



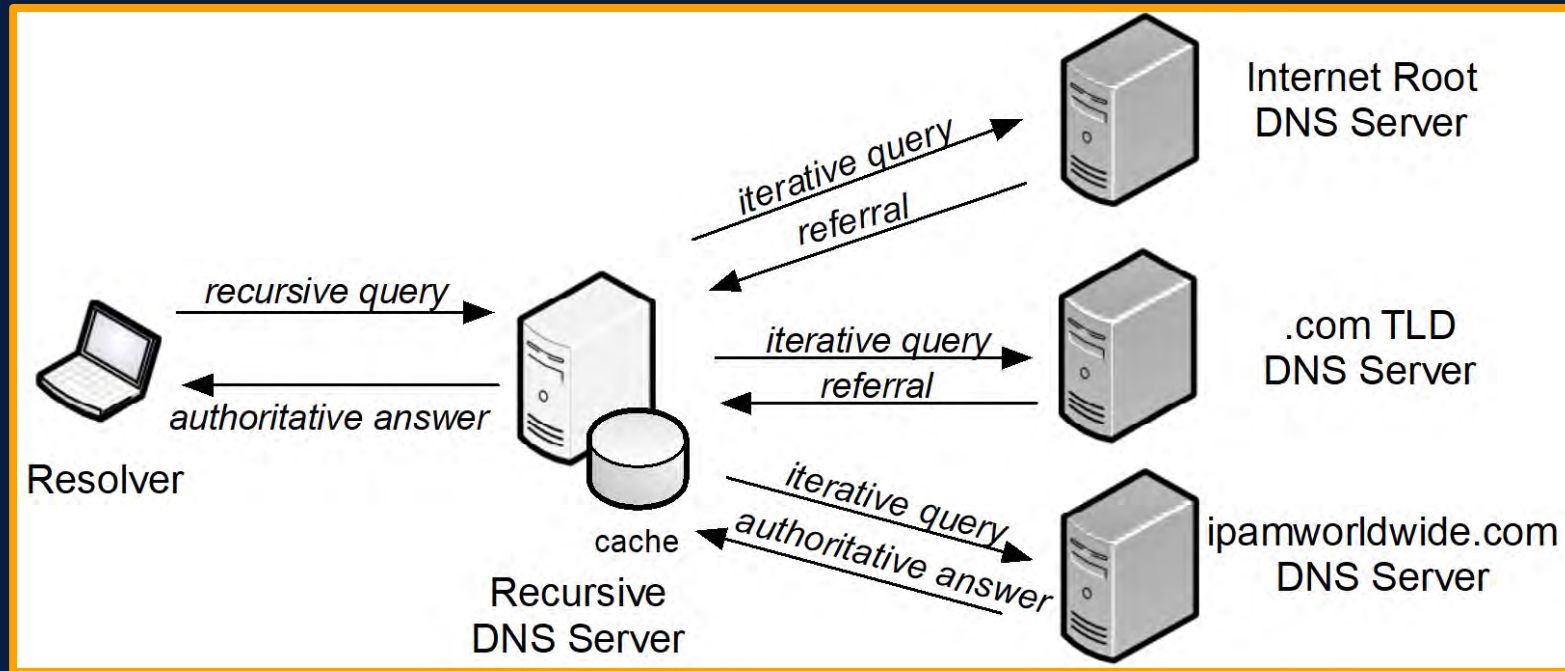
Extended DNS Errors

N3K Expert Webinar Series

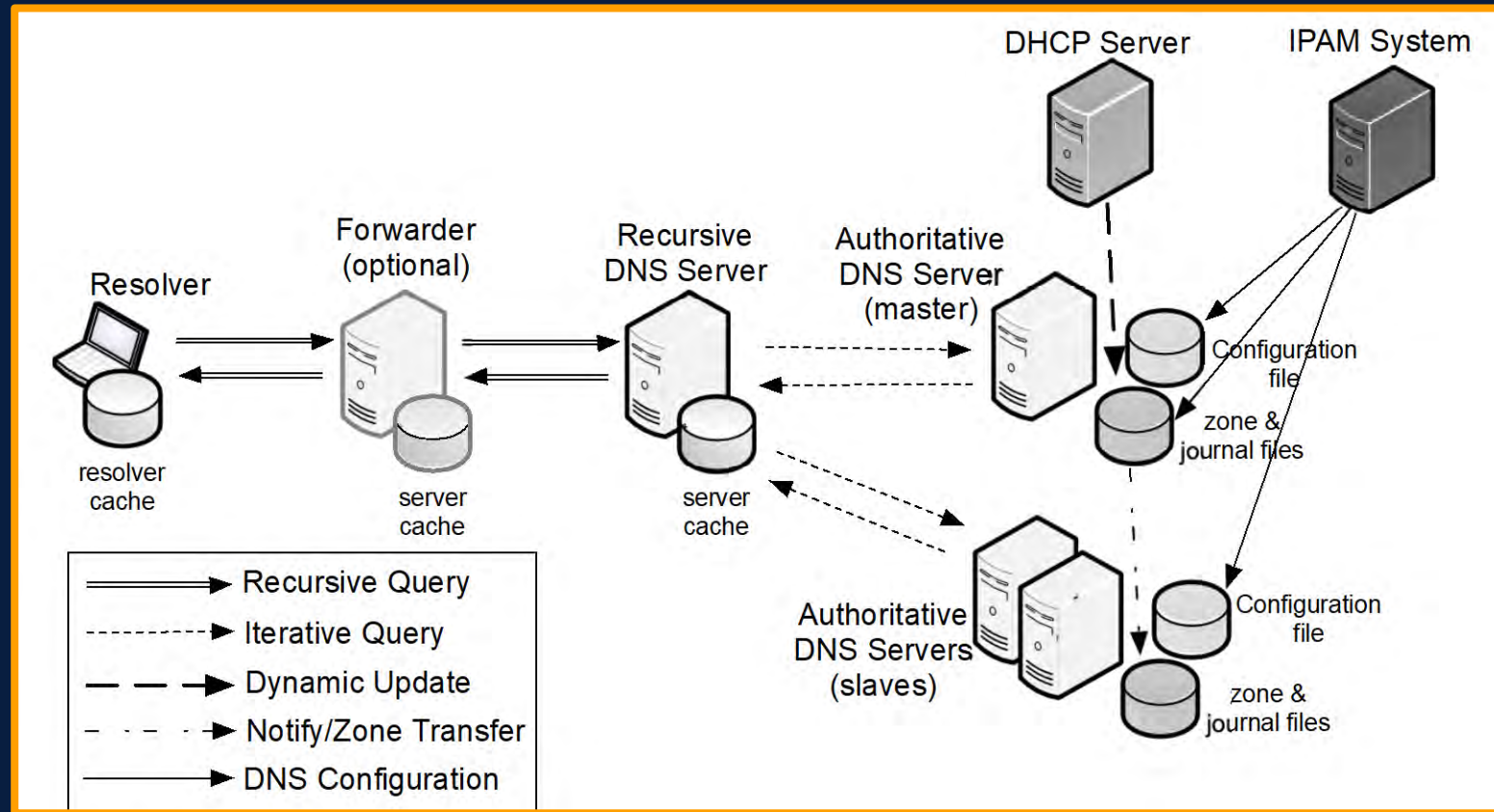
Andreas Taudte
Principal DDI Consultant

Last updated March 2023

Why not just use ping?



Why not just use ping?



DNS Response Codes

- **NOERROR** - No Error
- **FORMERR** - Format Error
- **SERVFAIL** - Server or Feature Problem
- **NXDOMAIN** - FQDN doesn't exist
- **NOTIMPL** - Not implemented
- **REFUSED** - Action refused
- **NotAuth** - Server not authoritative for Zone
- **NotZone** - Name not contained in Zone
- **prereq** - YXDomain, YXRRSet, NXRRSet

Extended DNS Errors (EDE)

- Defines Variety of **new Error Messages**¹ in DNS
- Extends **SERVFAIL** and **REFUSED** with Details **about the Cause**
- Reduces Complexity of Diagnosing DNS Issues (**the fun is lost**)
- **Does not affect** Processing of Response Codes (**RCODE**)
- Uses **EDNS0** Option to include extended Information
- **Unauthenticated** unless secured by Transaction (such as TSIG², DoH³ or DoQ⁴)

