IBM Networking OS™ 7.6 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 (December 2012)

Release Notes

This release supplement provide the latest information regarding IBM Networking OS 7.6 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* 7.6:

- *IBM Networking OS* 7.6 *Application Guide*
- *IBM Networking OS* 7.6 *Command Reference*
- *IBM Networking OS* 7.6 *ISCLI Reference*
- *IBM Networking OS* 7.6 *BBI Quick Guide*
- *RackSwitch G8052 Installation Guide*

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

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

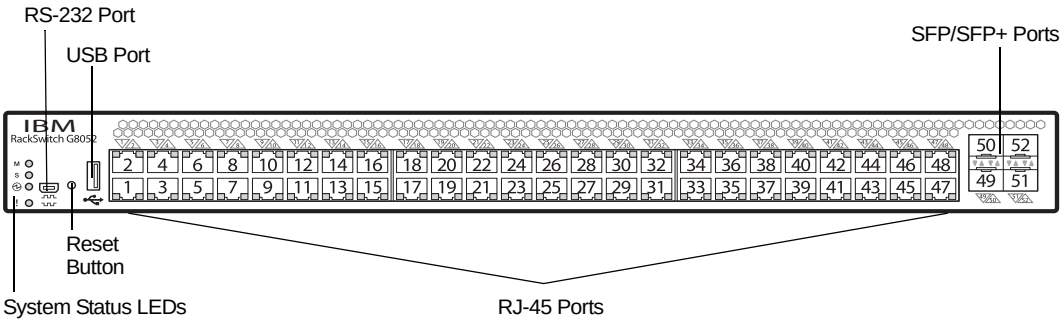
Please keep these release notes with your product manuals.

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 6.

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 7.6, 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.

Updating from IBM Networking OS 6.9 or Prior

CAUTION:
When you upgrade the switch software image, you must load the new boot image and the new software image before you reset the switch.

After updating:

- The default settings of SNMP community strings has changed. Check the new settings and reconfigure as appropriate.

Updating from IBM Networking OS 7.2 or Prior

After updating:

- The default time zone setting is different compared to release 7.2 and prior. In the prior releases, a default setting of US Pacific Time was used. In release 7.4 and above, no default is assumed. For switches that use the default US Pacific Time setting, after upgrading to release 7.4 or above it is recommended that the administrator review the configured time zone and make any appropriate changes. (ID: 60469)

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 18).

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 7.6 for RackSwitch G8052 (G8052) has been updated to include several new features, summarized in the following sections. For more detailed information about configuring G8052 features and capabilities, refer to the complete N/OS 7.6 documentation as listed on page 3.

BGP Route Reflector

The IBM N/OS implementation conforms to the BGP Route Reflection specification defined in RFC 4456.

As per RFC 1771 specification, a route received from an iBGP peer cannot be advertised to another iBGP peer. This makes it mandatory to have full-mesh iBGP sessions between all BGP routers within an AS. A route reflector—a BGP router—breaks this iBGP loop avoidance rule. It does not affect the eBGP behavior. A route reflector is a BGP speaker that advertises a route learnt from an iBGP peer to another iBGP peer. The advertised route is called the reflected route.

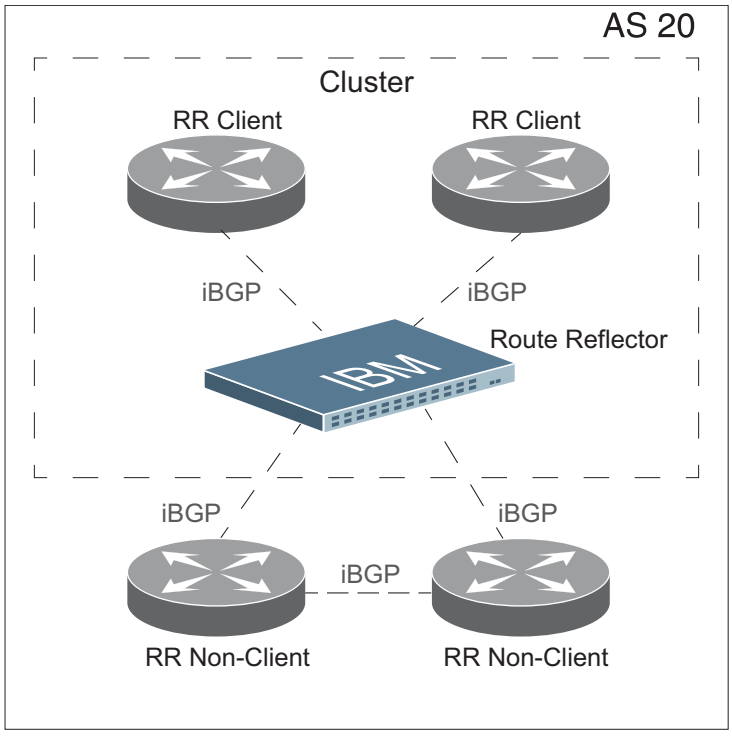
A route reflector has two groups of internal peers: clients and non-clients. A route reflector reflects between these groups and among the clients. The non-client peers must be fully meshed. The route reflector and its clients form a cluster.

