Mobilité IP

Olivier Togni

Université de Bourgogne

IEM/LIB

o.togni.u-bourgogne.fr

olivier.togni@u-bourgogne.fr

modifié le 29/09/2020

Plan

- Problématique et principes
- MobileIPv4
- MobileIPv6
- Problèmes et extensions de MIP

Ressources bibliographiques

- **IPv6 Théorie et pratique** 4ed, ***G. Cizault,***
  livre.g6.asso.fr → chapitre « Mobilité dans IPv6 »
- **Mobile IPv6 : Protocols & Implementations**, Li, Jinmei, Shima, *Morgan Kaufmann, 2009*
- **Mobile Ipv6: Mobility in a Wireless Internet** H. Soliman, ***Addison-Wesley Professional, 2004***
- **www.ietf.org RFC 6301, ...**
- **Linux Mobile-IPv6-HOWTO, 2004**

Problématique

Plusieurs «niveaux» de mobilité:
1. déplacement au sein du même réseau d'accès sans fil
=> mobilité nulle
2. déplacement avec changement de point d'accès au réseau
=> mobilité au niveau liaison
du pt de vue IP, pas de changement
3. déplacement d'un réseau à un autre
- déconnexion lors des déplacements => DHCP suffisant
- maintien des connexions actives en permanence
=> mobilité IP

Groupe de travail mobileIP (IETF)

Buts:

- **obtention d'adrIP automatique et joignable à cette adr**
- **pas de modification logicielle sur les hôtes fixes**
- **pas de modification des routeurs (log, tables routage)**
- **la plupart des paquets vers l'hôte mobile ne doivent faire aucun détour par le réseau de domiciliation du mobile**
- **pas de surcharge de service quand l'hôte mobile est chez lui**

Problématique

En théorie 1 @IP  **1 Interface**

En pratique: 1 @IP  **une localisation physique**

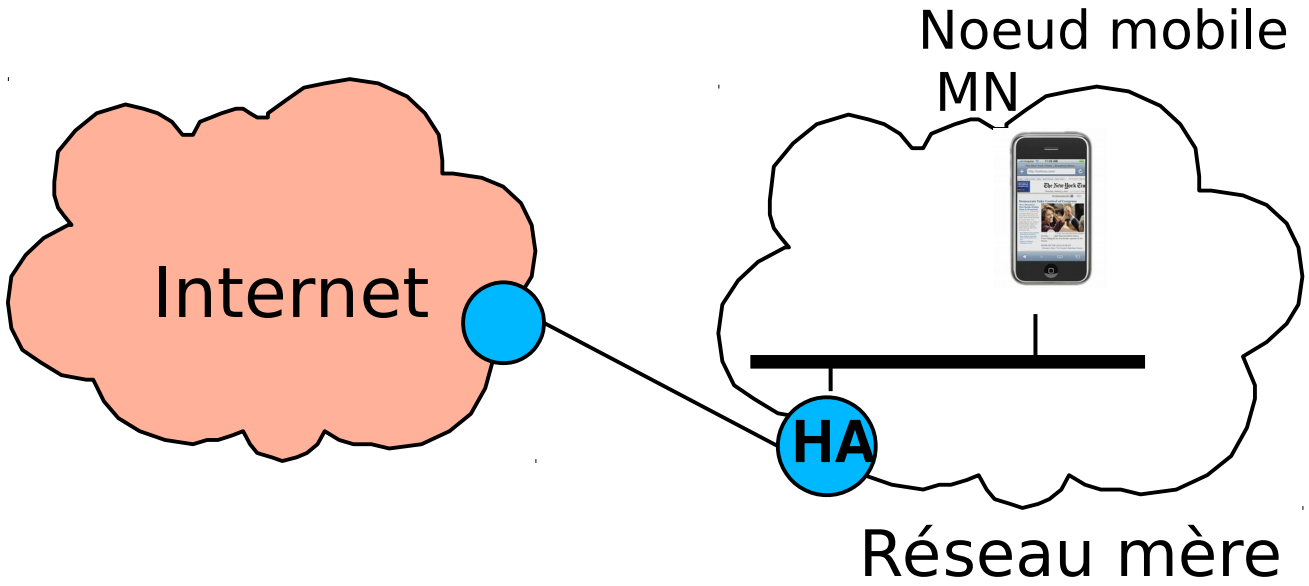
Car routage hiérarchique (1 pref = 1 réseau, fixe)

Terminologie

Réseau mère (Home Network, HN): réseau de domicile du mobile

Adresse mère (Home Adr, HoA): adr du mobile dans réseau mère

Agent mère (Home Agent, HA): entité gérant les fonctions de mobilité dans le (sous)réseau mère

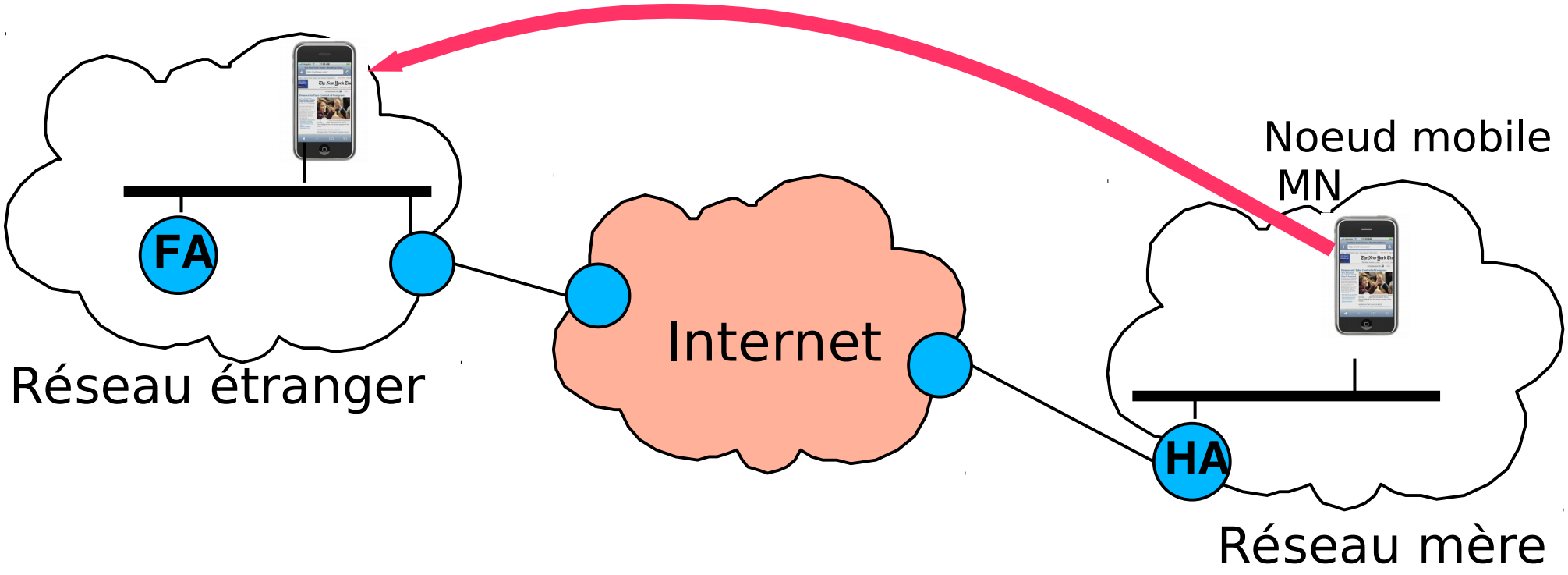


Terminologie

Réseau étranger (ou visité): réseau visité par un mobile

Adr temporaire (CoA: care-of-adresse): adr du mobile dans réseau étranger

Agent étranger (Foreign Agent, FA): entité gérant les fonctions de mobilité dans réseau étranger



