BIND-USERS and Other Debugging Experiences

Mark Andrews
Internet Systems Consortium
Mark_Andrews@isc.org
http://isc.org

BIND-USERS and Other Debugging Experiences

We will look at some typical debugging experiences from bind-users@isc.org as well as other public mailing lists. This will be done as a series of case studies.

We will then look at what, if any, conclusions can be drawn from these.

Case Study 1: WWW.REBUJIA.COM.CO

Hi Group

I need help for a question which is killing me!! I configured BIND 8 on CentOS for my web site and BIND resolves fine for some users but doesn’t in other cities.

this the result for dig:

Case Study 1: WWW.REBUJIA.COM.CO

```
# dig myhost.myserver.com.co

; <<>> DiG 9.3.2 <<>> myhost.myserver.com.co

;; QUESTION SECTION:
;myhost.myserver.com.co.          IN      A

;; ANSWER SECTION:
myhost.myserver.com.co.   7244    IN      A       xxxx.xxxx.xxxx.xxxx

;; AUTHORITY SECTION:
co.                     45247   IN      NS      cmcl2.nyu.edu.
        [snipped]

;; ADDITIONAL SECTION:
        [snipped]
```

Case Study 1: WWW.REBUJIA.COM.CO

Where could be the error?? Is a problem of the foreign ISP of my clients??

Please help and thanks in advanced!!!

Case Study 1: WWW.REBUJIA.COM.CO

The first step is extracting the required information out of the poster. At this stage most of the list has become fed up with requests for help that hide information necessary to actually proceed so the response is something like this:

Sorry all our crystal balls are broken.

If you want help I suggest that you stop hiding the necessary information to even start a diagnosis.

Case Study 1: WWW.REBUJIA.COM.CO

Sorry Barry, Mark

I used to hide info for security reasons, but you're right!!

This is the info for the domain which is in troubles
www.rebujia.com.co

Some people can open the site and others just don't do

Case Study 1: WWW.REBUJIA.COM.CO

```
# dig www.rebujia.com.co

; <<>> DiG 9.3.2 <<>> www.rebujia.com.co

;; QUESTION SECTION:
;www.rebujia.com.co.           IN      A

;; ANSWER SECTION:
www.rebujia.com.co.     842     IN      CNAME   proxy.rebujia.com.co.
proxy.rebujia.com.co.   842     IN      A       201.234.69.219

;; AUTHORITY SECTION:
      [snipped]

;; ADDITIONAL SECTION:
      [snipped]

;; Query time: 40 msec
;; SERVER: 200.30.115.163#53(200.30.115.163)
;; WHEN: Wed Jul  4 22:25:28 2007
;; MSG SIZE  rcvd: 292
```

Case Study 1: WWW.REBUJIA.COM.CO

What could be wrong?

Thanks in advanced

Case Study 1: WWW.REBUJIA.COM.CO

Having the real name of the problem domain it comes down to simple queries. Initially a "dig +trace www.rebujia.com.co"which, usually, gives the nameservers for the zone as known by the parent servers and the zone itself.

```
rebujia.com.co.        43200   IN      NS      dns1.consulcom.com.co.
rebujia.com.co.        43200   IN      NS      proxy.rebujia.com.co.
rebujia.com.co.        43200   IN      NS      chester.consulcom.com.co.
;; Received 139 bytes from 200.31.69.106#53(MINTAKA.UNIANDES.EDU.co) in 285
ms
```

```
www.rebujia.com.co.    604800  IN      CNAME   proxy.rebujia.com.co.
proxy.rebujia.com.co.  604800  IN      A       201.234.69.219
rebujia.com.co.        604800  IN      NS      proxy.rebujia.com.co.
;; Received 86 bytes from 201.234.69.219#53(proxy.rebujia.com.co) in 332 ms
```

Case Study 1: WWW.REBUJIA.COM.CO

This shows a basic configuration error. That being that the NS lists in the parent and child zones do not match.

This should have been caught by the CO registry as part of meeting their RFC 1034 operational requirements. This is not to single out CO; many registries fail to meet this obligation on them.

