

TCPDump DNS Output Resolution

Guy Bruneau

- The maximum allowable size for a UDP DNS response is 512 bytes.
- Minimum of 20 bytes reserved for IP header
- Eight must be reserved for UDP header
- This leaves 484 bytes for the DNS message
- IF the DNS datagram response exceeds 484 bytes, the response returns an answer with the truncated bit turned on.
- The information will then be passed on via TCP protocol. Blocking inbound traffic to tcp port 53 will prevent unauthorized zone transfers. This will also prevent any external host from resolving large responses.

Trace 1

```
host.my.com.321 dns.my.com.domain: 1+ (35)
Ident field (1)
Recursion Desired (+)
Length (35)
```

Trace 2

```
h.root-servers.net.domain dns.my.com.domain: 12420-
Ident field (12420)
Recursion not available (-)
```

Trace 3

```
seeker.net.domain dns.my.com.domain: 12421*1/3/3
This is an authoritative answer (*)
One answer/ three authoritative records/three additional records (1/3/3)
```

Trace 4

```
dns.verbose.com.domain dns.my.com.domain: 18033|7/0/0 (494) (DF)
DNS ID field (18033)
DNS record has been truncated (|)
One answer/ three authoritative records/three additional records (7/0/0)
Length (494)
Don't Frag bit set (DF)
```

Trace 5

```
query.net.2002 dns1.my.com.domain: 1243 inv_q+ [b2&3=0x980] A? . (27)
DNS ID field (1243)
Inverse query with recursion desired (inv_q+)
Bytes (b2&3)
```

TCPDump DNS Output Resolution

Guy Bruneau

Hex value (0x980)

Address query type A (See chart below) and it is a query (?)

Length (27)

Trace 6

dns1.my.com.domain query.net.2002: 1243 inv_qRefused [0q] 1/0/0 (27)

DNS ID (1243)

Inverse query (inv_q)

Positive ID. The name server responded to the query. (Refused)

No question (0q)

One answer/zero authoritative records/no additional records (1/0/0)

Length (27)

PRIVATE Na me (Type)	Numeric Value	Description	Type?	Query type?
A	1	IP address	*	*
NS	2	Name server	*	*
CNAME	5	Canonical name	*	*
PTR	12	Pointer record	*	*
HINFO	13	Host info	*	*
MX	15	Mail exchange record	*	*
AXFR	252	Request for zone transfer		*
or ANY	255	Request for all records		*