

La sécurité dans Mobile IPv6

Arnaud Ebalard - EADS Corporate Research Center France
Guillaume Valadon - The University of Tokyo - Esaki Lab / LIP6



Plan

1. IPv6
2. Mobile IPv6
3. Sécurité et Mobile IPv6
 1. Protections par défaut
 2. IPsec

IPv6

Différences avec IPv4

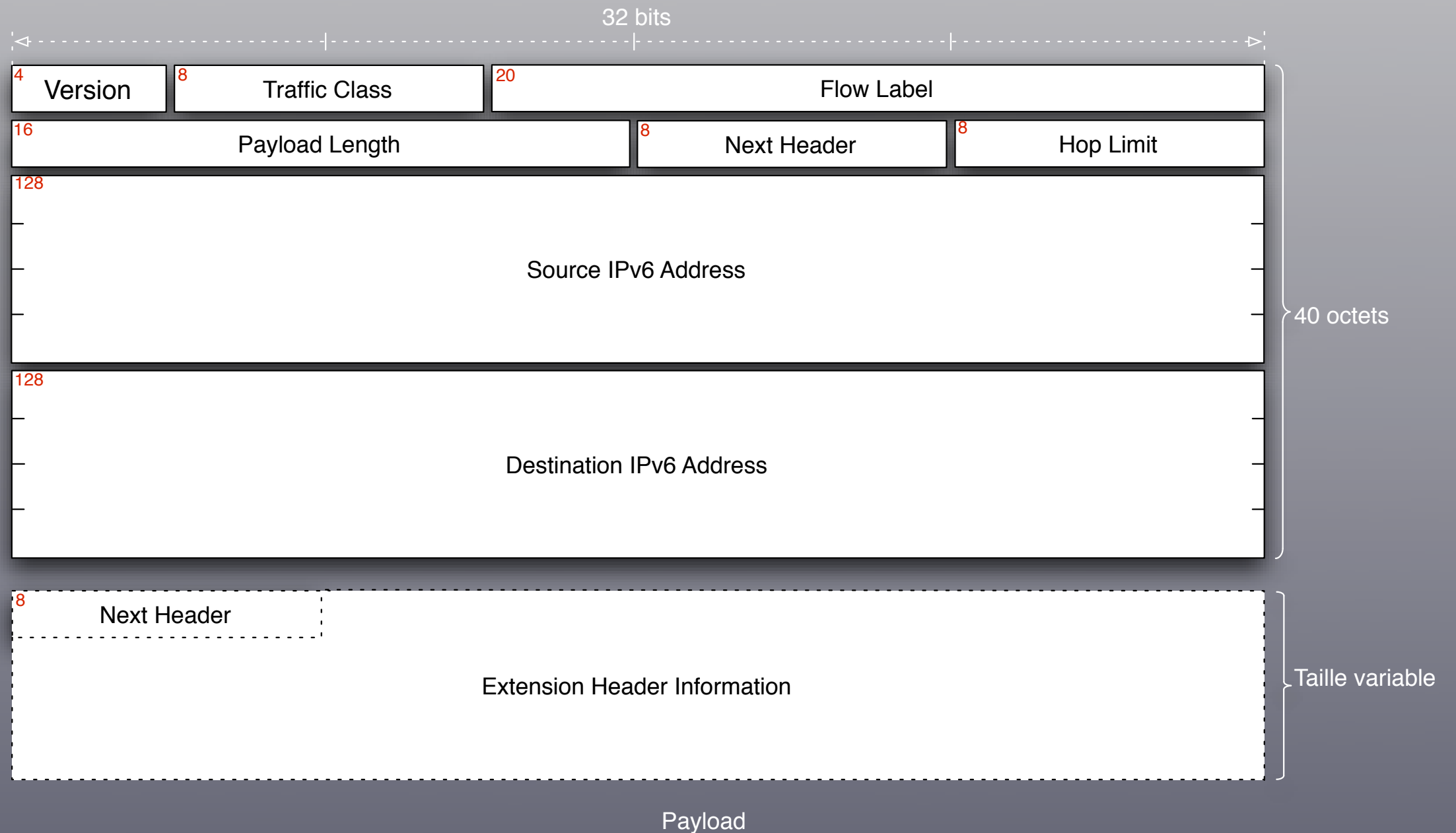
Changements fonctionnels

1. communications de bout en bout
2. mécanismes d'ARP intégrés à ICMP

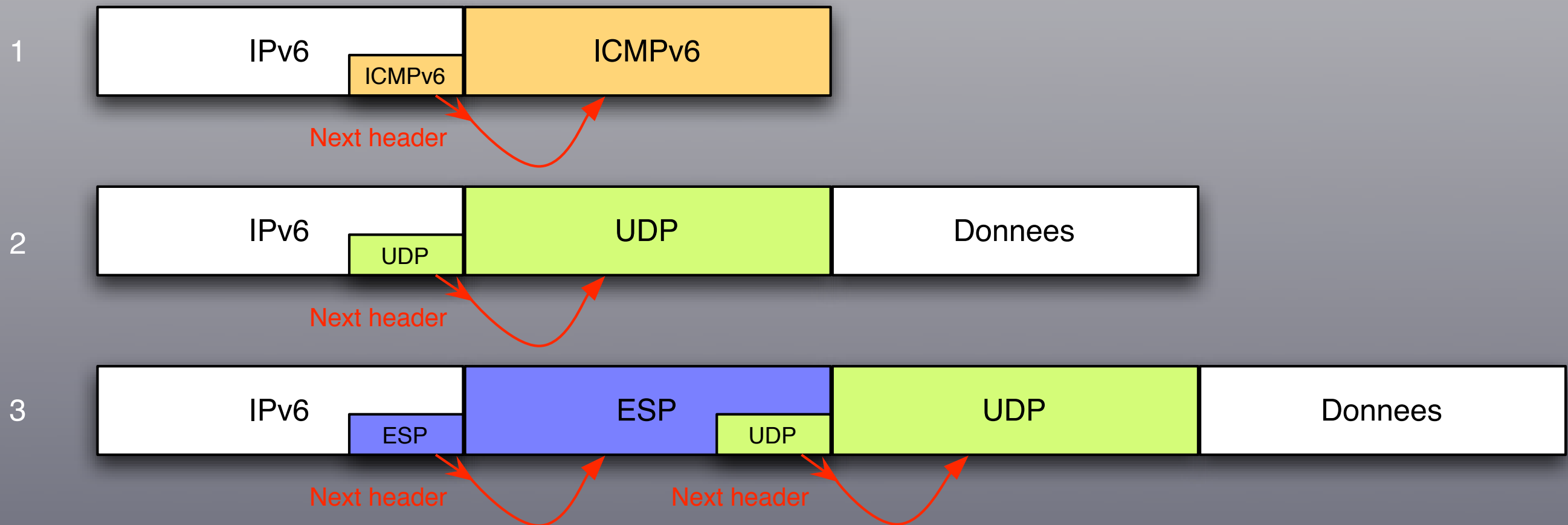
Changements structurels

1. entête de taille fixe
2. fragmentation à la source, pas de checksum
3. extensions via chaînage d'entêtes

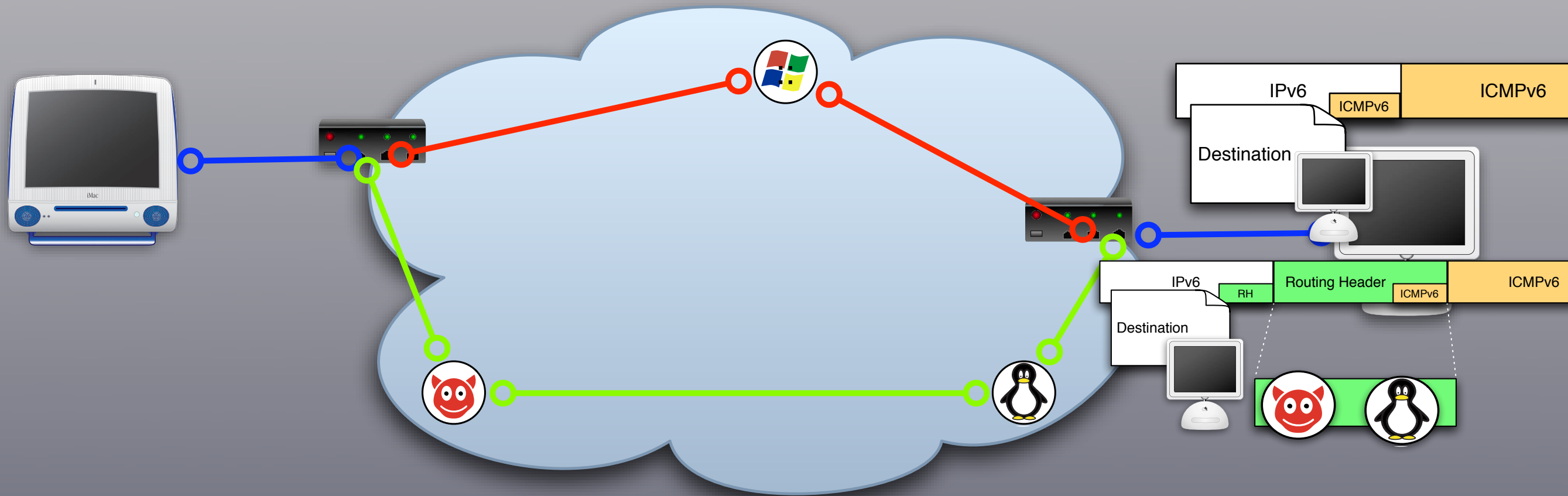
L'entête



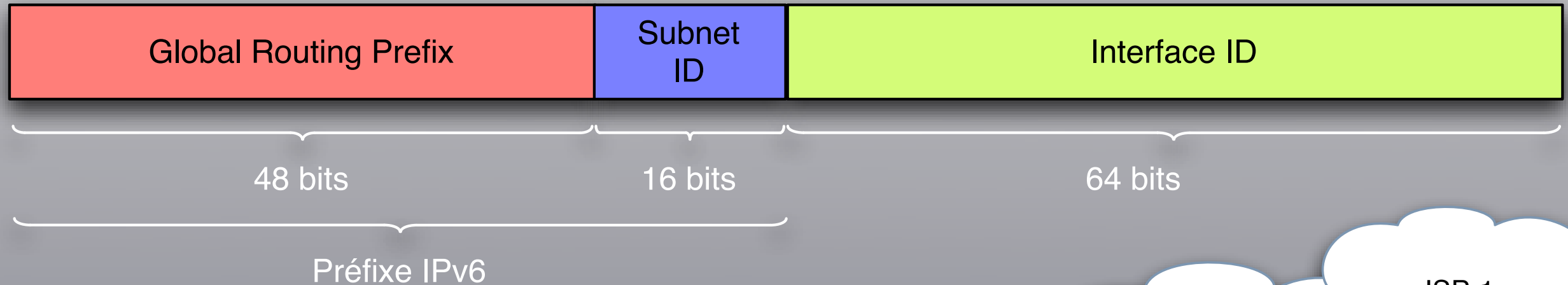
Principe des extensions



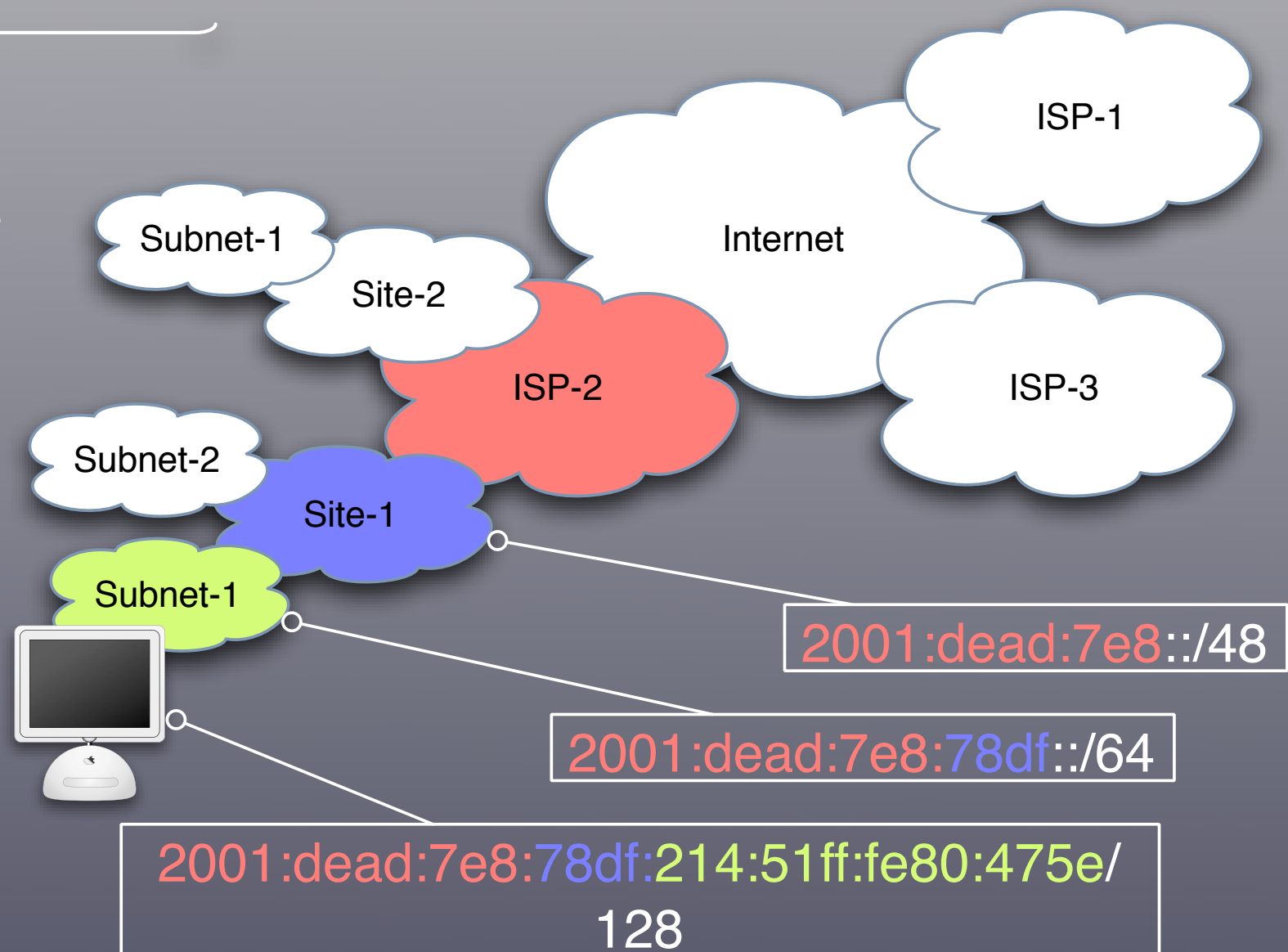
Routing Header



Adresses en IPv6



- découpage géographique hiérarchique
- préfixe de 64 bits
- interface ID généré dynamiquement



Auto-configuration

- mécanisme intégré à ICMPv6 (passif ou actif)
- Fonctionnement:
 1. Obtention du préfixe IPv6 annoncé par le routeur d'accès (RS/RA, Router Solicitation/Advertisement)
 2. Génération de l'interface ID, test d'unicité locale
 3. Génération de l'adresse via concaténation du préfixe et de l'interface ID

Mobile IPv6

Pourquoi ?

