QUANTUM

15 June 2023

LIGHTSPEED 10/25/40/100G QSFP28 PORTS

Administration Guide

CHECK POINT™

[Classification: Protected]

Check Point Copyright Notice

© 2022 - 2023 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.



LightSpeed 10/25/40/100G QSFP28 Ports Administration Guide



Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
15 June 2023	Updated: ■ *"Known Limitations" on page 42* - the TCPdump option "`-Q {in | out | inout}`" is not supported on the 100G Ports.
11 June 2023	Added information about the LightSpeed Appliances MLS200 and MLS400
04 June 2023	■ Changed the product name from "NVIDIA ConnectX 100G" to "2-Port Dual-Width 10/25/40/100G" ■ Changed the document title from "NVIDIA ConnectX 100G QSFP28 Ports Administration Guide" to "LightSpeed 10/25/40/100G QSFP28 Ports Administration Guide"
04 December 2022	Updated: ■ *"Known Limitations" on page 42* - correction from "breakout (DAC) cables" to "copper or fiber breakout cables"
01 December 2022	Updated: ■ *"Mapping of 100G Ports and Interface Names in Gaia OS" on page 9*
22 November 2022	Added: ■ *"Configuring SecureXL" on page 16* Updated: ■ *"Known Limitations" on page 42*
25 September 2022	Updated: ■ *"Known Limitations" on page 42*
18 September 2022	Updated: ■ *"Monitoring the 100G Ports" on page 23* ■ *"Monitoring Accelerated Connections with the CPView Tool" on page 29* ■ *"Monitoring Accelerated Connections with the "fwaccel" Command" on page 35* ■ *"Capturing Traffic with TCPdump" on page 39* ■ *"Known Limitations" on page 42*
30 August 2022	Added: ■ *"Viewing Connections Not Accelerated in Hardware" on page 38*
15 July 2022	Added: ■ *"Monitoring Accelerated Connections with the CPView Tool" on page 29* ■ *"Monitoring Accelerated Connections with the "fwaccel" Command" on page 35* ■ *"Known Limitations" on page 42*

Date	Description
01 June 2022	Updated: ■ *"Installing and Removing the 100G Card" on page 8* ■ *"Mapping of 100G Ports and Interface Names in Gaia OS" on page 9* ■ *"Monitoring the 100G Ports" on page 23* ■ *"Capturing Traffic with TCPdump" on page 39*
22 April 2022	Updated: ■ Rebranding - New Check Point logo ■ *"Monitoring the 100G Ports" on page 23*
17 January 2022	First release of this document

Table of Contents

Introduction ... *7*
Installing and Removing the 100G Card ... *8*
Mapping of 100G Ports and Interface Names in Gaia OS ... *9*
Configuring SecureXL ... *16*
SecureXL in Kernel Mode (KPPAK) ... *16*
SecureXL in User Mode (UPPAK) ... *17*
Viewing the Current SecureXL Mode ... *18*
Changing the Current SecureXL Mode ... *19*
Disabling SecureXL ... *20*
Monitoring the 100G Ports ... *23*
Viewing the Hardware Information for 100G Cards in CPView Tool ... *23*
Viewing the 100G Ports in CPView Tool ... *25*
Viewing the SecureXL Status for 100G Ports ... *26*
Viewing the Summary ... *27*
Monitoring Accelerated Connections with the CPView Tool ... *29*
Viewing the Traffic Rate and Concurrent Accelerated Connections ... *29*
Viewing the Top Accelerated Connections ... *31*
Viewing the Comparison Statistics for Accelerated Connections ... *32*
Viewing the Reasons for Non-Accelerated Traffic ... *34*
Monitoring Accelerated Connections with the "fwaccel" Command ... *35*
Viewing the Accelerated Connections ... *35*
Viewing the Statistics Summary for Accelerated Connections ... *36*
Viewing the Statistics for Accelerated Connections ... *37*
Viewing Connections Not Accelerated in Hardware ... *38*
Capturing Traffic with TCPdump ... *39*
Capturing Only the Accelerated Traffic ... *39*
Capturing Only the Non-Accelerated Traffic ... *40*
Capturing Only the Accelerated VLAN Traffic ... *40*
Capturing Accelerated Traffic Without RoCE Packets ... *41*
Known Limitations ... *42*

Introduction

This Administration Guide applies to these appliance models:

Appliance Model	Software Requirements
QLS800, QLS650, QLS450, QLS250	sk176466
MLS400, MLS200	sk176466

This guide uses these abbreviations:

Full Name	Description	Abbreviation
2-Port Dual-Width 10/25/40/100G QSFP28 Card	A dual-width NIC that uses specific pairs of slots in the appliance.	100G Card
10/25/40/100G QSFP28 Port	Port type on the dual-width NIC. In MLS400 appliances, these ports are built-in.	100G Port

In the supported appliance models, the 100G Ports accelerate the connections in hardware when packets are received on one 100G Port and are destined to go out another 100G Port of the same 100G Card.

Installing and Removing the 100G Card

For instructions how to install and remove a 100G Card, see:

Installing and Removing Line Cards

Mapping of 100G Ports and Interface Names in Gaia OS

Important:

- In Gaia OS, port names of the installed cards start from the name "`eth-01`" from the top left slot.
  If a card has several ports, then the port names are from `eth<X>-01` to `ethX-0<Y>`, where `<X>` is the slot number and `<Y>` is the last port number on the card.
- The 100G Card takes two consecutive interface names in Gaia OS.
  For example, if this card is installed in Slots 1+2 of the appliance, then in Gaia OS, the names of ports are based on the first slot's number, as in `eth1-01` and `eth1-02`.
  In addition, the 100G Card reserves the second NIC slot's numbering.
  The names `eth2-01` to `eth2-0<Y>`, as not used.
- You can move the installed cards from their default slots to different slots.
  The 100G Card supports only specific pairs of slots.
- Non-Maestro configuration refers to the connection of Security Appliances directly to your network and to the Check Point Management Server.
- Maestro configuration refers to the connection of Security Appliances to a Quantum Maestro Orchestrator that in turn connects to your network and to the Check Point Management Server.
  To connect to Quantum Maestro Orchestrators, you must use **only** the 100G Ports ports.
  It is **not** supported to connect other ports to Orchestrators.
  It is not necessary to remove other cards from the appliance.
  The appliance ignores other cards when it operates as a Maestro Security Group Member.

