Info0651 – Réseaux Informatiques

- IPv4
  - Protocoles et services auxiliaires
- IPv6

L A Steffenel – angelo.steffenel@univ-reims.fr

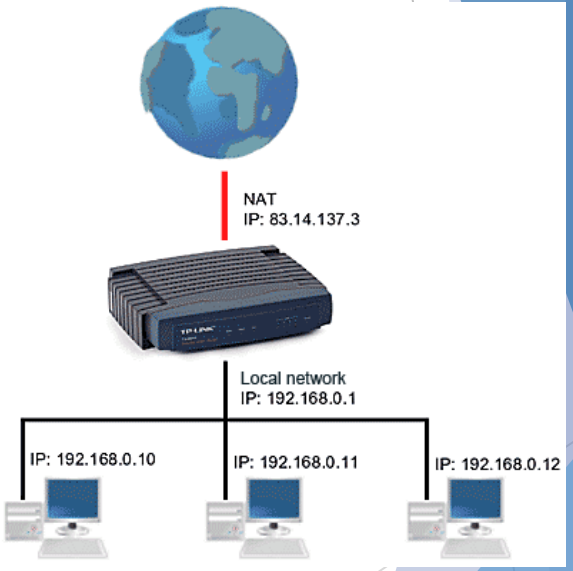
Université de Reims Champagne Ardenne

Objectifs de ce cours

- Étudier le comportement du NAT, des protocoles auxiliaires à IP (ICMP, etc) et comprendre ses limitations
- Introduire IPv6

NAT

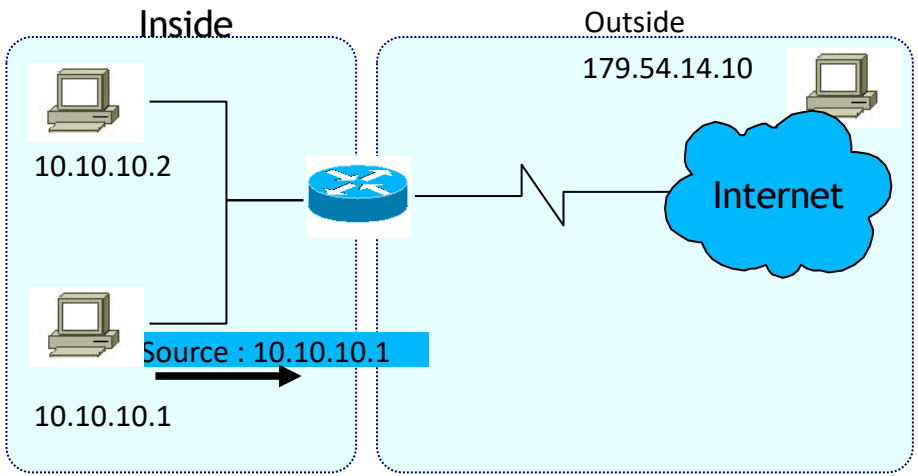
- La RFC 1918 a défini des plages d'adresses IP dites privées dans les 3 classes A, B et C
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Ces adresses servent à créer des réseaux privés, qui ne sont pas visibles de l'extérieur
  - Des règles "filtrent" ces routes



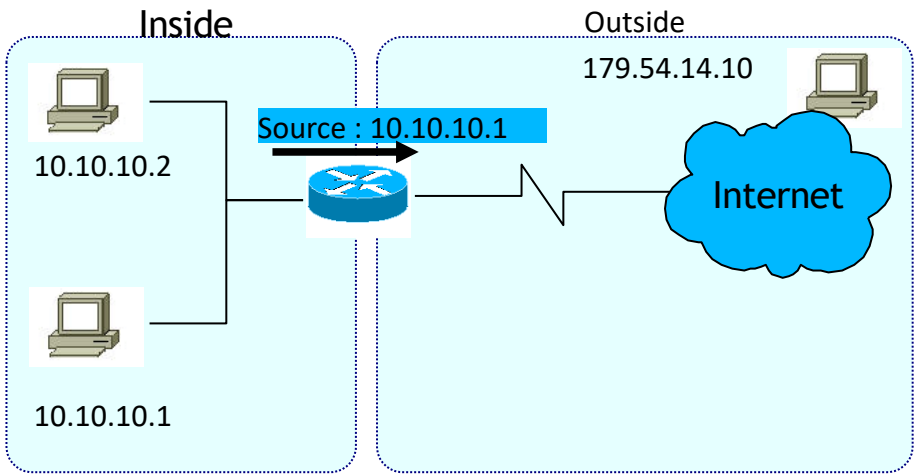
NAT

- Quand une machine interne à un réseau veux communiquer avec un hôte sur Internet il faut passer par un "traducteur d'adresses"
  1. Transmission du paquet au routeur de sortie
  2. Traduction de l'adresse de réseau privé en adresse publique
  3. Transmission du paquet modifié au hôte de destination
- Le serveur NAT doit garder une table de correspondance pour rediriger les messages reçus d'Internet

