- Partie 3 -
IPv6 et sécurité

Problèmes d 'IPv4

- taille de l'Internet **double** tous les 6 mois
- saturation de l'espace d'adressage prévue pour 2010
  - 150 000 réseaux en mars 2000
  - qlq millions d'ici peu
  - théoriquement, 16 millions de réseaux possibles mais la répartition en classe pose problème
- **saturation** de la classe B => allocation d'adresses de classe C contigües
- taille recommandée du datagramme insuffisante pour des longs chemins de données (576 octets)
- explosion de la taille des tables de routage

1000 réseaux sur le réseau central

- besoin de **QoS** pour les nouvelles applications multimédia (maintien du débit, garantie du délai !!!)
- plus de **sécurité** (chiffrement)

IPv6 : Objectifs

1. **Résoudre le problème de pénurie d'adresses d'IPv4 :**
   - 4.3 Milliards IPv4 disponibles – 240 Millions réellement utilisables
   - 172 millions de hosts IPv4 actifs (Janv. 2003)
   - 73 % des adresses IPv4 sont octoyées aux organismes nord-américains
     - Vietnam (100 Millions d'hab. – 4 classes C)
     - Sénégal (10 millions d'hab. - 16 adresses de classe C)
     - Tunisie (8 milions d'hab. – 16 classes C pour l'administration)
2. **Résoudre les problèmes de dimensionnement des tables de routage :**
   - Mars 2002: 150 000 routes IP4 + 400 routes IP6 ds les routeurs backbones BGP
   - Accroissement de 20% par an
   - L'horizon de l'Internet est de 40 routeurs
   - Route moyenne traverse 25 routeurs;
3. **Inclure de nouvelles fonctionnalités :**
   - le multipoint, la sécurité, la mobilité,
   - La configuration automatique des stations
   - La qualité de service, etc…

IPng : normalisation

- **1983 :** 100 ordinateurs TCP/IP dans le monde
- **1985** : création du DNS (Domain Name System)
- **1992** : Utilisation commerciale et explosion de la demande d'adresses IP
- **Juillet 1994** : Prise de conscience du risque de pénurie et création des groupes de travail IPNG (IP Next Generation) et NGTRANS (IPng Transition)
- **Décembre 1994** : Evaluation des propositions et choix de SIPP (Simple Internet Protocol Plus) renommé IPv6 [RFC 2460].
- **1996-1997** : déploiement du 6BONE (les réseaux IPv6 de test mondiaux)
- **Décembre 1998** : le plan d'adressage est sélectionné et création de l'ICANN (qui remplace l'IANA)
- **Juillet 1999** : début allocation des prefixes IPv6 par l'ICANN (qui remplace l'IANA)
- **1999 - …** : Elaboration des schémas de migration et d'intégration de IPv4-IPv6
- **Fin 2001** : 3GPP/UMTS adopte IPv6

IPv6 et Operating Systems

- CISCO IOS 12.2 et supérieure
- JUNIPER JUNOS 5.1 et supérieure

- Windows NT et Windows 2000 avec l'installation d'un patch
  - Research.microsoft.com/msripv6/
  - www.microsoft.com/Windows2000/technologies/communications/ipv6/
- Windows XP en natif
  - Taper la commande « ipv6 install » puis vérifier avec « ipv6 if »
  - Aplications IPv6 livrées : ping6, traceroute, ftp, telnet, IE, IPsec,
- MacOS 10.1 et MacOS X

- IBM AIX 4.3 et supérieure
- Solaris 8 et supérieure
- Compaq True64 UNIX et OpenVMS v5.1 et supérieure,
- HP-UX 11i et supérieure
- Linux 2.4 et supérieure (RedHat 7.1 – Mandrake 8.0)
- FreeBSD 4.0 et supérieure

Réseaux IPv6 existants

- Où trouver des services IPv6 ?
  - Réseaux de campus/sites (nuages IPv6 dans un océan IPv4)
  - Réseaux régionaux de collecte (non, problème majeur : tunneling IPv6 over IPv4)
  - Réseaux nationaux/internationaux (oui voir ci-dessous)