Adressage

Déplacements transparents aux applications

=> l'adr IP doit demeurer la même au fil du temps et sur les différents réseaux visités

=> Si terminal mobile en visite sur un réseau, tout trafic adressé à son adr mère doit être ré-acheminé vers ce réseau

Solution 1: le réseau étranger informe les réseaux voisins de la présence du terminal mobile chez lui

Solution 2: déplacer les fonctions de mobilité du coeur vers la périphérie: c'est l'agent mère qui est capable de déterminer à tout moment ou se trouve le mobile => proto spécifique entre agent mère et agent étranger ou mobile

Routage

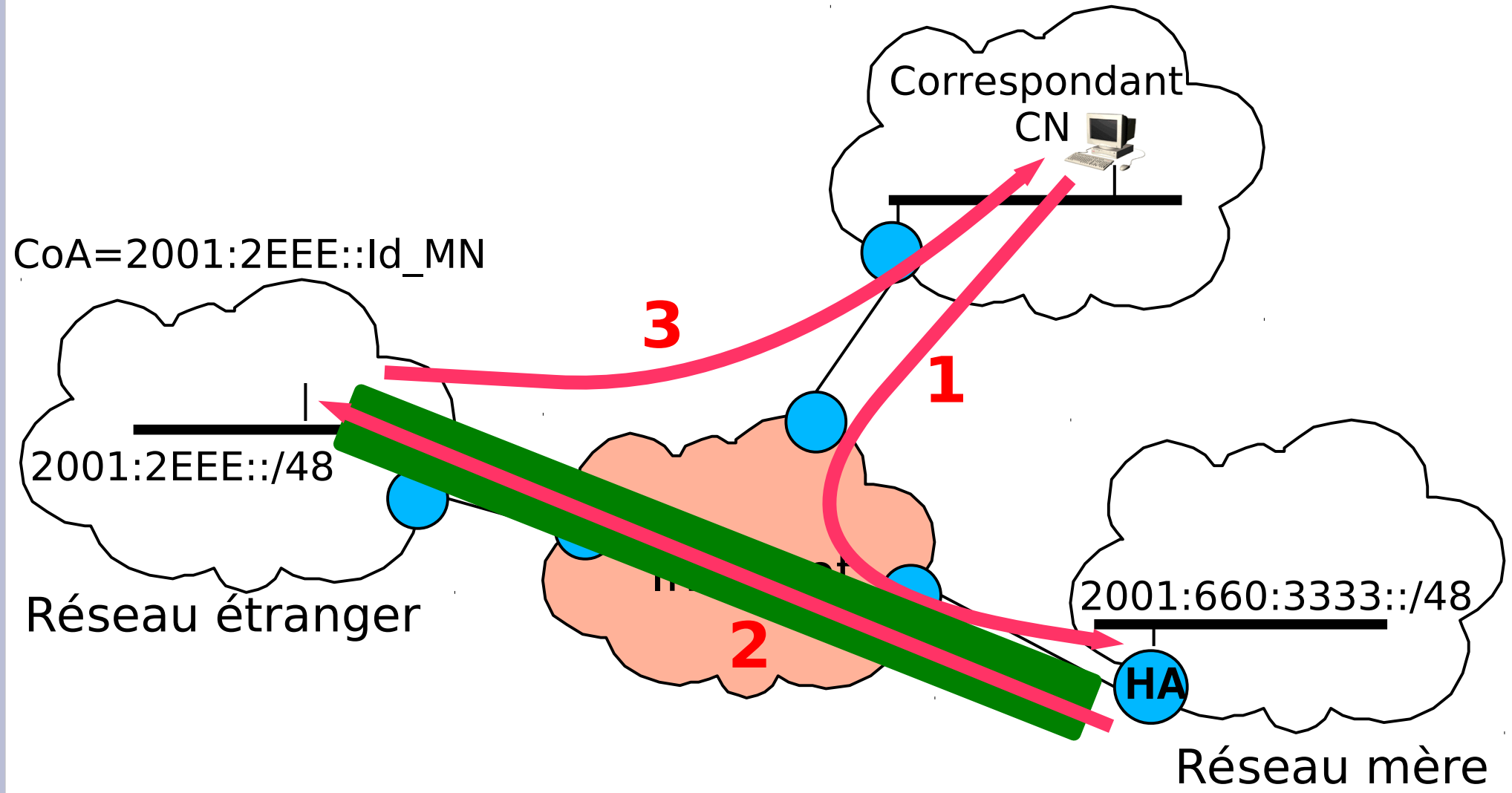
Envoi de datagrammes du corresp vers le mobile en voyage

- **Indirect: le corresp ne sait pas que mobile est en voyage paquets envoyés à l'agent mère qui les tunnelle vers l'agent étranger**
  - **+ transparent aux applications**
  - **- problème du routage triangulaire**
- **Direct: le corresp a un moyen de connaître la CoA du mobile:**

