Lenovo RackSwitch G8332

Release Notes

For Enterprise Network Operating System 8.4

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.

First Edition (September 2016)

Release Notes

This release supplement provides the latest information regarding Lenovo Enterprise Network Operating System 8.4 for the Lenovo RackSwitch G8332 (referred to as G8332 throughout this document).

This supplement modifies and extends the following Enterprise NOS documentation for use with *NOS* 8.4:

- *Lenovo RackSwitch G8332 Application Guide for Lenovo Enterprise Network Operating System* 8.4
- *Lenovo RackSwitch G8332 Command Reference for Lenovo Enterprise Network Operating System* 8.4
- *Lenovo RackSwitch G8332 Installation Guide*

The publications listed here are available from the following website:

http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp

Please keep these release notes with your product manuals.

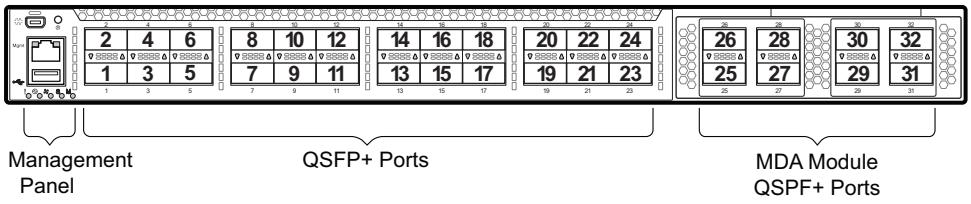
Hardware Support

Enterprise NOS 8.4 software is supported on the G8332, a high performance Layer 2-3 network switch

The G8332 is a 1U rack-mountable aggregation switch used for combining traffic from multiple high-speed server racks. The G8332 uses a wire-speed, non-blocking switching fabric that provides simultaneous wire-speed transport of multiple packets at low latency on all ports.

- Twenty-four 40 Gigabit Ethernet (GbE) Quad Small Form Pluggable Plus (QSFP+) ports, each of which can optionally be used as four 10 GbE SFP+ ports
- Eight additional 40 GbE QSFP+ ports through the Media Dependent Adapter (MDA) module

Figure 1. RackSwitch G8332 front panel



Updating the Switch Software Image

The switch software image is the executable code running on the G8332. A version of the image comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software supported for your G8332, go to the following website:

http://www.support.lenovo.com/

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

```
RS 8332> show version
```

The typical upgrade process for the software image consists of the following steps:

- Load a new software image and boot image onto an SFTP, FTP, or TFTP server on your network.
- Transfer the new images to your switch.
- Specify the new software image as the one which will be loaded into switch memory the next time a switch reset occurs.
- Reset the switch.

For instructions on the typical upgrade process, see "Loading New Software to Your Switch" on page 6.

Loading New Software to Your Switch

The G8332 can store up to two different switch software images (called `image1` and `image2`) as well as special boot software (called `boot`). When you load new software, you must specify where it should be placed: either into `image1`, `image2` or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

Attention: When you upgrade the switch software image, always load the new boot image and the new software image before you reset the switch. If you do not load a new boot image, your switch might not boot properly (To recover, see "Recovering from a Failed OS Image Upgrade" on page 10).

To load a new software image to your switch, you will need the following:

- The image and boot software loaded on an SFTP, FTP, or TFTP server on your network.

  Note: Be sure to download both the new boot file and the new image file.

- The hostname or IP address of the SFTP, FTP, or TFTP server.

  Note: The DNS parameters must be configured if specifying hostnames.

- The name of the new software image or boot file.

