



BlueField Modes of Operation

Table of contents

Introduction

NIC Mode

DPU Mode

DPU Mode Architecture

InfiniBand in DPU Mode

DPU Mode in Zero Trust

Moving Between Operation Modes

Identifying Which Mode BlueField is Currently Operating In

Changing Mode

Using External Host Command Line

Using External Host UEFI Menu

Using Arm OS command line

Using Arm UEFI Menu

Using DPU-BMC Redfish

Using Platform-BMC NC-SI OEM Commands

This document describes the modes of operation available for NVIDIA® BlueField® networking platforms (DPUs or SuperNICs).

Introduction

BlueField devices feature the following modes of operation:

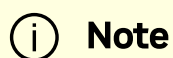
Mode of Operation	External Host Trust Level	Description	Default on SKUs	Can be Configured to All Other Modes?
NIC Mode	Host-trusted	The Arm cores of BlueField are inactive, and the device functions as an NVIDIA® ConnectX® network adapter.	SuperNIC SKUs default mode	Yes ¹
DPU Mode	Host-trusted	The Arm cores of BlueField are active, and the embedded Arm system runs services that manage the NIC resources and data path.	DPU SKUs default mode	Yes
	Zero Trust (restricted)	The Arm cores of BlueField are active, and the embedded Arm system runs services to manage the NIC resources and data path while enforcing restrictions on the external host (host isolation).	-	Yes

1. BFX H20 converged accelerator is limited to NIC Mode only. [___](#)

NIC Mode

In NIC Mode, BlueField operates as a ConnectX network adapter for the external host. For BlueField-3, the Arm cores are inactive, while for BlueField-2, the Arm cores are active but non-functional.

Operating in NIC Mode on BlueField-3 reduces power consumption, improves network performance, and minimizes the host memory footprint.



BlueField-3 SuperNIC SKUs are shipped in NIC Mode by default.

Note

Multi-host is not supported when BlueField is operating in NIC Mode.

DPU Mode

In this operation mode, Arm cores active, known also as embedded CPU function ownership (ECPF) mode, is the default mode for the BlueField DPU family of SKUs.

In DPU Mode, the NIC resources and functionality are owned and controlled by the embedded Arm subsystem. All network communication to the host flows through a virtual switch control plane hosted on the Arm cores that manages all networking traffic coming and going from the host.

While working in this mode, the BlueField is the trusted function managed by the data center and host administrator for provisioning, management and orchestration (eg. load network drivers, reset an interface, bring an interface up and down, update the firmware, change the mode of operation on BlueField, etc).

Note

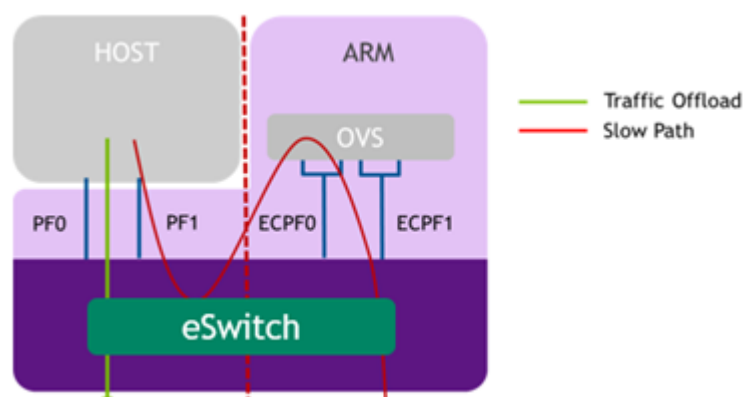
BlueField-2 DPU and BlueField-3 DPU SKUs are shipped in DPU Mode by default.

Note

Socket Direct is not supported when BlueField is operating in DPU Mode.

DPU Mode Architecture

In DPU Mode, the BlueField DPU provides the host system with access to network functions, while the host's capabilities are restricted and managed by the Arm processor within the BlueField.



