ADMINISTRATION RÉSEAU
RÉSEAUX PRIVÉS & IPV6

A. Guermouche

Plan

Plan

Pourquoi avoir des adresses privées?

- Gérer la pénurie d'adresses au sein d'un réseau
- Masquer l'intérieur du réseau par rapport à l'extérieur (le réseau peut être vu comme une seule et même machine)
- Améliorer la sécurité pour le réseau interne
- Assouplir la gestion des adresses du réseau interne
- Faciliter la modification de l'architecture du réseau interne

$\rightarrow$ Mécanisme de translation d'adresses (NAT - Network Address Translation)

Deux types de NAT :

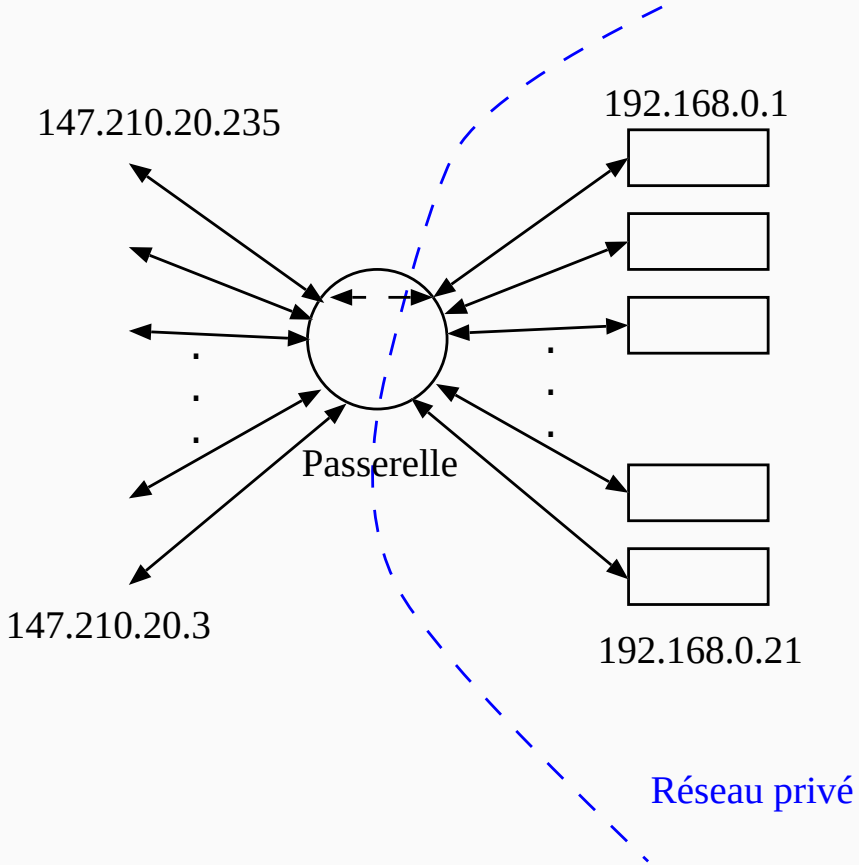
statique. association entre *n* adresses publiques et *n* adresses privées.

dynamique. association entre 1 adresse publique et *n* adresses privées.

Plan

NAT statique

Association entre une adresse publique et une adresse privée.



NAT statique

Association entre une adresse publique et une adresse privée.

Intérêt :

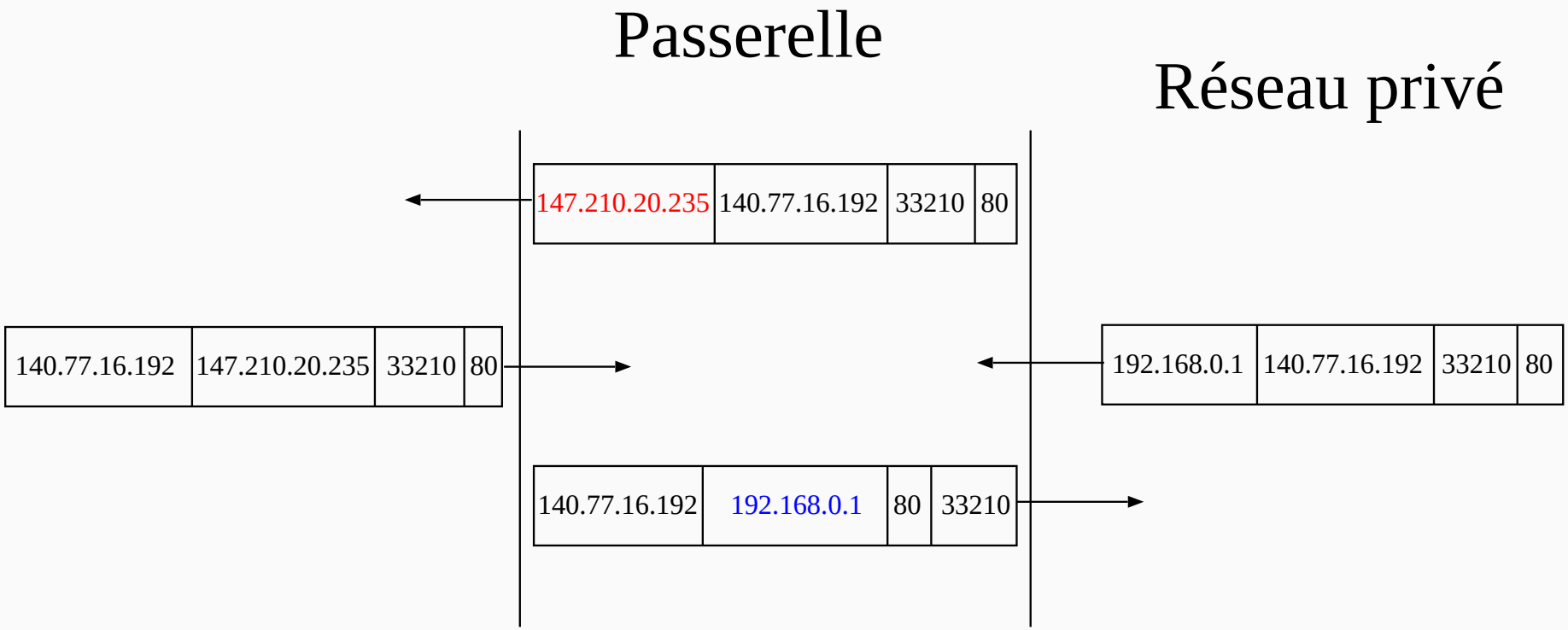
- Uniformité de l'adressage dans la partie privée du réseau (modification de la correspondance @publique/@privée facile)
- Sécurité accrue (tous les flux passent par la passerelle NAT)

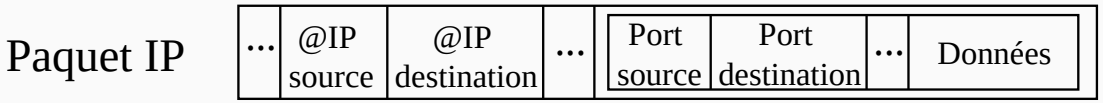
Inconvénient :

- Problème de pénurie d'adresses IP publiques non-résolu

NAT statique : Principe

Pour chaque paquet sortant (resp. entrant), la passerelle modifie l'adresse source (resp. destination).

