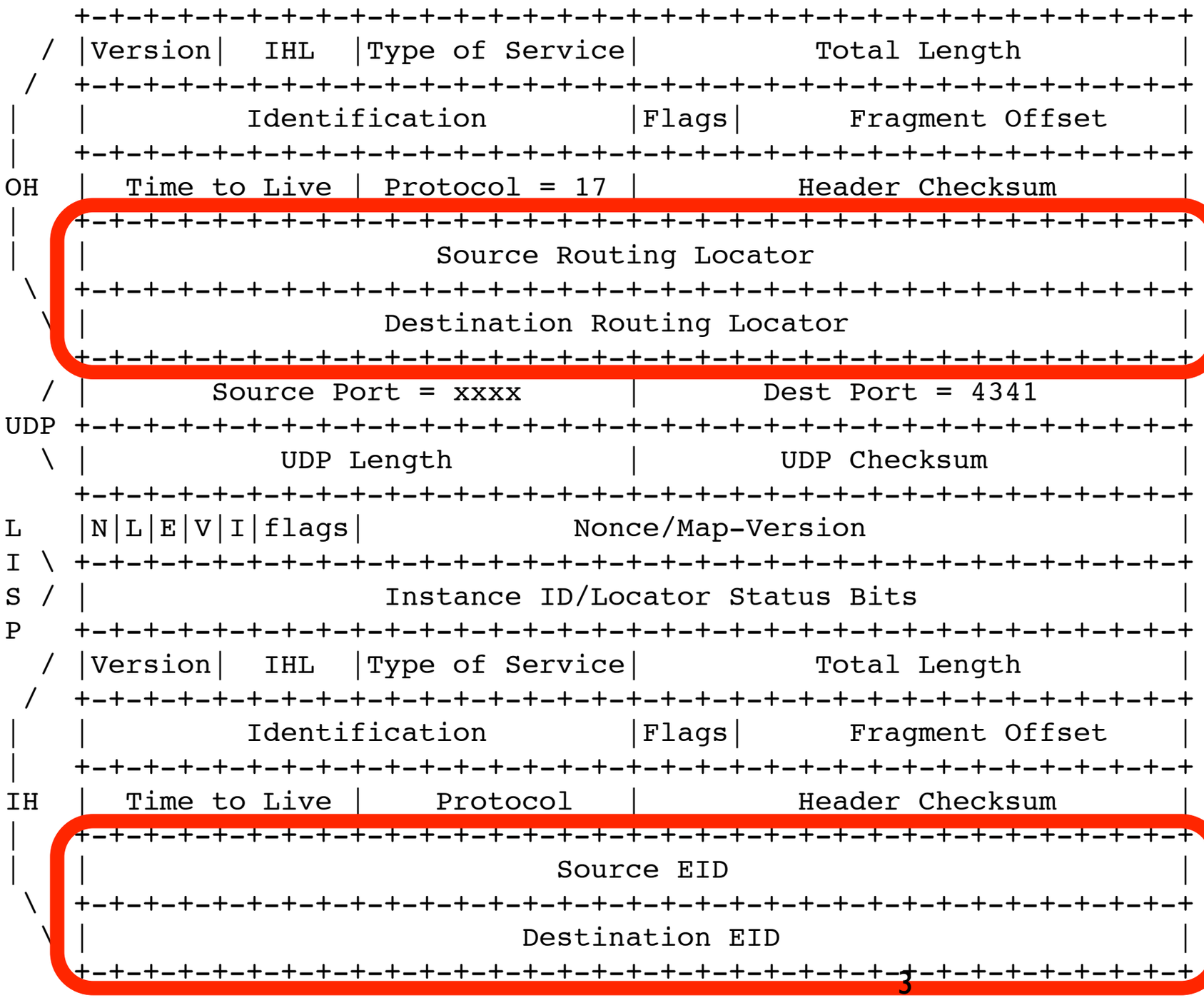
Update on
LISP Threats Analysis

~~draft-saucez-lisp-security-01.txt~~
~~draft-saucez-lisp-security-02.txt~~
~~draft-saucez-lisp-security-03.txt~~
~~draft-ietf-lisp-threats-00.txt~~
draft-ietf-lisp-threats-01.txt

Damien Saucez
Luigi Iannone
Olivier Bonaventure

Data-plane based attacks

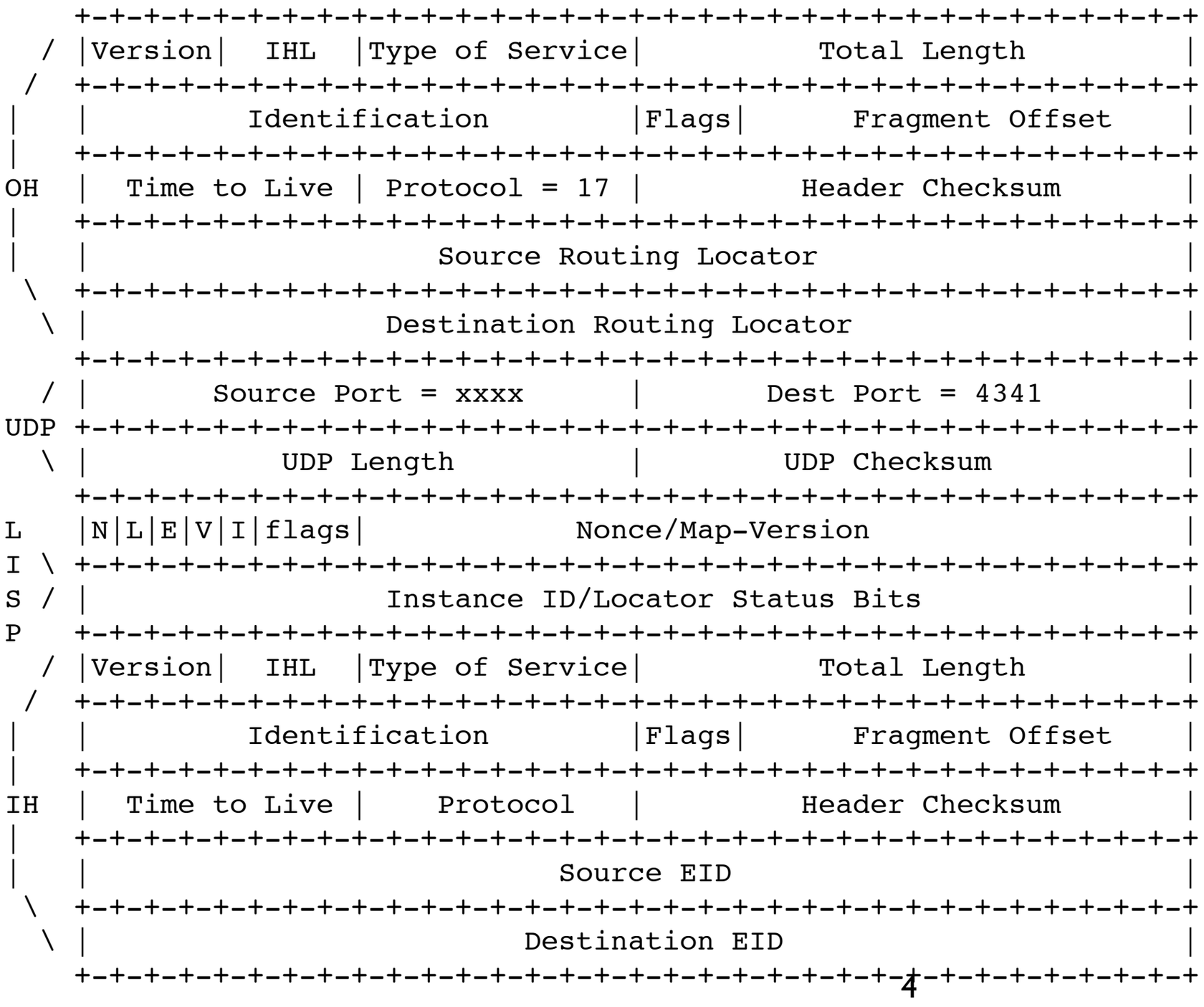
Spoofing



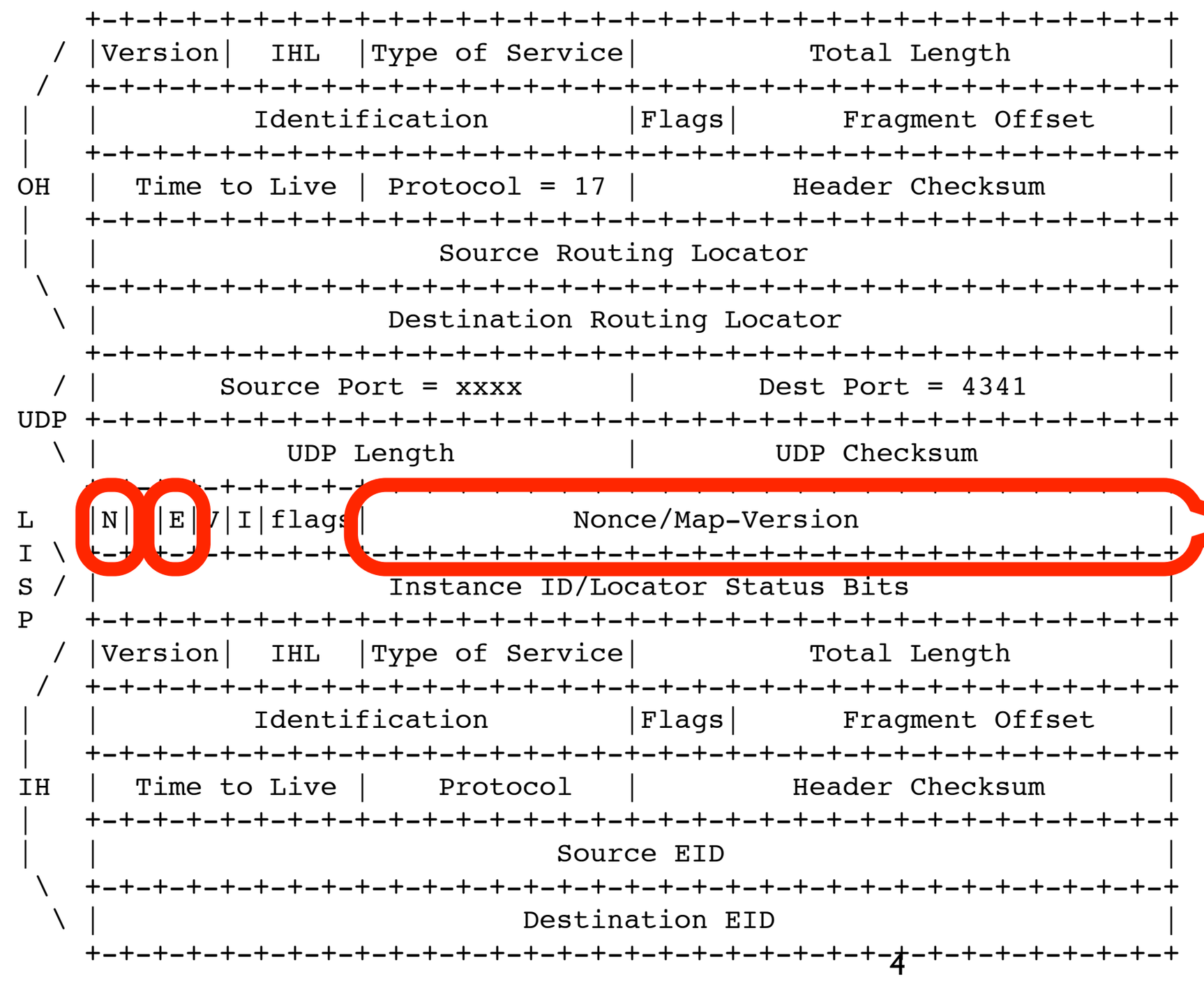
RLOC Spoofing

EID Spoofing

LISP header crafting
(potentially combined with spoofing)