Exemple

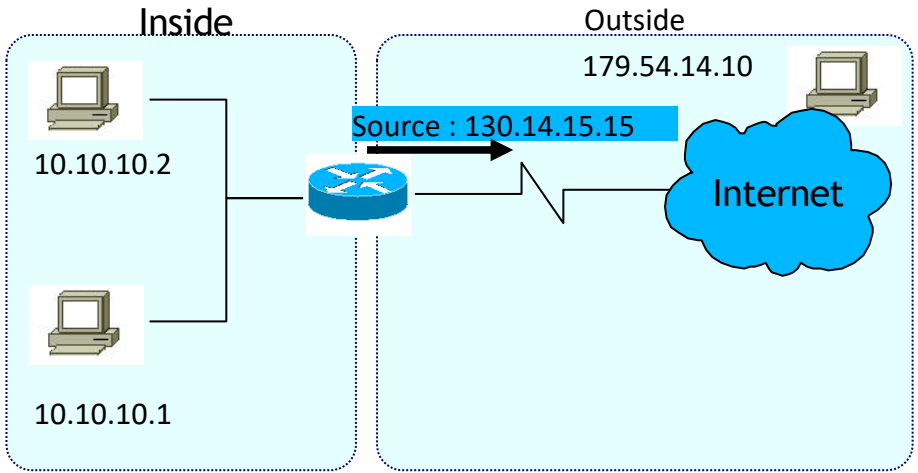


Exemple



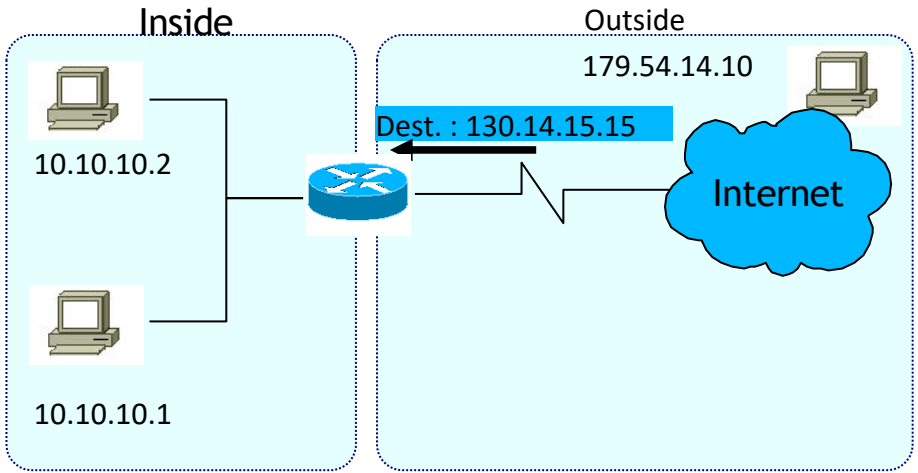
Adresse privée Interne	Adresse publique	Adresse destination
10.10.10.1	130.14.15.15	179.54.14.10

Exemple



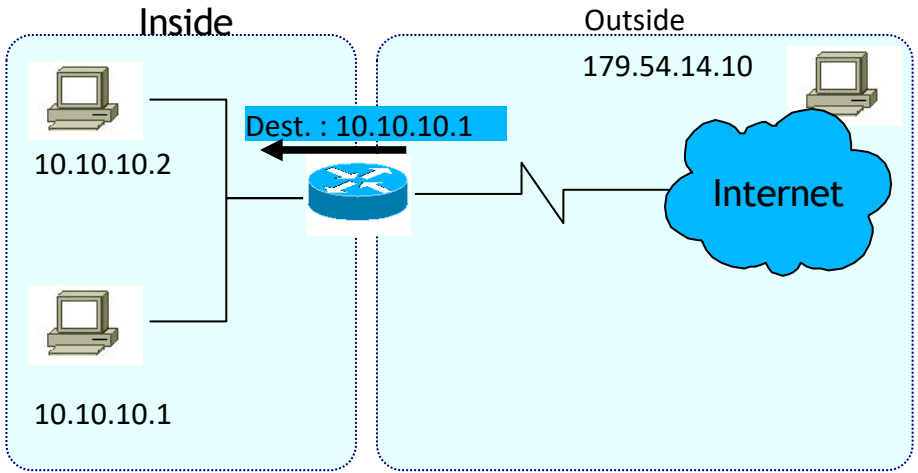
- Adresse privée Interne Adresse publique Adresse destination
- 10.10.10.1 130.14.15.15 179.54.14.10

Exemple



- Adresse privée Interne Adresse publique Adresse destination
- 10.10.10.1 130.14.15.15 179.54.14.10

