

FPANA: Combining PANA and FMIPv6 for Fast Authentication at Handover

draft-hiko-pana-fpana-00.txt

Yoshihiko Kainuma (Keio Univ.)

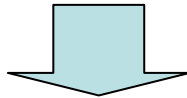
Natsuko Ono (BB Mobile/Japan Telecom)

Hideki Hayashi (BB Mobile/Japan Telecom)

Fumio Teraoka (Keio Univ.)

Motivation

- Goal: Intra-domain fast handover with AAA
 - e.g., streaming service on IEEE802.11a (54Mbps), fast L3 handover (gap time < 10ms), with AAA
- We have already achieved L3 driven fast handover using L2 triggers
 - draft-koki-mobopts-l2-abstractions-02.txt (in 62nd IETF)
 - However, AAA is not supported

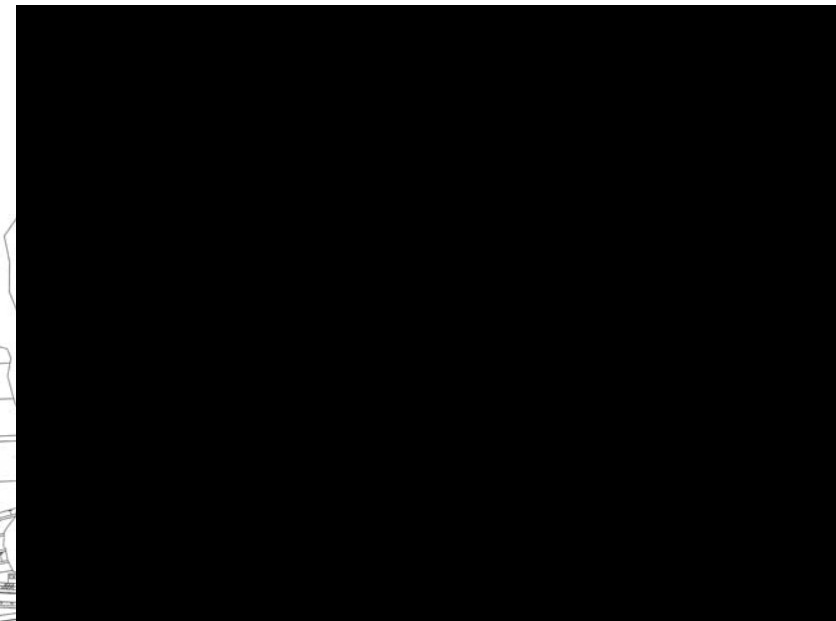
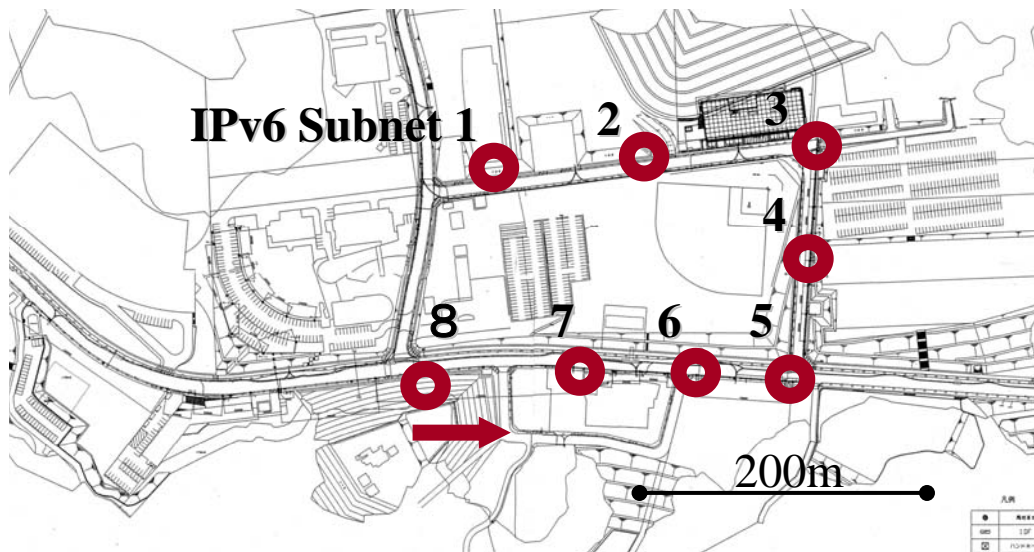


We want to make fast handover secure

Demo:L3-Driven Fast Handover Using L2 Triggers

(based on draft-koki-mobopts-l2-abstractions-02.txt)

