Overview of draft–16 for MIPv6

MIPv6 Design Team

March 19th, 2002

Basics

- Submitted yesterday, not in I-D directories yet
- For the moment can be accessed at:

  http://www.piuha.net/~jarkko/publications/mipv6/

  draft-ietf-mobileip-ipv6-pre16.txt (I-D format)

  mipv6-modified-parts-pre16.pdf (modified parts)
- Modifications based on the security discussions and decisions
- The document is in debt to various Internet Drafts that have been issued around this subject
- Still needs some work (expect draft–17 soon)

What's new

- Now securely usable on a global scale
- Routing topology has changed
  - Due to HAO restrictions
- Message sequences have changed
  - Due to RR, the new security mechanism
- Signalling formats have changed
  - Due to desire to allow IPsec usage on MN-HA and tunneled RR signaling
- Terminology has changed
  - Mainly due to formatting modifications, options => messages, sub-options => parameters, …
- Many changed sections

Still, it looks kind of familiar…

- New messages added but old ones intact
- Messages carried by new protocol instead of DO, but format still largely the same
- Route Optimization and Bidirectional tunneling functionally intact

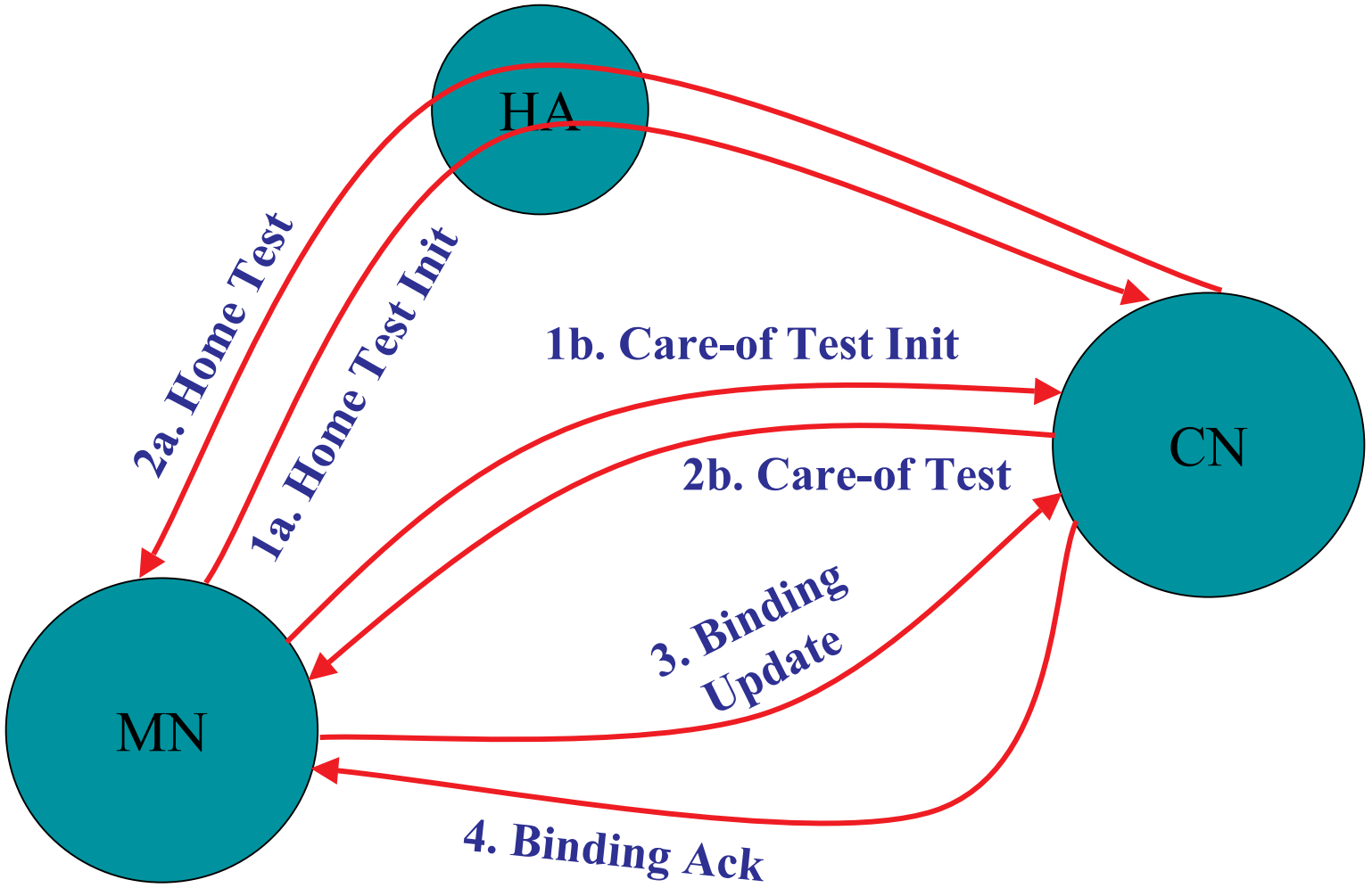
Document modifications

- 4.1. Overview
- 4.x. New protocols
- 4.4. Security Design (was authentication)
- 5.1. Mobility Header (was BU, BA, BR)
- 5.4. HAO
- 5.x. Routing Header Type 2
- 7.2. Requirements for all IPv6 Nodes
- 8. CN Behaviour
- 9.x. Protecting RR packets
- 10. MN Behaviour
- X. Future Enhancements
- 11. IANA Considerations
- 13. Security Considerations
- A.1. Modifications

Overview of functionality

- Return Routability procedure
- Home Address Option processing
- New role for Binding Request
- Message Formats

RR messaging



RR details and math

1a. HOTI: MN(HoA) -> CN: HoA
1b. COTI: MN(CoA) -> CN: CoA
2a. HOT: CN -> MN(HoA): K0, j
2b. COT: CN -> MN(CoA): K1, i
3. BU: MN(CoA) -> CN: HoA, CoA, MAC, j, i
4. BA: CN -> MN(CoA): MAC

- CN is stateless until a good BU is received
- K0 and K1 are cookies derived from a key known by CN
- BU and BA MACs are based the cookies
- The MACs are calculated over the messages
- CN is assured that BU is from someone on path