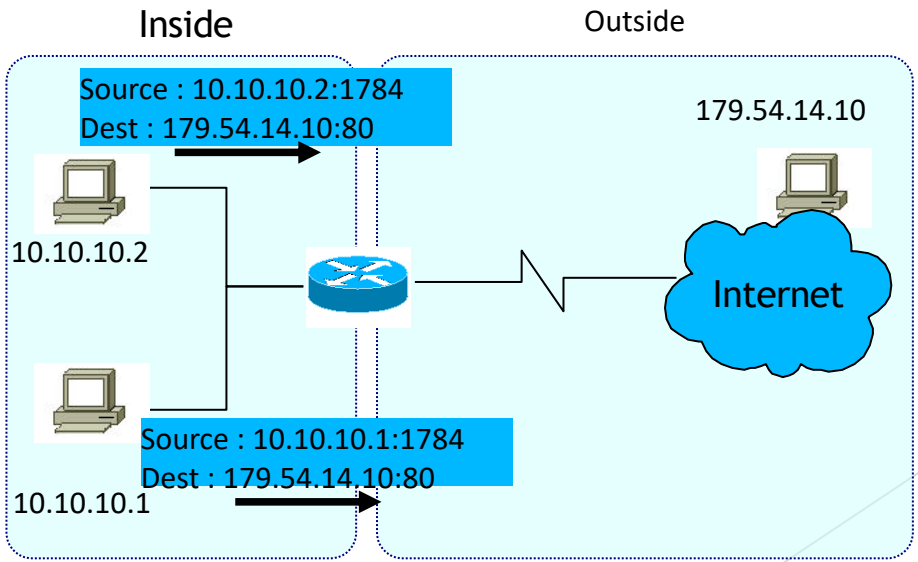
Exemple



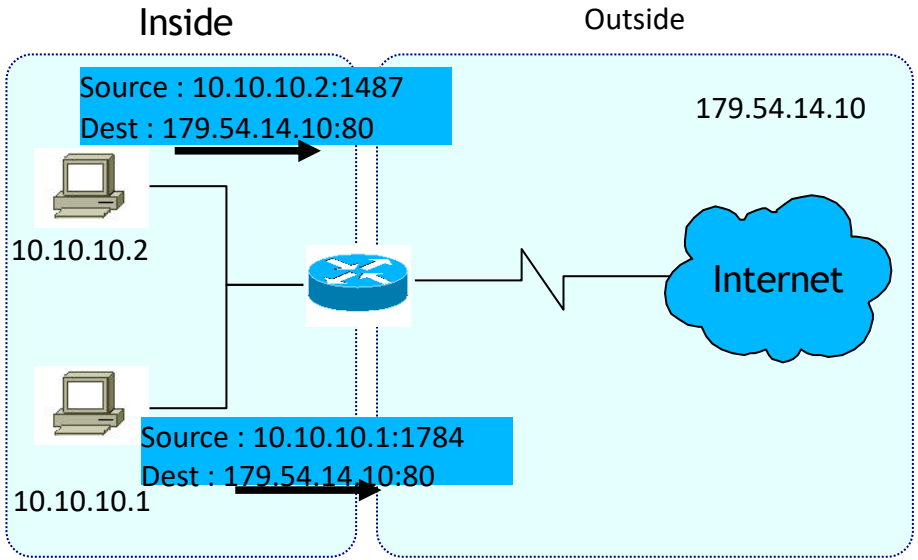
- Adresse privée Interne Adresse publique Adresse destination
- 10.10.10.1 130.14.15.15 179.54.14.10

Le PAT

Le PAT est une variante du NAT qui utilise un tableau de adresses/ports



Le PAT



- Adresse privée Interne — Adresse publique — Adresse destination
- 10.10.10.1:1784 — 130.14.15.15:1784 — 179.54.14.10:80
- 10.10.10.2:1487 — 130.14.15.15:1487 — 179.54.14.10:80

Limitations du NAT

- NAT viole le modèle architectural IP
  - Adresse unique
  - Connexion bout-en-bout interdite
- Le serveur NAT doit garder la trace des connexions
- Un max de 65536 connexions simultanées sont possibles
- Sécurité
  - Se cacher derrière un NAT n'est pas une garantie de sécurité
  - L'arrivée de IPv6 le prouve !

Le protocole ICMP

- ICMP (Internet Control Message Protocol)
  - Défini dans le RFC 950
- Protocole auxiliaire à IP car
  - IP ne vérifie pas si les paquets émis sont arrivés à leur destinataire
  - Si une passerelle ne peut router ou délivrer directement un paquet, il faut prévenir la source
  - Si un évènement anormal arrive sur le réseau, il faut pouvoir en informer l'hôte qui a émis le paquet

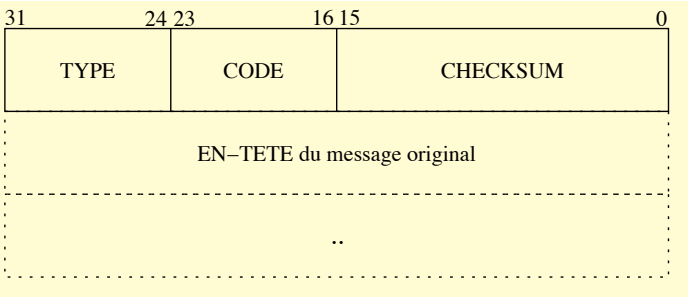
Traitement des messages ICMP

- Généralement ICMP est généré par la couche réseau (IP)
  - Certaines applications ont l'accès à ICMP
- Le traitement des messages se fait aussi sur la couche IP
  - quand un message d’erreur arrive pour un paquet émis, c’est la couche IP elle-même qui gère le problème, la plupart des cas sans en informer les couches supérieures

Format des Messages ICMP

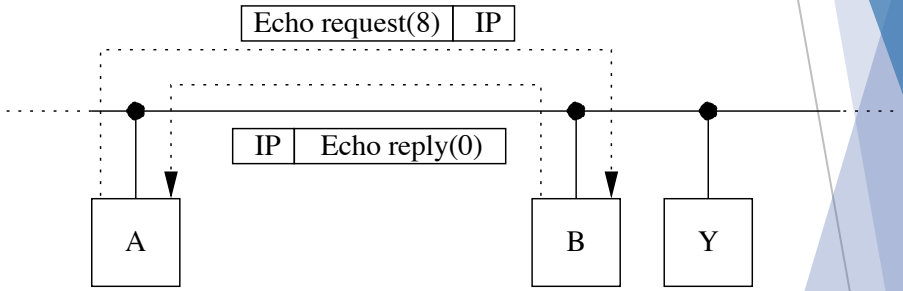
- Les paquets ICMP sont envoyés avec des entêtes IP
  - Raison : parfois il faut traverser plusieurs réseaux pour avertir un problème

Les messages ICMP sont composés :



Messages ICMP

- Echo Request (8), Echo reply (0)
- Utilisés pour l'application PING



- Time exceeded (11)
  - Chaque datagramme contient un champ TTL
  - Le message ICMP de type 11 indique que le TTL est expiré (utilisé pour l'une des variantes de traceroute)

Messages ICMP

- Destination Unreachable (3)
  - Quand une passerelle ne peut pas délivrer un datagramme IP
    Le champ CODE complète le message
    - 0 - Network unreachable
    - 1 - Host unreachable
    - 2 - Protocol unreachable
    - 3 - Port unreachable
    - 4 - Fragmentation needed and DF set
    - 5 - Source route failed

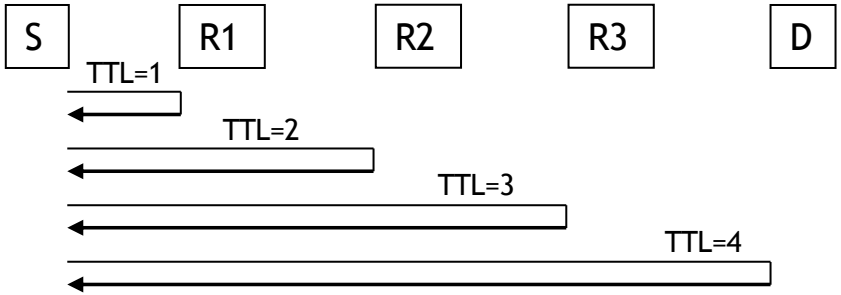
Outil ping

- Principe
  - exploite la fonction d'écho de ICMP
  - un routeur ou un hôte recevant un "*echo request*" retourne un "*echo reply*"
  - permet de
    - tester l'accessibilité d'une machine
    - obtenir des statistiques sur la qualité de la route
- Exemple

```
lsteffenel@cosy:~$ ping www.ufsm.br
PING www.ufsm.br (200.132.39.115) 56(84) bytes of data.
64 bytes from coral.ufsm.br (200.132.39.115): icmp_req=1 ttl=44 time=267 ms
64 bytes from coral.ufsm.br (200.132.39.115): icmp_req=2 ttl=44 time=272 ms
64 bytes from coral.ufsm.br (200.132.39.115): icmp_req=7 ttl=44 time=266 ms
64 bytes from coral.ufsm.br (200.132.39.115): icmp_req=8 ttl=44 time=266 ms
^C
--- www.ufsm.br ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8124ms
rtt min/avg/max/mdev = 266.508/268.193/272.549/1.849 ms
```

