Subject: Re: [PATCH] vlan: fix potential race in vlan_cleanup_module vs vlan_ioctl_handler
Posted by Patrick McHardy on Tue, 11 Dec 2007 10:38:38 GMT
View Forum Message <> Reply to Message

Pavel Emelyanov wrote:
> The vlan module cleanup function starts with
>
> vlan_netlink_fini();
> vlan_ioctl_set(NULL);
>
> The first call removes all the vlan devices and
> the second one closes the vlan ioctl.
>
> 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-emply 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.