Introduction

- **La couche réseau**
  - **Rôle** : amener les paquets de la source à la destination

fonctions

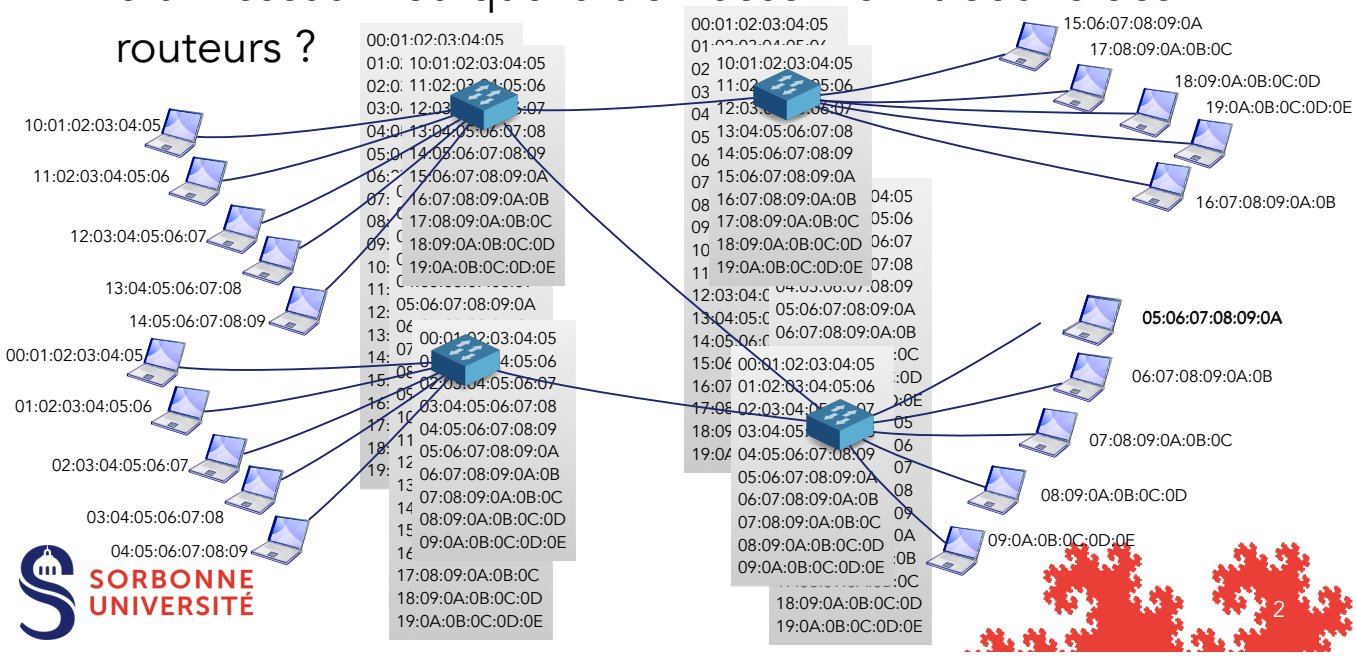
- **Gestion des adresses**
- **Choix du chemin approprié** (fonction de la topologie, du trafic)
- Contrôle de congestion (régulation du trafic).

  - **L'interface** entre la couche réseau et la couche transport est souvent l'interface entre le fournisseur de service et le client. Elle doit être clairement définie

SORBONNE UNIVERSITÉ

La couche réseau

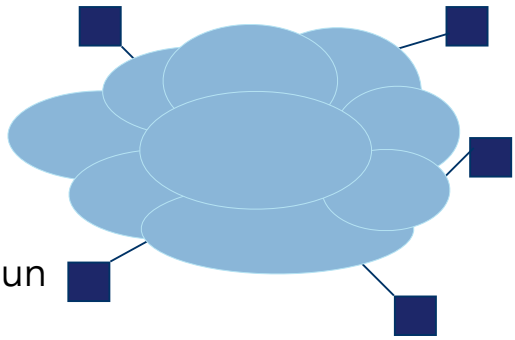
L'utilisation de VLAN permet d'étendre la couverture d'un réseau. Pourquoi a-t-on besoin d'introduire des routeurs ?



SORBONNE UNIVERSITÉ

Acheminement par datagramme

- A l'intérieur de chaque réseau, les nœuds utilisent la technologie spécifique de leur réseau (Ethernet, Wi-Fi, …)



- La couche réseau masque les spécificités et offre un service commun à toutes les applications, faisant apparaître l'ensemble de ces réseaux disparates comme un seul et unique réseau.

IP

Protocole en mode non connecté

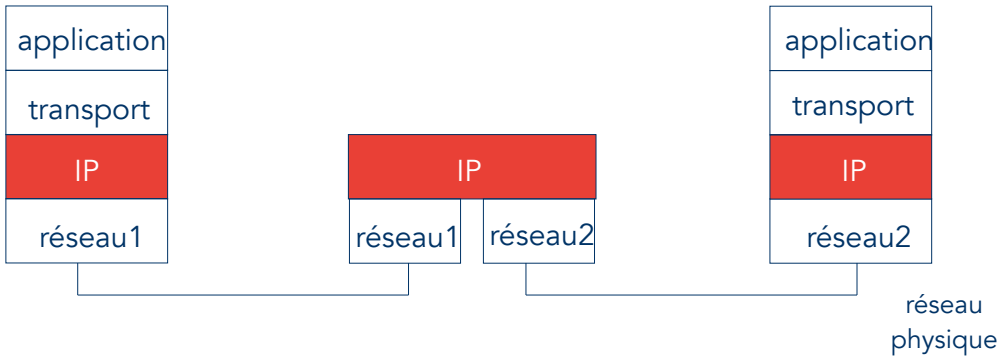
(= la colle qui relie l'Internet)

SORBONNE UNIVERSITÉ

Couche réseau

Acheminement par datagramme

Protocole IP : Internet Protocole



Caractéristiques de l'interface IP

- adresse unique et homogène
- transfert par blocs (datagrammes)
- service sans connexion

SORBONNE UNIVERSITÉ

Protocole IP

IP : Protocole **best-effort !**

- service en **mode non connecté**
  - ➡ absence d'états dans les routeurs
  - ➡ paquets traités indépendamment les uns des autres : on les appelle des datagrammes

- service **non fiable** mais les datagrammes ne sont pas éliminés sans raison !
- service de connectivité

avantages

robustesse
efficace pour les échanges brefs
simplicité d'utilisation

SORBONNE UNIVERSITÉ

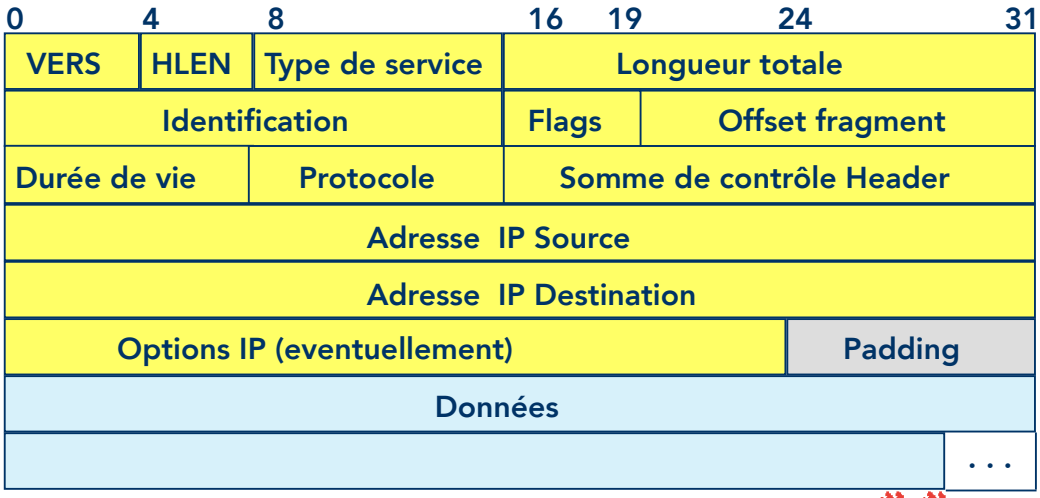
L'interconnexion de réseaux - Plan

- Les réseaux
- Le protocole IP
  - le datagramme
  - l'adressage IP
- Les protocoles de l'Internet
- L'adaptation des chemins

SORBONNE UNIVERSITÉ

Datagramme IP

L'unité de transfert de base dans un réseau internet est le datagramme qui est constituée d'un en-tête et d'un champ de données. (de 1.5KB, jusqu 'à 64KB)



Datagramme IP

Signification des champs du datagramme IP

- **VERS** : version de protocole IP (version 4)
- **HLEN** : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- **Longueur totale** : longueur totale du paquet (en-tête + données)
- **Type de service** : indique comment gérer le paquet dans les routeurs : priorité et QoS
- **Fragment offset, flags, identification** sont les champs de la fragmentation : nécessaire si un datagramme traverse un réseau physique qui véhicule des paquets de taille inférieure au datagramme considéré.

Datagramme IP

- **Durée de vie** : indique en nombre de sauts (nombre de routeurs), la durée maximale de transit du paquet sur l'internet.
- **Protocole** : identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du paquet (6 : TCP, 17 : UDP, 1: ICMP).
- **Somme de contrôle** de l'en-tête : permet de détecter les erreurs survenant dans l'en-tête du paquet.
- **OPTIONS** (facultatif et de longueur variable) concerne essentiellement des fonctionnalités de mise au point.
  - Enregistrement de route (chaque passerelle traversée ajoute son adresse IP dans le champ)
  - Routage strict/lâche prédéfini par l'émetteur : prédéfinit le routage en indiquant la suite des adresses IP dans l'option

Datagramme IP - encapsulation

0x0000 00 12 17 41 c2 c7 | 00 1a 73 24 44 89 | 08 00 | 45 00

@Eth dest. | @Eth src. | Type IPv4

0x0010 00 3c 27 30 00 00 80 01 80 d6 c0 a8 01 69 c0 a8

datagramme IP

0x0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66

0x0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

0x0040 77 61 62 63 64 65 66 67 68 69

Type	Protocole
800	Internet Protocol version 4 (IPv4)
806	Address Resolution Protocol (ARP)
8035	Reverse Address Resolution Protocol (RARP)
8100	VLAN-tagged frame (IEEE 802.1Q) & Shortest Path Bridging IEEE 802.1aq2
86DD	Internet Protocol, Version 6 (IPv6)
8847	MPLS unicast
8864	PPPoE Session Stage
...	...

Préambule	Adresse destinataire	Adresse source	Type	Données	CRC
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

Datagramme IP

0x0000 00 12 17 41 c2 c7 | 00 1a 73 24 44 89 | 08 00 | 45 00

@Eth dest. | @Eth src. | Type

0x0010 00 3c 27 30 00 00 80 01 80 d6 c0 a8 01 69 c0 a8

datagramme IP

0x0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66

0x0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

0X0040 77 61 62 63 64 65 66 67 68 69

Version	HLEN	Type de service	longueur totale
Identification		Flags	Offset fragment
TTL	Protocole	somme de contrôle	
adresse IP source			
adresse IP destination			
(options)			
données			

Datagramme IP

0x0000 00 12 17 41 c2 c7 | 00 1a 73 24 44 89 | 08 00 | 45 00

@Eth dest. | @Eth src. | Type | v IHL ToS

0x0010 00 3c 27 30 00 00 80 01 80 d6 c0 a8 01 69 c0 a8

longueur

0x0020 10 01 | 08 00 4d 56 00 01 00 05 61 62 63 64 65 66

0x0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

0X0040 77 61 62 63 64 65 66 67 68 69

IP version 4

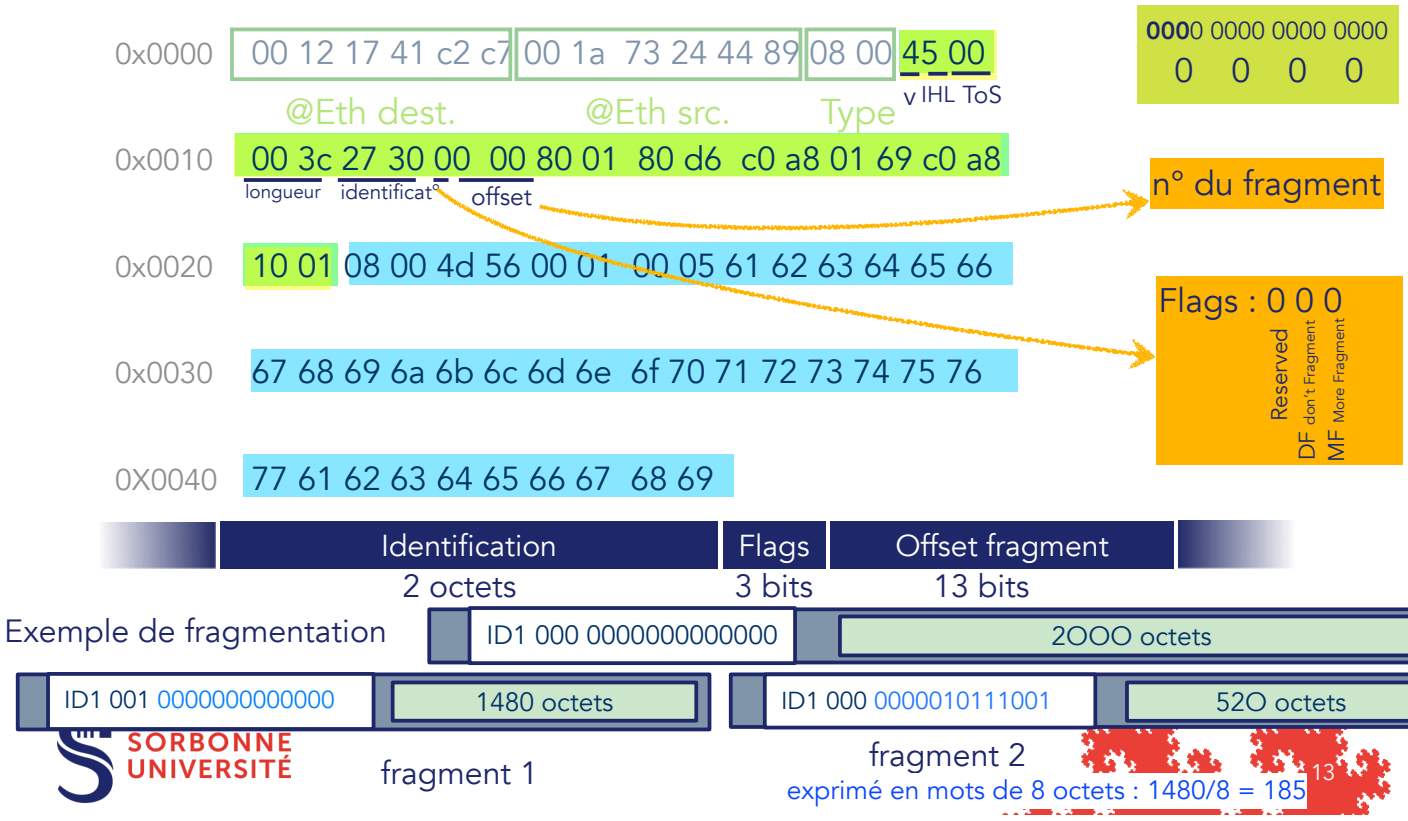
IP Header Length :
5*4 octets = 20 octets

ToS = 00000000
Priorité délai débit fiabilité coût MBZ

longueur totale
du datagramme IP
(entête + données)
= 3*16+12
= 60 octets

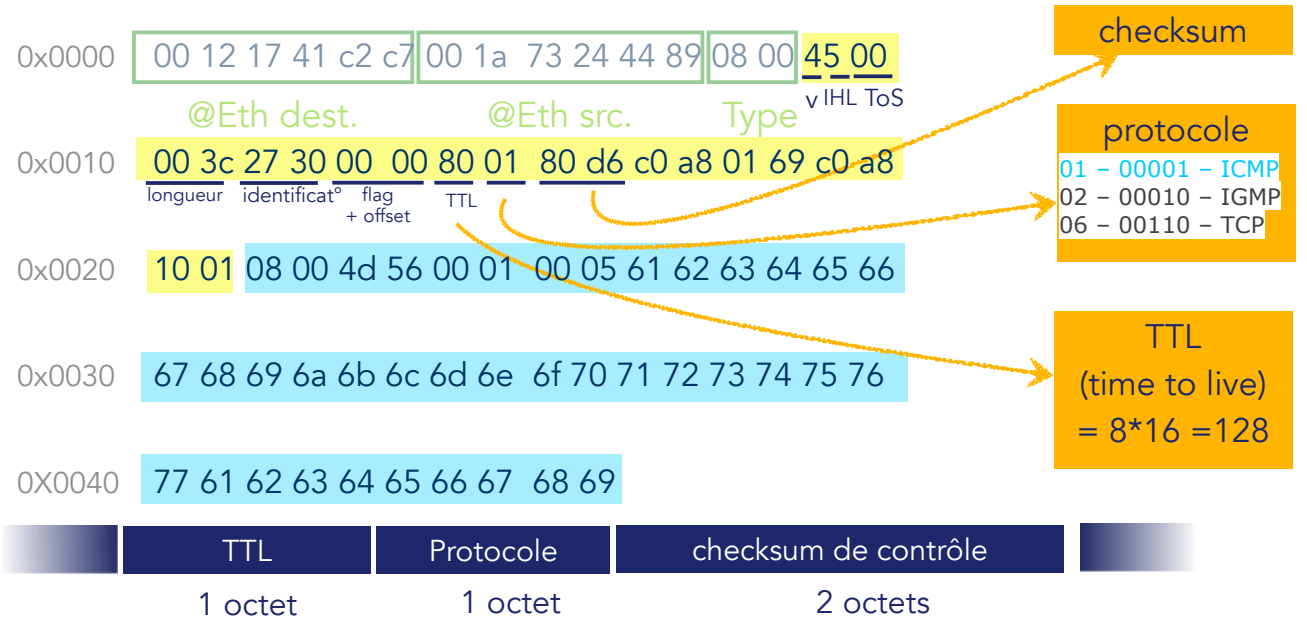
Version	HLEN	Type de service	longueur totale	
4 bits	4 bits	1 octet	2 octets	