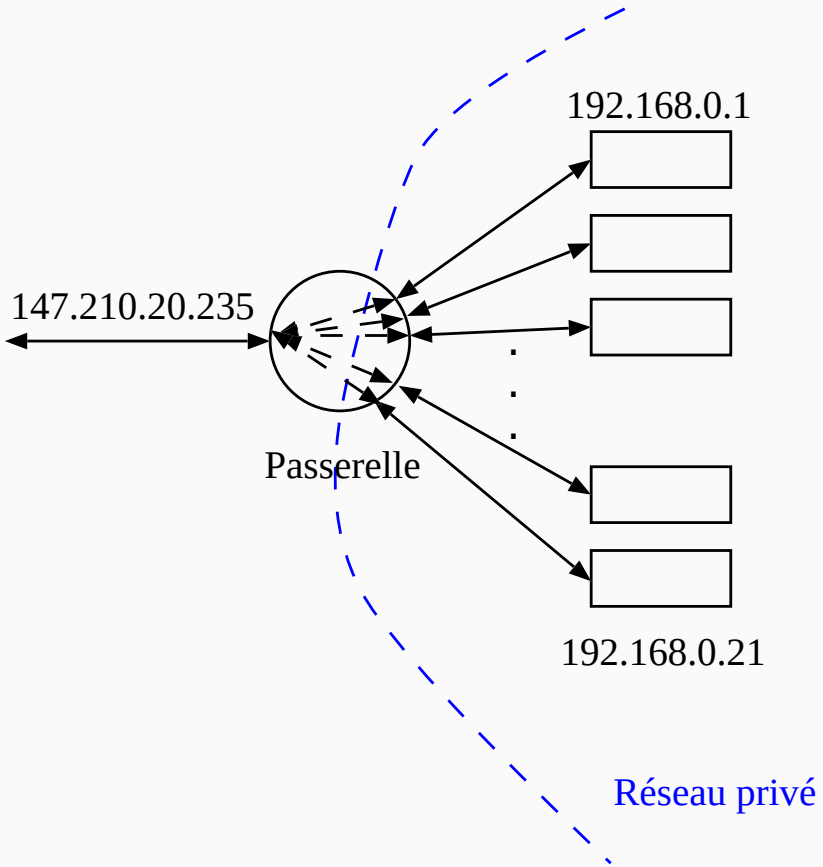




Plan

NAT dynamique : Masquerading

Association entre m adresses publiques et n adresses privées ($m < n$).



NAT dynamique : Masquerading

Association entre m adresses publiques et n adresses privées ($m < n$).

Intérêt :

- Plusieurs machines utilisent la même adresse IP publique pour sortir du réseau privé
- Sécurité accrue (tous les flux passent par la passerelle NAT)

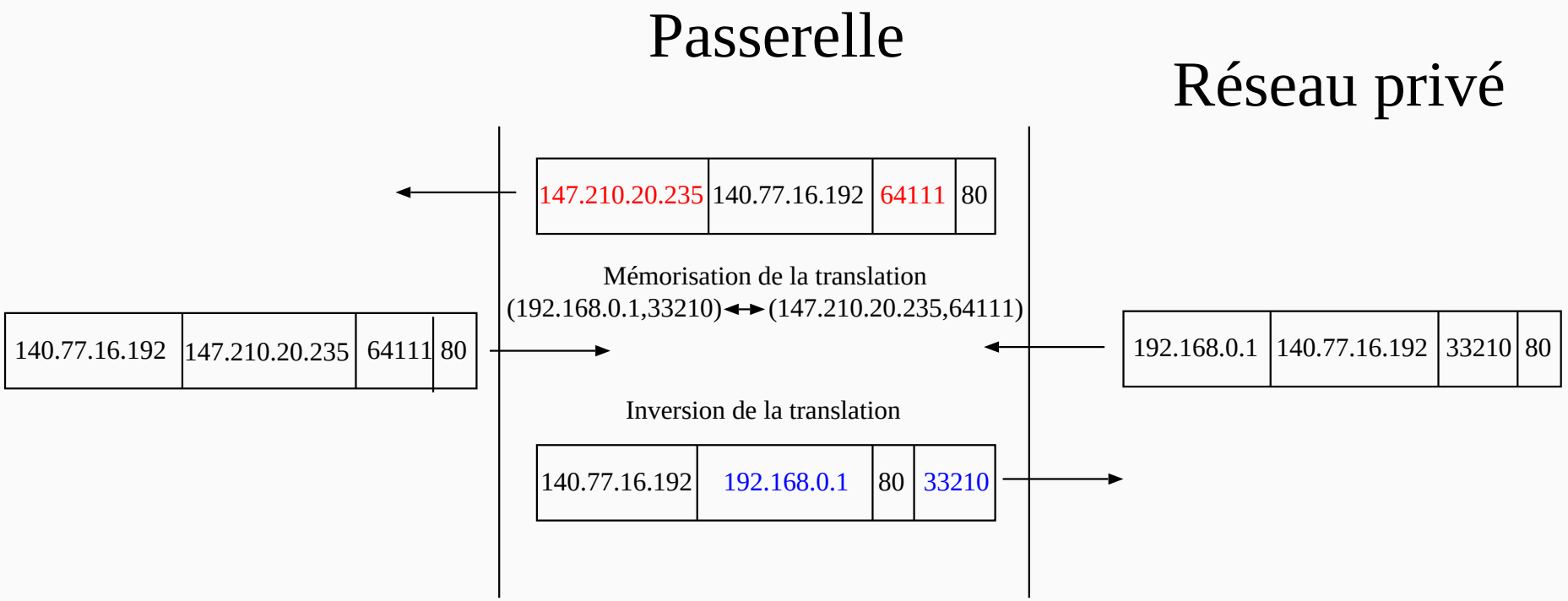
Inconvénient :