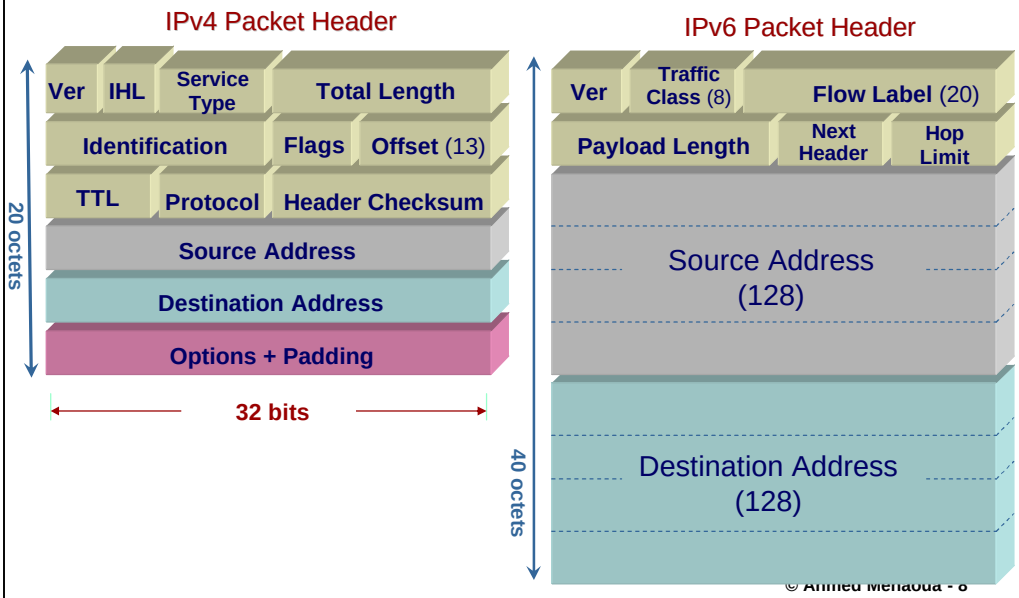
- Services commerciaux :
  - Offre commerciale de NT&T (depuis mars 1999) : 1er service d'interconnexion IPv6 à l'echelle mondiale (payant)
  - Offre commerciale de l'Opérateur scandinave Télia (depuis juin 2001). POP malmoe, stockolm, Londres, Oslo, …
  - En France : ISDnet (Cable&Wireless), Matra-Grollier, Nérim, Frontier On Line, Gitoyen, SDV Plurimedia, ClaraNet, Tiscali Telecom,
  - SPHINX, 3 Nœuds POP Français pour le transit IPv6 entre les ISP (géré par GIP-RENATER)

- Réseaux académiques :
  - Renater 3 (France métropolitaine, dom-tom)
  - Le G6Bone (France) : depuis 1996, 40 sites raccordés via des tunnels IPv6 dans IPv4
  - GEANT (réseau Pan-européen de la recherche – 3000 universités – co financé par la CEE)
  - Le 6Bone (Internet V6 experimental) : depuis 1996, 40 pays et 500 sites (www.6bone.net)

IPv6 : nouvelles fonctionnalités

1. **Autoconfiguration: « plug and play »**
   - **Protocoles DHCP v6 (Dynamic Host Configuraton protocol) [RFC 1541]**
   - **Protocole SAA (Stateless Address Autoconfiguration Protocol) [RFC 2462]**
     - **Construire une adresse IPv6 simplement**
   - **Protocole Neighbor Discovery (ND) [RFC 2461]**
     - **Découverte des voisins, adresses MAC (ARP), des routeurs,**
     - **Meilleure gestion de la mobilité, et du changement de prestataire,**
   - **Protocole Path MTU discovery (pMTU) [RFC 1981]**
     - **Réduire la fragmentation des paquets par les routeurs**
     - **pMTU compris entre 1280 et maxMTU**
     - **Exploite un message d'erreurs ICMPv6 « Paquet Trop grand » envoyé par les routeurs sur le chemin**