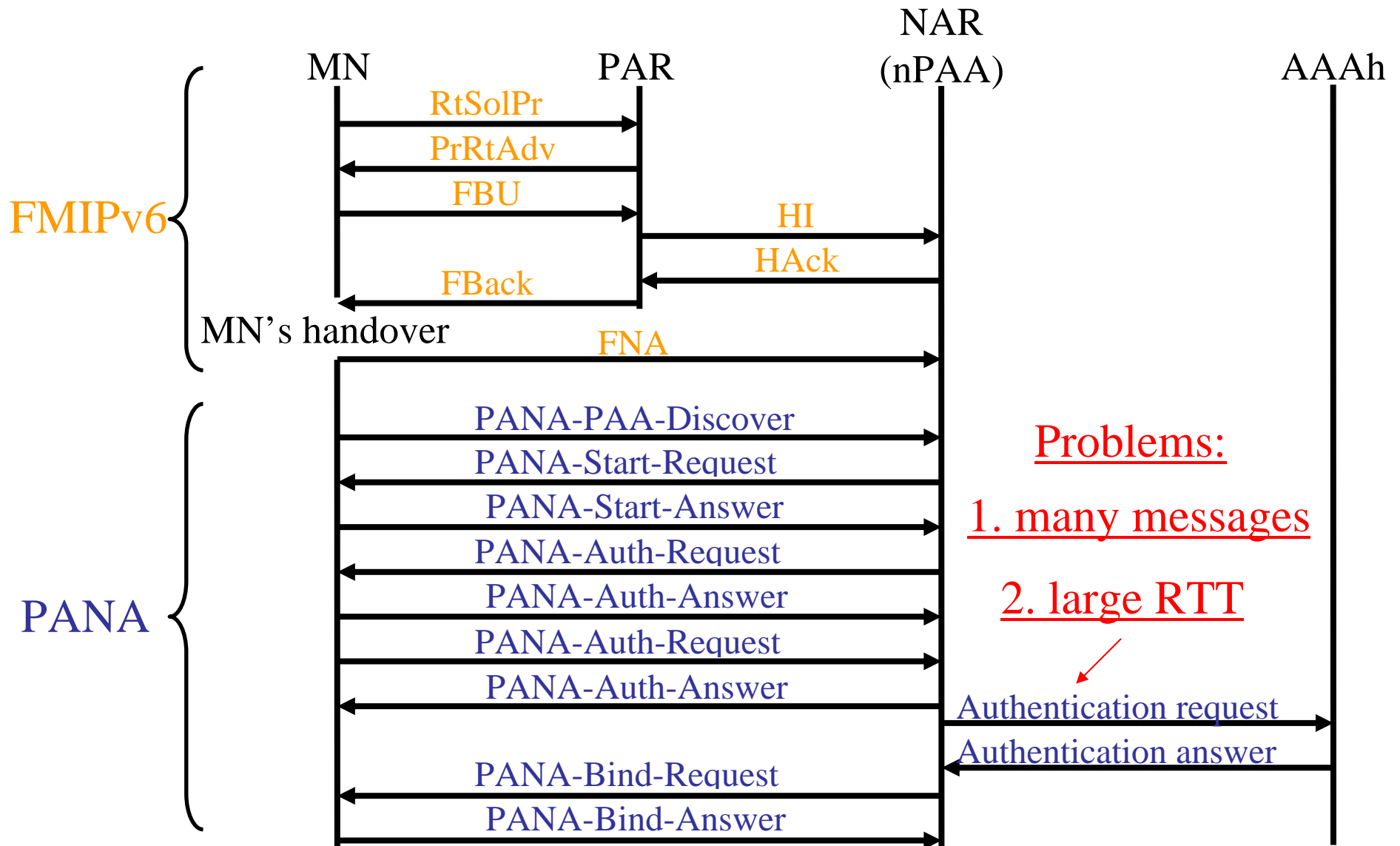
- Application: DVTS
 - half rate: 15Mbps
 - from MN in vehicle to fixed CN
- L3 mobility protocol: LIN6
- L2: IEEE802.11a (54Mbps)
- 8 IPv6 subnets
 - 8 access points / access routers
- Total gap time: 3-4 ms
 - L2 handover: 1-2 ms (fixed)
 - L3 handover: 1-2 ms (depends on RTT)