- Les machines du réseau interne ne sont pas accessibles de l'extérieur (impossibilité d'initier une connexion de l'extérieur)

NAT dynamique : Principe (1/2)

L'association de *n* adresses privées à 1 adresse publique nécessite, au niveau de la passerelle, de :

- modifier l'adresse source (resp. destination) des paquets sortant (resp. entrants)
- changer le numéro de port source pour les flux sortant



NAT dynamique : Principe (2/2)

Comment est ce que le routeur différencie les paquets qui lui sont destinés de ceux qu'il doit relayer?

À chaque nouvelle connexion :

1: Modifier l'adresse source et le port source : (@source_privée,port_source)$\rightarrow$(@publique,port_source')
2: Sauvegarder l'association dans la table `NAT`

Pour chaque paquet entrant :

3: Chercher une association correspondant au couple (@destination, port_destination)
4: **Si** $\exists$ une association dans la table `NAT` **Alors**
5: Modifier l'adresse de destination et le port de destination
6: Relayer le paquet
7: **Sinon**
8: /* Erreur de routage */
9: **Fin du Si**

NAT dynamique : Principe (2/2)

Comment est ce que le routeur différencie les paquets qui lui sont destinés de ceux qu'il doit relayer?

À chaque nouvelle connexion :

1: Modifier l'adresse source et le port source : (@source_privée,port_source)→(@publique,port_source')
2: Sauvegarder l'association dans la table `NAT`

Pour chaque paquet entrant :

3: Chercher une association correspondant au couple (@destination, port_destination)
4: **Si** ∃ une association dans la table `NAT` **Alors**
5: Modifier l'adresse de destination et le port de destination
6: Relayer le paquet
7: **Sinon**
8: /* Erreur de routage */
9: **Fin du Si**

Le routeur gère toutes les associations

⇒ Unicité de l'association (donc du port source après translation)

Problèmes liés à NAT dynamique

Comment faire de la translation d'adresse sur des protocoles qui ne sont pas basés sur TCP ou UDP (pas de numéro de port)?

- Nécessité d'implémenter une méthode spécifique au protocole (identifiant ICMP pour ICMP par exemple).
- Dans le cas des protocoles dont les paquets contiennent des données relatives aux adresses IP, il est nécessaire de mettre en place des "proxy" (`FTP` en mode actif par exemple).

Comment rendre joignables des machines du réseau local?

- Nécessité de faire de la redirection de port (port forwarding/mapping).

  Principe. Toutes les connexions entrantes sur un port donné sont redirigée vers une machine du réseau privé sur un port (qui peut être le même ou non).

Plan

Proxy ou mandataire

Définition :

