octet	Code op. 2 octets	@M src	@P src	@M dest	@P dest

Ex :
01 – Ethernet
02 – Experimental Ethernet
06 - IEEE 802 Networks
16 - Asynchronous Transmission Mode (ATM)

Ex :
0x0800 - IP

Ex :
01 - Token Ring
06 - Ethernet

Ex :
04 - IP v4
16 - IP v6

Ex :
01 – requête ARP
02 – réponse ARP

34

Exemple 1 : trame Ethernet contenant une requête ARP

« Qui a x.y.z.t ? » (arp who-has x.y.z.t tell a.b.c.d ?)

Type Mat. 0x0001	Type prot. 0x0800	Taille @Mat 0x06	Taille @prot. 0x04	Code op. 0x0001
@Mac src 6 octets (01:23:45:67:89:ab)				@ IP src 4 octets (a.b.c.d)
@Mac dest 6 octets (FF:FF:FF:FF:FF:FF)				@ IP dest 4 octets (x.y.z.t)

Code opération :

ARP request	0x0001
ARP reponse	0x0002
RARP request	0x0003
RARP reponse	0x0004

35

Exemple 1 (suite) : réponse ARP

« arp reply x.y.z.t is-at 00:11:22:33:44:55 »

Type Mat. 0x0001	Type prot. 0x0800	Taille @Mat 0x06	Taille @prot. 0x04	Code op. 0x0002
@Mac src 6 octets (00:11:22:33:44:55)				@ IP src 4 octets (x.y.z.t)
@Mac dest 6 octets (01:23:45:67:89:ab)				@ IP dest 4 octets (a.b.c.d)

Code opération :

ARP request	0x0001
ARP reponse	0x0002
RARP request	0x0003
RARP reponse	0x0004

36

Vulnérabilités issues de ARP

- Vulnérabilité à des attaques locales bien connues : pollution du cache ARP (ARP poisoning)
- De fausses informations sont envoyées (« arp is –at », « arp who-has »,), le cache arp ne contrôle pas les informations qui lui sont fournies (dépend de la mise en œuvre du protocole ARP par le SE).

37

RARP (RFC 903)
Reverse Address Resolution Protocol

- **ARP** : @IP ->@MAC **RARP**: @MAC -> @IP
- « Mon @MAC est xx:xx:xx:xx:xx:xx. Quelqu'un connait-il mon @IP ? »
- Permet à un hôte de récupérer son @IP au démarrage par interrogation d'un serveur RARP (station sans disque, imprimantes, ..)
- Même fonctionnement et même paquet
- **Obsolète** car désormais remplacé par BOOTP ou DHCP qui peuvent rendre le même service et ne nécessite pas de serveur RARP sur chaque réseau (**broadcast MAC limité**)

38

BOOTP (RFC 951)
Bootstrap Protocol

- Protocole d'amorçage du réseau au dessus de UDP (**les diffusions passent les routeurs**)
  - Le serveur informe la machine qui démarre de :
  - son @IP, @IP du serveur de fichiers qui contient son image disque, @IP du routeur par défaut, masque de sous-réseau
- **Inconvénients** : les tables de correspondances sont statiques (configurées manuellement).
- Pour y remédier, BOOTP est devenu Dynamic Host Configuration Protocol (DHCP)

39

DHCP (RFC 1531)
Dynamic Host Configuration Protocol

- Configuration manuelle ou assignation dynamique des adresses IP.
- Un serveur spécifique s'occupe d'assigner des configurations réseaux aux hôtes qui en font la demande.
- Le serveur n'est pas nécessairement sur le même réseau (passage par un relai DHCP).
- Permet aussi :
  - économie d'adresses IP : quand un hôte quitte le réseau, il restitue son adresse.
  - permet aux utilisateurs mobiles de rejoindre le réseau.

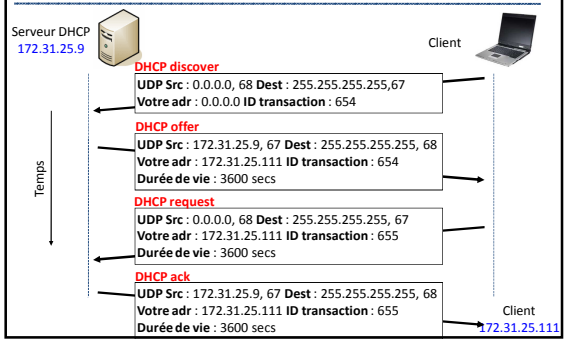
40

DHCP
Vue d'ensemble de l'obtention d'une adresse IP

- le poste diffuse un message (broadcast) DHCP discover
- le serveur DHCP répond avec le message (unicast) DHCP offer
- le poste diffuse une demande d'adresse IP [message DHCP request]
- le serveur DHCP envoie une adresse [message DHCP ack]

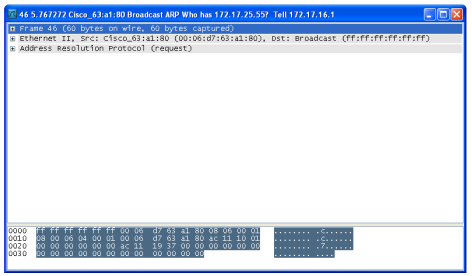
41

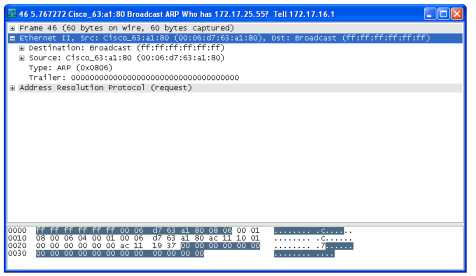
DHCP
Scénario d'attribution d'une adresse IP

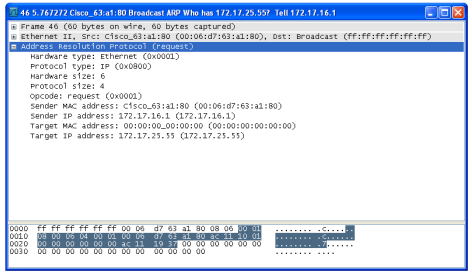


Quelques fichiers de configurations sous Linux

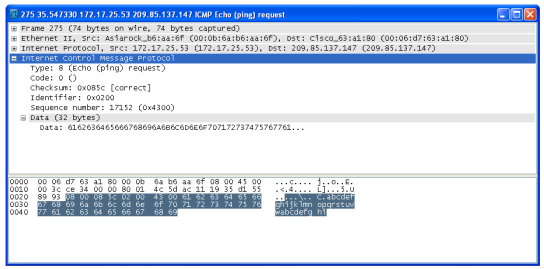
Fichier	Description	Exemple de contenu
/etc/hosts	donne un moyen d'assurer la résolution de noms	127.0.0.1 localhost localhost.localdomain 192.168.1.1 uranus.foo.org uranus
/etc/networks	permet d'affecter un nom logique à un **réseau**	localnet 127.0.0.0 foo-net 192.168.1.0
/etc/host.conf	donne l'ordre dans lequel le processus de résolution de noms est effectué	order hosts,bind
/etc/resolv.conf	permet d'affecter les serveurs de noms	nameserver 172.31.25.10 nameserver 193.49.62.9
/etc/network/interfaces	décrit les interfaces	Voir sur une machine de l'IUT.



