Special usage of SPI values

o The SPIs used for PIM will be staticly configured

What if the sequence number wraps around ?

- how long does it take to wrap around ?
  1 PIM message/second ===> 136 years

- Define rollover SPIs that are used when the existing SPI's sequence number overflows.

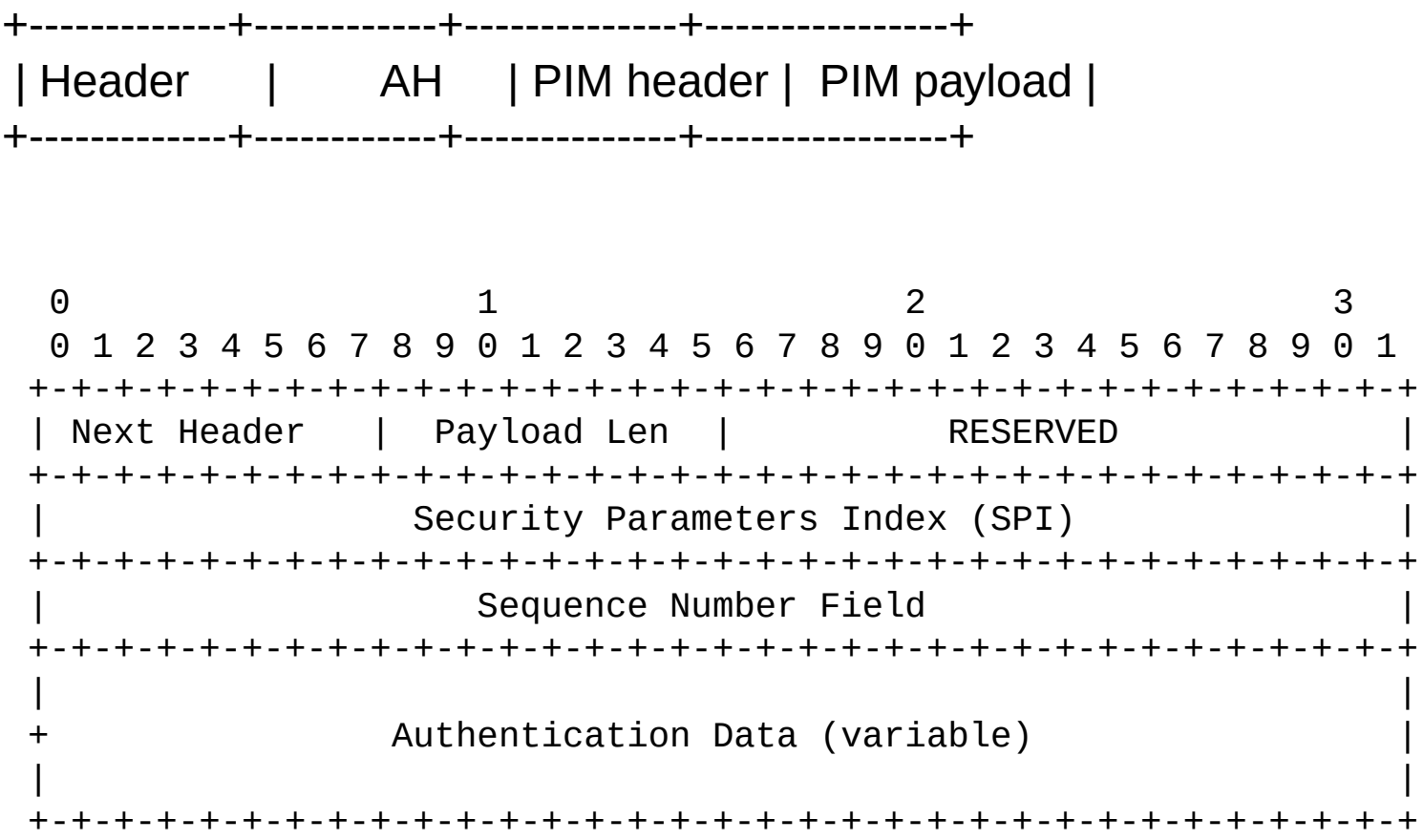
o When dynamic kep distribution mechanism becomes available, the SPIs can be obtained through the dynamic SA setup mechanism.
No need to change the current mechanism.

