

## Re: Event ID: 7050

**Source:** <http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2004-09/0083.html>

---

**From:** Ace Fekay [MVP] (*PleaseSubstituteMyActualFirstNamehotmail.com*)

**Date:** 09/02/04

Date: Thu, 2 Sep 2004 18:55:29 -0400

In news:%23SjBu9PkeHA.704@TK2MSFTNGP09.phx.gbl,  
Joan <anonymous@discussions.microsoft.com> made a post then I commented below

> *Hi Ace,*

>

> *I think that was my post at EventID, matches what I submitted. We've  
> gotten a few more 7050 errors that was not my co-worker doing a port  
> probe -- the new 7050 events happened at about 2:30 am and 3:30 am  
> est 6 days apart on all four DNS servers (two are AD empty root, two  
> are AD child) at HQ. Interestingly, too, even though all 4 servers in  
> same switch, our 2 AD Root servers also reported 7050 on two other  
> days at 11 am and 2 pm respectively, whereas the child servers did  
> not. The 11 am and 2pm I can possibly see as port probes (most of HQ  
> is software engineers), but 2:30 am and 3:30 am?*

>

> *None of the DNS servers are public, all internal and AD structure  
> hidden from Internet. DNS looks fine, no one is having problems, no  
> other errors (System, Application, Directory Service, NTFS, Security  
> logs).*

>

> *I still think first occurrence was port probe, too much coincidence  
> that 7050 occurred on every DNS server exactly when port probe done.  
> But I'm back to investigating cause of newest 7050s, if same cause or  
> not. Did a Google search, saw this thread and thought I'd post the  
> additional info. Still investigating.*

>

> *No need to reply.*

>

> *Regards,*

> *Joan*

Hmm, at a lost, because this is a new one and there's little on it.

According to this article:

<http://www.oriweb.com/updateip.htm>

It has something to do with dynamic updates. Maybe those are the times that the netlogon service from a particular DC is trying to update into DNS.

And another link I found, someone mentions it maybe a Winsock driver based error.

[http://www.mail-archive.com/imap\\_forum@list.ipswitch.com/msg89439.html](http://www.mail-archive.com/imap_forum@list.ipswitch.com/msg89439.html)

Now, if you isolate the machine that is trying the updates (netmon? retina?) and take a look at the NIC config, drivers, etc, maybe that can be a start? Determine if any DCs or DNS servers have multiple NICs, or teamed NICs, etc, for a start as well. Another link mentions the 'birthday' attack against BIND servers. But doesn't seem likely in your case, since its MS DNS.

--

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 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP

Microsoft Windows MVP - Windows Server - Directory Services

Security Is Like An Onion, It Has Layers

HAM AND EGGS: A day's work for a chicken;

A lifetime commitment for a pig.

--

=====