1. Etre joignable avec une adresse IPv6 unique peu importe le réseau d'attachement
 2. Rendre transparents les changements de médiums
 3. Conserver les connections lors des déplacements
- ➔ utiliser un laptop/PDA de la même manière qu'un téléphone portable

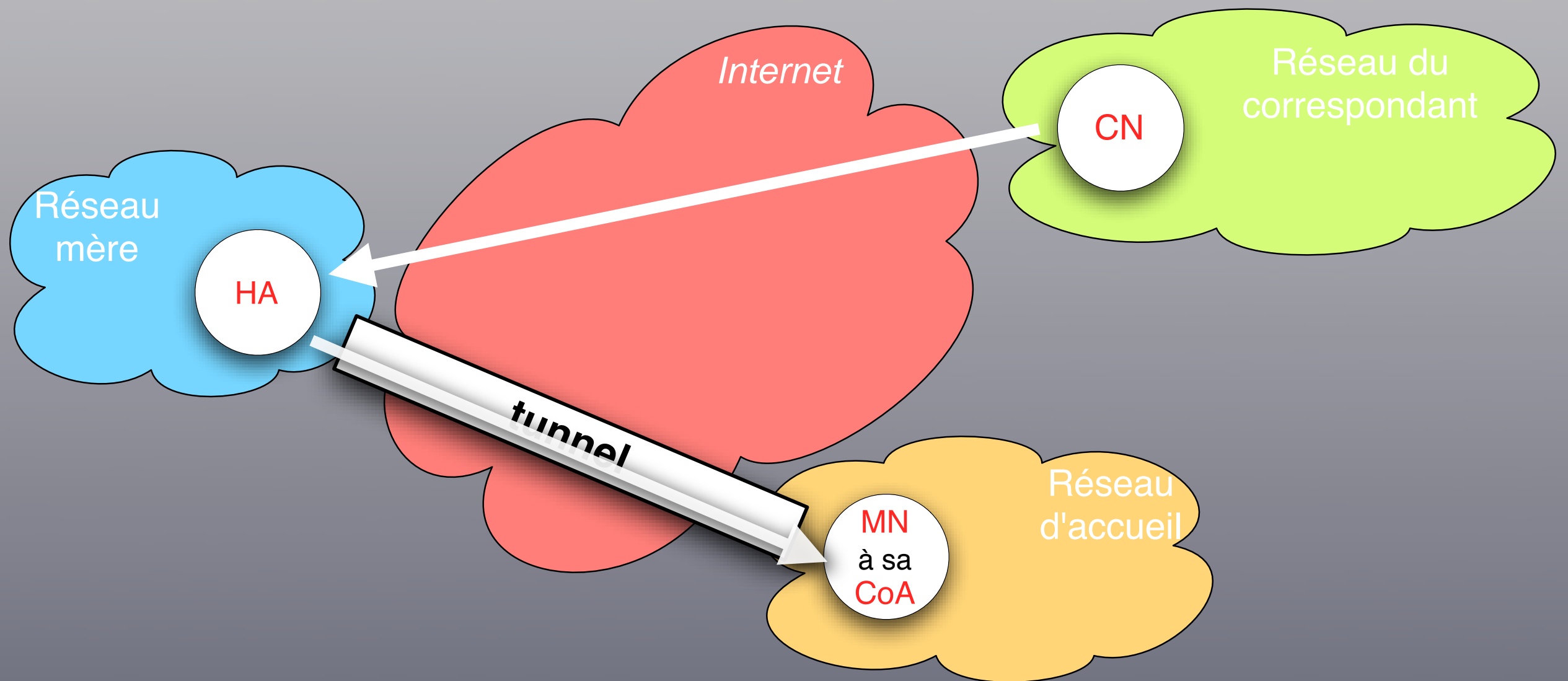
Challenges

- Le routage est géographique, l'adresse IP a une double fonction
 - ✓ **Identifier**: identifiant de la machine
 - ✓ **Locator**: localisation géographique dans le réseau
- Nouvelle architecture nécessaire:
 1. compatible avec les noeuds clients
 2. ne modifiant pas l'architecture de routage
 - ➔ MIPv6 seulement présent dans les noeuds finaux

Comment ?

- Intégration du protocole à la couche IP
- Découpler identifier et locator grâce a deux adresses: **HoA** (Home Address) et **CoA** (Care of Address)
- Trois nouvelles entités:
 1. **Mobile Node**: joignable partout avec la HoA peu importe sa CoA
 2. **Home Agent**: permet la correspondance CoA/HoA
 3. **Correspondent Node**