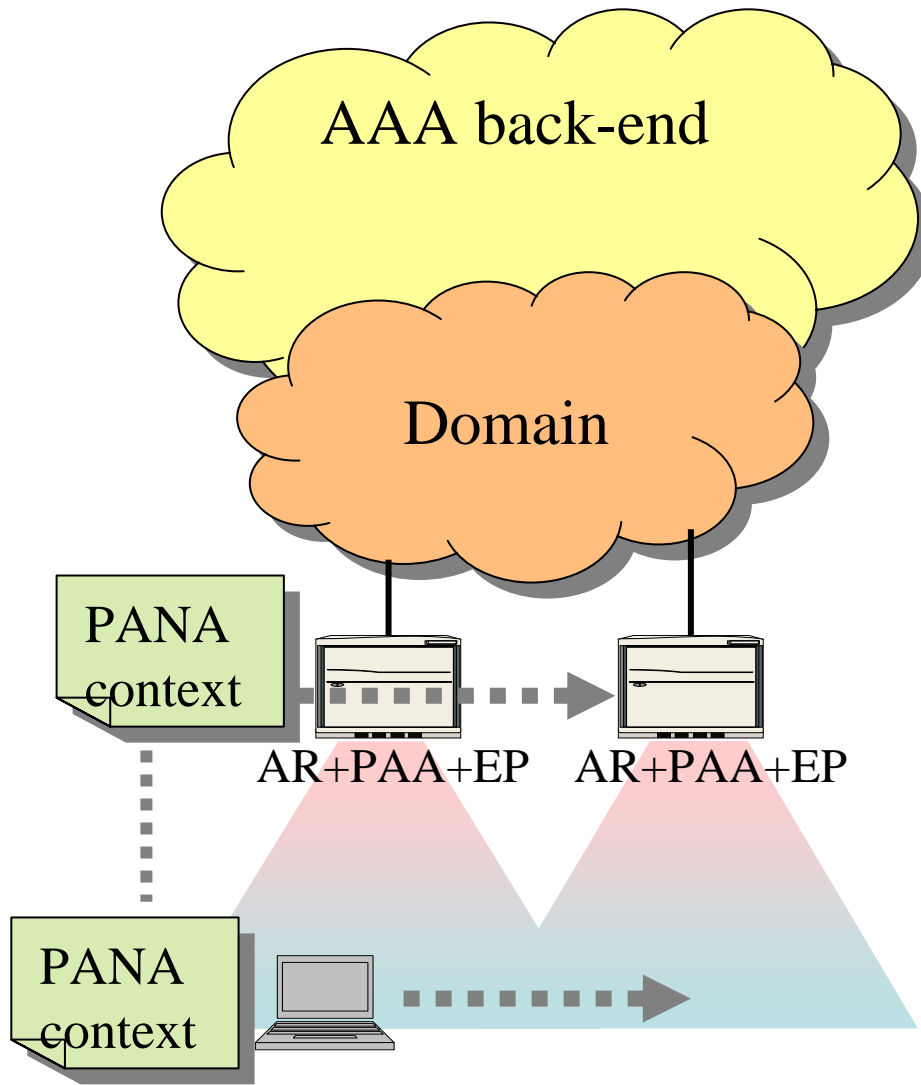
Receiver

sender

FMIPv6 (predictive mode) + PANA

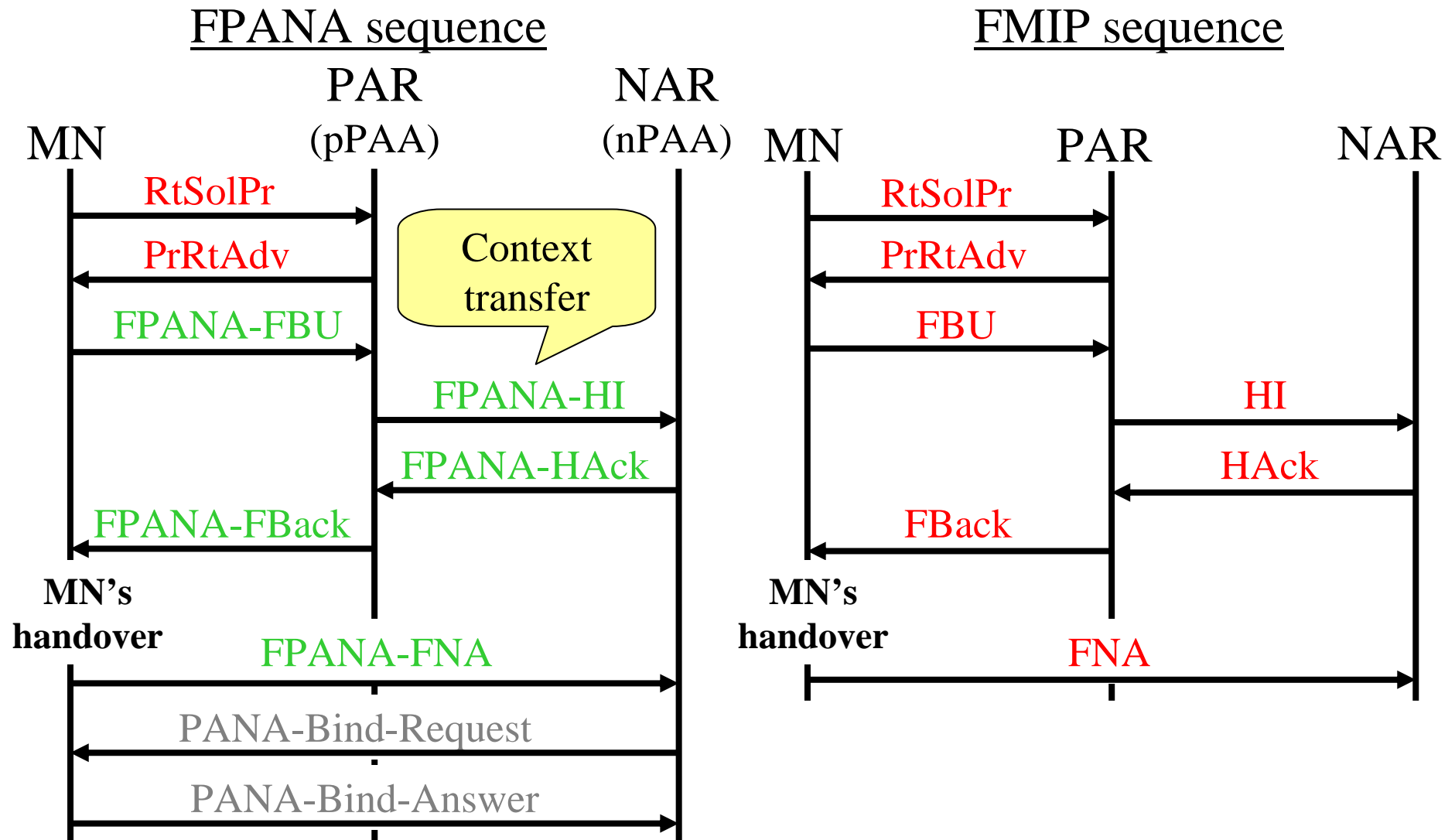


Proposal: FPANA

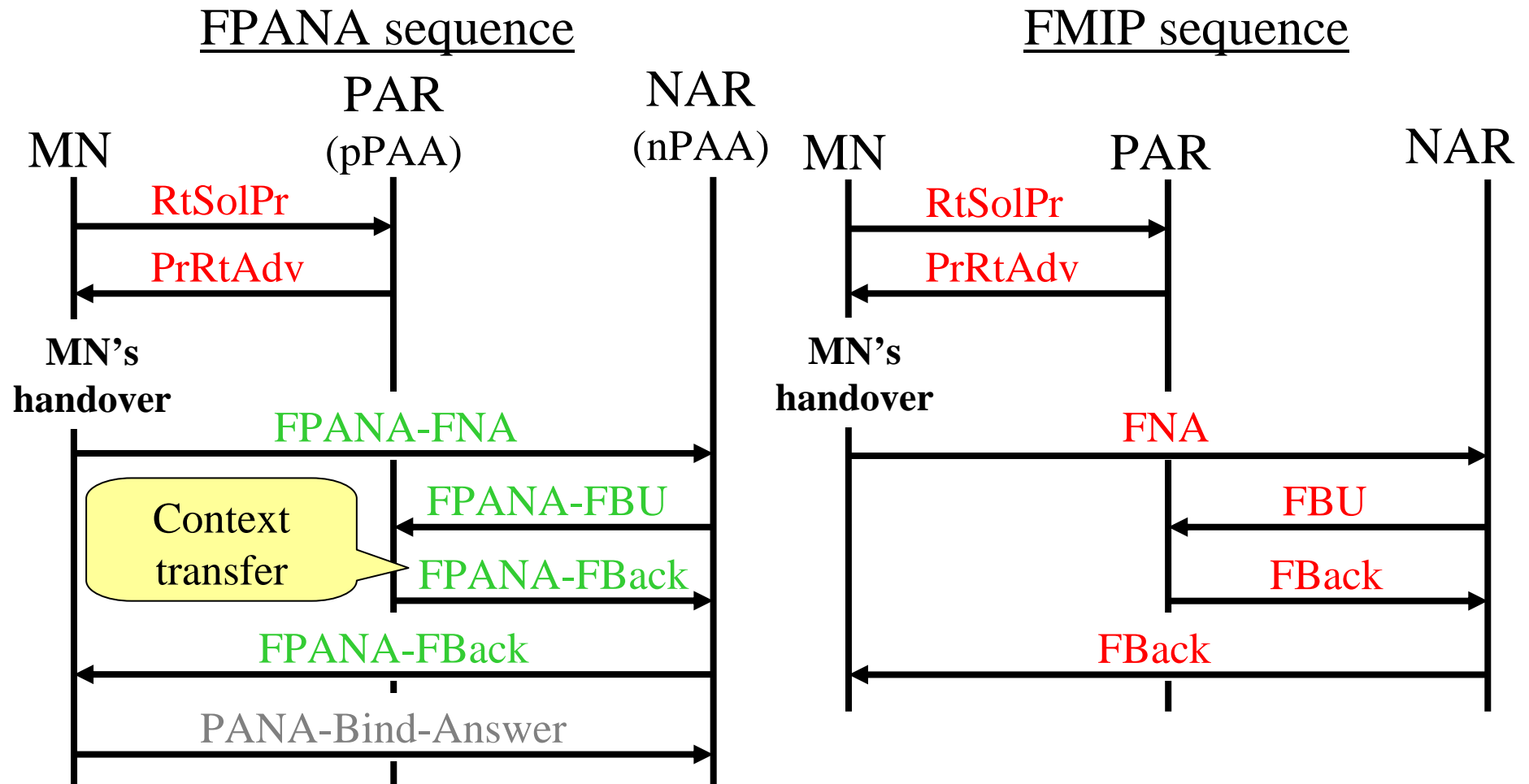


