HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

IPv6

Impacts et menaces

Nicolas Collignon
<Nicolas.Collignon@hsc.fr>

Plan

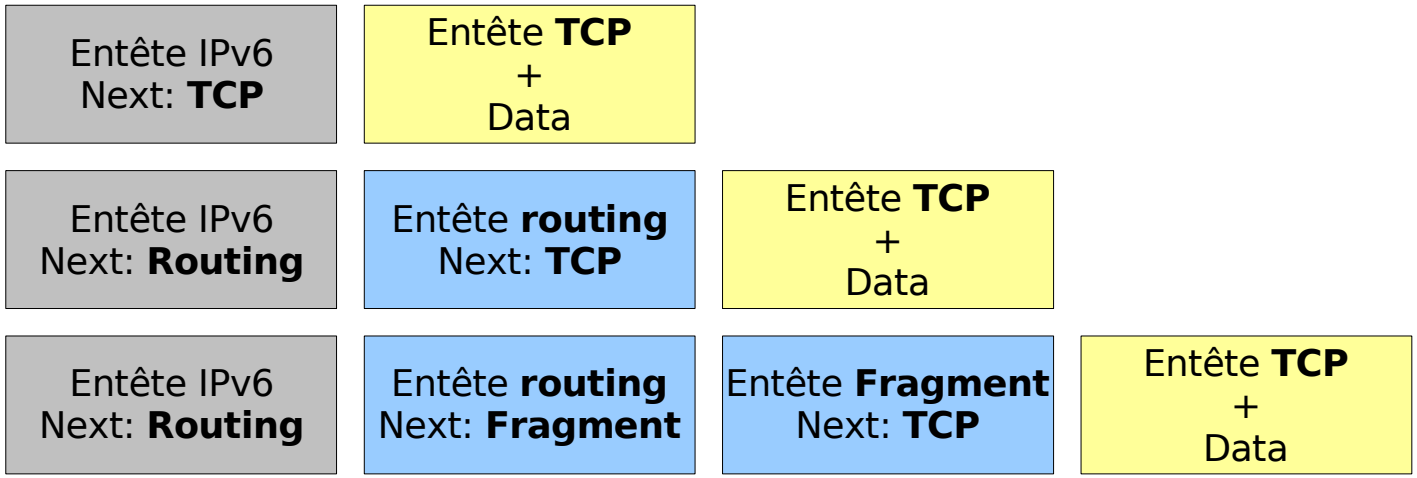
- IPv6 sur le lien
- Canaux cachés
- Routage et contournement d'ACL
- Découverte de réseaux
- Sécurité native du protocole et Systèmes de sécurité
- Impacts applicatifs
- Réseaux 3G et la mobilité IP

Neighbor Discovery

- Remplacement de ARP, niveau ICMPv6
- Basé sur le Multicast
- Auto-configuration des hôtes sur le lien. Tous les systèmes d'exploitation testés s'approprient:
  - Une ou plusieurs adresses Link-Local
  - Une ou plusieurs adresses globales si un routeur est sur le lien.
- Attaques envisageables:
  - Usurpation d'adresses de couche 2 indépendamment du type de transmission.
  - Déni de service sur les procédures DAD et NUD 
- SEND: 1 seul implémentation disponible (DoCoMo USA Labs)

L'en-tête IPv6

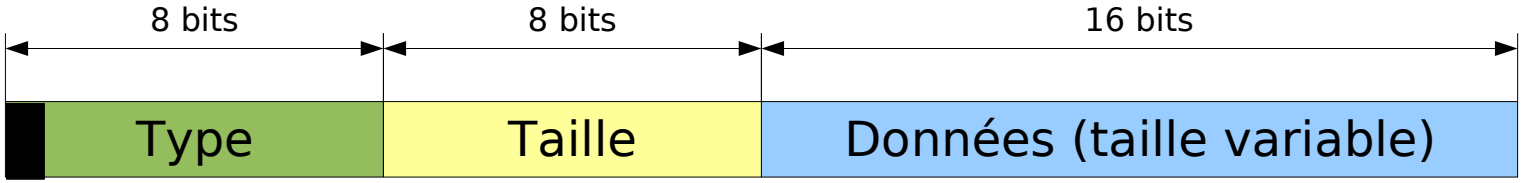
- L'en-tête de base de taille fixe : 40 octets
- Extensions IPv6 : Fragmentation, Routing ...



