PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE

Shinta Sugimoto

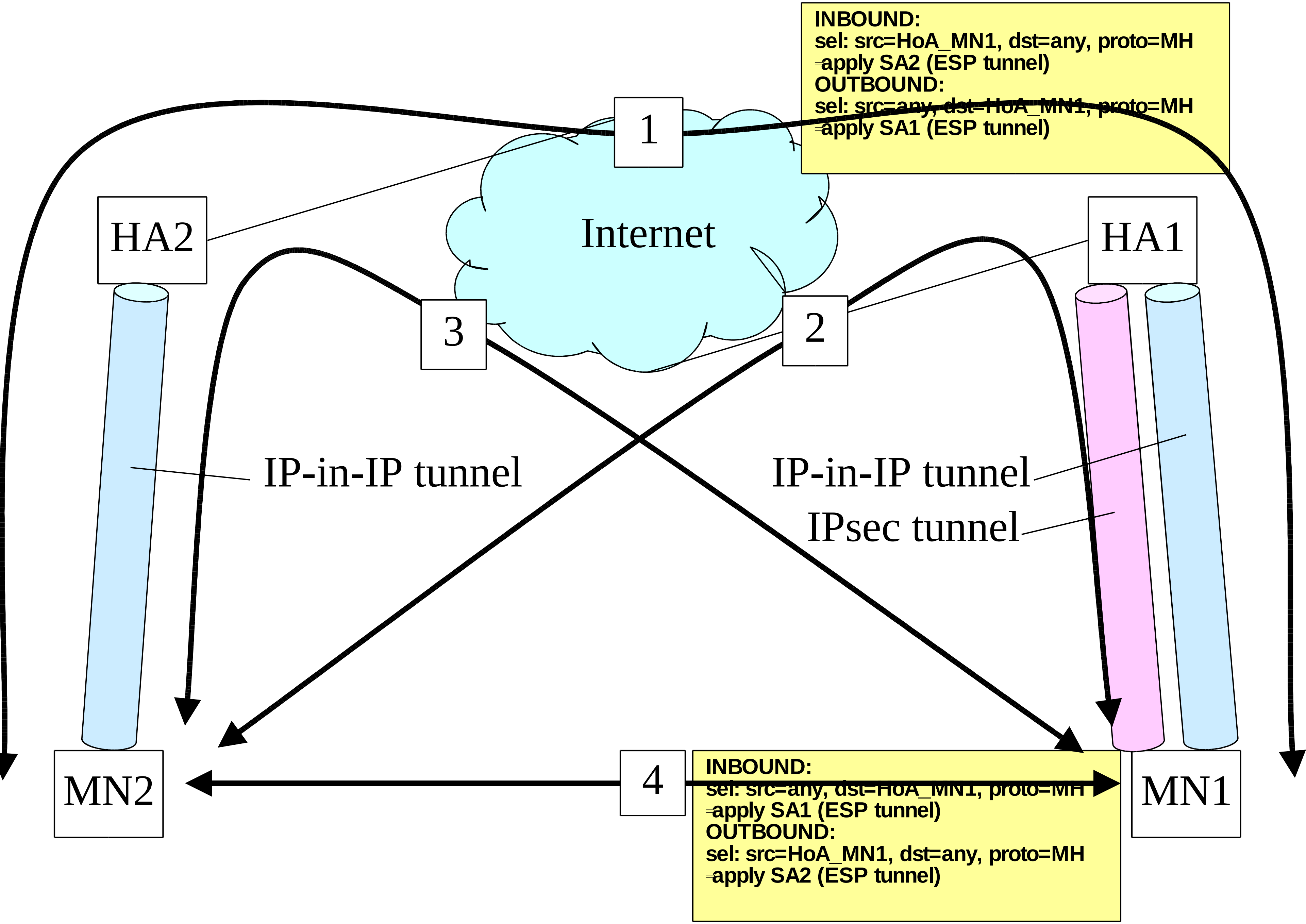
Ericsson/USAGI Project

Topics

- Background
- Do we need any interaction between Mobile IPv6 and IPsec/IKE?
- Extension to PF_KEY framework – MIGRATE
  - Basic mechanism
  - Message sequence
  - Limitation
- Implementation status