- Goal: Intra-domain fast handover with AAA
- Context transfer between ARs
- Use of **FMIP** messages for context transfer
 - fast handover + AAA
- Assumptions
 - AR, PAA, and EP are collocated.
 - IPsec SA is established between PAR and NAR in advance

Proposal: FPANA (predictive mode)

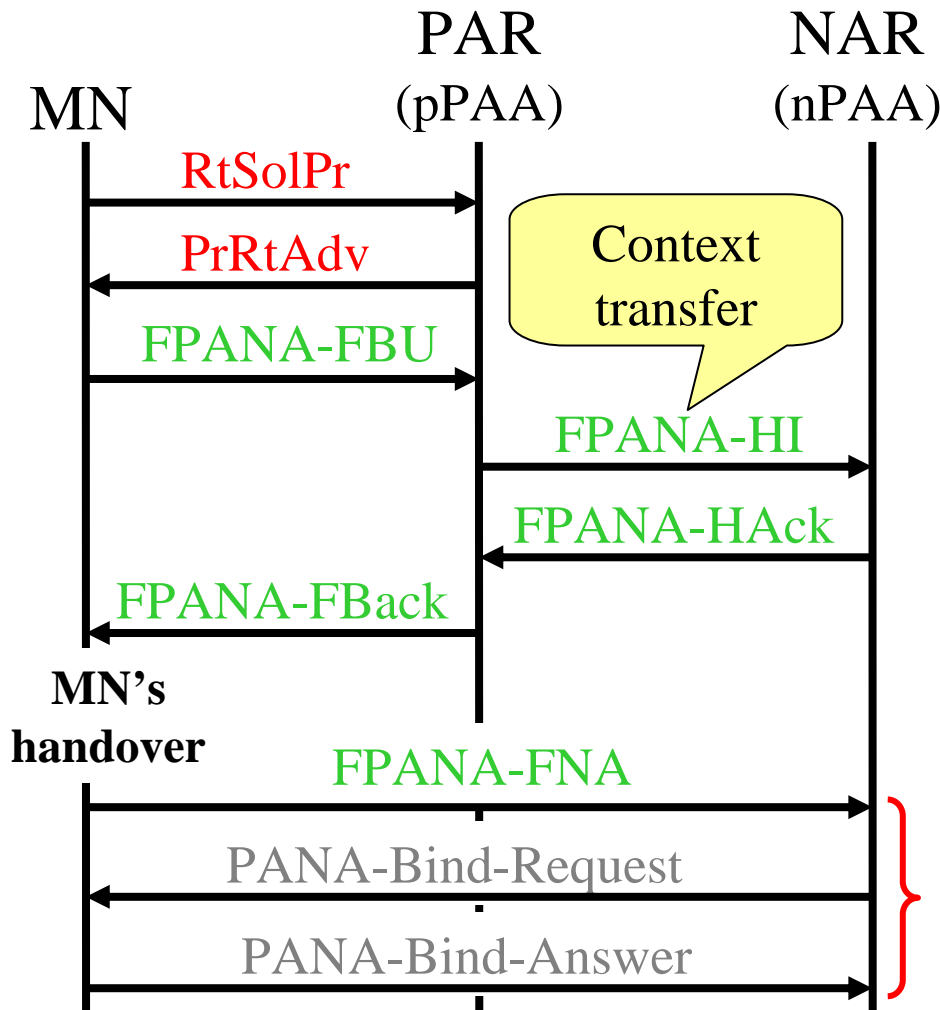


Proposal: FPANA (reactive mode)