Datagramme IP

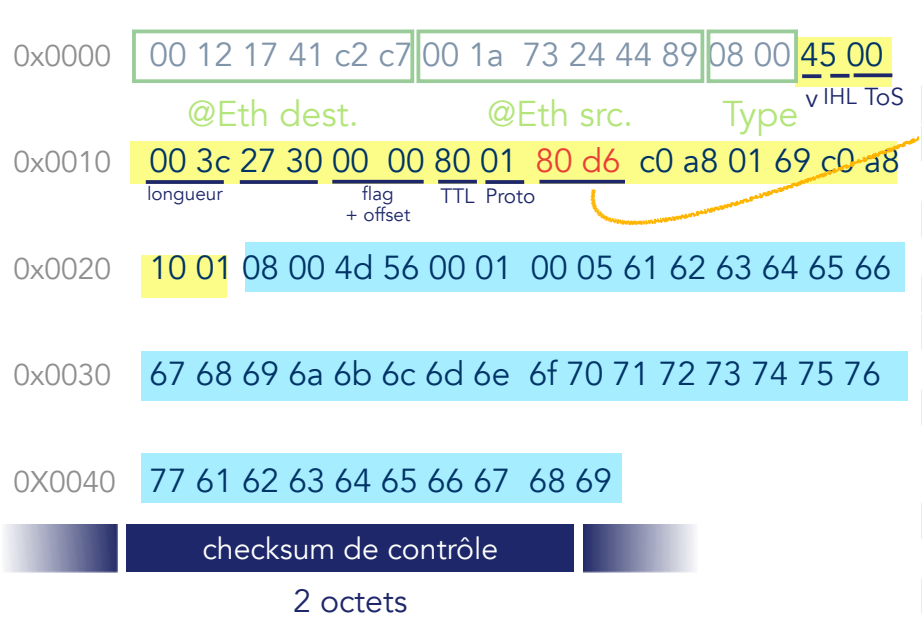


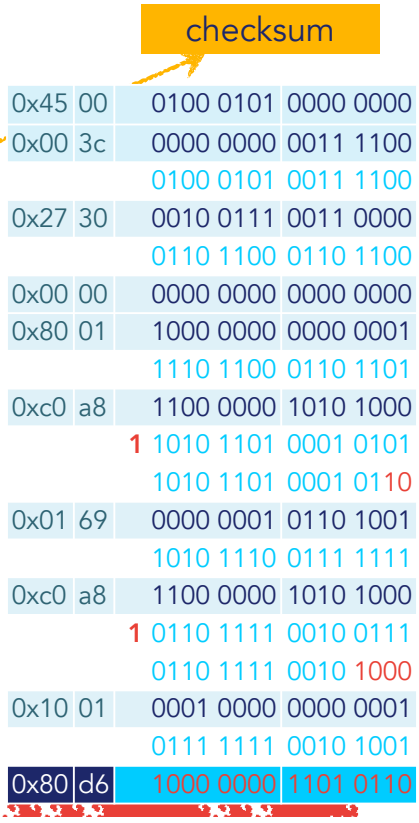
Exemple de fragmentation

Datagramme IP



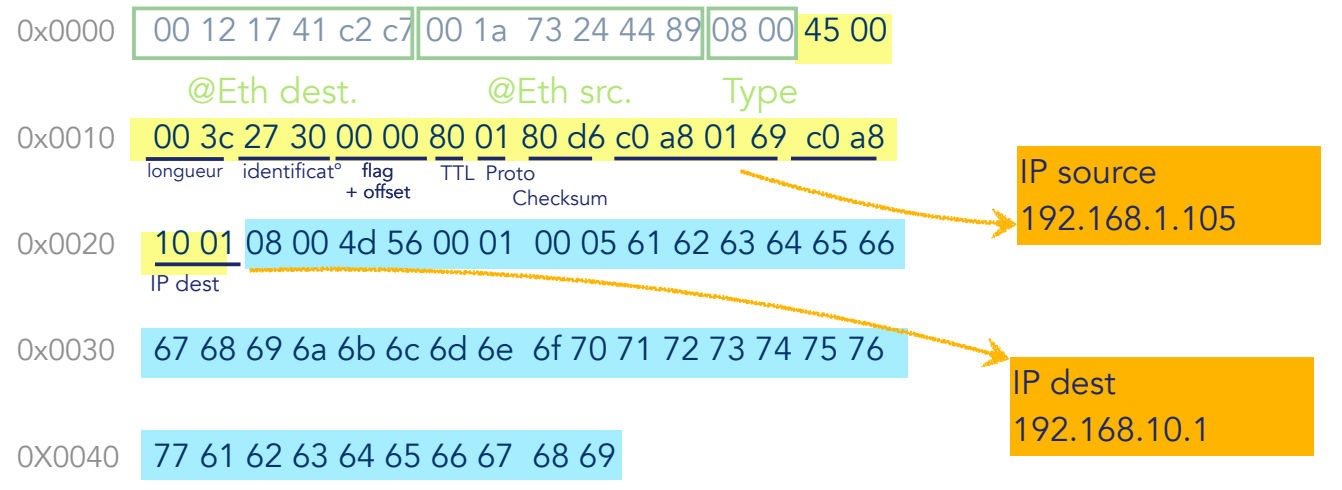
Datagramme IP





Couche réseau

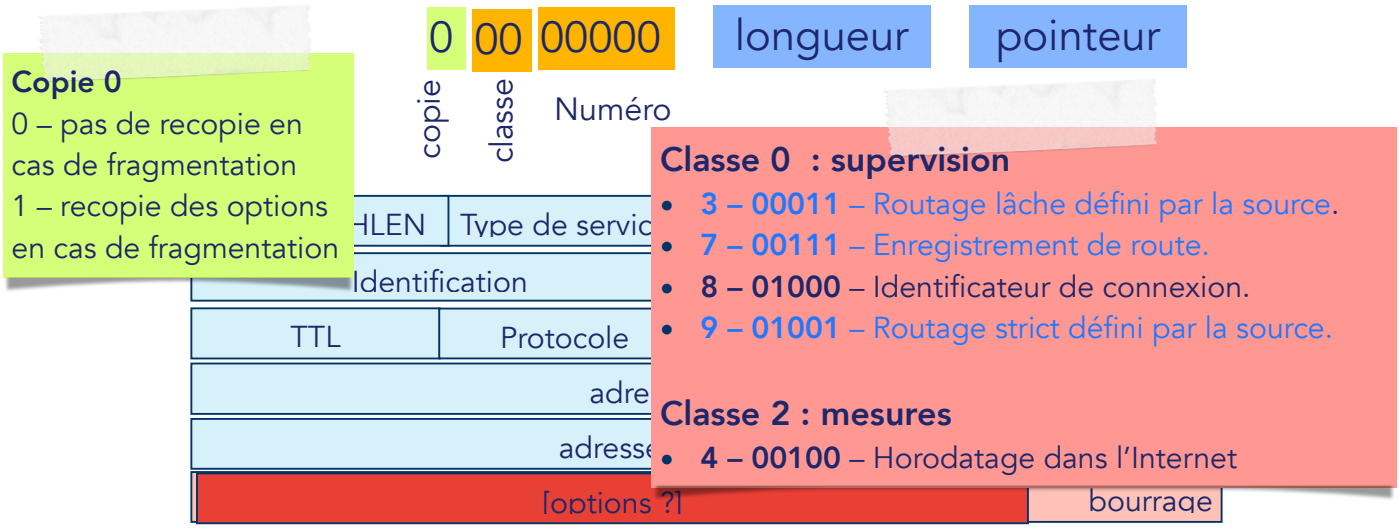
Datagramme IP



Datagramme IP

Champ option

entre 0 et 40 octets (multiple de 4 octets)



Copie 0
0 – pas de recopie en cas de fragmentation
1 – recopie des options en cas de fragmentation

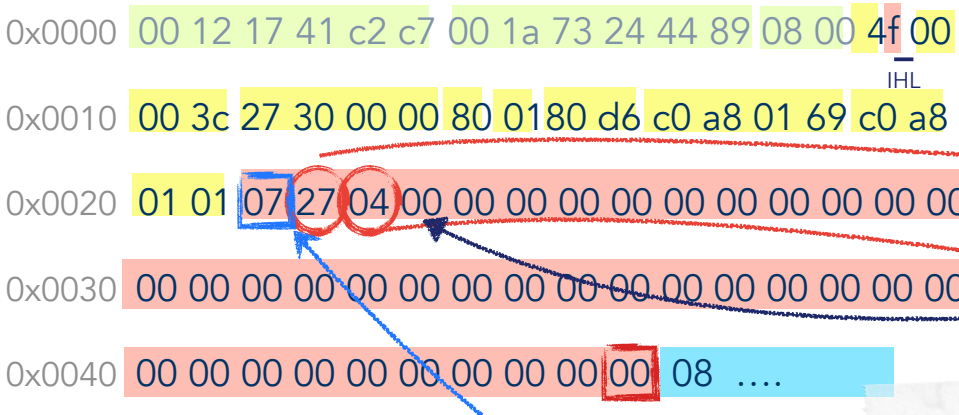
Classe 0 : supervision
- **3 – 00011** – Routage lâche défini par la source.
- **7 – 00111** – Enregistrement de route.
- **8 – 01000** – Identificateur de connexion.
- **9 – 01001** – Routage strict défini par la source.

Classe 2 : mesures
- **4 – 00100** – Horodatage dans l'Internet

SORBONNE UNIVERSITÉ

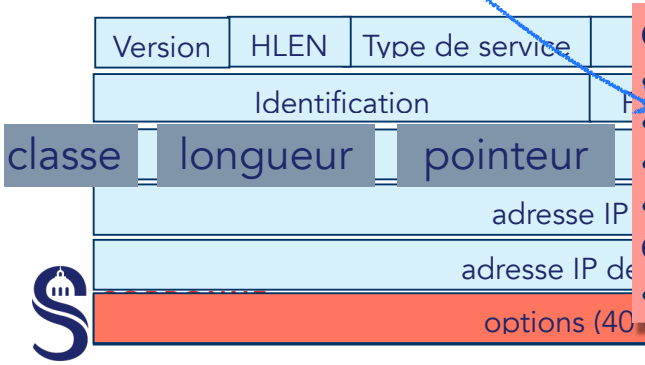
Datagramme IP

IP Header Length :
15*4 octets = 60 octets



longueur 0x27
= 39 octets

pointeur 0x04



Classe 0 : supervision
- **3 – 00011** – Routage lâche défini par la source.
- **7 – 00111** – Enregistrement de route.
- **8 – 01000** – Identificateur de connexion.
- **9 – 01001** – Routage strict défini par la source.

Classe 2 : mesures
- **4 – 00100** – Horodatage dans l'Internet

L'interconnexion de réseaux - Plan

- Le protocole IP
  - Datagramme IP
  - Adressage Internet
    - adresses IPv4
    - subnetting
    - CIDR
    - NAT
- Les protocoles de l'Internet
- L'adaptation des chemins

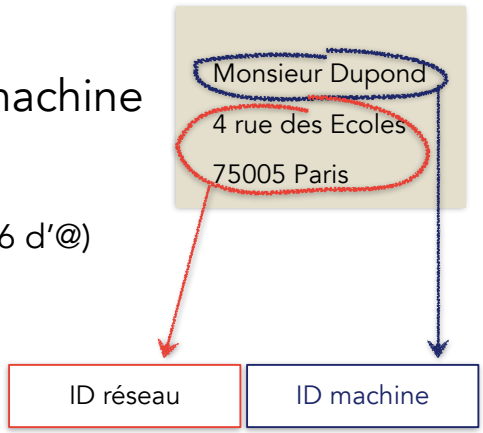
L'adressage Internet

But de l'adressage : fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion

- Une machine doit être accessible aussi bien par des humains que par d'autres machines
- Une machine doit pouvoir être identifiée par :
  - un nom (mnémotechnique pour les utilisateurs),
  - une adresse = **identificateur universel** de la machine,
  - une route précisant comment la machine peut être atteinte.