Outil traceroute

- 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"
  - permet d'identifier la route vers la destination

Outil Traceroute/Tracepath

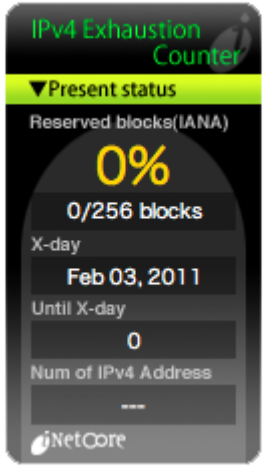
- Variations :
  - ICMP echo request avec TTL incrémental
  - UDP sur un port aléatoire
  - TCP sur un port aléatoire
- Dans tous les cas, l'outil reçoit des paquets ICMP 11 (Time Exceeded)
- Exemple :

```
lsteffenel@cosy:~$ traceroute access.grid5000.fr
traceroute to access.grid5000.fr (194.254.60.5), 30 hops max, 60 byte packets
 1  h1.univ-reims.fr (194.57.105.1)  0.304 ms  0.294 ms  0.310 ms
 2  10.1.81.254 (10.1.81.254)  0.459 ms  0.648 ms  0.821 ms
 3  rt1-223-a.actif.univ-reims.fr (192.168.223.1)  3.647 ms  3.671 ms  3.705 ms
 4  router1.actif.univ-reims.fr (192.168.123.1)  3.747 ms  3.772 ms  3.793 ms
 5  33.1.79.86.rev.sfr.net (86.79.1.33)  3.834 ms  3.857 ms  3.880 ms
 6  * * *
 7  te0-1-0-2-paris2-rtr-001.noc.renater.fr (193.51.189.105)  10.565 ms  10.587 ms  13.557 ms
 8  te0-3-4-0-paris1-rtr-001.noc.renater.fr (193.51.189.5)  71.983 ms  69.355 ms  69.407 ms
 9  * * *
10  inria-lille-projetgrid5000-vl536-gi8-4-lille-rtr-021.noc.renater.fr (193.51.183.177)  11.389 ms !X
* *
```

IPv6

Un peu d'Histoire

- Dans les années 90 :
  - Augmentation exponentielle de l'Internet
  - Augmentation du nombre d'entrées dans les tables de routage
- Allocation des adresses - Janvier 1996
  - Classe A - 100.00%
  - Classe B - 61.95%
  - Classe C - 36.44%
- Prévisions d'exhaustion du espace d'adressage
  - Première alerte - 1994
  - Depuis le 1er février 2011 tous les blocs ont été attribués
  - Fin des adresses disponibles : août 2011
    - http://www.ipv6forum.org/



IPv4 en chiffres

- Attribution des adresses IPv4
  - 3 706 650 000 vraiment utilisables
  - 2^{32} [4 294 967 296] - (classes D et E, réseaux 0 et 127 et RFC1918)
- 6,5 milliards d'habitants
  - 40% des adresses sont allouées aux USA
  - 3% des adresses sont allouées à la Chine

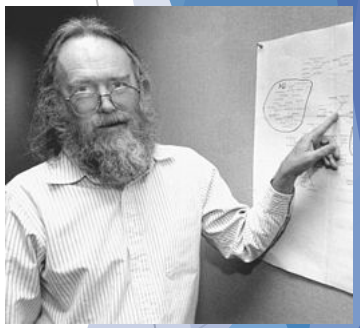
Comment les adresses étaient attribuées

- RFC 790 (septembre 1981) :

  "The assignment of numbers is also handled by Jon. If you are developing a protocol or application that will require the use of a link, socket, port, protocol, or network number ***please contact Jon*** *to receive a number assignment.*

  Jon Postel

  USC - Information Sciences Institute
  4676 Admiralty Way
  Marina del Rey, California 90291"



- Plus sérieusement, les blocs d'adresses étaient distribués sans trop de contrôle…
- jusqu'à la crise des adresses des années 1990

Mesures Palliatives - 1994

- Routage "classless"
  - CIDR (Classless Internet Domain Routing) (RFC 1519)
  - Adresse réseau = préfixe/longueur du préfixe
  - Limite les pertes d'adresses
- Agrégation des routes (réduction des tables de routage)
  - Réorganisation des adresses déjà alloués (RFC 1917)
- Plans d'adressage privés (RFC 1918)
  - Utilisation de proxies ou NAT