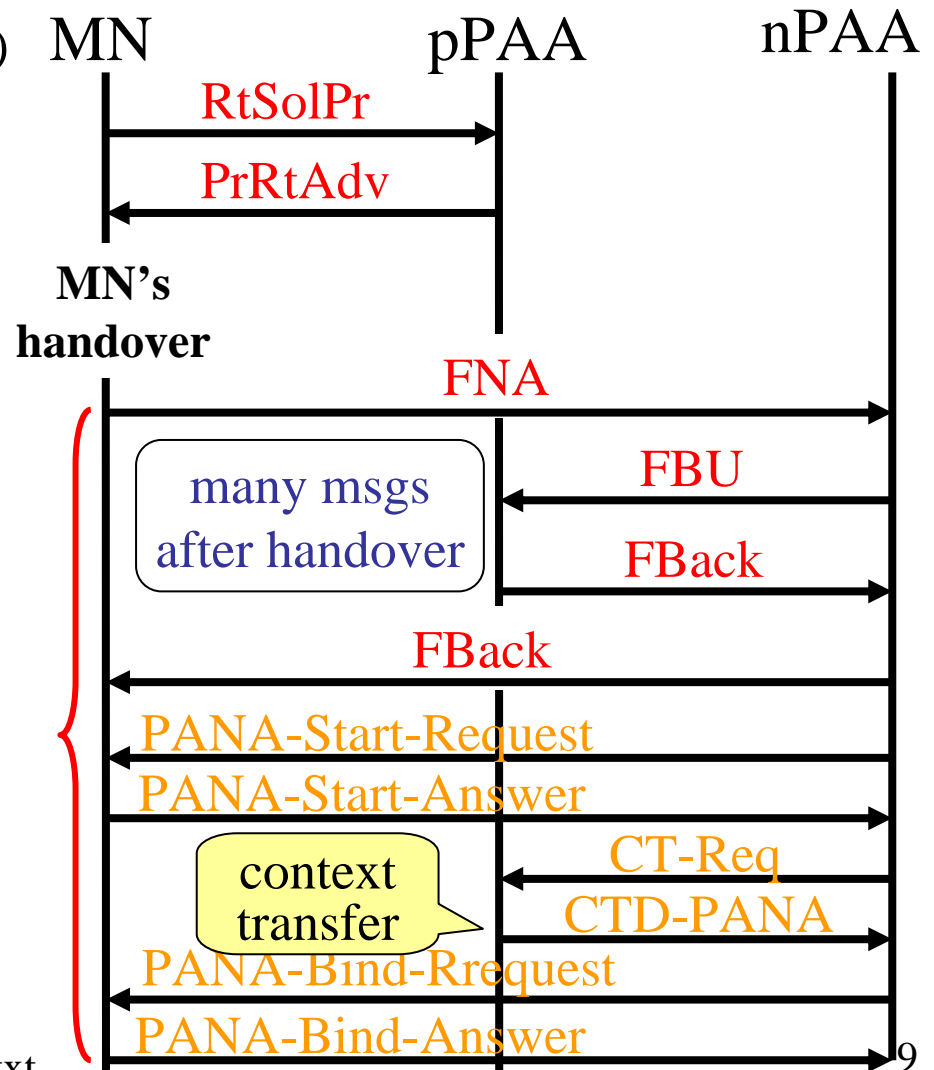


cf. draft-bournelle-pana-ctp-03

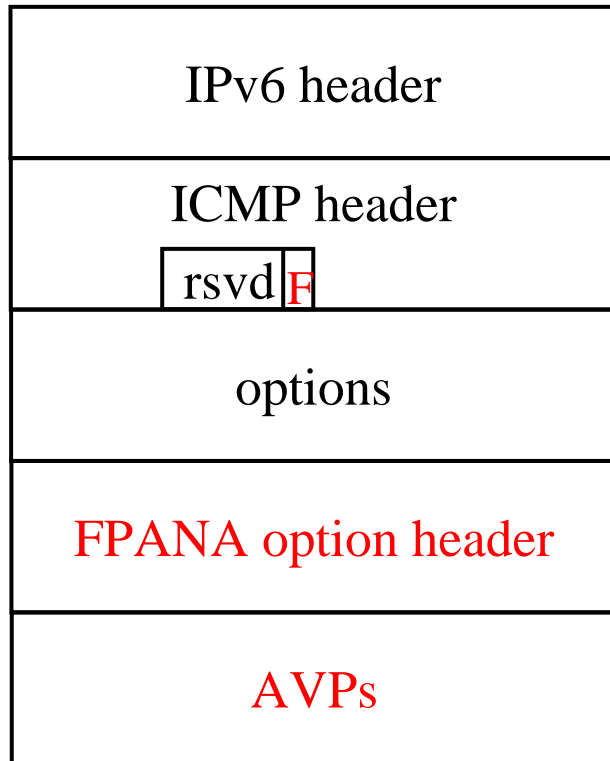
FPANA sequence (predictive)



ctp-03 sequence (reactive mode only)