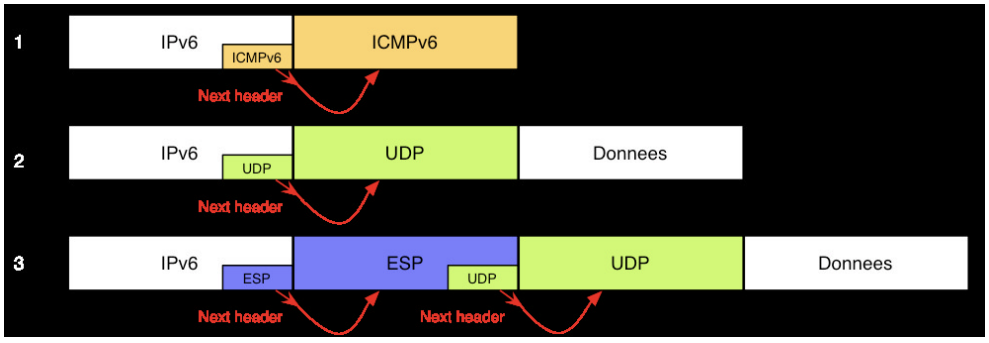
IPv4 vs IPv6



IPv6 : Extensions

- *Next header* (8 bits)
  - Indique le TYPE de l'en-tête encapsulé, et l'existence d'EXTENSIONS
    - IPv4 utilise les OPTIONS qui sont analysées par tous les routeurs
    - IPv6 utilise les EXTENSIONS qui peuvent être traitées :
      - par chaque nœud traversé (hop-by-hop) (HHH) = 0
      - par la destination finale uniquement (end-to-end) = 60
  - le TYPE peut correspondre à un protocole de niveau 3 ou 4
    - TCP (6), UDP (17), ICMPv6 (58), IPv6 (41), ou IPv4 (4)
  - ou à une ou plusieurs Extensions chaînées (taille multiple de 8 octets) :
    - Information de Routage par la source (RH) = 43
    - Info. d'authentification (AH) = 51
    - Info. de confidentialité (ESP Encapsulating Security Payload) = 50
    - Info. de fragmentation (FH) = 44

Chaînage des en-têtes



Header Type

Decimal	Keyword	Header Type
	HBH	Hop-by-hop (IPv6)
1	ICMP	Internet Control Message (IPv4)
2	IGMP	Internet Group Management (IPv4)
2	ICMP	Internet Control Message (IPv6)
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (IPv4 Encaptulation)
5	ST	Stream
6	TCP	
17	UDP	
29	ISO-TP4	
43	RH	Routing Header (IPv6)
44	FS	Fragmentation Header (IPv6)
45	IDRP	Interdomain Routing
51	AH	Authentication header (IPv6)
52	ESP	Encrypted Security Payload
59	Null	No next header
60	ISO-IP	CLNP
88	IGRP	
89	OSPF	Open Shortest Path First

IPv6 : adressage

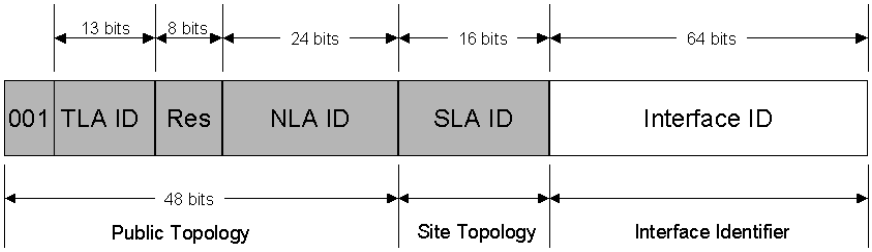
- **Passage de 4 à 16 octets pour l'adressage (RFC 3513):**
  - **2^{128} @ $3x10^{38}$ équipements adressables**
  - **$6x10^{22}$ adresses au m^2 sur terre**

- **Plan d'adressage agrégé : Adressage hiérarchique (RFC 2374)**
  - **Diminution taille des tables de routage / temps de traitement des paquets**
  - **En pratique :**
    - **10^{33} adresses (dû à la hiérarchie)**
    - **$3x10^{18}$ adresses par mètre carré sur la terre**

- **3 niveaux de hiérarchie :**
  1. **Une topologie publique (48 bits) : TLA Top Level Aggregator**
  2. **Une topologie de site (16 bits) : SLA Site Level Aggregator**
  3. **Un identifiant d'interface (64 bits) : IID Interface Identifier**