QLS800

Slots on the Front Panel (from left to right, from top to bottom):

1	2	3	4
5	6	7	8

By default, this appliance model has these cards installed:

Slots	Card	Names of Ports in Gaia OS - Non-Maestro configuration

1 + 2	100G Card	`eth1-01`
		`eth1-02`
		(`eth2-01:0<Y>` is reserved)

3 + 4	100G Card	`eth3-01`
		`eth3-02`
		(`eth4-01:0<Y>` is reserved)

5 + 6	100G Card	`eth5-01`
		`eth5-02`
		(`eth6-01:0<Y>` is reserved)

7 + 8	100G Card	`eth7-01`
		`eth7-02`
		(`eth8-01:0<Y>` is reserved)

QLS650

Slots on the Front Panel (from left to right, from top to bottom):

1	2	3	4
5	6	7	8

By default, this appliance model has these cards installed:

Slots	Card	Names of Ports in Gaia OS - Non-Maestro configuration

1 + 2	100G Card	`eth1-01`
		`eth1-02`
		(`eth2-01:0<Y>` is reserved)

3 + 4	100G Card	`eth3-01`
		`eth3-02`
		(`eth4-01:0<Y>` is reserved)

5 + 6	100G Card	`eth5-01`
		`eth5-02`
		(`eth6-01:0<Y>` is reserved)

7	10G Card	`eth7-01`
		`eth7-02`
		`eth7-03`
		`eth7-04`

8	10G Card	`eth8-01`
		`eth8-02`
		`eth8-03`
		`eth8-04`

QLS450

Slots on the Front Panel (from left to right, from top to bottom):

1	2	3	4
5	6	7	8

By default, this appliance model has these cards installed:

Slots	Card	Names of Ports in Gaia OS - Non-Maestro configuration	Names of Ports in Gaia OS - Maestro configuration (*)

1 + 2	100G Card	`eth1-01`
		`eth1-02`
		(`eth2-01:0<Y>` is reserved)
			`ethsBP1-01`
			`ethsBP1-02`

3 + 4	100G Card	`eth3-01`
		`eth3-02`
		(`eth4-01:0<Y>` is reserved)
			`ethsBP1-03`
			`ethsBP1-04`

5	10G Card	`eth5-01`
		`eth5-02`
		`eth5-03`
		`eth5-04`
			These ports are **not** supported

6	10G Card	`eth6-01`
		`eth6-02`
		`eth6-03`
		`eth6-04`
			These ports are **not** supported

7	Empty	N / A	N / A
8	Empty	N / A	N / A

(*) You can connect **all** available 100G Ports ports on a Security Appliance to Quantum Maestro Orchestrators on the Maestro Site.

- The first 100G Card card connects to each Orchestrator on the Site:
  - The first port on the card connects to one of the Downlink ports on the first Orchestrator
  - The second port on the card connects to one of the Downlink ports on the second Orchestrator
- The second 100G Card card connects to each Orchestrator on the Site:
  - The first port on the card connects to another Downlink port on the first Orchestrator
  - The second port on the card connects to another Downlink port on the second Orchestrator

QLS250

Slots on the Front Panel (from left to right):

1	2	3	4

By default, this appliance model has these cards installed:

Slots	Card	Names of Ports in Gaia OS - Non-Maestro configuration	Names of Ports in Gaia OS - Maestro configuration (*)

1 + 2	100G Card	`eth1-01`
		`eth1-02`
		(`eth2-01:0<Y>` is reserved)
			`ethsBP1-01`
			`ethsBP1-02`

3	10G Card	`eth3-01`
		`eth3-02`
		`eth3-03`
		`eth3-04`
			These ports are **not** supported

4	10G Card	`eth4-01`
		`eth4-02`
		`eth4-03`
		`eth4-04`
			These ports are **not** supported

(*) You must connect the two 100G Ports ports on a Security Appliance to Quantum Maestro Orchestrators on the Maestro Site:

- The first port on the card connects to one of the Downlink ports on the first Orchestrator
- The second port on the card connects to one of the Downlink ports on the second Orchestrator

MLS400

Notes:

- In this appliance model, the 100G Ports are built-in.

Network Ports on the Front Panel (from left to right):

1	2	Ventilation holes	3	4

By default, this appliance model has these 100G Ports:

Network Port	Port Type	Names of Ports in Gaia OS - Non-Maestro configuration	Names of Ports in Gaia OS - Maestro configuration (*)
1	100G Port	`eth1`	`ethsBP1-01`
2	100G Port	`eth2`	`ethsBP1-02`
3	100G Port	`eth3`	`ethsBP1-03`
4	100G Port	`eth4`	`ethsBP1-04`

(*) You can connect **all** available 100G Ports ports on a Security Appliance to Quantum Maestro Orchestrators on the Maestro Site:

- The 100G Port #1 connects to one of the Downlink ports on the first Orchestrator
- The 100G Port #2 connects to one of the Downlink ports on the second Orchestrator
- The 100G Port #3 connects to one of the Downlink ports on the first Orchestrator
- The 100G Port #4 connects to one of the Downlink ports on the second Orchestrator

MLS200

Network Ports on the Front Panel (from left to right):

1	2	On-board ports

By default, this appliance model has these cards installed and ports:

Slots	Card / Port Type	Names of Ports in Gaia OS - Non-Maestro configuration	Names of Ports in Gaia OS - Maestro configuration (*)

1 + 2	100G Card	`eth1-01`
		`eth1-02`
		(`eth2-01:0<Y>` is reserved)
			`ethsBP1-01`
			`ethsBP1-02`

On-board	On-board	`eth1`
		`eth2`
		`eth3`
		`eth4`
		`eth5`
		`eth6`
		`eth7`
		`eth8`
			These ports are **not** supported

(*) You must connect the two 100G Ports ports on a Security Appliance to Quantum Maestro Orchestrators on the Maestro Site:

- The first port on the card connects to one of the Downlink ports on the first Orchestrator
- The second port on the card connects to one of the Downlink ports on the second Orchestrator

Configuring SecureXL

The Gaia First Time Configuration Wizard automatically installs, enables, and configures SecureXL on your Security Gateway. No additional configuration is required.