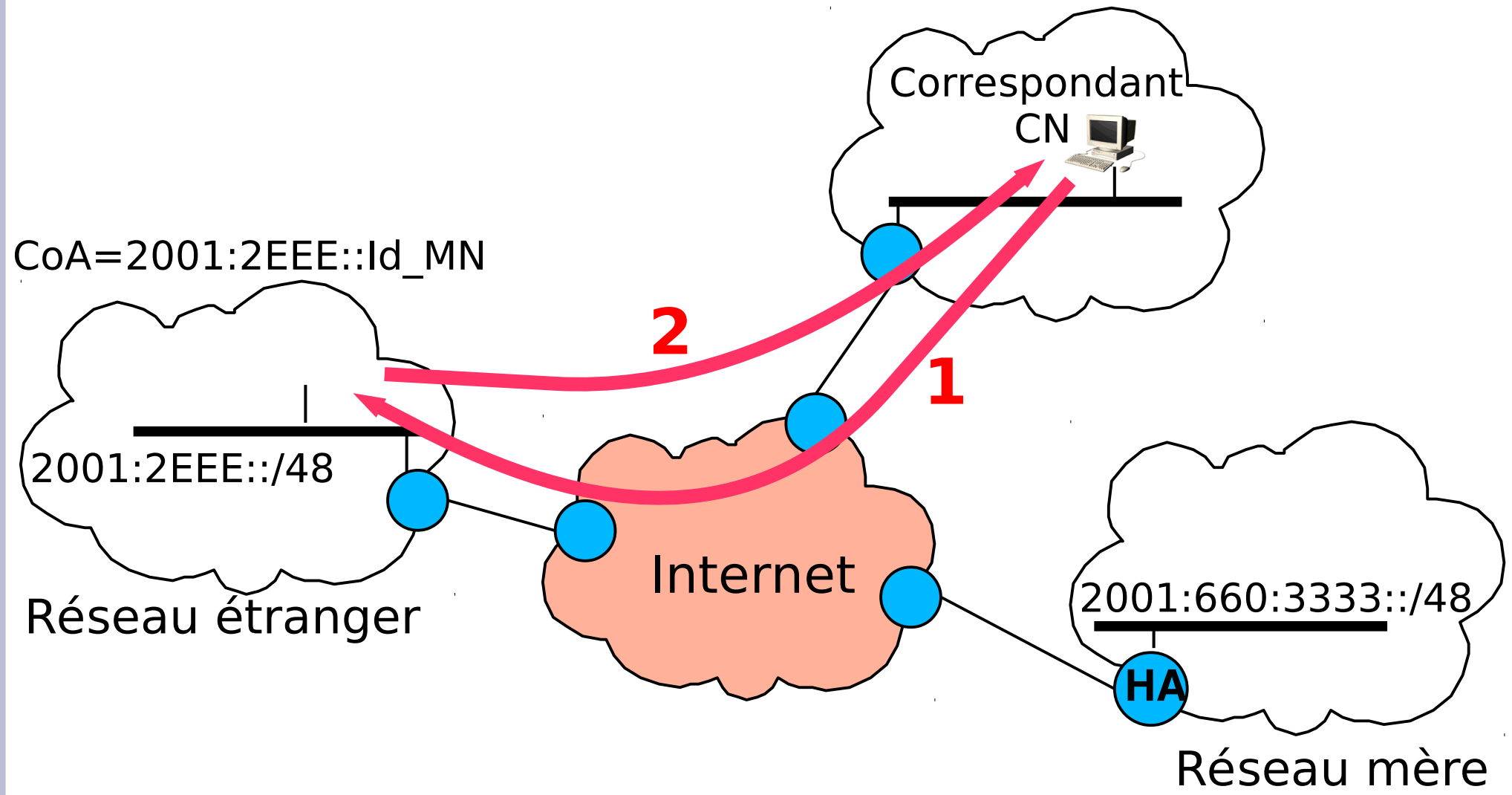
- soit après une première étape par routage indirect,

- soit un protocole spécial permet au corresp de dialoguer avec l'agent mère pour obtenir cette adr.

Routage indirect



Routage direct



MobileIP(v4)
RFC 3344 (08/2002)

Trois volets:

- **Détection d'agent**: protocoles pour que les agents diffusent les services qu'ils proposent et pour que les mobiles puissent solliciter les services

- **Inscription auprès de l'agent mère**: inscrire ou annuler inscription de la COA

- **Routage indirect**: proto pour que l'agent mère transmette les données aux terminaux mobiles: encapsulat°/décapsulat°, traitement des erreurs

Détection d'agent

Mobile qui se connecte doit identifier l'agent (étranger ou mère)
C'est cette détection qui permet à la couche réseau de s'apercevoir du déplacement dans un autre réseau

2 approches:

- **Annonce d'agent**
- **Recherche d'agent**

Détection d'agent

Annonce d'agent: annonce faite par extension du proto de détection de routeur

L'agent diffuse un message ICMP «detection de routeur» étendu (sur toutes les liaisons auxquelles il est relié) contenant son adr

+

- **bit agent mère H indique que le routeur fait office d'agent mère**
- **bit agent étranger F: agent étranger pour réseau auquel il est relié**
- **bit adhésion obligatoire R: indique au mobile qu'il doit se faire connaître de l'agent étranger**
- **bits d'encapsulation M et P indiquent si le mode d'encapsulation est différent de IP sur IP**
- **champs CoA: liste d'une ou plusieurs CoA fournies par l'agent étranger. Le mobile doit choisir une de ces CoA**

Détection d'agent

Recherche d'agent:

- **Le mobile peut ne pas attendre une annonce de routeur et diffuser un message ICMP 10 de «recherche d'agent»**

- **Tout agent qui reçoit ce message répond à l'auteur par une annonce d'agent**

Inscription agent mère

Pour communiquer adr temporaire à l'agent mère

1) Le mobile reçoit annonce agent étranger

2) mobile envoie message inscription à l'agent étranger (UDP 434) avec CoA choisie, adresse de l'agent mère (MA), adr mère du mobile (HoA), durée de validité de l'inscription et num inscr de 64bits

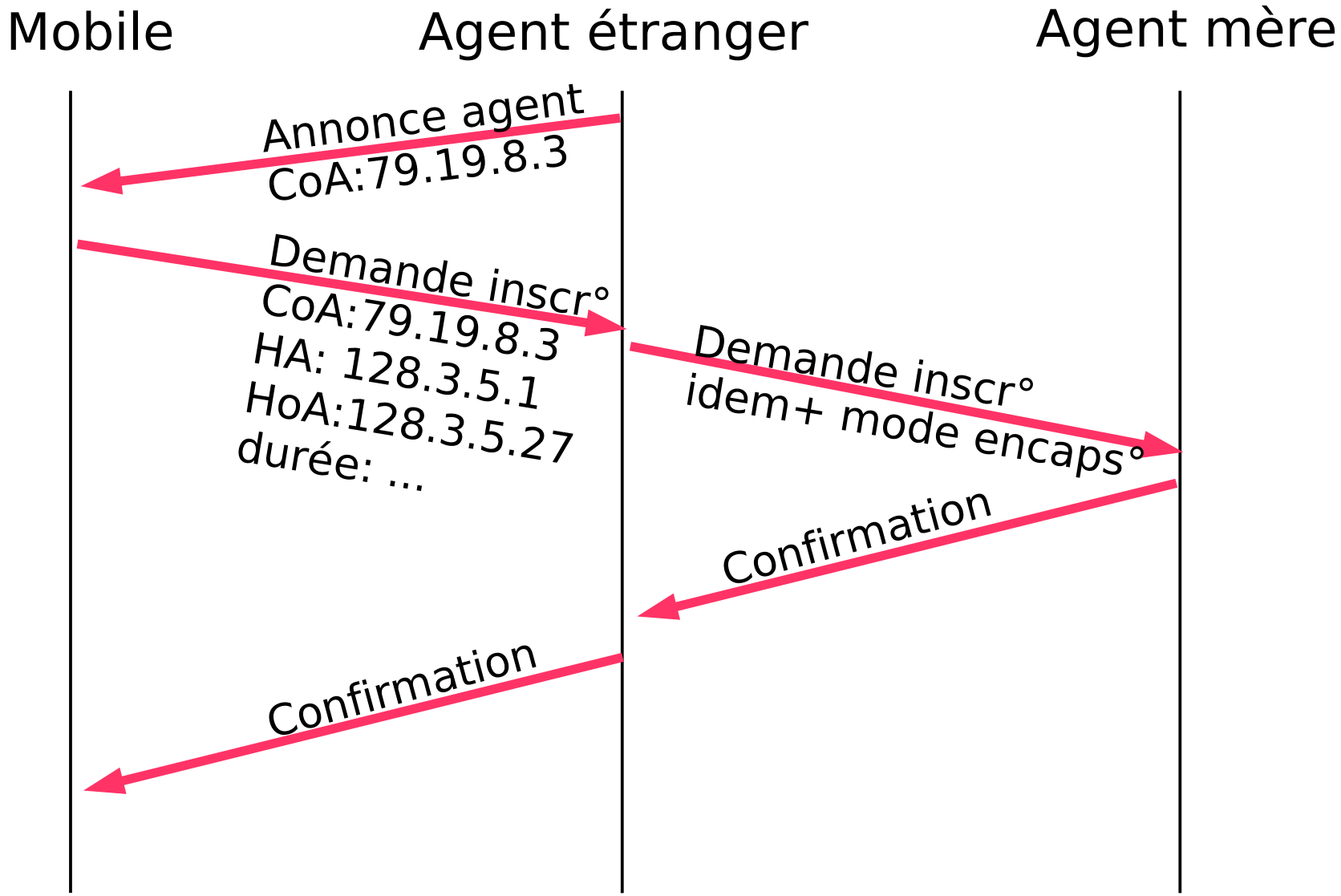
3) Agent étranger enregistre l'adr mère mobile puis envoie data inscription du mobile (UDP 434) à l'agent mère qui contient COA, MA, HoA, format d'encaps° souhaité, durée de validité et num inscription

