



# Troubleshooting DNS with dig

---

N3K Expert Webinar Series

**Andreas Taudte**  
Principal DDI Consultant

Last updated May 2023

# Housekeeping

---

- Timing, Schedule, Q&A Session
- Online Etiquette (microphones, distracting activities)
- Recording and Privacy



# Local Names can't be looked up

---

- Client's **TCP/IP Config.** (e.g. resolv.conf)
- **Zone Data File** contains the Resource Record in Question
- Name Server hasn't **loaded Zone** Data File
- Ensure Resource Records have **trailing Dots**, if they require them
- **Secondary** Name Server has **Problems** updating the Zone
- Parent Zone's **Delegation**

# Remote Names can't be looked up

---

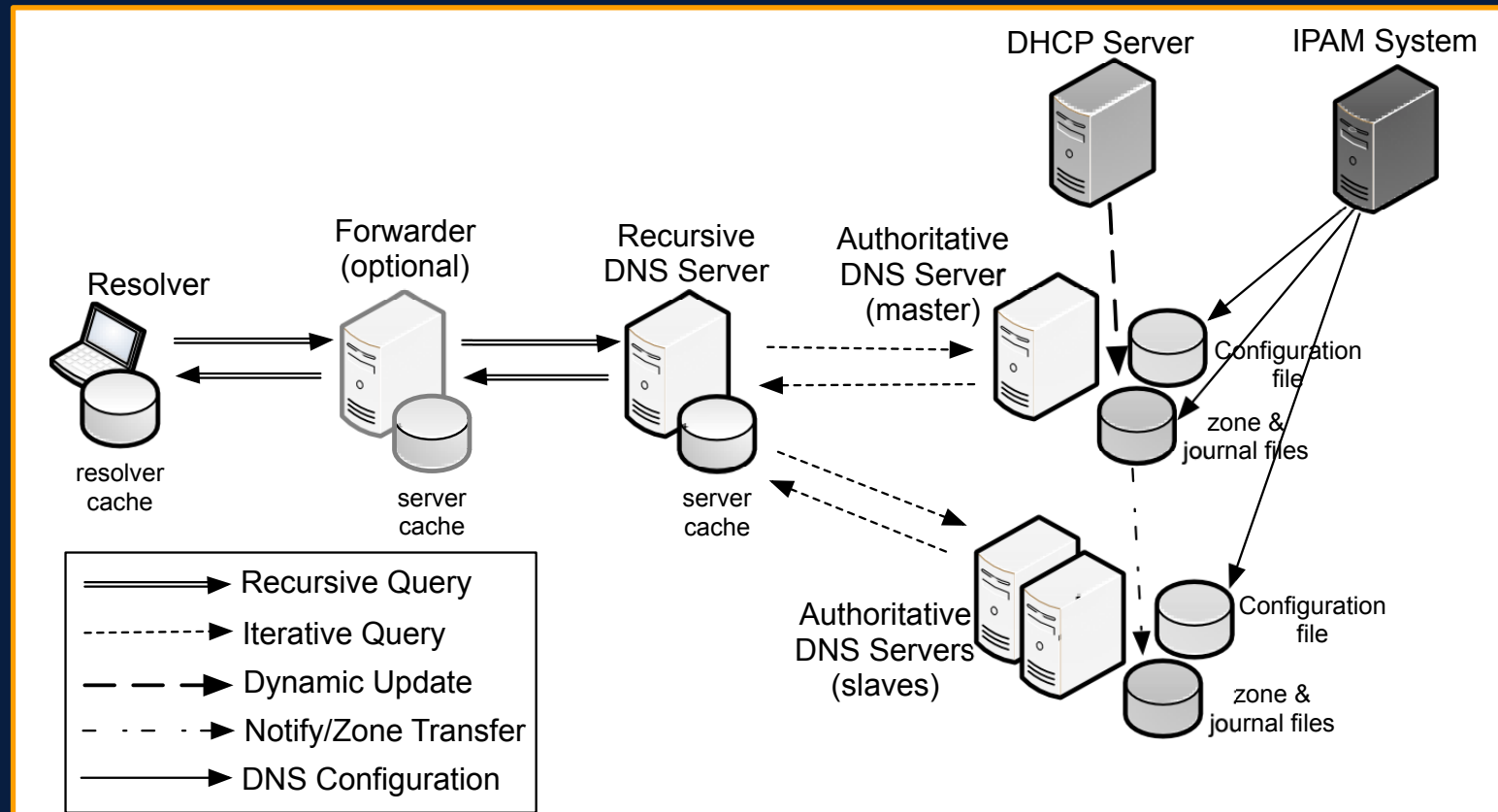
- Local Name **Server's Config**. (Root Hints, Forwarders, etc.)
- Remote Zone's Name Server **Reachability** (traceroute, nslookup, dig, etc.)
- Lame **Delegation** if remote Zone is new or has changed
- **FQDN** doesn't exist on remote Zone's Server

# Wrong or inconsistent Answers

---

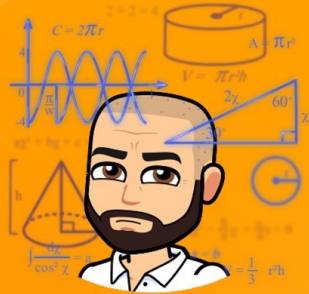

- Primary's Serial Number is lower than the Secondary's one
- Primary's Config. wasn't reloaded
- Secondary is having Trouble updating from its Primary
- Multiple Records are handled by Round-Robin
- Authoritative vs. Recursive (e.g. AAAA from Authoritative & PTR from Recursive)

# 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“**

**Experten Webinar  
mit Andreas Taudte**

<https://www.n3k.com/experten-webinar-reihe-mit-andreas-taudte-mr-ddi>

# Domain Information Groper (dig)

---

- Performs DNS **Lookups** and displays the **Answers**
- **Other** Lookup Tools tend to have **less Functionality**
- **No interactive Mode**, just Arguments
- **Batch Mode** for Reading Lookup Requests from a File



# Name-to-Address Mapping

```
myPro:~ andreas$ dig @2606:4700:4700::64 isc.org. AAAA

;<<>> DiG 9.18.11 <<>> @2606:4700:4700::64 isc.org. AAAA
;(1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46403
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;isc.org.                IN      AAAA

;; ANSWER SECTION:
isc.org.                 300    IN      AAAA    2001:4f8:1:f::66

;; Query time: 22 msec
;; SERVER: 2606:4700:4700::64#53(2606:4700:4700::64) (UDP)
;; WHEN: Fri May 19 10:03:21 CEST 2023
;; MSG SIZE rcvd: 64

myPro:~ andreas$
```

# Address-to-Name Mapping

```
myPro:~ andreas$ dig @2606:4700:4700::64 -x 2001:4f8:1:f::66

; <<>> DiG 9.18.11 <<>> @2606:4700:4700::64 -x 2001:4f8:1:f::66
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45623
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.0.1.0.0.0.8.f.4.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.0.1.0.0.0.8.f.4.0.1.0.0.2.ip6.arpa. 7200 IN PTR www.isc.org.

;; Query time: 728 msec
;; SERVER: 2606:4700:4700::64#53(2606:4700:4700::64) (UDP)
;; WHEN: Fri May 19 10:05:52 CEST 2023
;; MSG SIZE rcvd: 126

myPro:~ andreas$
```

# Digging authoritative and recursive DNS



```
myPro:~ andreas$ dig @2606:4700:4700::64 isc.org. MX +nostat +noquestion +noadditional +noauthority +noedns

;<<>> DiG 9.18.11 <<>> @2606:4700:4700::64 isc.org. MX +nostat +noquestion +noadditional +noauthority +noedns
;(1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49648
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
isc.org.          300      IN       MX       5 mx.pao1.isc.org.
isc.org.          300      IN       MX       10 mx.ams1.isc.org.

myPro:~ andreas$
```

```
myPro:~ andreas$ dig @2001:500:6b:2::26 isc.org. MX +nostat +noquestion +noadditional +noauthority +noedns +norecurse

;<<>> DiG 9.18.11 <<>> @2001:500:6b:2::26 isc.org. MX +nostat +noquestion +noadditional +noauthority +noedns +norecurse
;(1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1990
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 6

;; ANSWER SECTION:
isc.org.          300      IN       MX       10 mx.ams1.isc.org.
isc.org.          300      IN       MX       5 mx.pao1.isc.org.

myPro:~ andreas$
```

# Digging for Stats

---

```
myPro:~ andreas$ dig @2001:388:1:5001::100 sydney.edu.au. NS +noall +stats
;; Query time: 311 msec
;; SERVER: 2001:388:1:5001::100#53(2001:388:1:5001::100) (UDP)
;; WHEN: Fri May 19 13:00:57 CEST 2023
;; MSG SIZE rcvd: 388

myPro:~ andreas$ █
```

# Digging for Zone Transfer

```
myPro:~ andreas$ dig . axfr @lax.xfr.dns.icann.org | tail -n 10
ns1zim.telone.co.zw. 172800 IN A 41.220.30.81
ns1zim.telone.co.zw. 172800 IN AAAA 2c0f:f758:0:a::81
ns2zim.telone.co.zw. 172800 IN A 41.220.30.82
ns2zim.telone.co.zw. 172800 IN AAAA 2c0f:f758:0:a::82
. 86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023051900 1800 900 604800 86400
;; Query time: 1319 msec
;; SERVER: 192.0.32.132#53(lax.xfr.dns.icann.org) (TCP)
;; WHEN: Fri May 19 10:46:25 CEST 2023
;; XFR size: 24914 records (messages 83, bytes 1343873)
myPro:~ andreas$ █
```

# Digging the Internet Protocol

```
myPro:~ andreas$ dig isc.org. AAAA -4 +noall +stats
;; Query time: 37 msec
;; SERVER: 10.0.187.1#53(10.0.187.1) (UDP)
;; WHEN: Fri May 19 10:52:59 CEST 2023
;; MSG SIZE rcvd: 64

myPro:~ andreas$ dig isc.org. AAAA -6 +noall +stats
;; Query time: 8 msec
;; SERVER: fd00::2e3a:fdff:fed9:660#53(fd00::2e3a:fdff:fed9:660) (UDP)
;; WHEN: Fri May 19 10:53:32 CEST 2023
;; MSG SIZE rcvd: 64

myPro:~ andreas$
```

# Digging specific Port from specific Source Address

```
myPro:~ andreas$ dig @2003:c3:3f4c:4e00:e772:590:66c5:6f44 isc.org -b 2003:c3:3f4c:4e00:1478:6938:54f:376 +nocmd +nostats
;; communications error to 2003:c3:3f4c:4e00:e772:590:66c5:6f44#53: connection refused
;; communications error to 2003:c3:3f4c:4e00:e772:590:66c5:6f44#53: connection refused
;; communications error to 2003:c3:3f4c:4e00:e772:590:66c5:6f44#53: connection refused

;<<>> DiG 9.18.11 <<>> @2003:c3:3f4c:4e00:e772:590:66c5:6f44 isc.org -b 2003:c3:3f4c:4e00:1478:6938:54f:376 +nocmd +nostats
; (1 server found)
;; global options: +cmd
;; no servers could be reached

myPro:~ andreas$
```

```
myPro:~ andreas$ dig @2003:c3:3f4c:4e00:e772:590:66c5:6f44 isc.org -p 5353 -b 2003:c3:3f4c:4e00:1478:6938:54f:376 +nocmd +noauthority +noadditional +nostats
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8153
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
; COOKIE: 9e6464d9b17ab54e1d99952464677eb74f94cb26d2ce5e61 (good)
;; QUESTION SECTION:
;isc.org.                IN      A
;; ANSWER SECTION:
isc.org.                138    IN      A      149.20.1.66

myPro:~ andreas$
```

# Digging internationalized Domain Names (IDN)

```
myPro:~ andreas$ dig garten-am-mönchhof.de. AAAA +nostats +noauthority +noanswer +noedns

; <<>> DiG 9.18.11 <<>> garten-am-mönchhof.de. AAAA +nostats +noauthority +noanswer +noedns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1793
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
garten-am-mönchhof.de.      IN      AAAA

myPro:~ andreas$
```

```
myPro:~ andreas$ dig garten-am-mönchhof.de. AAAA +nostats +noauthority +noanswer +noedns +noidnout

; <<>> DiG 9.18.11 <<>> garten-am-mönchhof.de. AAAA +nostats +noauthority +noanswer +noedns +noidnout
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34367
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
xn--garten-am-mnchhof-9zb.de.  IN      AAAA

myPro:~ andreas$
```

```
myPro:~ andreas$ idn2 --quiet garten-am-mönchhof.de.
xn--garten-am-mnchhof-9zb.de.
myPro:~ andreas$
```



# Digging without EDNS Support

```
myPro:~ andreas$ dig customer.biz. AAAA +nostat +noquestion +noadditional +noauthority +norecurse
[... ]
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 56938
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: ab269fbf4c794e3c (echoed)

myPro:~ andreas$
```

```
myPro:~ andreas$ dig customer.biz. AAAA +nostat +noquestion +noadditional +noauthority +norecurse +noedns
[... ]
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54667
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
customer.biz.          600      IN       AAAA     2001:db8:fb0a::8d24:fb0a

myPro:~ andreas$
```

# Digging for the Name Server Identifier (NSID)

```
myPro:~ andreas$ dig @2620:fe::fe isc.org aaaa +nocmd +nostat +noquestion +noadditional +noauthority +nsid
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61676
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; NSID: 72 65 73 37 32 30 2e 61 6d 73 2e 72 72 64 6e 73 2e 70 63 68 2e 6e 65 74 ("res720.ams.rrdns.pch.net")
;; ANSWER SECTION:
isc.org.          300      IN       AAAA    2001:4f8:1:f::66

myPro:~ andreas$
```

```
myPro:~ andreas$ dig @2620:fe::fe isc.org aaaa +nocmd +nostat +noquestion +noadditional +noauthority +nsid
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34791
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; NSID: 72 65 73 36 30 30 2e 61 6d 73 2e 72 72 64 6e 73 2e 70 63 68 2e 6e 65 74 ("res600.ams.rrdns.pch.net")
;; ANSWER SECTION:
isc.org.          300      IN       AAAA    2001:4f8:1:f::66

myPro:~ andreas$
```

# Digging DNSSEC

```
myPro:~ andreas$ dig @2001:500:6b:2::26 isc.org. MX +nostat +noquestion +noanswer +noadditional +noauthority +norecurse +dnssec

; <<>> DiG 9.18.11 <<>> @2001:500:6b:2::26 isc.org. MX +nostat +noquestion +noanswer +noadditional +noauthority +norecurse +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY status: NOERROR id: 49469
;; flags: qr aa; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: f85cdb2962d7015b01000000646749e2a39075f6a89e9408 (good)
myPro:~ andreas$
```

```
myPro:~ andreas$ dig @2620:fe::fe isc.org. MX +nostat +noquestion +noanswer +noadditional +noauthority +dnssec

; <<>> DiG 9.18.11 <<>> @2620:fe::fe isc.org. MX +nostat +noquestion +noanswer +noadditional +noauthority +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY status: NOERROR id: 44777
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
myPro:~ andreas$
```

# Digging broken DNSSEC

```
myPro:~ andreas$ dig @2620:fe::fe fail01.dnssec.works. AAAA +nostat +noquestion +noadditional +noauthority

; <<>> 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: 65108
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

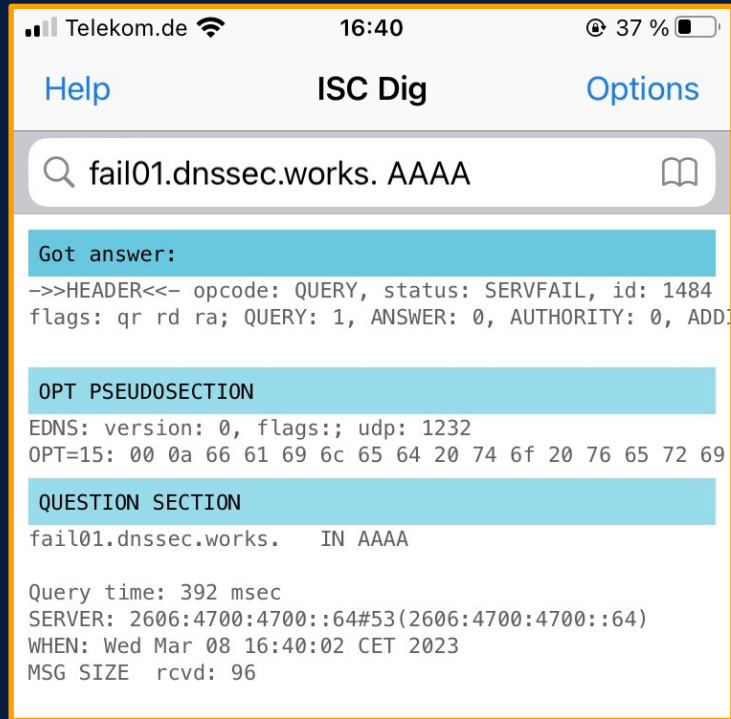
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
; EDE: 10 (RRSIGs Missing)
```

```
myPro:~ andreas$ 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: 64638
;; 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
```

# What else?



<https://apps.apple.com/us/app/isc-dig/id1115648880>

## kdig – Advanced DNS lookup utility

### Synopsis

`kdig [common-settings] [query [settings]]...`

`kdig -h`

### Description

This utility sends one or more DNS queries to a nameserver. Each query can have individual *settings*, or it can be specified globally via *common-settings*, which must precede *query* specification.

[https://www.knot-dns.cz/docs/2.6/html/man\\_kdig.html](https://www.knot-dns.cz/docs/2.6/html/man_kdig.html)

```
$ dog example.com A NS MX TXT
A example.com.          18h34m32s  93.184.216.34
NS example.com.         1d0h00m00s  "a.iana-servers.net."
NS example.com.         1d0h00m00s  "b.iana-servers.net."
A a.iana-servers.net.   14m08s + 199.43.135.53
AAAA a.iana-servers.net. 25m23s + 2001:500:8f::53
A b.iana-servers.net.   7m03s + 199.43.133.53
AAAA b.iana-servers.net. 5m11s + 2001:500:8d::53
MX example.com.         23h53m37s  0 ""
TXT example.com.        1d0h00m00s  "v=spf1 -all"
```

<https://dns.lookup.dog/>

# What's next?

---

DHCP Security Considerations	25% (8)
Low-Risk DNSSEC Implementation Plan	15% (5)
<b>Kea the Next-Gen DHCP</b>	<b>31% (10)</b>
IPAM Security Considerations	28% (9)

**32 responses**

# 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 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
  
```

- **Ekim Maurer** – „Why DDI needs to change“
- **Jens Hoffrichter** – „Lessons Learned for smooth Transition“
- **Tim Rooney** – „DDI Intent Driven Networking“
- **Peter Lowe** – „DNS Abuse Techniques Matrix“
- **Sif Baksh** – „The Power of DDI Automation“
- **Vadim Pavlov** – „The ioc2rpz Community“



# Thank you for your Time.



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