When the software requirements are met, use the following procedures to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

```
RS 8332# copy {sftp|tftp|ftp} {image1|image2|boot-image}
```

2. Enter the hostname or IP address of the SFTP, FTP or TFTP server.

```
Address or name of remote host: <name or IP address>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

   The exact form of the name will vary by server. However, the file location is normally relative to the SFTP, FTP or TFTP directory (for example, `tftpboot`).

4. If required by the SFTP, FTP or TFTP server, enter the appropriate username and password.

5. The switch will prompt you to confirm your request.

   Once confirmed, the software will begin loading into the switch.

6. When loading is complete, use the following commands to enter Global Configuration mode to select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot:

```
RS 8332# configure terminal
RS 8332(config)# boot image {image1|image2}
```

   The system will then verify which image is set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

7. Reboot the switch to run the new software:

```
RS 8332(config)# reload
```

   The system prompts you to confirm your request. Once confirmed, the switch will reboot to use the new software.

   Note: If you select "No" when asked to confirm the reload, any changes made to the configuration since the last reboot will be lost.

Updating vLAG Switches with Lenovo Network Enterprise OS 8.x

Following are the steps for updating the software and boot images for switches configured with vLAG:

1. Save the configuration on both switches using the following command:

```
RS 8332# copy running-config startup-config
```

2. Use FTP, STFP, or TFTP to copy the new Networking OS and boot images onto both vLAG switches. For more details, see "Loading New Software to Your Switch" on page 6.

3. Shutdown all ports except the ISL ports and the health check port on the primary switch (Switch 1).

   Note: Do not save this configuration.

4. Reload Switch 1. Switch 2 will assume the vLAG primary role. Once Switch 1 has rebooted, Switch 1 will take the vLAG secondary role.

5. Shutdown all ports except the ISL ports and the health check port on Switch 2.

   Note: Do not save this configuration.

6. Reload Switch 2. Switch 1 will assume the vLAG primary role. Once Switch 2 has rebooted, make sure that Switch 1 is now the vLAG primary switch and Switch 2 is now the vLAG secondary switch.

7. Verify the all the vLAG clients have converged using the following command:

```
RS 8332> show vlag information
```

Supplemental Information

This section provides additional information about configuring and operating the G8332 and Enterprise NOS.

The Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, 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.

```
Resetting the System ...
Memory Test ..............................
.
.
Boot Management Menu
        I - Change booting image
        C - Change configuration block
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        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 change the configuration block, press **C**, and follow the screen prompts.
- To perform a TFTP/Xmodem download, press **R** and follow the screen prompts.
- To reboot the switch, press **Q**. The booting process restarts.
- To exit the Boot Management menu, press **E**. The booting process continues.

Recovering from a Failed OS Image Upgrade

The Boot Management menu allows you to perform fundamental device management operations, such as selecting which software image will be loaded, resetting the G8332 to factory defaults or recovering from a failed image download.

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

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, SecureCRT, or PuTTY) and select the following serial port characteristics:
   - 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 G8332 and when the system begins displaying Memory Test progress (a series of dots), press **<Shift + B>**.

   The Boot Management menu will display:

```
Resetting the System ...
Memory Test ..............................
.
.
Boot Management Menu
        I - Change booting image
        C - Change configuration block
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        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)
        R) Reboot
        E) Exit

Option?:
```

   - If you choose option **X** (Xmodem serial download), go to Step 5.
   - If you choose option **T** (TFTP download), go to Step 6.

5. **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. You will see a display similar to the following:

```
... Waiting for the <Enter> key to be hit before the download can
start...
CC
```

   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, press **<Enter>** to start installing the image. If the file is a software image, enter the image number:

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

   The image install will begin. After the procedure is complete, the Recovery Mode menu will be re-displayed.

```
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)
        R) Reboot
        E) Exit

Option?:
```

   Continue to Step 7.