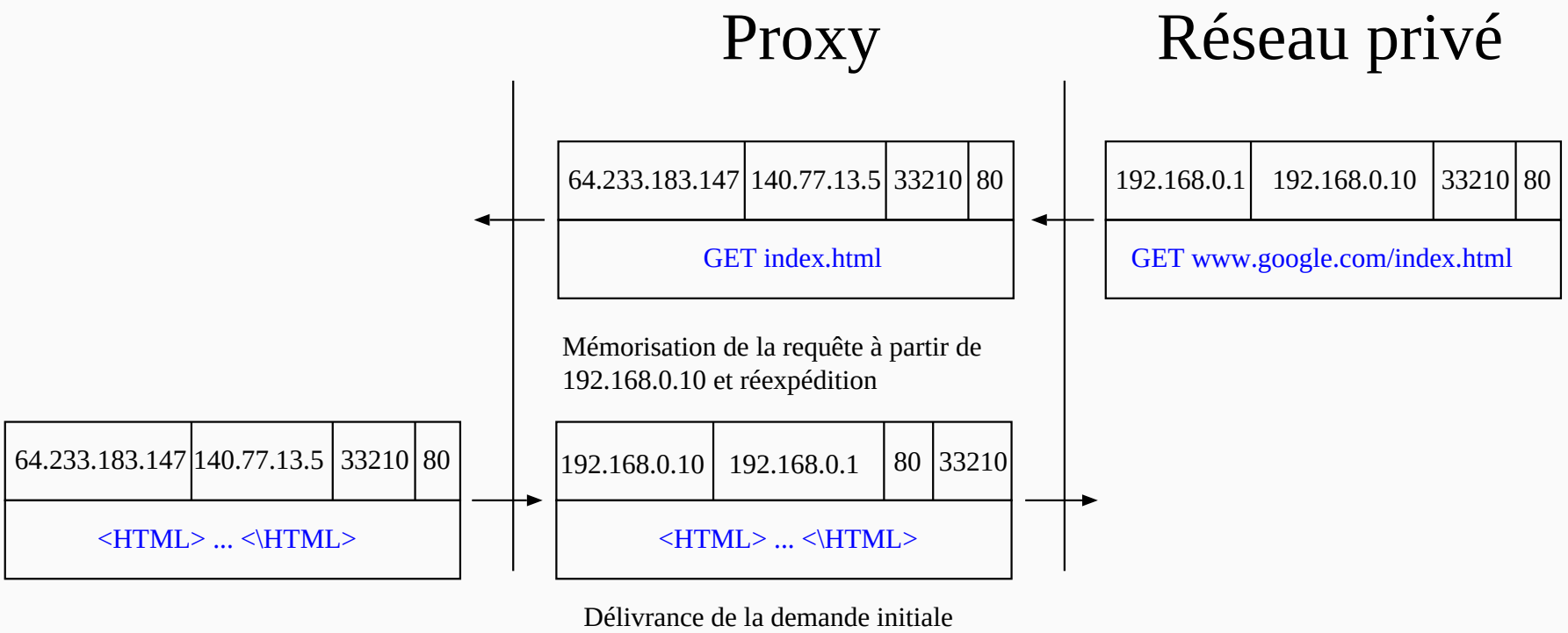
- Un proxy est un intermédiaire dans une connexion entre le client et le serveur
- Le client s'adresse toujours au proxy
- Le proxy est spécifique à une application donnée (`HTTP`, `FTP`, ...)

$\rightarrow$ Possibilité de modification des informations échangées entre le client et le serveur.

Proxy ou mandataire

Définition :

- Un proxy est un intermédiaire dans une connexion entre le client et le serveur
- Le client s'adresse toujours au proxy
- Le proxy est spécifique à une application donnée (`HTTP`, `FTP`, ...)



Plan

IPv6

Pourquoi?

Réponse pour le problème de la croissance de l'Internet

- Nouveaux réseaux
- Nouvelles machines/dispositifs
- Utilisation mobile/nomade

Comment?

Augmenter la longueur des adresses à 128 bits (16 octets) en gardant les bonnes propriétés d'IPv4

Avec 128 bits:

- Approximativement 506102 adresses par m^2 sur terre
- ou encore ~10^{28} adresses par habitant

Adressage IPv6

- Adresse sur 128 bits découpée en 8 mots de 16 bits
  - Utilisation de chiffres hexadécimaux pour gagner de la place
  - FEDC:0000:0000:0065:4321:0000:DEAD:BEEF
- Possiblité de supprimer les 0 de poids fort dans un block
  - FEDC:0000:0000:65:4321:0000:DEAD:BEEF
- Possibilité de supprimer les premiers blocks de 0 consécutifs pour les remplacer par ::
  - FEDC::65:4321:0000:DEAD:BEEF
- Exemple d'utilisation : http://[FEDC::65:4321:0000:DEAD:BEEF]

Modèle d'adressage

Chaque interface a plusieurs adresses différentes

Link local, préfixé par FE80::/10 (1111 1110 10)