¹<https://www.rfc-editor.org/info/rfc8914>

²<https://www.rfc-editor.org/info/rfc8945>

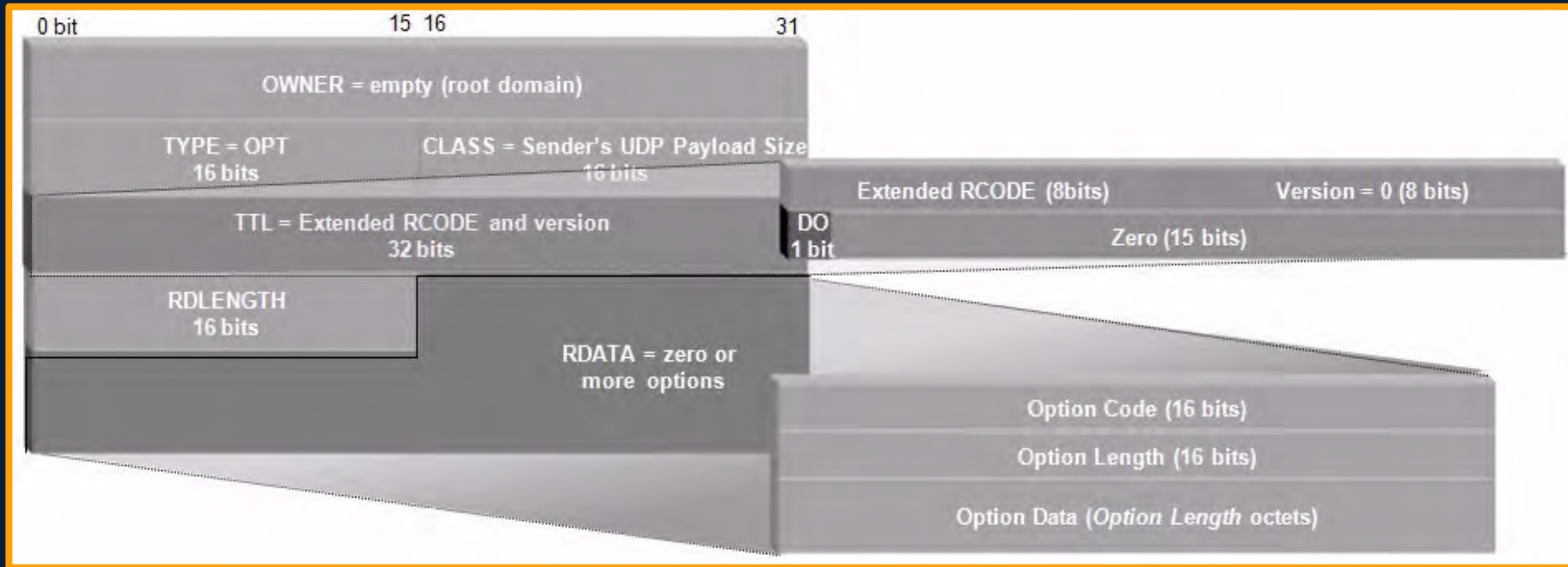
³<https://www.rfc-editor.org/info/rfc8484>

⁴<https://www.rfc-editor.org/info/rfc9250>

Extension Mechanisms for DNS

- DNS Responses typically small in Size (less than 512 Bytes)
- Version 0 (EDNS0) defines **OPT Pseudo Record Record**
 - Used to **advertise Capabilities of Sender**
 - Placed in **ADDITIONAL SECTION** by Resolver or Server
 - UDP-based DNS Message of **up to 4096 Bytes**
- Required for Features like
 - DNSSEC validation,
 - DNS COOKIE option or
 - Name Server Identifier (NSID)

EDNSo Format



Testing EDNS Compatibility



EDNS Compliance Tester

Zone Name:

Server (optional):

Address (optional): (IPv4 or IPv6)