SecureXL can work in these modes:

SecureXL Mode	Description
User Mode (UPPAK)	SecureXL runs as processes in the user space (UPPAK - "User Space Performance Pack"). This is the default mode after you install the R81.10 Jumbo Hotfix Accumulator Take 81 or higher. See: ■ *"Viewing the Current SecureXL Mode" on page 18*. ■ *"Changing the Current SecureXL Mode" on page 19*.
Kernel Mode (KPPAK)	SecureXL runs as a kernel module in the kernel space (KPPAK - "Kernel Space Performance Pack"). This is the default mode when you install the R81.10 Jumbo Hotfix Accumulator Takes 61-79. See *"Viewing the Current SecureXL Mode" on page 18*.

SecureXL in Kernel Mode (KPPAK)

SecureXL runs as a kernel module in the kernel space (KPPAK - "Kernel Space Performance Pack").

Description

SecureXL kernel modules:

SecureXL in Kernel Mode uses these kernel modules:

- `$PPKDIR/boot/modules/sim_kern_64_3_10_64.o`
- `$PPKDIR/boot/modules/sim_kern_64_3_10_64_v6.o`

SecureXL configuration file:

SecureXL in Kernel Mode uses this configuration file for its parameters:

- `$PPKDIR/conf/simkern.conf`

SecureXL in User Mode (UPPAK)

SecureXL runs as processes in the user space (UPPAK - "User Space Performance Pack").

Description

Limitations when SecureXL works in User Mode (UPPAK):

See *"Known Limitations" on page 42* > Section *"SecureXL" on page 43*.

SecureXL user space processes:

SecureXL in User Mode uses these processes and log files:

Process	Log File	Description
`$PPKDIR/bin/usim_x86`	`/var/log/usim_x86.elg`	The main SecureXL process.
`$PPKDIR/bin/usim_wd_agent`	N / A	The Watch Dog process that monitors the main SecureXL process "`usim_x86`". If the main process crashes, this Watch Dog process starts it again.
`$PPKDIR/bin/usim_launcher`	N / A	Starts the main SecureXL process "`usim_x86`" during boot.

SecureXL configuration file:

SecureXL in User Mode uses this configuration file for its parameters:

- `$PPKDIR/conf/simkern.conf`

SecureXL core dump files:

SecureXL in User Mode creates these files when its user space processes crash:

- `/var/log/dump/usermode/usim_x86.<PID>.core`
- `/var/log/dump/usermode/lcore-worker<ID>.core`
- `/var/log/dump/usermode/fwk_snd<ID>.core`
- `/var/log/usim_crash/crash_list`

Viewing the Current SecureXL Mode

Procedure

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Examine the SecureXL status and mode. `fwaccel stat`
4	Examine the column **Name**: ■ `KPPAK` - Kernel Mode ■ `UPPAK` - User Mode

For information about the "`fwaccel`" command, see the *Performance Tuning Administration Guide* for your version.

Example output:

```
[Expert@MyGW:0]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |enabled    |eth0,eth1,eth2           |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN, |
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256, |
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyGW:0]#
```

Changing the Current SecureXL Mode

You can change the current SecureXL mode between User Mode (UPPAK) and Kernel Mode (KPPAK).

Procedure

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Run: `cpconfig`
4	Enter the number of the **Check Point SecureXL** option.
5	The menu shows the current SecureXL mode.
6	Enter the number of the **Change SecureXL Mode** option.
7	Enter **y** to confirm the change.
8	Exit from the `cpconfig` menu.
9	Reboot.
10	Examine the SecureXL status and mode. `fwaccel stat`

For information about the "`fwaccel`" command, see the *Performance Tuning Administration Guide* for your version.

Disabling SecureXL

It is not supported to disable SecureXL.
You can disable SecureXL only if Check Point Support explicitly instructs you to do so for debug purposes.

Explanation and Procedure

Starting from R80.20, you can disable the SecureXL only *temporarily*.

The SecureXL starts automatically when you start Check Point services (with the `cpstart` command), or reboot the Security Gateway (Scalable Platform Security Group Member).

Important:

- If you disable the SecureXL, this change does **not** survive reboot.
  SecureXL remains disabled until you enable it again on-the-fly, or reboot the Security Gateway.
- If you disable the SecureXL, this change applies only to new connections that arrive after you disabled the acceleration.
  SecureXL continues to accelerate the connections that are already accelerated.
  Other non-connection oriented processing continues to function (for example, virtual defragmentation and VPN decrypt).

For information about the "`fwaccel`" command, see the *Performance Tuning Administration Guide* for your version.

To disable SecureXL for IPv4 temporarily

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Examine the SecureXL status. `fwaccel stat`
4	Disable the SecureXL. `fwaccel off [-a]`
5	Examine the SecureXL status. `fwaccel stat`

To disable SecureXL for IPv6 temporarily

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Examine the SecureXL status. `fwaccel6 stat`
4	Disable the SecureXL. `fwaccel6 off [-a]`
5	Examine the SecureXL status. `fwaccel6 stat`

To enable SecureXL again for IPv4

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Examine the SecureXL status. `fwaccel stat`
4	Enable the SecureXL. `fwaccel on [-a]`
5	Examine the SecureXL status. `fwaccel stat`

To enable SecureXL again for IPv6

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to Gaia Clish, or Expert mode.
3	Examine the SecureXL status. `fwaccel6 stat`
4	Enable the SecureXL. `fwaccel6 on [-a]`
5	Examine the SecureXL status. `fwaccel6 stat`

Monitoring the 100G Ports

For more information about the CPView Tool, see sk101878.

Viewing the Hardware Information for 100G Cards in CPView Tool

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **SysInfo**.
4	In the output, refer to the section **Hardware Information** > sub-section **Devices**.

Example output (truncated):

```
|-------------------------------------------------------------------------------
| CPVIEW.SysInfo
|-------------------------------------------------------------------------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced
|-------------------------------------------------------------------------------
| Configuration Information:
|
| Platform                      Gaia 64Bit
| Configuration                 Check Point Security Gateway
| CoreXL Status                 On
| CoreXL instances              43
| Dynamic Balancing Status      Off
| SecureXL Status               On
| USFW Status                   On
| UPPAK Status                  On
| -----------------------------------------------------------------------------
| General information:
|
| System uptime                 11 days, 18:39:10
| Last policy install time      25Aug2022 19:10:00
| Last policy name              Standard
| -----------------------------------------------------------------------------
| Version Information:
|
| fw1_wrapper package version   R81.10
|
|                Branch Name    Build Number
| FW User Mode   XXX            XXX
| FW Kernel      XXX            XXX
| Accel Module   XXX            XXX
| Adpdrv Module  XXX            XXX
| SIM Module     XXX            XXX
| -----------------------------------------------------------------------------
| Hardware Information:
|
| HW Model  Quantum LightSpeed QLS250
|
| Devices              Type                Slot      Status    Firmware
| Expansion-1          2x100GbE LightSpeed 1         Connected 22.31.2302
```

Viewing the 100G Ports in CPView Tool

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **Network** > **Interfaces** > **Overview**.
4	In the output, refer to the column **Driver**. The 100G Ports use the **mlx5_core** driver.

Example output (truncated):

```
|-------------------------------------------------------------------------------------------------------------
--------------------
| CPVIEW.Network.Interfaces

|-------------------------------------------------------------------------------------------------------------
--------------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced

|-------------------------------------------------------------------------------------------------------------
--------------------
| Traffic Distribution Interfaces Top-Protocols Top-Connections LightSpeed-Top-Connections Templates

|-------------------------------------------------------------------------------------------------------------
--------------------
| Overview Traffic

|-------------------------------------------------------------------------------------------------------------
--------------------
| Interface Information:

|

| Interface      State     Type      Port      Driver    Firmware                  Speed     IPv4
     IPv6
| lo             On        loopback  N/A       N/A       N/A                       N/A       127.0.0.1/8
     Not Configured
| Mgmt           On        ethernet  TP        igb       1.63, 0x8 0.0.0           10000M
192.168.3.59/24    Not Configured
| eth5-01        On        ethernet  OTHER     mlx5_core 22.31.2302                N/A       Not
Configured     Not Configured
| eth5-02        On        ethernet  OTHER     mlx5_core 22.31.2302                N/A       Not
Configured     Not Configured
| eth5-03        On        ethernet  OTHER     mlx5_core 22.31.2302                N/A       Not
Configured     Not Configured
| eth5-04        On        ethernet  OTHER     mlx5_core 22.31.2302                N/A       Not
Configured     Not Configured
```

Viewing the SecureXL Status for 100G Ports

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `fwaccel stat`
3	In the output, refer to these rows: ■ `LightSpeed Accel` Shows the state of the 100G Port acceleration. ■ `LightSpeed Low Latency Mode` Shows how the Host Appliance offloads the connections to the 100G Ports.

Example output:

```
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |UPPAK    |enabled    |Mgmt,mlx7-01,mlx7-02,    |Acceleration,Cryptography    |
|  |         |           |mlx4-01,mlx4-02,mlx5-01, |                             |
|  |         |           |mlx5-02,mlx1-01,mlx1-02, |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |eth7-01,eth7-02,eth4-01, |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |eth4-02,eth5-01,eth5-02, |ESP,LinkSelection,DynamicVPN,|
|  |         |           |eth1-01,eth1-02          |NatTraversal,AES-XCBC,SHA256,|
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+
Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : enabled (Cards:enabled,enabled,enabled,enabled)
LightSpeed Low Latency Mode : disabled
```

Notes:

- By default, the Host Appliance starts to offload the connection to the 100G Ports only after 10 megabytes of traffic passes in this connection.
- An Administrator can enable the "**LightSpeed Low Latency Mode**", in which the Host Appliance starts to offload the connection to the 100G Ports immediately when this connection opens.
- To change the state of the LightSpeed Low Latency Mode, run:

  ```
  fwaccel low_latency {on | off}
  ```

  This command:
  - Applies immediately
  - Does not require a reboot
  - Survives a reboot

Viewing the Summary

Note - This output is intended for Check Point Support only.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
2	Run: `ls_info`

Example:

```
[Expert@Appliance:0]# ls_info
LightSpeed Information:

Number of SmartNIC cards: 4
mlx7-01 firmware-version: 22.31.2302
mlx7-02 firmware-version: 22.31.2302
mlx4-01 firmware-version: 22.31.2302
mlx4-02 firmware-version: 22.31.2302
mlx5-01 firmware-version: 22.31.2302
mlx5-02 firmware-version: 22.31.2302
mlx1-01 firmware-version: 22.31.2302
mlx1-02 firmware-version: 22.31.2302

This is Check Point CPinfo Build 914000227 for GAIA
[PPACK]
        HOTFIX_R81_10_JHF_MAIN       Take:  96

Blades enabled:
fw

Firewall is User mode
SecureXL is in User mode

SecureXL and HW accel status:
|UPPAK |enabled
LightSpeed Accel : enabled (Cards:enabled,enabled,enabled,enabled)
LightSpeed Low Latency Mode : enabled

Dynamic Balancing is currently Off

#fwaccel stats -s
Accelerated conns/Total conns    : 31/31 (100%)
LightSpeed conns/Total conns     : 0/31 (0%)
Accelerated pkts/Total pkts      : 100712/3848813 (2%)
LightSpeed pkts/Total pkts       : 0/3848813 (0%)
F2Fed pkts/Total pkts            : 3748101/3848813 (97%)

#fwaccel stats (cumulative)
hw accel inbound bytes                  0    hw accel packets                        0
hw accel outbound bytes                 0    hw accel conns                          0
hw accel total conns                    0    hw accel tcp conns                      0
hw accel non-tcp conns                  0

LightSpeed Connection Count
Total LightSpeed Conns: 0
LightSpeed Accounting Conns: 0
LightSpeed PXL Conns: 0
LightSpeed Other Conns (all other flags except A,S,N,L): 0

Ipsctl Errors/Drops
net:dev:adp:ipsctl:slot:1:kern:ipsctl:stats:errors:registration = 1
net:dev:adp:ipsctl:slot:1:cpu:0:nip:ingress:stats:rx_vlan_drop = 3
net:dev:adp:ipsctl:slot:1:nip:rx_vlan_drop = 3
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:11:stats:fw_pkt_drops = 10
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:37:stats:fw_pkt_drops = 3
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:36:stats:fw_pkt_drops = 17
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:39:stats:fw_pkt_drops = 21
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:38:stats:fw_pkt_drops = 9
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:1:stats:fw_pkt_drops = 17
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:2:stats:fw_pkt_drops = 6
net:dev:adp:ipsctl:slot:1:fwk_snd:cpu:3:stats:fw_pkt_drops = 17
[Expert@Appliance:0]#
```

Monitoring Accelerated Connections with the CPView Tool

For more information about the CPView Tool, see sk101878.