- Possibilité de canaux cachés:
  - Champs non utilisés du protocole → peu de stockage, faible débit
  - Utilisation d'extensions « maison » → pas discret, problèmes de routage

Le format TLV

- Type – Length – Value



Flag « silencieux »

- Contrôle du comportement des récepteurs
- Extensions IPv6 : Hop-by-Hop, Destination
- Canal caché via options TLV
  - discret
  - limité en taille par le MTU

Les entêtes de routage

- Principe étendu du « *source routing* »
  - En IPv4, l'adresse finale était toujours l'adresse de destination et les routeurs intermédiaires passés dans des options
  - En IPv6 l'adresse de destination change au fur et à mesure du transit du paquet
- Analyse des entêtes nécessaire pour filtrer en sortie 
- La plupart des hôtes accessibles sur IPv6 acceptent ces entêtes

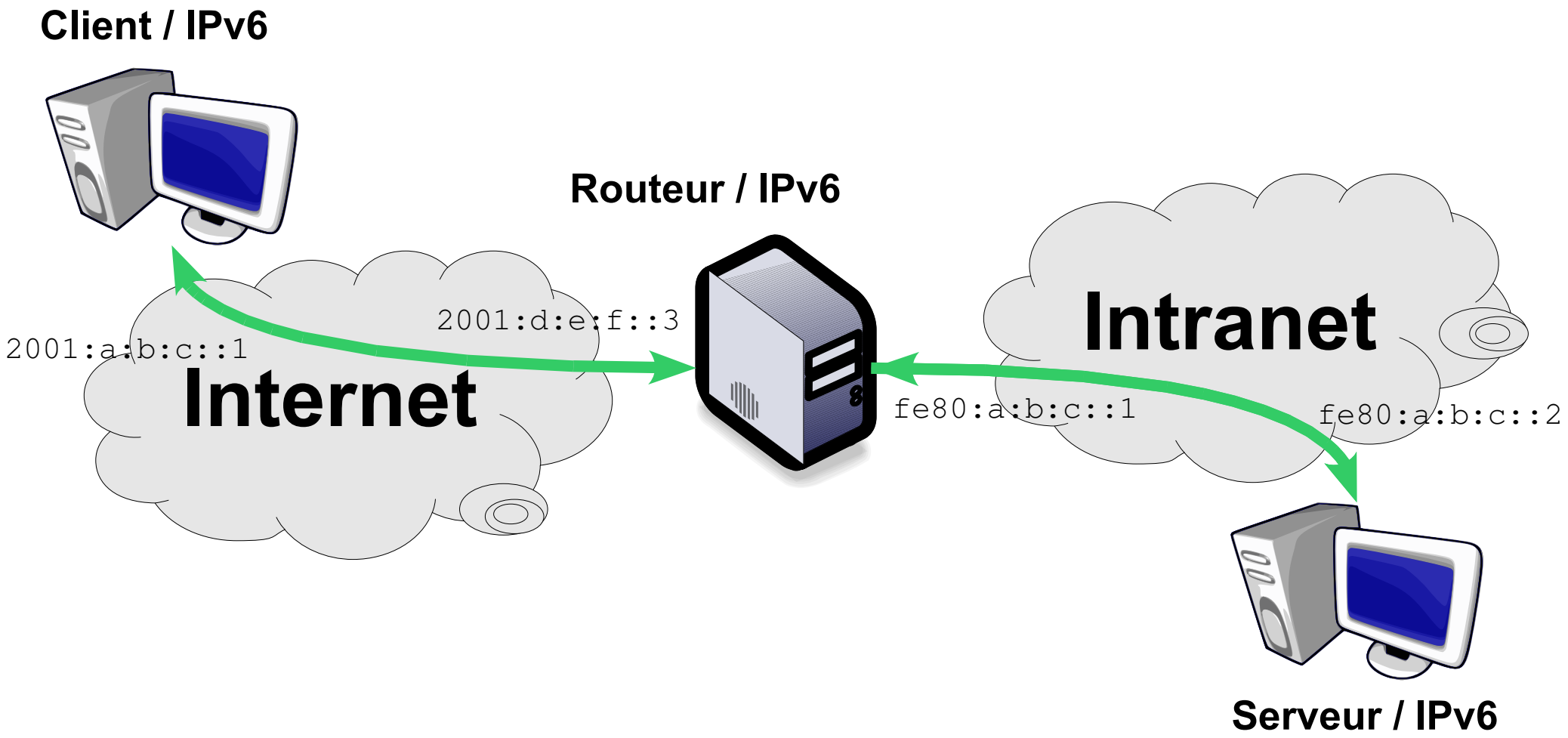
Traces de Routing Headers Type 0

No.	Time	Source	Destination	Protocol	Info
29	376.886200	2001:[redacted]a20::10	2001:[redacted]32::1	ICMPv6	Echo request
30	377.944369	2001:[redacted]a20::10	2001:[redacted]32::1	ICMPv6	Echo request
31	378.944421	2001:[redacted]a20::10	2001:[redacted]32::1	ICMPv6	Echo request
32	379.708938	2001:[redacted]0:216:cbff:fe8b:8a45	2001:[redacted]a20::10	ICMPv6	Echo reply
33	379.748928	2001:[redacted]0:216:cbff:fe8b:8a45	2001:[redacted]a20::10	ICMPv6	Echo reply
34	379.748931	2001:[redacted]0:216:cbff:fe8b:8a45	2001:[redacted]a20::10	ICMPv6	Echo reply

```
    Source address: 2001:[redacted]a20::10 (2001:[redacted]a20::10)
    Destination address: 2001:[redacted]f32::1 (2001:[redacted]:f32::1)
▽ Routing Header, Type 0
    Next header: ICMPv6 (0x3a)
    Length: 4 (40 bytes)
    Type: 0
    Segments left: 2
    address 0: 2001:[redacted]200::a012 (2001:[redacted]200::a012)
    address 1: 2001:[redacted]0:216:cbff:fe8b:8a45 (2001:[redacted]0:216:cbff:fe8b:8a45)
▷ Internet Control Message Protocol v6
```

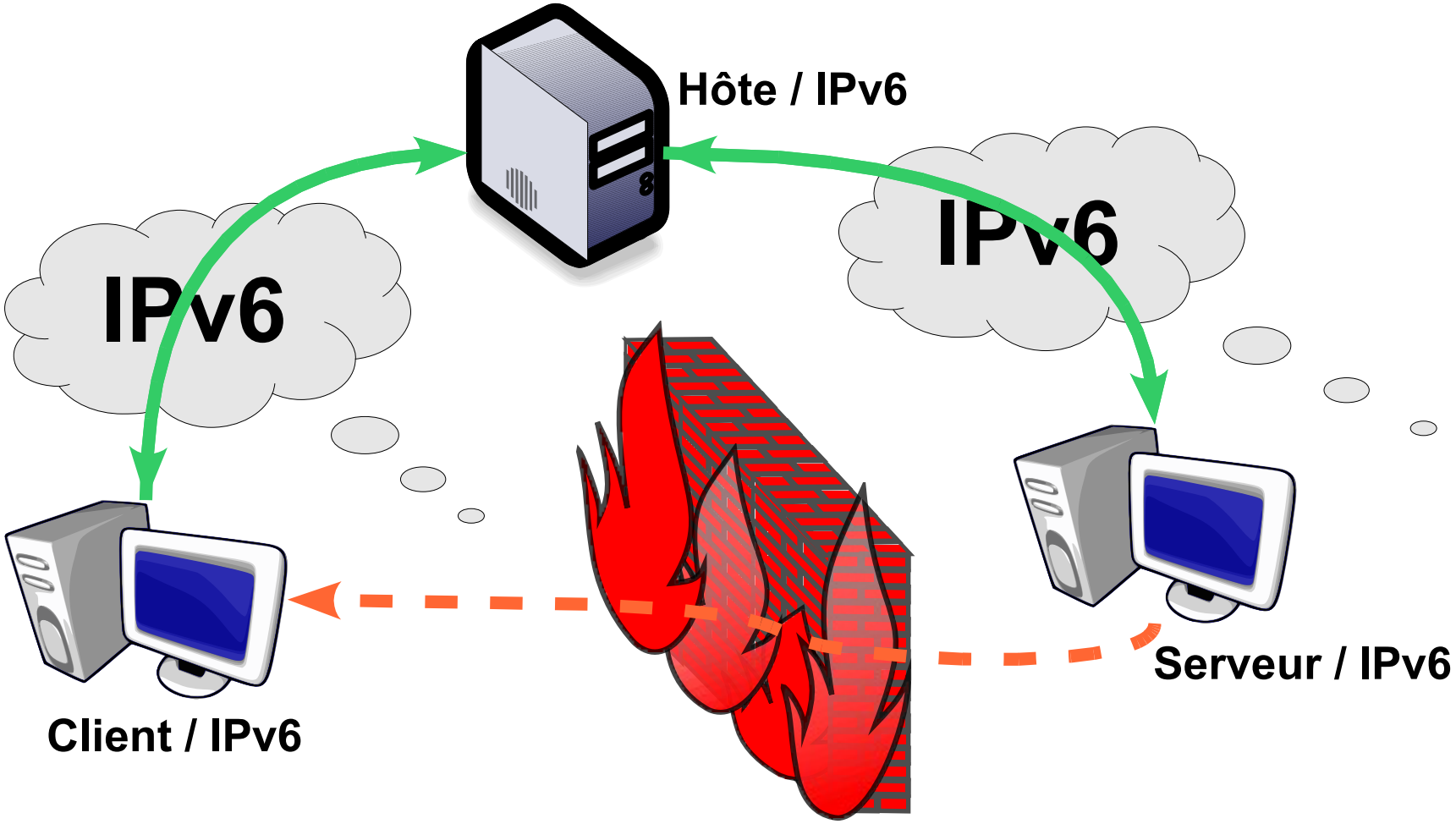
Contournement de périmètre

- Évasion de périmètre: global, site-local, link-local, node-local



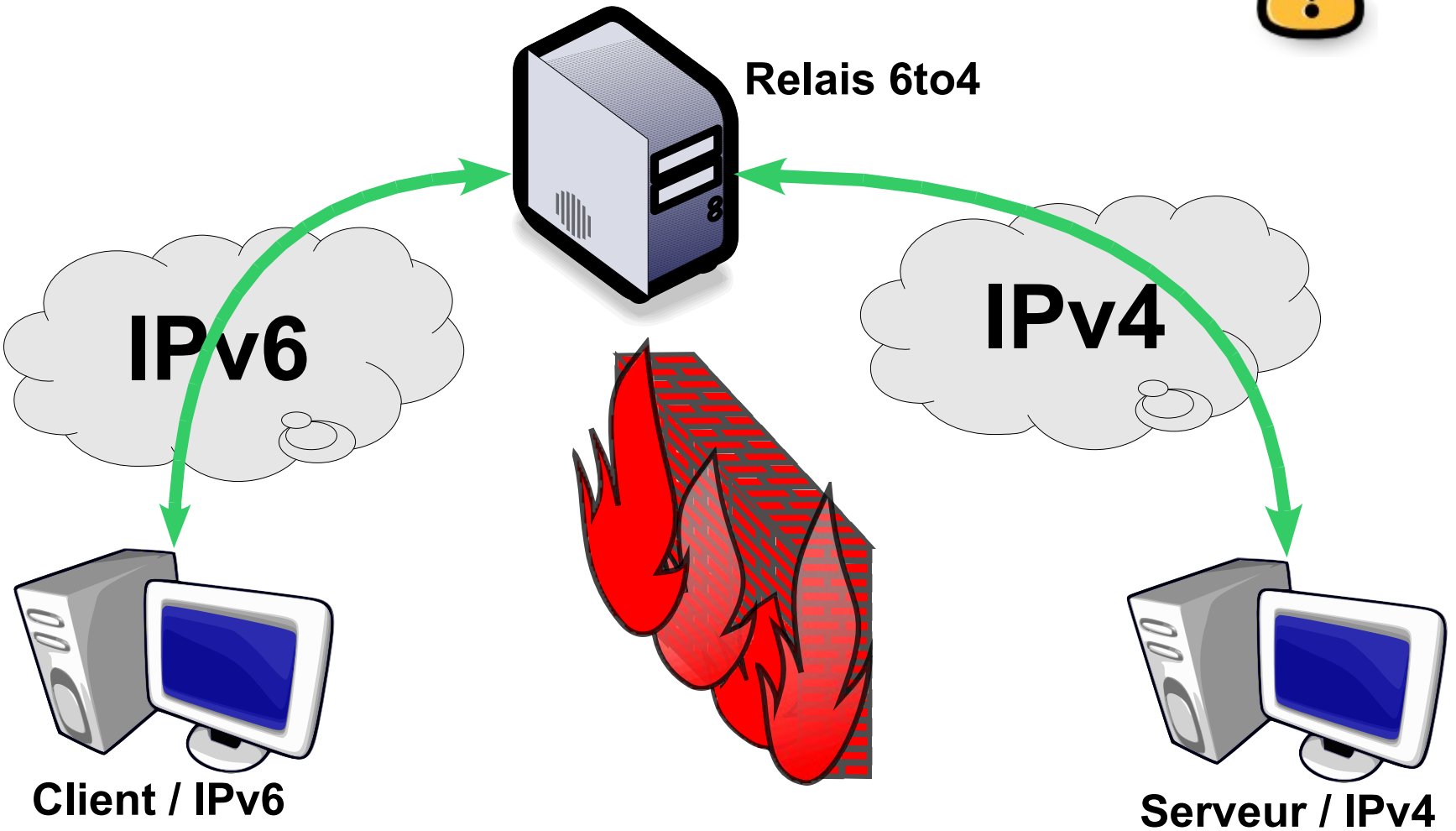
ACL: IPv6 vers IPv6

- Contournement d'ACL basées sur l'adresse de destination
- Possibilité d'établir des tunnels bidirectionnels



ACL: IPv6 vers IPv4

- Communications vers adresses IPv4 publiques via 6to4
- Relais 6to4 ouverts et accessibles sur Internet



Découverte d'un réseau IPv6

- Avec les adresses Multicast du protocole ND sur le lien
- Utilisation des DNS