When a route reflector receives a route from an iBGP peer, it selects the best path based on its path selection rule. It then does the following based on the type of peer it received the best path from:

- A route received from a non-client iBGP peer is reflected to all clients.
- A route received from an iBGP client peer is reflected to all iBGP clients and iBGP non-clients.

In Figure 2, the G8052 is configured as a route reflector. All clients and non-clients are in the same AS.

Figure 2. iBGP Route Reflector



The following attributes are used by the route reflector functionality:

- ORIGINATOR ID: BGP identifier (BGP router ID) of the route originator in the local AS. If the route does not have the ORIGINATOR ID attribute (it has not been reflected before), the router ID of the iBGP peer from which the route has been received is copied into the Originator ID attribute.This attribute is never modified by subsequent route reflectors. A router that identifies its own ID as the ORIGINATOR ID, it ignores the route.
- CLUSTER LIST: Sequence of the CLUSTER ID (i.e. router ID) values representing the reflection path that the route has passed. The value configured with the `RS G8052(config-router-bgp)# cluster-id <ID>` command (or the router ID of the route reflector if the cluster-id is not configured) is prepended to the Cluster list attribute. If a route reflector detects its own CLUSTER ID in the CLUSTER LIST, it ignores the route. Up to 10 CLUSTER IDs can be added to a CLUSTER LIST.

Route reflection functionality can be configured as follows:

1. Configure an AS.

```
RS G8052(config)# router bgp
RS G8052(config-router-bgp)# as 22
RS G8052(config-router-bgp)# enable
```

2. Configure a route reflector client.

```
RS G8052(config-router-bgp)# neighbor 2 remote-address 10.1.50.1
RS G8052(config-router-bgp)# neighbor 2 remote-as 22
RS G8052(config-router-bgp)# neighbor 2 route-reflector-client
RS G8052(config-router-bgp)# no neighbor 2 shutdown
```

Note: When a client is configured on the G8052, the switch automatically gets configured as a route reflector.

3. Verify configuration.

```
RS G8052(config)# show ip bgp neighbor 2 information

BGP Peer 2 Information:
  2: 10.1.50.1         , version 0, TTL 255, TTL Security hops 0
    Remote AS: 0, Local AS: 22, Link type: IBGP
    Remote router ID: 0.0.0.0,    Local router ID: 9.9.9.9
    next-hop-self disabled
    RR client enabled
    BGP status: connect, Old status: connect
    Total received packets: 0, Total sent packets: 0
    Received updates: 0, Sent updates: 0
    Keepalive: 0, Holdtime: 0, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 0
```

Once configured as a route reflector, the switch, by default, passes routes between clients. If required, you can disable this by using the following command:

```
RS G8052(config-router-bgp)# no client-to-client reflection
```

You can view the route reflector BGP attributes attached to a BGP route using the following command:

```
RS G8052(config-router-bgp)# show ip bgp information 5.0.0.0 255.255.255.0
BGP routing table entry for 5.0.0.0/255.255.255.0
Paths: (1 available, best #1)
Multipath: eBGP
 Local
        30.1.1.1 (metric 0) from 22.22.1.1(17.17.17.17)
        Origin: IGP, localpref 0, valid, internal, best
        Originator: 1.16.0.195
        Cluster list: 17.17.17.17
```

Restrictions

Consider the following restrictions when configuring route reflection functionality:

- When a CLUSTER ID is changed, all iBGP sessions are restarted.
- When a route reflector client is enabled/disabled, the session is restarted.