Note - It can take up to 60 seconds for statistics data about the 100G Ports to accumulate before it appears in CPView.

Viewing the Traffic Rate and Concurrent Accelerated Connections

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **Network** > **Traffic**.
4	In the output, refer to the rows **LightSpeed**. **Note** - The numbers in these rows are accumulative for all installed and enabled 100G Cards and 100G Ports.

Example output (truncated):

```
|-------------------------------------------------------------------------------------------------------------------
---------------
| CPVIEW.Network.Traffic

|-------------------------------------------------------------------------------------------------------------------
---------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced

|-------------------------------------------------------------------------------------------------------------------
---------------
| Traffic Distribution Interfaces Top-Protocols Top-Connections LightSpeed-Top-Connections Templates

|-------------------------------------------------------------------------------------------------------------------
---------------
| Traffic Rate:

|

|              Inbound packets/sec  Outbound packets/sec      Inbound bits/sec     Outbound bits/sec
Connections/sec
| Host                          3                   13                 1,504                  105K
            0
| LightSpeed                91,097                91,097                  992M                  992M
           13
| -------------------------------------------------------------------------------------------------------------------
---------------
| Concurrent Connections:

|

|                                          Connections    Non-TCP         TCP handshake       TCP
established TCP closed
| FW                                                 4          0                     0
   4          0
| Host Streaming                                     0          0                     0
   0          0
| Host SXL (including LightSpeed)                   26          0                     0
  26          0
| LightSpeed                                        26          0                     0
  26          0
| -------------------------------------------------------------------------------------------------------------------
---------------
```

Viewing the Top Accelerated Connections

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **Network** > **Traffic** > **LightSpeed-Top-Connections**.

Example output (truncated):

```
|-------------------------------------------------------------------------------------------
| CPVIEW.Network.LightSpeed-Top-Connections
|-------------------------------------------------------------------------------------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced
|-------------------------------------------------------------------------------------------
| Traffic Distribution Interfaces Top-Protocols Top-Connections LightSpeed-Top-Connections
|-------------------------------------------------------------------------------------------
| LightSpeed Connections distribution summary:
|
| Connection                                  Protocol             Slot     Mbps       pps
| 1.1.1.100:3333 -> 2.2.2.200:22              TCP:ssh              1        0          4
```

Viewing the Comparison Statistics for Accelerated Connections

You can see the comparison statistics for accelerated connections in all 100G Ports.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **Advanced** > **SecureXL** > **Side-by-Side**. **Notes:** ■ This page always shows **four** columns for 100G Ports (even if your appliance has fewer 100G Cards installed). ■ Columns and the corresponding Slots: • "**LightSpeed-1**" refers to Slots 1 + 2. • "**LightSpeed-2**" refers to Slots 3 + 4. • "**LightSpeed-3**" refers to Slots 5 + 6. • "**LightSpeed-4**" refers to Slots 7 + 8. See *"Mapping of 100G Ports and Interface Names in Gaia OS" on page 9*.

Example output (truncated):

```
|-------------------------------------------------------------------------------------------------------------------
--------------------
| CPVIEW.Advanced.SecureXL

|-------------------------------------------------------------------------------------------------------------------
--------------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced

|-------------------------------------------------------------------------------------------------------------------
--------------------
| Logging CPU-Profiler Memory Network SecureXL ClusterXL CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-
Tracker UP HTTP-Parser
|-------------------------------------------------------------------------------------------------------------------
--------------------
| Side-by-Side Drops Backplane Reorder-IS Network-per-CPU Offload-decision F2V-reasons LightSpeed2Host-
Reasons Advanced
|-------------------------------------------------------------------------------------------------------------------
--------------------
| Side-by-Side

|

|

|                                    SND        LightSpeed-1        LightSpeed-2        LightSpeed-3
  LightSpeed-4
| Inbound packets/sec              11,328                 N/A                 N/A                 N/A
          N/A
| Outbound packets/sec                 0                 N/A                 N/A                 N/A
          N/A
| Inbound bits/sec                   121M                 N/A                 N/A                 N/A
          N/A
| Outbound bits/sec                    0                 N/A                 N/A                 N/A
          N/A
| Connections/sec                      0                 N/A                 N/A                 N/A
          N/A
| Concurrent connections             227                 N/A                 N/A                 N/A
          N/A
| Dropped Packets                      0                 N/A                 N/A                 N/A
          N/A
|

| Mbufs Allocated           1,184,040,381
| Mbufs Free                1,183,980,186
|
|                       RTE Mbuf In Use  RTE Mbuf Available
| CPU Socket 0                   68,246             980,327
```

Viewing the Reasons for Non-Accelerated Traffic

You can see the reasons why traffic is not accelerated and is forwarded to the host appliance.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `cpview`
3	From the top, click **Advanced** > **SecureXL** > **LightSpeed2Host-Reasons**.

Example output (truncated):

```
|-------------------------------------------------------------------------------------------------------------
-------------
| CPVIEW.Advanced.SecureXL.LightSpeed2Host-Reasons

|-------------------------------------------------------------------------------------------------------------
-------------
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced

|-------------------------------------------------------------------------------------------------------------
-------------
| Logging CPU-Profiler Memory Network SecureXL ClusterXL CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-
Tracker UP
|-------------------------------------------------------------------------------------------------------------
-------------
| Side-by-Side Drops Backplane Reorder-IS Network-per-CPU Offload-decision F2V-reasons LightSpeed2Host-
Reasons Advanced
|-------------------------------------------------------------------------------------------------------------
-------------
| Reasons LightSpeed accelerated packets are received by host:

|

| Reason                                    Packets

| Invalid TCP header/packet length                1
| Invalid UDP header/packet length                2
| Fragmented Packet                              12
```

Monitoring Accelerated Connections with the "fwaccel" Command

Important - The statistics for connections (packets and bytes) the 100G Ports accelerate, are updated every 60 seconds. You cannot change this interval.