- **3 types d'adresse IPv6 :**
  1. **globales (utilisation du plan agrégée),**
  2. **site local ou link local, etc… (adresses privées)**
  3. **compatible IPv4 ou adresse "mappée« (tunneling)**

Plan d'adressage Agrégé



- ***Format Prefix*** **(3 bits)** — **Type de Plan d'adressage**
  - **001 : plan agrégé**
  - **010 : plan de test**
- ***Top Level Aggregator*** **(13 bits)** — **identifie les fournisseurs/opérateurs internat.**
- ***Reserved*** **(8 bits)** — **pour utilisation future (entre TLA et NLA)**
- ***Next Level Aggregator*** **(24 bits)** — **identifie les fournisseurs/opérateurs régionaux ainsi que l'identifiant du site (décomposition et allocation sous la responsabilité du TLA)**
- ***Site Level Aggregator*** **(16 bits)** — **identifie les sous-réseaux dans le site (sous la responsabilité de l'administrateur du site)**

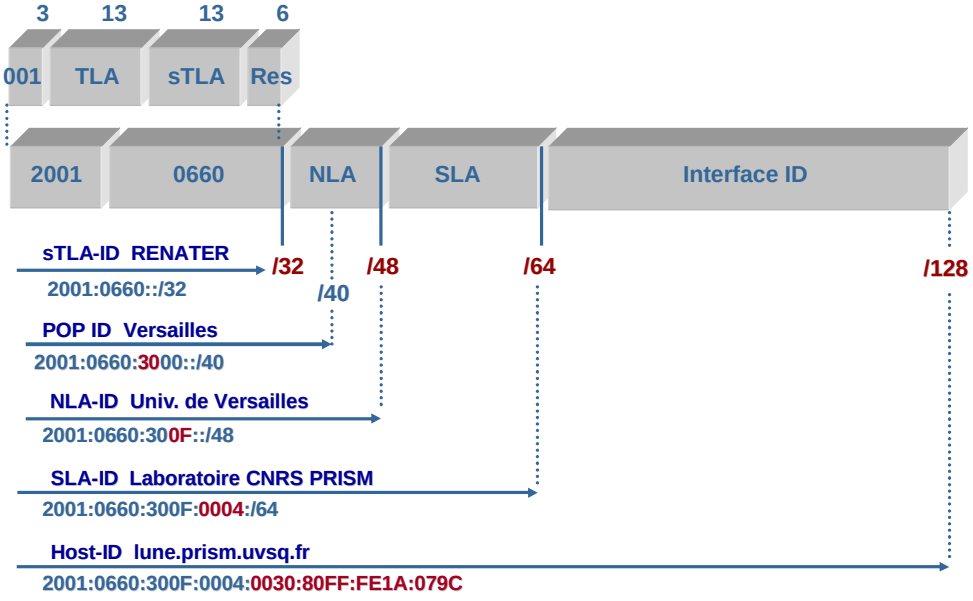
Allocation des Adresses

Attribution des Adresses

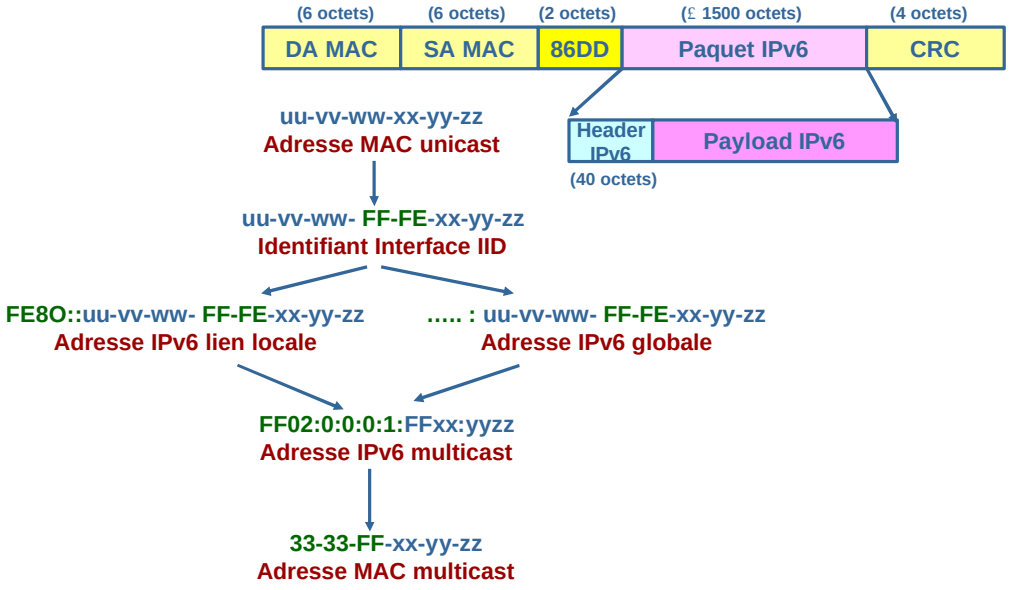
- **Pour obtenir un préfixe sub-TLA de 32 bits en Europe (délais 48h):**
  - **Être membre du RIPE-NCC (Réseaux IP Européen-Network Coordination Centre)**
    - **Abonnementt annuel : 2750-3750-5250 Euros (dépend du nbre @ utilisés)**
  - **Remplir le formulaire RIPE-195 sur www.ripe.net puis l'envoyer à hostmaster@ripe.net**
    - **France Telecom** **2001:0688::/32** **(depuis juin 2000)**
    - **Renater** **2001:0660::/32**
    - **Nerim** **2001:07A8::/32**
    - **Tiscali** **2001:BC8::/32**

- **4 Conditions d'attribution à vérifier (Phase de BootStrap):**
  1. **Être un opérateur IPv4 avec au moins 3 peering actifs avec d'autres AS**
  2. **Avoir au moins 40 clients IPv4 ou une expérience sur le réseau test 6bone (pTLA)**
  3. **Envisager d'offrir des services IPv6 dans les 12 prochains mois**
  4. **Maintenir un service DNS forward (AAAA) et reverse (ip6.int)**

Allocation des Adresses

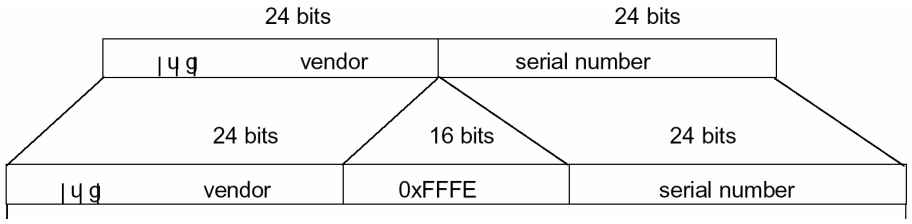


IPv6 et Ethernet



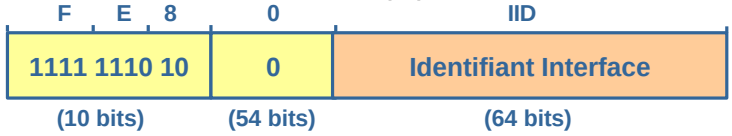
Plan d'adressage Agrégé

– ***Interface Identifier*** **(IID) (64 bits)** **identifie le terminal**
  - **conversion de l'adresse MAC (48 bits)**
  - **Exemple :**
    – **adresse MAC : 02:A0:24:E3:FA:4B**
    – **adresse IID : 02A0:24FF:FEE3:FA4B**



Adresse IPv6 spéciales

– **Lien locale :** Validité restreinte à un lien/segment Ethernet
  - Configuration automatique lors du boot de la machine par l'ajout du préfixe « FE80::0/64 » à l'identifiant de l'interface (IID)



– **Site Locale :** Validité restreinte à un réseau IP interne

– **IPV4 compatible :** pour traverser un backbone IPV6 par tunneling

Autoconfiguration

3 procédures possibles d'autoconfiguration d'une interface :

1. Création d'une adresse Lien-locale

- **Combiner** le préfixe FE80::/64 et l'adresse MAC de la machine,
- **Vérifier** l'unicité de l'adresse au moyen des messages ICMPv6 « Sollicitation d'un voisin » et « Annonce d'un voisin »

2. Autoconfiguration sans Etat (adresse globale)

- **Combiner** le prefixe du site reçu d'un routeur (message Router Advertisement) et l'adresse MAC de la machine
- **Vérifier** l'unicité de l'adresse au moyen des messages ICMPv6 « Sollicitation d'un voisin » et « Annonce d'un voisin »