RFC 1034: 4.2.2. Administrative considerations

As the last installation step, the delegation NS RRs and glue RRs necessary to make the delegation effective should be added to the parent zone. The administrators of both zones should insure that the NS and glue RRs which mark both sides of the cut are consistent and remain so.

Case Study 1: WWW.REBUJIA.COM.CO

Querying each server listed the parent zone showed that one of them, chester.consulcom.com.co, did not have a address record for proxy.rebujia.com.co. This was the reason lookups for www.rebujia.com.co "failed" some of the time.

Case Study 1: WWW.REBUJIA.COM.CO

```
; <<>> DiG 9.3.4 <<>> +norec www.rebujia.com.co @chester.consulcom.com.co
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 50952
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.rebujia.com.co.            IN      A

;; ANSWER SECTION:
www.rebujia.com.co.     86400   IN      CNAME   proxy.rebujia.com.co.

;; AUTHORITY SECTION:
rebujia.com.co.         86400   IN      SOA     chester.consulcom.com.co. root.rebujia.com.co. 2005103103 10800 3600
604800 86400

;; Query time: 312 msec
;; SERVER: 200.21.82.114#53(200.21.82.114)
;; WHEN: Thu Jul  5 13:47:03 2007
;; MSG SIZE  rcvd: 115
```

Case Study 1: WWW.REBUJIA.COM.CO

Further investigation showed that the SOA records were also not consistent.

% dig +short soa rebujia.com.co @chester.consulcom.com.co

chester.consulcom.com.co. root.rebujia.com.co. 2005103103 10800 3600 604800 86400

% dig +short soa rebujia.com.co @dns1.consulcom.com.co

chester.consulcom.com.co. root.rebujia.com.co. 2005103103 10800 3600 604800 86400

% dig +short soa rebujia.com.co @proxy.rebujia.com.co

proxy.rebujia.com.co. root.rebujia.com.co. 2006031601 28800 7200 604800 86400

Case Study 1: WWW.REBUJIA.COM.CO

Alternatively "dig +trace www.rebujia.com.co" could have queried chester.consulcom.com.co returning a negative response. Note the SOA record.

```
rebujia.com.co.        43200   IN      NS      proxy.rebujia.com.co.
rebujia.com.co.        43200   IN      NS      chester.consulcom.com.co.
rebujia.com.co.        43200   IN      NS      dns1.consulcom.com.co.
;; Received 139 bytes from 157.253.1.13#53(CDCNET.UNIANDES.EDU.co) in 1583 ms

www.rebujia.com.co.    86400   IN      CNAME   proxy.rebujia.com.co.
rebujia.com.co.        86400   IN      SOA     chester.consulcom.com.co.
root.rebujia.com.co. 2005103103 10800 3600 604800 86400
;; Received 115 bytes from 200.21.82.114#53(chester.consulcom.com.co) in 757 ms
```

Case Study 1: WWW.REBUJIA.COM.CO

In this case the procedure would have been the same except that you look for nameservers which supply the address records.

This one could have been diagnosed by a automatic zone checking tool like that at http://www.dnsstuff.com/ (http://www.dnsreport.com/).

Case Study 1: WWW.REBUJIA.COM.CO

If you were managing a caching server and had to have lookups succeed then a short term operational work around would have been to add a forward zone for REBUJIA.COM.CO which directed queries to PROXY.REBUJIA.COM.CO (201.234.69.219) only.

```
zone "REBUJIA.COM.CO" {
        type forward;
        forwarders { 201.234.69.219; };
        forward only;
};
```

Case Study 2: WATERCO.COM.MY

In this case email was failing to waterco.com.my. "named" was able to get a response but dig was failing.

Case Study 2: WATERCO.COM.MY

Hi guys,

We've been unable to send mails to waterco.com.my and mails always bounce back saying that its a DNS issue. Digging further, we can get a response via 'dig wa terco.com.my' but no responses via 'dig @ns1.waterco.com.my waterco.com.my mx' or 'dig @ns2.waterco.com.my waterco.com.my mx'. Is there any logic to this? We seem to think that its probably some weird firewall issue but have no experience troubleshooting these cases.