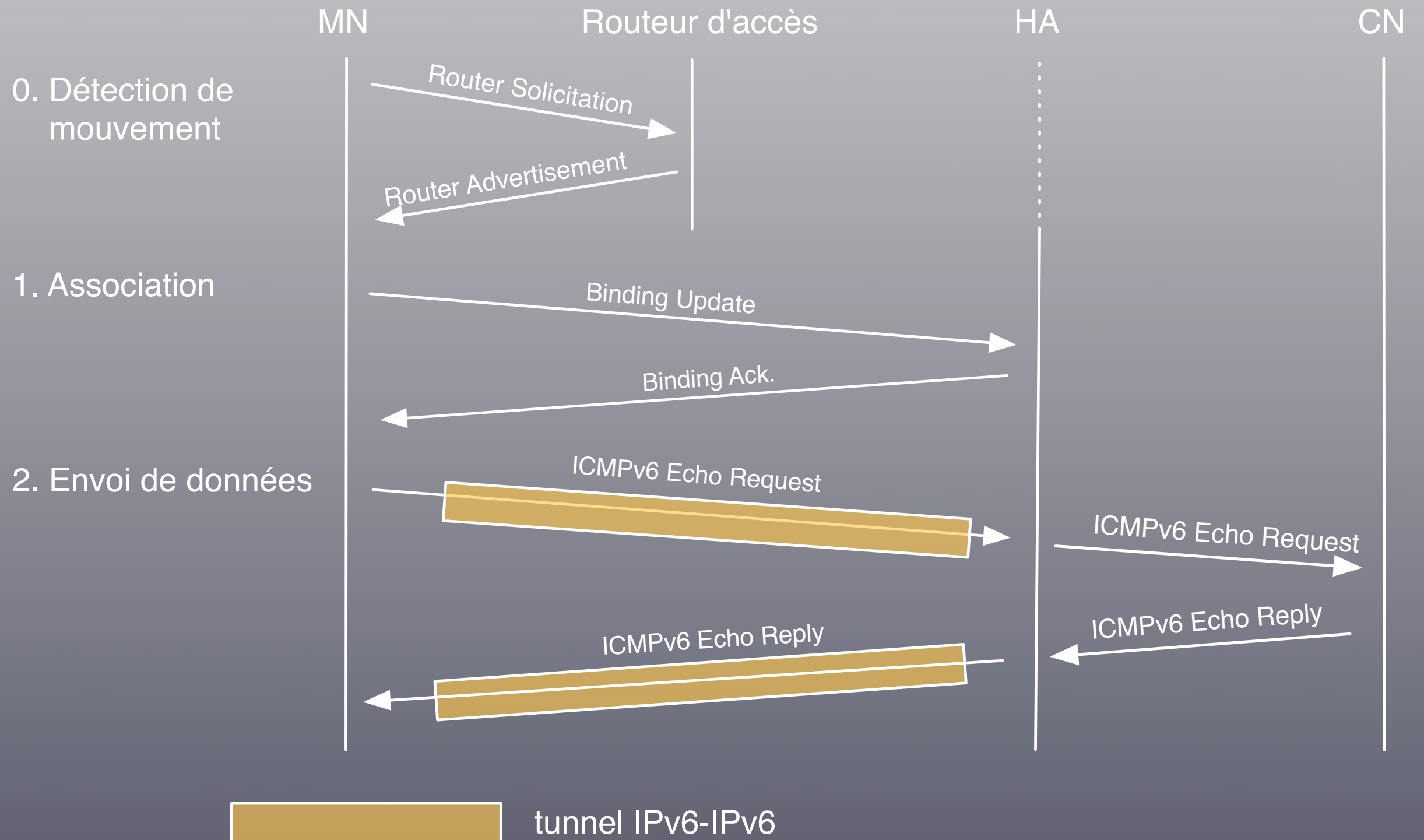
Fonctionnement



HoA: adresse constante du MN; *identifier*

CoA: adresse du MN dans le réseau d'accueil; *locator*

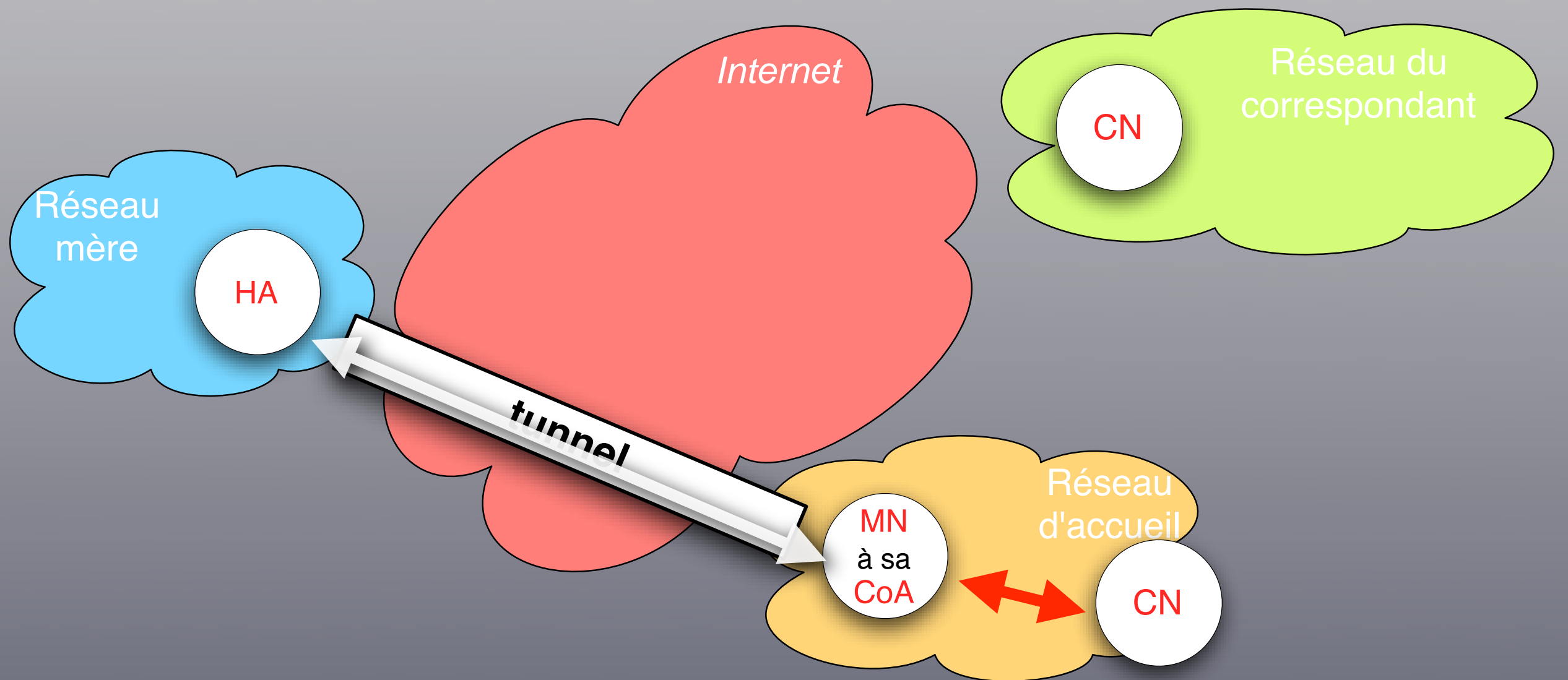
En détails



Nouvelles extensions

- **Home Address Option**
 - ingress filtering
 - fournit l'adresse source du paquet (HoA)
- **Routing Header Type 2**
 - assure le routage vers la position physique du MN (locator)