Background

- Mobile IPv6 uses IPsec to protect messages exchanged between MN and HA as specified in RFC 3775, RFC 3776:
  - Home Registration signals (BU/BA)
  - Return Routability messages (HoTI/HoT)
  - MIPv6 specific ICMPv6 messages (MPS/MPA)
  - Payload packets
- SA pairs are necessary to be established between the MN and HA in static or dynamic manner
- Tunnel mode SAs are necessary to be updated whenever the MN performs movement



INBOUND:
sel: src=HoA_MN1, dst=any, proto=MH
⇒apply SA2 (ESP tunnel)
OUTBOUND:
sel: src=any, dst=HoA_MN1, proto=MH
⇒apply SA1 (ESP tunnel)

INBOUND:
sel: src=any, dst=HoA_MN1, proto=MH
⇒apply SA1 (ESP tunnel)
OUTBOUND:
sel: src=HoA_MN1, dst=any, proto=MH
⇒apply SA2 (ESP tunnel)

Necessary Interactions between Mobile IPv6 and IPsec/IKE

- Update endpoint address of tunnel mode SA
  - Mobile IPv6 component may not have full access to SADB
- Update endpoint address stored in SPD entry which is associated with tunnel mode SA
  - IKE should be able to continuously perform key negotiation and re-keying
- IKE daemon should update endpoint address of the IKE connection (aka K-bit) to keep its alive while the MN changes its CoA

Requirements

- Modifications to the existing software (Mobile IPv6 and IPsec/IKE stack) should be kept minimum
- The mechanism should not be platform dependent

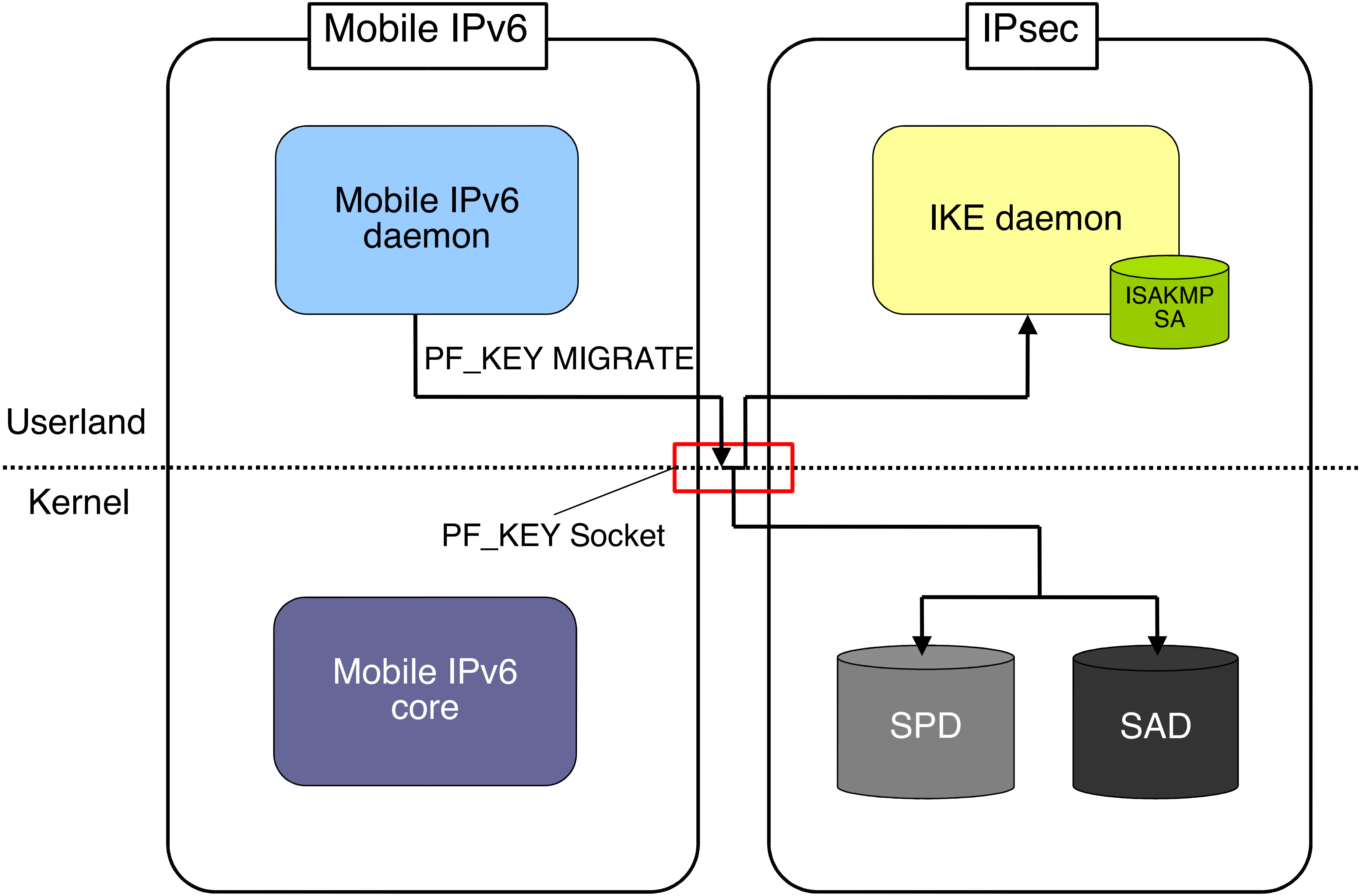
Extension to PF_KEY framework – PF_KEY MIGRATE

