Lenovo RackSwitch G8296

Release Notes

For Lenovo Cloud Network Operating System 10.8

Lenovo™

Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices* and *User Guide* documents on the Lenovo *Documentation* CD and the *Warranty Information* document that comes with the product.

Release Notes

This release supplement provides the latest information regarding Lenovo Cloud Network Operating System 10.8 for the Lenovo RackSwitch G8296 (referred to as G8296 throughout this document).

This supplement modifies and extends the following Cloud NOS documentation for use with *CNOS* 10.8:

- *Lenovo Network Application Guide for Lenovo Cloud Network Operating System 10.8*

- *Lenovo Network Command Reference for Lenovo Cloud Network Operating System 10.8*

- *Lenovo Network Python Programming Guide for Lenovo Cloud Network Operating System 10.8*

- *Lenovo Network REST API Programming Guide for Lenovo Cloud Network Operating System 10.8*

- *Lenovo RackSwitch G8296 Installation Guide for Lenovo Network Operating System*

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.

Note: The Lenovo Cloud Network OS is based on the Embedded Linux Integration Environment (ELIE). To obtain open source code licenses, go to https://github.com/lenovo/ELIE/tree/master/elie-1.7.1/licenses/. For details on how to obtain open source code, please contact Lenovo Support.

Hardware Support

CNOS 10.8 software is supported on the G8296 high performance Layer 2-3 network switches.

The G8296 is a 2U rack-mountable aggregation switch. The G8296 uses a wire-speed, non-blocking switching fabric that provides simultaneous wire-speed transport of multiple packets at low latency on all ports.

● Eighty-six 10 Gigabit Ethernet (GbE) Small Form Pluggable Plus (SFP+) ports which also support legacy 1 GbE connections

● Ten 40 GbE Quad Small Form Pluggable Plus (QSFP+) ports, two of which (Ethernet 1/87 and Ethernet 1/88) can optionally be used as four 10 GbE SFP+ ports

Figure 1. G8296 front panel
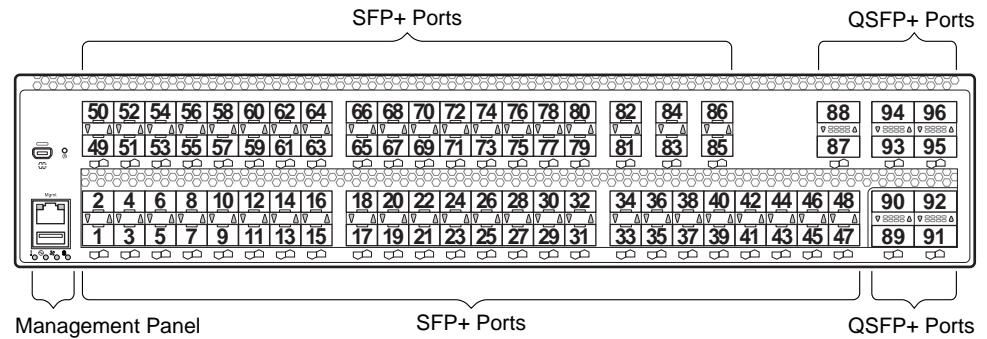
Converting the Switch Software Image from CNOS to ENOS

The new Lenovo Cloud Network OS image cannot coexist on the switch with your legacy 8.x Lenovo NOS. All previous configuration will be lost. If you are running Lenovo CNOS, follow these instructions to replace the operating system with Lenovo NOS 8.x.

