Subject: Re: Re: [PATCH] Copy mac_len in skb_clone() as well
Posted by dev on Thu, 15 Mar 2007 10:19:00 GMT
View Forum Message <> Reply to Message

David Miller wrote:
> From: Alexey Dobriyan <adobriyan@sw.ru>
> Date: Wed, 14 Mar 2007 16:07:11 +0300
>
>
>>ANK says: "It is rarely used, that's wy it was not noticed.
>>But in the places, where it is used, it should be disaster."
>>
>>Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>
>
>
> Applied.
>
> What bug triggered that helped you discover this? Or is it
> merely from a code audit?
Ohhh, it is a fairy-tale to tell the truth :)
We had some unexplainable problems with java application in OpenVZ kernel.
It didn't work sometimes, but worked fine (!) with CONFIG_SLAB_DEBUG.
Alexey blamed java :), but ...
Then we found that poising one of the bits in slab cache was curing it.
After that we found that the problem is related to fclone cache.
And then we found that not all the fields are initialized during cloning.
The bug was related to our own skb->field we introduced,
but we analyzed the code and found this as well.

Thanks,
Kirill