

Lenovo RackSwitch G8124-E

Release Notes

for Networking OS 8.3

LenovoTM

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 (August 2015)

© Copyright Lenovo 2015
Portions © Copyright IBM Corporation 2014.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

Release Notes

This release supplement provides the latest information regarding Lenovo Networking OS 8.3 for the Lenovo RackSwitch G8124-E (referred to as G8124-E throughout this document).

This supplement modifies and extends the following Lenovo N/OS documentation for use with N/OS 8.3:

- *Lenovo RackSwitch G8124-E Application Guide for Networking OS 8.3*
- *Lenovo RackSwitch G8124-E ISCLI Command Reference for Networking OS 8.3*
- *Lenovo RackSwitch G8124-E Installation Guide*

The publications listed above 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.

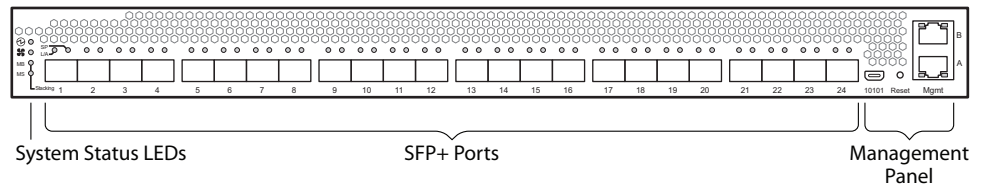
Hardware Support

N/OS 8.3 software is supported on the G8124-E, a high performance Layer 2-3 network switch.

The G8124-E contains 24 ten Gigabit Small Form-factor, Pluggable (SFP+) slots and two 1Gb management ports. The 10Gb SFP+ slots can accept 1Gb copper transceivers, 10Gb optical transceivers, or Direct Attach Cables (DAC).

Note: If a DAC is not programmed to meet MSA specifications (including length identifier), the switch disables the port and generates a syslog message indicating that the DAC is not approved.

Figure 1. RackSwitch G8124-E front panel:



Updating the Switch Software Image

The switch software image is the executable code running on the G8124-E. 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 G8124-E, 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 G8124E# 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 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.

Note: Due to Lenovo firmware security guidelines, it is not possible at this time to upgrade or migrate a switch from IBM Networking OS to Lenovo Networking OS.

Updating VLAG Switches with Lenovo Networking OS 8.x

Following are the steps for updating the software image and boot image for switches configured with VLAG:

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

```
RS G8124E(config)# copy running-configuration startup-configuration
```

2. Use TFTP or FTP to copy the new OS image and boot image onto both vLAG switches.
3. Shut down 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
5. Once Switch 1 has rebooted, Switch 1 will take the secondary role.
6. Shut down all ports except the ISL ports and the health check port on Switch 2.

Note: Do not save this configuration.

7. Reload Switch 2, Switch 1 will reassume the vLAG primary switch role.
8. Once Switch 2 has reloaded, make sure Switch 1 has transitioned to vLAG primary and Switch 2 has transitioned to secondary.
9. Verify all the vLAG clients have converged using the following command:

```
RS G8124E(config)# show vlag information
```

Loading New Software to Your Switch

The G8124-E 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 Software Upgrade” on page 9](#)).

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

- The image and boot software loaded on an 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 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 G8124E(config)# copy {sftp|tftp|ftp} {image1|image2|boot-image}
```

2. Enter the hostname or IP address of the 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 FTP or TFTP directory (for example, `tftpboot`).

4. If required by the 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 G8124E# configure terminal  
RS G8124E(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 G8124E(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.

New and Updated Features

N/OS 8.3 for RackSwitch G8124-E has been updated to include several new features, summarized in the following sections. For more detailed information about configuring G8124-E features and capabilities, refer to the complete N/OS 8.3 documentation as listed on [page 3](#).

BGP Pre Append AS path

This enhancement facilitates the process of routing maps by influencing the BGP route selection so that one path is preferred over another. This is especially useful when customers are dual home to two different Internet Service Providers (ISPs) and they want to have a primary path to one ISP and use the other ISP as a backup path.

Dynamic ARP Inspection

This enhancement enables the device to intercept and examine all ARP requests and response packets in a subnet. The feature discards those packets with invalid IP to MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

EasyConnect

This feature is designed to simplify switch configuration by applying predefined configuration modes. Once launched, the user is requested a minimal set of input information (e.g. hostname, netmask, server and uplink ports) and the tool is automatically customizing the switch accordingly.

OpenSSL RC4 Vulnerability

This release disables the usage of the RC4 cipher in the VMWare client to avoid security vulnerabilities.

SNSC

This release adds the option to disable terminal prompting in SNSC.

Spanning Tree Protocol (STP) Range Enhancement

Existing Spanning Tree Protocol (STP) commands now support configuration of a range of STP groups at once. STP range groups configurations are also displayed in a configuration dump.

Supplemental Information

This section provides additional information about configuring and operating the G8124-E and N/OS.

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 at 10:55:49 Sun Apr 19, 2015...
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: I
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

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 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 XModem Download (for example, HyperTerminal, SecureCRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 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 G8124-E, and when the system begins displaying Memory Test progress (a series of dots), press **<Shift B>**. The Boot Management menu will display:

```
Resetting at 10:55:49 Sun Apr 19, 2015..
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 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.
- 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.
```

- 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)      R) Reboot
    E) Exit

Option?:
```

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>**.
- 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 G8124-E-8.2.1.0_OS.img from TFTP server 10.10.98.100
```

- 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)      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 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:
 - o Speed: 9600 bps
 - o Data Bits: 8
 - o Stop Bits: 1
 - o Parity: None
 - o 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 **X** for **Xmodem 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 ****
Un-Protected 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 ****
Un-Protected 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.

VLAGs

For optimal VLAG operation, adhere to the following configuration recommendations:

- Any port-related configuration, such as applied ACLs, must be the same for all ports included in the same VLAG, across both peer switches.
- Configure VLAG health checking as shown in the *Application Guide*.

After configuring VLAG, if you need to change any configuration on the VLAG ports, you must adhere to the following guidelines:

- If you want to change the STP mode, first disable VLAG on both the peers. Make the STP mode-related changes and re-enable VLAG on the peers.
- If you have MSTP on, and you need to change the configuration of the VLAG ports, follow these steps:

On the VLAG Secondary Peer:

1. Shutdown the VLAG ports on which you need to make the change.
2. Disable their VLAG instance using the command:
RS G8124E (config)# no vlag adminkey <key> enable (or)
RS G8124E (config)# no vlag portchannel <number> enable
3. Change the configuration as needed.

On the VLAG Primary Peer:

4. Disable the VLAG instance.
5. Change the configuration as needed.
6. Enable the VLAG instance.

On the VLAG Secondary Peer:

7. Enable the VLAG instance.
8. Enable the VLAG ports.

Note: This is not required on non-VLAG ports or when STP is off or when STP is PVRST.

Known Issues

This section describes known issues for N/OS 8.3 on the RackSwitch G8124-E.

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.

BGP Debug

While enabling or disabling BGP debug for a particular peer/IP address, the logging behavior may not be as expected. Following is a workaround: (ID: 59104)

To enable BGP debug for a particular peer:

1. Enable BGP debug for all the peers.
2. Disable BGP debug for all the peers.
3. Enable BGP debug for a particular peer.

To disable BGP debug for a particular peer:

1. Enable BGP debug for all the peers.
2. Disable BGP debug for all the peers.
3. Enable BGP debug for all the peers except the one for which you want it disabled.

Debug

Lenovo N/OS 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.

Deployment Profiles

- When changing from a different deployment profile, if a resource in the new profile has less capacity than is in use in the prior profile, an error message may be logged when the mode is changed. (ID: 64009)

FCoE

- The FCoE connection between the server and the FCF will be retained even if you disable CEE/FIP/vNIC on the switch. To avoid this scenario, either reboot the switch, or disable and re-enable the ports connected to the sever and the FCF after you disable CEE/FIP/vNIC. (ID:41915)

- By default the "VLAN Name" and "Port and Protocol ID" LLDP TLVs are disabled on a port. These two TLVs are added to the LLDP PDU for each VLAN that is configured in a port. This may cause the length of LLD PDU to exceed the Ethernet packet size if there are nearly 40 or more VLANs configured on a port, or if the VLAN names are too long. There is a possibility that the DCBX TLVs may not be added to the LLDP TLV due to the length. Because of this the FCoE connection will not form on that port. It is recommended to avoid enabling the "VLAN Name" and "Port and Protocol ID" TLV if you have high number of VLANs configured and FCoE is enabled on that port. (ID: 42446)
- The FIP Snooping option for automatic VLAN creation is not recommended for use with the Emulex Virtual Fabric Adapter. Disable automatic VLAN creation when connecting the switch to an Emulex Virtual Fabric Adapter. (ID: 51529)
- When using DCBX to synchronize Priority-base Flow Control (PFC) with a peer (using the PFC TLV option), PFC operation on the switch port will not be disabled as expected when PFC is not available on the peer. To resolve this, manually disable PFC on ports connected to devices that do not participate in PFC. (ID: 62114)
- Disruption to FCoE connections and FCoE traffic may be expected when changing the LACP mode. It is recommended that the administrator halt FCoE traffic before changing any switch configuration. (ID: 67044)

IKEv2

IKEv2 cannot be configured on management ports. Configure IKEv2 only on data ports. (ID: 57427)

IPsec

- When configuring IPsec to operate between Lenovo switches, keys of various lengths are supported. However, when using IPsec to connect with non-IBM devices, the manual policy session keys must be of the following fixed lengths:
 - For the AH key:
 - SHA1 = 20 bytes
 - MD5 = 16 bytes
 - For the ESP auth key:
 - SHA1 = 20 bytes
 - MD5 = 16 bytes
 - For the ESP cipher key:
 - 3DES = 24 bytes
 - AES-cbc = 24 bytes
 - DES = 8 bytes

ISCLI

If a port needs to be a member of more than 500 VLANs, we recommend that you first shutdown the port and then add the port as a member of the VLANs. (ID: 70739)

LACP

Under heavy switch load conditions, LACP links may flap when configured with short timeout mode. To stabilize LACP under heavy load, it is recommended to use the long timeout mode instead. (ID: 66173)

PIM

- PIM may be configured via the ISCLI only. PIM configuration and information is not available using the CLI menu system, the BBI, or via SNMP. (ID: 38443, 39279, 39445, 39849, 40046)
- PIM supports standard multicast frame sizes. However, uncommon use of jumbo frames for multicasts has not been confirmed for PIM operation.
- PIM Source-Specific Multicast (PIM-SSM) is not supported.
- Anycast RP is not supported.
- PIM RP filters are not supported.
- PIM is not supported simultaneously with vNICs or FCoE.
- When using the clear ip pim mroute command to clear a large list of PIM neighbor entries, the PIM state on the switch can lose synchronization with its PIM neighbors. If this occurs, synchronize PIM by globally disabling and then re-enabling PIM on the switch.

OSPF

- Some changes to OSPF configuration (such as creating a new area or changing an area's type) may result in OSPF state reconvergence. (ID: 46445, 48483)
- OSPFv3 over IPsec
 - This combination can only be configured only on a per-interface basis.
 - The current implementation for OSPFv3 allows the use of only one protocol (AH or ESP) at any given time. AH and ESP cannot be applied together.

Ports and Transceivers

- The port speed setting is not configurable for Finisar SFPs. Updating from BLADEOS 6.5 (or prior) to N/OS 6.8 (or later) will result in port speed configuration settings being reset to default values for ports using Finisar SFPs. (ID: 55063)

Private VLANs

- The sequence in which a private VLAN is configured is not the same as displayed in the output of the show running-config command. Hence, if you copy and paste the private VLAN configuration from the output of the above command, the private VLAN configuration will be lost. (ID: 67169)
- Traffic with secondary VLAN ID is not forwarded to promiscuous ports. (ID: 70980)

Routed Ports

SNMP or BBI should not be used to configure routed ports, or to configure any other feature if a routed port is already configured on the switch.

If a routed port is configured on the switch, the configuration, apply, and save commands are not displayed in BBI; in SNMP, you may be able to enter the configuration commands, but you will not be able to save the configuration. (ID: 57983)

SNMP

- Port information displayed in MIBs related to port-based VLANs does not distinguish between a regular port or a trunk port. Use the **RS G8052(config)# show mac-address-table static** command to view details on regular ports and trunk ports. (ID: 57194)
- If you delete multiple VLANs using SNMP, you may see an error if the SNMP packet size exceeds 1800 bytes. (ID: XB228120)

Spanning Tree

- When using LACP with PVRST, it is not recommended to configure the switch as the STP root bridge. When doing so, traffic can be discarded for up to 30 seconds on affected LACP ports while initial STP path states are being resolved (discarding, learning, forwarding). (ID: 63315)
- After changing from MSTP to a different STP mode, some MSTP commands will still appear in the configuration file. The non-applicable MSTP commands do not affect switch operation and can be ignored. (ID: 64388)

Statistics

The “all events” counter for OSPFv3 includes the total number of changes associated with any OSPFv3 interface, including changes to internal states. (ID:38783)

VLANs

- When a VLAN appears in the VLAN range for a port in a configuration dump, this does not guarantee that the port is actually a member of that VLAN. The actual port to VLAN mapping can be displayed by using the show vlan command. (ID:XB267491)
- When VLAG ports are removed from a VLAG VLAN, the port list still contains both the VLAG ports just removed and the ISL ports. (ID:XB278681)

VMready

- VMs belonging to different ESX servers cannot ping each other across different VM groups. Because the VM groups belong to different VLANs, this is appropriate and expected behavior.