Extensible Provisioning Protocol (EPP) mapping for DNS Time-To-Live (TTL) values

Gavin Brown, Principal Engineer, GDS Technical Services

IETF 118, Prague, regext working group
2023-11-09

ICANN

Background

- This extension allows EPP clients to set TTL values for DNS records published in the parent zone:
  - NS, DS for domains
  - DNAME for IDN variants
  - A/AAAA for glue
- Adopted by the WG back in May
- Has attracted some interest as (if used correctly) it can mitigate operational risk in several scenarios

Current state of play

- The current XML syntax allows validation of command frames using the XSD with a minimum of business logic (simplifying implementation)
- However, it does so by encoding “data” (specifically DNS record types) as “markup”

```
<ttl:NS>3600</ttl:NS>
<ttl:DS>600</ttl:NS>
```

- This feels like a leaky abstraction and is “inelegant”

Resolving the dilemma

- I brought this dilemma to the ICANN meeting in Hamburg (CPH TechOps and ccNSO TechDay) hoping to solicit some ideas
- I'm doing the same today!
- Need to make progress so absent suggestions from the WG, I am going to proceed with implementing a new syntax

Proposed new syntax

- “Global” TTL model (one TTL for all record types) will be removed
- New `<ttl:ttl>` syntax:
  - Mandatory “for” attribute which contains the DNS record type mnemonic
- New normative language to ensure:
  - Duplicate elements are forbidden
    - eg. this isn’t allowed:

```
<ttl:ttl for=”NS”>3600</ttl:ttl>
<ttl:ttl for=”NS”>7200</ttl:ttl>
```

  - “Inappropriate” elements are forbidden
    - e.g can’t specify NS/DS/DNAME TTLs for host objects
- “Cascading effect” of A/AAA TTLs will be removed

Example #1 - domain create with host objects

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <domain:create
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>example.com</domain:name>
        <domain:period unit="y">2</domain:period>
        <domain:ns>
          <domain:hostObj>ns1.example.net</domain:hostObj>
          <domain:hostObj>ns2.example.net</domain:hostObj>
        </domain:ns>
        <domain:registrant>jd1234</domain:registrant>
        <domain:contact type="admin">sh8013</domain:contact>
        <domain:contact type="tech">sh8013</domain:contact>
        <domain:authInfo>
          <domain:pw>2fooBAR</domain:pw>
        </domain:authInfo>
      </domain:create>
    </create>
    <extension>
      <ttl:create
        xmlns:ttl="urn:ietf:params:xml:ns:epp:ttl-1.0">
        <ttl:ttl for="NS">3600</ttl:ttl>
        <ttl:ttl for="DS">900</ttl:ttl>
        <ttl:ttl for="DNAME"/>
      </ttl:create>
    </extension>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

Example #2 - host create

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <host:create
        xmlns:host="urn:ietf:params:xml:ns:host-1.0">
        <host:name>ns1.example.com</host:name>
        <host:addr ip="v4">192.0.2.2</host:addr>
        <host:addr ip="v4">192.0.2.29</host:addr>
        <host:addr ip="v6">1080::8:800:200C:417A</host:addr>
      </host:create>
    </create>
    <extension>
      <ttl:create
        xmlns:ttl="urn:ietf:params:xml:ns:epp:ttl-1.0">
        <ttl:ttl for="A">3600</ttl:ttl>
        <ttl:ttl for="AAAA">7200</ttl:ttl>
      </ttl:create>
    </extension>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

Example #3 - domain create with host attributes

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <domain:create
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>example.com</domain:name>
        <domain:period unit="y">2</domain:period>
        <domain:ns>
          <domain:Attr>
            <domain:hostName>ns1.example.com</domain:hostName>
            <domain:hostAddr ip="v4">192.0.2.2</domain:hostAddr>
          </domain:Attr>
          <domain:Attr>
            <domain:hostName>ns2.example.net</domain:hostName>
          </domain:Attr>
        </domain:ns>
        <domain:registrant>jd1234</domain:registrant>
        <domain:contact type="admin">sh8013</domain:contact>
        <domain:contact type="tech">sh8013</domain:contact>
        <domain:authInfo>
          <domain:pw>2fooBAR</domain:pw>
        </domain:authInfo>
      </domain:create>
    </create>
    <extension>
      <ttl:create
        xmlns:ttl="urn:ietf:params:xml:ns:epp:ttl-1.0">
        <ttl:ttl for="NS">3600</ttl:ttl>
        <ttl:ttl for="A">86400</ttl:ttl>
      </ttl:create>
    </extension>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

Pros & cons

- The new syntax is simpler
- …but will require more work for servers to implement
- There is a balance to be struck, does this get it right?

Questions, comments, feedback?

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg