Subject: Re: [PATCH 3/3] Fix race in ipv6_flowlabel_opt() when inserting two labels
Posted by davem on Thu, 18 Oct 2007 12:19:19 GMT
View Forum Message <> Reply to Message

From: Pavel Emelyanov <xemul@openvz.org>
Date: Thu, 18 Oct 2007 15:59:14 +0400

> In the IPV6_FL_A_GET case the hash is checked for flowlabels
> with the given label. If it is not found, the lock, protecting
> the hash, is dropped to be re-get for writing. After this a
> newly allocated entry is inserted, but no checks are performed
> to catch a classical SMP race, when the conflicting label may
> be inserted on another cpu.
>
> Use the (currently unused) return value from fl_intern() to
> return the conflicting entry (if found) and re-check, whether
> we can reuse it (IPV6_FL_F_EXCL) or return -EEXISTS.
>
> Also add the comment, about why not re-lookup the current
> sock for conflicting flowlabel entry.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

Applied.