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

Hello,

syzbot found the following crash on:

HEAD commit: 05f22368 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=87d1195ff40591f
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+0x1e6/0x3296
__dev_queue_xmit+0x4a9/0x710 net/core/filter.c:2106
__bpf_clone_redirect net/core/filter.c:2111
bpf_prog_bb15b996d00816f9+0x71c/0x1000
bpf_test_run+0x1c3/0x490 net/bpf/test_run.c:44
bpf_prog_test_run_skb+0x44a/0x840 net/bpf/test_run.c:310
bpf_prog_test_run kernel/bpf/syscall.c:2108 [inline]
do_sys_bpf+0x1664/0x2b90 kernel/bpf/syscall.c:2884
__se_sys_bpf kernel/bpf/syscall.c:2825 [inline]
x64_sys_bpf+0x4c/0x600 kernel/bpf/syscall.c:2825
do_syscall_64+0x70c/0x770 arch/x86/entry/common.c:290
entry_SYSCALL_64_after_hwframe+0x144/0xa9

read to 0xffff8880a8e19689 of 2 bytes by task 9969 on cpu 1:

batadv_tt_local_add+0x3d1/0x1020 net/batman-adv/translation-table.c:799
__netdev_start_xmit include/linux/netdevice.h:4420 [inline]
xmit_one net/core/dev.c:3280 [inline]

02/18/2020
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.