Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB Switches

Release Notes

For Lenovo Campus NOS 8.4.3

Lenovo™

Note: Before using this information and the product it supports, read the product *Warranty Information* document and the *Important Notices* document included with the product.

First Edition (March 2019)

Release Notes

This release supplement provides the latest information regarding Lenovo Campus NOS 8.4.3 for the Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB switches (referred to as CE0128XB/CE0152XB throughout this document).

This supplement extends the following documentation for use with the CE0128XB/CE0152XB:

- *Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB CLI Command Reference*
- *Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB Quick Start Guide*
- *Lenovo CE0128TB/CE0128PB and CE0152TB/CE0152PB Web GUI Reference*

These publications are available from the following website:

https://systemx.lenovofiles.com/help/topic/com.lenovo.systemx.common.nav.doc/overview_rack_switches.html?cp=0_5

Please keep these release notes with your product manuals.

Known Issues

This section describes known issues for Campus NOS 8.4.3 on the Lenovo CE0128XB/CE0152XB switches.

Operations, Administration, and Management

Deleting backup image may take a couple of minutes.

Table 1. *OAM*

Description	Triggers	Workaround
Deleting the backup image takes approximately two minutes per unit. During that time, the console is locked.	Using the delete backup command to delete the backup image from the CLI or Web interface.	Do not delete the backup image. Downloading a new backup image overwrites the existing image.

Routing

Error message `Reconciliation failed for db L3_LPM(17)` may be observed when, in a stack configuration, the master unit, with maximum number of static routes such as 512 learned/configured, reboots.

Table 2. *Routing*

Description	Triggers	Workaround
The routing interface reserves a connected route in the hardware table which reduces number of static/connected and dynamic routes that can be added. This results in hardware route addition failure. As long as the total number of routes does not exceed the device capacity, it doesn't impact the functionality.	Configuring the maximum limit of static/connected and dynamic routes and then reloading the master switch either by a stack failover or a reload.	Do not configure the maximum static/connected and dynamic routes.

Log messages such as `USL: Failed to update control flags: vlan 119 flags 16384 hwRv -4 dbRv 0` may be observed when a stack member is rebooted in a stacking configuration.

Table 3. *Routing*

Description	Triggers	Workaround
There is no impact to functionality. The issue is observed when a stack member unit is reloaded when the stack master is learning routes.	Reloading one or more stack member units while the stack master is learning dynamic routes or while the stack master is being configured with static/connected routes.	None. The failed operation is retried and succeeds eventually.

Interfaces

10G SFP+ ports may not link up after reboot when the switch has both 1G SFP and 10G SFP+ transceivers connected.

Table 4. *Interfaces*

Description	Triggers	Workaround
When both 1G SFP modules and 10G SFP+ modules are present, the 10G ports may not link up after reload.	Reloading the stack where both 1G SFP and 10G SFP+ transceivers are present in 10G ports.	As a workaround, the 10G SFP+ port can be **shutdown/no shutdown** to recover the link.

Security

No Secure Protocol Level(s) are displayed in the CLI output of the command **show ip http**.

Table 5. *Security*

Description	Triggers	Workaround
Since SSLv3, TSL1.0, TLS1.1 secure protocols are disabled by default, the **show ip http** command does not display any secure protocol. This does not impact functionality, as TLS 1.2 is enabled by default and cannot be disabled.	This is the switch default behavior.	There is no workaround for this issue.

When 512-bit keys are used to generate a certificate, HTTPS connectivity may fail with some browsers.

Table 6. *Security*

Description	Triggers	Workaround
The EC cipher digest size is too large to be signed by a 512-bit RSA certificate. Use 1024-bit or 2048-bit keys to generate certificates.	Generating an RSA key of less than 1024 bits when using the **key-generate** command in Crypto Certificate Generate mode. The default RSA key size is 1024 bits.	Generate keys using 1024 or 2048-bit keys using the **key-generate** [*length*] command in Crypto Certificate Generate mode. The **crypto certificate generate** command generates a certificate using a 2048-bit key.