To download all necessary software images, go to the following website:

http://support.lenovo.com

1. Download the ENOS boot image to the switch and enter **y** to confirm the download operation.

```
G8296> enable
G8296# cp tftp tftp://<tftp server IP>/G8296-8.4.1.0_Boot.imgs system-image
boot vrf management
Confirm download operation? (y/n) [n] y
Download in progress
..........
Copy Success

Install image...This takes about 90 seconds. Please wait
Check image signature succeeded
Extracting image: 100%
Installing eNOS RFS:
Updating flash: 100%
Extracting image: 100%
Installing eNOS Kernel:
Updating flash: 100%
Extracting image: 100%
Installing eNOS DFT:
Updating flash: 100%
Extracting image: 100%
Installing uboot:
Updating flash: 100%
Boot image installation succeeded.
```

2. Download the ENOS system image to the switch and enter **y** to confirm the download operation.

```
G8296# cp tftp tftp://<tftp server IP>/G8272-8.4.1.0_OS.imgs system-image os
vrf management
Confirm download operation? (y/n) [n] y
Download in progress
..........
Copy Success
Install image...This takes about 90 seconds. Please wait
Check image signature succeeded
Extracting image: 100%
Installing E-NOS image to image1
Installing image to E-NOS image1: 100%
Boot image installation failed.
OS image installation succeeded.
```

3. Reload the switch, confirming the operation when prompted.

```
G8296# reload

reboot system (y/n) ? y
```

4. After the switch reloads, log in and verify that the switch is running the ENOS 8.x image.

```
G8296# show boot

Current running image version: 8.4.1.0
Currently set to boot software image1, unknown config block.
NetBoot: disabled, NetBoot tftp server:  , NetBoot cfgfile:
Current boot Openflow protocol version: 1.0
USB Boot: disabled
Currently profile is default, set to boot with default profile next time.
Current FLASH software:
  image1: version 8.4.1.0 downloaded 10:29:59 Wed Nov 23, 2016, Mode
Stand-alone
  image2: version 8.4.1.0 downloaded 10:32:19 Wed Nov 23, 2016, Mode
Stand-alone
  boot kernel: version 8.4.1.0
Currently scheduled reboot time: none
```

Converting the Switch Software Image from ENOS to CNOS

The new Lenovo Cloud Network OS image cannot coexist on the switch with your legacy 8.x Lenovo NOS. All previous configuration will be lost. If you are running Lenovo NOS 8.x, follow these instructions to replace the operating system with Lenovo CNOS.

To download all necessary software images, go to the following website:

http://support.lenovo.com

1. Connect to the switch through the console terminal. Make sure you are running Lenovo NOS 8.4.1 or later.

   To determine the software version currently used on the switch, use the following switch command:

   ```
   G8296> show version [brief]
   ```

   If you are running a version of Lenovo ENOS earlier than 8.4.1, download and install a more recent version of the Lenovo NOS image before going to the next step.

2. From the 8.4.1 or later image, download the Cloud NOS image:

   ```
   G8296> enable
   G8296# copy tftp image1 address <TFTP server address> filename <location on TFTP
   server relative to tftpboot location>/G8296-CNOS-10.8.2.0.imgs mgt-port
   ```

   Note: CNOS consists of a single image to install that contains all components, including boot and operating system.

   During the download, you are presented with the following message:

   ```
   WARNING: This is the ONLY region with valid bootable image.
            If download fails, switch will not be able to boot.
            Please download into image2 to prevent potential fatal error!

   Confirm overwriting the ONLY bootable image (y/n) ?
   ```

   Enter **y** to continue.

   ```
   Confirm overwriting the ONLY bootable image (y/n) ? y
   Image download started to image1
   File appears valid
   Download in progress
   ........................
   ```

3. When the image is successfully downloaded, the switch will ask you to confirm the update:

```
Download Complete
Valid image detected.
Processing 10.x upgrade image - all data in /user will be lost, including
configuration
Confirm upgrade (y/n) ?
```

Enter **y** to continue.

```
Confirm upgrade (y/n) ? y
```

4. When the download has completed, reset the switch:

```
G8296# reload
Reset will use software "image1" and the active config block.
>> Note that this will RESTART the Spanning Tree,
>> which will likely cause an interruption in network service.
Confirm reload (y/n) ?
```

Enter **y** to continue the reload.