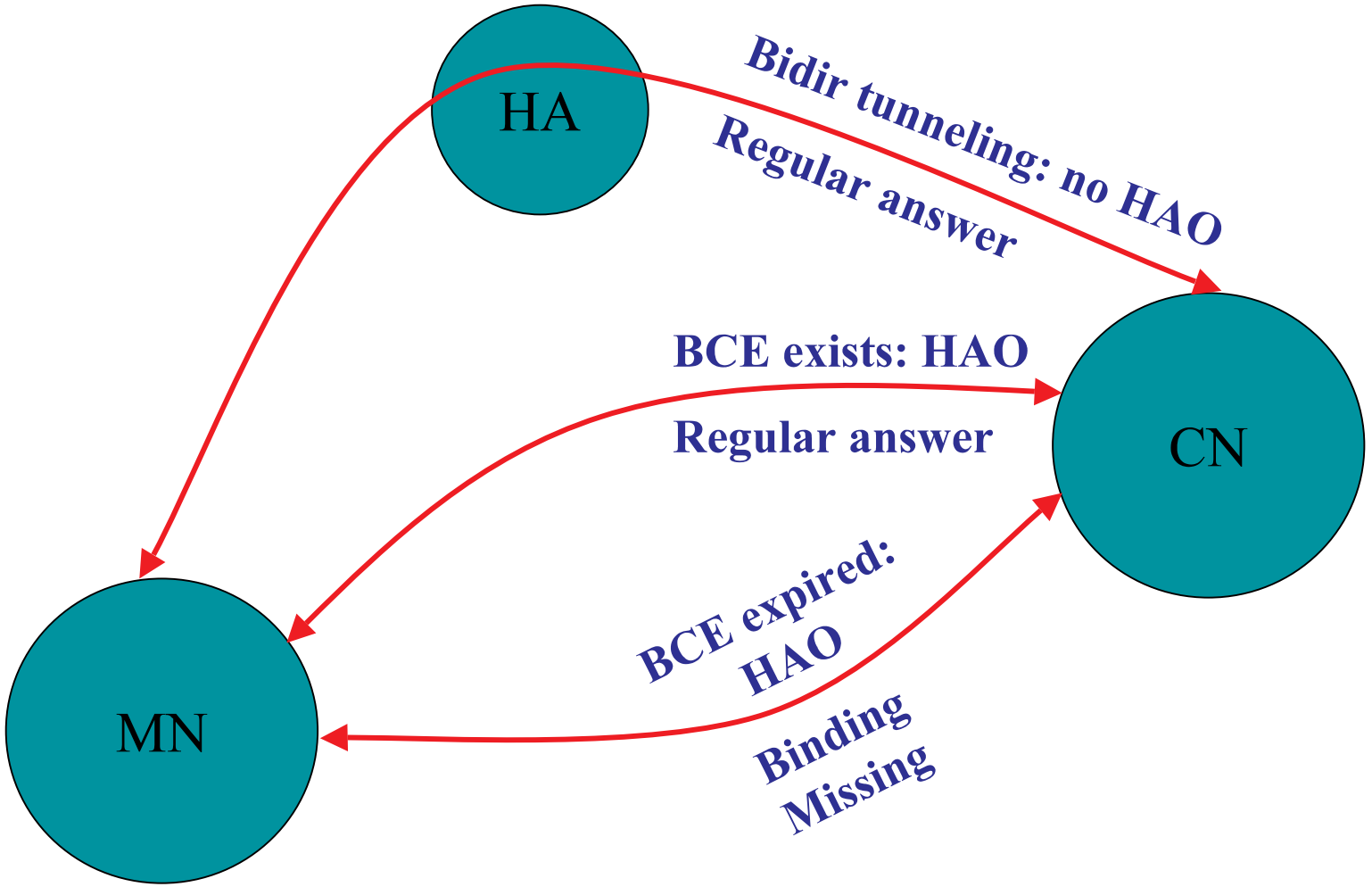
RR details and math

- with CN liveness and BM verification through COTI/COT

1a. HOTI: MN(HoA) -> CN: P0, HoA
1b. COTI: MN(CoA) -> CN: P1, CoA, [HoA]
2a. HOT: CN -> MN(HoA): K0, j, P0
2b. COT: CN -> MN(CoA): K1, i, P1, [MAC]
3. BU: MN(CoA) -> CN: P2, HoA, CoA, MAC, j, i
4. BA: CN -> MN(CoA): MAC
5. BM: CN -> MN(CoA):

- CN is stateless until a good BU is received
- K0 and K1 are cookies derived from a key known by CN
- BU and BA MACs are based the cookies
- The MACs are calculated over the messages (and P2 in step 4)
- CN is assured that BU is from someone on path

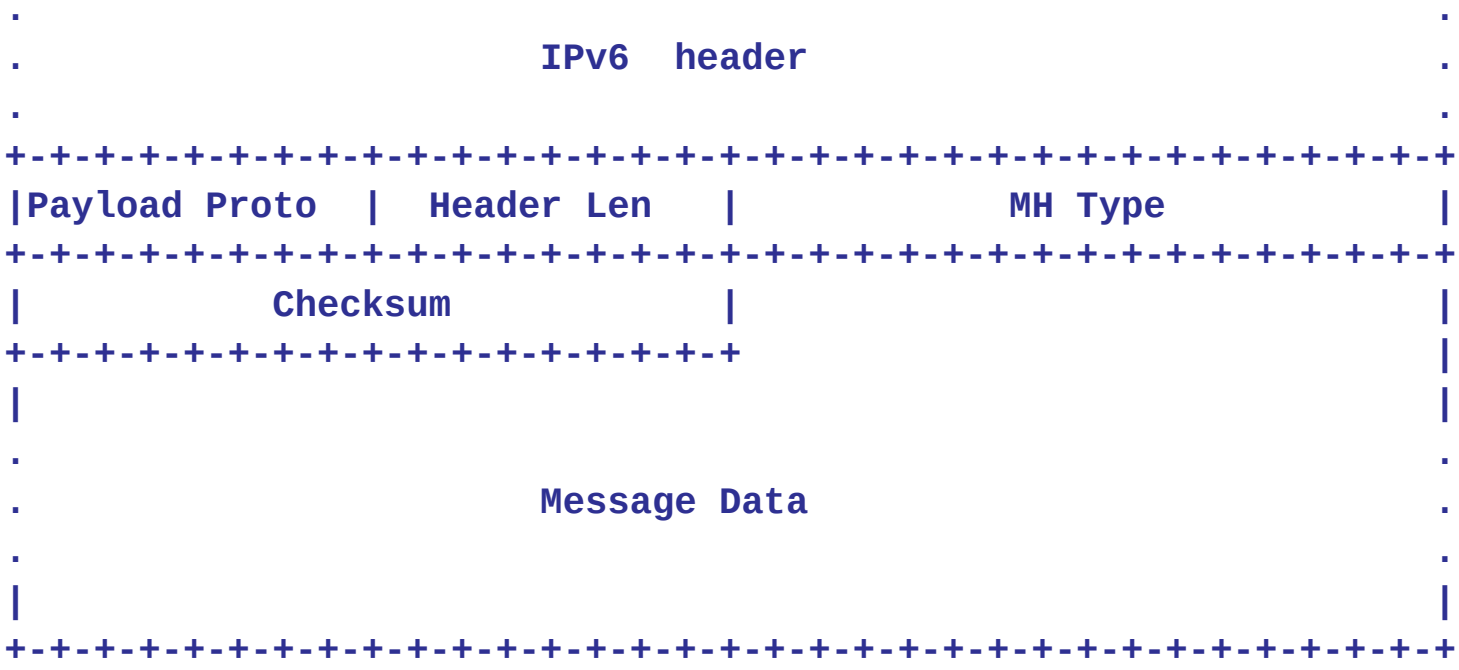
Usage of HAO
- and related messaging



New role for Binding Request

- Detection of mobile nodes may not be possible anymore for the CN!
  - Bidirectional tunneling hides the fact that the node is mobile
- Binding Request in draft-16 has become a kind of a “Binding Refresh Request”
- Responsibility for starting Route Optimisation on the MN side