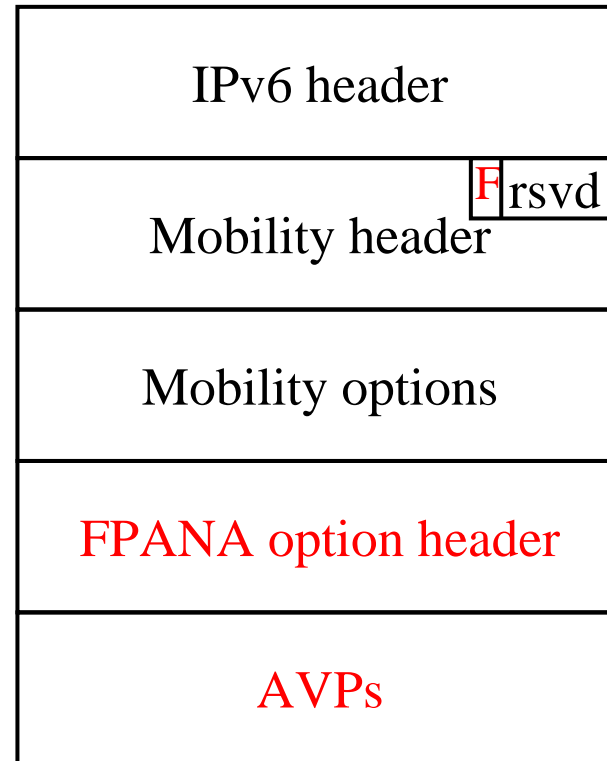


FPANA Message Formats



FPANA message
using ICMP

- FPANA-HI
- FPANA-Hack
- FPANA-NAack



FPANA message
using Mobility header

- FPANA-FBU
- FPANA-FNA
- FPANA-FBack

FPANA Option Header

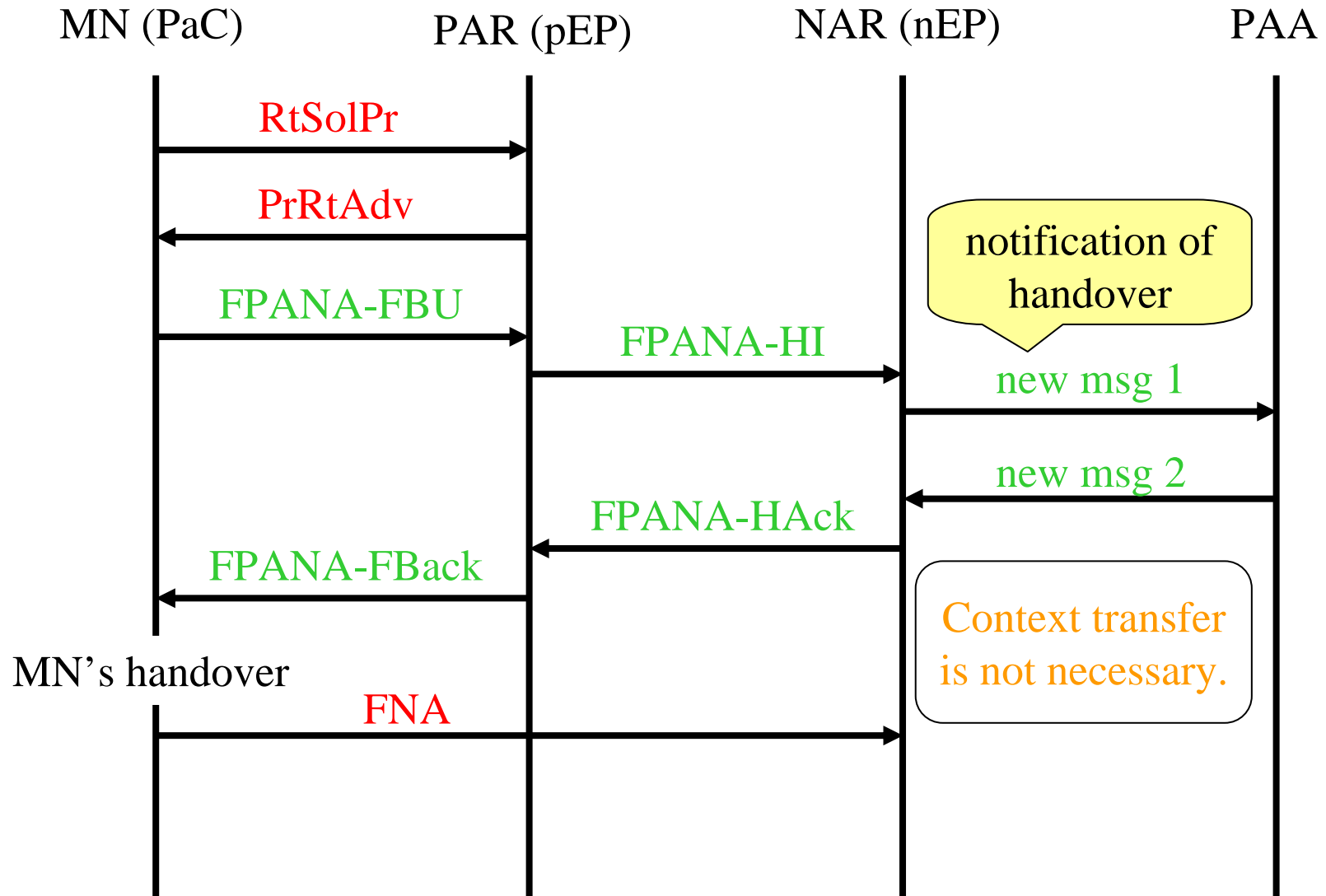
Type	Length	FPANA transaction ID
Message type	reserved	