6. **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>**. 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 G8332-8.4.1.0_OS.imgs from TFTP server 10.10.98.100
```

   b. If the file is a software image, you will be prompted to enter an image number:

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

   The following message is displayed when the image download is complete:

```
Image2 updated succeeded
Updating install log. File G8332-8.4.1.0_OS.imgs installed from
10.10.98.100 at 15:29:30 on 12-3-2015
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)
        R) Reboot
        E) Exit

Option?:
```

   Continue to Step 7.

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 the Escape key (**<Esc>**) to re-display the Boot Management menu.

Recovering from a Failed Boot Image Upgrade

Use the following procedure to recover from a failed boot image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (such as HyperTerminal, CRT, or PuTTY) and select the following serial port characteristics:
   - Speed: 9600 bps
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift B>** while the Memory Test is in progress and the dots are being displayed.
4. Select **R** to boot in recovery mode. Then choose option **X** (Xmodem serial download). You will see the following display:

```
Perform xmodem download

To download an image use 1K Xmodem at 115200 bps.
```

5. When you see the following message, change the Serial Port characteristics to 115200 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.You will see a display similar to the following:

```
Extracting images ... Do *NOT* power cycle the switch.
**** RAMDISK ****
UnProtected
38 sectors
Erasing Flash...
................................... done
Erased 38 sectors
Writing to Flash...9....8....7....6....5....4....3....2....1....done
Protected 38 sectors
**** KERNEL ****
UnProtected
24 sectors
Erasing Flash...
....................... done
Erased 24 sectors
Writing to Flash...9....8....7....6....5....4....3....2....1....
```

   b. When you see the following message, change the Serial Port characteristics to 9600 bps:

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

   Boot image recovery is complete.

New and Updated Features

Enterprise NOS 8.4 for the G8332 has been updated to include several new features, summarized in the following sections. For more detailed information about configuring G8332 features and capabilities, refer to the complete Enterprise NOS 8.4 documentation as listed on page 3.

NSX Gateway for vSphere

NSX is a VMware virtualized network platform that offers the operational model of a virtual machine over a network. Virtual networks function in a similar way to virtual machines for computers. NSX builds virtual networks inside software, providing a full set of networking services, such as logical switching, routing, firewall, load balancing, VPN, quality of service (QoS), and monitoring.

The integration of NSX and Lenovo switches offers the following benefits to deploying network virtualization within software defined cloud networking:

- Virtual and physical workloads can be connected upon demand on a common logical segment regardless of hypervisor, IP subnet, or physical location.
- Holistic views of the virtual and physical topology increase operational efficiency.
- Network virtualization with NSX does not require IP multicast to learn or forward broadcast, unknown unicast, or multicast packets.
- A single point of management and control (NSX API) can be used for configuring logical networks across hypervisors and physical access switches.

Note: Lenovo is actively working with VMware to complete the certification for NSX Gateway for vSphere. NSX Gateway for vSphere support is available in this release while VMware certification is pending. Lenovo will fully support the NSX Gateway for vSphere implementation throughout the certification process. Please work with the controller vendor on issues related to the controller.

TACACS+ Two Level Authentication

When TACACS+ is used to control switch access and the CLI Enable Mode is configured to require a password, a second authentication for the Enable command will be required.

Easy Connect

This feature is designed to simplify switch configuration by applying pre-defined configuration modes. Once launched, the user is prompted to input certain parameters (such hostname, netmask, server and uplink ports, and vLAG information) and this feature will automatically custom configure the switch.

Support for 256 PVRST Instances

The number of STP groups supported in the PVRST protocol has been increased to 256. For optimal performance, it is recommended that you stay wtihin a maximum of 14 interfaces or aggregated links (including vLAGs) with 4K MAC table entries when deploying 256 STP groups.

Security Feature Support

This feature supports Secure I/O Module (SIOM) framework by managing security policies based on the IOM mode (Secure/Legacy). A secure version of LDAP using startTLS and LDAPS is supported. Cryptographic Provisioning is also supported.

Certificate Signing Request (CSR)

This feature enhances the certificate management capabilities on the switch by incorporating the ability to generate a Certificate Signed Request which can be submitted to an external Certificate Authority (CA) for obtaining a signed certificate. The capability to support CSR and process the CA signed certificate thereof is made available from multiple user interfaces including BBI, SNMP, and CLI.

Password Encryption

This feature enables all passwords in the switch to be encrypted using industry-standard encryption methods.

ACL Redirect to Trunk Support

This feature enables the switch to steer traffic based on a combination of a physical port and Layer 2-4 protocol header fields.

vLAG Peer Gateway

This feature enables a vLAG switch to act as an active gateway for packets that are addressed to the router MAC address of the vLAG peer.

SNMPv1 Default Community String Removal

This feature removes the default read/write community string for SNMP v1/2c from the factory default configuration.

Default UserID with Default Password That Must Be Reset at First Login

This feature adds a default user "`USERID`" at UID 1 with default password "`PASSW0RD`" and prompts for a change of the default password at first login.

Two-Tier vLAG (4xVRRP w/vLAG)

VRRP can work as Full Active-Active or Half Active-Active under a two tier vLAG topology. Full Active-Active means both two tier vLAGs can route L3 traffic for the related VRRP domain. Half Active-Active means vLAGs will do L2/L3 forwarding for the related VRRP domain based on the local and peer VRRP role.

DHCP Snooping

DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers. It provides security by filtering untrusted DHCP packets and by building/maintaining a DHCP Snooping binding table.

Configurable Syslog Port

This feature adds support for a configurable syslog host server port for both primary and secondary syslog host servers.

STP Debugging Enhancement

The STP display has been enhanced to display the current and previous STP STG root information.

SLP IPv6 Support

SLP has been enhanced with support for IPv6.

Known Issues

This section describes known issues for Enterprise NOS 8.4 on the Lenovo RackSwitch G8332.

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

Debug

Enterprise NOS debug commands are for advanced users. Use the debug commands with caution as they can disrupt the operation of the switch under high load conditions. This could be dangerous in mission-critical production environments. Before debugging, check the MP utilization to verify there is sufficient overhead available for the debug functionality. When debug is running under high load conditions, the CLI prompt may appear unresponsive. In most cases, control can be returned by issuing a `no debug` <*function*> command.

- Enterprise NOS debug commands are for advanced users. Use the debug commands with caution as they can disrupt the operation of the switch under high load conditions. This could be dangerous in mission-critical production environments. Before debugging, check the MP utilization to verify there is sufficient overhead available for the debug functionality. When debug is running under high load conditions, the CLI prompt may appear unresponsive. In most cases, control can be returned by issuing a `no debug` <*function*> command.
- Removing the MDA board while the switch is operating, without prior MDA shutdown, may generate the following error message:

  ```
  i2cWrite_byte MDA LM75 0:0xee @ 0x00 1 Error 5 (1)
  ```

  This error is not critical and does not interfere with any switch functionality (ID: XB262550, XB264278).

EVB

When a VM cannot be associated, the console may be flooded with syslog messages stating that the validation has failed. (ID: XB191291)

FCoE

- Globally enabling or disabling CEE may halt L3 traffic. To avoid this, temporarily suspend data traffic when changing CEE settings. Otherwise, reload the switch to fix the disrupted traffic. (ID: XB137860)
- When using static trunks to set up FCoE links between two switches, both participating switches must have their corresponding portchannels enabled. Otherwise, multicast frames may enter loops and cause frame drops. (ID: XB260972)
- After enabling FIP snooping on an FIP Snooping Bridge, it may take up to two minutes for the FCoE sessions to initiate. (ID: XB262043)

- When displaying FC zone status information for a VLAN, the PWWN member count indicates the number of unique members, instead of the total number. PWWN members that belong to multiple zones, are counted only once. (ID: XB256730, XB258881)
- When changing the FIP Keep Alive Advertisement period, it is recommended to wait for a duration five times longer than the highest value in the interval before submitting another change. For instance, when increasing the period from 20 to 75 seconds, or decreasing it from 75 to 45 seconds, it is recommended to wait for 75 x 5 = 375 seconds before changing it again.

  It is also recommended to divide large FIP Keep Alive Advertisement period changes in smaller increments. For instance, if lowering the value from 90 seconds to 4 seconds, you should lower it from 90 to 20 seconds in a first stage and, after waiting for 90 x 5 = 450 seconds, lower the period from 20 to 4 seconds in a second stage. (ID: XB268990)

IGMP

- The switch keeps forwarding IPMC traffic with IP options to multicast routers after the IGMP group expires. (ID: XB256781)
- Avoid scenarios where IGMP is enabled on one VLAN while another VLAN has flooding disabled (but no IGMP configuration). Otherwise, the report processing mechanism may, after several minutes, generate out of memory messages for reports sent at a high rate over multiple member ports in the VLAN with flooding disabled. To avoid this, lower the IGMP CoPP rate to 2000 pps or less, or stop the IGMP reports stream. (ID: XB258760)

Jumbo Frames

All jumbo frames are counted as multicast packets on the ingress ports. (ID: XB261919)

LACP

Up to 104 portchannels can be created, but the verified scaling limit is 64 portchannels

MDA

Repeatedly enabling and disabling the MDA board may lock up random ports. To fix this, remove and reinstall the affected transceiver. (ID: XB263409)

MLD

In case the multicast flooding feature is disabled, MLD packets are still software flooded for at least one IPv6 interface configured. It does not have to be linked to the VLAN where the MLD packets need to be flooded. (ID: LV305657)

NAT

DNAT+NAPT rules that map destination IP addresses between the default and the inside/outside realm will route packets at CoPP rates if only the destination IP addresses match, wile the destination port numbers do not match. To avoid this:

- Do not create DNAT rules mapping destination IPs between the default realm and the inside/outside realm.
- Do not create DNAT+NAPT rules that do not match the packets' L4 destination port numbers.
- If either of these are unavoidable, define additional DNAT+NAPT rules to match all the L4 destination ports employed in traffic. (ID: XB266690)

OpenFlow

- Static FDB flows are stored as ACL flows. (ID: XB262456)
- Using a port.mod message to change the OFPPC_NO_FLOOD bit does not reprogram the already installed flows. (ID: XB259385)
- When you configure a port to use OpenFlow, spanning tree protocol is automatically disabled on that port. (ID: XB266710)

PIM

Receiving multicast packets at rates of 1,000,000 pps, or within the 100K . 111K pps range, causes slow learning for (S, G) entries. To avoid this, configure the Control Plane Protection bandwidth for the unknown?]destination packets (queue 0 by default) to a prime number larger than 1000 as shown in the following example:

```
RS 8332(config)# qos protocolpacketcontrol ratelimitpacketqueue 0 2113
```

(ID: XB261554)

QSFP+

When changing a QSFP port from 10G mode to 40G mode, a port error will occur if any previously configured 10G port settings do not apply to the new 40G state, preventing further configuration of the port. The administrator must manually clear the 10G port settings that do not apply to 40G prior to changing modes. (ID: 62576)

SLP

Abbreviated IPv6 addresses are not supported in Service Location Protocol (SLP) strings. All IPv6 addresses used in SLP request strings must be extended. For example, the SLP request:

```
slptool findattrs
service:io-device.Lenovo:management-module://2001::1
```

will not work. Instead, you must use the extended form of the IPv6 address:

```
slptool findattrs
service:io-device.Lenovo:management-module://2001:0000:0000:
0000:0000:0000:0001
```

Virtual Aggregation Link Groups (vLAG)

- If Protocol Independent Multicast (PIM) is configured in a VLAG topology, when disabling and re-enabling IGMP or IGMP snooping on a secondary VLAG switch, some of the PIM outgoing interfaces may fail to change back from forwarding to pruned state. To limit this issue, it is recommended to wait at least 1 minute between disabling and enabling back IGMP or IGMP snooping on a secondary VLAG switch when running PIM. (ID: XB264621)
- VLAG scalability is limited by system load. Under heavy load, when disabling and enabling back multiple VLAG instances on a switch, some of the instances on its peer may remain in LOCAL-UP state instead of changing to FORMED state. (ID: XB263527)

VRRP

Virtual router interfaces do not support Telnet sessions. (ID: XB255037)