4) Agent mère reçoit cette demande, vérifie authenticité et exactitude Puis associe HoA et COA qui lui ont été communiqué. Tous les data destinés à HoA seront récupérés et encapsulés vers la CoA

5) L'agent envoie une confirmation d'inscription contenant HA, MA, durée et num inscription vers l'agent étranger

6)L'agent étranger transmet la confirmation au mobile.

Inscription agent mère



Refus d'inscription

Raisons possibles:

- **Administrativement interdit**
- **Ressources insuffisantes de l'agent**
- **Méthode authentification du mobile invalide**
- **Agent mère injoignable**

MobileIP et sécurité

Sécurité omniprésente avec mobileIP

Authentification nécessaire du mobile car utilisateur mal intentionné pourrait
- épier les données transmises par le mobile en déplacement
- enregistrer une fausse CoA auprès de l'agent mère et ainsi détourner les datagrammes destinés à une IP donnée

=> IETF a choisi IPsec pour sécuriser la signalisation relative à la mobilité

MobileIPv6
(RFC 3775, 2004)

Plus facile grâce notamment à la possibilité pour une interface d'avoir plusieurs adresses
modifications apportée au proto ND (découverte des voisins):

- **annonce du routeur (RA): bit H indique que le routeur fait office d'agent mère + 3options:**
  - **information sur le préfixes (permet aux agents mère d'apprendre les adr des autres HA)**
  - **intervalle de publication (spécifie l'intervalle de diff des msg RA, utile pour le mobile pour son algo de détection de mvt)**
  - **infos sur l'agent mère (infos spécifiques à son rôle d'HA)**

MIP6

Envoi des RA:
Normalement, RA envoyés toutes les 3 sec max
Avec MIPv6, cet intervalle est configuré pour les HA entre 0.5 et 1,5 s => permet de réduire le handoff (handover, temps pendant lequel le mobile n'est plus sur le réseau)

Adresses: config avec ou sans état
adr mères: préfixes annoncés par les routeurs+id_interface
dans réseau étranger: adr temporaires=préfixes +id_interf . Une seule adr temporaire primaire.

MIP6: routage

Correspondant vers mobile:

- envoi du paquet à adr mère L'agent mère agit comme proxy en interceptant les paquets et les tunnelant vers l'adr tempo primaire du mobile (utilise proxyARP ou proxyND)
- envoi direct vers mobile: grâce à une extension de routage (de type 2, pas la même que le loose source routing), avec @src=corresp, adr dest=CoA et extension routage contenant la HoA

MIP6: routage

Réponse du mobile: le mobile indique son adr tempo dans le champ source du paquets et ajoute dans une extension «destination» sont adr mère

Pourquoi adr src=tempo?

Pour éviter le problème de mascarade: de nombreux routeurs interdisent la propagation de paquets ayant comme adr src une adr n'appartenant pas à leur réseau

MIP6: Cache des associations

Structure implantée dans tout noeud IPv6

Pour chaque noeud Ipv6 associe la CoA primaire avec la HoA
Avant chaque envoi de paquets, consultation du cache:
- **si entrée présente, adr dst=CoA**
- **si non, paquet envoyé à HoA**

CoA1 <---> HoA1
CoA2 <---> HoA2
CoA3 <---> HoA3
:
:

MIP6: liste des mises à jour des associations

Structure maintenue par le mobile: conserve l'ensemble des correspondants en cours, pour maintenir leur association

Gérée par 4 options de l'extension «destination»

- mise a jour association: avertir corresp ou HA du changement
- ack assoc°: acquiter mise a jour + authent° obligatoire
- demande mise a jour association: demande à un mobile l'envoi
- adr principale: pour envoi au correspondant
  2 sous options: identifiant unique et liste des HA

MIP6: différences/v4

Par rapport à Ipv4:

- plus d'agent étranger
- extension de routage plutôt qu'encapsulation
- anycasting pour découverte des HA:
  préfixe réseau + fdff:ffff:ffff:fffe
- routes mieux optimisées

MIP6: implantations

- Linux MIPLv6 2.0 (fév 2006)
- *BSD Kamé
- Microsoft: patch pour XP SP1
- Routeurs: CISCO, 6WIND

