Functional decomposition

multi6 wg meeting - IETF 61

MULTI6 dt: J. Arkko, M. Bagnulo,
I. van Beijnum, G. Huston, E.
Nordmark, M. Wasserman, J. Ylitalo.

Goal of the document

- Walkthrough the possible messages of a multi6 protocol for preserving established communications through locator changes
- Agnostic to the security mechanism used in protecting the control messages

Outline

- Initial contact
- Capabilities detection
- M6 host-pair context establishment
- Locator set management
- Re-homing procedure
- Removal of M6 session state

Initial contact

- Required information
  - ULID
  - reachable locator
- If ULID == reachable locator, then no special M6 capabilities required
- If ULID =! reachable locator, then move to capabilities detection

Failure during start-up

- If the locator for initial contact unreachable the options are:
    - (App) retries using different address (locator & ULID).
    - Keep the ULID and change the locator. Needs M6 support, so cap. detection.
        - Transparent to apps

M6 Capabilities detection

- Node Configuration
- DNS Configuration
- Host-Based Dynamic Discovery
  - Independent
  - Integrated (preferred)

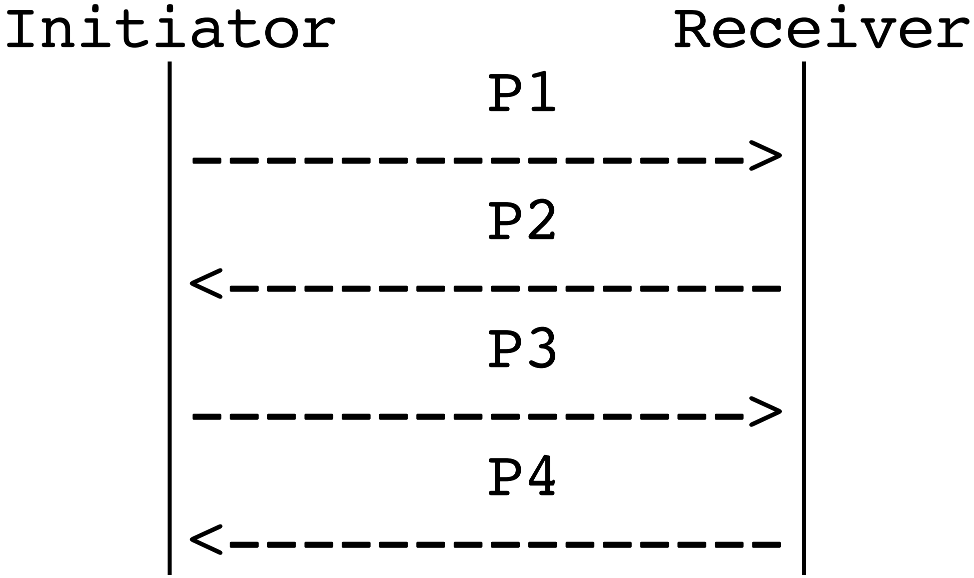
M6 host-pair context establishment

- ULIDs
- at least one locator per host
- additional locators?
- context tag? -> demux
- Security information
    - cookie/key/hash chain anchor to require on path presence to the peer
        - can be used for following messages
    - additional security info to prevent future (time-shifted) attacks

M6 host-pair context establishment

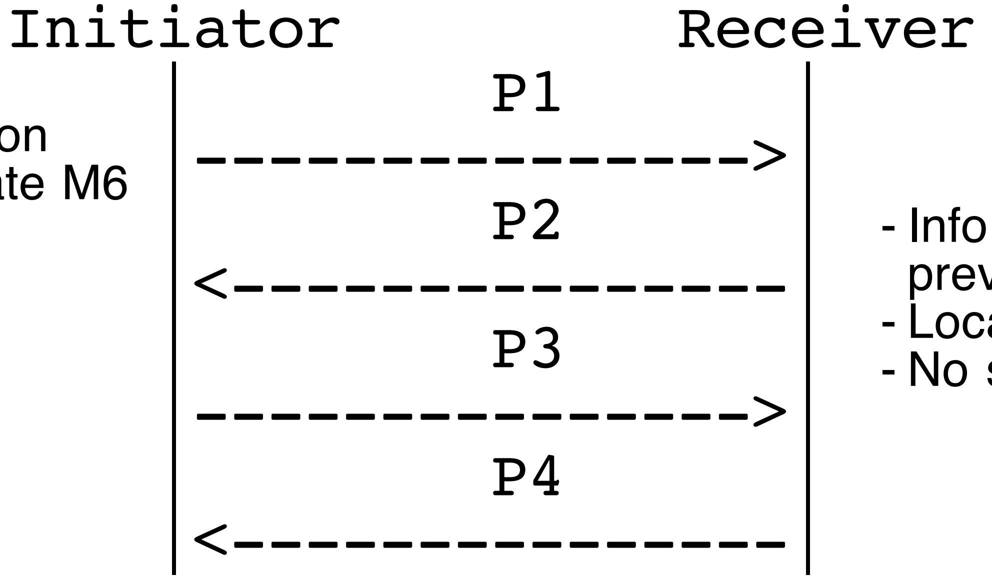
- DoS protection
  - Memory exhaustion (state)
  - CPU exhaustion (?)
  - the receiver should not create state before the initiator
  - => 4 way handshake

M6 host-pair context establishment exchange



```
Initiator           Receiver
    |        P1        |
    |----------------->|
    |        P2        |
    |<-----------------|
    |        P3        |
    |----------------->|
    |        P4        |
    |<-----------------|
```

