

## Re: Event ID: 5504

**Source:** <http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2004-07/0245.html>

---

**From:** InBan (*InBan\_at\_discussions.microsoft.com*)

**Date:** 07/06/04

Date: Mon, 5 Jul 2004 19:27:03 -0700

Its good to know I'm not the only one this is nagging at. Some of the other guys in IT in my organization didn't seem very interested in trying to pin this one down, but there is just something about it that bothers me.

A note on my config; no forwarders to external servers are used, all clients use only internal DNS. Internal DNS servers are configured to use root hints. 127.0.0.1 is not used to specify a DNS server in the servers IP Config. Internal DNS servers are configured to use themselves, by their static assigned IP, and their peers.

Here is some real food for thought. Check out the details of this packet capture. The first packet is a query sent to a root hint server (source and destination are the ip of the internal DNS server and the gateway). The second packet is the response from the root hint. The response is from a different root hint than the query was sent to, there are just so many of these I just grabbed two, they are all essentially identical.

(note I doctored it a little because I don't like exposing my internal IP addresses to the world, though a determined individual could pull the info from the hex, it would be rather pointless.):

Frame 25976 (69 bytes on wire, 69 bytes captured)

Arrival Time: Jun 30, 2004 12:04:27.340885000

Time delta from previous packet: 0.000065000 seconds

Time since reference or first frame: 133.065232000 seconds

Frame Number: 25976

Packet Length: 69 bytes

Capture Length: 69 bytes

Ethernet II, Src: 00:0x:xx:xx:xx:xx, Dst: 00:x0:xx:x0:xx:xx

Destination: 00:x0:xx:x0:xx:xx (192.168.xx.xxx)

Source: 00:0x:xx:xx:xx:xx (192.168.xx.x)

Type: IP (0x0800)

Internet Protocol, Src Addr: 192.168.xx.x (192.168.xx.x), Dst Addr: 192.228.79.201 (192.228.79.201)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 55

Identification: 0xd92a (55594)

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0  
Time to live: 128  
Protocol: UDP (0x11)  
Header checksum: 0x742f (correct)  
Source: 192.168.xx.x (192.168.xx.x)  
Destination: 192.228.79.201 (192.228.79.201)  
User Datagram Protocol, Src Port: 1273 (1273), Dst Port: domain (53)  
Source port: 1273 (1273)  
Destination port: domain (53)  
Length: 35  
Checksum: 0x3382 (correct)  
Domain Name System (query)  
Transaction ID: 0x217b  
Flags: 0x0000 (Standard query)  
0... .. = Response: Message is a query  
.000 0... .. = Opcode: Standard query (0)  
... ..0. .... = Truncated: Message is not truncated  
... ..0 .... = Recursion desired: Don't do query recursively  
... .. .0. .... = Z: reserved (0)  
... .. ..0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
localhost: type A, class inet  
Name: localhost  
Type: Host address  
Class: inet

0000 00 c0 9f 10 de 21 00 06 5b fd 9d 97 08 00 45 00 .....!..[.....E.  
0010 00 37 d9 2a 00 00 80 11 74 2f c0 a8 1c 06 c0 e4 .7.\*....t/.....  
0020 4f c9 04 f9 00 35 00 23 33 82 21 7b 00 00 00 01 O....5.#3.!{....  
0030 00 00 00 00 00 00 09 6c 6f 63 61 6c 68 6f 73 74 .....localhost  
0040 00 00 01 00 01 .....

---

Frame 25984 (144 bytes on wire, 144 bytes captured)  
Arrival Time: Jun 30, 2004 12:04:27.404963000  
Time delta from previous packet: 0.021646000 seconds  
Time since reference or first frame: 133.129310000 seconds  
Frame Number: 25984  
Packet Length: 144 bytes  
Capture Length: 144 bytes  
Ethernet II, Src: 00:x0:xx:x0:xx:xx, Dst: 00:0x:xx:xx:xx:xx  
Destination: 00:0x:xx:xx:xx:xx (192.168.xx.x)  
Source: 00:x0:xx:x0:xx:xx (192.168.xx.xxx)  
Type: IP (0x0800)  
Internet Protocol, Src Addr: 192.112.36.4 (192.112.36.4), Dst Addr: 192.168.xx.x (192.168.xx.x)  
Version: 4

Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..0. = ECN-Capable Transport (ECT): 0  
    .... ...0 = ECN-CE: 0  
Total Length: 130  
Identification: 0x66c4 (26308)  
Flags: 0x00  
    ..0. = Don't fragment: Not set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 128  
Protocol: UDP (0x11)  
Header checksum: 0x1284 (correct)  
Source: 192.112.36.4 (192.112.36.4)  
Destination: 192.168.xx.x (192.168.xx.x)  
User Datagram Protocol, Src Port: domain (53), Dst Port: 1273 (1273)  
Source port: domain (53)  
Destination port: 1273 (1273)  
Length: 110  
Checksum: 0x5556 (correct)  
Domain Name System (response)  
Transaction ID: 0x217b  
Flags: 0x8403 (Standard query response, No such name)  
    1... .. = Response: Message is a response  
    .000 0... .. = Opcode: Standard query (0)  
    .... .1.. .. = Authoritative: Server is an authority for domain  
    .... ..0. .... = Truncated: Message is not truncated  
    .... ...0 .... = Recursion desired: Don't do query recursively  
    .... .... 0... .. = Recursion available: Server can't do recursive queries  
    .... .... .0.. .... = Z: reserved (0)  
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server  
    .... .... .... 0011 = Reply code: No such name (3)  
Questions: 1  
Answer RRs: 0  
Authority RRs: 1  
Additional RRs: 0  
Queries  
    localhost: type A, class inet  
        Name: localhost  
        Type: Host address  
        Class: inet  
Authoritative nameservers  
    <Root>: type SOA, class inet, mname A.ROOT-SERVERS.NET  
        Name: <Root>  
        Type: Start of zone of authority  
        Class: inet  
        Time to live: 1 day  
        Data length: 64  
        Primary name server: A.ROOT-SERVERS.NET  
        Responsible authority's mailbox: NSTLD.VERISIGN-GRS.COM