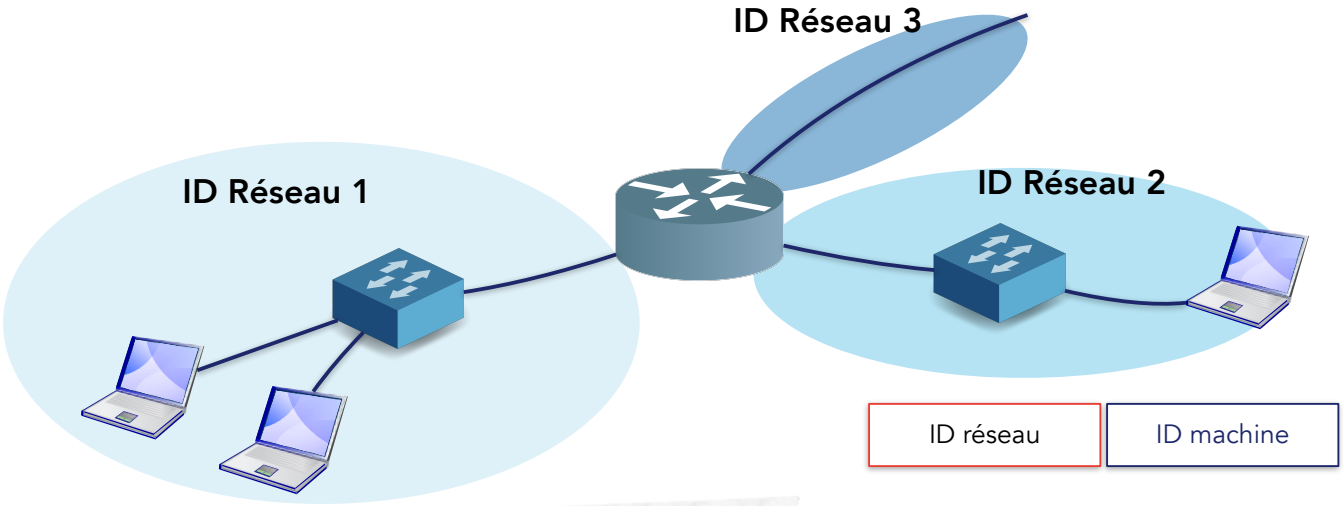
L'adressage Internet

- Adressage IP
  - sert à identifier la position d'une machine
  - Adresses IP :
    - **@ IPv4** : codée sur 4 octets (soit 4 294 967 296 d'@)
      notation décimale pointée : 132.227.28.16
    - @ IPv6 : codée sur 16 octets (soit 3,4e38 @ !!)



Pour qu'une adresse soit **routable** :
- l'**identifiant réseau** (**Net-Id**) doit être unique dans l'Internet
- l'**identifiant de la machine** (**host-Id**) doit être unique dans son réseau

L'adressage Internet

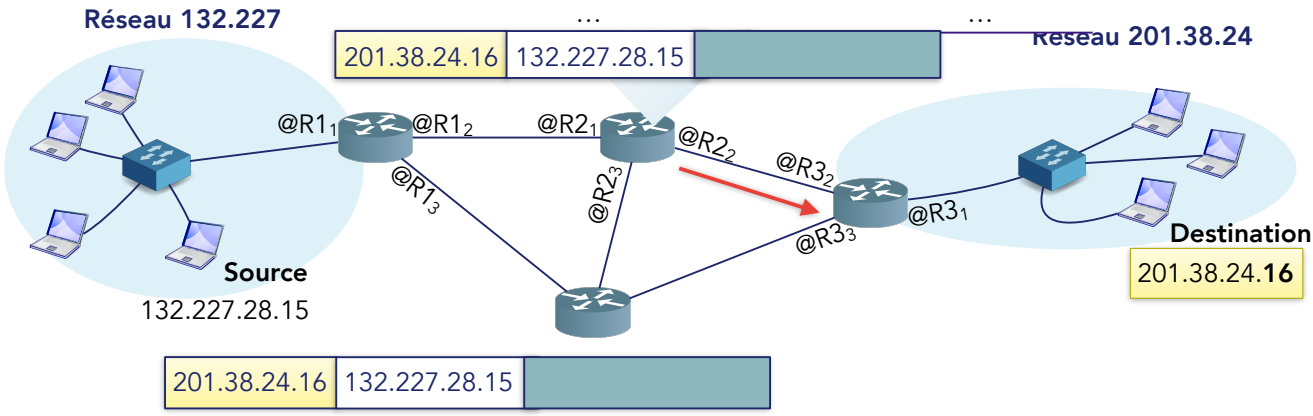


un **routeur** est une passerelle entre deux ou plusieurs réseaux physiques ayant chacun un préfixe réseau différent

L'adressage Internet

Utilisation des adresses IP pour acheminer les données au travers de l'Internet

destination	prochain routeur
réseau 132.227	@R1$_2$
réseau 128.10	@R4$_1$
machine 201.38.25.19	@R4$_1$
réseau 201.38.24	@R3$_2$
…	…



L'adressage Internet

Notation de l'adresse IP : quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP :

notation binaire : 10000000 00001010 00000010 00011110

notation décimale pointée : 128.10.2.30

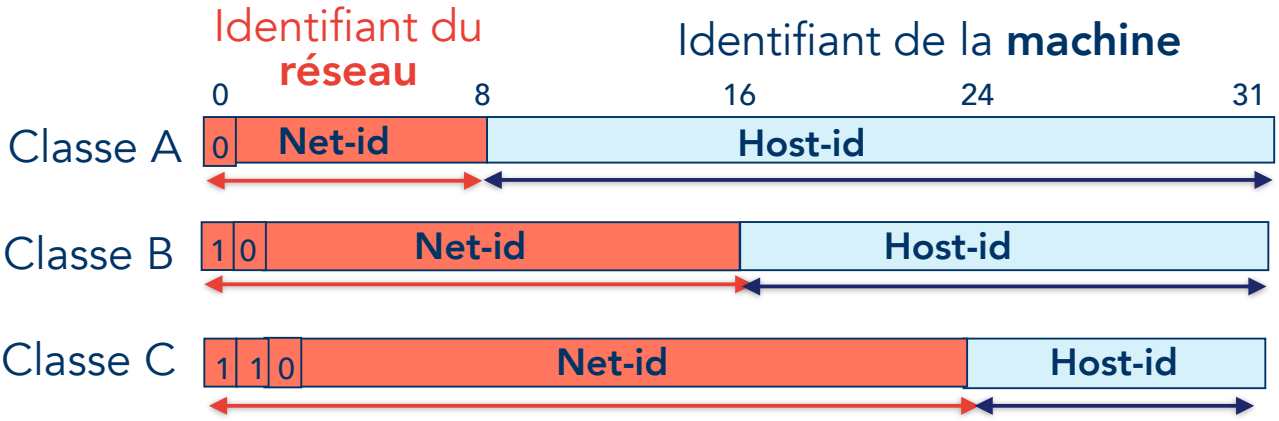
Une adresse IP dont la valeur **host-id** ne comprend que des **'1'** ou des **'0'** **ne peuvent être attribuée à une machine** réelle

- Adresse **machine locale** : 00.....00 | ID machine
  adresse IP dont le champ **Net-id** ne contient que des **'0'**
- Adresse **réseau** : Net-ID | 00...00
  adresse IP dont la partie **Host-id** ne comprend que des **'0'**.
- Adresse **de diffusion locale** : Net-ID | 11...11
  adresse IP dont la partie **Host-id** ne comprend que des **'1'**.

Sur combien de bits le **Net-ID** est-il codé ?

L'adressage Internet

- A l'origine : **classes d'adresse**



L'adressage Internet

- De quelle classe est l'adresse : 192.175.28.32 ?
- En déduire :
  - le Net-ID
  - le Host-ID
  - l'adresse de réseau sur le quel cette machine se trouve
  - l'adresse en diffusion de ce réseau

chaque machine possède une adresse vers elle-même (**@de loopback 127.x.x.x)**

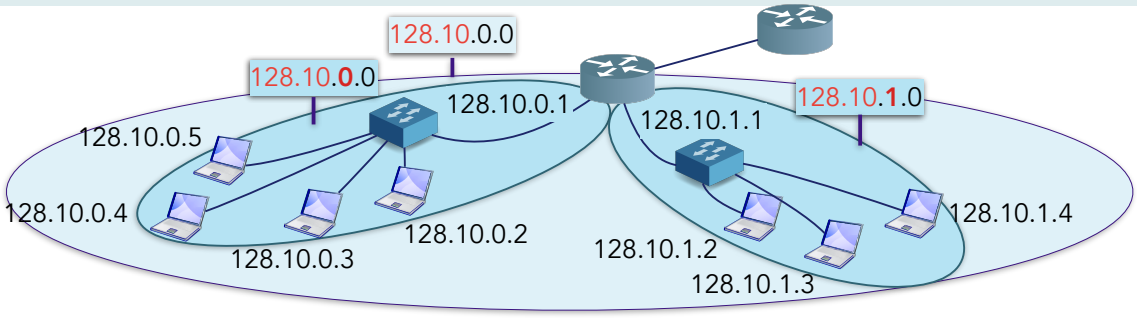
Le sous-adressage

En 1984 le **sous-adressage** a été introduit afin

- de limiter la consommation d'adresses IP
- et de diminuer :
  - la gestion administrative des adresses IP,
  - la taille des tables de routage des passerelles,
  - la taille des informations de routage,
  - le traitement effectué au niveau des passerelles.

Plusieurs réseaux distincts se partagent le même Net-ID (de classe A, B ou C). On dit alors que ces réseaux physiques sont des **sous-réseaux (*subnet*)** du réseau d'adresse IP.

Le sous-adressage



Le préfixe **128.10.0.0** est attribué à un administrateur.

L'administrateur veut séparer son réseau en 2 sous-réseaux physiques, et prend le premier octet de son host-Id pour définir des adresses de sous-réseau.

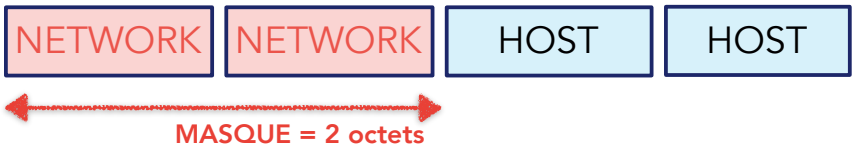
Il pourra alors mettre au plus 2^8-2 = 254 machines par sous-réseau

Le **masque** d'adresse informe sur la longueur du Net-ID à considérer

Le sous-adressage

Vu des routeurs de l'internet comme le réseau : 128.10. 0. 0

Classe B



De l'intérieur du réseau les sous-réseaux sont disjoints :

128. 10 . 1 . 0 **128. 10 . 2** . 0

MASQUE définit la longueur du Net-Id

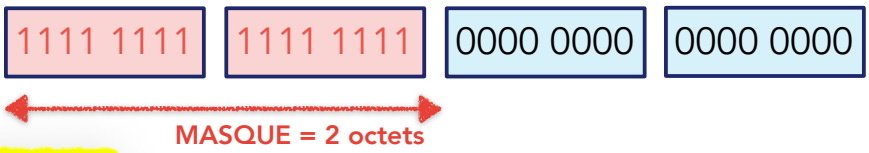
Masque du **sous-réseau**

SORBONNE UNIVERSITÉ

Le sous-adressage

255 . 255 . 0 . 0

Classe B



Le **masque** d'adresse s'écrit
comme une adresse IP
les bits du NetID <— 1
les bits du HostID <—- 0

255 . 255 . 255 . 0

Masque du **sous-réseau**

SORBONNE UNIVERSITÉ

Le sous-adressage

Combien de bits faut-il attribuer pour créer les sous réseaux ?