5. When the switch finishes rebooting, log in and verify the image to make sure it is the correct image running the correct version of the software:

```
G8296> enable
G8296# display boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.8.2.0, downloaded 08:56:56 UTC Tue Feb 7 2017
  standby image: version 10.8.2.0, downloaded 10:56:42 UTC Tue Feb 7 2017
  Uboot: version 10.8.2.0, downloaded 08:56:58 UTC Tue Feb 7 2017
  ONIE: version 10.8.2.0, downloaded 14:48:08 UTC Tue Feb 7 2017
Currently set to boot software active image
Current port mode: default mode
```

Note: If this is first time switching NOS versions the image version may appear as unknown. To fix this:

6. Reinstall the CNOS image again following standard image install methods:

```
G8296# cp tftp tftp://<TFTP server address>/G8296-CNOS-10.8.2.0.imgs
system-image all vrf management
Confirm download operation? (y/n) [n] y
```

7. When prompted to change the active boot image to the standby image, enter **y** to confirm:

```
Boot loader now contains Software Version 10.8.2.0
Standby image now contains Software Version 10.8.2.0
Switch is currently set to boot active image.
Do you want to change that to the standby image? (y/n) [n] y
Switch is to be booted with standby image.
```

Note: After this step, reloading the switch is not mandatory.

Supplemental Information

This section provides additional information about configuring and operating the G8296 and CNOS.

The Boot Management Menu

The Boot Management menu allows you to switch the software image or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **Shift + B**. The Boot Management menu appears.

```
The system is going down for reboot NOW!
INIT: reboot: Restarting system
...

Press shift-B for startup menu or shift-R for recovery mode: ..
Running Startup Menu
...

Boot Management Menu
        I - Change booting image
        C - Change configuration to factory default
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        P - Reset the Network Administrator (admin) password
        B - Reset the password required to enter privileged exec mode
        Q - Reboot
        E - Exit
Please choose your menu option:
```

The Boot Management menu allows you to perform the following actions:

● To change the booting image, press **I** and follow the screen prompts.

● To reset the switch configuration to factory defaults, press **C** and follow the screen prompts.

● To boot in recovery mode, press **R**.

● To reset the Network Administrator account (admin) password, press **P** and follow the screen prompts.

● To reset the password required to enter Privileged EXEC configuration mode, press **B** and follow the screen prompts.

● To reload the switch, press **Q**. The reloading process will start again.

● To exit the Boot Management menu, press **E**. The reloading process continues.

Recovering from a Failed Software Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.

2. Open a terminal emulator program that supports TFTP (preferred) or Xmodem download (for example, HyperTerminal, SecureCRT, PuTTY). If using Xmodem, make sure the following settings are in effect:

    *   Speed: 9,600 bps
    *   Data Bits: 8
    *   Stop Bits: 1
    *   Parity: None
    *   Flow Control: None

3. To access the Boot Management menu, you must interrupt the boot process from the Console port. Boot the G8296, and when the system begins displaying Memory Test progress (a series of dots), press **Shift + B**. The Boot Management menu will display:

```
The system is going down for reboot NOW!
INIT: reboot: Restarting system
...

Press shift-B for startup menu or shift-R for recovery mode: ..
Running Startup Menu
...

Boot Management Menu
        I - Change booting image
        C - Change configuration to factory default
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        P - Reset the Network Administrator (admin) password
        B - Reset the password required to enter privileged exec mode
        Q - Reboot
        E - Exit
Please choose your menu option:
```

4. Select **R** for Boot in recovery mode. You will see the following display:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit


Option?:
```

- If you choose option **T** (TFTP download), go to step 5.

- If you choose option **X** (Xmodem serial download), go to step 6.

5. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
IP addr    :
Server addr:
Netmask    :
Gateway    :
Image Filename:
```

a. Enter the required information and press **Enter**.

b. You will see a display similar to the following:

```
Host IP    : 10.10.98.110
Server IP  : 10.10.98.100
Netmask    : 255.255.255.0
Broadcast  : 10.10.98.255
Gateway    : 10.10.98.254
Installing image G8296-CNOS-10.8.2.O_OS.imgs from TFTP server
10.10.98.1OO
```

c. When you see the following prompt, enter the image number where you want to install the new software and press **Enter**.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

d. The following message is displayed when the image download is complete. Continue to step 7.