Viewing the Accelerated Connections

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Run: `fwaccel conns -l"` In the output, refer to these columns: ■ `Flags` • The flag "`H`" means "Hardware" - the connection is accelerated in hardware • If the connection is processed on the Host Appliance, then the last flag appears as a period "`.`" ■ `LS Pkts` • This counter shows the number of packets in the connection that the 100G Ports accelerate

Example output:

```
Source          SPort Destination     DPort PR Flags                TCP state        C2S i/f S2C i/f Inst
PPAK ID Policy ID (FW/UP)        CPU LS Pkts     Host Pkts   Host Bytes  Last Seen  Duration   TTL/Timeout
--------------- ----- --------------- ----- -- -------------------- ---------------- -------- -------- ----
------- -----------------        --- ----------- ----------- ----------- ---------- ---------- -----------
      1.1.1.100  3333       2.2.2.200  1234  6 ...................H      Established   17/16    16/17     3
     0 2758591385/1641440335    3           345          3        226B        15s         15s    3575/3590
      2.2.2.200  1234       1.1.1.100  3333  6 ..........L........H      Established   17/16    16/17     3
     0 2758591385/1641440335    3           345          3        226B        15s         15s    3575/3590
```

Viewing the Statistics Summary for Accelerated Connections

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `fwaccel stats -s`
3	In the output, refer to these rows: ■ `Accelerated conns/Total conns` ■ `LightSpeed conns/Total conns` ■ `Accelerated pkts/Total pkts` ■ `LightSpeed pkts/Total pkts` ■ `F2Fed pkts/Total pkts`

Note - The numbers for "`Total pkts`" in these rows are accumulative for all installed and enabled 100G Cards and 100G Ports.

Example output:

```
Accelerated conns/Total conns : 1/25 (4%)
LightSpeed conns/Total conns : 24/25 (96%)
Accelerated pkts/Total pkts   : 2503/106368396 (0%)
LightSpeed pkts/Total pkts    : 106240973/106368396 (99%)
F2Fed pkts/Total pkts         : 124920/106368396 (0%)
F2V pkts/Total pkts              : 0/106368396 (0%)
CPASXL pkts/Total pkts           : 0/106368396 (0%)
PSLXL pkts/Total pkts            : 0/106368396 (0%)
CPAS pipeline pkts/Total pkts    : 0/106368396 (0%)
PSL pipeline pkts/Total pkts     : 0/106368396 (0%)
QOS inbound pkts/Total pkts      : 0/106368396 (0%)
QOS outbound pkts/Total pkts     : 0/106368396 (0%)
Corrected pkts/Total pkts        : 0/106368396 (0%)
```

Viewing the Statistics for Accelerated Connections

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `fwaccel stats`
3	In the output, refer to this section: `LightSpeed Accelerated Path`

Note - The numbers in these rows are accumulative for all installed and enabled 100G Cards and 100G Ports.

Example output (for brevity, only the applicable section is shown):

```
Name                          Value         Name                          Value
----------------------------  ------------  ----------------------------  ------------

LightSpeed Accelerated Path
-------------------------------------------------------------------------------------
hw accel inbound bytes          6799422272    hw accel packets                106240973
hw accel outbound bytes         6799422272    hw accel conns                          0
hw accel total conns                     0    hw accel tcp conns                      0
hw accel non-tcp conns                   0
```

Viewing Connections Not Accelerated in Hardware

You can see which connections are not accelerated in hardware and why.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Run: `fwaccel conns -z`

Example output:

```
Source          SPort Destination     DPort PR C2S i/f S2C i/f Flags      Flags EX    Not LS Accelerated
Reason
--------------- ----- --------------- ----- -- ------- ------- ---------- ----------  ----------------------
----
   192.168.1.3 54920      172.20.4.5  5201  6   16/17   17/16 0x00000000 0x00004000 Flag (PXSXL medpath)
   192.168.1.3 54894      172.20.4.5  5201  6   16/17   17/16 0x00000000 0x00000000 Flag (Threshold)

Idx Interface
--- ---------
  0 lo
  1 Mgmt
  3 eth3-01
  7 eth3-04
 16 eth1-01
 17 eth1-02

Total number of connections: 2
Total number of links: 0
```

Capturing Traffic with TCPdump

This section provides instructions for capturing the traffic that passes through the 100G Ports.

Notes:

- For information about the available TCPdump "*<options>*", see https://www.tcpdump.org/manpages/tcpdump.1.html.
- To capture traffic on a VLAN interface that is configured on a 100G Port, you must specify the VLAN ID in the TCPdump syntax.
  Example for capturing TCP traffic on VLAN 200 configured on port eth1-01:

  ```
  tcpdump -i eth1-01 vlan 200 and tcp
  ```

- When you capture traffic on a Bond interface that is configured on 100G Ports, you cannot see the traffic accelerated from the 100G Ports.
  To see the accelerated traffic, you must run the TCPdump directly on the 100G Ports.
  Example:
  If bond2 consists of the 100G Ports `eth1-01` and `eth1-02`, then to see the accelerated traffic, run:

  ```
  tcpdump -i eth1-01 <options>
  ```

  ```
  tcpdump -i eth1-02 <options>
  ```

- The TCPdump option "`-Q {in | out | inout}`" is not supported on the 100G Ports.

Capturing Only the Accelerated Traffic

You can capture only the traffic that is accelerated in 100G Ports.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Run: `tcpdump [<options>] -i <Name of 100G Port> [<options>]`

Capturing Only the Non-Accelerated Traffic

You can capture only the non-accelerated traffic that is forwarded to the host appliance.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Run: `tcpdump [<options>] -i <Name of 100G Port> --host-only [<options>]`

Capturing Only the Accelerated VLAN Traffic

You can capture only the traffic with VLAN tags that is accelerated in 100G Ports.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.

3	Run:
	`tcpdump [<options>] -i <Name of 100G Port> vlan <VLAN ID> [<options>]`
	Example for eth1-01.200 (VLAN 200 on eth1-01):
	`tcpdump [<options>] -i eth1-01 vlan 200 [<options>]`

Capturing Accelerated Traffic Without RoCE Packets

Traffic capture on 100G Ports may also show the RoCE (RDMA over Converged Ethernet) packets.

