IETF INTERIM DNSOP 23 APRIL 2020

TOM PUSATERI

TIM WATTENBERG

TIMEOUT RR'S

TIMEOUT RESOURCE RECORDS

- DNS Resource Record lifetimes informed by an application are not synchronized between primary and secondary servers or across primary server restarts
- Proprietary and non-interoperable solutions exist but no standards solution
- This solution provides for timeout of resource records on primary server (reference counting) or by external UPDATE manager (garbage collection)
- Applicable for UPDATEs from DHCP servers, SRV records from Active Directory Controllers, PTR, SRV, & TXT records from UPDATES in Unicast Service Discovery, ACME Certificate Management (provisioning & TLSA) and many more use cases.

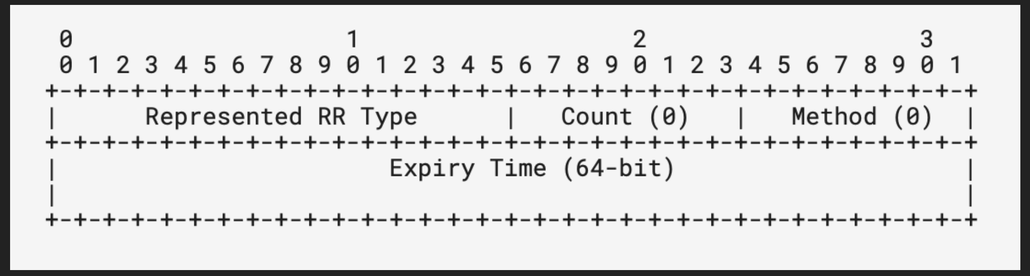
ABSOLUTE VS. RELATIVE TIME

- Resource records synchronize between servers without being changed. By using absolute time, TIMEOUT records can remain static
- Some expiry time values are learned via relative offsets.
  - Some IoT devices don't have real-time clock hardware.
  - EDNS(0) Update Lease Option uses relative lifetimes and can be added to UPDATE
  - Primary server can generate the TIMEOUT records converting to absolute time
- Other devices with synchronized clocks can generate TIMEOUT records directly and include them in the UPDATE with the records they represent

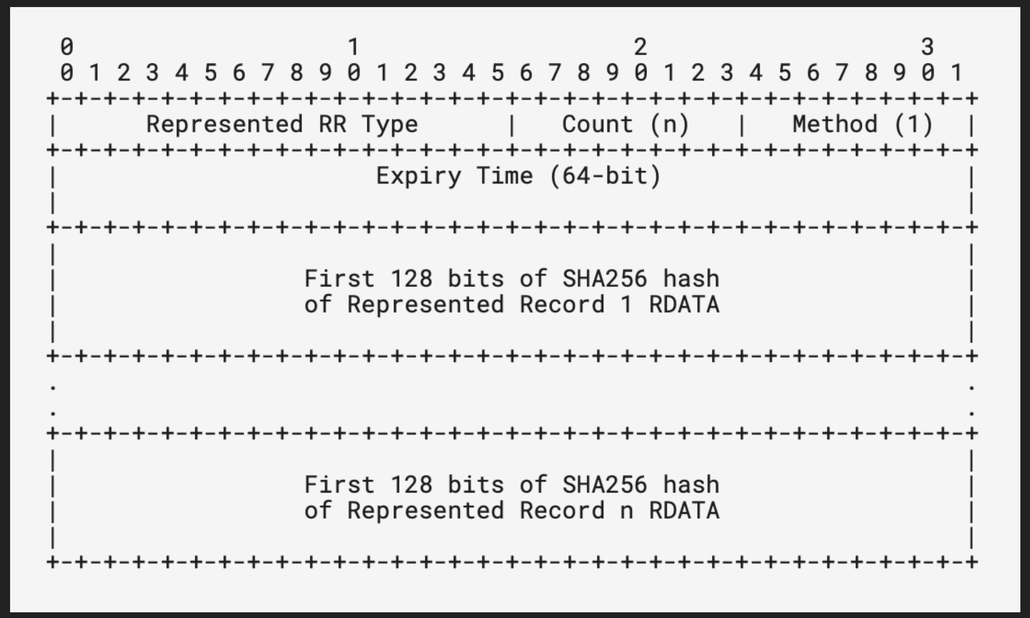
WIRE FORMAT

- Count is the number of Hashes present after Expiry Time
- Length of HASH implied by registered Method
  - Method 0 - No HASH
  - Method 1 - First 128 bits of SHA-256
- Fixed HASH lengths regardless of variable size of RDATA

TIMEOUT with no HASH needed



TIMEOUT with HASH(s)



SIMPLE EXAMPLE

- (3) UPDATEs are sent at time Tn with records on right (top)
- TIMEOUT records could be included in the UPDATEs (bottom) with lease lifetime Ln setting expiry time as Tn + Ln

Address records from DHCP server

Name	RR Type	Value
s.example.com.	A	192.0.2.5
s.example.com.	AAAA	2001:db8::5
5.2.0.192.in-addr.arpa.	PTR	s.example.com.
5.0.0.0.0.0.0.0.0.0.0.0.0.b8.d.1.20.ip6.arpa.	PTR	s.example.com.

Corresponding TIMEOUT records

Owner Name	Type	Cnt	Mth	Expire
s.example.com.	A	0	0	Tn+Ln
s.example.com.	AAAA	0	0	Tn+Ln
5.2.0.192.in-addr.arpa.	PTR	0	0	Tn+Ln
5.0.0.0.0.0.0.0.0.0.0.0.0.b8.d.1.20.ip6.arpa.	PTR	0	0	Tn+Ln

EXAMPLE WITH HASHES

- An UPDATE is sent from Printer A at time Ta with record lifetime La
- An UPDATE is sent from Printer B at time Tb with record lifetime Lb
- TIMEOUT records could be included in the UPDATEs with expiry times Ta + La and Tb + Lb, respectively
- C = count, M = method

Printer A Service Advertisement

Owner name	RR Type	Value
_ipp._tcp.example.com.	PTR	p1._ipp._tcp.example.com.
p1._ipp._tcp.example.com.	SRV	0 0 631 p1.example.com.
p1._ipp._tcp.example.com.	TXT	paper=A4
p1.example.com.	A	192.0.2.1
p1.example.com.	AAAA	2001:db8::1

Printer B Service Advertisement

Owner name	RR Type	Value
_ipp._tcp.example.com.	PTR	p2._ipp._tcp.example.com.
p2._ipp._tcp.example.com.	SRV	0 0 631 p2.example.com.
p2._ipp._tcp.example.com.	TXT	paper=B4
p2.example.com.	A	192.0.2.2

Corresponding TIMEOUT records

Owner Name	Type	C	M	Expire / Hash
_ipp.tcp.example.com.	PTR	1	1	Ta+La 69D67BCB98E8809702B9DFCA6B865558
_ipp.tcp.example.com.	PTR	1	1	Tb+Lb 7EBE34BC8B3E7306F8FCF1D6805331E1
p1._ipp._tcp.example.com.	SRV	0	0	Ta + La
p1._ipp._tcp.example.com.	TXT	0	0	Ta + La
p2._ipp._tcp.example.com.	SRV	0	0	Tb + Lb
p2._ipp._tcp.example.com.	TXT	0	0	Tb + Lb
p1.example.com.	A	0	0	Ta + La
p1.example.com.	AAAA	0	0	Ta + La
p2.example.com.	A	0	0	Tb + Lb