Déploiement: assez faible

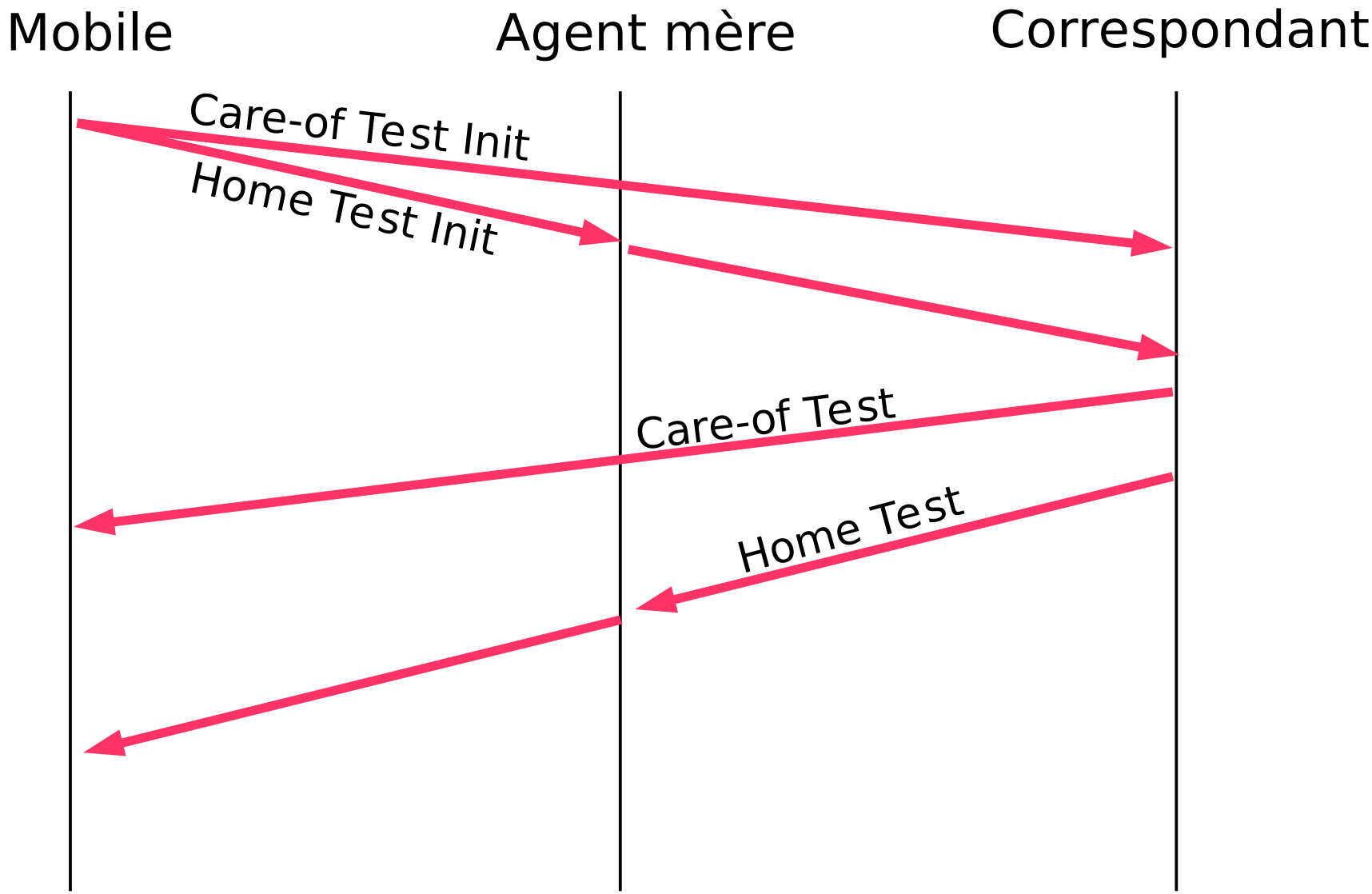
- Au japon, suivi des patients en temps réel depuis l'ambulance jusqu'à l'hôpital
- Beaucoup de terminaux mobiles intègrent un Linux
  => LTE-5G/MIPv6: le duo gagnant?

MIP6: Test de routage retour

Donne une garantie au correspondant que le mobile peut être atteint par sa Coa et HoA avant d'accepter les BU

- **Mises à jour d'association (BU) fréquentes**
  => la procédure de test doit être légère
- **Mobile et corresp ne se connaissent pas à priori**
  => pas de secret partagé permettant de chiffrer leur BU et BA et IPSec trop lourd pour ça
- **Deux phases en // pour tester CoA et HoA**
  utilise nombres aléatoires indexés

MIP6: Test de routage retour



Problèmes liés à MIP

- **Technologie récente**: réseaux sans fil de grande étendue (WIMAX) déployés seulement depuis 2003

- **Réel besoin?** Session d'application ont une durée de vie courte.
  Ex: HTTP: requête-réponse mais quid du streaming?

- **Routage non optimal**: résolu avec optimisation de route, mais cela demande que tout le monde l'intègre

- **Agents mère:** points critiques pour les performances
  => redondance possible: VHA (virtual home agent): 1 primaire et plusieurs secondaires en cas de panne ou pour équilibrer charge

- **Surcharge de signalisation** au changement de réseau => limiter le nombre de changements de réseaux

Problèmes de MIP

- **Possibilité d'oscillation** (changement fréquent entre 2 adr tempo):
  par ex si plusieurs points d'accès disponibles en même temps

- **Multicast**: pour s'abonner le mobile peut utiliser ses 2 adresses
  - si CoA => réinscription au groupe
  - si HoA=> le HA devra tunneler les paquets

- **Sécurité**: mise a jour assoc et ack assoc sont des points sensibles:
  - possibilité écouter position du mobileIP
  - possibilité usurper identité d'un mobile

Mobilité par le réseau : PMIP

- **Proxy Mobile IPv6 (PMIP6, RFC 5213) : mobilité IP gérée par le réseau => restreinte à un domaine**
- **Mêmes fonctionnalités que Mobile IP**
- **Sans modification de la pile protocolaire des hôtes**
- **Déplacement (chgt de réseau d'accès) sans changement d'adr IP**
- **Deux entités PMIP : Local Mobile Anchor (LMA) et Mobile Acces Gateway (MAG)**

Extensions

Mobile IPv6 peut fonctionner partout, mais

- délais de handoff (qques secondes) trop grand

- pas de possibilité pour l'opérateur de contrôler la mobilité des terminaux

Solutions:

- **Micro-mobilité**
- **Techniques d'amélioration du handoff**

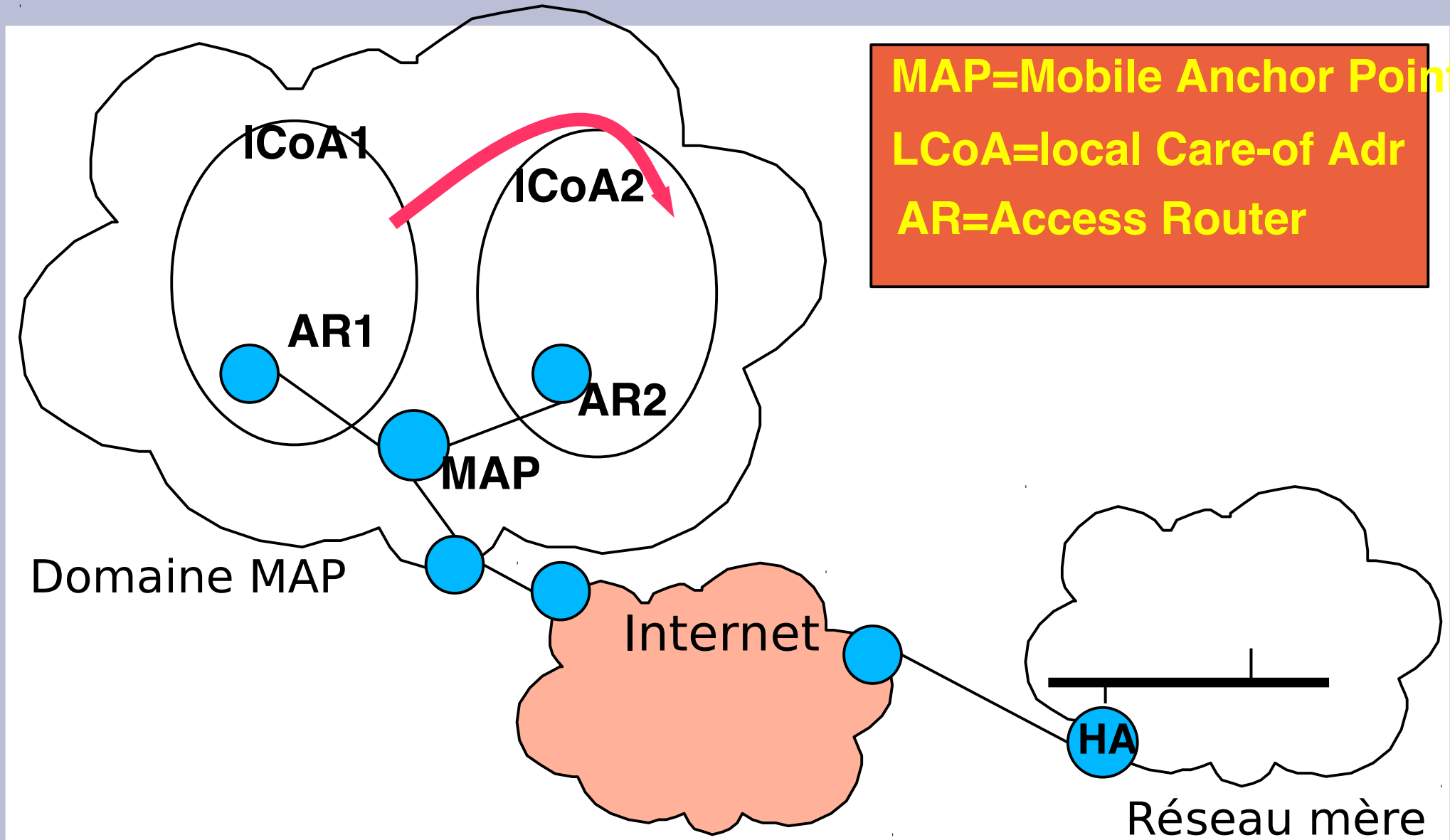
Micro-mobilité

But: rendre les déplacements du mobile à l'intérieur d'un domaine (de mobilité) transparent au HA et aux correspondants

La mobilité entre les domaines est faite par MobileIPv6
Les paquets à dest de la CoA d'un mobile sont dirigés vers le point d'attachement du mobile dans le domaine suivant deux techniques:

- **Cellular IP: modification du routage à l'intérieur du domaine: une route spécifique est maintenue du mobile vers la passerelle d'entrée du domaine. Pas possible à l'échelle de l'Internet.**
- **HMIPv6 (RFC 4140, aout 2005, INRIA): mobilité hiérarchique où le fonctionnement de MIPv6 est reproduit à l'intérieur du domaine. Solution avec contrôle par le réseau: NCHMIPv6 de FT R&D.**

Micro-mobilité



Fast Handovers for MobileIPv6
(RFC 4068, 08/2005)

Amélioration du handover par réduction du délai nécessaire à l'acquisition d'une nouvelle adresse temporaire lors d'un changement de routeur d'accès et retransmission des paquets entre l'ancien et le nouveau routeur d'accès.

Terminologie:
- PAR previous acces router: routeur d'accès dans réseau visité
- NAR next access router: routeur d'accès du prochain réseau visité
- FBU fast binding update, FNA: fast neighbor Adv

Fast Handovers for MobileIPv6 (RFC 4068, 08/2005)

- Connaissance des réseaux voisins (le mobile interroge son PAR): reçoit une liste des points d'accès voisins et les infos concernant les routeurs d'accès associés (adr IP, préfixe réseau, ...)

- Si qualité du signal baisse pour le mobile => sélection d'un autre point d'accès et construction d'une nouvelle CoA (nCoA)

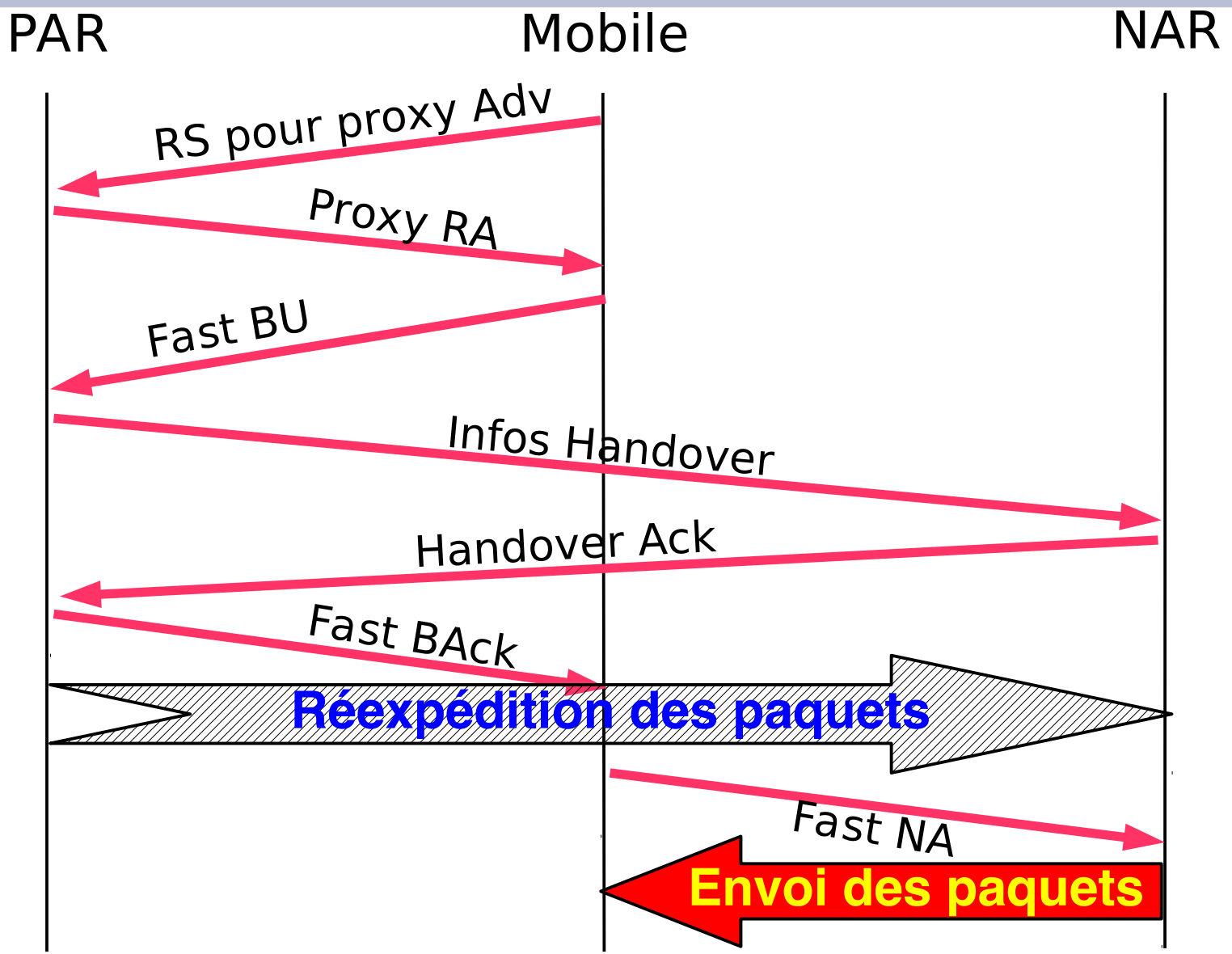
- Le mobile informe son PAR qu'il va bouger en émettant un FBU qui contient nCoA, et l'adr du nouveau routeur d'accès NAR. Le PAR informa le NAR qu'un handover va avoir lieu et lui transmet la nCoA pour vérification

Fast Handovers for MobileIPv6 (RFC 4068, 08/2005)

- à réception de l'Ack du NAR, le PAR acquitte le FBU et commence à faire suivre les paquets à dest de l'ancienne CoA dans un tunnel vers la nCoA
  Le NAR stocke les paquets en attendant l'arrivée du mobile.