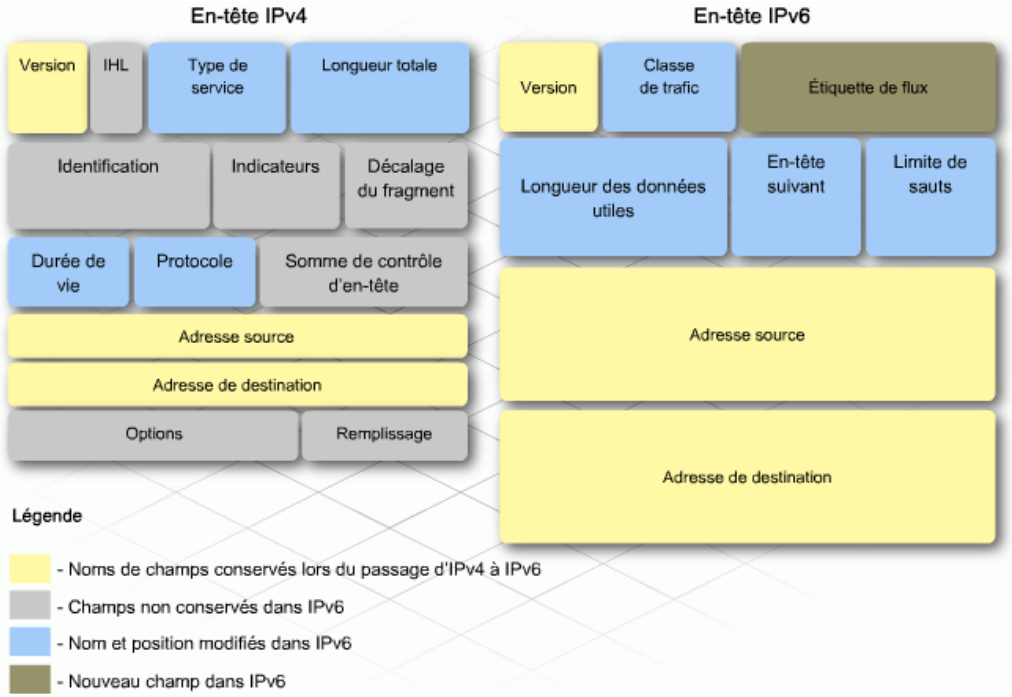
IPv6 – Une nouvelle version de IP

- LA réponse pour le problème de la croissance de l'Internet
  - Nouveaux réseaux
  - Nouvelles machines/dispositifs
  - Utilisation mobile/nomade
- Augment le format des adresses à 128 bits (16 octets)
- Garde les bonnes choses de IPv4
  - Format fixe et bien connu pour l'entête
  - Taille d'adresses fixe
- Départ avec les bonnes habitudes
  - Réseaux structuré et hiérarchisé
    - Distribution "logique" et géographique

128 bits - Est-ce que cela suffit ?

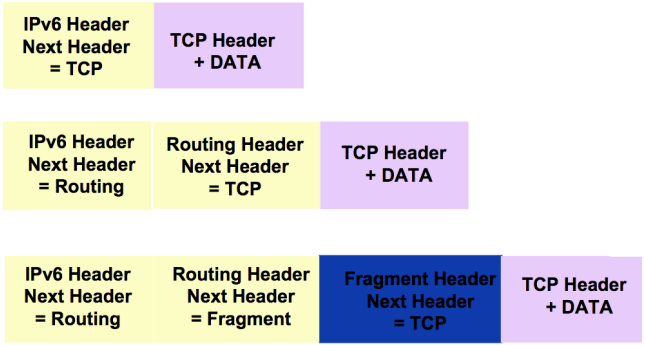
- Longueur des adresses = 128 bits
  - Pour rappel, IPv4 compte avec des adresses de 32 bits
- **Attention : 2^{128} >>>>>> 4 x 2^{32}**
  - $2^{32} = 4.2 \times 10^{9}$
    - 4 294 967 296
  - $2^{128} = 3.4 \times 10^{38}$
    - 340 282 366 920 938 463 463 374 607 432 768 211 456
- Pour comparaison
  - Étoiles observables dans le ciel = $2^{52} = 4.5 \times 10^{15}$
  - Approximativement 506 102 adresses par m^2 sur terre
  - ou 5×10^{28} adresses pour chaque habitant de la planète

Ce que change dans les entêtes



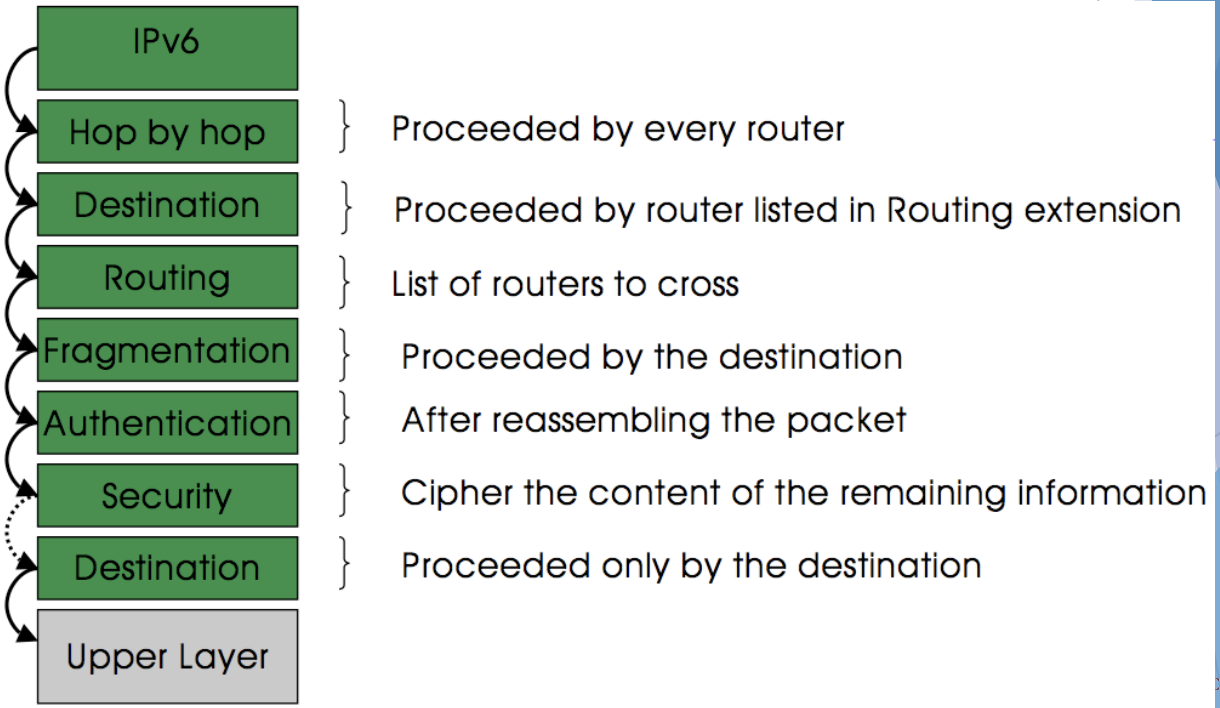
Les Extensions IPv6

- Optionnelles, utilisées à la place des options IPv4
  - Insérées entre l'entête IPv6 et les données (TCP, etc.)
  - Le protocole n'est pas figé, il peut évoluer avec le temps



- Les extensions ne sont pas traitées par aucun nœud intermédiaire
  - Exception: l'extension "hop by hop"

Les Extensions et leur Ordre



L'Adressage IPv6

- Adresse sur 128 bits découpée en 8 mots de 16 bits.
  - Utilisation de chiffres hexadécimaux pour gagner de la place
- Exemple: **FEDC:0000:0000:0210:EDBC:0000:6543:210F**
- Format compressé
  - compression des 0 d'entête - FEDC**:0:0:**210:EDBC**:0:**6543:210F
  - Remplacer une séquence de 0 par :: **(une seule fois)**
    - FEDC**::**210:EDBC**:0:**6543:210F
    - FF01:**0:0:0:0:0:0:**1 → FF01**::**1
    - **0:0:0:0:0:0:0:**1 → **::**1
    - **0:0:0:0:0:0:0:**0 → **::**
- Exemple d'utilisation :
  - http://[2001:1234:12::1]:8080

UNIVERSITÉ DE REIMS CHAMPAGNE ARDENNE

Adresses Spécifiques

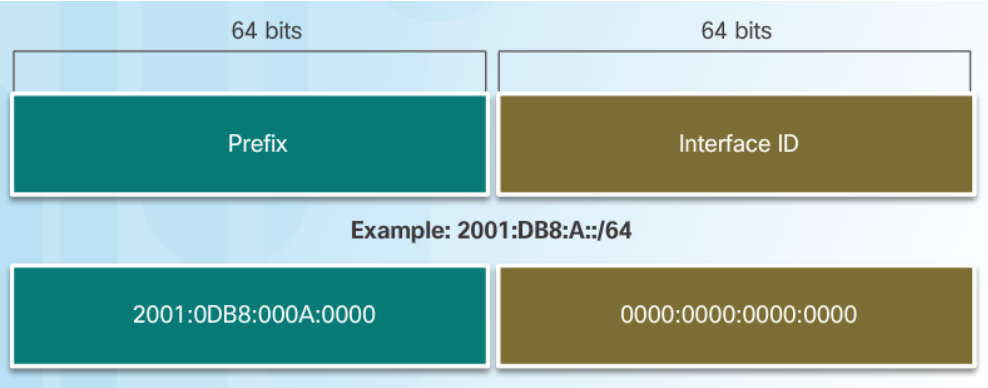
- loopback
  - 0:0:0:0:0:0:0:1 => ::1
- unspecified
  - Indique l'absence d'une adresse
  - 0:0:0:0:0:0:0:0 => ::
  - Ne doit pas être utilisée comme adresse de destination

IPv6 – types d'adresses

- Adresses Unicast
  - Associées à une seule interface
  - IPv6 contient plusieurs types (global, link local, etc).
- Multicast
  - Adresse de diffusion "un vers plusieurs"
  - Permet une utilisation plus efficace du réseau
  - Remplace (avantageusement) la diffusion Broadcast
- Anycast - "un vers le plus proche"
  - Permet à plusieurs dispositifs de partager une même adresse
    - Tous les nœuds doivent offrir les mêmes services
  - Les routeurs décident quel est le dispositif le plus proche
  - Adapté à l'équilibrage de charge et au contexte
- **On n'a plus les adresses de BROADCAST !**

Et les masques IPv6 (Préfixes) ?

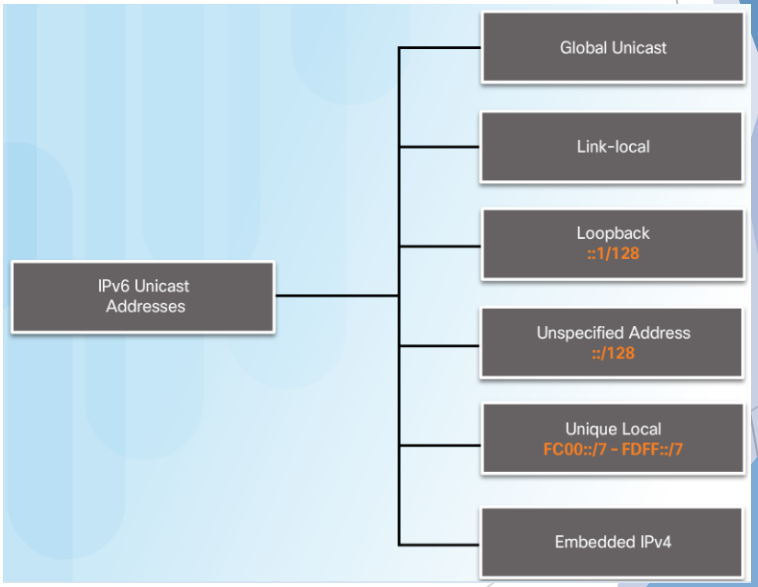
- Tout comme dans IPv4, le préfixe IPv6 est utilisé pour indiquer le nombre de bits de la partie hôte
  - La longueur du préfixe peut aller de 0 à 128
  - Le préfixe typique pour les LANs est /64



Adresses IPv6

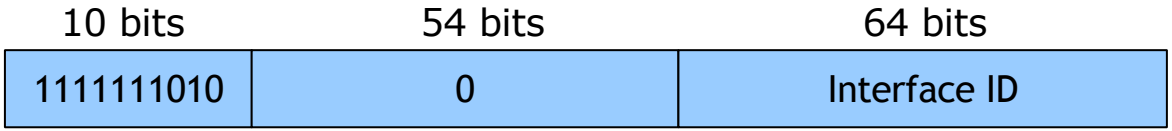
- **Dans IPv6, une interface peut avoir plusieurs adresses simultanément !!!!**
- **Alors on peut avoir :**