- Adresses simples
  - Motifs courants: « beef », « cafe », « abcd » ...
  - Adresses séquentielles: DHCP, GGSN
- Optimisations d'un scan ICMPv6
  - Adresses EUI-64
    - cible un fabriquant d'équipements réseaux particulier
    - 64 bits → 48 bits / fabriquant
  - Entête de routage
    - Pour 1 paquet envoyé, 1 à 30 machines scannées

IPsec en natif

- Obligation précisée dans les RFCs
- Reprend exactement les mêmes principes qu'en IPv4
  - Dans l'esprit initial, toute communication devait être chiffrée en mode transport, avec négociation automatique entre machines.
  - De fait IPsec ne sert qu'en mode tunnel ...
- Même mécanismes de sécurité et contraintes qu'en IPv4
  - Installation de certificats
  - Configuration IKE
- Problèmes avec les flux Multicast
- Problème à l'initialisation avec le *Neighbor Discovery*.
  « La poule avant l'oeuf ? »

Dilemme pour les IDS

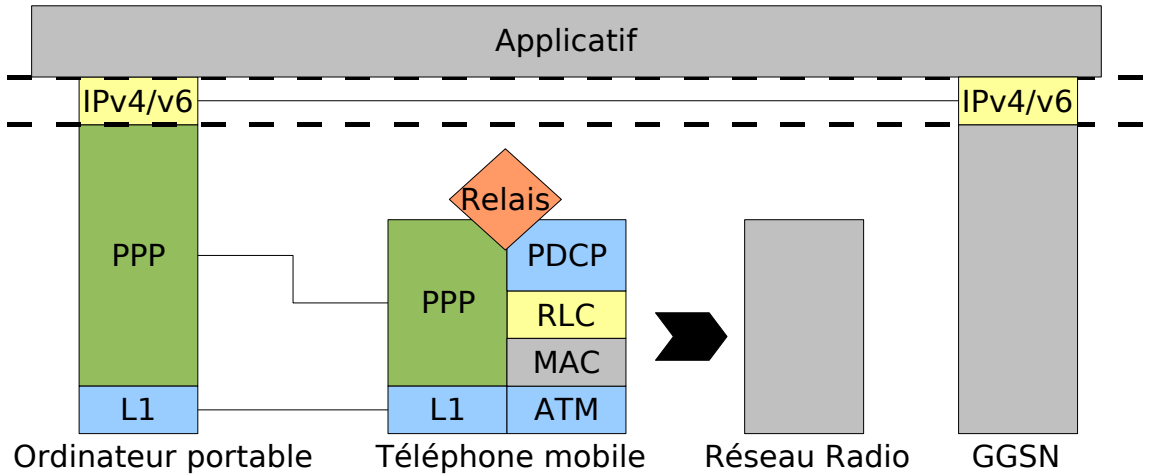
- Facile de posséder une énorme quantité d'adresses pour lancer des attaques.
  - /64 → plusieurs milliards de scans TCP avec des adresses uniques
- Remplissage des tables d'états

