

---

Subject: Re: [PATCH] vlan: fix potential race in vlan\_cleanup\_module vs  
vlan\_ioctl\_handler

Posted by [davem](#) on Tue, 11 Dec 2007 10:41:38 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

From: Patrick McHardy <kaber@trash.net>

Date: Tue, 11 Dec 2007 11:38:38 +0100

> Pavel Emelyanov wrote:  
> > AFAIS there's a tiny race window between these two  
> > calls - after rtnl unregistered all the vlans, but  
> > the ioctl handler isn't set to NULL yet, user can  
> > manage to call this ioctl and create one vlan device,  
> > and that this function will later BUG\_ON seeing  
> > non-empty hashes.  
>  
> Indeed, I can't see anything preventing this.  
>  
> > I think, that we must first close the vlan ioctl  
> > and only after this remove all the vlans with the  
> > vlan\_netlink\_fini() call.  
>  
> That looks correct, thanks Pavel. Dave, please apply.

Applied to net-2.6, thanks!

---