Initially Defined Extended DNS Errors



- 0 Other
- 1 Unsupported DNSKEY Algorithm
- 2 Unsupported DS Digest Type
- 3 **Stale Answer**
- 4 Forged Answer
- 5 DNSSEC Indeterminate
- 6 **DNSSEC Bogus**
- 7 Signature Expired
- 8 Signature Not Yet Valid
- 9 DNSKEY Missing
- 10 **RRSIGs Missing**
- 11 No Zone Key Bit Set
- 12 NSEC Missing
- 13 **Cached Error**
- 14 **Not Ready**
- 15 **Blocked**
- 16 Censored
- 17 Filtered
- 18 Prohibited
- 19 **Stale NXDOMAIN Answer**
- 20 Not Authoritative
- 21 Not Supported
- 22 **No Reachable Authority**
- 23 **Network Error**
- 24 Invalid Data

```
myPro:~ andreas$ dig @2606:4700:4700::64 fail01.dnssec.works. AAAA

; <<>> DiG 9.18.11 <<>> @2606:4700:4700::64 fail01.dnssec.works. AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL id: 45955
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EDE: 10 (RRSIGs Missing): (failed to verify fail01.dnssec.works. AAAA)
;; QUESTION SECTION:
;fail01.dnssec.works.      IN      AAAA

;; Query time: 62 msec
;; SERVER: 2606:4700:4700::64#53(2606:4700:4700::64) (UDP)
;; WHEN: Tue Mar 14 17:55:03 CET 2023
;; MSG SIZE rcvd: 96
```

```

< Domain Name System (response)
  Transaction ID: 0xaa67
  > Flags: 0x8182 Standard query response, Server failure
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  > Queries
  > Additional records
    < <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1232
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
      > Z: 0x0000
      Data length: 48
    < Option: Extended DNS Error
      Option Code: Extended DNS Error (15)
      Option Length: 44
      Option Data: 000a6661696c6564420746f20766572696667920666169
      Info Code: RRSIGs Missing (10)
      Extra Text: failed to verify fail01.dnssec.works. AAAA
    [Request In: 475]
    [Time: 0.073228000 seconds]
```