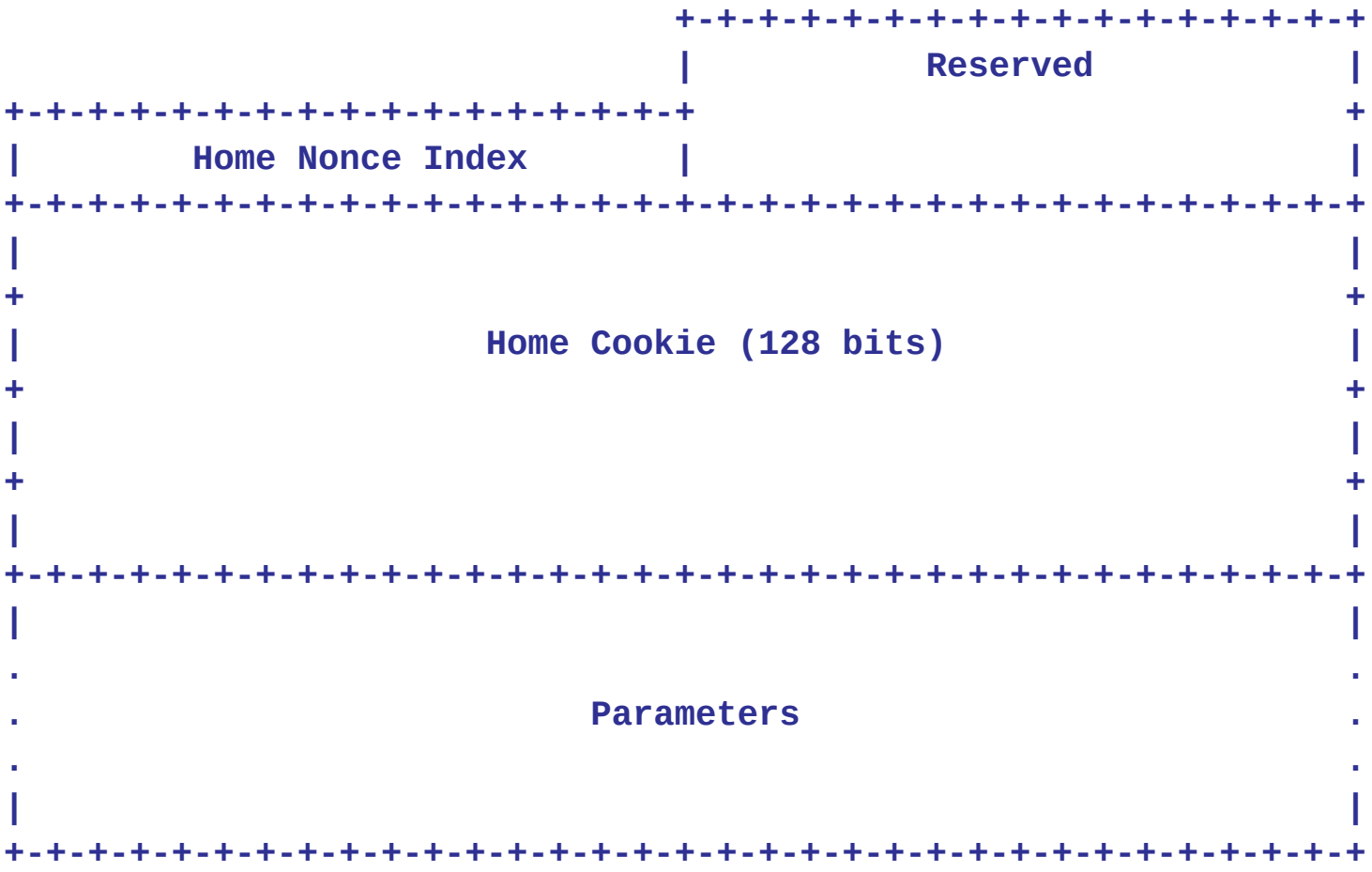
Mobility Header format