- **Type**
 - FPANA option (TBD)
- **Length**
 - length of FPANA option header and AVPs
- **FPANA transaction ID**
 - for matching between request and answer
- **Message type**
 - FPANA-FBU 1
 - FPANA-HI 2
 - FPANA-Hack 3
 - FPANA-FBack 4
 - FPANA-FNA 5
 - FPANA-NAack 6

Transferred Parameters

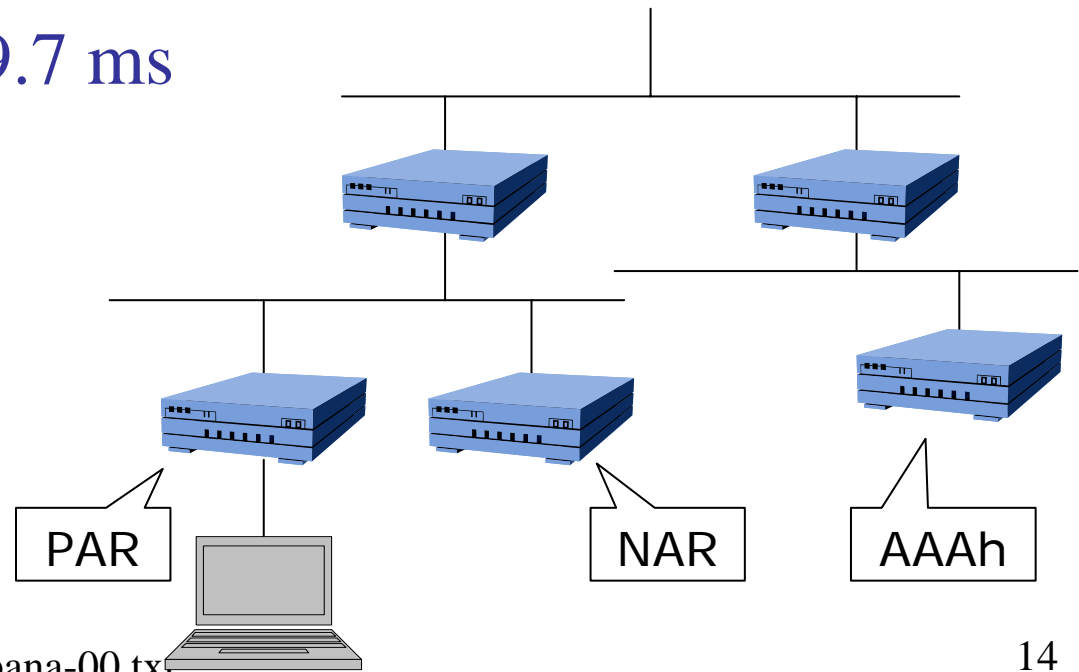
- FPANA
 - PANA_MAC_KEY
 - session lifetime
 - nonce
 - IPS information
 - retransmission interval
- cf. draft-bournelle-pana-ctp-03.txt
 - Session-Lifetime elapsed
 - AAA-Key-int
 - ISP-Identifer, ISP-Name
 - NAP/ISP Separate Authentication

cf. Multi-hop PANA + FPANA



Implementation and Evaluation

- FPANA test code was implemented on FreeBSD-5.3.
- FMIP (predictive) + PANA: $12.4 \text{ ms} + \text{RTT}_{\text{NAR-AAAh}}$
 - $\text{RTT}_{\text{NAR-AAAh}} : O(10 \text{ ms})$ in case of domestic,
 $O(100 \text{ ms})$ in case of international.
- FPANA (predictive): 9.7 ms
 - no access to AAAh



Questions & Comments

- Next steps ?