3. Autoconfiguration avec Etat (adresse globale)

- Via un serveur DHCPv6

IPv6 et Programmation

- **Les applications IPv4 existantes doivent être mise à jour pour fonctionner sur un terminal IPv6-only,**
- **L'interface de programmation (API) sous Unix (Socket) et sous Windows (WinSock) s'est enrichie de :**
  1. **Nouvelles structures de données adresses**
  2. **Nouveaux types de données**
  3. **Nouvelles fonctions de conversions d'adresses**
  4. **Nouvelles primitives de conversion entre noms et adresses**

IPv6 et Programmation

- **Nouvelles déclarations de types et protocoles :**

```
# define   PF_INET6      AF_INET6
sock = socket (PF_INET6, SOCK_DGRAM, 0);
```

- **Nouvelles structures pour stocker les adresses IPv6 :**

```
Struct sockaddr_in6   {
    u_int8_t          sin6_len;          /*  longueur de la structure  */
    sa_family_t       sin6_family;       /*  AF_INET6   */
    in_port_t         sin6_port;         /*  numéro de port   */
    unint32_t         sin6_flowinfo;     /*  identificateur de flux  */
    struct  in6_addr  sin6_addr;         /*  adresse IPv6   */
    uint32_t          sin6_scope_id;     /*  portée de l'adresse  */
```

- **Nouvelles primitives de conversion entre noms et adresses :**

  gethostbyname(), gethostbyaddr(), getservbyname() et getservbyport(),* remplacées par : *getaddrinfo(), getnameinfo()

- **Nouvelles primitives de conversion d'adresses (texte <-> numérique):**

  inet_addr() et inet_ntoa() remplacées par : inet_pton() et inet_ntop()

Faiblesses

- Services de confidentialité et d'intégrité des données niveau de l'application (PGP/PEM, S-HTTP) :
  - Pas assez flexible
  - Propre aux applications

IPSec

Sécurité au niveau de chaque paquet IP

Les services IPsec

- **IPsec offre :**
  - **Sécurisation du niveau Réseau :**
    - **Authentification - Non-répudiation**
    - **Confidentialité - Intégrité**
    - **Anti-rejeu**
  - **Deux modes d'utilisation d'IPsec**
    - **Mode transport**
    - **De bout en bout**
  - **Mode tunnel**
    - **Encapsulation des données**
    - **VPN**

- **IPsec permet :**
  - **Création de VPN**
  - **Sécuriser les accès distants (Utilisation nomade)**
  - **Protection d'un serveur sensible**

Composants d'IPsec

- Protocoles de sécurité :
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)
- Protocole d'échange de clefs :
  - Internet Key Exchange (IKE)
- Bases de données internes :
  - Security Policy Database (SPD)
  - Security Association Database (SAD)

Politique de sécurité d'IPsec

- Politiques = ensemble de règles
- Locale à chaque machine
- Expression :
  - Règles de « filtrage »
  - Pas de norme de représentation

IPv6 : Conclusion

- **Raisons pour l'adoption de IPv6 :**
  1. **Pénurie d'adresses**
     - **Le réveil des pays de la zone Asie Pacifique**
  2. **Autoconfiguration**
     - **Grands parcs de machines**
  3. **Trouver une Killer application (exemple du Web pour l'adoption de TCP/IPv4)**
     - **Téléphonie mobile (GPRS, UMTS)**
     - **Domotique**
     - **Applications peer-to-peer (jeux réparties, voix sur IP)**
- **Raisons qui freinent l'adoption d'IPv6 :**
  1. **Disponibilté tardive du code IPv6 dans les terminaux et routeurs**
  2. **Manque d'applications compatibles IPv6 (règles de programmation non intégrées)**
  3. **Clients n'adoptent pas IPv6 car Opérateurs n'offrent pas d'interconnexion IPv6, mais opérateurs n'offrent pas d'accès IPv6 car pas de demandes de clients**
  4. **Le principal marché (Amérique du Nord) ne pousse pas vers la migration**
  5. **Frein psychologique : Complexité apparente des nouveaux protocoles**