**Description**

I got a kernel panic on my vkernel trying to ping6 another vkernel on the same host. I might have done an incorrect network configuration, but I guess it shouldn't panic anyway.

Here is what I've done.

Two fresh vkernels with ipv6_enable=yes in rc.conf started with:

```
/boot/kernel/kernel -m 1g -r /vhost/vm0.img -I /var/run/vknet
```

and

```
/boot/kernel/kernel -m 1g -r /vhost/vm1.img -I /var/run/vknet
```

vknetd is executed as "/usr/sbin/vknetd -U -t tap0".

I run the following version of DragonFly (on all three machines: host and both vkernels):

```
# uname -a
DragonFly 5.8-RELEASE DragonFly v5.8.0rc1.28.g3e3e37-RELEASE #2: Sun Mar 1 17:46:44 CET 2020 root@fi.zta.lk:/usr/obj/usr/src/sys/VKERNEL64 x86_64
```

On one of the vkernels I first check that I can ping the other one:

```
# ping6 fe80::201:68ff:fef8:f5f8%vke0
PING6(56=40+8+8 bytes) fe80::201:68ff:fef8:f5f8%vke0 --> fe80::201:71ff:fe0c:f607%vke0
16 bytes from fe80::201:71ff:fe0c:f607%vke0, icmp_seq=1 hlim=64 time=0.371 ms
16 bytes from fe80::201:71ff:fe0c:f607%vke0, icmp_seq=2 hlim=64 time=0.262 ms
^C
--- fe80::201:71ff:fe0c:f607%vke0 ping6 statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/std-dev = 0.262/0.317/0.371/0.054 ms
```

Then do the following to get the panic:

```
# route add -inet6 fe80::201:71ff:fe0c:f607 -iface vke0
add host fe80::201:71ff:fe0c:f607: gateway vke0
```

```
# ping6 fe80::201:71ff:fe0c:f607
PING6(56=40+8+8 bytes) fe80::201:68ff:fef8:f5f8%vke0 --> fe80::201:71ff:fe0c:f607%vke0
16 bytes from fe80::201:68ff:fef8:f5f8%vke0, icmp_seq=1 hlim=64 time=0.371 ms
16 bytes from fe80::201:68ff:fef8:f5f8%vke0, icmp_seq=2 hlim=64 time=0.262 ms
panic: assertion "sdl->sdl_family == AF_LINK && sdl->sdl_alen != 0" failed in nd6_resolve at /usr/src/sys/netinet6/nd6.c:2031
```

CPU0 stopping CPUs: 0x0000000000000002
stopped
Stopped at 0x70bde9: movb $0,0xa0c83c(%rip)
db> trace
Debugger() at 0x70bde9
panic() at 0x4c7710
nd6_resolve() at 0x60ab55
ether_output_frame() at 0x59427c
ip6_output() at 0x6026a1
rip6_output() at 0x610e9f
rip6_output() at 0x611446
netmsg_sync_handler() at 0x5a1739

--
Aleksej Lebedev