IBM Networking OS™ 6.9 for RackSwitch™ G8052

Release Notes

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 IBM *Documentation* CD and the *Warranty Information* document that comes with the product.

First Edition (February 2012)

Release Notes

This release supplement provide the latest information regarding IBM Networking OS 6.9 for the RackSwitch G8052 (referred to as G8052 throughout this document).

This supplement modifies and extends the following IBM N/OS documentation for use with *N/OS* 6.9:

- *IBM Networking OS* 6.9 *Application Guide*
- *IBM Networking OS* 6.9 *Command Reference*
- *IBM Networking OS* 6.9 *ISCLI Reference*
- *IBM Networking OS* 6.9 *BBI Quick Guide*
- RackSwitch G8052 *Installation Guide*

The publications listed above are available from the IBM support website:

`http://www.ibm.com/support`

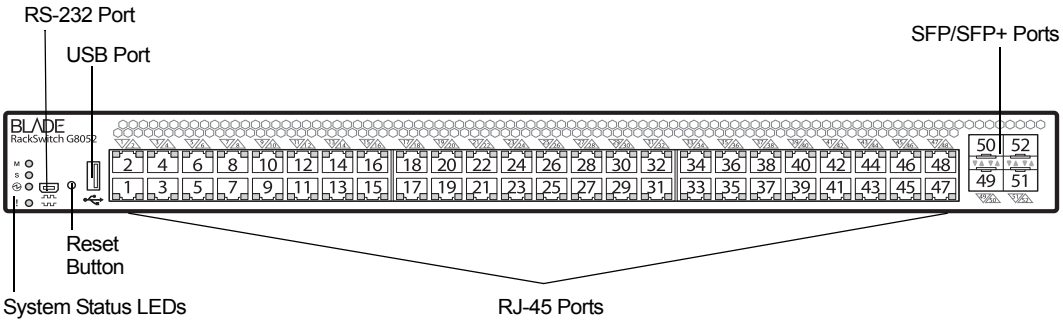
Please keep these release notes with your product manuals.

Hardware Support

The switch unit contains the following ports:

- Forty-eight 10/100/1000BaseT ports (RJ-45)
- Four 10GbE SFP+ ports
- USB port for mass storage
- RS-232 serial console port

Figure 1. RackSwitch G8052 Front Panel



Updating the Switch Software Image

The switch software image is the executable code running on the G8052. 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 G8052, go to the following website:

http://www.ibm.com/systems/support

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

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 using the CLI, ISCLI, or BBI, see "Loading New Software to Your Switch" on page 5.

CAUTION:
Although the typical upgrade process is all that is necessary in most cases, upgrading from (or reverting to) some versions of N/OS or BLADEOS requires special steps prior to or after the software installation process. Please be sure to follow all applicable instructions in the following sections to ensure that your switch continues to operate as expected after installing new software.

Special Software Update Issues

When updating to N/OS 6.9, the following special conditions may apply, depending on the version of software currently installed on your switch. These conditions are cumulative: If updating from version 2.0 (for example), follow the recommendations in order, beginning with those for 2.0, and then continue with all that apply, such as for "3.0 and prior," "4.0 and prior," and so on.

Updating from BLADEOS 6.4 or Prior

After updating:

- The default for STP/PVST Protection mode is different compared to release 6.4 and prior. In release 6.6, STP/PVST Protection is disabled by default. After upgrading, review the STP settings and make any appropriate changes.
- The default for static route health check is different compared to release 6.4 and prior. In release 6.6, static route health check is disabled by default. After upgrading, review the static route health check settings and make any appropriate changes.

- The legacy FDP update rate has been deprecated in favor of independent hotlinks FDB updates in all switch configuration interfaces.

Interface	Old Commands	New Commands
Menu CLI	`/cfg/l2/update <x>`	`/cfg/l2/hotlink/sndrate <x>`
ISCLI	`spanning-tree uplinkfast max-update-rate <x>`	`hotlinks fdb-update-rate <x>`
BBI	Configure | Layer 2 | Uplink Fast | Update Rate Dashboard | Layer 2 | Uplink Fast | STP Uplink Fast Rate	Configure | Layer 2 | Hot Links | FDB update rate Dashboard | Layer 2 | Hot Links | FDB update rate

  These changes are also reflected in the SNMP MIB.

  After upgrading, review the hotlinks FDB settings and make any appropriate changes

- The CLI `BGPTOECMP` option has been deprecated.

Updating from BLADEOS 6.6 or Prior

After updating:

- The default mode for Spanning Tree is different compared to prior releases. The default mode is now PVRST. After upgrading, it is recommended that the administrator review the STP settings and make any appropriate changes.

Loading New Software to Your Switch

The G8052 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.

CAUTION:
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 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 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 one of the following procedures to download the new software to your switch. You can use the N/OS CLI, the ISCLI, or the BBI to download and activate new software.