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option?:
```

6. **Xmodem download**: When you see the following message, change the Serial Port characteristics to 115,200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

a. Press **Enter** to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start XModem on your terminal emulator.

b. When you see the following message, change the Serial Port characteristics to 9,600 bps:

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

c. When you see the following prompt, enter the image number where you want to install the new software and press **Enter**.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

d. The following message is displayed when the image download is complete. Continue to step 7.

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option?:
```

7. Image recovery is complete. Perform one of the following steps:

- Press **R** to reboot the switch

- Press **E** to exit the Boot Management menu

- Press **Esc** to re-display the Boot Management menu

New Features in This Release

This release of Lenovo Cloud Network OS contains the following significant fixes, enhancements, and other changes.

802.1Q encapsulation

802.1Q encapsulation inserts a 802.1Q tag into Ethernet frames transmitted through a Layer 3 routed port that identifies to which VLAN the frame belongs.

802.1Q encapsulation adds a 802.1Q tag after the source and destination MAC address fields of the outgoing routed packet. The tag contains the VLAN identifier which can be configured for each Layer 3 routed interface.

BGP Unnumbered and BFD

BGP unnumbered can be used in conjunction with Bidirectional Forwarding Detection (BFD). It extends the capabilities of BGP unnumbered to make setting up large configurations easier and faster by enabling BFD on all BGP unnumbered neighbors.

Changing the Default Network Administrator Password

After logging onto the switch for the first time or after updating the switch firmware to 10.8 from an earlier version, a screen prompt appears requesting you to change the default network administrator password.

```
You are required to change your default 'admin' user password immediately
Changing password for admin.

Current Administrator password:

Choose a strong password (Min 8 chars, at least 1 uppercase, 1 lowercase,
1 number etc.)
New Administrator password:
Retype new Administrator password:
```

You must enter the current network administrator password, then set up a new password and then enter it a second time for confirmation.

CNOS requires the use of strong passwords for users to access the switch. Strong passwords enhance security because they make password guessing more difficult.

Data Center Interconnect

Data Center Interconnection (DCI) is a wide area architecture between data centers. It ensures that data is consistent, it allows virtualized workloads to be moved quickly, and it makes for an easier deployment of high availability solutions between different geographical locations.

DCI enables the bridging of Layer 2 services between multiple locations across existing Layer 3 IP networks. Virtual Extensible LAN (VXLAN) provides a high availability DCI framework for connecting two or more data centers. It does not require specialized hardware and it is deployable using any network devices that support VXLAN.

Lenovo offers a DCI solution that can be configured statically or by using Multi-protocol Border Gateway Protocol (MP-BGP) Ethernet Virtual Private Network (EVPN). High Availability (HA) topologies using Virtual Link Aggregation Group (vLAG) are possible for both configuration options.

Explicit Congestion Notification

Explicit Congestion Notification (ECN) extends the functionality of Weighted Random Early Detection (WRED) by marking packets instead of discarding them when the average queue length exceeds the configured threshold. Network devices configured with WRED and ECN use the marking of packets as a signal that the network is congested and packet transmission is slowed down.

IPv4 Next-hop Health Check

IPv4 next-hop health checking is used to verify if the IPv4 next-hop is reachable or not. It uses Address Resolution Protocol (ARP) to periodically send ARP request to the next-hops that have associated routes present in the switch's routing table.

Lenovo Intelligent Network Controller

Lenovo Intelligent Network Controller (LINC) is a Software-Defined Networking (SDN) solution from Lenovo which provides network virtualization with service chaining capability to offer flexibility, agility, and scalability needed for modern cloud data centers.

Lenovo Intelligent Network Controller is based on the OpenContrail R3.2 release.