Special usage of SPI values

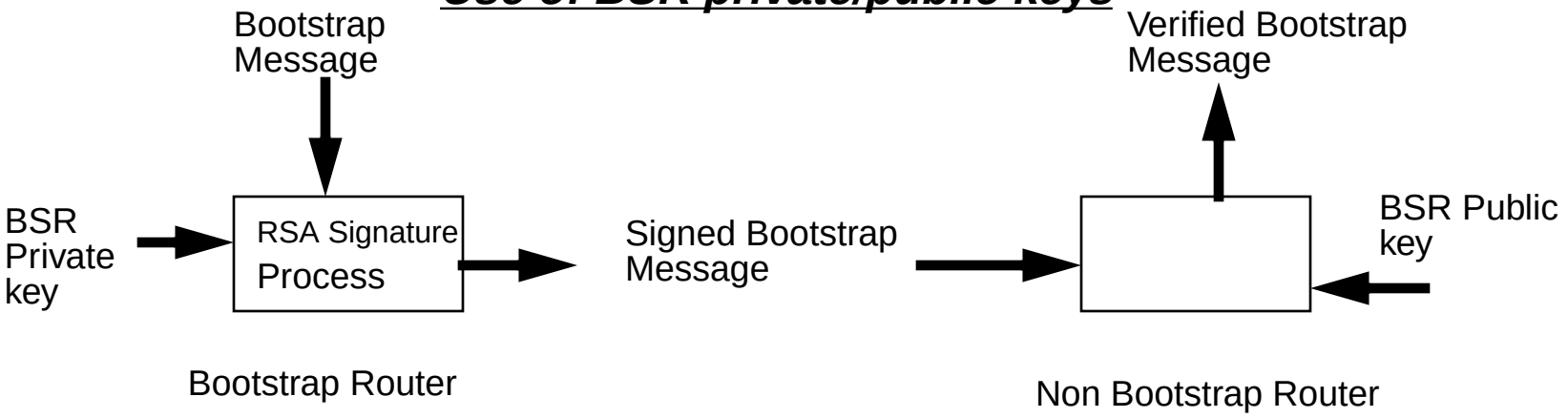
o Will ask IANA to assign three PIM specific values:

SPI: 0, not used
1, SKIP
2, equal opportunity, HMAC-MD5-96
3, Candidate RP advertisement HMAC-MD5-96
4, Bootstrap router PKCS#1 RSA signature
5 - 128, reserved with other configured keys
rest, reserved with dynamicly distributed keys

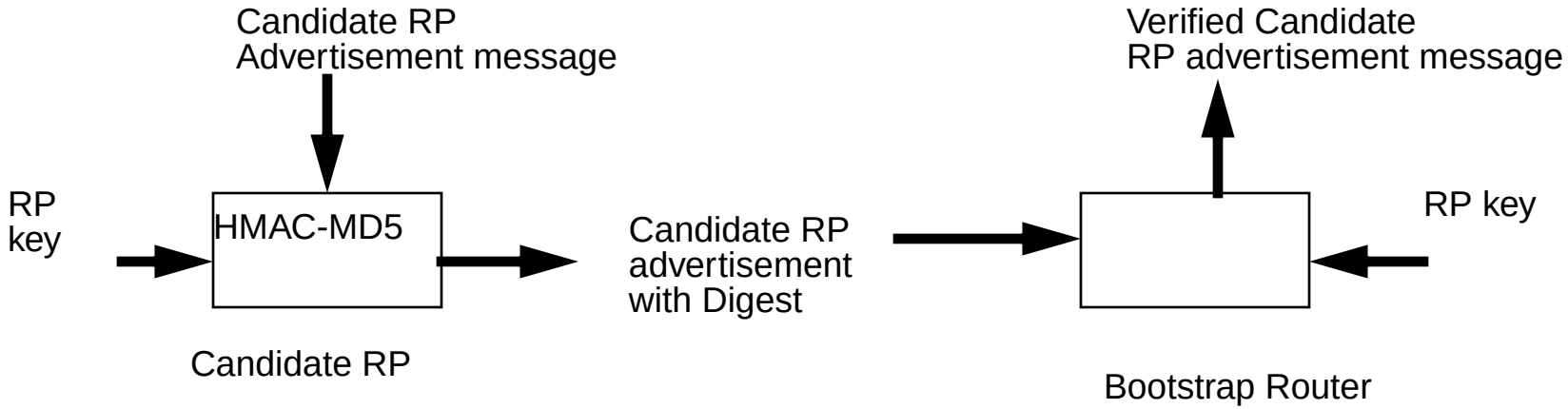
Message Format, Authentication Header from IPSEC