- Introduce a new PF_KEY message named MIGRATE which is to be issued by Mobile IPv6 components to inform movement
- PF_KEY MIGRATE requests system and user application to update SADB as well as SPD:
  - Tunnel mode SA entry
  - SPD entry which is associated with the tunnel mode SA
- It is beneficial if the message can also be used to handle K-bit

PF_KEY MIGRATE – message format

• Selector Information:	
– Source address	3ffe:501:ffff:100:1:2:3:4/128 (HoA)
– Destination address	::/128
– Upper layer protocol (i.e. MH)	135 (MH)
– Direction (inbound/outbound)	1 (outbound)
• Old SA Information:	
– Old tunnel source address	3ffe:501:ffff:500:1:2:3:4/128 (Old-CoA)
– Old tunnel destination address	3ffe:501:ffff:100::1/128 (HA address)
– Protocol (ESP/AH)	50 (ESP)
• New SA Information:	
– New tunnel source address	3ffe:501:ffff:400:1:2:3:4/128 (New-CoA)
– New tunnel destination address	3ffe:501:ffff:100::1/128 (HA address)
– Protocol (ESP/AH)	50 (ESP)

For instance, in order for the MN to update its outbound SP entry and associated Tunnel Mode SA to protect MH messages…


Mobile IPv6
IPsec
Mobile IPv6 daemon
IKE daemon
ISAKMP SA
PF_KEY MIGRATE
Userland
Kernel
PF_KEY Socket
Mobile IPv6 core
SPD
SAD