Traffic Management and Paths

The Embedded Control and Processing Framework (ECPF) controls the NIC's embedded switch (eswitch). All network traffic between the host interface and the network initially passes through the BlueField's Arm processor via Representors. This path, where traffic is processed by the Arm processor, is referred to as the "slow path".

To improve performance, the Arm processor can define rules in the eswitch through the ECPF, allowing packets to bypass the Arm processor and be processed directly by the eswitch. This is known as the "fast path", which reduces latency and increases throughput by offloading traffic processing from the Arm to the eswitch.

A virtual switch running on the Arm processor may integrate both slow path and fast path functionalities by processing and classifying only the first packet of a new flow. For subsequent packets in the flow, the virtual switch defines eswitch rules, enabling fast path processing for the remainder of the traffic.

Initialization Process

At startup, network access to the host is initially blocked. This restriction remains until the virtual switch running on the Arm processor loads the default out-of-box rules to manage the ECPF on the BlueField. Once these rules are loaded, network traffic to the host is automatically enabled.

Note

The driver on the host system can only be loaded after the driver on the BlueField has been loaded and has completed NIC configuration. Additionally, all Interface Configuration Memory (ICM) is allocated by the ECPF and resides in the BlueField's memory.

InfiniBand in DPU Mode

In DPU Mode, when operating with an InfiniBand network, OpenSM must be executed from the BlueField Arm side rather than the host side. Similarly, InfiniBand management tools such as `sminfo`, `ibdev2netdev`, and `ibnetdiscover` can only be used from the BlueField Arm side and are not accessible from the host side.

DPU Mode in Zero Trust

Zero Trust, also known as Restricted Mode, is a specialized variation of DPU Mode that enhances security by preventing the host system administrator from accessing BlueField from the host side. Once Zero Trust mode is enabled, the BlueField must be fully controlled by the data center administrator via the Arm cores or the BMC connection, rather than through the host.

This mode enforces security and isolation by restricting the host from performing operations that could compromise BlueField. The following operations can be restricted individually in Zero Trust mode:

- Port ownership – The host cannot assign itself as the port owner

- Hardware counters – The host is denied access to hardware counters
- Tracer functionality – The tracer functionality is blocked
- RShim interface – The RShim interface is disabled
- Firmware flash – firmware flashing from the host is restricted

Zero Trust mode ensures a robust security boundary between the host and BlueField, making it an ideal configuration for environments requiring strict control and isolation.

Moving Between Operation Modes

Transitioning between operation modes can be achieved through various configuration interfaces as presented in the following table.

Note

Some configuration interfaces may be locked out when operating in Zero Trust (Restricted) Mode.

Interface	From	To	Configuration option available by default, for this interface?	Configuration option can be locked-out ² for this interface?
External Host command line	DPU Mode	NIC Mode	Yes	Yes
	NIC Mode	DPU Mode	Yes	Yes
	DPU Mode	DPU Mode with Zero Trust	No	Always blocked
	DPU Mode with Zero Trust	DPU Mode	No	Always blocked
	DPU Mode with Zero	NIC Mode	Not supported	N/A