You can exclude these RoCE packets from the traffic capture.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Run: `tcpdump [<options>] -i <Name of 100G Port> ether proto not 0x8915 [<options>]`

Known Limitations

Limitations that apply to LightSpeed Appliances that run R81.10 with the R81.10 Jumbo Hotfix Accumulator:

Category	Limitation	Resolved In
Jumbo Hotfix Accumulator		
Jumbo Hotfix Accumulator	**Warning** - It is not supported to uninstall the Jumbo Hotfix Accumulator from a LightSpeed Appliance appliance and reboot. You can only install a higher Take of the Jumbo Hotfix Accumulator.	–
Software Blades		
Firewall	LightSpeed Appliances with 100G Ports are shipped with a license that supports only the Firewall Software Blade. You can purchase licenses for additional Software Blades. However, the 100G Ports accelerate the traffic only for the Firewall Software Blade.	–
QoS	QoS Software Blade not supported.	–
Features		
IPv6	IPv6 traffic is not supported (do **not** enable the IPv6 support in Gaia on the LightSpeed Appliances).	–
Cluster	Cluster is not supported in these modes: ■ ClusterXL Load Sharing (Unicast and Multicast). ■ ClusterXL Active-Active. ■ Multi-Version Cluster (MVC). ■ VRRP Cluster.	–
VSX	VSX mode is not supported.	–
NAT	These NAT features are not supported: ■ NAT64. ■ NAT46.	–
IP Reachability Detection	IP Reachability Detection (Bidirectional Forwarding Detection, BFD) is not supported.	–

Category	Limitation	Resolved In
Policy Based Routing	Policy Based Routing (PBR) is not supported.	–
IoC	It is not supported to use the Threat Prevention Custom Intelligence Feeds feature (sk132193) to import IP Address lists to a blacklist.	
SecureXL Note - UPPAK mode is available from R81.10 Jumbo Hotfix Accumulator Take 81		
Drop Templates	SecureXL Drop Templates (see sk153832) are not supported.	–
Rate Limiting rules	SecureXL Rate Limiting rules for DoS Mitigation (see sk112454) configured with these commands are not supported: ▪ `fwaccel dos deny` ▪ `fwaccel dos allow` ▪ `fwaccel dos rate`	–
Expired connections	When SecureXL works in User Mode (UPPAK), it might take the Security Gateway an additional maximum of 60 seconds to delete expired connections that are accelerated in hardware from the Security Gateway's Connections table. This is by design, to prevent the overhead of reading the hardware too frequently. Example: If you configured the Session Timeout of a service to 40 seconds, it might take the Security Gateway a maximum of 40 seconds + 60 seconds = 100 seconds to delete the expired connections for this service.	–
Traffic statistics	When SecureXL works in User Mode (UPPAK), traffic statistics on the Security Gateway do not contain packets and bytes for connections that are accelerated in hardware. This applies to: ▪ CPView > **Network** > **Interfaces** > **Traffic**. ▪ Output of the "`fwaccel stats -s`" command. Traffic statistics for the physical interface contains packets and bytes for connections that are accelerated in hardware for all VLAN interfaces configured on this physical interface.	–

Category	Limitation	Resolved In
CPU utilization	Output of the "`top`" and "`ps`" commands may show that SecureXL user space processes consume the CPU at 100%. This is because the SecureXL processes are constantly polling the network interface drivers. This does **not** trigger inspection bypass because of a high CPU load. To see the actual CPU utilization, use one of these: ■ The CPView tool (sk101878) on the Security Gateway (click `CPU` > `Overview` > `Host`). ■ SNMP query on the Security Gateway (the OID tree 1.3.6.1.4.1.2620.1.6.7.5). ■ SmartConsole: 1. From the left navigation panel, click **Gateways & Servers**. 2. Right-click the Security Gateway object > click **Monitor**. 3. From the left, open **System Counters** and click **System**.	–
CPU affinities	It is not supported to change the CPU affinities of SecureXL user space processes.	–
USFW and KSFW	If you change the Firewall mode from User Mode (USFW) to Kernel Mode (KSFW), then SecureXL mode changes from User Mode (UPPAK) to Kernel Mode (KPPAK).	–
Slowpath (F2F)	When SecureXL works in User Mode (UPPAK), the Security Gateway performance for the Slowpath traffic is lower compared to Kernel Mode (KPPAK). Firewall path, or Slow path (F2F) is a packet flow when the SecureXL cannot accelerate the packet. In such case, SecureXL forwards the packet to the CoreXL layer, and one of the CoreXL Firewall performs full inspection.	–
CoreXL		
Dynamic Balancing	Dynamic Balancing of CoreXL Firewall Instances is not supported. On LightSpeed Appliances, this feature is disabled by default.	–
IPv4 CoreXL Firewall Instances	When you change the default CoreXL configuration in the "`cpconfig`" menu, configure the number of IPv4 CoreXL Firewall Instances based on this formula: `63 ≥ (Number of IPv4 CoreXL Firewall Instances) ≥ ((Total Number of CPU Cores in the Appliance) - 36)` If you configure 36 or more IPv4 CoreXL SND Instances, then the 100G Cards use a maximum of 36 IPv4 CoreXL SND Instances.	–
IPv4 CoreXL Firewall Instances	When SecureXL works in User Mode (UPPAK), the maximum supported number of IPv4 CoreXL Firewall Instances is 63. `63 ≥ (Number of IPv4 CoreXL Firewall Instances)`	–