Loading Software via the N/OS CLI

1. Enter the following Boot Options command:

   ```
   >> # /boot/gtimg
   ```

2. Enter the name of the switch software to be replaced:

   ```
   Enter name of switch software image to be replaced
    ["image1"/"image2"/"boot"]: <image>
   ```

3. Enter the hostname or IP address of the FTP or TFTP server.

   ```
   Enter hostname or IP address of FTP/TFTP server: <hostname or IP address>
   ```

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

   ```
   Enter name of file on FTP/TFTP server: <filename>
   ```

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

5. Enter your username for the server, if applicable.

   ```
   Enter username for FTP server or hit return for
   TFTP server: {<username> /<Enter>}
   ```

   If entering an FTP server username, you will also be prompted for the password. The system then prompts you to confirm your request. Once confirmed, the software will load into the switch.

6. If software is loaded into a different image than the one most recently booted, the system will prompt you whether you wish to run the new image at next boot. Otherwise, you can enter the following command at the `Boot Options#` prompt:

   ```
   Boot Options# image
   ```

   The system then informs you of which software image (`image1` or `image2`) is currently set to be loaded at the next reset, and prompts you to enter a new choice:

   ```
   Currently set to use switch software "image1" on next reset.
   Specify new image to use on next reset ["image1"/"image2"]:
   ```

   Specify the image that contains the newly loaded software.

7. Reboot the switch to run the new software:

```
Boot Options# reset
```

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

Loading Software via the ISCLI

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

```
Router# copy {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:

```
Router# configure terminal
Router(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:

```
Router(config)# reload
```

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

Loading Software via BBI

You can use the Browser-Based Interface to load software onto the G8052. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. Click the Configure context tab in the toolbar.
2. In the Navigation Window, select System > Config/Image Control.

   The Switch Image and Configuration Management page appears.
3. If you are loading software from your computer (HTTP client), skip this step and go to the next. Otherwise, if you are loading software from a FTP/TFTP server, enter the server's information in the FTP/TFTP Settings section.
4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
   - If you are loading software from a FTP/TFTP server, enter the file name and click **Get Image**.
   - If you are loading software from your computer, click **Browse**.

     In the File Upload Dialog, select the file and click **OK**. Then click **Download via Browser**.

   Once the image has loaded, the page refreshes to show the new software.

New and Updated Features

N/OS 6.9 for RackSwitch G8052 (G8052) has been updated to include Edge Virtual Bridging, summarized in the following sections. For more detailed information about configuring G8052 features and capabilities, refer to the complete N/OS 6.9 documentation as listed on page 3.

Virtual Link Aggregation Group (VLAG)

Typically, Spanning Tree Protocol (STP) is used to prevent broadcast loops, blocking redundant uplink paths. This has the unwanted consequence of reducing the available bandwidth between the layers by as much as 50%. In addition, STP may be slow to resolve topology changes that occur during a link failure, and can result in considerable MAC address flooding.

Using VLAGs, the redundant uplinks remain active, utilizing all available bandwidth.

Following enhancements have been made to the VLAG functionality:

- VLAG Global Enable: Before configuring VLAG, you must enable it globally using the command: `RS G8052 (config)# vlag enable.`
- STP On/Off: You can implement VLAG with STP enabled or disabled. If you enable STP, you must use MSTP or PVRST.
- Role election: A VLAG switch may be elected as a primary or secondary switch based on the VLAG system priority and local system MAC address. However, once a switch has been elected as primary, any other switch that comes up will be a secondary switch even if it has lower VLAG priority and MAC address.
- VLAG system MAC: A unique system MAC address is generated for the VLAG switches using the configured Tier ID. Both the VLAG switches use this system-mac as the designated bridge identifier on port channels that are configured for VLAG to provide a single link view to the access switch. It is important that you use a unique Tier ID for each VLAG pair you configure. You must configure a Tier ID on the VLAG peers using the command:
  `RS G8052(config)# vlag tier-id <`*ID*`>`
- Startup delay: Configuring VLAG startup delay prevents traffic loss when a VLAG switch reboots. After the ISL is up, the vLAG ports are enabled only after the configured VLAG startup delay.
- VLAG Capacity: Support for up to 31 VLAG groups and 16K MAC addresses.

Note: The current VLAG release does not interoperate with systems running 6.8 or previous versions of VLAG. Please update all VLAG switches using the latest image. New configuration commands have been added and some old commands have been deprecated or modified. Please see the *IBM Networking OS 6.9 ISCLI Reference Guide* for details.

Note: If you had configured health check in earlier versions of VLAG, please reconfigure using the new command:
`RS G8052(config)# vlag hlthchk peer-ip <`*IP address*`>`

Supplemental Information

This section provides additional information about configuring and operating the G8052 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 the System ...
Memory Test ..............................