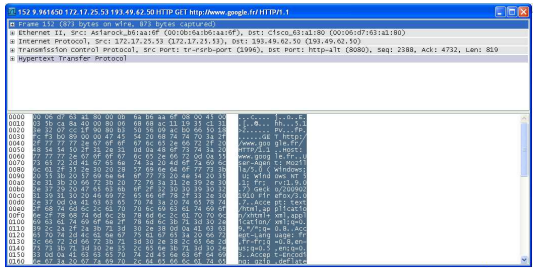




En-tête Ethernet	ARP	+ bourrage	Remorque Ethernet



En-tête Ethernet	En-tête IP	ICMP	Remorque Ethernet



En-tête Ethernet	En-tête IP	En-tête TCP	HTTP	Remorque Ethernet

Faiblesses IPv4

- Saturation du nombre d'adresses (Ipv4 subsiste encore que grâce aux techniques CIDR et NAT).
- Pas de sécurité
- Si une machine change de réseau, alors son adresse doit changer.

49

Objectifs d'IPv6

- Supporter des milliards d'hôtes, même avec une allocation inefficace des adresses, plus de pénurie…
- Réduire la taille des tables de routage
- Simplifier le protocole pour un traitement rapide des paquets par les routeurs
- Sécurité : confidentialité et authentification
- Accorder plus d'importance à la qualité de service (réservation de ressources)
- Support mobilité des machines
- Compatibilité avec IPv4
- Évolutif

50

De IPv4 à IPv6

IPv4
2^{32} addresses
(RFC 791, 1981)

IPv6
2^{128} addresses
(RFC 2460, 1998)

51

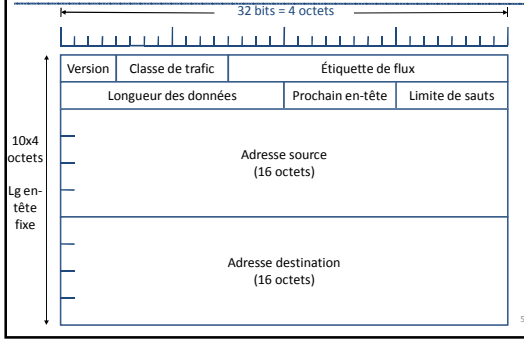
Quantité d'adresses IPv6

- $2^{128} = 2^{10x12+8} \approx 2^8.10^{36}$ soit plus de 256.10^{36} adresses..
- Si la terre était recouvert d'ordinateurs (y compris les étendues d'eau), IPv6 autoriserait $7x10^{23}$ adresses par m^2… (> nombre d'Avogadro)
- L'espace des adresses ne sera pas exploité efficacement. Résultat étude à partir des numéros de téléphone : 1000 adresses par m^2 dans le cas le plus pessimiste.

52

IPv6 (RFC 2460-2466)

En-tête IPv6



53

Description en-tête IPv6

- **Version** : 4 ou 6
- **Classe de trafic** : normal ou temps réel (trafic multimédia)
- **Étiquette de flux** (stade expérimental) : prévu pour établir des pseudo-connexions avec des propriétés et des exigences particulières (table de traitement spécifique dans routeurs)
- **Longueur des données** : ne compte pas les 40 octets d'en-tête (longueur en-tête fixe)
- **Prochain en-tête** : précise un en-tête facultatif (en-tête ipv6 simplifié en introduisant des en-têtes facultatifs). Si plus d'en-tête facultatif indique le protocole encapsulé.
- **Limite de sauts** = TTL d'IPv4 : décrémenté de 1 à chaque saut (plus d'ambiguïté sur le nom).

54

Adressage IPv6

- Adresses sur 16 octets noté de la manière suivante :
  8000:0000:0000:0000:0123:4567:89AB:CDEF
- Optimisations :
  8000:0000:0000:0000:123:4567:89AB:CDEF
  8000::123:4567:89AB:CDEF
- IPv4 :
  ::172.31.25.9

55

Passage graduel de IPv4 à IPv6

- IPv4 pas mis hors service du jour au lendemain.
- Progressivement des îlots migrent vers IPv6 communiquent entre eux via des tunnels.
- Tous ces îlots finiront par fusionner, et l'Internet sera totalement converti à IPv6.

56

Exercice

Quels sont les champs de l'en-tête IPv4 absents de l'en-tête IPv6 ?

57