Category	Limitation	Resolved In
Multi-Queue configuration	When you change the CoreXL configuration in the "`cpconfig`" menu, the Multi-Queue configuration changes to its default settings.	–
Multi-Queue		
Multi-Queue configuration	After you change the default Multi-Queue configuration in the "`mq_mng`" command, you must reboot the appliance.	–
Multi-Queue configuration	When you change the CoreXL configuration in the "`cpconfig`" menu, the Multi-Queue configuration changes to its default settings.	–
Interfaces / Ports		
Speed	100G Card does not support the 25 Gbps speed.	–
Link	If you change the configuration of one 100G Card port (link up/down, MTU, and so on), it causes the link to go down and then up on the other 100G Card port. Therefore, schedule a maintenance window to make the required changes in the configuration of the 100G Ports.	–
802.1ad	802.1ad (QinQ) is not supported.	–
Jumbo Frames	Jumbo Frames are not supported.	–
VxLAN	VxLAN interfaces are not supported. SecureXL does not accelerate traffic that passes through these interfaces.	–
GRE	GRE interfaces are not supported. SecureXL does not accelerate traffic that passes through these interfaces.	–
Monitor Mode	Monitor Mode on interfaces is not supported.	–
Bond	Gaia Portal can possibly log out an administrator when configuring Bond interfaces on the 100G Ports. The configuration is saved. The administrator must log in again to continue.	–
Bond	To create a Bond Interface that accelerates traffic, you must use the physical ports of the same 100G Card.	–
Bond	When you change the state of one physical port in a Bond Interface to down / up, the other physical port in the Bond Interface also changes its state to down / up.	–

Category	Limitation	Resolved In
Bond	Bond may become unstable because of LACP packet losses (on the network or in the interface). **Workaround** - Configure the LACP "`slow`" rate for this Bond on each side: ■ On the host appliance - see the *Gaia Administration Guide* for your version > Chapter "*Network Management*" > Section "*Network Interfaces*" > Section "*Bond Interfaces (Link Aggregation)*". ■ On the corresponding switch - see the vendor documentation.	–
Breakout Cables	100G Ports do not support copper or fiber breakout cables.	–
`mlx<Number>`	Ignore the interfaces with the names "`mlx<Number>`" (for example, "`mlx1-01`"). These are shadow interfaces for the Poll Mode Driver (PMD) the 100G Ports use.	–
`cpfifo<Number>`	Ignore the interfaces with the names "`cpfifo<Number>`" (for example, "`cpfifo1_0`"). These are control plane interfaces. You cannot configure these interfaces.	–
`gre0` and `gretap0`	Ignore the interfaces with the names "`gre0`" and "`gretap0`". By default, Gaia OS loads the GRE kernel driver. Therefore, Gaia OS has these interfaces in the administratively down state.	–
Traffic outage	In a very rare case, the 100G Ports might stop receiving and transmitting packets. **Workaround:** 1. Shut down the appliance (in Gaia Portal or Gaia Clish). 2. Disconnect the power cables from the appliance. 3. Connect the power cables from the appliance. 4. Power on the appliance.	
Traffic Capture For more information, see *"Capturing Traffic with TCPdump" on page 39*.		
VLAN	To capture traffic on a VLAN interface that is configured on a 100G Port, you must specify the VLAN ID in the TCPdump syntax.	–
Bond	To capture traffic that is accelerated in a Bond interface that is configured on 100G Ports, you must run the TCPdump directly on the 100G Ports.	–

Category	Limitation	Resolved In

Direction	The TCPdump option "`-Q {in | out | inout}`" is not supported on the 100G Ports.
	If you use this option in the syntax, the TCPdump tool shows an error.
	Example:
	`[Expert@HostName:0]# tcpdump -eni eth3-01 -Q out`
	`Translating Check Point pseudo interface eth3-01 to RDMA sniffer interface mlx5_0 for packet capture`
	`tcpdump: mlx5_0: pcap_setdirection() failed: Setting direction is not implemented on this platform`
	`[Expert@HostName:0]#`
		–

Maestro Configuration		
Ports	You must use only the 100G Ports to connect to Quantum Maestro Orchestrators. You must disconnect cables between Quantum Maestro Orchestrators and all other line cards and ports on the appliance.	–
Command Line		
`smartctl`	The output of the "`smartctl -a /dev/sda1`" command in the Expert mode shows: `Device is: Not in smartctl database` This is a cosmetic issue only.	–
`ethtool -i`	Output of the "`ethtool -i <Name of Interface>`" command shows different drivers in SecureXL UPPAK mode and SecureXL KPPAK mode.	–
`ethtool -G`	If you change the RX / TX ring sizes with the "`ethool -G`" command, then you must configure: ▪ The values that are multiples of 32 for interfaces that use Intel drivers ▪ The values that are multiples of 2 for interfaces that use Mellanox drivers	–

`ethtool -S`	Immediately after the appliance boot, the output of this command in the Expert mode:
	`ethtool -S <Name of 100G Port>`
	can show non-zero values in the counters **rx_phy_crc_errors** and **rx_phy_symbol_errors**.
	This is a cosmetic issue only.
	Example:
	`[Expert@QLS-800:0]# ethtool -S eth1-01 | grep -E "rx_phy_crc_errors|rx_phy_symbol_errors"`
	`rx_phy_crc_errors: 4294963909`
	`rx_phy_symbol_errors: 4294963909`
	`[Expert@QLS-800:0]#`
		–

Category	Limitation	Resolved In
`dmesg`	The output of the "`dmesg`" command in the Expert mode shows these errors on the appliance: `pci 0000:XX:00.X: BAR <NUMBER>: failed to assign [mem size 0x<NUMBER> 64bit pref]` You can safely ignore these messages.	–
HW Diagnostics		
"HW Diagnostics" menu	Below the "**HW Diagnostics**" menu, messages about "`LOM module`" and "`LOM`" can possibly appear in this scenario: 1. A LOM Card is installed in the appliance. 2. You connect your computer to the Console port on the appliance. 3. During the appliance boot, you press any key to enter the Boot Menu. 4. In the Boot Menu, you select "`HW Diagnostics`" and press the Enter key (see sk97251). Example messages: ▪ `LOM module not updated with system date and time` ▪ `Unable to communicate with LOM`	–
"HW Diagnostics" log file	The log file from the "**HW Diagnostics**" > "`Networking Test`" shows incorrect names of interfaces in this scenario: 1. You connect your computer to the Console port on the appliance. 2. During the appliance boot, you press any key to enter the Boot Menu. 3. In the Boot Menu, you select "`HW Diagnostics`" and press the Enter key (see sk97251). 4. In the "`HW Diagnostics`" menu, you select "`Diagnostics`" (or "`Custom`" > "`Networking Test`") and press the Enter key. 5. In the "`HW Diagnostics`" menu, you select "`Save Logs`". 6. You examine the "`NETWORK_TEST_<Date>_<Time>.log`" file. This is a cosmetic issue only.	–