Extended Error Conclusions and Non-Conclusions from WGLC #2
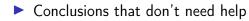
Wes Hardaker

November 18, 2019

Overview

- Conclusions that don't need help

Overview

- Conclusions that don't need help

- Conclusions that weren't conclusions

Registry changes

- ▶ Only one issue was easily resolved
- ▶ Registry ranges simplified to:

0	-	49151	First come, first served
49152	-	65280	Private use

DNS UDP overflow

- Overflow happens all the time (e.g. glue)
- Normally the *TC bit* signals overflow
    - Some important information was excluded
    - Hint to resolver hinted to retry over TCP

EDE overflow

- ► EDE can cause overflow, of course
  - ► But: more important info shouldn't be dropped!
  - ► Therefore: EDE should be dropped first
  - ► Set the TC bit?

EDE overflow

- ▶ EDE can cause overflow, of course
    - ▶ But: more important info shouldn't be dropped!
    - ▶ Therefore: EDE should be dropped first
    - ▶ Set the TC bit?

- ▶ Problems
    - ▶ TC seems extreme; EDE is only supplimental
    - ▶ Retrying over TCP seems extreme
    - ▶ The EDE information may be UDP only even

A New Idea is Floated

- Suggestion from Viktor Dukhovni's colleague:
    - add a new EDNS0 bit
    - use this instead of the TC bit
    - "non-essential diagnostic information was left out"

- Thoughts?

Forwarding Handling

- ▶ Multiple LC comments stated:
  - ▶ we need to handle forwarding!

- ▶ Discussions with multiple people lead to some options

Forwarding Options (1/2)

(All options listed for completeness)

1. ~~Mandate: no forwarding of EDE happens~~
2. Mandate: resolver/forwarders should simply copy forward
3. MAY copy and adjust the extra-text field
   - adding additional information
   - e.g., where it came from.
   - (unlikely to be popular)

Forwarding Options (2/2)

4. Could add tracing elements to the packet
   4.1 Add a single source by the EDE generating entity
   4.2 ~~Add multiple sources (e.g. traceroute)~~
   4.3 RECOMMEND adding source indication to extra-info
5. ~~Add a new EDE code for supplemental information.~~
   - another "multiple source" mechanism
   - IE: this records details of EDEs above it
6. Make the document experimental
   - deal with it after deployment experience
7. Your idea here!!

Forwarding Options (2/2)

4. Could add tracing elements to the packet
   4.1 Add a single source by the EDE generating entity
   4.2 ~~Add multiple sources (e.g. traceroute)~~
   4.3 RECOMMEND adding source indication to extra-info
5. ~~Add a new EDE code for supplemental information.~~
   - ▶ another "multiple source" mechanism
   - ▶ IE: this records details of EDEs above it
6. Make the document experimental
   - ▶ deal with it after deployment experience
7. Your idea here!!

Adding a source field

```
                                       1   1   1   1   1   1
       0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 0:  |                          OPTION-CODE                          |
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 2:  |                         OPTION-LENGTH                         |
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 4:  | INFO-CODE                                                     |
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 6:  | SRC_LENGTH                                                    |
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 8:  / SRC_FIELD (which can be zero length)      *** NEW ***         /
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
10:  / EXTRA-TEXT (can be zero length)...                            /
     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Source Field Options

1. NSID
2. hostname (fqdn)
3. ip address
4. URL (eg from doh)
5. ip:port
6. cert subject name
7. . . .

Source Field Options

1. NSID *(not reinventing the wheel)*
2. hostname (fqdn)
3. ip address
4. URL (eg from doh)
5. ip:port
6. cert subject name
7. . . .

NSID Definition: RFC5001

```
2.4.  Presentation Format

   User interfaces MUST read and write the contents of the NSID option
   as a sequence of hexadecimal digits, two digits per payload octet.

   The NSID payload is binary data.  Any comparison between NSID
   payloads MUST be a comparison of the raw binary data.  Copy
   operations MUST NOT assume that the raw NSID payload is null-
   terminated.  Any resemblance between raw NSID payload data and any
   form of text is purely a convenience, and does not change the
   underlying nature of the payload data.

   See Section 3.3 for discussion.
```

Next steps

- is a single NSID source field acceptable
- forward everything and add your own