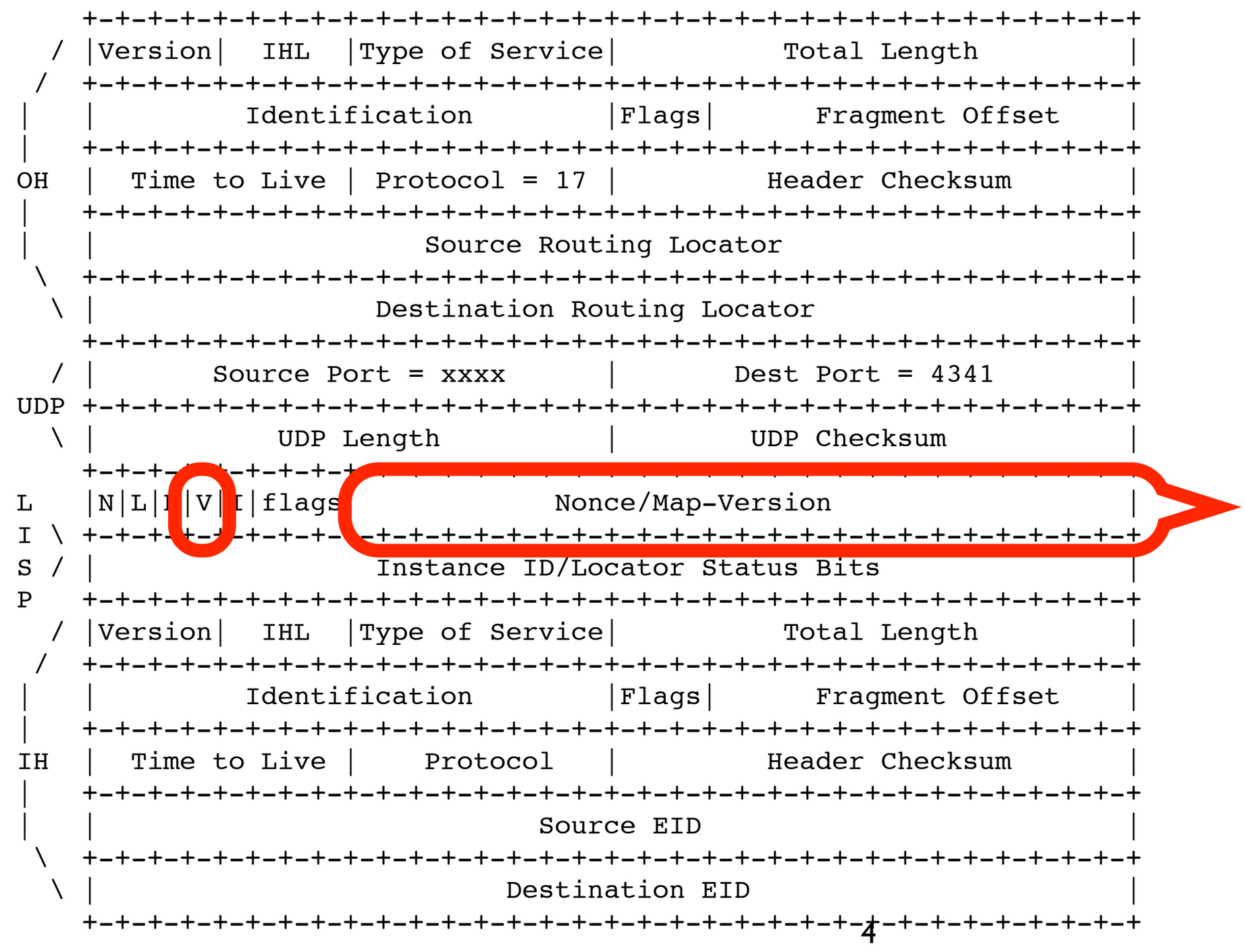


LISP header crafting
(potentially combined with spoofing)



Nonce present and/or force echo-noncing

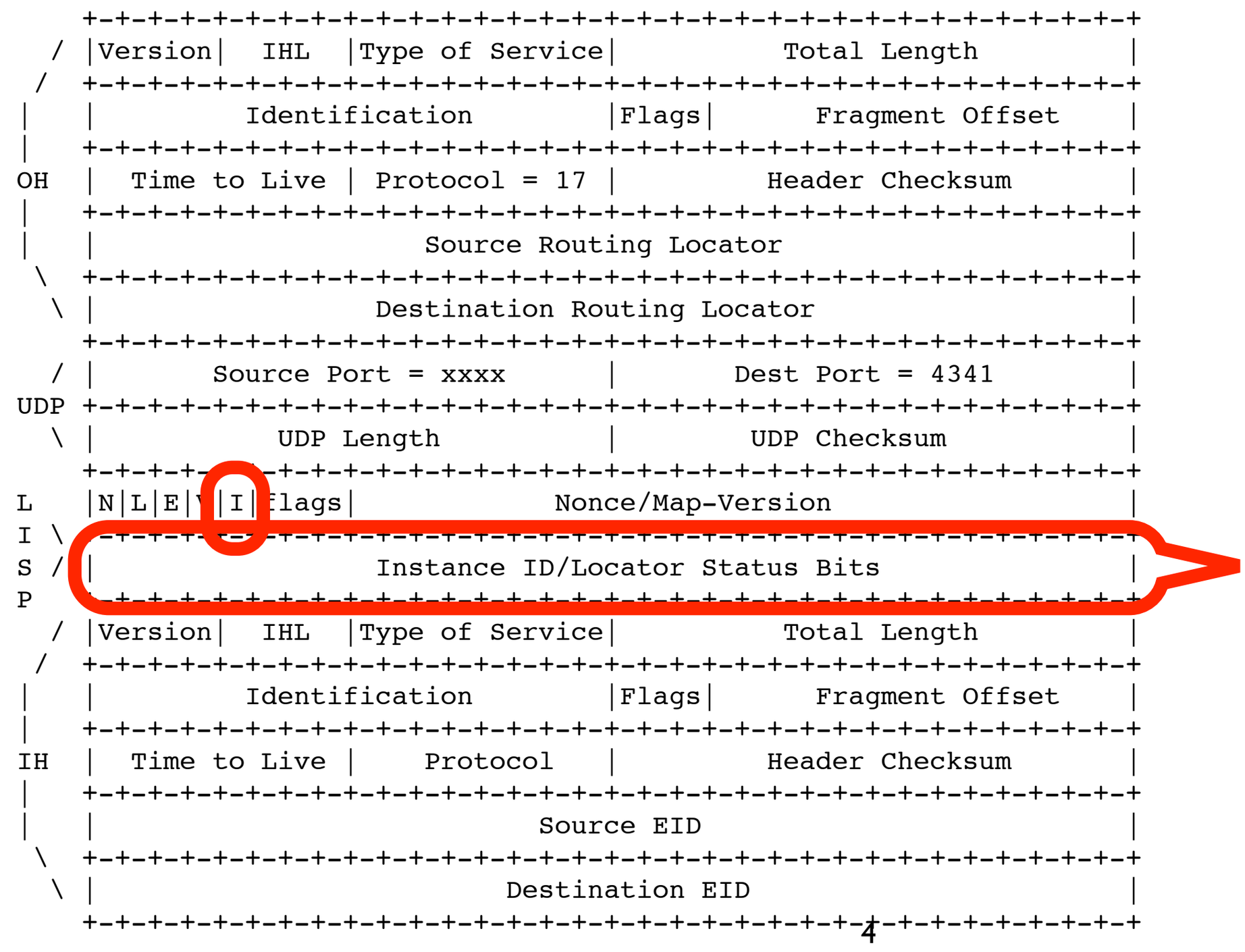
LISP header crafting
(potentially combined with spoofing)