- Le choix du découpage dépend des perspectives d'évolution du site.
- Il faut indiquer sur combien de bits est codé le NetId : masque

Classe B :

8 bits permettent de définir 256 sous-réseaux de $2^8 - 2 = 254$ machines chacun.

…**4 bits** permettent de définir $2^4 = 16$ sous-réseaux de $2^8 - 2 = 4094$ machines.

Classe C :

4 bits pour la partie sous-réseau donne 4 bits pour le host-id soit 16 sous-réseaux de 14 machines chacun.

Lorsque le sous-adressage est ainsi défini, toutes les machines du réseau doivent s'y conformer sous peine de dysfonctionnement du routage —> configuration rigoureuse.

SORBONNE UNIVERSITÉ

Couche réseau

Le sous-adressage

Masque : permet de spécifier la longueur du préfixe Net-id d'une @

notations du MASQUE

sous forme d'une adresse

- décimale pointée 255 · 255 · 240 · 0
- binaire 11111111 . 11111111 . 11110000 . 0000000

longueur du préfixe

@ réseau / **masque** (# bits contigus du masque) 128 · 10 · 27 · 140 / 20

adresse IP	128.10.27.140		10000000	00001010	00011011	10001100
masque (/20)	255.255.240.0	ET	11111111	11111111	11110000	00000000
@ réseau	**128.10.16.0 / 20**		10000000	00001010	00010000	00000000

SORBONNE UNIVERSITÉ

Le CIDR

- Si une entreprise planifie d'avoir 1000 machines
  - 1 adresse de classe C ne suffit pas (255)
  - 1 adresse de classe B introduit une sous-utilisation (65536)
  - 4 adresses de classe C suffiraient !!

adresse réseau	1er octet	2e octet	3e octet	4e octet
193.37.140.0/24	**11000001**	**00010101**	**100011** 00	00000000
193.37.141.0/24	**11000001**	**00010101**	**100011** 01	00000000
193.37.142.0/24	**11000001**	**00010101**	**100011** 10	00000000
193.37.143.0/24	**11000001**	**00010101**	**100011** 11	00000000

Les 4 adresses peuvent être remplacées par une seule **193.37.140.0/22**

l'IETF introduit le concept de **Supernetting** ou **CIDR**.

SORBONNE UNIVERSITÉ

Le CIDR

- Supernetting (CIDR) = agrégation de plusieurs @

Avantages

- **réduit la taille des tables de routage (agrégation des entrées)** :
  - routage plus efficace,
  - mémoire des routeurs moins importante,
  - identification plus rapide du "match" [@IP - entrée]
- **optimise de l'utilisation des adresses réseau**

inconvénient

Complexifie le routage : le choix de la route se base sur **le « Longest Prefix Mach ».**

Variable Length Subnet Mask

Problème : L'utilisation d'un seul masque de sous-réseau sur un préfixe de réseau donné verrouille le nombre fée stations par sous-réseau.

idée : pour une adresse de réseau donnée, on peut définir des masques de sous-réseau de taille variable

VLSM (Variable Length Subnet Mask) = sous-réseau d'un sous-réseau

sous-réseau 1	207.21.24.0	/27
sous-réseau 2	207.21.24.32	/27
sous-réseau 3	207.21.24.64	/27
sous-réseau 4	207.21.24.96	/27
sous-réseau 5	207.21.24.128	/27
sous-réseau 6	207.21.24.160	/27
sous-réseau 7	207.21.24.192	/27
sous-réseau 8	207.21.24.224	/27

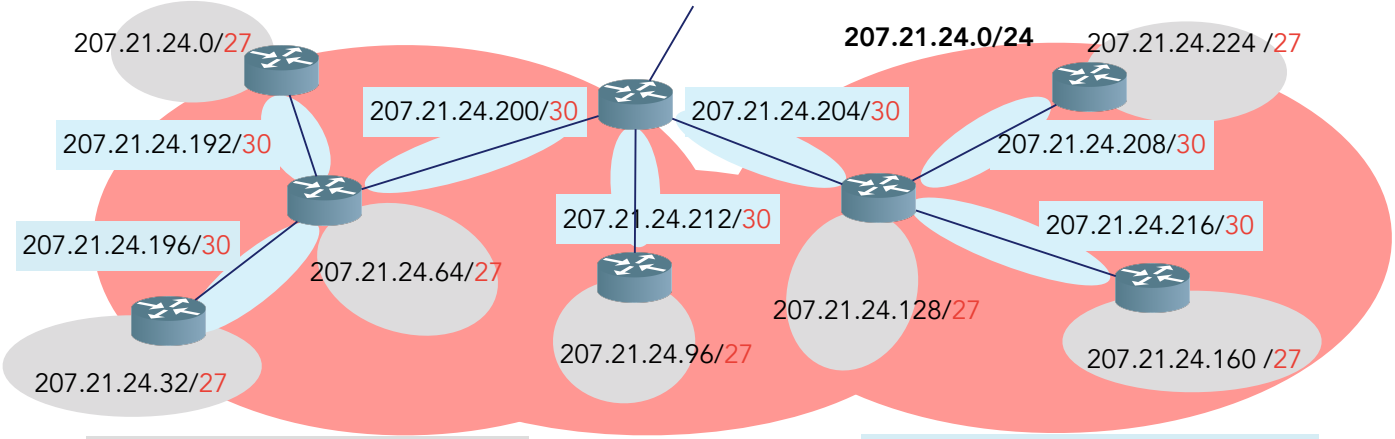
sous-réseau 1	207.21.24.192	/30
sous-réseau 2	207.21.24.196	/30
sous-réseau 3	207.21.24.200	/30
sous-réseau 4	207.21.24.204	/30
sous-réseau 5	207.21.24.208	/30
sous-réseau 6	207.21.24.212	/30
sous-réseau 7	207.21.24.216	/30
sous-réseau 8	207.21.24.230	/30

207.21.24.192	110 **000** 00
207.21.24.196	110 **001** 00
207.21.24.200	110 **010** 00
207.21.24.204	110 **011** 00
207.21.24.208	110 **100** 00
207.21.24.212	110 **101** 00
207.21.24.216	110 **110** 00
207.21.24.224	110 **111** 00

SORBONNE UNIVERSITÉ

7 sous-réseaux de 30 machines et 8 sous-réseaux de 2 machines

Variable Length Subnet Mask



sous-réseau 1	207.21.24.0	/27
sous-réseau 2	207.21.24.32	/27
sous-réseau 3	207.21.24.64	/27
sous-réseau 4	207.21.24.96	/27
sous-réseau 5	207.21.24.128	/27
sous-réseau 6	207.21.24.160	/27
sous-réseau 7	207.21.24.192	/27
sous-réseau 8	207.21.24.224	/27

207.21.24.	000**00000**
207.21.24.	001**00000**
207.21.24.	010**00000**
207.21.24.	011**00000**
207.21.24.	100**00000**
207.21.24.	101**00000**
207.21.24.	110**00000**
207.21.24.	111**00000**

sous-réseau 1	207.21.24.192	/30
sous-réseau 2	207.21.24.196	/30
sous-réseau 3	207.21.24.200	/30
sous-réseau 4	207.21.24.204	/30
sous-réseau 5	207.21.24.208	/30
sous-réseau 6	207.21.24.212	/30
sous-réseau 7	207.21.24.216	/30
sous-réseau 8	207.21.24.230	/30

SORBONNE UNIVERSITÉ

7 sous-réseaux de 30 machines et 7 sous-réseaux de 2 machines

Adresses privées

- Les adresses IP publiques étaient obtenues auprès d'une structure l'ICANN (anciennement IANA) qui déléguaient le pouvoir d'attribution des adresses au RIPE.

Au 25 novembre 2019, le RIPE NCC a annoncé la pénurie d'IPv4, après avoir effectué sa dernière attribution /22 IPv4 à partir des dernières adresses restantes. "Nous sommes maintenant à court d'adresses IPv4."

- IETF a défini des adresses privées en attendant le déploiement massif d'IPv6

adresses privées
10.0.0.0 /255
172.16.0.0/12
192.168.0.0/16

SORBONNE UNIVERSITÉ

Adresses privées

Les adresses privées peuvent être utilisées à la place d'adresses publiques dans les cas suivants :

- Un intranet non public
- Un laboratoire de test
- Un réseau domestique

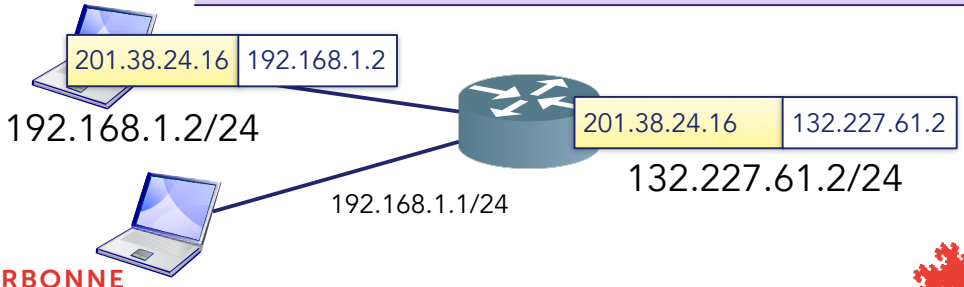
NAT (Network Address Translation)
est la traduction d'adresses réseau.
En pratique, le NAT est utilisé pour permettre aux hôtes qui utilisent un adressage privé à accéder à Internet.

SORBONNE UNIVERSITÉ

NAT

- Les traductions NAT peuvent se produire de manière dynamique ou statique.
- Routeurs NAT est leur capacité à utiliser la traduction d'adresses de port (PAT), qui permet à plusieurs adresses internes de mapper vers la même adresse globale (many-to-one NAT).
- des centaines de nœuds à adresse privée peuvent accéder à Internet en utilisant une seule adresse globale.