Digging Broken DNSSEC

```
myPro:~ andreas$ dig @2620:fe::fe fail01.dnssec.works. AAAA +nostat +noquestion +noadditional +noauthority
;; communications error to 2620:fe::fe#53: timed out

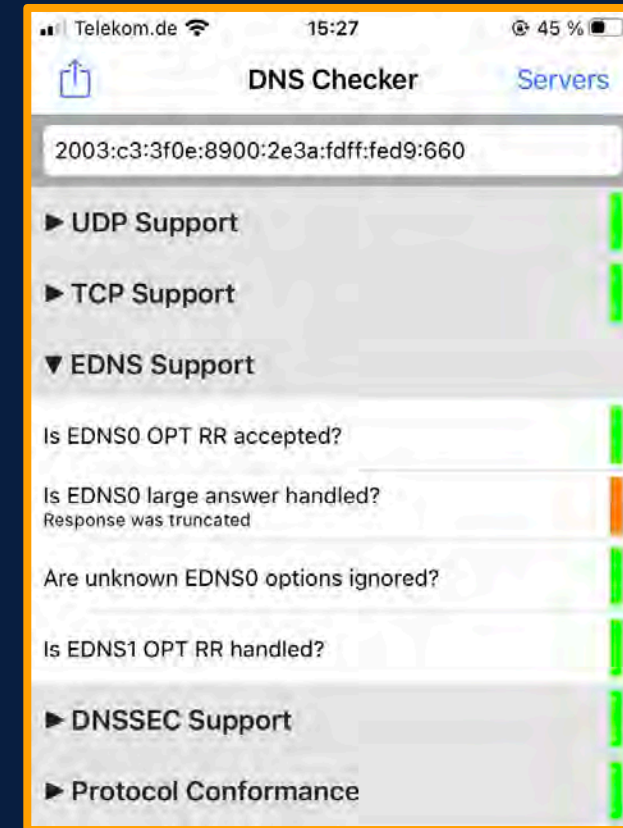
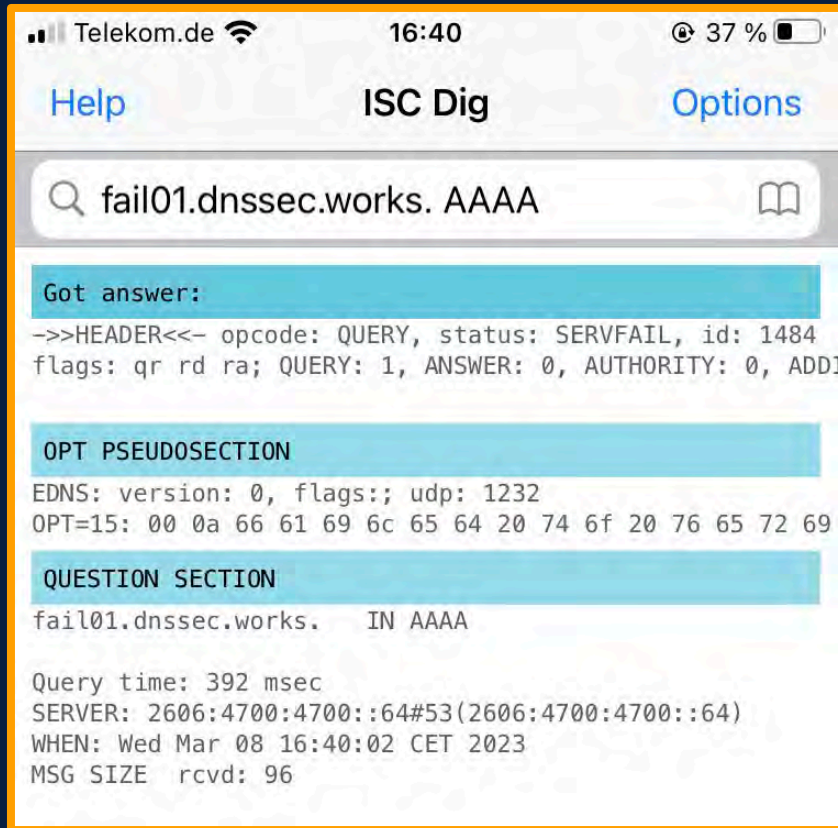
; <<>> DiG 9.18.11 <<>> @2620:fe::fe fail01.dnssec.works. AAAA +nostat +noquestion +noadditional +noauthority
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31866
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 10 (RRSIGs Missing)
myPro:~ andreas$
```

```
myPro:~ andreas$ dig @2620:fe::fe fail01.dnssec.works. AAAA +nostat +noquestion +noadditional +noauthority +cdflag
; <<>> DiG 9.18.11 <<>> @2620:fe::fe fail01.dnssec.works. AAAA +nostat +noquestion +noadditional +noauthority +cdflag
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10870
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 10 (RRSIGs Missing)
;; ANSWER SECTION:
fail01.dnssec.works. 3600 IN AAAA 2a01:198:2b6:1000:203:2dff:fe29:8424
myPro:~ andreas$
```

Digging on the Phone



<https://apps.apple.com/us/app/isc-dig/id1115648880>
<https://apps.apple.com/de/app/isc-dns-checker/id1141834002>

What's next?

Polls Names not recorded ; Results shared ✕

Expert Webinar 2023-04-27

- DHCP Security Considerations
- DNS Security Strategy
- Low-Risk DNSSEC Implementation Plan
- Kea the Next-Gen DHCP

Greedy for more?



https://ddiug.de

```
1 0 1 0 1 0 1 0 0 0 1 0 0 1 0 0
0 1 0 1 0 1 1 1 1 1 1 1 0 0 1 1
1 0 1 0 1 0 0 0 0 0 D 1 0 1 1 0 0
0 0 1 0 0 1 1 1 H 0 1 0 0 1
0 1 0 1 0 0 1 C 0 0 1 1
1 0 0 1 0 P 1 1 0 0
1 1 0 D I 0 1
0 0 1 N P 1 0
0 0 S A 0
1 M
```

<https://www.n3k.com/en/services/trainings>



Thank you for your Time.



N3K Network Systems
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn
+49 7131 594 95 0
info@n3k.de