Invalid map-version

LISP header crafting

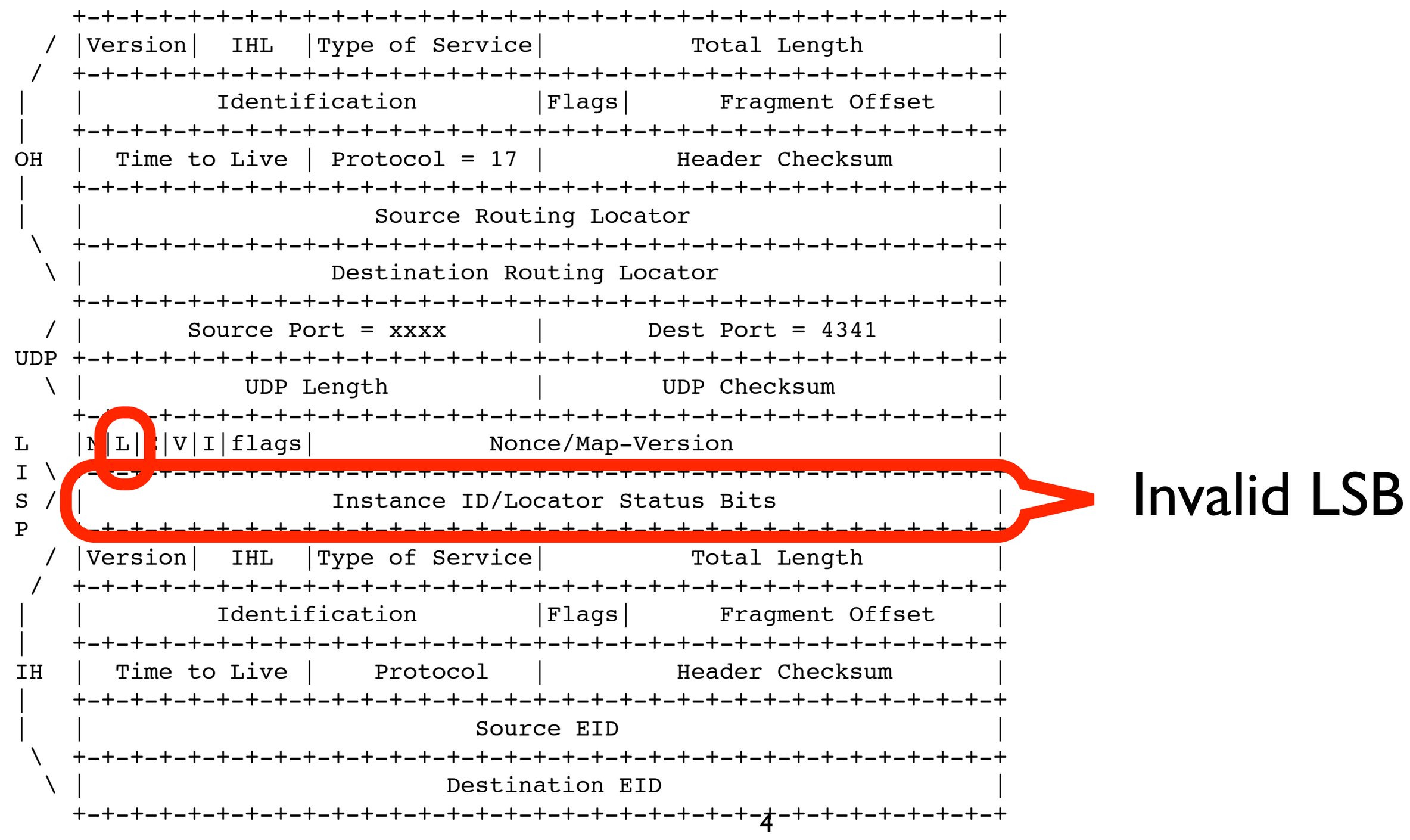
(potentially combined with spoofing)



