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.

Third Edition (December 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:

http://systemx.lenovofiles.com/help/topic/com.lenovo.systemx.common.nav.doc/overview_rack_switches.html

Please keep these release notes with your product manuals.

Significant Changes

Release 8.4.3.9 has the following features added.

Password Recovery

The software provides a password recovery procedure that relies upon gaining access to Password Recovery mode using the boot menu option during system startup.

The boot menu option is **Password recovery mode**. If the user chooses this option and starts the application, both the password for admin and the login-type for admin are skipped while applying the startup-configuration. This allows a user to login to the device as *admin* with the default password.

Note: The password recovery option is available only on the serial console session.

This is applicable only for the session, when the user has started the device with the **Password recovery mode** option. If the device is re-started, the device expects the password as per the startup configuration.

After starting the device in the Password recovery mode, the user has to configure the password and save it. Password recovery mode is only for the admin user and not for any other user.

California Privacy Law Enforcement on Lenovo CE0128XB/CE0152XB Switches

This feature enforces the California Privacy Law for Management Access to the switches. The law is defined in:

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

under Section 1. Title 1.81.26. *Security of Connected Devices*.

Conformance to this law requires adhering to at least one of the following two features:

1. The preprogrammed password is unique to each device manufactured.
2. The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

As per this law, Lenovo CE0128XB/CE0152XB switches enforce the Privacy Law in the CLI and Web GUI management interfaces per feature 2.

Note: The user will be asked to change the factory-default password on logging in for the first time into the switch using either the CLI or the Web UI. The term *user* implies to the users that the switch has a part of the factory-default configuration: admin, guest.

Note: This is applicable to both HTTP and HTTPS web sessions.

Note: This applies for the case when the user upgrades from 8.4.3.2 or 8.4.3.7 to 8.4.3.9 and had the default password set for admin and guest accounts. If the user had a non-default password set, the non-default password is retained and there is no request to change it at first login after the upgrade.

Significant Changes

Release 8.4.3.7 has new U-boot code.

When the device with the latest build of 8.4.3.7 is made Active image, issue the **update bootcode** command to update the bootloader from the new image.

Note: This is a required mandatory step. Enter the **reload** command to run the image. The bootcode version printed during bootup should be U-Boot 2012.10-00018-g5b93572cc9 (Jun 28 2019 - 14:28:54). The operation image version should be 8.4.3.7.

```
(CE0152PB)#update bootcode

Power to the device must be maintained.
Are you sure (y/n)? y

Updating boot code, please wait ...

Success!
```

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 Ethernet ports always report the link as *up* with a certain SFP 1000 BASE-T copper transceiver, regardless of the actual status.

Table 4. *Interfaces*

Description	Triggers	Workaround
When using an SFP 1000 BASE-T copper transceiver (P/N: 78P3177) with the switch, the link status is always up, even when there is no cable plugged into the SFP module.	Using the SFP 1000 BASE-T copper transceiver (P/N: 78P3177).	Consider using a different transceiver.

SFP+ ports belonging to the same internal interface must be configured to the same speed.

Table 5. *Interfaces*

Description	Triggers	Workaround
Due to a hardware limitation, SFP+ ports that belong to the same internal interface must be configured to operate at the same speed.	Using transceivers operating at 1G and 10G speeds on the same internal interface.	SFP transceivers operating at 1G must use different internal interfaces than SFP+ transceivers operating at 10G. On CE0128TB/CE0128PB platforms, ports 25 and 26 belong to one internal interface, and ports 27 and 28 belong to the other internal interface. On CE0152TB/CE0152PB platforms, ports 49 and 50 belong to one internal interface, and ports 51 and 52 belong to the other internal interface.

Insertion and removal of a transceiver causes a link flap on the partner link for interfaces sharing the same internal interface.

Table 6. *Interfaces*

Description	Triggers	Workaround
On links that share an internal interface, inserting or removing a transceiver causes a link flap on the partner link. On CE0128TB/CE0128PB platforms, ports 25 and 26 share an internal interface, and ports 27 and 28 share an internal interface. On CE0152TB/CE0152PB platforms, ports 49 and 50 share an internal interface, and ports 51 and 52 share an internal interface.	Inserting or removing a transceiver on linked ports.	None.

False warning saying that there are pending changes to be saved.

Table 7. *Interfaces*

Description	Triggers	Workaround
False warning saying that there are pending changes to be saved when the user tries to reload the switch.	This can happen even with no recent configuration changes, when 1G copper SFP transceivers are used for SFP+ uplink ports.	None.

Security

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

Table 8. *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 9. *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.