- Vers une généralisation d'IPsec
- Structure des paquets IPv6 modulaires
  - Possibilité de changer la structure des paquets pour lancer une attaque
  - Plus de possibilité de canaux cachés
- Suivi de sessions applicatives partagées entre les protocoles IPv4 et IPv6
  - FTP, SCTP ...

Impacts applicatifs et systèmes

- Faible impact sur la majorité des protocoles applicatifs
- Impact sur certaines applications à cause de l'espace d'adressage:
  - Identification de session par adresse IP
  - Les adresses temporaires, « *Privacy Extension* »
- Vulnérabilités de tous types concernant IPv6 découvertes à ce jour: GNU/Linux, FreeBSD, OpenBSD, NetBSD, Solaris, Windows, Cisco IOS ...
  - mauvaises manipulations des entêtes ou des données utilisateurs
  - mauvais calculs de la taille des entêtes ou des options TLV
  - Correction retardée en IPv6 de failles IPv4 anciennes (MS06-064)

Particularités de IPv6 sur réseaux 3G



- Difficulté de forger les trames au niveau du téléphone
  - Pile « cachée »
  - Réalisable si réseau mobile en IP (UMA)
- Liaisons Point à Point limitées par leur nature
- Problèmes de facturation
  - Tunnels Mobile/Mobile dans les sessions à l'acte
  - Sur-facturation au volume d'un hôte s'il accepte les « *Routing Headers* »

Mobilité IPv6

- Standardisé, prévu pour 3GPPv2
- Très complexe à mettre en oeuvre
- Changement de topologie du réseau traditionnel
  - Il devient difficile de faire de la sécurité périmétrique (nécessite de laisser passer les tunnels, adresses Anycast ...)
  - Filtrage des « *Routing Headers* » remis en cause 
- Utilisation de la mobilité détournée
  - déni de service (*flood*) sur l'adresse fixe d'un client GPRS.

en bref ...

- Il est très long de « scanner » un réseau ?
  - *ça dépend...*
    Thèse de la difficultés plus grande des « worms » à se propager sur un réseau IPv6 est à reconsidérer
- Il est facile d'obtenir un accès IPv6 sur un réseau IPv4 connecté à Internet ?
  - *Oui .. il existe de nombreux mécanismes de cohabitation*
- Le protocole IPv6 est complexe et ses impacts sont nombreux ?
  - *Oui .. niveau administration, routage, sécurité et développement.*
    Plus de 100 RFCs !

Prochains rendez-vous

- **Formation ISO27001 Lead Auditor** :
  - Certification ISO27001 Lead Auditor par **LSTI**
  - **http://www.hsc.fr/services/formations/**

Lyon : 27 nov -1 déc
Paris : 4 - 8 décembre
Genève : 22-26 janvier
Toulouse : 5-9 février

- **Sécurité VoIP & Enquêtes post-incident**
  - Tutoriels les 22 et 23 novembre 2006

http://www.infosecurity.com.fr/?Jpto=116&IdNode=11

le salon de la sécurité informatique FRANCE
22 et 23 nov. 2006 Cnit Paris La Défense
www.infosecurity.com.fr

- **Surveillance et détection sous Linux**
  - Tutoriel en deux parties le 1er février 2007
  - **http://www.solutionslinux.fr/**

solutions Linux

Questions ?

Nicolas.Collignon@hsc.fr
http://www.hsc.fr/