Invalid instance ID

LISP header crafting

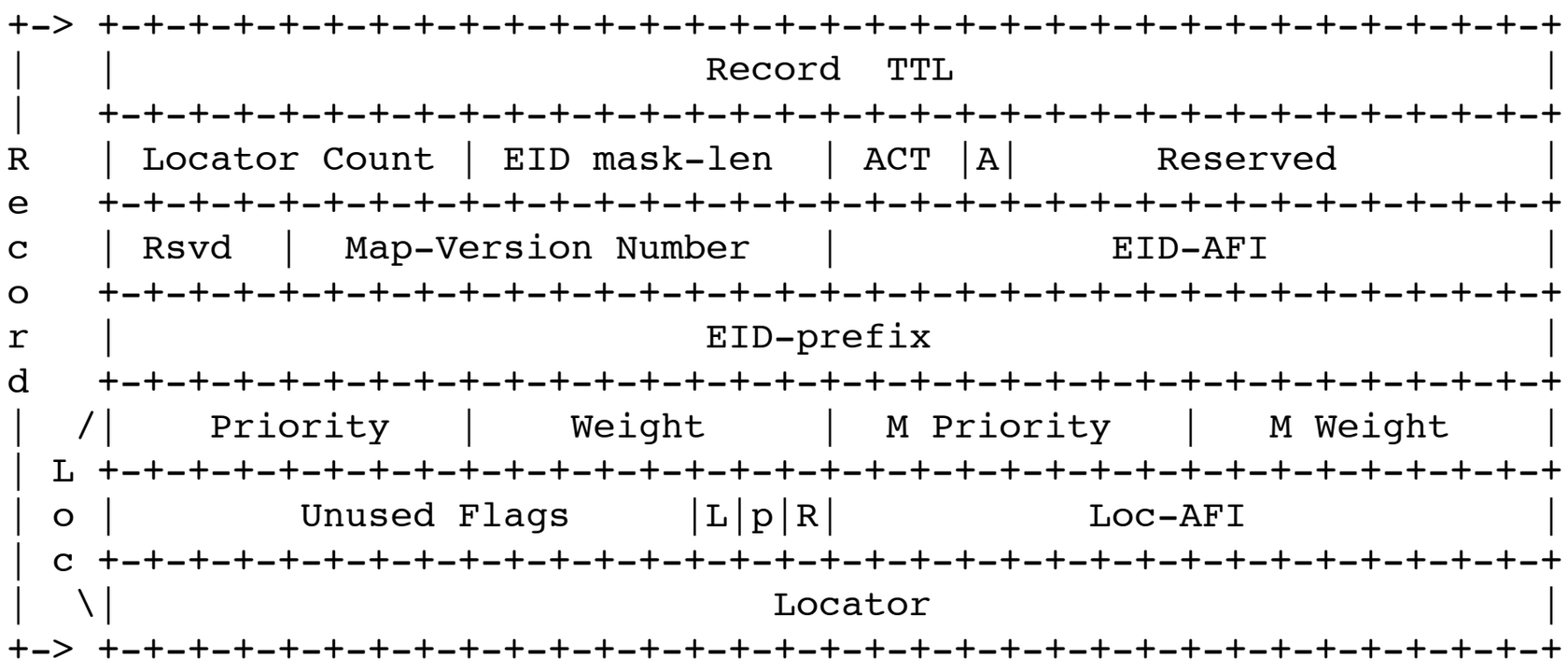
(potentially combined with spoofing)



