Using NTP Extension Fields without Authentication

draft-mizrahi-ntp-extension-field-00

Tal Mizrahi

Marvell
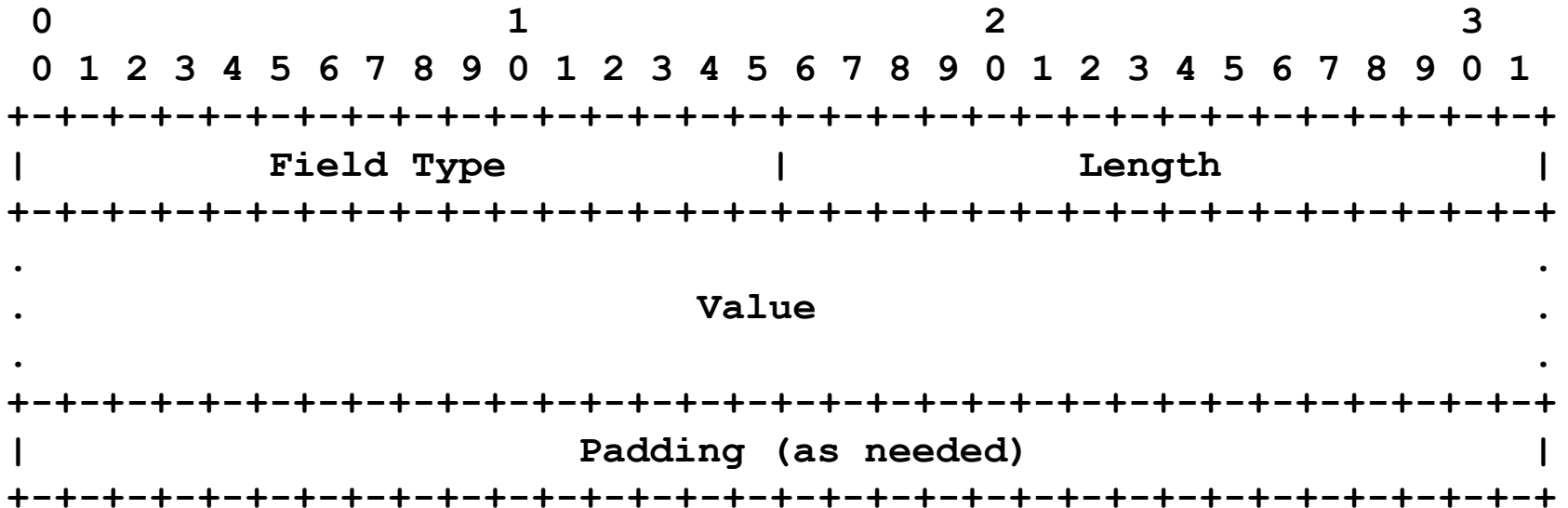
IETF Meeting 85, November 2012

Background

▶ **The NTP header includes:**
- ▪ Fixed fields.
- ▪ Optional fields.

▶ **Optional fields (NTPv4):**
- ▪ Message Authentication Code (MAC)
  - – 24 octets
  - – 20 octets
  - – 4 octets (crypto NAK)
- ▪ Extension fields

Extension Field Format (NTPv4)

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Field Type           |             Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                             Value                             .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Padding (as needed)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
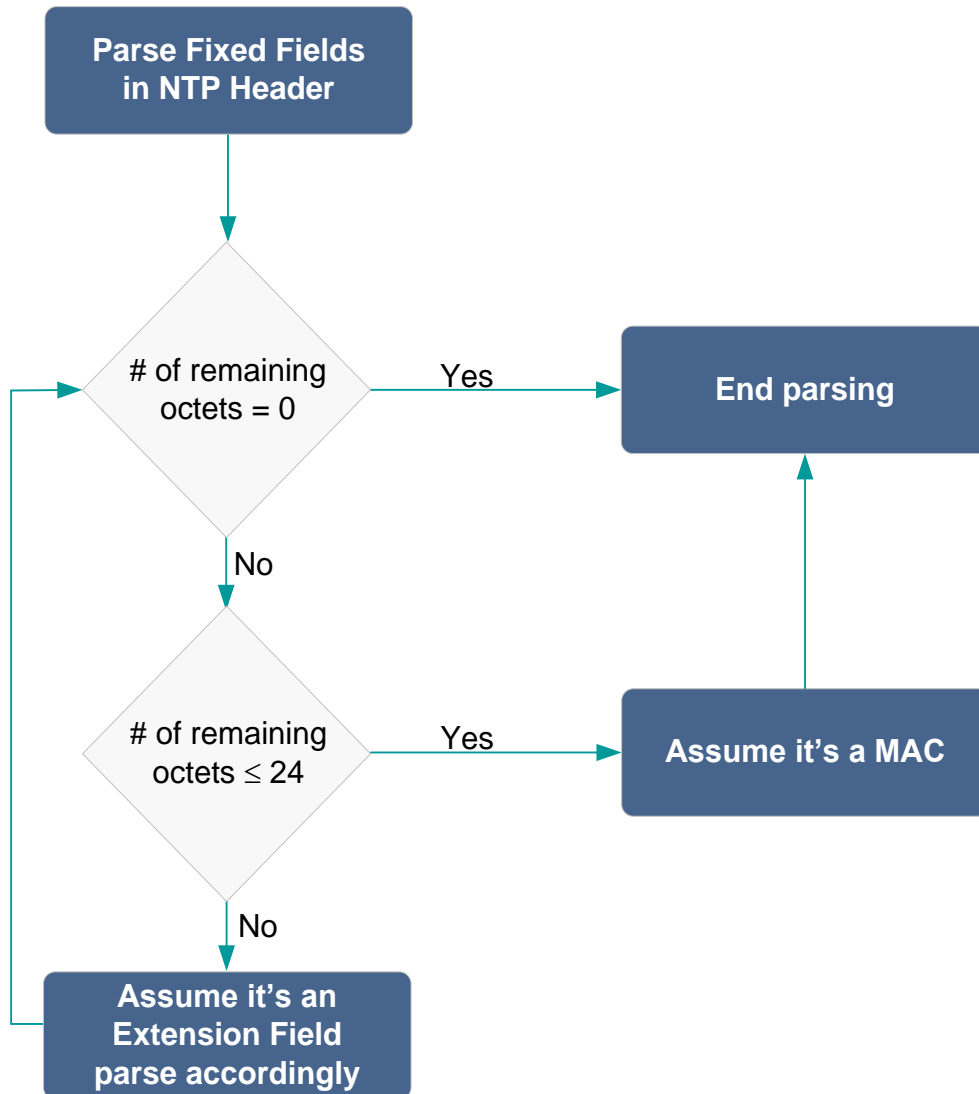
Goal of this Draft

▶ **The problem:**

- RFC 5905, 5906 imply that extension fields are <u>generic</u> tools for future features, independent of authentication.