ISCLI

Configuration command syntax related to the following have been updated to match industry standard:

- Ports and trunking
- VLANs
- Spanning Tree Protocol (STP)

The updated commands are not executable in releases prior to 7.6. In this release, support for legacy command syntax will be provided in parallel with the updated syntax.

Following commands have been updated:

Table 1. ISCLI Command Syntax Updates

Legacy Syntax	Industry Standard Syntax
Ports and Trunking	
RS G8052(config-if)# **duplex any**	RS G8052(config-if)# **duplex auto**
RS G8052(config-if)# **flowcontrol receive**	RS G8052(config-if)# **flowcontrol receive** {**on**|**off**}
RS G8052(config-if)# **flowcontrol send**	RS G8052(config-if)# **flowcontrol send** {**on**|**off**}
RS G8052(config-if)# **name**	RS G8052(config-if)# **description**
RS G8052(config-if)# **broadcast-threshold**	RS G8052(config-if)# **storm-control broadcast level pps**
RS G8052(config-if)# **multicast-threshold**	RS G8052(config-if)# **storm-control multicast level pps**
RS G8052(config-if)# **dest-lookup-threshold**	RS G8052(config-if)# **storm-control unicast level pps**
VLANs	
RS G8052(config-if)# **no tagging**	RS G8052(config-if)# **switchport mode access**
RS G8052(config-if)# **tagging**	RS G8052(config-if)# **switchport mode trunk**
RS G8052(config-if)# **pvid** *<VLAN ID>* RS G8052(config-vlan)# **member** *<port number or range>*	RS G8052(config-if)# **switchport access vlan** *<VLAN ID>*
RS G8052 (config-if)# **pvid 1**	RS G8052(config-if)# **no switchport access vlan**

Table 1. ISCLI Command Syntax Updates

Legacy Syntax	Industry Standard Syntax
RS G8052(config-if)# **pvid** *<VLAN ID>*	RS G8052(config-if)# **switchport trunk native vlan** *<VLAN ID>*
RS G8052(config)# **vlan** *<VLAN ID or range>* RS G8052(config-vlan)# **member** *<port number or range>*	RS G8052(config-if)# **switchport trunk allowed vlan** {**add** *<VLAN ID or range>* |*<VLAN ID or range>*}
RS G8052(config)# **vlan** *<VLAN ID or range>* RS G8052(config-vlan)# **no member** *<VLAN ID or range>*	RS G8052(config-if)# **switchport trunk allowed vlan remove** *<VLAN ID or range>*
RS G8052(config)# **vlan** *<VLAN ID or range>*	RS G8052(config-if)# **no switchport trunk allowed vlan**
RS G8052(config-vlan)# **no member** *<VLAN ID or range>*	RS G8052(config-if)# **switchport trunk allowed vlan none**
Not Applicable	RS G8052(config-if)# **switchport trunk allowed vlan all**
RS G8052(config-if)# [**no**] **tag-pvid**	RS G8052(config-if)# [**no**] **vlan dot1q tag native**
Not Applicable	RS G8052(config)# [**no**] **vlan dot1q tag native**
RS G8052(config)# [**no**] **vlan** *<VLAN ID or range>*	RS G8052(config)# [**no**] **vlan** *<VLAN ID or range>*
RS G8052(config-vlan)# **no enable**	RS G8052(config-vlan)# **shutdown**
RS G8052(config-vlan)# **enable**	RS G8052(config-vlan)# **no shutdown**
Private VLANs	
RS G8052(config-vlan)# **private-vlan type** {**primary**|**isolated**|**community**} RS G8052(config-vlan)# **private-vlan enable**	RS G8052(config-vlan)# **private-vlan** {**primary**|**isolated**|**community**}
RS G8052(config-vlan)# **no private-vlan type**	RS G8052(config-vlan)# **no private-vlan** {**primary**|**isolated**|**community**}
RS G8052(config-vlan)# **private-vlan map** *<primary VLAN ID>*	RS G8052(config-vlan)# **private-vlan association** [**add**|**remove**] *<secondary VLAN list>*
RS G8052(config-vlan)# **member** *<port number>*	RS G8052(config-if)# **switchport mode** [**trunk**] **private-vlan promiscuous** RS G8052(config-if)# **switchport private-vlan mapping** [**trunk**] *<primary VLAN ID>*
RS G8052(config-vlan)# **no member** *<port number>*	RS G8052(config-if)# **no switchport private-vlan mapping** [**trunk**]