Case Study 2: WATERCO.COM.MY

```
# dig waterco.com.my mx

; <<>> DiG 9.4.0 <<>> waterco.com.my mx

;; QUESTION SECTION:
;waterco.com.my.                IN      MX

;; ANSWER SECTION:
waterco.com.my.         3600    IN      MX      10 mx.waterco.com.my.

;; AUTHORITY SECTION:
waterco.com.my.         3597    IN      NS      ns2.waterco.com.my.
waterco.com.my.         3597    IN      NS      ns1.waterco.com.my.

;; ADDITIONAL SECTION:
mx.waterco.com.my.      3600    IN      A       60.51.231.187
```

Case Study 2: WATERCO.COM.MY

```
# dig @ns1.waterco.com.my waterco.com.my mx

; <<>> DiG 9.4.0 <<>> @ns1.waterco.com.my waterco.com.my mx
; (1 server found)
;; global options:  printcmd
;; connection timed out; no servers could be reached
```

I’ve contacted the domain owner but they seem to say that everything’s alright at their end. Can anybody help verify if you guys are also seing the same thing? Any assistance rendered is greatly appreciated. Thanks!

Case Study 2: WATERCO.COM.MY

At first this looked like a simple bad firewall issue. Using "dig -b 0.0.0.0#<port>" got responses for some ports and not others.

Case Study 2: WATERCO.COM.MY

dig +norec mx waterco.com.my +dnssec @60.51.231.186

09:11:14.198020 220.239.253.18.62437 > 60.51.231.186.53: 48867 [1au] MX? waterco.com.my. (43)

09:11:19.198128 220.239.253.18.62437 > 60.51.231.186.53: 48867 [1au] MX? waterco.com.my. (43)

dig -b0.0.0.0#23002 +norec mx waterco.com.my +dnssec @60.51.231.186

09:11:23.178069 220.239.253.18.23002 > 60.51.231.186.53: 29989 [1au] MX? waterco.com.my. (43)

09:11:23.557357 60.51.231.186.53 > 220.239.253.18.23002: 29989* 1/2/4 MX mx.waterco.com.my. 10 (146)

Case Study 2: WATERCO.COM.MY

The solution to this would have been to add firewall rules which let though

DNS queries and the responses before any blocking rules

e.g. For IPFW

allow udp from any to 60.51.231.186/31 port 53 in
allow udp from 60.51.231.186/31 port 53 to any out
allow tcp from any to 60.51.231.186/31 port 53 in
allow tcp from 60.51.231.186/31 port 53 to any out
<add blocking rules here>

Case Study 2: WATERCO.COM.MY

Others however pointed out responses with bad source ports.

$ dig @ns1.waterco.com.my waterco.com.my mx

;; reply from unexpected source: 60.51.231.186#1077, expected 60.51.231.186#53

;; reply from unexpected source: 60.51.231.186#1077, expected 60.51.231.186#53

;; reply from unexpected source: 60.51.231.186#1077, expected 60.51.231.186#53

Case Study 2: WATERCO.COM.MY

Which leads me to believe that there is a broken NAT implementation in front of the nameserver.

Case Study 3: BLUEPAGES.COM.SA

In this example we are looking at why queries for bluepages.com.sa sometimes fail and why a "rndc flush" makes queries work again.

Case Study 3: BLUEPAGES.COM.SA

Dear List,

I have a problem with my DNS cache which I can’t know exactly what it is.

Today a record could not be resolved and when I issued the command "rndc flush" the server started resolving again

Here is the record I was trying to resolve

Case Study 3: BLUEPAGES.COM.SA

```
; <<>> DiG 9.3.3rc2 <<>> bluepages.com.sa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 936
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bluepages.com.sa.              IN      A

;; ANSWER SECTION:
bluepages.com.sa.       85233   IN      A       207.106.22.33

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jan 30 12:42:37 2007
;; MSG SIZE  rcvd: 50
```

Case Study 3: BLUEPAGES.COM.SA

I have posted something like this earlier and it was solved by setting the ncache to 1 now i think it is back again, however the named -4 didn’t really help doing anything

I have bind V8 as well and it never faces this problem

Do I need to send more information?