• Quand le mobile effectue le handoff de niveau 2, il émet un FNA (fast neighbor adv) pour informer le NAR de sa présence
Il peut alors effectuer le BU vers le home agent et les corresp afin de recevoir directement les paquets de ceux-ci.

FHMIP6


PAR
Mobile
NAR
RS pour proxy Adv
Proxy RA
Fast BU
Infos Handover
Handover Ack
Fast BAck
Réexpédition des paquets
Fast NA
Envoi des paquets

FHMIP6

Procédure assez complexe qui nécessite

- coopération entre niveau 2 et niveau 3

- hypothèse que les routeurs d'accès communiquent entre eux => domaine d'usage restreint

NEMO: Network Mobility (IETF)

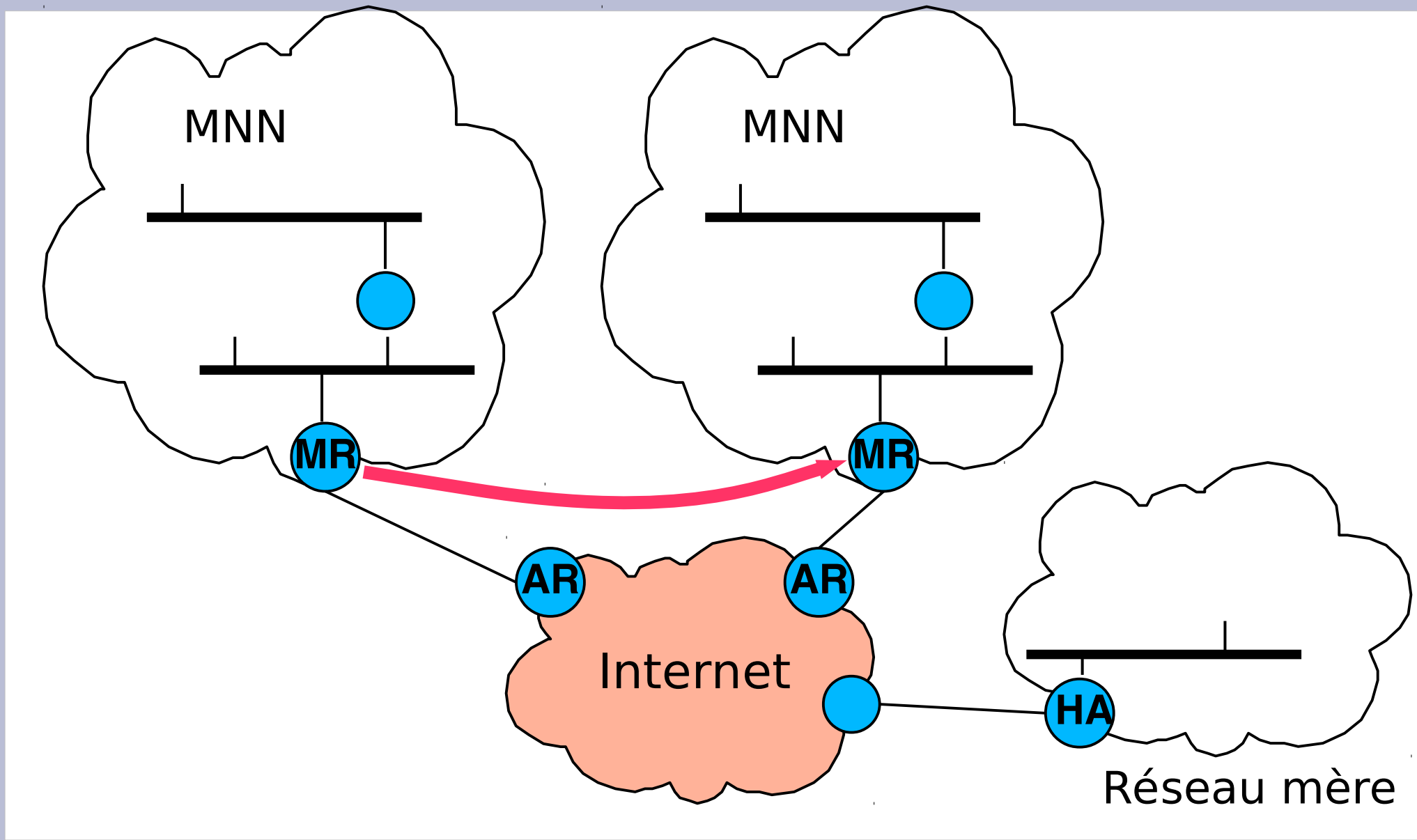
Si même les routeurs sont mobiles

MR=Mobile Router
AR=Access Router
MNN=Mobile Network nodes

Utilisation:

- **réseaux de capteurs (pour communiquer des données via le net)**
- **réseaux d'accès dans transports en commun**
- **réseaux personnels (PAN personnal Area Net): appareils électroniques de petite taille (montre, cardio, téléph, PDA,...)**

NEMO



NEMO

MIPv6 non adaptée pour la mobilité des réseaux:
la spécification ne permet pas au HA de rediriger les paquets pour les noeuds situés derrière le MR
mécanisme d'optimisation du routage inadéquat
=> solution spécifique mais concept proche

2 étapes pour permettre un déploiement rapide:

- **support de base (RFC 3963 en 2005): solution simple permettant de maintenir les sessions pour l'ensemble des MNN, sans optimisation de routage**

- **support étendu: pb d'optimisation de routage en cours d'étude**

NEMO: support de base

Sur le modèle de MIPv6, avec tunnel bidir entre le MR et le HA.

Tous les noeuds du réseau mobile partagent le ou les mêmes préfixes (MNP: Mobile Network Prefix)
Le MR aura plusieurs adr pour chacune de ses interfaces externes:

- **MRHoA= adr permanente: identifie le MR dans réseau mère**
- **MRCoA= adr obtenue dans le sous-réseau visité sur lequel l'inteface externe du MR s'ancre**

Seuls les MR changeant leur point d'ancrage obtiennent cette nouvelle adr, les autres MNN conservent leur adr
=> la mobilité leur est transparente

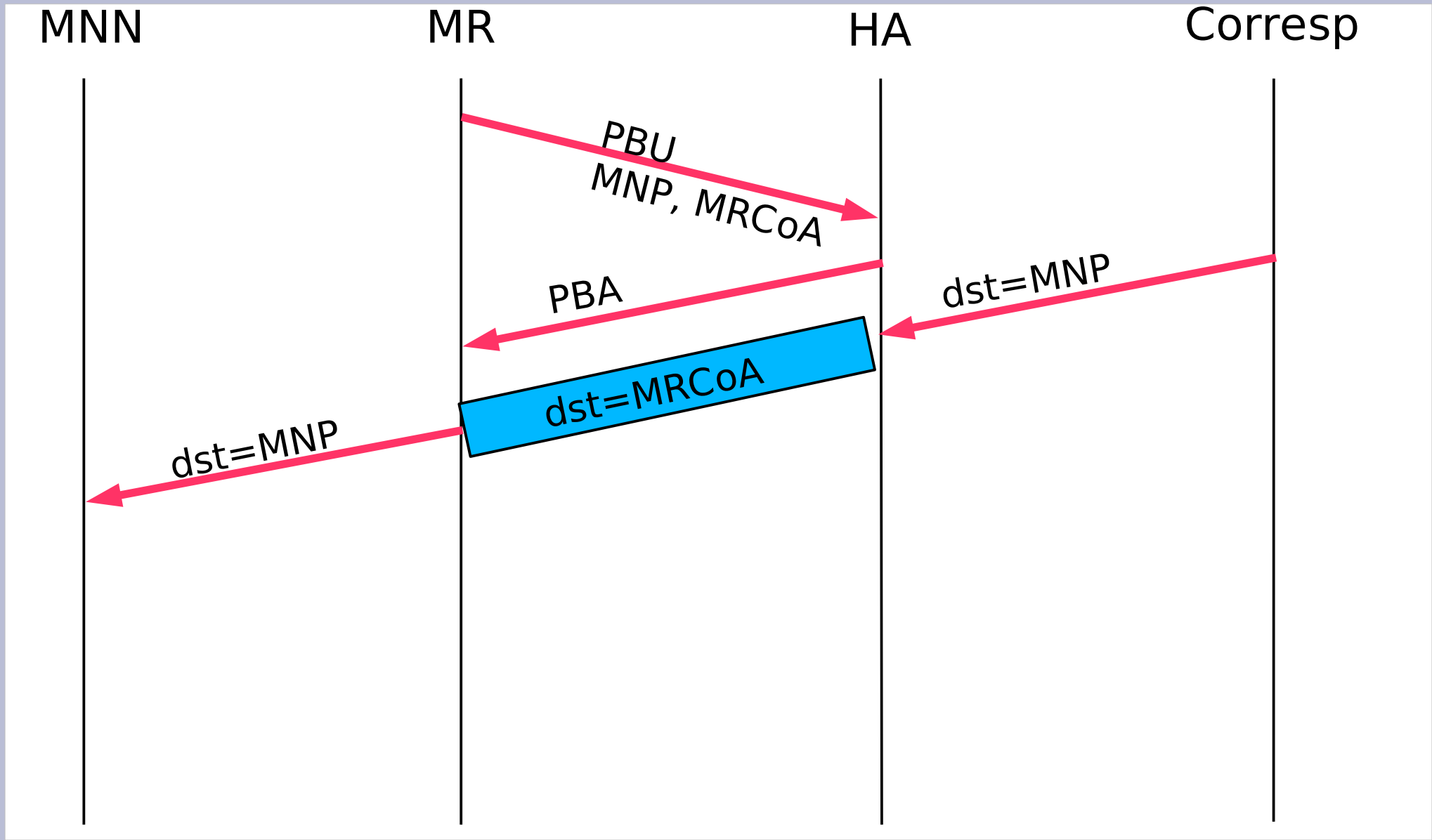
NEMO: support de base

Le MRCoA est envoyée au HA dans msg «Mise à jour des préfixes» (PBU) => MNP et MRCoA mis en cache par HA qui doit encapsuler les paquets à dest des stations du réseau mobileIPv6

Comm entre corresp et MNN: le corresp ne connait pas MRCoA => envoi au réseau mère
Le HA encapsule vers le MR (MRCoA)
Le MR décapsule et propage sur l'interface interne

Pb en cours d'étude: multidomiciliation
SHIM6=level3 multihoming (draft, oct 2007)

NEMO



UMIP
(Usagi-patched mobile Ipv6 for Linux)

- Implantation open-source de MIPv6 et NEMO basic
- Basé sur MIPL2 (plus maintenu)
- Recompiler le noyau linux avec options de mobilité
- Démon mip6d pour HA, MN, CN

HA

- Activer le forwarding(forwarding=1)
- Activer le proxy ND (proxy_ndp=1)
- Activer radvd
- mip6d.conf :

```
NodeConfig HA;

## List of interfaces where we serve as Home Agent

Interface "eth0" ;


## IPsec configuration
```

MN

- **mip6d.conf**

```
NodeConfig MN;

## Support route optimization with other MNs
DoRouteOptimizationCN enabled;

## Use route optimization with CNs
DoRouteOptimizationMN enabled;

UseCnBuAck enabled;

MnDiscardHaParamProb enabled;

Interface "eth0";

MnRouterProbes 1;

MnHomeLink "eth0" {
HomeAddress 3ffe:501:ffff:100::1/64;
#          address              opt.
#MnRoPolicy     3ffe:2060:6:1::3  enabled;
#MnRoPolicy                       disabled;
}

## IPsec configuration
UseMnHaIPsec enabled;

## Key Management Mobility Capability
KeyMngMobCapability disabled;

IPsecPolicySet {
      HomeAgentAddress 3ffe:2620:6:1::1;
      HomeAddress 3ffe:2620:6:1::1234/64;
      IPsecPolicy Mh UseESP 1 2;
      IPsecPolicy ICMP UseESP 5;
      IPsecPolicy TunnelMh UseESP 3 4;
}
```

CN

- **mip6d.conf**

```
# This is an example of mip6d Correspondent Node configuration file


NodeConfig CN;


## If set to > 0, will not detach from tty

#DebugLevel 0;


## Support route optimization with MNs

DoRouteOptimizationCN enabled;
```

Mobilité niveau 3+

- **SCTP (Stream Control Transport Protocol, RFC 4960)**
  - **(niveau 4) avec ajout d'adresses dynamiques (m-SCTP, RFC 5061)**
- **HIP (Host Identity Protocol, RFC 4423)**
  - **Espace d'identité (HI) => associer sockets aux HI plutot qu'aux @IP**
  - **Association HI-IP dynamique**

HIP

- HI = clé cryptographique publique
  - 1 host = au moins 1 clé publique ou privée
  - Si publique => unicité au niveau mondial et stokkage au niveau global (DNS)
  - Utilisée pour authentification durant la phase de connexion

HIP

- **Mobilité :**
  - **Pendant connexion : envoi d'un message HIP readdress (REA) sur le canal sécurisé**
  - **Pendant phase de connexion ou mobilité des deux pairs : besoin d'un serveur relais temporaire (Rendez-vous server) pour renvoi des msg HIP**