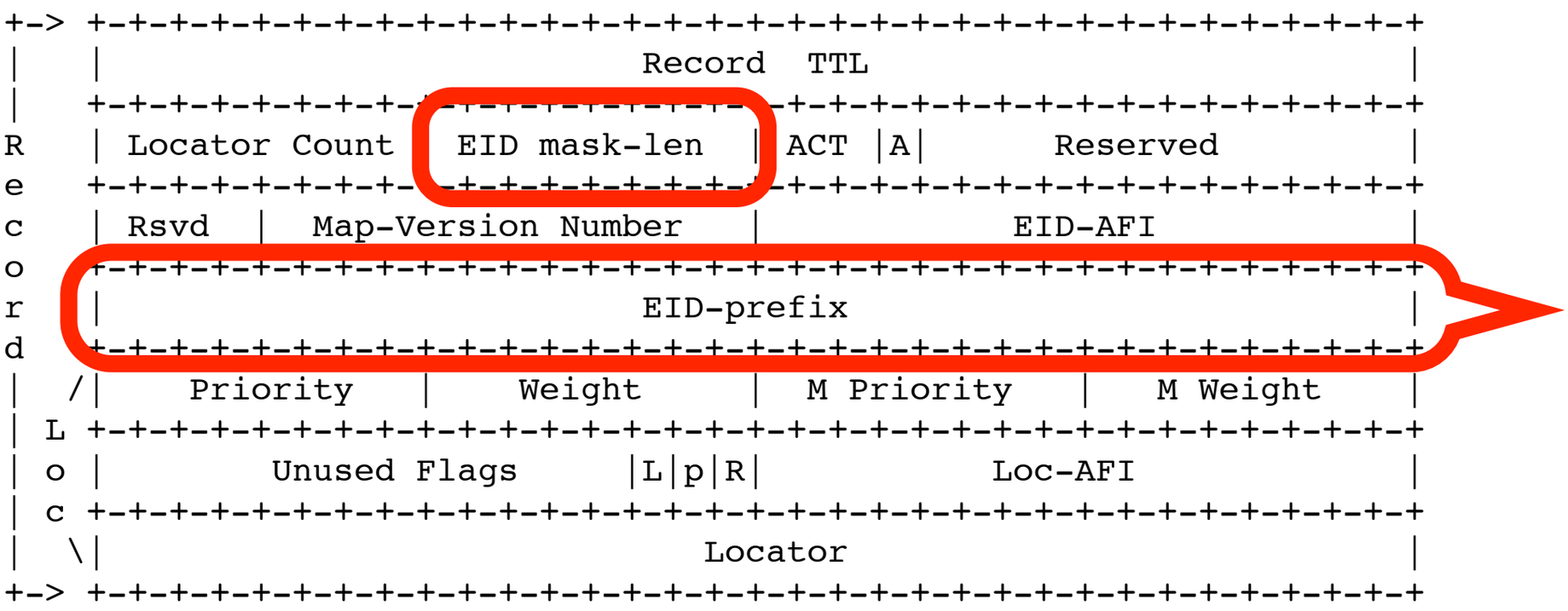
Invalid LSB

Control-plane based attacks

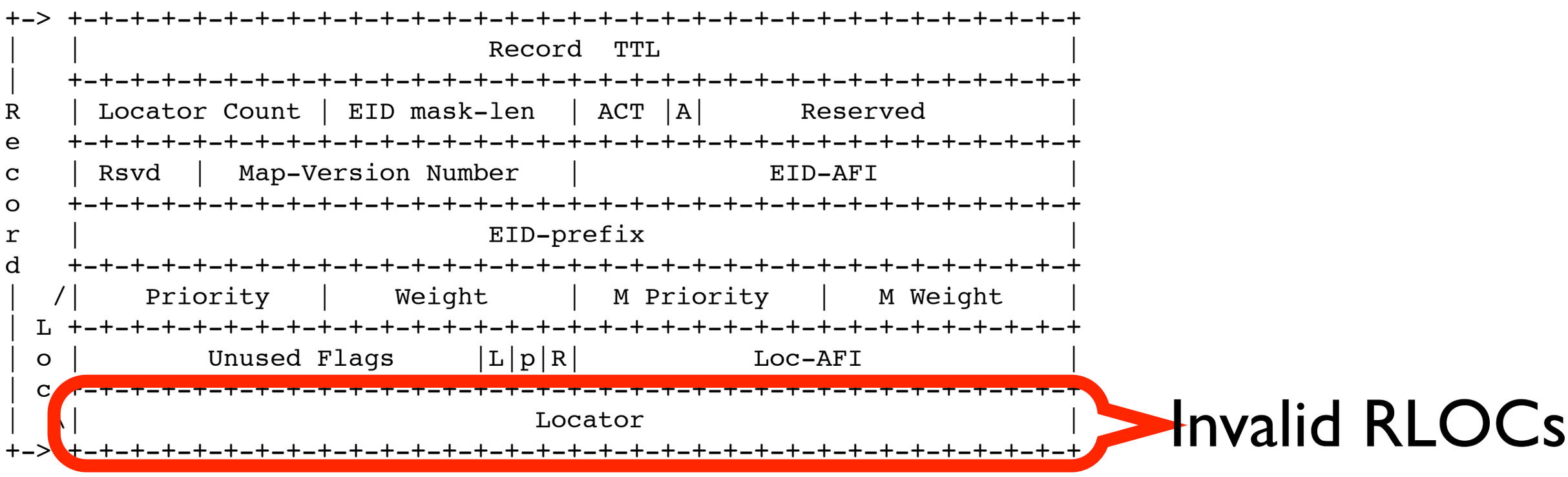
Forge the mappings



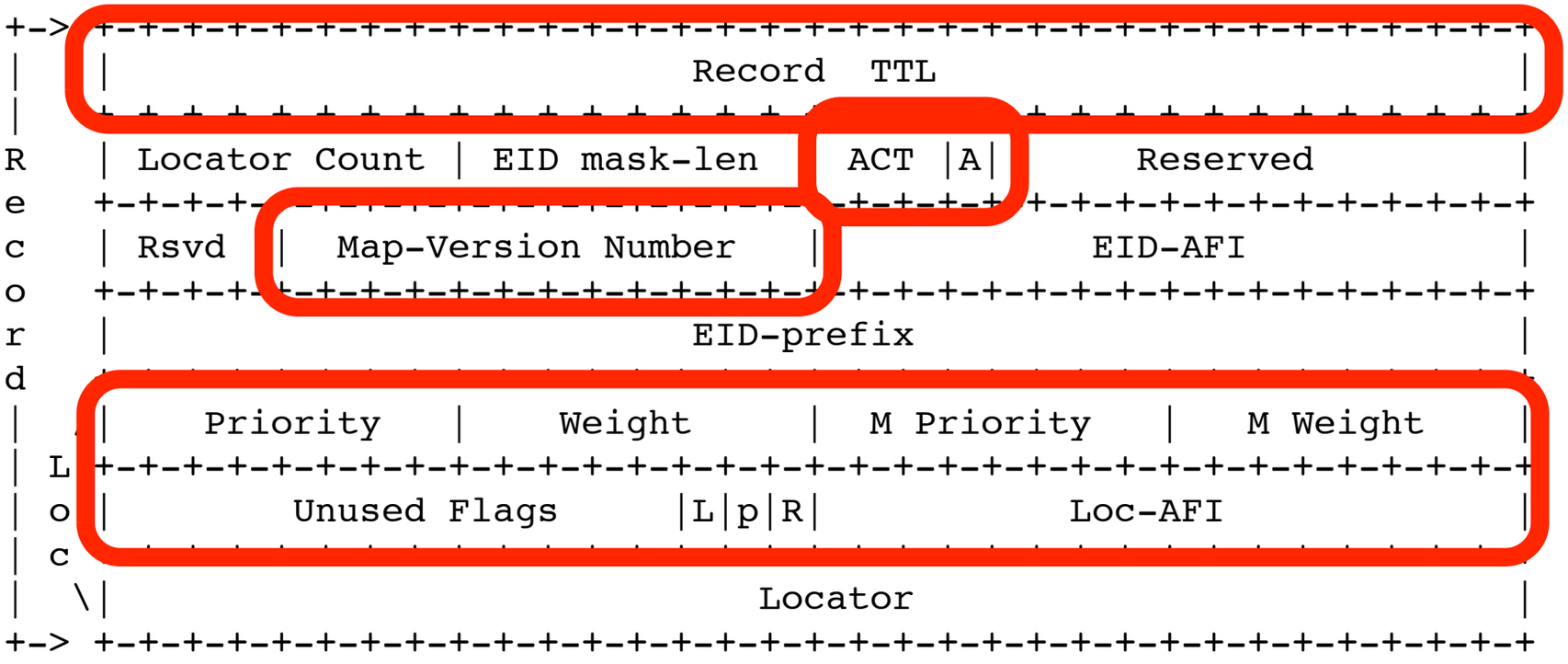
Forge the mappings



Forge the mappings



Forge the mappings



But control-plane is more than Map-Reply

- Amplification (send a Map-Request with a spoofed RLOC)
- SMR bit
- P bit
- Mappings piggybacking

Main changes

- Editorial polishing
  - typos
  - rephrasing
- Added new threat
  - Cache overflow with de-aggregation
- Added LISP-DDT
  - in conjunction with LISP+ALT
- References update

New threat

- Cache overflow with de-aggregation (remember jeff's mails)
  - an ETR attacker can force an ITR to send a Map-Request for her legitimate EIDs
  - the ETR returns either positive or negative Map-Reply
  - the reply is massively de-aggregated into a lot of artificially small EID prefixes
- Example
  - *planete-xtr* sends one ping6 packet to an EID behind *damien-xtr* with source EID 12610:D0:212D::DEAD
  - *damien-xtr* sends Map-Request for 12610:D0:212D::DEAD
  - as 12610:D0:212D::/48 belongs to *planete-xtr*, if *planete-xtr* is malicious, she can return up to 2^80 de-aggregated prefixes upon *damien-xtr* request...

LISP-DDT

- LISP Delegated Database Tree (LISP-DDT) is a DNS like mapping system... wait Vina and Darrel presentations!
  - MR iteratively sends DDT Map-Requests to DDT nodes in DDT hierarchy
  - DDT nodes reply with Map-Referrals that give pointers to her children
  - DDT MSes forward Map-Requests to registered ETRs
- The iterative behavior of the MR in LISP-DDT implies state at the MR
  - a malicious ITR can cause MR‘s memory to be overloaded by Map-Requests for a large amount of different EIDs
  - compromised LISP-DDT can provide fake referrals to control mapping delivery
- Need some minor revisions to fit draft-fuller-lisp-ddt-01.txt

Next Steps...

- We tried to document all the categories of attack against LISP, any other?
- Integrate further comments (if any)
- Is the document ready for last-call?