A Filter Rule Mechanism for Multi-access Mobility

draft-larsson-monami6-filter-rules-01.txt

Conny Larsson

Henrik Levkowetz

Tero Kauppinen

Heikki Mahkonen

(heikki.mahkonen@ericsson.com)

Problem Overview

About Policy:

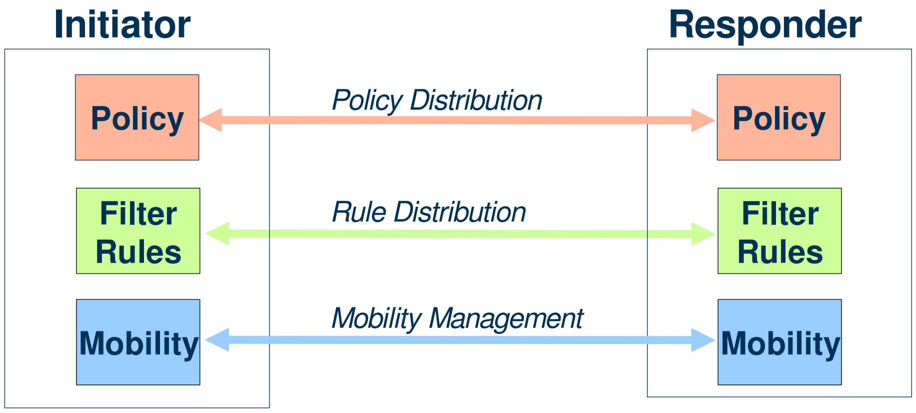
- Policies can be defined by both the initiator and responder.
- Policies are described in an abstract high level "language" and influence for instance which interface to use given the current state of the node.
- Policies could either be pre-installed in the node or distributed dynamically in runtime.
- Policies are generally asymmetric, i.e. two communicating nodes do not need to have the same set of policies.

Filter Rules:

- Filer rules can be defined by both the initiator and responder.
- Filter rules could either be pre-installed in the node or distributed dynamically in runtime.
- Filter rules are typically created when an event occurs, e.g. at the launch of applications.
- Filter rules may be useful not only for MIPv6 (Monami6) but also for MIPv4, HIP and possibly SHIM6 and other protocols.

Mobility Management:

- Mobility Management signaling is used to bind and rebind filter rules to the recipient entity (i.e. care-of address) in the stack.
- Used when the available access types are changed in a node.



Scope for draft-larsson-monami6-filter-rules:

- Defines a filter rule transfer mechanism.
- Defines a Filter Interface Identifier (FIID)

Filter Rule Transfer Mechanism

- A filter consists of a set of filter rules
- Filter rules:
  - Each filter rule is associated with a Filter Interface Identifier (FIID).
  - The filter rule definition language is OpenBSD’s Packet Filter.
  - A filter rule operates on individual packets, and is used to capture the notion of generalized flows.
  - Filter rules may be defined by both the mobile node and the network side.
  - Filter rules could either be static (i.e. preconfigured) or dynamically defined, e.g. when an application opens a socket.
  - Applications can dynamically define filter rules for a specific traffic flow.
  - The set of filter rules should exist on both sides.

Filter Rule Transfer Mechanism

Packet Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Length             |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option Type  |    Status     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       PF Payload  .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- The protocol used to distribute the filter rules is UDP
- The filter rules are stored in ASCII text format (PF Payload)
- The transfer mechanism is bi-directional
  - i.e. both involved nodes are able to modify the filter rules
- PF Update includes the entire packet filter specification
  - Optimizations possible but not defined in current version.
- Two messages are defined:
  - Packet Filter Update
  - Packet Filter Acknowledgement