Thank you

Case Study 3: BLUEPAGES.COM.SA

Performing a "dig +trace bluepages.com.sa" shows dig complaining about there being no addresses for ns1.egysol.com.

```
bluepages.com.sa.       172800  IN      NS      ns2.egysol.com.
bluepages.com.sa.       172800  IN      NS      ns1.egysol.com.
;; Received 80 bytes from 147.28.0.39#53(RIP.PSG.COM) in 3955 ms
```

dig: couldn’t get address for ’ns1.egysol.com’: not found

As the zone worked some of the time this was indication of one of two errors.

- 1. a glue only address record.
- 2. a broken load balance that incorrectly returns "Name Error" (NXDOMAIN) for AAAA queries.

Case Study 3: BLUEPAGES.COM.SA

In this case it was that ns1.egysol.com and ns2.egysol.com don't exist according to the servers for egysol.com. There are glue A records in the COM zone for them.

The stand response is:

Complain to the administrators of the egysol.com zone that there are missing records address records for ns1.egysol.com and ns2.egysol.com.

Case Study 3: BLUEPAGES.COM.SA

```
% dig ns egysol.com @a.gtld-servers.net

; <<>> DiG 9.3.2-P2 <<>> ns egysol.com @a.gtld-servers.net

;; QUESTION SECTION:
;egysol.com.                    IN      NS

;; ANSWER SECTION:
egysol.com.             172800  IN      NS      ns1.egysol.net.
egysol.com.             172800  IN      NS      ns2.egysol.net.

;; ADDITIONAL SECTION:
ns1.egysol.net.         172800  IN      A       216.246.41.231
ns2.egysol.net.         172800  IN      A       216.246.41.232

;; Query time: 461 msec
;; SERVER: 2001:503:a83e::2:30#53(2001:503:a83e::2:30)
;; WHEN: Wed Jan 31 00:00:00 2007
```

Case Study 3: BLUEPAGES.COM.SA

```
% dig ns1.egysol.com @216.246.41.231

; <<>> DiG 9.3.2-P2 <<>> ns1.egysol.com @216.246.41.231
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 65104
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ns1.egysol.com.                        IN      A

;; AUTHORITY SECTION:
egysol.com.             86400   IN      SOA     ns1.egysol.net. root.server.egysol.net.
2006082801 86400 7200 3600000 86400

;; Query time: 229 msec
;; SERVER: 216.246.41.231#53(216.246.41.231)
```

Case Study 3: BLUEPAGES.COM.SA

And as commonly happens when you start looking at zone containing a misconfiguration. You will find that there are multiple errors. In this case if you query using the glue records from the COM zone you finde that the nameservers also do not match.

Case Study 3: BLUEPAGES.COM.SA

```
% dig bluepages.com.sa mx @207.106.22.124

; <<>> DiG 9.3.2-P2 <<>> bluepages.com.sa mx @207.106.22.124

;; QUESTION SECTION:
;bluepages.com.sa.              IN      MX

;; ANSWER SECTION:
bluepages.com.sa.       86400   IN      MX      10 mail.bluepages.com.sa.

;; AUTHORITY SECTION:
bluepages.com.sa.       86400   IN      NS      ns1.rapidns.com.
bluepages.com.sa.       86400   IN      NS      ns2.rapidns.com.

;; ADDITIONAL SECTION:
mail.bluepages.com.sa.  86400   IN      A       207.106.22.33
ns1.rapidns.com.        86400   IN      A       207.106.22.124
```

Case Study 4: EXAMPLE.COM

This one comes from the dnssec-deployment deployment list. Where there was a assumption that EXAMPLE.COM would be a good test domain for the ISC's DLV registry. A quick check showed that lookups for EXAMPLE.COM were failing. Named was also logging validation errors.