Routage triangulaire

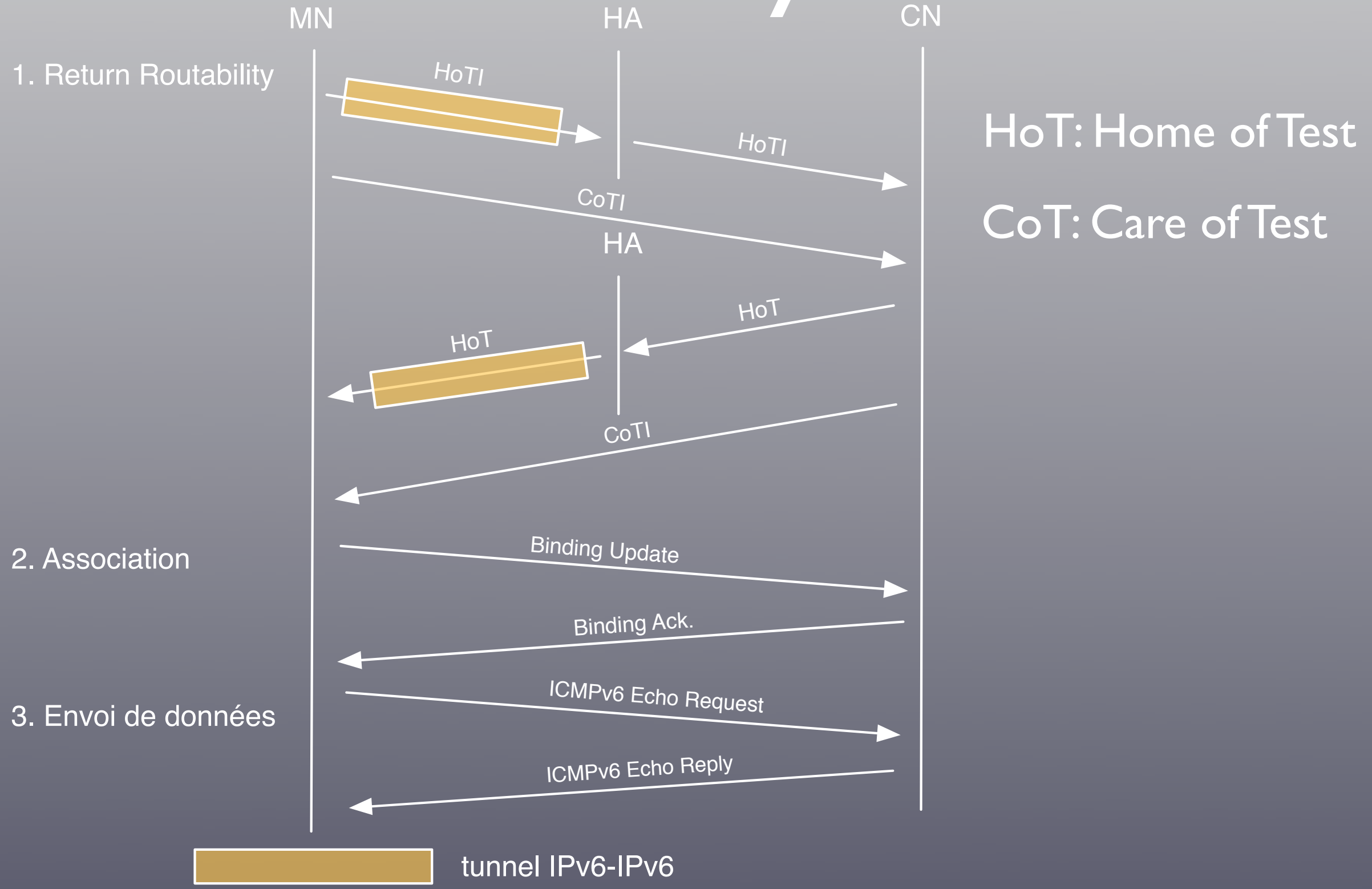


Obtenir un routage optimal

Challenges

- Optimiser la communication MN/CN de façon sûre
- Garantir la relation identifier/locator en se basant sur le routage
 - ✓ vérifier que le MN est joignable à la CoA et à la HoA
- ➔ générer une clé permettant de signer le message Binding Update à destination du CN