Multiple VRF Instances

CNOS now supports multiple Virtual Routing and Forwarding (VRF) instances. VRF allows multiple instances of a routing table to coexist and to work simultaneously on a switch. You can segment network paths without using multiple devices while running separate routing protocol instances and forwarding tables.

VRF now supports up to nine instances: eight instances for data traffic and one instance for management traffic.

Private VLANs

Private VLANs provide Layer 2 isolation between the ports within the same broadcast domain. Private VLANs can control traffic within a VLAN domain and provide port-based security for host servers.

REST/Python API Enhancement

REST and Python APIs have been introduced or updated for the following:

- OSPF
- BGP DiffServ Code Point (DSCP) marking
- Routes Maps (GET only)
- 802.1Q Encapsulation
- IPv4 Next-hop Health Check
- Network Time Protocol (NTP)
- Network Virtualization (NWV)
- Private VLANs
- Virtual Extensible LAN (VXLAN)
- Data Center Interconnect (DCI)
- Telemetry
- Secure Shell (SSH)
- SSH Public Key Authentication
- Telnet
- Network Policy Agent (NPA)
- REST Server
- Hardware Switch Controller (HSC)

Secure Hash Algorithm

Network Time Protocol (NTP) now supports Secure Hash Algorithm 1 (SHA-1) encrypted authentication.

Open Shortest Path First (OSPF) and Bidirectional Forwarding Detection (BFD) now support SHA-2 encrypted authentication.

SSH Public Key Authentication

Public Key Authentication (PKA) is a cryptographic system that offers an alternative for local SSH authentication, by providing the switch with a pair of keys: a public key and a private key.

When connecting to switch via SSH, the SSH server encrypts messages exchanged during the session using the public key. Only the SSH client that has the matching private key can decrypt the messages and thus successfully authenticate with the SSH server.

System Logging Enhancement

When configuring remote syslog servers on the switch, you can now also specify the transport protocol (TCP or UDP) and the port used for communication.

User Action Logging Enhancement

User actions executed on the switch are logged and saved to a file without displaying them on the console, or on Telnet and SSH terminals. User action logging has a severity level of informational (6).

You can now enable user action logging when using the CLI, REpresentational State Transfer (REST), or Simple Network Management Protocol (SNMP).

vSphere Distributed Switch Support for ThinkAgile Network Orchestrator

The ThinkAgile Network Orchestrator (TNO) now supports VMware's vSphere Distributed Switch (vDS) through integration with vCenter. TNO can be used with both VMware and Nutanix environments. TNO's dynamic port and security (QoS) configuration is now integrated with VMware's distributed vSwitch.

Known Issues

This section describes known issues for CNOS 10.8 on the Lenovo RackSwitch G8296.

Note: Please check the Change History documentation posted with the Switch Firmware to check if any of these issues have been fixed in the latest release.

BGP

When the switch detects that it cannot reach the next-hop in a route, the BGP instance does not deactivate the route from its routing table. The route is deactivated only when the BGP session with the next-hop times out. (ID: 135910)

Copying Configuration Files

When copying a new configuration file over the switch's current running configuration, CNOS does not overwrite the old configuration. Instead, it appends the new configuration over the old one, leaving settings that are not present in the new configuration intact. It only overwrites settings present in both configurations. (ID: 133055)

Firmware Downgrade

When performing a firmware downgrade from CNOS 10.7 or later to CNOS 10.6 or an earlier version, the following warning message appears:

```
WARNING: Downgrade from 10.7.x or later to 10.6.x or earlier version
detected. This downgrade would require a manual configuration change when
the switch comes up on 10.6.x or earlier version. Prior to proceeding
with the downgrade, please keep 10.6.x or earlier version startup-config
file handy by using 'copy file config-10.6' command.
```

The warning message is incorrect. The actual command is:

```
G8296# copy file config-10-6
```

The warning message will be corrected in the next firmware release. (ID: 141384)

LACP

The default behavior of Link Aggregation Control Protocol (LACP) Individual has been changed. Now, by default, LACP enabled ports transition to suspend.