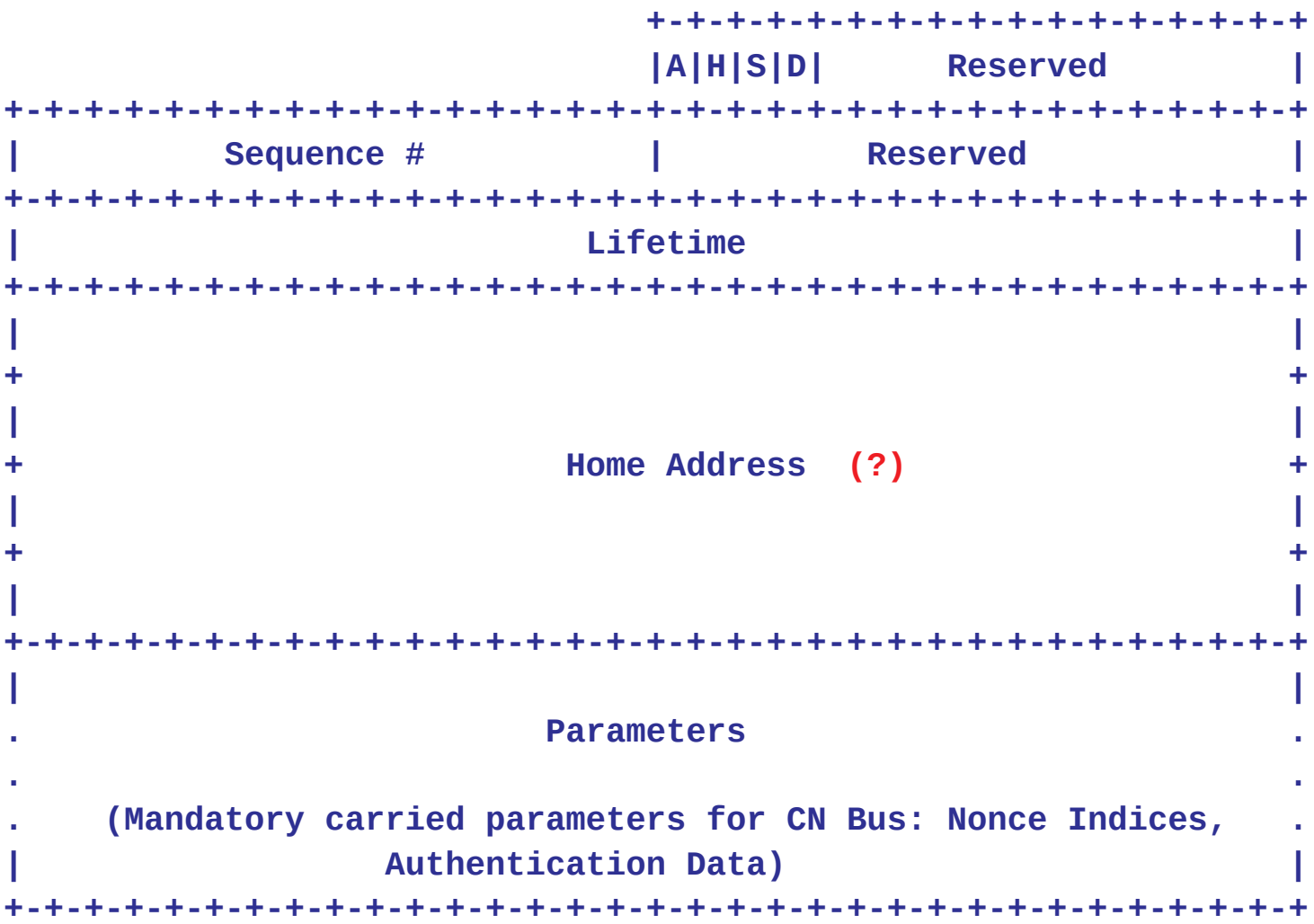
Messages carried in this format:

- **Binding Request**
- **Home Test Init, Home Test, Care-of Test Init, Care-of Test**
- **Binding Update, Binding Ack**
- **Binding Missing**

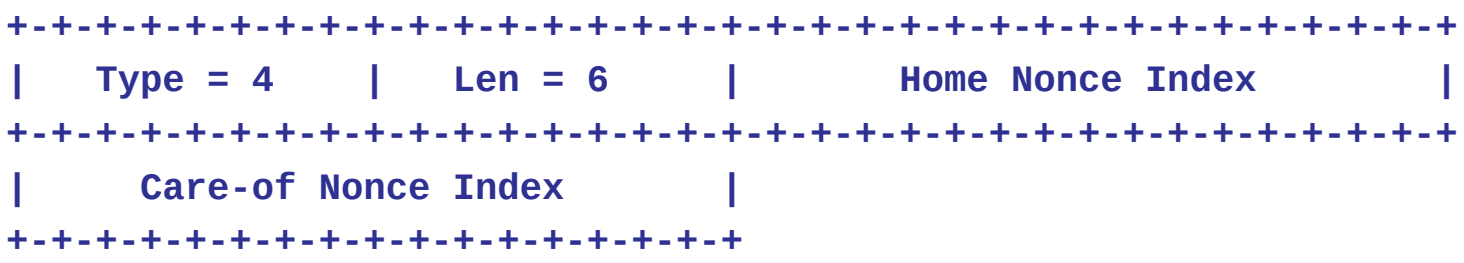
Home Test message data



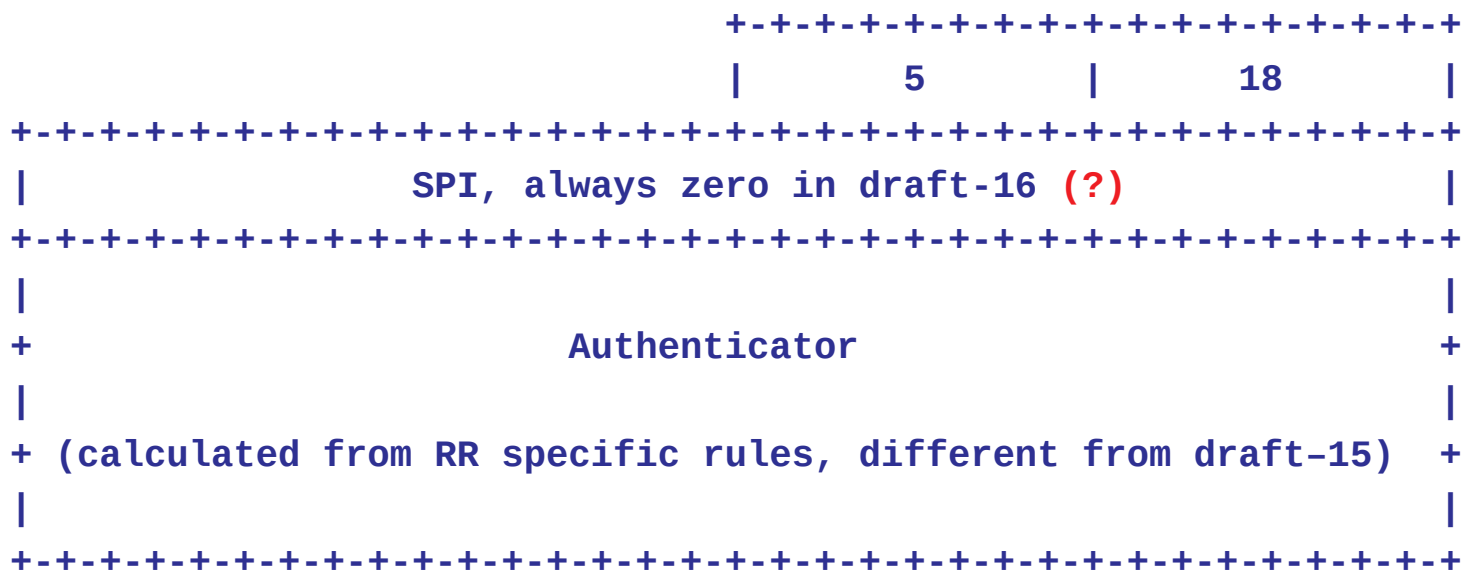
Binding Update message data



Nonce Indices parameter



Authentication Data parameter



Summary

- Main new things: RR, HAO, formats
- Questions, comments?
- Some open issues remain and will be discussed later