Return Routability Procedure



Sécurité et Mobile IPv6

Attaques envisageables

1. Communications entre MN et HA : signalisation et données

➔ *IPsec*

2. Communications directes entre MN et CN : signalisation et données

➔ *Return Routability Procedure*

3. Infrastructure réseau

➔ *Stateless behavior, Careful design*

Protection de l'infrastructure

Challenges et solutions

- consigne: “Do no harm to the existing Internet”
- Prévenir le spoofing
 1. preuve de possession de l’adresse (HoA)
 2. extensions spécifiques : HAO et RH Type 2
- Prévenir les DoS
 1. contre l’infrastructure : émission des messages en “un pour un”
 2. contre les CN : caractère sans état des échanges


Communications entre MN et CN

Return Routability Procedure

- Echange HoT/HoTI, CoT/CoTI et BU/BACK
 1. CN : vérifier que le MN peut communiquer avec sa HoA et sa CoA
 2. MN : générer une clé permettant de signer les BU émis à destination du CN
- Problèmes possibles (MiTM, eavesdropping)
 1. attaquant sur le réseau mère;
 2. attaquant sur le réseau d'accueil
 3. attaquants sur les deux réseaux

Communications entre MN et HA

IPsec

- Pertinence du choix d'IPsec
 1. Partie intégrante d'IPv6
 2. Communications de bout en bout
 - Ce qu'il faut protéger
 1. Messages de signalisation (i.e. BU et BACK)
 2. Return Routability Procedure (HoTI/HoT)
 3. Trafic de données (i.e. tunnel MN/HA)
-  Problèmes liés à l'interaction MIPv6/IPsec/IKE

Trafic de signalisation

Généralités

- Protection requise, paire de SA ESP en mode transport (requis)
- Support du static keying obligatoire, du dynamic keying optionnel
- Protection de la CoA
- SP et SA configurées avec la HoA du MN et l'adresse du HA.
- Sélection sur le Mobility Header (i.e. I35)

Coordination IPsec / MIPv6

- Binding Update :
 - Emission : protection par IPsec, switch des CoA et HoA entre l'option HAO et le champ source du header IPv6
 - Réception : switch des adresses, puis traitement par IPsec
- Binding Ack : même principe mais sur le contenu du Routing Header Type 2

Bootstrapping

- La mise en place des SA est un préalable à la procédure de “Home Registration” avec le HA
 - En Static Keying, aucun problème
 - En Dynamic Keying, IKE doit utiliser la CoA pour la négociation des SA associées à la HoA.
 - ➔ L’adresse du sélecteur de SA et celle du peer différent
- Extension PF_KEY SADB_X_EXT_PACKET :
 - inclus le paquet ayant déclenché le SADB_ACQUIRE
 - fournit le contexte au démon IKE

Trafic de données & RRP

Bootstrapping

- Initialement, les SP [/SA] en mode tunnel référencent la HoA du MN.
- Mise à jour effectuée lors du bootstrapping faisant suite à la “Home Registration”
- Maintien à jour de la CoA du MN via MIGRATE

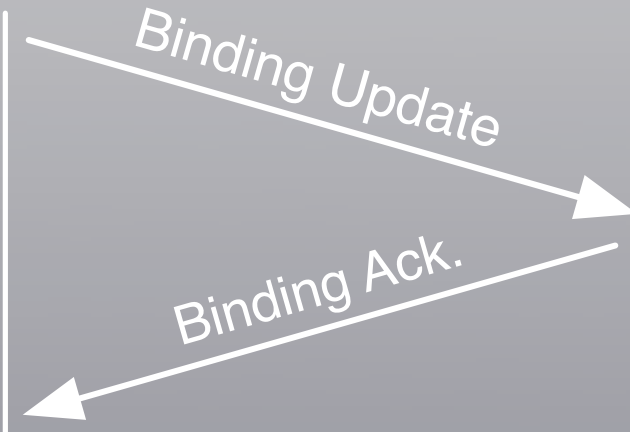
Migration des SA

- Nouvelle interface PF_KEY MIGRATE
- Emission du MIGRATE par MIPv6 à :
 - l'envoi d'un BU par le MN
 - la réception d'un BU par le HA
- Réception par :
 - le noyau pour MAJ des SPD/SAD
 - [le démon IKE pour MAJ de sa session]
- Négociation dynamique du support : **K-bit**

Tunnel IPsec
HA-> HoA

Tunnel IPsec
HoA -> HA

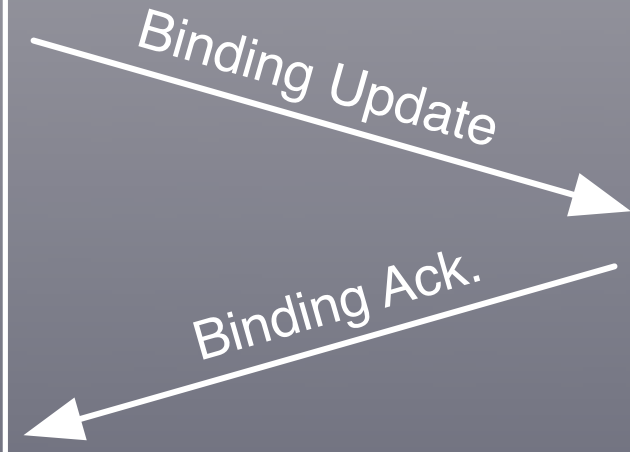
MN HA



Tunnel IPsec
CoA_1 -> HA

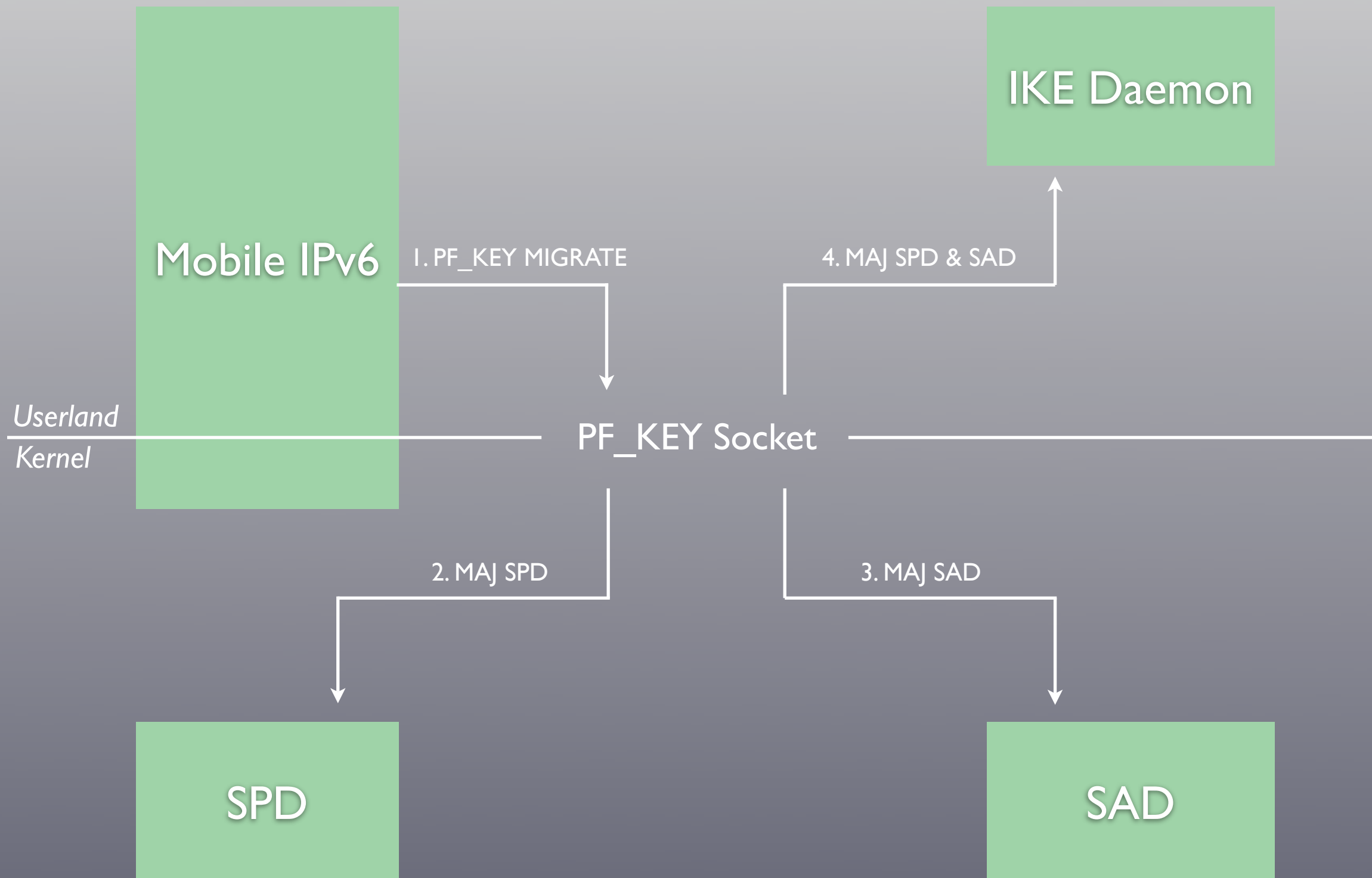
Tunnel IPsec
HA -> CoA_1

Mouvement



Tunnel IPsec
CoA_2 -> HA

Tunnel IPsec
HA -> CoA_2



Conclusion

- Séparation identifier et locator compatible avec l'Internet *actuel*
- Mécanismes de sécurité: RRP et IPsec
- Fin de la sécurité périmétrique ?
- Travaux futurs
 1. IPsec entre MN et CN
 2. utilisation en environnement PKI
 3. IKEv2

Démonstration

Questions ?
Café ?