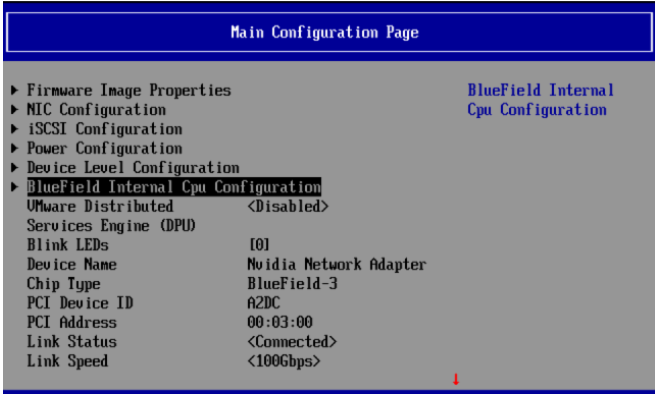
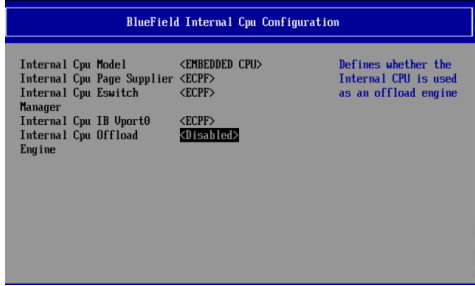
Interface	From	To	Configuration option available by default, for this interface?	Configuration option can be locked-out ² for this interface?
	Trust			
Host UEFI Menu	DPU Mode	NIC Mode	Yes	Yes
	NIC Mode	DPU Mode	Yes	Yes
	DPU Mode	DPU Mode with Zero Trust	No	Always blocked
	DPU Mode with Zero Trust	DPU Mode	No	Always blocked
	DPU Mode with Zero Trust	NIC Mode	Not supported	N/A
Arm OS command line	DPU Mode	NIC Mode	Yes	No
	NIC Mode	DPU Mode	N/A	N/A
	DPU Mode	DPU Mode with Zero Trust	Yes	No
	DPU Mode with Zero Trust	DPU Mode	Yes	No
	DPU Mode with Zero Trust	NIC Mode	Not supported	N/A
Arm UEFI Menu	DPU Mode	NIC Mode	Yes	No
	NIC Mode	DPU Mode	Yes	No
	DPU Mode	DPU Mode with Zero Trust	No ³	No
	DPU Mode with Zero Trust	DPU Mode	No ³	No
	DPU Mode with Zero	NIC Mode	Not supported	N/A

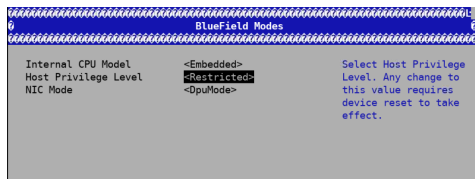
Interface	From	To	Configuration option available by default, for this interface?	Configuration option can be locked-out ² for this interface?
	Trust			
DPU-BMC Redfish	DPU Mode	NIC Mode	Yes	No
	NIC Mode	DPU Mode	Yes	No
	DPU Mode	DPU Mode with Zero Trust	No ³	No
	DPU Mode with Zero Trust	DPU Mode	No ³	No
	DPU Mode with Zero Trust	NIC Mode	Not supported	N/A
Platform-BMC NC-SI OEM commands	DPU Mode	NIC Mode	Yes	No
	NIC Mode	DPU Mode	Yes	No
	DPU Mode	DPU Mode with Zero Trust	No ³	No
	DPU Mode with Zero Trust	DPU Mode	No ³	No
	DPU Mode with Zero Trust	NIC Mode	Not supported	N/A

1. Blocked or restricted

2. Roadmap

Identifying Which Mode BlueField is Currently Operating In

Interface	Command	Response
Using external host command line	<pre>host> sudo mlxconfig -d /dev/mst/<device> q INTERNAL_CPU_OFFLOAD_ENGINE</pre>	<p>Output format:</p> <pre>R0 INTERNAL_CPU_OFFLOAD_ENGINE ENABLED(0)</pre> <ul style="list-style-type: none"> ENABLED(0) means BlueField is running in DPU Mode DISABLED(1) means BlueField is running in NIC Mode R0 is marked for read only, and indicates DPU Mode with Zero Trust
Using external host UEFI (HII) menu	<p>Navigate to specific device and select BlueField Internal Cpu Configuration</p> 	<p>Internal Cpu Offload Engine</p> <p>indicates the mode BlueField is currently operating in:</p> <ul style="list-style-type: none"> Disabled – BlueField is operating in NIC Mode Enabled – BlueField is operating in DPU Mode 
Using Arm UEFI (GUI) menu	<p>Access the Arm UEFI menu by pressing the Esc button twice on the console and navigate to Device Manager → System Configuration → BlueField Modes .</p>	<p>The NIC Mode menu indicates the mode BlueField is currently operating in:</p> <ul style="list-style-type: none"> NicMode – BlueField is operating in NIC Mode