Case Study 4: EXAMPLE.COM

I’ve turned on DLV and am now seeing the following in my lame servers log:

05-Jun-2007 14:15:02.305 not insecure resolving ’example.com/DNSKEY/IN’: 2001:4f8:3::9#53

05-Jun-2007 14:15:02.305 no valid KEY resolving ’ns.sql1.example.com/A/IN’: 2001:4f8:0:2::13#53

05-Jun-2007 14:15:02.481 no valid RRSIG resolving ’example.com/DNSKEY/IN’: 204.152.184.64#53

05-Jun-2007 14:15:02.574 no valid RRSIG resolving ’example.com/DNSKEY/IN’: 204.152.184.135#53

05-Jun-2007 14:15:02.676 no valid RRSIG resolving ’example.com/DNSKEY/IN’: 192.83.249.98#53

05-Jun-2007 14:15:02.789 no valid RRSIG resolving ’example.com/DNSKEY/IN’: 204.152.188.234#53

05-Jun-2007 14:15:02.893 no valid RRSIG resolving ’example.com/DNSKEY/IN’: 2001:4f8:0:2::13#53

Case Study 4: EXAMPLE.COM

A quick check of the DLV record for EXAMPLE.COM at EXAMPLE.COM.DLV.ISC.ORG. showed one DLV record for a DNSKEY with a key id of 6228.

; <<>> DiG 9.5.0a5 <<>> example.com.dlv.isc.org dlv +noall +answer

;; global options: printcmd

example.com.dlv.isc.org. 2789 IN DLV 6228 5 1 B280187CD54405313E1DD0A01D7017E541423B84

Checking the DNSKEY records for EXAMPLE.COM showed two DNSKEY records none of which had a matching key id. To get dig to display the key id I used the +multiline option.

Case Study 4: EXAMPLE.COM

```
; <<>> DiG 9.5.0a5 <<>> example.com dnskey +noall +answer +multi
;; global options:  printcmd
example.com.            3600 IN DNSKEY 256 3 5 (
                        AwEAAc0bKpCWMGAAELhoPW5GUPS7rrG7y91RaNv3Mhk8
                        yRcBX5mu8/dEinnJUdzTBQ1N60I4K51M7IH467uFAzjm
                        PW5vQvirmwP1tUSFO/TmVvEsrIkW74cAaA0CY9P3gJEt
                        vsHk2Y+SSD/3KjEVPTpEPzNAUDj6WZ+BkLA6HX7VOfXV
                        ) ; key id = 25227
example.com.            3600 IN DNSKEY 257 3 5 (
                        AQPH6gSh2qGkyvF4U+PNqeYBMNNkHBc3EUI435vdYjlj
                        Nap3E7OsOUm3W1I9ZYRksZK2jnYUdKL0J+RJaApI8cxu
                        WA2jnttxEfIRklAidRa90SbX5EgsBOt2mWcwJ5i4HEfa
                        f0i9ONuPBpTEB4KpjOP9VSCbeBuCBZvccJbQojdzhw==
                        ) ; key id = 59910
```

Case Study 4: EXAMPLE.COM

A valid trust linkage should look like this. In this case there are two DLV records, with different hashes, for the DNSKEY with id 59910. This corresponds to the DNSKEY with the KSK bit (0x0001) set in flags. I've also add +dnssec to show the RRSIG records.

```
; <<>> DiG 9.5.0a6 <<>> example.com.dlv.isc.org dlv +noall
+answer +dnssec
;; global options:  printcmd
example.com.dlv.isc.org.    3469    IN      DLV     59910 5 1
0988FD7DEF5CAD0D05AE7285032C9F7F8D8189F2
example.com.dlv.isc.org.    3469    IN      DLV     59910 5 2
C7CBF21EAB99EE42C5D3D5A6AA68A1189981AD5EA228E52856F8
94928C72
example.com.dlv.isc.org.    3469    IN      RRSIG   DLV 5 5 3600
20070806233248 20070707233248 52578 dlv.isc.org.
```