Limitations of PF_KEY MIGRATE

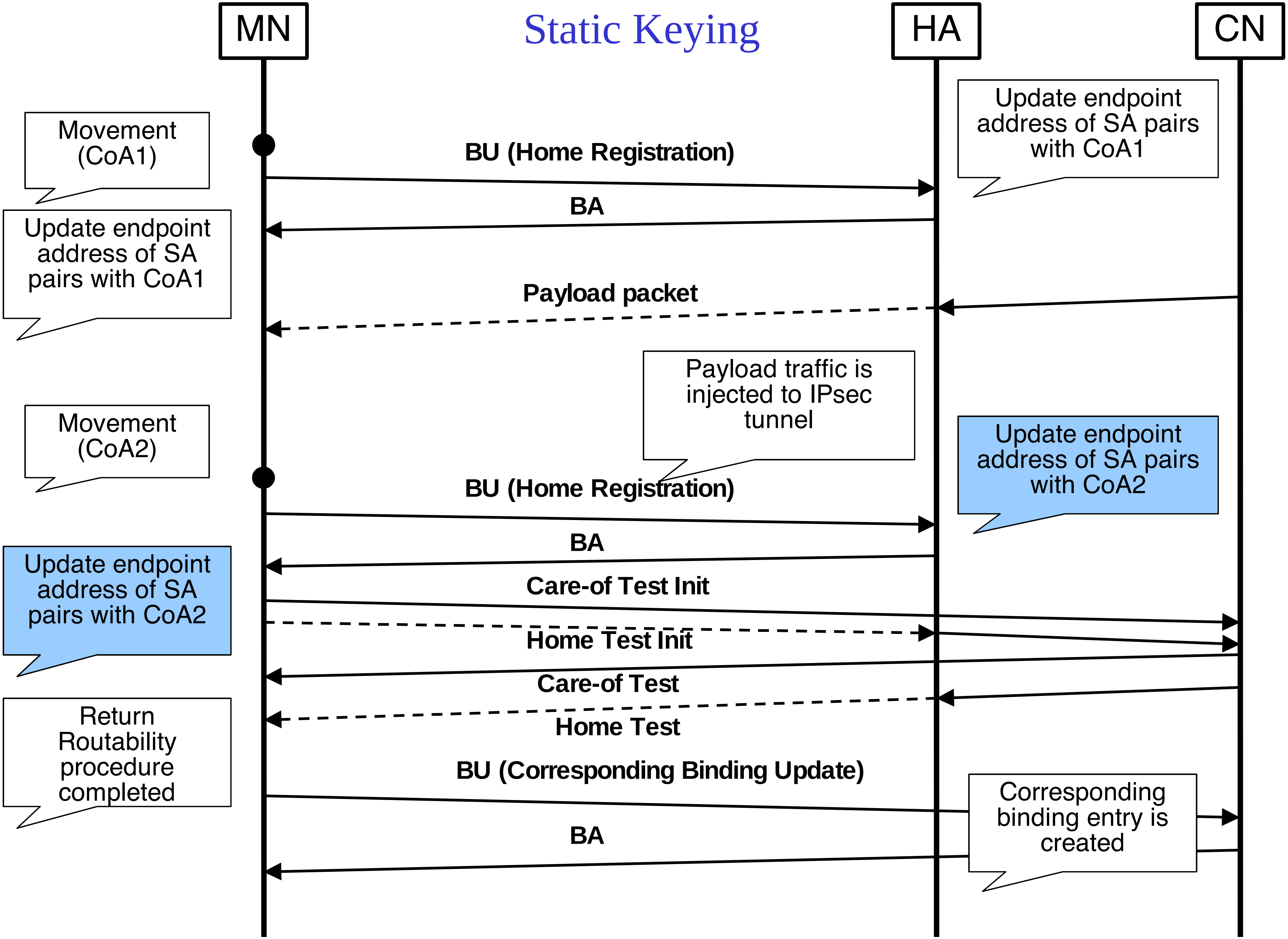
- There is an ambiguity in the way to specify target SADB entry:
  - Current scheme to specify target SADB entry does not seem to be the best solution
  - Mobile IPv6 is required to sequentially maintain the binding record
- Delivery of PF_KEY MIGRATE message cannot be guaranteed:
  - When a message is lost, there will be an inconsistency between Mobile IPv6 and IPsec database

Implementation Status

- KAME/BSD Platform
- MIPL2.0 on Linux-2.6
  - Prototype Implemented
  - To be tested in Connectathon 2005