Interface	Command	Response																																								
		<ul style="list-style-type: none"><code>DpuMode</code> – BlueField is operating in DPU Mode 																																								
Using DPU BMC Redfish	<pre>curl -k -u root:'<PASSWORD>' -X GET https://<bmc_ip>/redfish/v1/Systems/Bluefield/Oem/Nvidia</pre>	<p>Read <code>Mode</code> field:</p> <pre>{ ... "Mode": "<DpuMode>" or "<NicMode>" ... }</pre> <ul style="list-style-type: none"><code>"Mode" : NicMode</code> – BlueField is operating in NIC Mode<code>"Mode" : DpuMode</code> – BlueField is operating in DPU Mode																																								
Using platform BMC NC-SI OEM commands	<p><i>Get Command = 0x13, Parameter = 0x33</i></p> <table><tr><th>Off set</th><th>31:24</th><th>23:16</th><th>15:8</th><th>7:0</th></tr><tr><td>0:15</td><td colspan="4">NC-SI OEM Header (OEM Command)</td></tr><tr><td>16:19</td><td colspan="4">Mellanox Manufacture ID (IANA) = 0x8119</td></tr><tr><td>20:23</td><td>Command rev=0x00</td><td>MLNX Cmd ID= 0x13</td><td>Parameter=0x33</td><td>Reserved</td></tr><tr><td>24:</td><td colspan="4">Checksum 31:0</td></tr></table>	Off set	31:24	23:16	15:8	7:0	0:15	NC-SI OEM Header (OEM Command)				16:19	Mellanox Manufacture ID (IANA) = 0x8119				20:23	Command rev=0x00	MLNX Cmd ID= 0x13	Parameter=0x33	Reserved	24:	Checksum 31:0				<p>Response format:</p> <table><tr><th>Of fs et</th><th>31:24</th><th>23:16</th><th>15:8</th><th>7:0</th></tr><tr><td>0:15</td><td colspan="4">NC-SI OEM Header (OEM Command)</td></tr><tr><td>16:19</td><td colspan="2">Response Code</td><td colspan="2">Reason Code</td></tr></table>	Of fs et	31:24	23:16	15:8	7:0	0:15	NC-SI OEM Header (OEM Command)				16:19	Response Code		Reason Code	
Off set	31:24	23:16	15:8	7:0																																						
0:15	NC-SI OEM Header (OEM Command)																																									
16:19	Mellanox Manufacture ID (IANA) = 0x8119																																									
20:23	Command rev=0x00	MLNX Cmd ID= 0x13	Parameter=0x33	Reserved																																						
24:	Checksum 31:0																																									
Of fs et	31:24	23:16	15:8	7:0																																						
0:15	NC-SI OEM Header (OEM Command)																																									
16:19	Response Code		Reason Code																																							

Interface	Command					Response				
	Offset	31:24	23:16	15:8	7:0	Offset	31:24	23:16	15:8	7:0
	27					20:23	Mellanox Manufacture ID (IANA) = 0x8119			
						24:27	Command rev=0x00	MLNX Cmd ID=0x12	Parameter=0x33	Reserved
						28:31				Offload engine
						32:35	Checksum 31:0			
	Response field:									

Changing Mode

For the configuration to take effect, Arm and NIC components must undergo a reset. Power cycle is recommended.