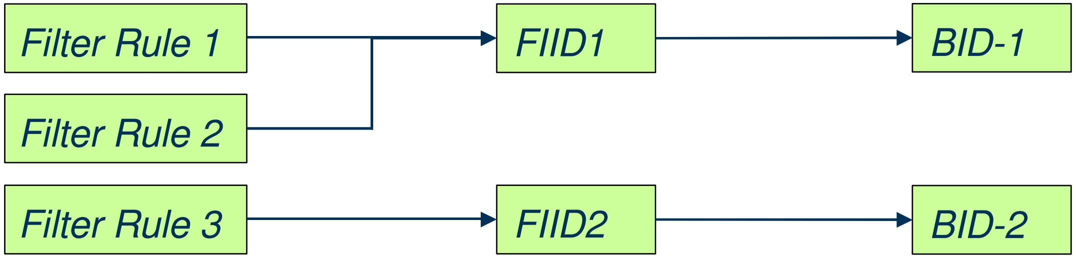
Filter Rule Transfer Mechanism

Two levels of indirection when mapping FIID to BID

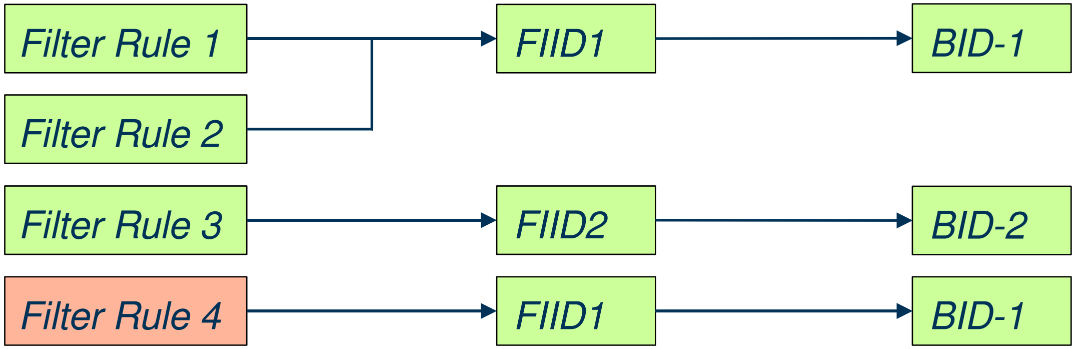
Updates to the filter rules are independent of the binding between FIID and BID

Example 1: New filter rule created, e.g. when an application opens a socket.

Existing set of filter rules:



Event causing a new filter rule to be created:



A modified set of filter rules must be sent to the filtering peer, however, no binding information needs to be updated.

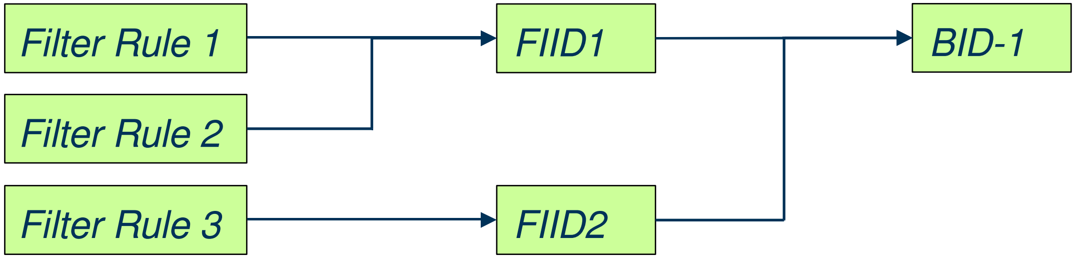
Filter Rule Transfer Mechanism

Two levels of indirection when mapping FIID to BID

Updates to the filter rules are independent of the binding between FIID and BID

Example 2: A new physical interface is added.

Existing interfaces:



Filter Rule 1

Filter Rule 2

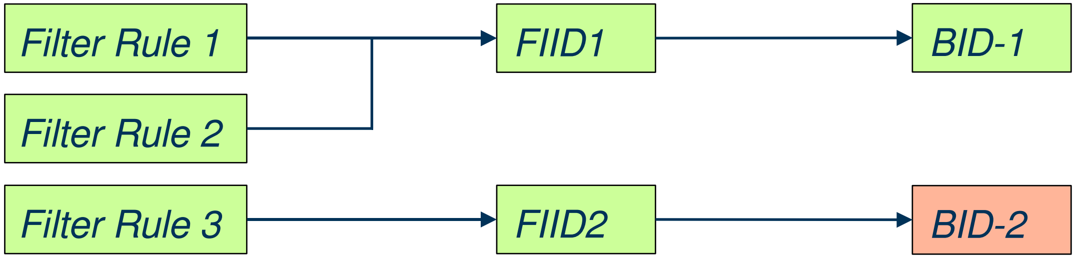
Filter Rule 3

FIID1

FIID2

BID-1

A new interface is activated:



Filter Rule 1

Filter Rule 2

Filter Rule 3

FIID1

FIID2

BID-1

BID-2

The binding between FIID and BID must be updated, however, the set of filter rules does not have to be updated.

Filter Rule Transfer Mechanism

Summary

- Policy, filter rule and mobility management are separate issues and should be handled by separate protocols.
- The proposed protocol is independent of the mobility protocol.
  - It works equally well for MIPv6, MIPv4, HIP and other mobility protocols.
- IP version agnostic since it’s built on UDP.
- Bi-directional, e.g., in MIP either the MN or the HA may send filter rule updates.