Table of Contents

Improving Fault Tolerance - Bypass Mode Network Cards

Why do you recommend purchasing SILICOM cards?
The reasons are as follows:

- The cards have bypass functionality.
- The delivery package can include licenses for the required drivers for maximum performance - DPDK & Libzero. These cards are marked with -SQ1 (example for a 10GbE card).

Does bypass work on SILICOM network cards when the power is off?

- Optical bypass - works when the power is off (tested on the PE210G2BPI9-SR-SQ1 short-range/fiber card).
- Copper bypass - works when the power is off (tested on the PEG6BPi6 card).

Is there manual control of bypass on SILICOM network cards?
DPI manages the bypass automatically.
If necessary, manual control of the bypass is possible using the bpctl_util utility:

- bpctl_util all get_bypass - get the state of bypass
- bpctl_util all set_bypass on - activate bypass
- bpctl_util all set_bypass off - deactivate bypass

Problem: we purchased a used card and the bypass does not work, what should we do?
The problem is related to the card being reconfigured as a standard one, i.e., with bypass functionality disabled.
Diagnosis:

```
bpctl_util all get_std_nic
07:00.0 standard
07:00.1 slave
07:00.2 standard
07:00.3 slave
```

It should be non-standard.

To set the card to bypass mode, perform the following:

```
bpctl_util all set_std_nic off
```

This command switches the mode to non-standard, i.e., with bypass mode enabled.

Explanation regarding bypass switching time?
Activating the bypass takes a short time interval of about 0.5 seconds (by default), but due to interface renegotiation, it can ultimately take a longer time interval. Below is an explanation regarding bypass switching from the manufacturer.
Such switching duration can affect BGP, OSPF, and other mechanisms due to a brief connection interruption (duration may vary, see the description below) or multiple interruptions as in the case of

server or service reboot (*service →interruption→bypass→interruption→ service*). In this case, the session recovery time (BGP, OSPF) depends on their settings and can take up to several tens of seconds. To reduce this interval, you need to configure the session recovery time after a connection break. **For example**, on Juniper equipment, set hold-timer down to 500ms to avoid BGP session termination and routing table reconfiguration:

```
set interfaces <ifname> hold-time up 500 down 500
```

where 500 ms is the wait timeout before the operational status of the interface changes.

```
Basically, the time for the bypass mechanism to switch from one mode to
another is 10mS.
The timing that you are seeing relates to re-establishing the link and then
re-establishing
the connection (with new routing tables in switches and devices).
This switch to bypass mode is done in our product by physically connecting
the pair of
ports together (wire to wire). This means that when this happens, our
product is actually out
of the picture, and the start of the traffic with this new connection will
depend on
the two networking devices (router / switch / device) on how they link
together and how
they establish the connection again. You can try to force fix mode (not
auto-neg,
change to force 1G FD or so) this might reduce the time needed for the
negotiation.
Not sure how much.
For the change from bypass mode to normal mode - all the above also stand as
well.
The networking devices (router / switch / device) lose the link with each
other and
start establishing the connection with the Silicom NIC. Here you have more
control as
the link is done between the two devices and your system (Check that all the
devices
are set to the same speed settings).
From our customer and our experience, a 1-3 second time is reasonable to get
the Copper 1G link
to be established between 2 network devices.
```

Everything is fine except that one port on the network works in bypass mode and does not filter traffic.
If it is configured (in/out_dev) but does not switch, try resetting the bypass switch on the card to its initial state:

```
bpctl_util all set_bypass off
bpctl_util all set_dis_bypass off
bpctl_util all set_bypass_pwoff on
bpctl_util all set_bypass_pwup on
bpctl_util all set_std_nic off
```

```
bpctl_util all get_bypass_change on
bpctl_util all get_tx on
bpctl_util all get_tpl off
bpctl_util all get_wait_at_pwup off
bpctl_util all get_hw_reset off
bpctl_util all get_disc off
bpctl_util all get_disc_change off
bpctl_util all get_dis_disc off
bpctl_util all get_disc_pwup off
bpctl_util all get_wd_exp_mode bypass
bpctl_util all get_wd_autoreset disable
```

If it doesn't help, the card is defective, replace it under warranty.

Configuring Juniper so that switching to and from bypass does not lead to route reconfiguration.

```
set interfaces <ifname> hold-time up 500 down 500

show xe-5/2/0
 description "-= 20G UPLINK LAGG =-";
hold-time up 1000 down 1000;
gigether-options {
 802.3ad ae1;
}
```

Configuring Cisco so that switching to and from bypass does not lead to route reconfiguration.

```
int fa0/0
ip bgp fast-external-fallover deny
```

Note:

```
The BGP Fast-external-fallover command terminates external BGP sessions of
any directly adjacent peer if the link used to reach the peer goes down
without waiting for the hold-down timer to expire.
```

List of all dna interfaces and their MAC addresses
grep ^ /sys/class/net/dna?/address

How to check if the card is equipped with bypass
To check for the presence of bypass, run the command:

```
lspci -v|grep -A1 Eth
```

For cards with bypass, the Subsystem field will indicate:

```
Subsystem: Silicom Ltd. Device
```