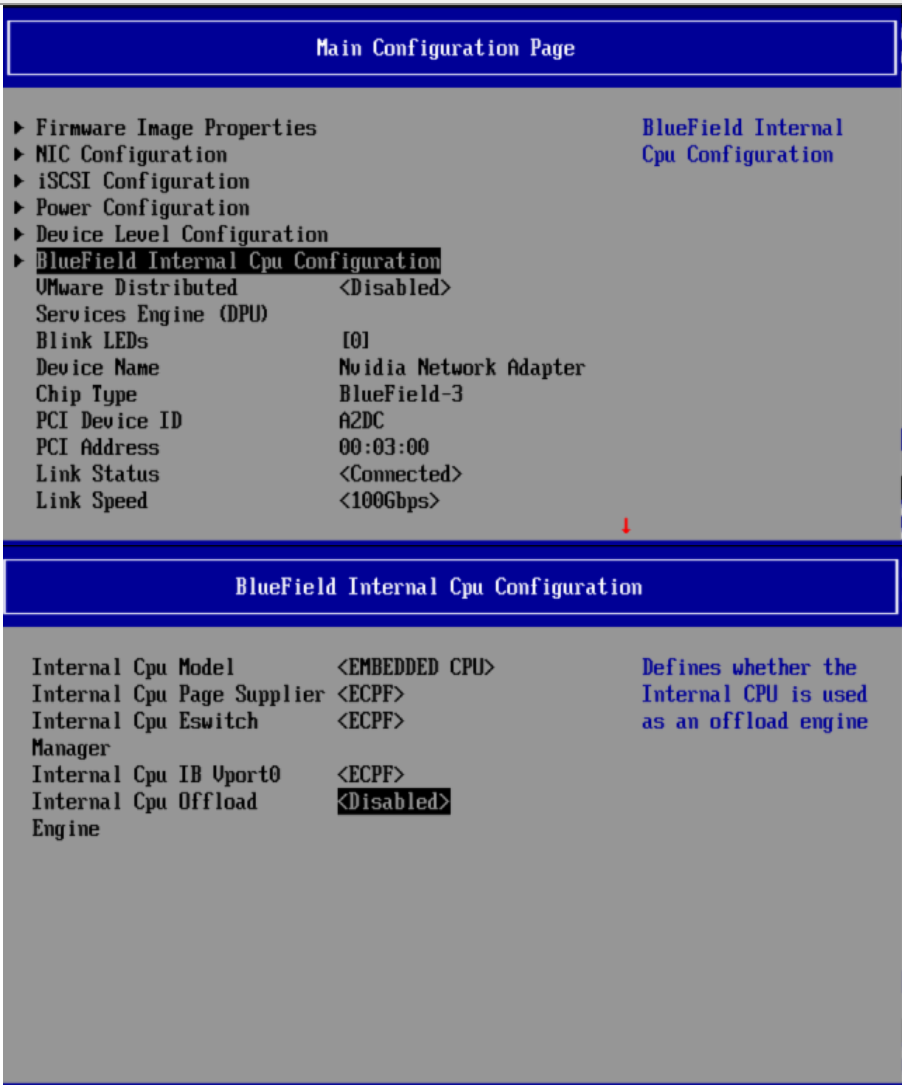
Using External Host Command Line

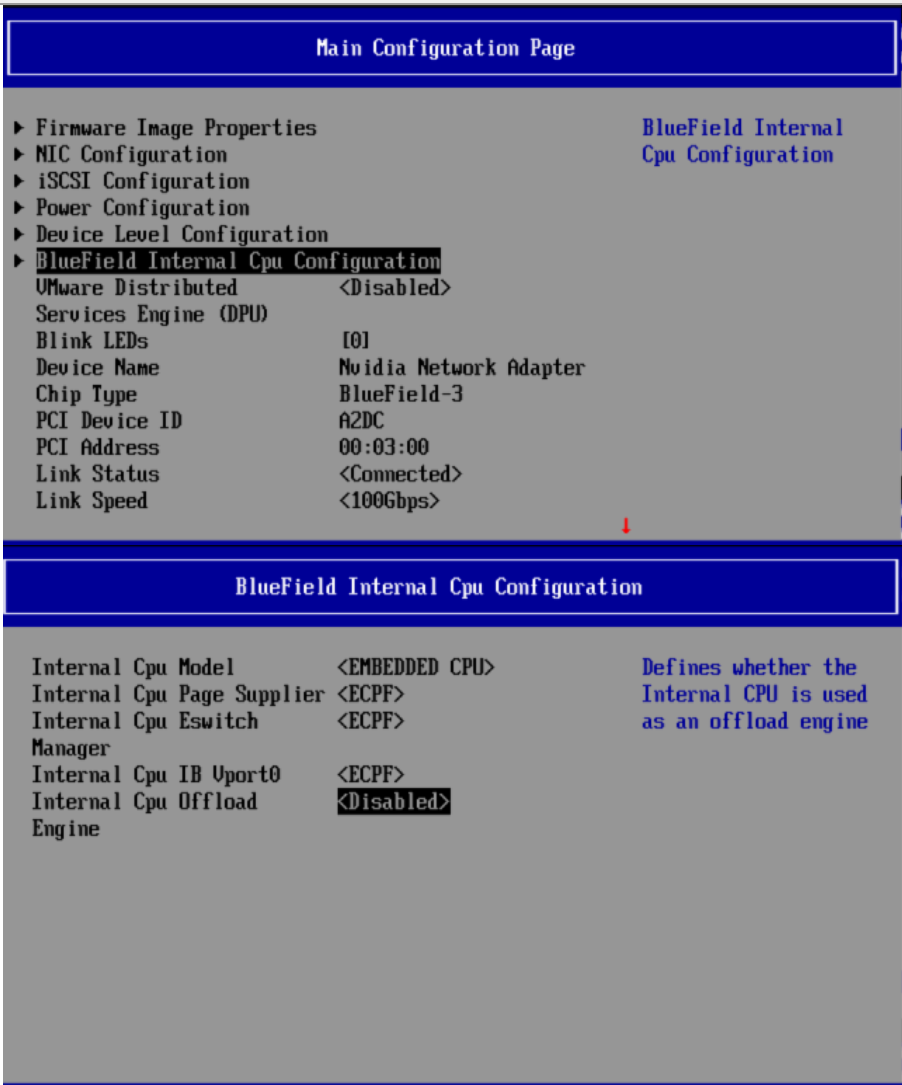
From Mode	To Mode	Command
DPU Mode	NIC Mode	<p>For BlueField-3:</p> <pre>host> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_OFFLOAD_ENGINE=1</pre> <p>For BlueField-2:</p> <pre>host> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_PAGE_SUPPLIER=1 INTERNAL_CPU_ESWITCH_MANAGER=1 INTERNAL_CPU_IB_VPORT0=1 INTERNAL_CPU_OFFLOAD_ENGINE=1</pre>
NIC Mode	DPU Mode	<p>For BlueField-3:</p> <pre>host> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_OFFLOAD_ENGINE=0</pre> <p>For BlueField-2:</p> <pre>host> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_PAGE_SUPPLIER=0 INTERNAL_CPU_ESWITCH_MANAGER=0 INTERNAL_CPU_IB_VPORT0=0 INTERNAL_CPU_OFFLOAD_ENGINE=0</pre>
DPU Mode	DPU Mode with	N/A

From Mode	To Mode	Command
	Zero Trust	
DPU Mode with Zero Trust	DPU Mode	N/A
DPU Mode with Zero Trust	NIC Mode	<p>Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.</p> <div>  Warning <ul style="list-style-type: none"> • Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode. • Ensure to disable Zero Trust configuration before transitioning to NIC Mode. • Operating in NIC Mode with Zero Trust (Restricted) configuration is not supported and may lead to undefined behavior. </div>

Using External Host UEFI Menu

From Mode	To Mode	Command
DPU Mode	NIC Mode	

From Mode	To Mode	Command
		 <p>Select BlueField Internal Cpu Configuration.</p> <p>To enable NIC Mode, set Internal Cpu Offload Engine to Disabled.</p>
NIC Mode	DPU Mode	

From Mode	To Mode	Command
		 <p>Select BlueField Internal Cpu Configuration.</p> <p>To enable DPU Mode, set Internal Cpu Offload Engine to Enabled.</p>
DPU Mode	DPU Mode with Zero Trust	N/A
DPU Mode with Zero Trust	DPU Mode	N/A
DPU Mode	NIC Mode	Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.