Table 1. ISCLI Command Syntax Updates

Legacy Syntax	Industry Standard Syntax
RS G8052(config-vlan)# **member** *<port number>*	RS G8052(config-if)# switchport mode private-vlan {**host**|**trunk secondary**}
RS G8052# **show private-vlan**	RS G8052# **show vlan private-vlan**
RS G8052(config-vlan)# [**no**] **private-vlan enable**	RS G8052(config-vlan)# [**no**] **private-vlan enable**
STP	
RS G8052(config)# **spanning-tree mstp cist-add-vlan** *<1-4094>* RS G8052(config)# [**no**] **spanning-tree stp** *<STG number>* **vlan <1-4094>**	RS G8052(config)# [**no**] **spanning-tree mst** *<instance ID>* **vlan** *<1-4094>*
RS G8052(config)# [**no**] **spanning-tree stp** *<STG number>* **enable**	RS G8052(config)#[no] spanning-tree mst <instance id> enable
RS G8052(config)# **spanning-tree mstp cist-bridge priority** *<0-65535>* RS G8052(config)# **spanning-tree stp** *<STG number>* **bridge priority** *<0-65535>*	RS G8052(config)# **spanning-tree mst** *<instance ID>* **priority** *<0-65535>*
RS G8052(config)# **spanning-tree mstp cist-bridge maximum-age** *<6-40>*	RS G8052(config)# **spanning-tree mst max-age** *<6-40>*
RS G8052(config)# **spanning-tree mstp cist-bridge forward-delay** *<4-30>*	RS G8052(config)# **spanning-tree mst forward-time** *<4-30>*
RS G8052(config)# **spanning-tree mstp maximum-hop** *<4-60>*	RS G8052(config)# **spanning-tree mst max-hops** *<4-60>*
RS G8052(config-if)# [**no**] **spanning-tree stp** *<STG number>* **enable** RS G8052(config-if)# [**no**] **spanning-tree mstp cist enable**	RS G8052(config-if)# [**no**] **spanning-tree mst** *<instance ID>* **enable**
RS G8052(config-if)# **spanning-tree mstp cist interface-priority** *<0-240>* RS G8052(config-if)# **spanning-tree stp** *<STG number>* **priority** *<0-240>*	RS G8052(config-if)# **spanning-tree mst** *<instance ID>* **port-priority** *<0-240>*
RS G8052(config-if)# **spanning-tree mstp cist path-cost** *<0-200000000>* RS G8052(config-if)# **spanning-tree stp** *<STG number>* **path-cost** *<0-200000000>*	RS G8052(config-if)# **spanning-tree mst** *<instance ID>* **cost** *<0-200000000>*
RS G8052(config-if)# **spanning-tree mstp cist hello** *<1-10>*	RS G8052(config-if)# **spanning-tree mst hello-time** *<1-10>*
RS G8052(config-if)# [**no**] **spanning-tree edge**	RS G8052(config-if)# [**no**] **spanning-tree portfast**

Table 1. ISCLI Command Syntax Updates

Legacy Syntax	Industry Standard Syntax
RS G8052(config-PortChannel)# **spanning-tree stp** *<STG number>* **enable** RS G8052(config-PortChannel)# [**no**] **spanning-tree mstp cist enable**	RS G8052(config-PortChannel)# [**no**] **spanning-tree mst** *<instance ID>* **enable**
RS G8052(config-PortChannel)# **spanning-tree mstp cist interface-priority** *<0-240>* RS G8052(config-PortChannel)# **spanning-tree stp** *<STG number>* **priority** *<0-240>*	RS G8052(config-PortChannel)# **spanning-tree mst** *<instance ID>* **port-priority** *<0-240>*
RS G8052(config-PortChannel)# **spanning-tree mstp cist path-cost** *<0-200000000>* RS G8052(config-PortChannel)# **spanning-tree stp** *<STG number>* **path-cost** *<0-200000000>*	RS G8052(config-PortChannel)# **spanning-tree mst** *<instance ID>* **cost** *<0-200000000>*
RS G8052(config-PortChannel)# **spanning-tree mstp cist hello** *<1-10>*	RS G8052(config-PortChannel)# **spanning-tree mst hello-time** *<1-10>*
RS G8052(config-PortChannel)# [**no**] **spanning-tree edge**	RS G8052(config-PortChannel)# [**no**] **spanning-tree portfast**
RS G8052(config)# **default spanning-tree mstp cist** RS G8052(config)# **default spanning-tree stp** *<STG number>*	RS G8052(config)# **default spanning-tree mst** *<instance ID>*
RS G8052# **show spanning-tree stp** *<STG number>* **bridge**	RS G8052# **show spanning-tree** [**vlan** *<VLAN ID>*] **bridge**
RS G8052# **show spanning-tree** [**mstp cist information**]	RS G8052# **show spanning-tree mst 0 information**
Not Applicable	RS G8052# **show spanning-tree** [**root**|**blockedports**]
RS G8052# **show spanning-tree stp** *<STG number>* [**information**] RS G8052# **show spanning-tree mstp cist** [**information**] RS G8052# **show spanning-tree mstp mrst**	RS G8052# **show spanning-tree mst** *<instance ID>* [**information**] RS G8052# **show spanning-tree mst configuration**

