

Re: current panics when Netgear WG511T ejected

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2007-03/msg00620.html>

- *From:* "Bruce M. Simpson" <bms@xxxxxxxxxxx>
 - *Date:* Tue, 27 Mar 2007 01:41:52 +0100
-

Tom Uffner wrote:

slightly different this time, but it still panics. seems to be trying to delete nonexistent addresses. should it even be here? i don't have any multicast addrs defined, just one dhcp-assigned unicast addr.

Yup, it should be there.

The IP stack will always join 224.0.0.1, this is standards compliant behaviour. Even if you have no multicast addresses explicitly configured by yourself or any application, the multicast code is always used on any system configured with INET.

I believe this new patch should fix your panic. Because the hardware is being ejected, the netinet part of the stack won't see the detach first, but net will, and this is where the panic is happening.

In this particular case, net is doing the cleanup because of the unexpected detach. It looks like it is the ll_ifma which is causing problems. The problem with ll_ifma is that it is also linked into the if_multiaddrs tailq; we must link AF_LINK addresses in this tailq or things like joining a link-layer group alone will not work. As such it will get seen twice by the same function but in a different role.

Previously FreeBSD would just leak memory instead of panicking in situations like this. I rewrote this code to null out the ifp's when ifnet was detached, so that netinet could detect the detach of the underlying layer, and not try to reenter the net code improperly; this was particularly important to avoid bad situations with locking. If the interface needs Giant, the locking is particularly nasty.

Regards,
BMS

--- //depot/vendor/freebsd/src/sys/net/if.c 2007/03/20 03:17:45

+++ //depot/user/bms/netdev/sys/net/if.c 2007/03/27 00:40:17

@@ -2512,21 +2512,27 @@

/*

- * If the ifnet is detaching, null out references to ifnet,
- * so that upper protocol layers will notice, and not attempt
 - * to obtain locks for an ifnet which no longer exists.
 - * It is OK to call rt_newmaddrmsg() with a NULL ifp.
 - + * to obtain locks for an ifnet which no longer exists. The
 - + * routing socket announcement must happen before the ifnet

Re: current panics when Netgear WG511T ejected

```
+ * instance is detached from the system.
*/
if (detaching) {
#ifdef DIAGNOSTIC
printf("%s: detaching ifnet instance %p\n", __func__, ifp);
#endif
- ifma->ifma_ifp = NULL;
+ /*
+ * ifp may already be nulled out if we are being reentered
+ * to delete the ll_ifma.
+ */
+ if (ifp != NULL) {
+ rt_newmaddrmsg(RTM_DELMADDR, ifma);
+ ifma->ifma_ifp = NULL;
+ }
}

if (--ifma->ifma_refcount > 0)
return 0;

- rt_newmaddrmsg(RTM_DELMADDR, ifma);
-
/*
* If this ifma is a network-layer ifma, a link-layer ifma may
* have been associated with it. Release it first if so.
```

freebsd-current@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-current>

To unsubscribe, send any mail to "freebsd-current-unsubscribe@xxxxxxxxxxxxx"