The new KCSAN (concurrency sanitizer) reported a problem with the TT code: [https://lists.open-mesh.org/pipermail/b.a.t.m.a.n/2019-November/019024.html](https://lists.open-mesh.org/pipermail/b.a.t.m.a.n/2019-November/019024.html)

Hello,

syzbot found the following crash on:

```
HEAD commit: 05f223688657b18495d0213b8247010c17e1e8ed x86, kcsan: Enable KCSAN for x86
git tree: https://github.com/google/ktsan.git kcsan
console output: https://syzkaller.appspot.com/x/log.txt?x=1195a0d4e00000
kernel config: https://syzkaller.appspot.com/x/.config?x=87d11955f40591f
dashboard link: https://syzkaller.appspot.com/bug?extid=1d5dadec56d9e87f0aac
compiler: gcc (GCC) 9.0.0 20181231 (experimental)
```

Unfortunately, I don't have any reproducer for this crash yet.

**IMPORTANT:** if you fix the bug, please add the following tag to the commit:

```
Reported-by: syzbot+1d5dadec56d9e87f0aac@syzkaller.appspotmail.com
```

```
write to 0xffff8880a8e19698 of 2 bytes by task 10064 on cpu 0:
batadv_tt_local_add+0x21b/0x1020 net/batman-adv/translation-table.c:799
__netdev_start_xmit include/linux/netdevice.h:4420 [inline]
netdev_start_xmit include/linux/netdevice.h:4434 [inline]
xmit_one net/core/dev.c:3280 [inline]
dev_hard_start_xmit+0x149/0x2b0 net/core/dev.c:3296
__dev_queue_xmit+0x149/0x2b0 net/core/dev.c:3307
netdev_start_xmit include/linux/netdevice.h:4434 [inline]
xmit_one net/core/dev.c:3280 [inline]
```

```
read to 0xffff8880a8e19698 of 2 bytes by task 9969 on cpu 1:
batadv_tt_local_add+0x3d1/0x1020 net/batman-adv/translation-table.c:801
batadv_interface_tx+0x398/0xae0 net/batman-adv/soft-interface.c:249
__netdev_start_xmit include/linux/netdevice.h:4420 [inline]
```
The relevant code is:

```c
if (batadv_is_wifi_hardif(in_hardif))
    tt_local->common.flags |= BATADV_TT_CLIENT_WIFI;
else
    tt_local->common.flags &= ~BATADV_TT_CLIENT_WIFI;
```

So removing and adding this flag is not correctly protected with a method which prevents data races.