Network Time Protocol (NTP)

New commands added to provide the following:

- Detailed information on NTP association:

```
RS G8052(config)# show ntp associations

address            ref clock            st           when(s)
offset(s)
#192.168.13.33      -                    16           -          0
*192.168.13.57      192.168.1.111        3            32         11

* - synced
# - unsynced
```

- Minimize number of syslogs when NTP synchronization fails or system clock is updated:

```
RS G8052(config)# [no] ntp sync-logs        (Enable logs for information on sync failures)

RS G8052(config)# [no] ntp offset <0-86400>   (Set minimum clock change to trigger logs)
```

OSPFv3

Enhancements based on RFC5340.

SNMP

Community Strings

Added support for 8 read-only and read-write community strings for SNMP v1 and SNMPv2. If any one of the community strings is matched, then read-only or read-write access will be granted. Use the following commands to add or delete community strings:

```
To add:
RS G8052(config)# snmp-server read-community-additional <1-32 characters>
(or)
RS G8052(config)# snmp-server write-community-additional <1-32 characters>

To delete:
RS G8052(config)# no snmp-server read-community <1-32 characters>
(or)
RS G8052(config)# no snmp-server write-community <1-32 characters>
```

VLANs

Up to 2048 VLANs can be configured on the RackSwitch G8052.

USB Support

The file naming convention used for loading files from the USB port has changed. The switch model portion has been updated. Only the following filename formats are now supported:

- `RSG8052_Boot.img`
- `RSG8052_OS.img`
- `RSG8052_replace1_OS.img`
- `RSG8052_replace2_OS.img`
- `RSG8052.cfg`
- `RSG8052_replace.cfg`

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, SecureCRT, 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:

- 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 have MSTP 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 7.6 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)

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

- IBM 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.

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

- When configuring IPsec to operate between IBM 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

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.
  - IPsec does not support OSPFv3 virtual links. (ID: 48914)

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)

Port Routing

- Using the ISCLI, routing can be enabled or disabled on a per-port basis using the [no] `switchport` command in the `interface port` or `interface portchannel` modes. Configuration of this feature is not currently supported in the menu-based CLI. (ID: 62846)

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

- Promiscuous mode cannot be enabled for VLANs via the BBI. The configuration fails, but does not notify the user of an error. Use the ISCLI mode instead. (ID: 66417)

Routed Ports

- When MSTP is globally enabled and a routed port is configured, if you need to disable STP, change the global STP mode to RSTP and then disable STP. (ID: 58532)
- IBM N/OS CLI, 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 IBM N/OS CLI or BBI; in SNMP, you may be able to enter the configuration commands, but you will not be able to save the configuration. (ID: 57983)

sFlow

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

SNMP

- 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)
- Port information displayed in MIBs related to port-based VLANs does not distinguish between a regular port or a trunk port. Use the `show mac-address-table static` command to view details on regular ports and trunk ports. (ID: 57194)

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)

VLAG

- The following features are not supported on ports participating in VLAGs:
  - Hotlinks
  - IGMP relay
  - Private VLANs
- In a multi-layer VLAG topology, the VLAG ports may be disabled in CIST if you change the STP mode on the secondary switch to MSTP. (ID: 58696)

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.