Case Study 4: EXAMPLE.COM

```
; <<>> DiG 9.5.0a6 <<>> example.com dnskey +noall +answer +multi +dnssec
;; global options:  printcmd
example.com.            3527 IN DNSKEY 256 3 5 (
                        AwEAAc0bKpCWMGAAELhoPW5GUPS7rrG7y91RaNv3Mhk8
                        yRcBX5mu8/dEinnJUdzTBQ1N60I4K51M7IH467uFAzjm
                        PW5vQvirmwP1tUSFO/TmVvEsrIkW74cAaA0CY9P3gJEt
                        vsHk2Y+SSD/3KjEVPTpEPzNAUDj6WZ+BkLA6HX7VOfXV
                        ) ; key id = 25227
example.com.            3527 IN DNSKEY 257 3 5 (
                        AQPH6gSh2qGkyvF4U+PNqeYBMNNkHBc3EUI435vdYjlj
                        Nap3E7OsOUm3W1I9ZYRksZK2jnYUdKL0J+RJaApI8cxu
                        WA2jnttxEfIRklAidRa90SbX5EgsBOt2mWcwJ5i4HEfa
                        f0i9ONuPBpTEB4KpjOP9VSCbeBuCBZvccJbQojdzhw==
                        ) ; key id = 59910
example.com.            3527 IN RRSIG DNSKEY 5 2 3600 20070621185816 (
                        20070522185816 25227 example.com.
                        <SIGNATURE> )
example.com.            3527 IN RRSIG DNSKEY 5 2 3600 20070621185816 (
```

Case Study 4: EXAMPLE.COM

While this example involved the DLV record. Identical analysis is applicable to a regular secure delegation involving the DS record.

Case Study 5: UM

This appeared recently on the dns-operations list. It appeared to be a attempt to convert UM over to DNSSEC.

Case Study 5: UM

To start with there were some basic DNS problems that should have been addressed before any attempt was made.

The three servers list in the root are consistant w.r.t. plain DNS. The fourth server (unldns.unl.edu, only listed in the um zone) isn't configured to serve UM.

Case Study 5: UM

% dig ns um +short

flag.ep.net.

unldns.unl.edu.

ns.isi.edu.

berkeley.ip4.int.

% dig +nssearch um

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server ns.isi.edu in 160 ms.

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server berkeley.ip4.int in 200 ms.

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server flag.ep.net in 194 ms.

%

Case Study 5: UM

```
% dig soa um @unldns.unl.edu +norec

; <<>> DiG 9.3.4 <<>> soa um @unldns.unl.edu +norec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 6483
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;um.                            IN      SOA

;; Query time: 250 msec
;; SERVER: 129.93.1.1#53(129.93.1.1)
;; WHEN: Mon Jul 16 08:36:16 2007
;; MSG SIZE  rcvd: 20
```

Case Study 5: UM

The DNSSEC coversion itself raised issues.

Of the 3 servers listed in the root only one of them is DNSSEC enabled.

- ns.isi.edu is running BIND 8.3.3 so it needs to be upgraded.
- berkeley.ip4.int is running BIND 9.3.1 so it needs dnssec to be enabled.

Case Study 5: UM

% dig +nssearch um +dnssec

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server ns.isi.edu in 162 ms.

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server flag.ep.net in 200 ms.

RRSIG SOA 5 1 86400 20070810143321 20070711143321 64982 um. <SIGNATURE> from server flag.ep.net in 201 ms.

SOA flag.ep.net. hostmaster.nic.um. 2006120115 43200 3600 1209600 86400 from server berkeley.ip4.int in 201 ms.

%

Conclusions

Most DNS errors are more visible from outside.

Most DNS errors are detectable in the regular checks that should be being performed.

Types of check to perform plain zones.

- NS record checks with and without EDNS and DO
- A record checks with and without EDNS and DO
- AAAA record checks with and without EDNS and DO
- Check that the serial numbers match.

If you get a FORMERR to the EDNS checks repeat the check within 30 seconds to check that the clienthas not been black listed.

Note the address record checks should be performed even for non-glue.

Conclusions

Multiple source ports need to be tested with including but not limited to:

- port 53
- rpc ports
- botnet C&C ports

Conclusions

Types of additional checks to perform DNSSEC zones.

- DNSKEY/DS/DLV record checks match. If KSK bits are set that you have DS/DLV records for all KSK DNSKEYS.
- Check that all servers for the zone have DNSSEC enable.

Acknowledgements

Clip art from <http://www.webweaver.nu/clipart/>.

RFC 1034: 4.2.2. Administrative considerations

As the last installation step, the delegation NS RRs and glue RRs necessary to make the delegation effective should be added to the parent zone. The administrators of both zones should insure that the NS and glue RRs which mark both sides of the cut are consistent and remain so.

HOW DO WE GET THIS ENFORCED?