M6 host-pair context establishment exchange



Initiator

Receiver

P1

P2

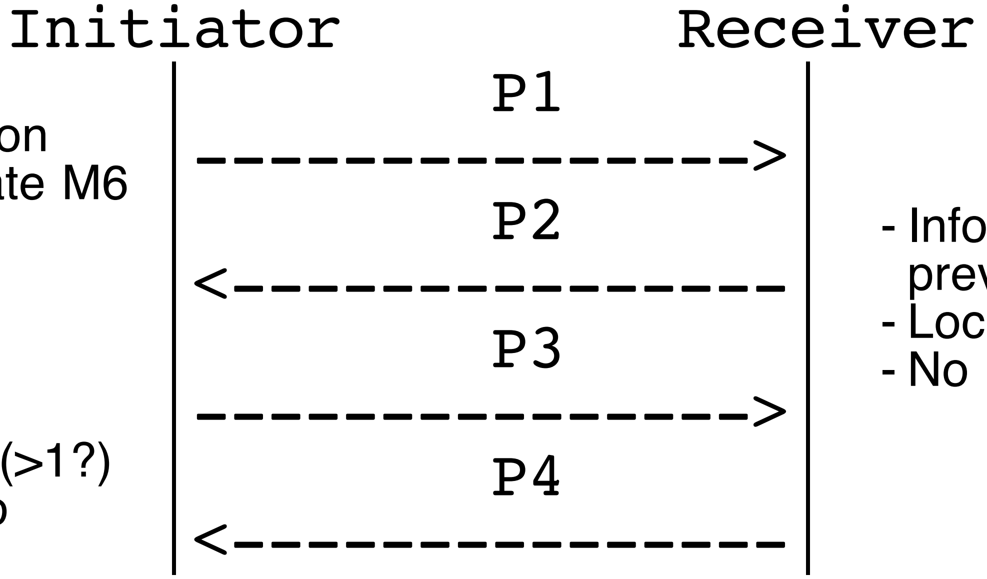
P3

P4

- Cap detection
- Req to initiate M6

- Info I to prove previous contact P3
- Locator set?
- No state created

M6 host-pair context establishment exchange



Initiator

Receiver

P1 ------------------->

P2 <-------------------

P3 ------------------->

P4 <-------------------

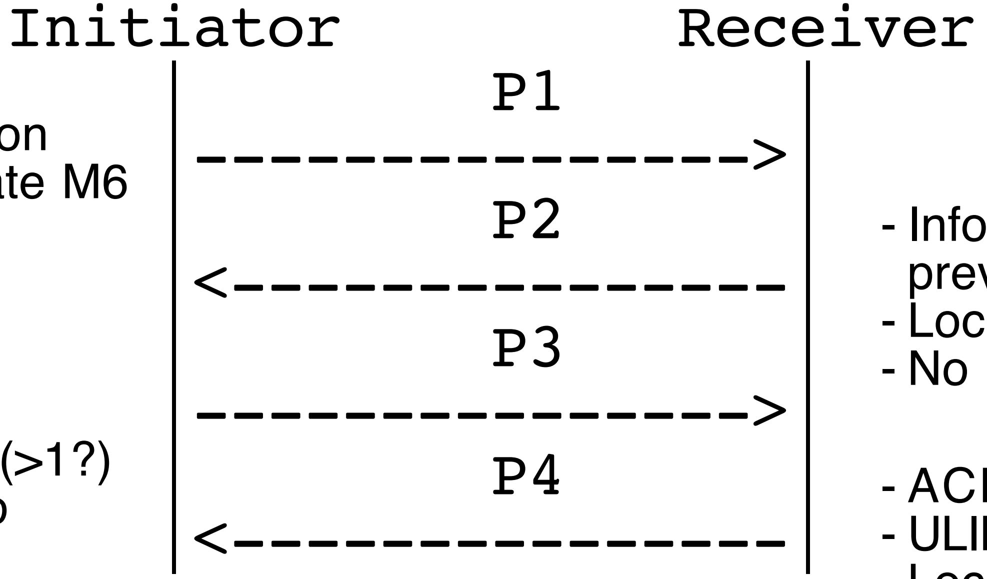
- Cap detection
- Req to initiate M6

- Info I
- ULIDs
- Locator set (>1?)

+ Security info
    - locator
    - cookie/key/hc

- Info I to prove previous contact P3
- Locator set?
- No state created

M6 host-pair context establishment exchange



Initiator Receiver

P1 ------------------>

P2 <------------------

P3 ------------------>

P4 <------------------

- Cap detection
- Req to initiate M6

- Info I to prove previous contact P3
- Locator set?
- No state created

- Info I
- ULID
- Locator set (>1?)

+ Security info
  - locator
  - cookie/key/hc

- ACK
- ULID
- Locator set (>1?)

+ Security info
  - locator
  - cookie/key/hc

Locator set management

- adding new locators
- removing existing locators
  - local reasons such as deprecated address (RADV)
- Possible approaches
  - incremental - add/rm/ack
  - atomic - loc set/ack

Locator set management security

- Adding locators
  - time-shifted attack protection
  - Not enough with cookie/key exchanged in context establishment
- Removing locators
  - May be enough with cookie/key exchanged in context establishment

Rehoming

- new locator pair used for the communication
- rehoming steps
  - detecting failure
  - exploring alternative locator pairs
  - re-homing to reachable locator pair
- Verification of reachability (current and prospective pairs)
  - Reachability test exchange
  - Not trivial when unidirectional paths (see Jari's presentation for the complex stuff)

Removal of M6 session state

- Unilateral
  - no packet exchange required
  - non-existent context error msg may be needed
  - Potential security issues?
- Coordinated
  - Close/Close_Ack for each (NOID)
- Security
  - Initial cookie/key/hca
  - error msg?