IP adresse locale		IP adresse globale	
192.168.1.2	**TCP port source 1234**	132.227.61.2	**TCP port source 2934**
192.168.1.3	**TCP port source 1234**	132.227.61.2	**TCP port source 2935**



SORBONNE UNIVERSITÉ

LU3IN133 réseaux informatiques

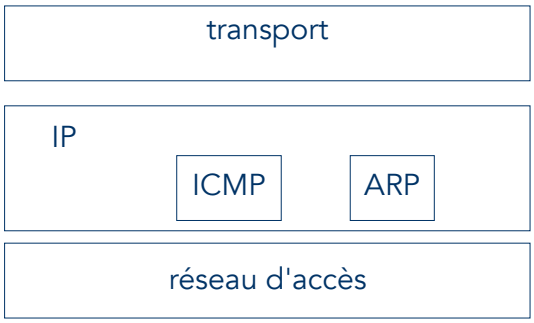
L'interconnexion de réseaux - Plan

- Les réseaux
- Le protocole IP
- Les protocoles de l'Internet
  - ICMP
  - ARP
  - DHCP
- L'adaptation des chemins

SORBONNE UNIVERSITÉ

Protocole de contrôle ICMP

- Motivation
  - pas de signalisation dans IP
    - pas de retour d'information
    - pas de messages d'anomalies



- ICMP (Internet Control Message Control)
  - instrumentation et test
  - signalisation d'anomalies (paquet trop grand, destination inaccessible, paquet détruit,…)
  - mise en œuvre obligatoire
  - messages ICMP encapsulés dans des datagrammes IP

SORBONNE UNIVERSITÉ

Messages ICMP

- format

Type	Code	Checksum
[données]		

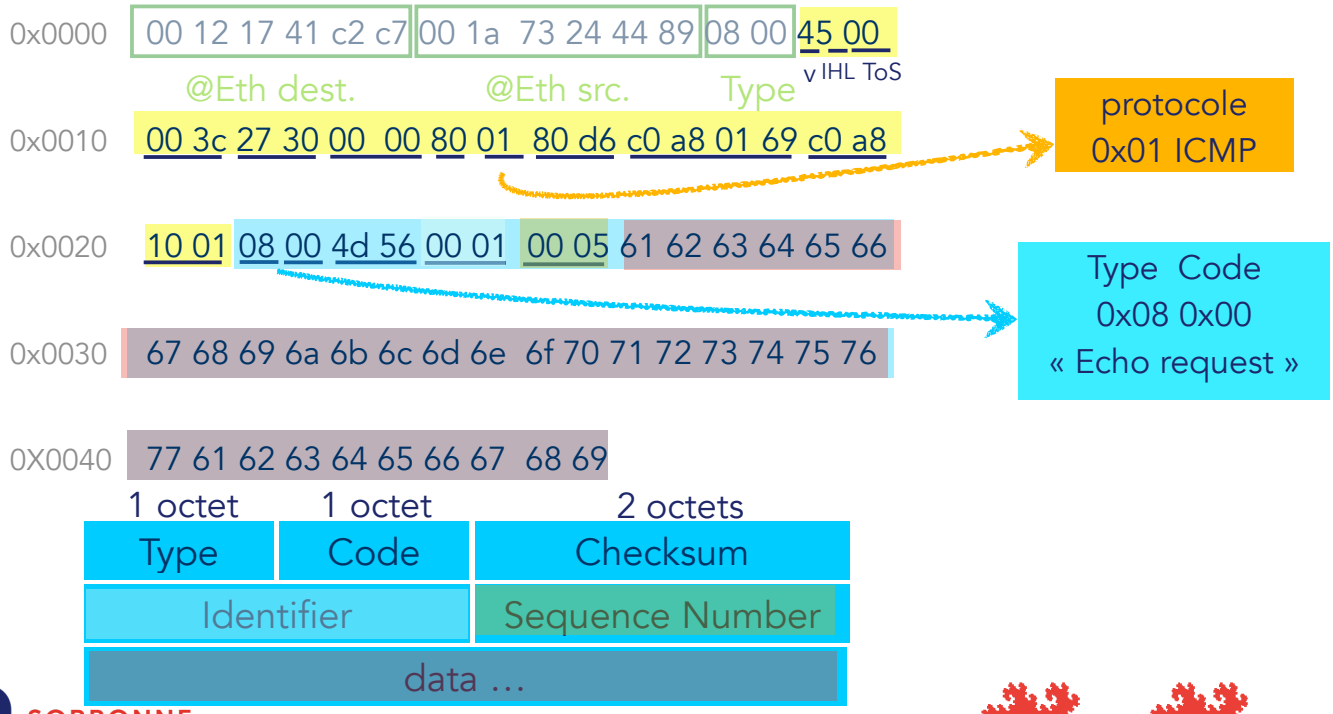
  - les messages ICMP ont tous le même format pour le premier mot de 32 bits
- champ type

Type	Message	Objet
0	Echo Reply	Réponse en écho.
3	Destination Unreachable	Destination inaccessible.
4	Source Quench	Interruption de la source.
5	Redirect	Redirection, changement de route.
8	Echo	Demande d'écho.
11	Time Exceeded	Temps de vie d'un datagramme dépassé.
12	Parameter Problem	Datagramme mal formé.
13	Timestamp	Demande de date d'estampillage.
14	Timestamp Reply	Réponse à une demande d'estampillage.
15	Information Request	Demande d'information.
16	Information Reply	Réponse à une demande d'information.
17	Address Mask Request	Demande de masque d'adresse.
18		Réponse à une demande de masque d'adresse.

TYPE « Destination Unreachable » Codes
0 Net Unreachable
1 Host Unreachable
2 Protocol Unreachable
3 Port Unreachable
4 Fragmentation Needed and Don't Fragment was Set
5 Source Route Failed
6 Destination Network Unknown
7 Destination Host Unknown
8 …

TYPE « Time Exceeded » Codes
0 Time to Live exceeded in Transit
1 Fragment Reassembly Time Exceeded

Messages ICMP



The data received in the echo message must be returned in the echo reply message

Messages ICMP

Outil **ping** permet de

tester l'accessibilité d'une machine

obtenir des statistiques sur la qualité de la route

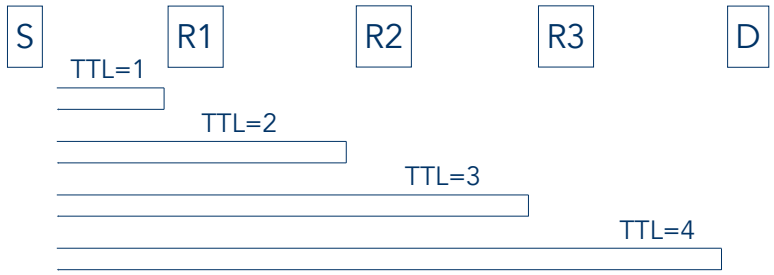
- **ping** exploite la fonction d'écho de ICMP
- un routeur ou un hôte recevant un "echo request" retourne un "echo reply

```
$ ping castor.univ-reunion.fr
PING castor.univ-reunion.fr (194.199.73.51): 56 data bytes
64 bytes from 194.199.73.51: icmp_seq=0 ttl=246 time=570.800 ms
64 bytes from 194.199.73.51: icmp_seq=1 ttl=246 time=581.364 ms
64 bytes from 194.199.73.51: icmp_seq=2 ttl=246 time=571.022 ms
64 bytes from 194.199.73.51: icmp_seq=3 ttl=246 time=572.722 ms
64 bytes from 194.199.73.51: icmp_seq=4 ttl=246 time=579.121 ms
64 bytes from 194.199.73.51: icmp_seq=5 ttl=246 time=571.619 ms
^C
----castor.univ-reunion.fr PING Statistics----
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 570.800/574.441/581.364/4.598 ms
```

Messages ICMP

Outil **traceroute** permet d'identifier la route vers la destination

Principe : transmet des paquets vers une destination, en partant d'un TTL de 1 et en l'incrémentant



si un routeur décrémente le TTL à 0, il retourne un message ICMP "TTL expiré"

Messages ICMP

- Outil Traceroute
- exemple

```
$ traceroute castor.univ-reunion.fr
traceroute to castor.univ-reunion.fr (194.199.73.51), 30 hops max, 40 byte packets
 1  olympe-61-0 (132.227.61.200)  0.219 ms  0.246 ms  0.234 ms
 2  r-scott.reseau.jussieu.fr (134.157.251.126)  0.878 ms  0.875 ms  0.845 ms
 3  r-jusren.reseau.jussieu.fr (134.157.254.126)  0.967 ms  0.895 ms  0.933 ms
 4  jussieu.cssi.renater.fr (194.214.109.21)  1.566 ms  1.288 ms  2.091 ms
 5  nio-n1.cssi.renater.fr (194.214.109.5)  1.804 ms  2.582 ms  2.260 ms
 6  nio-n3.cssi.renater.fr (193.51.206.170)  11.752 ms  22.965 ms  23.103 ms
 7  reunion.cssi.renater.fr (193.51.206.186)  587.128 ms  580.797 ms  571.993 ms
 8  cs-iremia.univ-reunion.fr (195.220.151.53)  568.513 ms  569.076 ms  580.685 ms
 9  castor.univ-reunion.fr (194.199.73.51)  570.421 ms  589.480 ms  567.862 ms
```

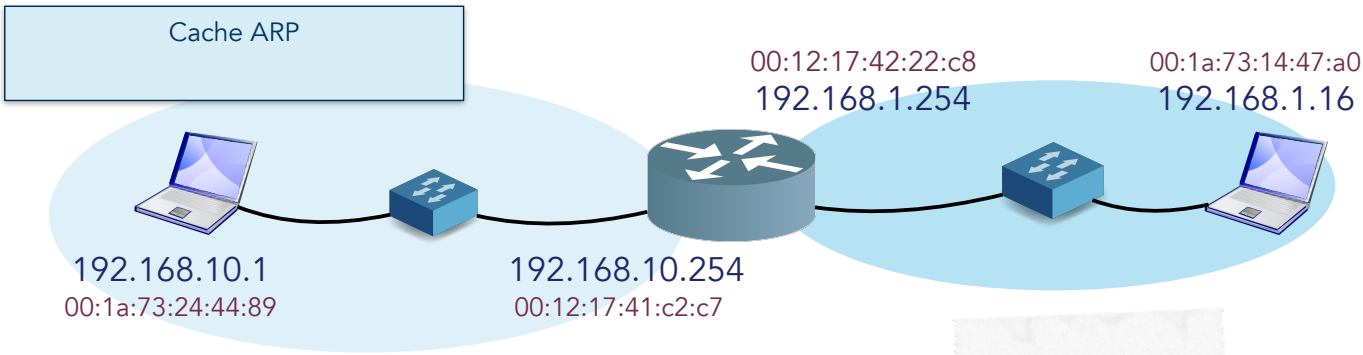
L'interconnexion de réseaux - Plan

- Les réseaux
- Le protocole IP
- Les protocoles de l'Internet
  - ICMP
  - ARP
  - DHCP
- L'adaptation des chemins

Protocole ARP

- Adresse Internet versus adresse physique
  - Le besoin de 2 adresses
    - La communication entre machines ne peut s'effectuer qu'au travers l'interface physique
    - Les applications connaissent les adresses IP, comment établir le lien adresse IP / adresse physique?
  - La solution : ARP (Address Resolution Protocol)
    - Mise en place dans TCP/IP d'un protocole de bas niveau appelé Address Resolution Protocol (ARP)
    - **Rôle de ARP** : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine de destination

Protocole ARP



192.168.10.1	192.168.1.16	

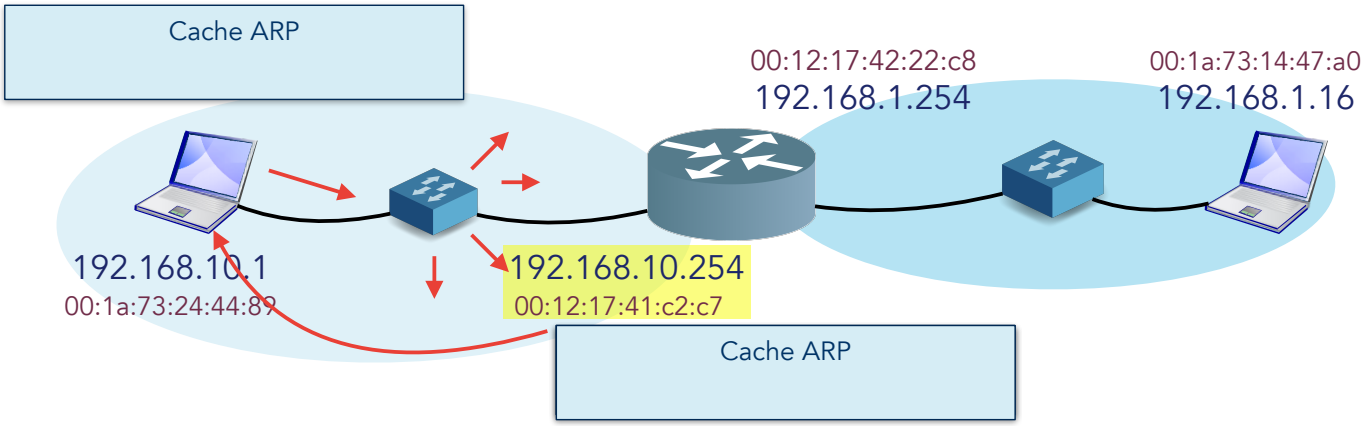
Datagramme IP

Comment trouver l'adresse MAC du destinataire de la trame ?

: : : : :	00:1a:73:24:44:89	IP

Trame Ethernet

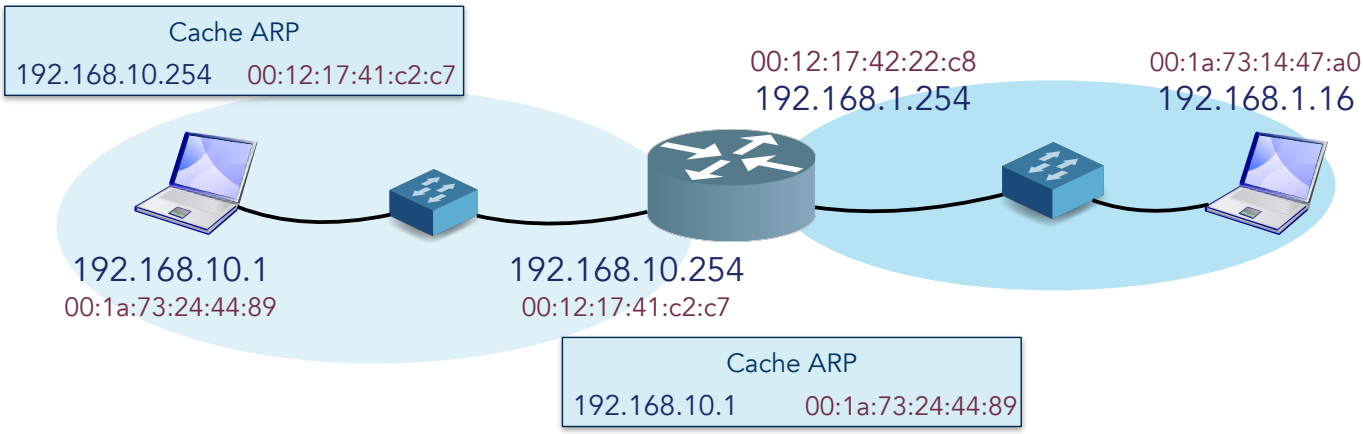
Protocole ARP



FF:FF:FF:FF:FF:FF	00:1a:73:24:44:89	ARP	192.168.10.1 demande : quelle est l'@ MAC associée à l'@ IP 192.168.10.254 ?

00:1a:73:24:44:89	00:12:17:41:c2:c7	ARP	192.168.10.254 répond l'@ MAC associée à mon @ IP est 00:12:17:41:c2:c7

Protocole ARP



Datagramme IP

00:12:17:41:c2:c7	00:1a:73:24:44:89	IP	192.168.10.1	192.168.1.16	

Trame Ethernet

Protocole ARP

Paquet ARP

0x0000 FF FF FF FF FF FF 00 1a 73 24 44 89 **08 06** 00 01
0x0010 08 00 06 04 **00 01** 00 1a 73 24 44 89 c0 a8 0a 01
0x0020 00 00 00 00 00 00 c0 a8 0a fe

HW type		Protocole type
HW @ length	Proto @ length	**Operation**
Sender hw @ [taille variable]		
sender Proto @ [taille variable]		
target HW @ [taille variable]		
proto HW @ [taille variable]		

Hardware type
01 - Ethernet
Protocol type
0x0800 - IP
Hardware Address Length
06 - Ethernet
Protocol Address Length
4 - IP v4
6 - IP v6
Operation
01 - *Request requête*
02 - *Reply réponse*

L'interconnexion de réseaux - Plan

- Les réseaux
- Le protocole IP
- Les protocoles de l'Internet
  - ICMP
  - ARP
  - DHCP
- L'adaptation des chemins

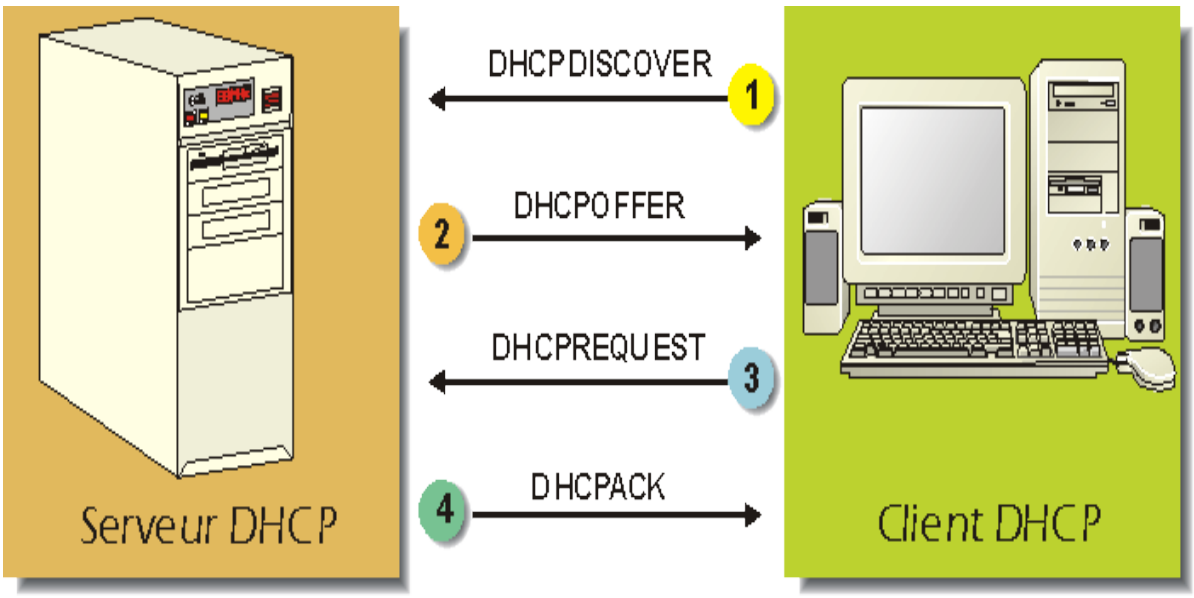
Les protocoles de l'Internet : DHCP

- Qui choisit quelle adresse attribuer à une machine ?
  - L'ingénieur système du réseau
  - Le fournisseur d'accès Internet
- L'adresse peut être :
  - fixe
  - attribuée dynamiquement (DHCP)

DHCP

- Principes du protocole DHCP
  - 1 serveur DHCP distribue des adresses IP.
    - Le serveur sert de base pour toutes les requêtes DHCP (1 serveur avec un adresse IP fixe par réseau).
    - Le mécanisme de base de la communication est BOOTP
      - Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau.
      - Pour trouver et dialoguer avec le serveur DHCP, la machine va émettre un paquet spécial de diffusion sur le LAN.
      - Lorsque le serveur DHCP reçoit ce paquet, il répond par un autre paquet de diffusion (le client n'a pas forcément son adresse IP et n'est donc pas joignable directement) contenant toutes les informations requises pour le client.