Serial number: 2004062901  
Refresh interval: 30 minutes  
Retry interval: 15 minutes  
Expiration limit: 7 days  
Minimum TTL: 1 day

```
0000 00 06 5b fd 9d 97 00 c0 9f 10 de 21 08 00 45 00 ..[.....!..E.  
0010 00 82 66 c4 00 00 80 11 12 84 c0 70 24 04 c0 a8 ..f.....p$...  
0020 1c 06 00 35 04 f9 00 6e 55 56 21 7b 84 03 00 01 ...5...nUV!{....  
0030 00 00 00 01 00 00 09 6c 6f 63 61 6c 68 6f 73 74 .....localhost  
0040 00 00 01 00 01 00 00 06 00 01 00 01 51 80 00 40 .....Q..@  
0050 01 41 0c 52 4f 4f 54 2d 53 45 52 56 45 52 53 03 .A.ROOT-SERVERS.  
0060 4e 45 54 00 05 4e 53 54 4c 44 0c 56 45 52 49 53 NET..NSTLD.VERIS  
0070 49 47 4e 2d 47 52 53 03 43 4f 4d 00 77 73 92 b5 IGN-GRS.COM.ws..  
0080 00 00 07 08 00 00 03 84 00 09 3a 80 00 01 51 80 .....:....Q.
```

The expiration, retry and refresh interval have to do with the frequency/regularity of the messages. But I don't know what is setting those values.

Ian Bagnald  
MCSE:Security  
MCSA:Security  
COMPITA A+

"Ace Fekay [MVP]" wrote:

```
> In news:85E4036F-4D2E-41EA-8E23-AE830696B5DF@microsoft.com,  
> InBan <InBan@discussions.microsoft.com> asked for help and I offered my  
> suggestions below:  
> > Sorry for the slow response. No it is not a single label domain, and  
> > yes secure against cache pollution is enabled. Actually my first  
> > concern when I saw all those errors was cache poisoning, but I'm  
> > convinced that is not the case. If this is a configuration issue, its  
> > not an obviouse one, and if its an issue with the Windows DNS  
> > implementation, its not (well) published.  
> >  
> >  
> > This is an elusive issue. I understand as well that if it were an illegal  
> > character in a client, and the client were to register, then I believe it  
> > would appear as if the DNS server itself is querying to the Root servers,  
> > assuming (none of us have asked your config yet) that you have all your  
> > machines using your DNS, but assuming you don't have a forwarder configured.  
> > Please correct me if my assumption is incorrect. Not saying it would or  
> > would not fix it, but do you have forwarding configured? IF you do, try  
> > removing it, but from the looks, it seems that you may not?  
> >  
> > As for the localhost resolution, that seems odd that it would try to query  
> > the Roots for it. Do you by chance have 127.0.0.1 as your DNS address? I  
> > guess it would be prudent if we can ask for some config info, such as an  
> > ipconfig /all, is DNS mutlihomed, if so, is it performing NAT, and anything  
> > else you can think of that may or may not be relevant at first glance.
```

>  
> Also, as Kevin mentioned earlier, a saturated link can cause this. If during  
> the time the errors popped up, can you recall if there is heavy Internet  
> traffic across your link, such as file transfers, or something else? Do you  
> have logging set or anyway to check bandwidth usage by time/date stamp? Most  
> ISPs offering T1s have some sort of administration page that show  
> statistics, etc. I remember one guy called me with a saturated link that  
> wound up being a server that gotted 'pubbed'. It got pubbed twice. Two  
> separate instances. I removed both and it cleaned it up, but he wasn't  
> getting 5504s since his forwarding scheme was to his main office and not  
> from that location. So maybe if in a situation where there's saturation or a  
> DNS server overloaded, it could retrieve a valid packet, but due to  
> corruption, DNS is translating it as something else and results in that  
> error. Just maybe that hotfix takes care of this, but as for regression  
> testing as Natalie asked previously, I don;t know anyone that has applied  
> it, nor has anyone posted any issues about it as of yet.  
>  
> Hope we can come down to a resolution here. 5504's come up time to time, but  
> they wind up being an internal client name issue, but not from what you're  
> describing, and frankly, believe it or not, I thought about this off and on  
> all weekend.  
>  
>  
> --  
> Regards,  
> Ace  
>  
> Please direct all replies ONLY to the Microsoft public newsgroups  
> so all can benefit.  
>  
> This posting is provided "AS-IS" with no warranties or guarantees  
> and confers no rights.  
>  
> Ace Fekay, MCSE 2000, MCSE+I, MCSA, MCT, MVP  
> Microsoft Windows MVP – Active Directory  
>  
> HAM AND EGGS: A day's work for a chicken;  
> A lifetime commitment for a pig.  
> --  
> =====  
>  
>  
>