From Mode	To Mode	Command
with Zero Trust		<div>  Warning <ul style="list-style-type: none"> Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode. Ensure to disable Zero Trust configuration before transitioning to NIC Mode. Operating in NIC Mode with Zero Trust (Restricted) configuration is not supported and may lead to undefined behavior. </div>

Using Arm OS command line

From Mode	To Mode	Command
DPU Mode	NIC Mode	<p>For BlueField-3:</p> <pre>bf> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_OFFLOAD_ENGINE=1</pre> <p>For BlueField-2:</p> <pre>bf> sudo mlxconfig -d /dev/mst/<device> s INTERNAL_CPU_PAGE_SUPPLIER=1 INTERNAL_CPU_ESWITCH_MANAGER=1 INTERNAL_CPU_IB_VPORT0=1 INTERNAL_CPU_OFFLOAD_ENGINE=1</pre>

From Mode	To Mode	Command
NIC Mode	DPU Mode	Not Applicable (Arm OS is not available)
DPU Mode	DPU Mode with Zero Trust	<pre>bf> \$ sudo mlxprivhost -d /dev/mst/<device> r -- disable_rshim --disable_tracer -- disable_counter_rd --disable_port_owner</pre>
DPU Mode with Zero Trust	DPU Mode	<pre>bf> \$ sudo mlxprivhost -d /dev/mst/<device> p</pre>
DPU Mode with Zero Trust	NIC Mode	<p>Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.</p> <div>  Warning <ul style="list-style-type: none"> • Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode. • Ensure to disable Zero Trust configuration before transitioning to NIC Mode. • Operating in NIC Mode with Zero Trust (Restricted) configuration is not supported and may lead to undefined behavior. </div>

Using Arm UEFI Menu

From Mode	To Mode	Command
DPU Mode	NIC Mode	<ol style="list-style-type: none"> 1. Access the Arm UEFI menu by pressing the Esc button twice on the console. 2. Select Device Manager → System Configuration → BlueField Modes. 3. Set the NIC Mode option to NicMode to enable NIC Mode. <div data-bbox="574 529 1464 768" data-label="Code-Block"> <pre> Internal CPU Model <Embedded> Host Privilege Level <Privileged> NIC Mode <NicMode> 000000000000000000000000L: 0 DpuMode 0 0 NicMode 0 0 Unavailable 0 000000000000000000000000L: </pre> </div> 4. Exit BlueField Modes and System Configuration and make sure to save the settings. 5. Exit the UEFI setup using the "reset" option. The configuration is not yet applied and BlueField is expected to boot in DPU Mode. 6. Issue power cycle to apply new configuration.
NIC Mode	DPU Mode	<ol style="list-style-type: none"> 1. Access the Arm UEFI menu by pressing the Esc button twice on the console. 2. Select Device Manager → System Configuration → BlueField Modes. 3. Set the NIC Mode option to DpuMode to enable DPU Mode. <div data-bbox="574 1339 1464 1579" data-label="Code-Block"> <pre> Internal CPU Model <Embedded> Host Privilege Level <Privileged> NIC Mode <NicMode> 000000000000000000000000L: 0 DpuMode 0 0 NicMode 0 0 Unavailable 0 000000000000000000000000L: </pre> </div> 4. Exit BlueField Modes and System Configuration and make sure to save the settings. 5. Exit the UEFI setup using the "reset" option. The configuration is not yet applied and BlueField is expected to boot in NIC Mode. 6. Issue power cycle to apply new configuration.

From Mode	To Mode	Command
DPU Mode	DPU Mode with Zero Trust	Roadmap
DPU Mode with Zero Trust	DPU Mode	Roadmap
DPU Mode with Zero Trust	NIC Mode	<p>Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.</p> <div>  Warning <ul style="list-style-type: none"> Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode. Ensure to disable Zero Trust configuration before transitioning to NIC Mode. Operating in NIC Mode with Zero Trust (Restricted) configuration is not supported and may lead to undefined behavior. </div>

Using DPU-BMC Redfish

From Mode	To Mode	Command
DPU Mode	NIC Mode	<pre>curl -k -u root:'password' -H 'content-type: application/json' -d '{"Mode": "NicMode"}' -X POST</pre>