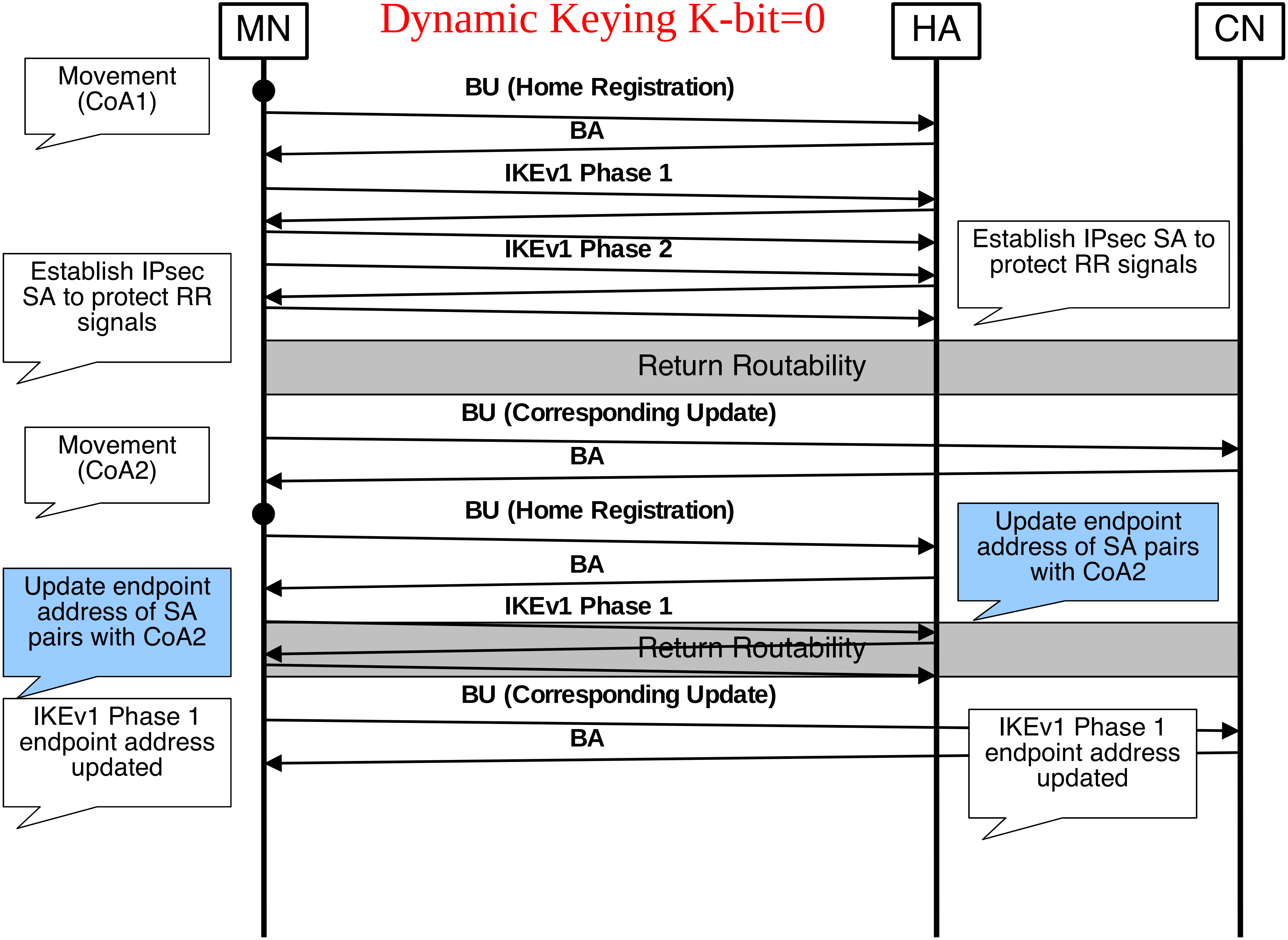
Thank you!
&
Any Questions?

Static Keying



MN
HA
CN
Movement (CoA1)
Update endpoint address of SA pairs with CoA1
BU (Home Registration)
BA
Update endpoint address of SA pairs with CoA1
Payload packet
Payload traffic is injected to IPsec tunnel
Movement (CoA2)
BU (Home Registration)
Update endpoint address of SA pairs with CoA2
BA
Update endpoint address of SA pairs with CoA2
Care-of Test Init
Home Test Init
Care-of Test
Home Test
Return Routability procedure completed
BU (Corresponding Binding Update)
Corresponding binding entry is created
BA

Dynamic Keying K-bit=0



MN

HA

CN

Movement (CoA1)

BU (Home Registration)

BA

IKEv1 Phase 1

IKEv1 Phase 2

Establish IPsec SA to protect RR signals

Establish IPsec SA to protect RR signals

Return Routability

BU (Corresponding Update)

BA

Movement (CoA2)

BU (Home Registration)