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
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 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

Recovering from a Failed 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, CRT, 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 **3** for **Xmodem download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. 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.
6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash.............. done

Writing to Flash.............done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash.......................................... done

Writing to Flash.............................................done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash........... done

Writing to Flash...........done

Protected 8 sectors
```

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

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<**Esc>**) to re-display the Boot Management menu.
9. Select **3** to start a new **XModem Download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <**Enter>** to continue the download.

11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** Switch OS ****


Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...

Un-Protected 27 sectors

Erasing Flash.............................. done

Writing to Flash.............................done

Protected 27 sectors
```

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

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<**Esc>**) to re-display the Boot Management menu.
15. Select **4** to exit and boot the new image.

VLAGs

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

- The ISL should include enough ports to accommodate the peer-to-peer traffic.
- Any port-related configuration, such as applied ACLs, should 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 follow the guidelines given below:

- 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 want to add a port to an ISL trunk/VLAN, or if you want to remove any particular port from an ISL trunk/VLAN, first shutdown that port. Make the necessary changes and re-enable the port.
- If you have STP on, and you need to change the configuration of the VLAG ports, follow the steps below:

  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 G8052 (config)# no vlag adminkey <key> enable` (or)
     `RS G8052 (config)# no 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.

Known Issues

This section describes known issues for N/OS 6.9 on the RackSwitch G8052.

BBI

In the BBI Dashboard, MSTP information area, CIST information, CIST bridge information and CIST ports information is displayed in the **General** page. There is no display available for the **CIST Bridge** or **CIST Ports** menu items. (ID: 35988)

Hotlinks

Prior to enabling hotlinks, Spanning-Tree should be globally disabled using the following command (ID: 47917):

```
RS G8052(config)# spanning-tree mode dis
```

IP Gateways

When a link is disabled and then re-enabled, you might see the following notifications, which can be ignored (ID: 42953, 37969):

```
Static route gateway x is down.
Static route gateway x is up.
```

IPsec

- IPsec does not support virtual links. (ID: 48914)
- Packet fragmentation over IPsec is supported in transport mode only. Fragmentation is not available in tunneling mode. (ID: 50291)

OSPF

- Cannot redistribute fixed/static/RIP/eBGP/iBGP routes into OSPF on a switch with two NSSA areas enabled. The following message appears on the console when trying to export routes to multiple NSSA areas (ID: 37181):
  `Limitation: Cannot export routes to multiple NSSA areas concurrently.`
- When OSPFv3 is enabled, the OSPF backbone area (0.0.0.0) is created by default and is always active. (ID: 37932)
- 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. Configuration based on virtual links is not currently supported.
  - 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.

Port Mirroring

If the traffic line rate on the monitor port exceeds the port's rate, pause frames are sent. To avoid pause frames, disable Flow Control on the mirrored ports. (ID: 27755)

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)

sFlow

- Egress traffic is not sampled. Port sFlow sampling applies only to ingress traffic. (ID: 42474)

SNMP

- In the current N/OS 6.8.1 release, the Enterprise ID in the switch SNMP MIB has been changed from the BLADE Network Technologies ID (26543) to the IBM ID (20301). This change can cause compatibility problems for applications that manage the switch using SNMP, such as BladeHarmony Manager. The upcoming release, 6.8.2, will correct this problem by reverting to the original (BLADE) Enterprise ID. (ID:55383)
- SNMP read and write functions are enabled by default. For best security practices, if these functions are not needed for your network, it is recommended that you disable these functions prior to connecting the switch to your network. (ID: 40056)
- When Directed request is enabled, users connected via Telnet cannot be ejected from the switch. (ID: 37144)

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)

VLAG

- The following features are not supported on ports participating in VLAGs:
  - Hotlinks
  - IGMP relay
  - Private VLANs
- While IGMP queries are being sent at the rate of more than 1 packet per second on a VLAG port, if you flap the VLAG port, the Mrouter may be learnt on both the ISL and the VLAG. You may see two entries in the table. You may also see the multicast traffic flow to the ISL. However, the multicast traffic is discarded on the VLAG peer switch and hence traffic will not be doubled at the receiver. This issue is seen intermittently. (ID: 55814)
- If you are configuring VLAG with STP ON and you have more than 8000 MAC addresses, some of the MAC addresses may be flooded. If you flap the ISL link, you may lose some traffic. To overcome this issue, clear the MAC address table using the command `RS G8052# clear mac-address-table`. (ID: 56939, 57383)
- In a multi-layer VLAG setup, if the STP root bridge or the backup root bridge is on a VLAG switch, STP convergence time may be twice the forward delay when the STP root bridge or the backup root bridge comes back online after a reload. To avoid this situation, we recommend that you configure a switch that is outside the VLAG multi-layer environment to be the STP root bridge. (ID: 57370)

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.