When upgrading the firmware to CNOS 10.8 from 10.7 or an earlier version, the following LACP behavior occurs:

- For Link Aggregation Groups (LAGs) with default configuration, before the upgrade, LACP enabled ports transition to individual state when not receiving Link Aggregation Control Protocol Data Units (LACPDUs). After the firmware upgrade, the LACP configuration remains the same, but LACP enabled ports now transition to suspended state when no LACPDUs are received.

  To configure the LACP enabled ports as individual, use the following command on a LAG:

  ```
  G8296(config)# interface port-channel <LAG number (1-4096)>
  G8296(config-if)# no lacp suspend-individual
  ```

- For LAGs with non-default configuration, if before the upgrade LACP enabled ports transition to suspended state when not receiving LACPDUs, then after the firmware upgrade this behavior remains the same. However, the LACP configuration is changed to reflect the new default behavior: the LACP individual setting for LAGs is removed from the switch's running configuration. (ID: 132111)

Network Virtualization Gateway

The following limitations exist:

- For optimal performance, we recommend that the number of VLAN-VXLAN Network Identifier (VNI) mappings does not exceed 1,000 entries. Going above this limit leads to longer convergence times when attaching or detaching the Lenovo hardware Layer 2 gateway to or from NSX logical switches. (ID: 99467)

- For optimal Equal Cost Multiple Paths (ECMP) load balancing, we recommend that only Layer 3 routed ports are used for connecting to spine switches. (ID: 123627)

- When broadcast, unknown unicast, and multicast (BUM) traffic is received on the switch, it is replicated on all member ports of the same VXLAN Network, except the port that is the source port of the BUM traffic. This is displayed in the source port statistics as dropped packets. (ID: 95658)

- Throughput statistics of the southbound interface of the VXLAN gateway do not display on the NSX GUI. (ID: 113832)

- After Bidirectional Forwarding Detection (BFD) failover, when using the default value for the probe interval of 300 ms, the active service node election takes approximately three seconds to occur. (ID: 116882)

- The VLAN used in VLAN-VXLAN Network Identifier (VNI) mapping must be used exclusively for switching within the associated VNI domain. Different access vPorts belonging to the same VLAN must be mapped to the same VNI. Hence, only one-to-one VLAN-VNI bindings are supported. (ID: 100606, 123143)

- In case all network ports go down on one of the vLAG switches, all ingress traffic received on the local access ports is flooded to all other local access ports from the same VXLAN Network Identifier (VNI). Flooding stops when the network ports are back up. (ID: 110732)

- In High Availability (HA) mode, the recommended maximum number of local unicast MAC addresses is 32,000. If this limit is exceeded, MAC address synchronization between the vLAG switches might not work properly. More than 32,000 unicast MAC addresses can be used, but the synchronization process fails to function normally. (ID: 113145)

REST API

VMware vSphere Distributed Switch (vDS) information retrieval is not supported using REST API. (ID: 138329)

SolarWinds

After setting up a SFTP/SCP server using SolarWinds, the switch fails most times to establish a connection to the server. We recommend using other SFTP/SCP servers. (ID: 135539)

System Logging

The switch does not send syslog messages to syslog servers defined using DNS that are accessible through the default Virtual Routing and Forwarding (VRF) instance. DNS defined syslog servers using the management VRF instance are able to receive syslog messages from the switch. (ID: 135438)

Telemetry

Sometimes, when the egress CPU queue is full, Buffer Statistics Tracking (BST) gets disabled and telemetry messages are no longer sent to remote monitoring servers. Use REST to re-enable BST. (ID: 139654)

vLAG

When upgrading the firmware of vLAG peer switches one by one to CNOS 10.8 from 10.7 or an earlier version, vLAG configuration consistency checks fail on both vLAG peer switches until the upgrade process is complete for both. (ID: 131917)