Update endpoint address of SA pairs with CoA2

BA

Update endpoint address of SA pairs with CoA2

IKEv1 Phase 1

Return Routability

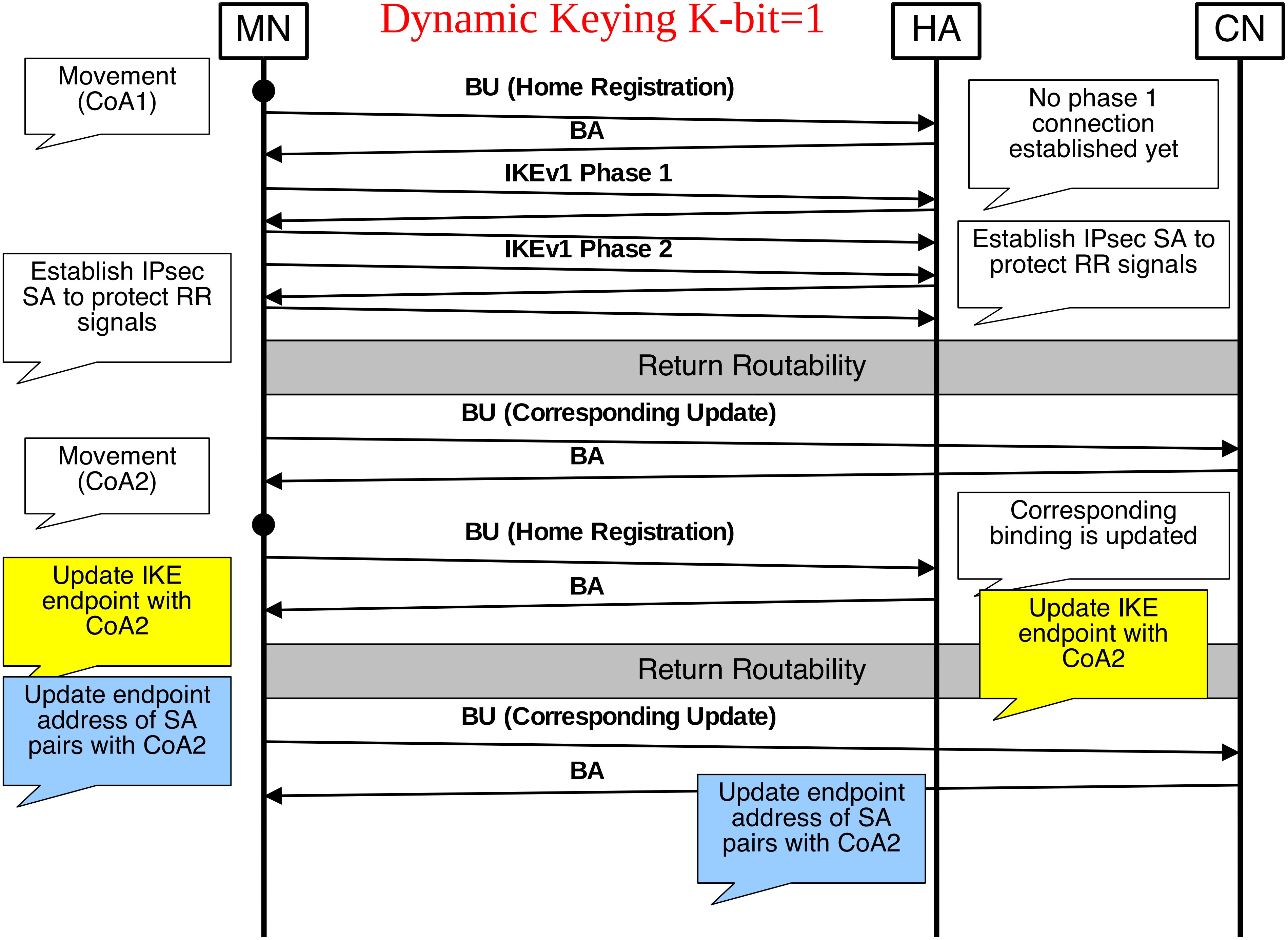
IKEv1 Phase 1 endpoint address updated

BU (Corresponding Update)

BA

IKEv1 Phase 1 endpoint address updated

Dynamic Keying K-bit=1



MN

HA

CN

Movement (CoA1)

BU (Home Registration)

BA

No phase 1 connection established yet

IKEv1 Phase 1

IKEv1 Phase 2

Establish IPsec SA to protect RR signals

Establish IPsec SA to protect RR signals

Return Routability

BU (Corresponding Update)

BA

Movement (CoA2)

Corresponding binding is updated

BU (Home Registration)

BA

Update IKE endpoint with CoA2

Update IKE endpoint with CoA2

Return Routability

Update endpoint address of SA pairs with CoA2

BU (Corresponding Update)

BA

Update endpoint address of SA pairs with CoA2