- Utilisé uniquement entre des hôtes IPv6 adjacents
- Les paquets ne sont PAS transmis par les routeurs
- Assigné automatiquement au démarrage

Unique local, préfixé par FC00::/7 (1111 110)

- Utilisé uniquement en interne sur un réseau
- Non routable sur l'Internet mondial

Global

- Équivalent à une adresse publique IPv4

Types d'adresse IPv6

Adresses Unicast

- Associées à une seule interface

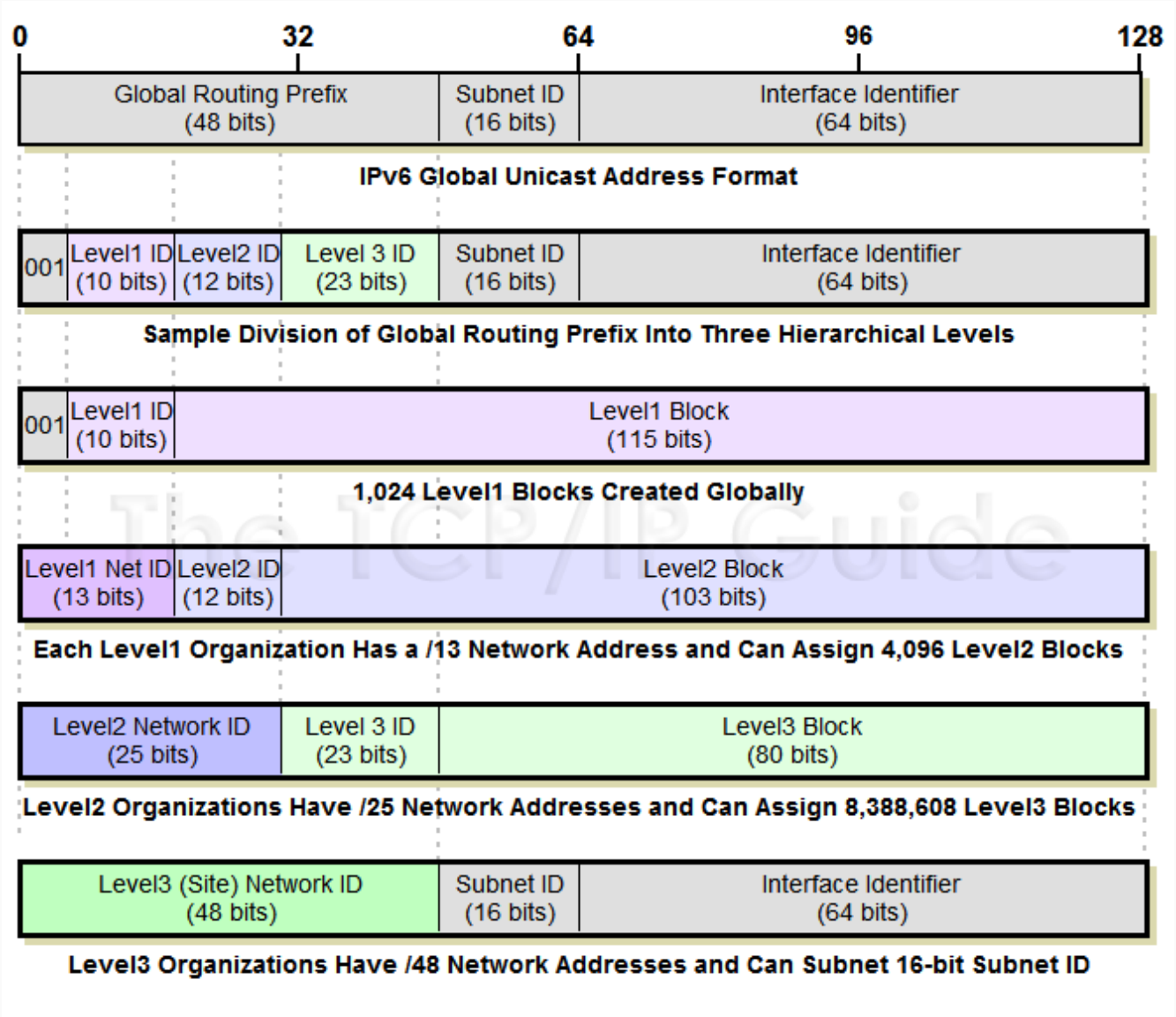
Adresses Multicast

- Adresse de diffusion « un vers plusieurs »
- Remplace (avantageusement) le Broadcast

Adresses Anycast

- « un vers le plus proche »
- Un identifiant pour un ensemble d'interfaces (appartenant généralement à différents noeuds).
- Un paquet envoyé à une adresse anycast est délivré à l'une des interfaces identifiées par cette adresse (la plus "proche").