From Mode	To Mode	Command
		<pre>https://bmc_ip/redfish/v1/Systems/Bluefield/Oem/Nvidia/Actions/Mode.Set</pre> <p>To apply configuration, two consecutive Arm reboots are required.</p>
NIC Mode	DPU Mode	<pre>curl -k -u root:'password' -H 'content-type: application/json' -d '{"Mode": "DpuMode"}' -X POST https://bmc_ip/redfish/v1/Systems/Bluefield/Oem/Nvidia/Actions/Mode.Set</pre> <p>To apply configuration, two consecutive Arm reboots are required.</p>
DPU Mode	DPU Mode with Zero Trust	Roadmap
DPU Mode with Zero Trust	DPU Mode	Roadmap
DPU Mode with Zero Trust	NIC Mode	<p>Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.</p> <div>  Warning <ul style="list-style-type: none"> Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode. Ensure to disable Zero Trust configuration before transitioning to NIC Mode. Operating in NIC Mode with Zero Trust (Restricted) configuration is not </div>

From Mode	To Mode	Command
		supported and may lead to undefined behavior.

Using Platform-BMC NC-SI OEM Commands

From Mode	To Mode	Command						
DPU Mode	NIC Mode	Command = 0x12, Parameter = 0x33						
		<table><tr><td>Offset</td><td>31:24</td><td>23:16</td><td>15:8</td><td>7:0</td></tr></table>	Offset	31:24	23:16	15:8	7:0	
		Offset	31:24	23:16	15:8	7:0		
		0:15	NC-SI OEM Header (OEM Command)					
		16:19	Mellanox Manufacture ID (IANA) = 0x8119					
		20:23	Command rev=0x00	MLNX Cmd ID= 0x12	Parameter= 0x33	Reserved		
		24:27				Offload engine		
		28:31	Checksum 31:0					
		<table><tr><th>Field</th><th>Size</th><th>Offset in NC-SI Command</th><th>Description</th></tr><tr><td>Offload engine</td><td>1 bit</td><td>27.0</td><td>0x0: Enabled – DPU Mode 0x1: Disabled – NIC Mode</td></tr></table>	Field	Size	Offset in NC-SI Command	Description	Offload engine	1 bit
Field	Size	Offset in NC-SI Command	Description					
Offload engine	1 bit	27.0	0x0: Enabled – DPU Mode 0x1: Disabled – NIC Mode					
For NIC Mode, set the offload engine bit to 0x1.								
NIC Mode	DPU Mode	Command = 0x12, Parameter = 0x33						

From Mode	To Mode	Command				
		bytes/ bits	31:24	23:16	15:8	7:0
		0:15	NC-SI OEM Header (OEM Command)			
		16:19	Mellanox Manufacture ID (IANA) = 0x8119			
		20:23	Command rev=0x00	MLNX Cmd ID= 0x12	Parameter =0x33	Reserved
		24:27				Offload engine
		28:31	Checksum 31:0			
		Field	Size	Offset in NC-SI Command		Description
		Offload engine	1 bit	27.0		0x0: Enabled - DPU Mode 0x1: Disabled - NIC Mode
		For DPU Mode, set the offload engine bit to 0x0.				
DPU Mode	DPU Mode with Zero Trust	Roadmap				
DPU Mode with Zero Trust	DPU Mode	Roadmap				
DPU Mode with Zero Trust	NIC Mode	Not supported. Move from DPU Mode with Zero Trust to DPU Mode first, and then from DPU Mode to NIC Mode.				
		<div><div></div><div>Warning<ul style="list-style-type: none">Perform a <u>system-level reset</u> when moving from Zero Trust to DPU Mode before configuring NIC Mode.</div></div>				

From Mode	To Mode	Command
		<ul style="list-style-type: none"> • Ensure to disable Zero Trust configuration before transitioning to NIC Mode. • Operating in NIC Mode with Zero Trust (Restricted) configuration is not supported and may lead to undefined behavior.

Warning

Separated Host Mode is obsolete for BlueField DPU/SuperNIC SKUs and should not be used, even if it remains visible in some configuration menus or options.

Note

Separated Host Mode is available only for BlueField controller SKUs, where the BlueField Arm OS is the sole CPU/OS in the chassis.

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality. NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice. Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete. NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and

conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document. NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk. NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

© Copyright 2025, NVIDIA. PDF Generated on 05/05/2025