  - **Global Unicast** – adresse global unique, routable sur Internet
  - **Link-local** – adresse local, utilisé à l'intérieur d'un segment (équivaut à l'adresse MAC en couche 3). Utilisé pour les communications "internes" (routage, etc.)
  - **Unique Local** – adresse IPv6 limité à l'intérieur d'un LAN. À proscrire



UNIVERSITÉ DE REIMS CHAMPAGNE ARDENNE

Adresses Lien Local



FE80::/64

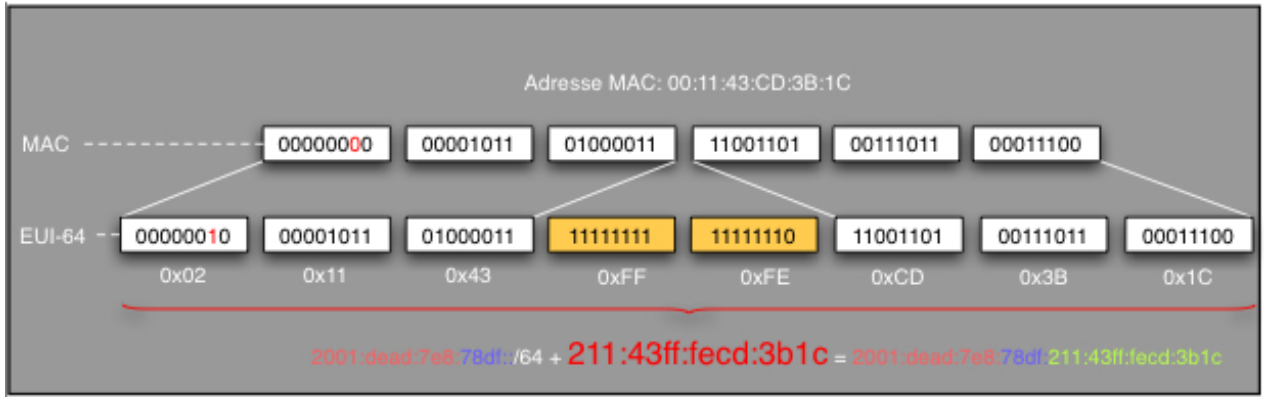
```
machine ~ # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:11:43:CD:3B:1C
          [..]
          inet6 addr: fe80::211:43ff:fecd:3b1c/64 Scope:Link
          [..]

machine ~ # ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:11:43:CD:3B:1D
         [..]
          inet6 addr: fe80::211:43ff:fecd:3b1d/64 Scope:Link
         [..]
```

- **Comment obtenir l'Interface ID ?**

UNIVERSITÉ DE REIMS CHAMPAGNE ARDENNE

Interface ID

- Interface ID - Format EUI-64 obtenu en modifiant la représentation d'une adresse MAC sur 48 bits



- Pour s'assurer que l'adresse choisie corresponde à une adresse globale unique MAC, le bit universal/local **(U/L bit)** est défini comme **1** pour l'étendue globale **(0 pour l'étendue locale)**
  - **Le U/L bit est le 7ème bit du premier octet**

UNIVERSITÉ DE REIMS CHAMPAGNE ARDENNE

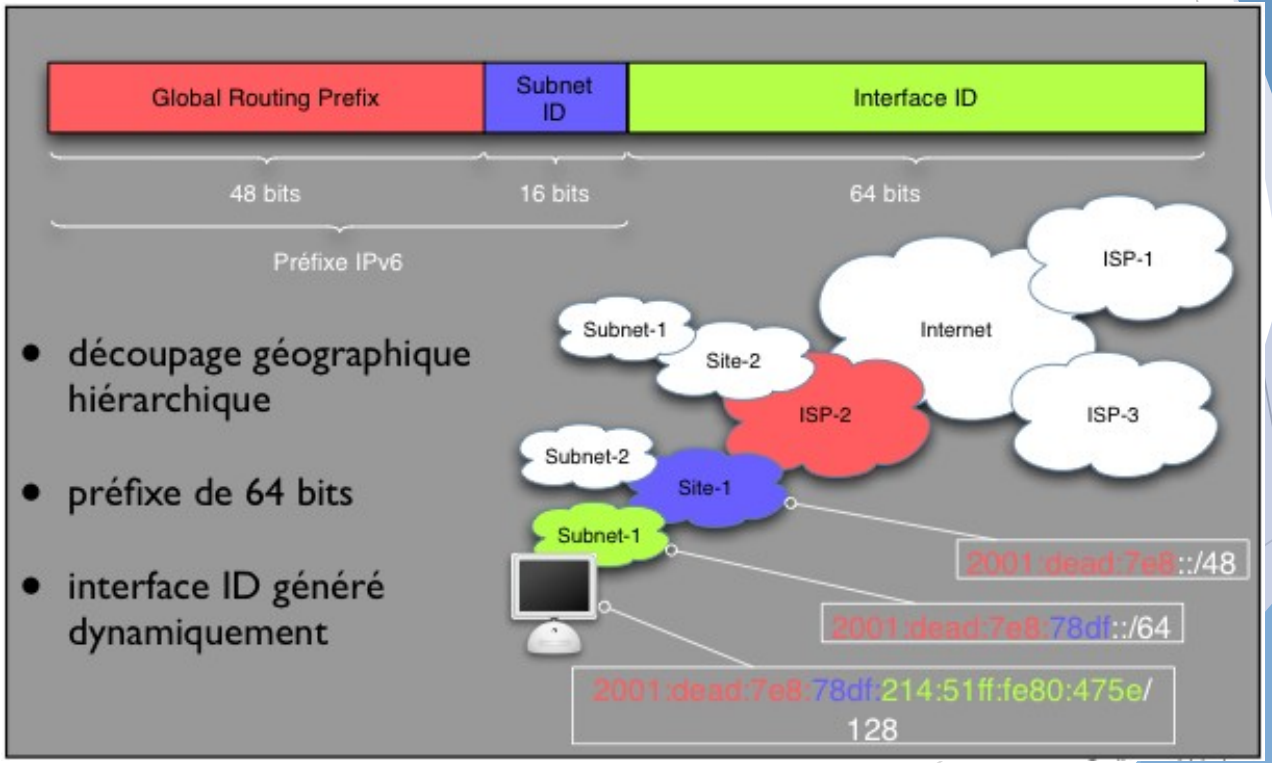
Les adresses globales "disponibles"

- L'espace d'adressage unicast IPv6 comprends tout l'espace IPv6
  - a l'exception du ***FF00::/8 (1111 1111)***, réservé aux adresses **multicast**
- Les adresses ***2000::/3 (001)*** à ***E000::/3 (111)***, doivent utiliser le format ***Extended Universal Identifier (EUI)-64***
  - obtenu à partir des adresses MAC des interfaces réseau
- Aujourd'hui, l'IANA distribue aux FAI des adresses IPv6 dans le plage ***2001::/16***.
  - généralement composé d'un préfixe global de **48 bits** et un identifiant de sous-réseau de **16 bits**

Adressage IPv6

- Espace d'adressage (IETF)
  - 0000::/8 Reserved by IETF [RFC3513]
  - 2000::/3 Global Unicast [RFC3513]
  - ~~FC00::/7 Unique Local Unicast [RFC4193]~~
  - FE80::/10 Link Local Unicast [RFC3513]
  - FEC0::/10 Reserved by IETF [RFC3879]
  - FF00::/8 Multicast [RFC3513]

Adresses Globales



Comment est attribuée une IPv6 ?

- De manière statique
- Auto-configuration (stateless)
  - Intégrée dans le protocole
  - Génération automatique des adresses à partir d'informations reçues par le routeur et de l'adresse MAC
  - L'auto-configuration est un processus à plusieurs étapes
  - Peut représenter quelques risques de sécurité
- DHCPv6
  - Un serveur DHCP est responsable pour l'attribution des adresses
  - L'administrateur garde un peu plus de contrôle sur les machines admises

Résultat

```
machine ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:43:CD:3B:1C
          inet addr:203.178.135.36  Bcast:203.178.135.128  Mask:255.255.255.128
          inet6 addr: 2001:200:0:1cd7:211:43ff:fecd:3b1c/64 Scope:Global
inet6 addr: fe80::211:43ff:fecd:3b1c/64 Scope:Link

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

Autoconfiguration ?

- En IPv4 on avait ARP et RARP qui pouvaient être utilisés pour le BOOTP
  - Ancêtre du DHCP
- En IPv6 on fait de l'auto-configuration grâce à la **découverte des voisins**
- Découverte de voisins
  - résolution IPv6 -> MAC (comme ARP avec IPv4)
- Découverte des routeurs
  - Obtention d'informations pour l'auto-configuration d'adresses
- Détection d'accessibilité des voisins
- Détection des adresses dupliquées
- Découverte des préfixes et paramètres du réseau

Les Quatre Messages

- Router Solicitation (RS)
  - utilisé par un nœud pour découvrir les routeurs sur le réseau
- Router Advertisement (RA)
  - utilisé par un routeur pour annoncer le préfixe à utiliser et d'autres options (ex: MTU du lien)
- Neighbor Solicitation (NS)
  - permet à un nœud de demander l'adresse MAC correspondante à une adresse IPv6
- Neighbor Advertisement (NA)
  - réponse au message NS

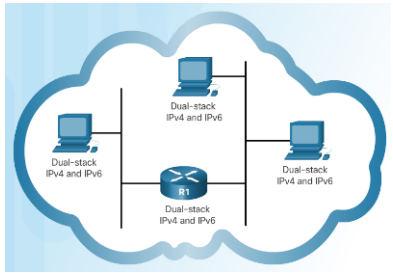
L'auto-configuration en résumé

- Soit donné l'adresse MAC 00:17:f2:ea:59:46

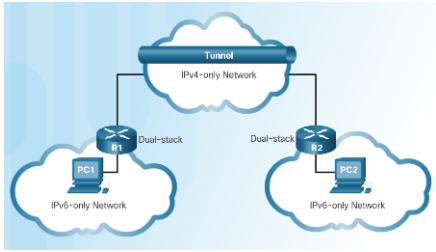
1. création d'une adresse lien-local
   - (fe80::**217:f2ff:feea:5946**)
2. vérification d'unicité de l'adresse lien-local
   - message NS sans réponse
3. récupération du préfixe IPv6 du lien
   - RS/RA (ex: **2001:db8:42**::/64)
4. création de l'adresse globale
   - (**2001:db8:42::217:f2ff:feea:5946**)
5. vérification d'unicité de l'adresse globale

Coexistence IPv4 et IPv6

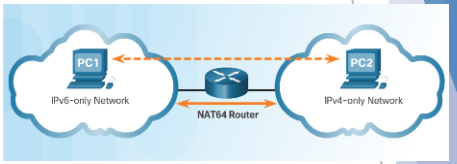
- Il existe plusieurs techniques de migration IPv4 à IPv6



Dual stack - Les dispositifs executant autant la pile IPv4 que la pile IPv6



Tunneling –Les paquets IPv6 sont encapsulés pour traverser des réseaux IPv4



Traduction - Network Address Translation 64 (NAT64) permet à un dispositif IPv6 de contacter un dispositif IPv4

UNIVERSITÉ DE REIMS CHAMPAGNE ARDENNE

En Résumé

- IPv4 a été la base de l'Internet actuelle
  - Adressage de taille fixe
  - Mécanisme de sous-réseaux
- Problèmes de IPv4
  - Espace d'adressage réduit
  - Mauvaise distribution des adresses
- Ce qui IPv6 apporte de nouveau
  - Espace d'adressage plus grand
  - Organisation vraiment hiérarchique
  - Découverte automatique du réseau
  - Peu de rupture avec le modèle précédent