Use of BSR private/public keys



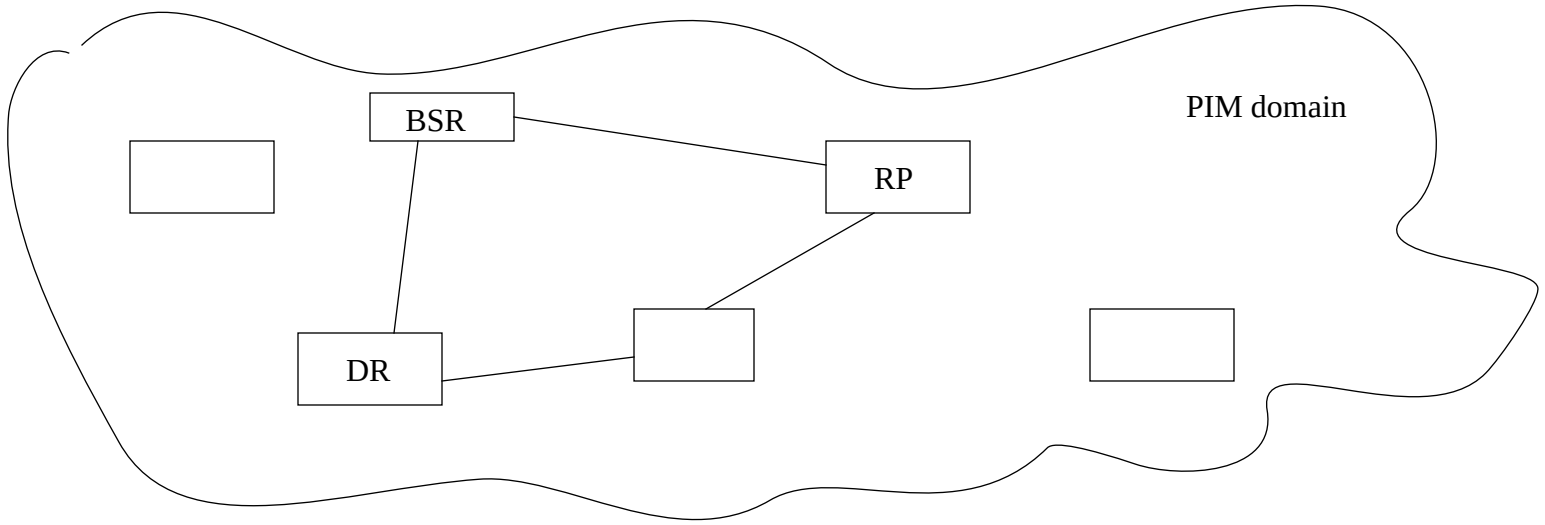
Use of RP Key



All other routers will accept the bootstrap message if the RSA signature verification process succeeds.

- "RP key"
  Candidate RPs share another MD5 key, with the candidate BSRs.

- "Equal opportunity key"



o "Differentiated capabilities" method (HMAC-MD5-96/ HMAC-SHA1-96, RSA)

- "BSR private key", "BSR public key"
  BSR signs an entire bootstrap message, and attach the signature

Authentication Methods (static keys)**:**

o “**Equal Opportunity” method** (HMAC-MD5-96, HMAC-SHA1-96 based)

All routers share the same secret to compute digests

What to protect in PIM:(continued)

- Register/Register-stop messages

  Affects a single group/router per message. No massive derivative actions

What to Protect in PIM:

o <u>"Single hop" messages</u>:

Join/prune/graft/graft-ack/assert/hello

o <u>"Multihop" messages</u>:

- Bootstrap messages
  Contains Group-to-RP mapping, used by all routers

- Candidate RP advertisement messages
  "Good" RP needed for sparse mode to function

Purposes:

o Protection from unwanted protocol behavior.

- Allow exchange of protocol messages only with authorized routers

- Detect and discard bogus messages.

o Privacy of message contents is a non-goal.

- Purpose
- What to protect, how much to protect
  - What security options to use
  - How to do it

Authenticating PIM version 2 messages

<draft-ietf-pim-v2-auth-00.txt>

Liming Wei (editor)

lwei@cisco.com

(Other contributors: Dinio Farinacci, Dave Meyer, Dan Harkins, Brian Weis, Achutha Rao, Tom Pusateri, ...)

All mistakes are assumed to be the presenter's.