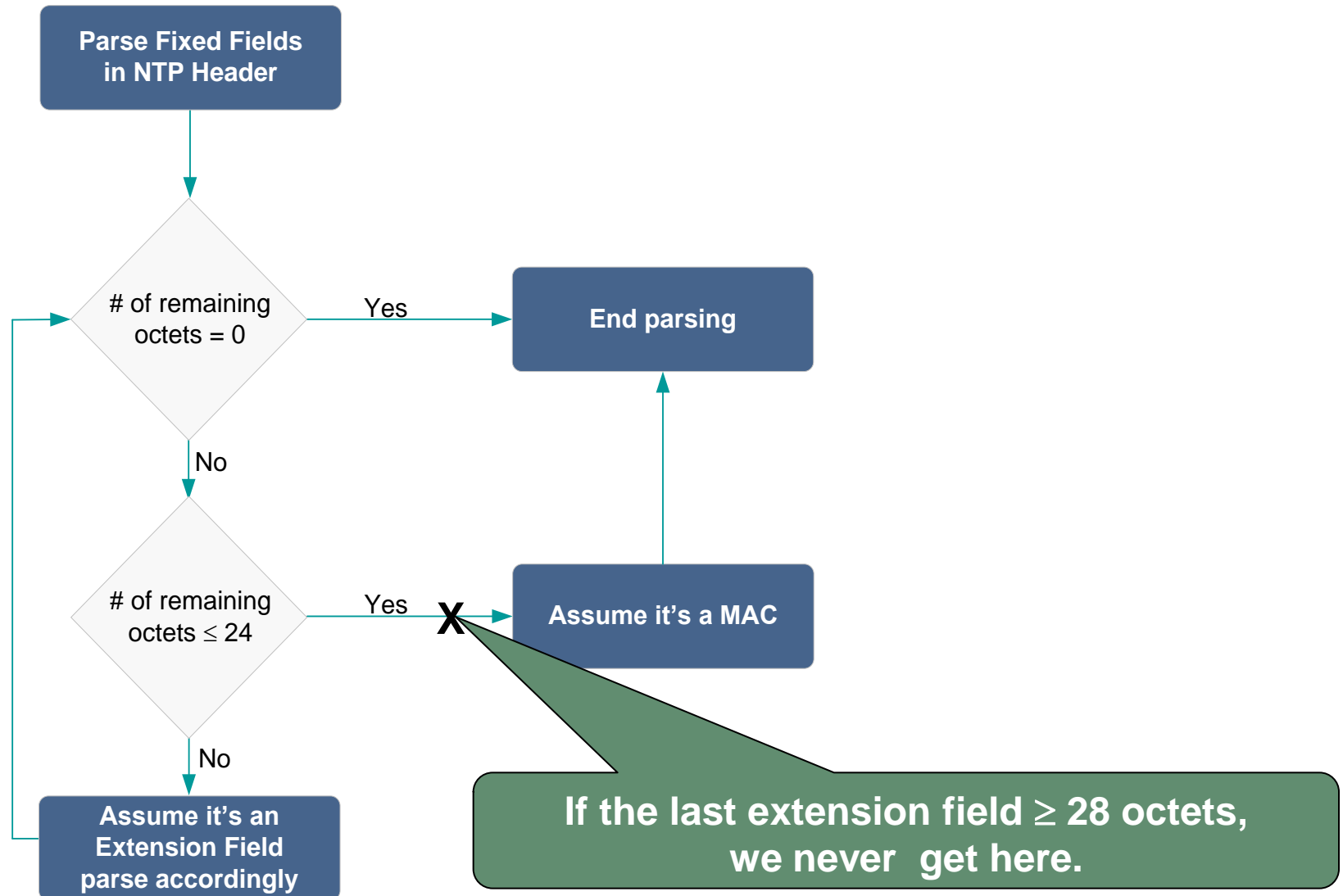- RFC 5905, 5906 imply that extension fields can only be used when a MAC is present.

▶ **Goal:**

- Clarify the ambiguity.

RFC 5906 (Autokey) – Extension Field Parsing

```
┌─────────────────────┐
│   Parse Fixed Fields│
│   in NTP Header     │
└─────────────────────┘
          │
          ▼
      ◇ # of remaining ◇  ──── Yes ────▶  ┌──────────────┐
        octets = 0                        │  End parsing  │
          │                               └──────────────┘
          No                                      ▲
          │                                       │
          ▼                                       │
      ◇ # of remaining ◇  ──── Yes ────▶  ┌──────────────────┐
        octets ≤ 24                        │ Assume it's a MAC │
          │                               └──────────────────┘
          No
          │
          ▼
┌─────────────────────┐
│   Assume it's an     │
│   Extension Field    │
│   parse accordingly  │
└─────────────────────┘
```

RFC 5906 (Autokey) – Extension Field Parsing

```
┌─────────────────────┐
│  Parse Fixed Fields │
│    in NTP Header    │
└─────────────────────┘
           │
           ▼
     ╱─────────╲
    ╱ # of remaining ╲         Yes      ┌──────────────┐
    ╲ octets = 0     ╱  ─────────────▶  │  End parsing  │
     ╲─────────╱                        └──────────────┘
           │                                    ▲
           │ No                                 │
           ▼                                    │
     ╱─────────╲                                │
    ╱ # of remaining ╲    Yes    X    ┌──────────────────────┐
    ╲ octets ≤ 24    ╱  ────────────▶ │  Assume it's a MAC    │
     ╲─────────╱                      └──────────────────────┘
           │
           │ No
           ▼
┌─────────────────────┐
│   Assume it's an    │
│   Extension Field   │
│  parse accordingly  │
└─────────────────────┘
```

If the last extension field $\geq$ 28 octets, we never get here.

6

This Draft: Using Extension Fields Without Authentication

▶ **The last extension field MUST be at least 28 octets long.**

▶ **Other extension fields (if any): at least 16 octets long (NTPv4).**

▶ **Compatible with existing implementations complying to RFC 5905, RFC 5906.**

Next Steps

▶ **Feedback from WG.**

▶ **Adopt as WG document.**

▶ **Consider extending the document to define a more general and flexible usage of extension fields.**

▶ **Issue an erratum for RFC 5905, rephrasing:**

"In NTPv4, one or more extension fields can be inserted after the header and before the MAC, which is always present when an extension field is present."