Les protocoles de l'Internet : DHCP



DHCP

- Attribution d'une adresse statique ou dynamique
  - Un serveur DHCP fournit généralement des adresses dynamiques
    - un même ordinateur peut alors recevoir successivement 2 adresses différentes
  - mais il peut aussi fournir une adresse IP fixe à un client bien particulier.
    - Ceci ne doit être utilisé que de manière modérée, sinon, le serveur DHCP ne sert à peu près plus à rien

DHCP

- Dialogue avec le serveur
  - Les messages DHCP sont transmis via UDP.
  - DHCP fonctionne donc en mode non connecté.
  - Numéros de ports :
    - Le client n'utilise que le port 68 pour envoyer et recevoir ses messages
    - le serveur envoie et reçoit ses messages sur un seul port, le port 67.
  - Format de la trame BOOTP/DHCP
    - La trame DHCP est en fait la même que BOOTP
    - Le passage de paramètres (nom de la machine...) se fait par l'intermédiaires d'options.
      - Les options sont documentées dans la RFC2132. Elles portent toutes un numéro qui les identifie. Par exemple,
        - option 15 : donne au client le nom de domaine du réseau.
        - option 53 : DHCPACK

DHCP

- Format de la trame

  op : vaut 1 pour BOOTREQUEST (requête client), 2 pour BOOTREPLY (réponse serveur)

  htype : type de l'adresse hardware

  hlen : longueur de l'adresse hardware (en octet). C'est 6 pour une adresse MAC

  hops : peut être utilisé par des relais DHCP

  xid : nombre aléatoire choisi par le client et qui est utilisé pour reconnaître le client

  secs : le temps écoulé (en secondes) depuis que le client a commencé sa requête

  flags : flags divers

octet 1	octet 2	octet 3	octet 4
op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (variable)			

DHCP

ciaddr : adresse IP du client, lorsqu'il en a déjà une
yiaddr : la (future) adresse IP du client
siaddr : adresse IP du (prochain) serveur à utiliser
giaddr : adresse IP du relais (passerelle par exemple) lorsque la connexion directe client/ serveur n'est pas possible
chaddr : adresse hardware du client
sname : champ optionnel. Nom du serveur
file : nom du fichier à utiliser pour le boot
options : Champs réservé pour les options. un client DHCP doit être prêt à recevoir au minimum 576 octets, mais il peut demander au serveur de restreindre la taille de ses messages.

octet 1	octet 2	octet 3	octet 4
op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (variable)			

DHCP

- Fonctionnement :
  - Le premier paquet émis par le client est un paquet de type **DHCPDISCOVER**.
  - Le serveur répond par un paquet **DHCPOFFER** pour soumettre entre autre une adresse IP au client.
  - Le client établit sa configuration, puis fait un **DHCPREQUEST** pour valider son adresse IP (requête en diffusion car **DHCPOFFER** ne contient pas son adresse IP).
  - Le serveur répond simplement par un **DHCPACK** avec l'adresse IP pour confirmation de l'attribution.
- Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace, mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP...

DHCP

- Types de messages DHCP :
  - **DHCPDISCOVER** (1) pour localiser les serveurs DHCP disponibles et demander une première configuration
  - **DHCPOFFER** (2) réponse du serveur à un message DHCPDISCOVER, qui contient les premiers paramètres
  - **DHCPREQUEST** (3) requête diverse du client pour par exemple prolonger son bail
  - **DHCPDECLINE** (4) le client annonce au serveur que l'adresse est déjà utilisée
  - **DHCPACK** (5) réponse du serveur qui contient des paramètres et l'adresse IP du client
  - **DHCPNAK** (6) réponse du serveur pour signaler au le client que son bail est échu ou si le client annonce une mauvaise configuration réseau
  - **DHCPRELEASE** (7) le client libère son adresse IP
  - **DHCPINFORM** (8) le client demande des paramètres locaux, il a déjà son adresse IP

DHCP

- Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées avec une date de début et une date de fin de validité : un bail.

  - Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme:
    - **L'adresse du DNS** (Résolution de noms)
    - **L'adresse de la passerelle** par défaut (pour sortir du réseau où le DHCP vous a installé).
    - **L'adresse du serveur DHCP**.
  - Le bail peut être prolongé sur demande du client ou sur proposition du serveur. Si le serveur ne reçoit pas de réponse valide, il rend disponible l'adresse IP.

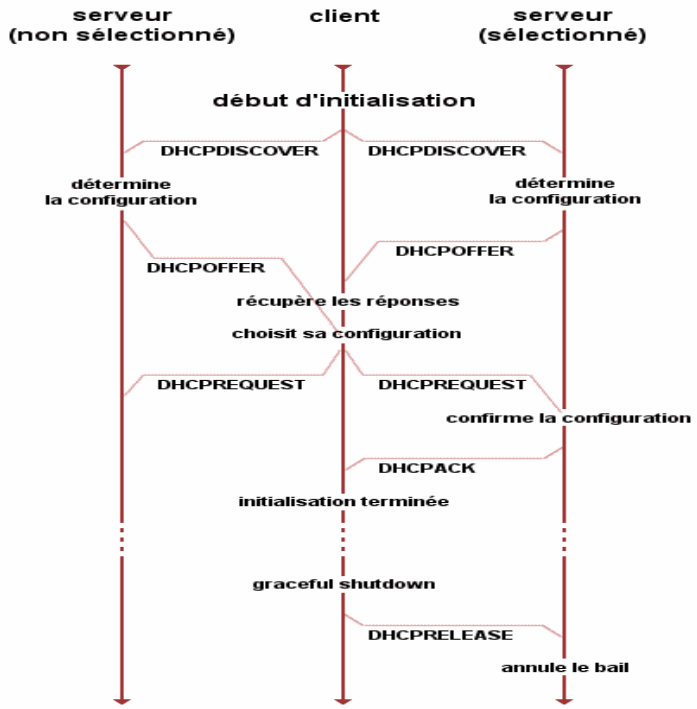
DHCP

- Optimisation de l'attribution des adresses IP en jouant sur la durée des baux.
  - Le problème est là :
    - si toutes les adresses sont allouées et si aucune n'est libérée au bout d'un certain temps, plus aucune requête ne pourra être satisfaite.
      - Sur un réseau où beaucoup d'ordinateurs se branchent souvent, il est intéressant de proposer des baux de courte durée. Mais attention de ne bloquer de la bande passante sur des petits réseaux fortement sollicités.
      - Sur un réseau constitué en majorité de machines fixes, très peu souvent rebootées, des baux de longues durées suffisent.
    - il est recommandé de ne pas créer de baux inutilement courts, ceci entraînant une augmentation significative du broadcast sur le réseau. Le compromis est à trouver entre la durée moyenne de connexion des utilisateurs, la réserve d'adresses IP du serveur, le nombre d'abonnés...

DHCP

- L'expiration du bail
  - DHCP est préventif : il attend 50% de la durée du bail pour demander son prolongement
    - pour cela le client contacte le serveur d'origine par un message (DHCPREQUEST).
    - Si le prolongement de son bail est accepté par le serveur, il lui envoi un message (DHCPACK) afin que le client puisse se mettre a jour avec cette nouvelle durée.
  - Si le client n'obtient pas de réponse il va attendre 7/8e de la durée du bail et va demander à tous les serveurs DHCP s'ils peuvent prolonger la durée de son bail.
    - Les serveurs DHCP peuvent répondre par un (DHCPACK) pour prolonger le bail du client.
  - Si un serveur ne peut pas prolonger son bail, il va envoyer un message (DHCPNACK) au client qui devra recommencer toute la procédure de demande d'un bail ip.

DHCP

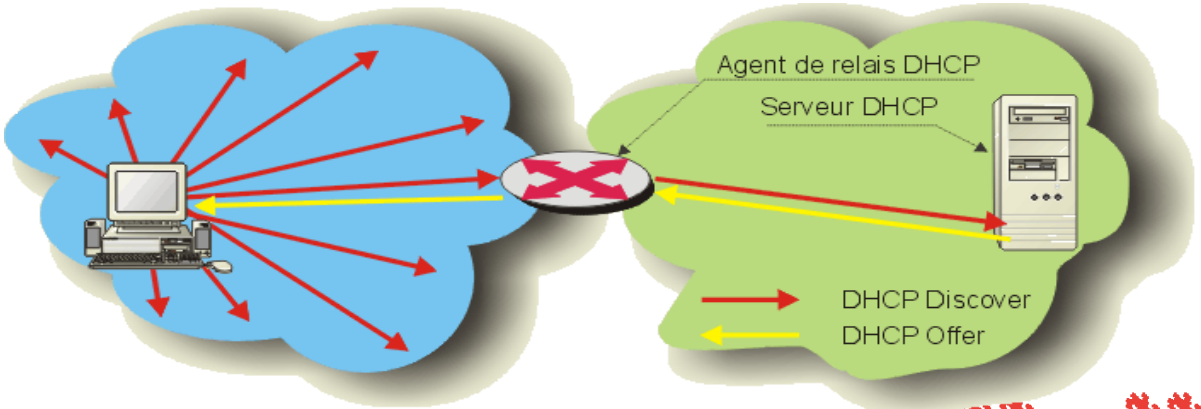


DHCP

- Installation d'un serveur
  - On est pas obligé d'installer un serveur DHCP par réseau
  - Le serveur ne dispose pas forcément d'une adresse IP dans la même classe que celles qui constituent sa plage d'adresses.
  - la négociation se fait alors de la manière suivante :
    - Les requêtes DHCP doivent pouvoir atteindre le serveur qui est situé sur un autre réseau, elles doivent donc passer les routeurs, (théoriquement impossible).
    - Installation sur un ou plusieurs routeurs d'un agent de relais qui va intercepter les requêtes en diffusion et les transmettre à un serveur DHCP connu de cet agent.

DHCP

- C'est **l'agent de relais** situé sur la passerelle qui va faire l'intermédiaire et le client réussira tout de même à obtenir une adresse, donnée par un DHCP situé sur un autre réseau, mais relayé par l'agent de relais.



DHCP/DNS

- Fonctionnement de l'interaction de mise à jour DHCP/DNS
  - Le serveur DHCP peut être utilisé pour conserver et mettre à jour les enregistrements de ressources de pointeur (PTR) et d'adresses (A) pour le compte de ses clients activés DHCP.
  - Ce processus nécessite l'utilisation d'une option DHCP supplémentaire : l'option FQDN client (option 81).
    - Cette option permet au client de fournir au serveur DHCP :
      - son nom de domaine complet (FQDN) ,
      - des instructions sur la manière dont il souhaite que le serveur traite les mises à jour DNS dynamiques pour son compte (le cas échéant).

DHCP/DNS

- le serveur peut être configuré de l'une des manières suivantes pour traiter les demandes de client :
  - Le serveur DHCP conserve et met à jour les informations du client auprès de ses serveurs DNS conformément à la demande du client.
  - Le serveur DHCP effectue toujours la sauvegarde et la mise à jour des informations du client auprès de ses serveurs DNS configurés.
  - Le serveur DHCP n'effectue jamais la sauvegarde et la mise à jour des informations du client auprès de ses serveurs DNS configurés.