Subject: [PATCH] Freeing alive inet6 address
Posted by den on Fri, 07 Sep 2007 10:21:18 GMT
View Forum Message <> Reply to Message

From: Denis V. Lunev <den@openvz.org>

addrconf_dad_failure calls addrconf_dad_stop which takes referenced address
and drops the count. So, in6_ifa_put perrformed at out: is extra. This
results in message: "Freeing alive inet6 address" and not released dst entries.

Signed-off-by: Denis V. Lunev <den@openvz.org>
Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>

```
--- ./net/ipv6/ndisc.c.ipv6dad 2007-09-03 16:54:32.000000000 +0400
+++ ./net/ipv6/ndisc.c 2007-09-07 13:34:30.000000000 +0400
@@ -736,7 +736,7 @@ static void ndisc_recv_ns(struct sk_buff
      * so fail our DAD process
      */
     addrconf_dad_failure(ifp);
-    goto out;
+    return;
    } else {
     /*
      * This is not a dad solicitation.
```

Subject: Re: [PATCH] Freeing alive inet6 address
Posted by davem on Tue, 11 Sep 2007 09:08:18 GMT
View Forum Message <> Reply to Message

From: "Denis V. Lunev" <den@openvz.org>
Date: Fri, 7 Sep 2007 14:21:18 +0400

> From: Denis V. Lunev <den@openvz.org>
>
> addrconf_dad_failure calls addrconf_dad_stop which takes referenced address
> and drops the count. So, in6_ifa_put perrformed at out: is extra. This
> results in message: "Freeing alive inet6 address" and not released dst entries.
>
> Signed-off-by: Denis V. Lunev <den@openvz.org>
> Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>

I've seen this bug myself just a week before heading to
Europe for conferences and intended to look into it.

Thanks a lot for fixing this, patch applied.