Structure d'une adresse IPv6



source http://www.tcpipguide.com/free/diagrams/ipv6unicastsample.png

Neighbour Discovery Protocol (NDP)

Neighbour Discovery

IPv6 utilise une série de protocoles connus sous le nom de *Neighbour Discovery*, qui prennent la forme de messages ICMPv6 unicast ou multicast locaux

- 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

NDP: Types des messages

Router Solicitation (RS)

Utilisé par un noeud 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)

Neighbour Solicitation (NS)

Permet à un noeud de demander l'adresse MAC correspondante à une adresse IPv6

Neighbour Advertisement (NA)

Réponse au message NS

Plus un message de type *Redirect*

Structure d'une adresse mutlicast (1/2)

Types

- Tous les noeuds dans un ségment ff02::1
- Tous les routeurs dans un ségment ff02::2
- cas particulier de *solicited-node multicast address*: ff02::1:ffxx:xxxx où les x correspondent aux 24 bits de poids faible de l'adresse IPv6 du noeud.

Quid de l'adresse MAC?

Toutes les adresses multicast de la couche 3 ont une adresse MAC de couche 2 correspondante (33:33:xx:xx:xx:xx) où xx:xx:xx:xx sont les 32 derniers bits de l'adresse multicast de la couche 3

Structure d'une adresse mutlicast (2/2)

Exemple:

- Je souhaite envoyer un multicast vers le groupe contenant le noeud dont l'adresse est 2001:44b8:41e1:cc00:843e:7b93:daa0:6e09
- L'adresse de multicast de type *solicited-node* sera construite comme suit:

  adresse unicast 2001:44b8:41e1:cc00:843e:7b93:daa0:6e09
  adresse multicast ff02::1:ffa0:6e09 (24 derniers bits)
- Lorsque ce paquet sera envoyé, l'adresse MAC de destination sera 33:33:ff:a0:6e:09
  - Conserver les 32 bits de poids faible de l'adresse de multicast ff02::1:ffa0:6e09
  - Les concaténer à 33:33 pour former une adresse MAC valide: 33:33:ff:a0:6e:09

SLAAC: *Stateless address autoconfiguration*

SLAAC est un mécanisme d'auto-configuration en deux phases.

Phase 1 - Étapes pour la connectivité locale

1. Génération de l'adresse locale de liaison : Chaque fois qu'une interface IPv6 compatible avec le multicast est mise en service, le noeud génère une adresse locale de liaison pour cette interface.
2. Détection des doublons (*DAD*): Avant d'attribuer la nouvelle adresse locale à son interface, le noeud vérifie que l'adresse est unique. Pour ce faire, il envoie un message de sollicitation du voisin destiné à la nouvelle adresse. S'il y a une réponse, l'adresse est alors un double et le processus s'arrête, nécessitant l'intervention de l'adminstrateur.
3. Si l'adresse est unique, le noeud l'attribue à l'interface pour laquelle elle a été générée.

SLAAC: *Stateless address autoconfiguration*

SLAAC est un mécanisme d'auto-configuration en deux phases.

Phase 2 - Étapes de la connectivité globale

1. Annonce du routeur : Le noeud envoie une sollicitation au routeur pour inciter tous les routeurs sur le lien à lui envoyer des annonces de route. En réponse à ce message, le routeur annonce un préfixe de sous-réseau à utiliser par les hôtes.
2. Génération d'adresses globales : Lorsqu'il reçoit un préfixe de sous-réseau d'un routeur, l'hôte génère une adresse globale en ajoutant l'ID d'interface au préfixe fourni.
3. Utiliser DAD pour vérifier que la nouvelle adresse est unique et finaliser la configuraiton.