Lenovo Flex System SI4093 System Interconnect Module

Release Notes

for Networking OS 8.2

lenovo.

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

Release Notes

This release supplement provides the latest information regarding Lenovo Networking OS 8.2 for the SI4093 System Interconnect Module.

This supplement modifies and extends the following Networking OS documentation for use with N/OS 8.2:

- *Lenovo Networking OS Application Guide for the SI4093 System Interconnect Module*
- *Lenovo Networking OS ISCLI Reference for the SI4093 System Interconnect Module*
- *SI4093 System Interconnect Module User's Guide*

The publications listed are available at the following address:

http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp

Please keep these release notes with your product manuals.

Hardware Support

N/OS 8.2 software is supported on the SI4093 System Interconnect Module for the Lenovo Flex System. The SI4093 System Interconnect Module (SI4093), shown in Figure 1, is a high performance network switch that features tight integration with the Lenovo Flex System chassis management module.

Figure 1. SI4093 System Interconnect Module Faceplate
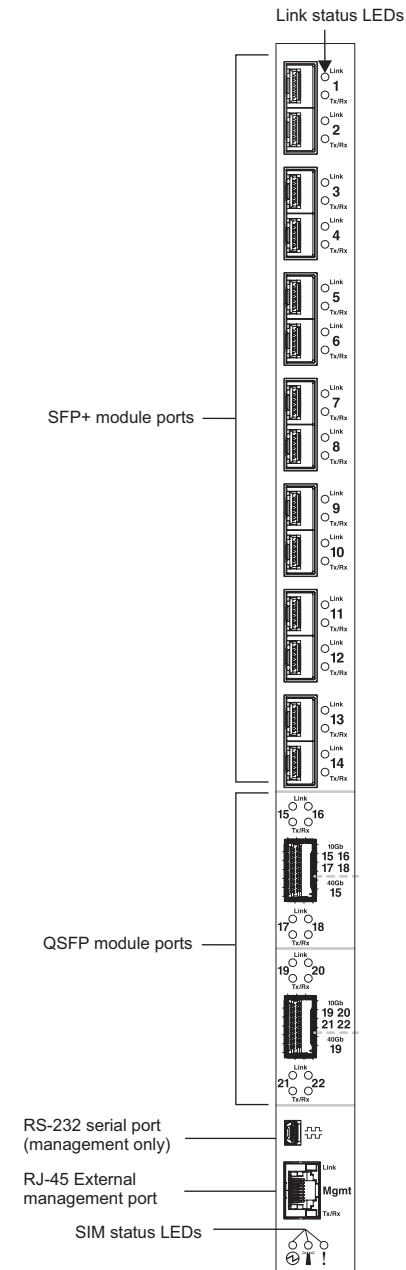
The SI4093 provides pay-as-you-grow scalability. With optional licensing, you can expand the number of available ports. Depending on the installed licenses, the scalable switch can provide up to sixty-four 10 Gigabit Ethernet (GbE) ports.

With all optional licenses installed, the SI4093 has the following port capacities:

- Forty Two internal 10Gb SFP+ ports
- Fourteen external 10Gb SFP+ ports
- Two 40Gb QSFP+ ports
- One 1Gb RJ-45 external management port
- One 1Gb internal management port
- One mini-USB serial port

For additional details about port counts and optional licensing, please refer to the *SI4093 User's Guide*.

Updating the Switch Software Image

The switch software image is the executable code running on the SI4093. 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 SI4093, go to the following website:

http://www.ibm.com/support

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

```
SI4093# 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.

Loading New Software to Your Switch

The SI4093 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 8).

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 ISCLI or the BBI to download and activate new software.

Follow these steps to load software onto your switch:

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

```
SI4093# 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:

```
SI4093# configure terminal
SI4093(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:

```
SI4093(config)# reload
```

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

Supplemental Information

This section provides additional information about configuring and operating the SI4093 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.

```
Flex Module Present ...
  Check Flex Module Power status
  Flex Module Power On.
  Flex Module Out of Reset
 LASH: 32 MB
L2: 512 KB enabled
NAND: 1024 MiB
  eTSEC1 is in sgmii mode.

  PCIE1 connected to Slot1 as Root Complex (base address e000a000)
  PCIE1 on bus 00 - 01
Net: eTSEC1, eTSEC3 [PRIME]

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: R
```

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 software image recovery, press R and follow the screen prompts.
- To reboot the switch press Q and follow the screen prompts.
- 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, 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 **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
        R) Reboot
        E) Exit

Option?:
```

- If you choose option **X** (Xmodem serial download), go to step 5.

- If you choose option **TS** (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.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

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 6.8.3_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.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

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 a Failed Boot Image

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 (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. Press **R** for Boot in Recovery Mode, then press **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.

Chassis Management Module

When configuring the IP interface, which is dedicated to the internal management port (IF128, MGT1), you cannot use a subnet that is already configured on any other enabled interface (IF1-127). This results in IF128 being disabled and an IP configuration of all zeros displayed on the CMM user interface. The CMM event log will indicate that a "Duplicate route" was detected.

For example, consider is configured or enabled to the following IP address and mask:

```
Interface information:
127: IP4 192.168.71.120  255.255.255.0
```

The switch will reject an attempt made from the CMM CLI to configure the internal management port (MGT1, IF128) to the following IP address and mask:

```
system:switch[1]> ifconfig -i 192.168.71.130 -s 255.255.255.0
```

In this scenario, the switch rejects the attempt by disabling any current configuration on IF128, and responds to the CMM with an IP address, mask, and gateway that contains all zeros.

On the CMM CLI, the resulting condition appears as follows:

```
system:switch[1]> ifconfig
Ethernet ScSE
Enabled
-c  static
-i  0.0.0.0
-s  0.0.0.0
-g  0.0.0.0
system:mm[1]> displaylog
1  I  IOMod_01  04/03/12  08:02:49  (iomodule01) Duplicate route detected
to I/O module iomodule01.
2  I  IOMod_01  04/03/12  08:02:49  (iomodule01) I/O module 1 IP address
was changed to 0.0.0.0.
```

External Port Link Negotiation

Autonegotiation settings for each external switch port should be the same as those of the devices being connected. In a valid configuration, both ends of a port link are set with autonegotiation on, or both ends are set to specific speed and link properties with autonegotiation disabled.

Port Mirroring Tags BPDU Packets

When you perform port mirroring, Spanning Tree BPDU packets are VLAN tagged at the monitoring port. This is standard behavior of port mirroring on the SI4093. All mirrored egress traffic is tagged.

Secure Management Network

The following SI4093 attributes are reserved to provide secure management access to and from the chassis management module:

- MGT port (MGT1)
- IP interface 12, 128
- Gateway 4
- STG 128

For more information about remotely managing the SI4093 through the external ports, see "Accessing the Switch" in the *Lenovo Networking OS 8.2 Application Guide*.

Secure Shell (SSH)

Because SSH key generation is CPU intensive, the SI4093 attempts to avoid unnecessary key generation. The process generates three server keys:

1. One key is generated to replace the current server key, if used.

2. A second key is generated as a spare, in case the current server key is used and the specified interval expires.

3. A third key is generated for use at the next reboot.

Therefore, if you never login via SSH, you will only see two key generation events. You may see all three events directly following a reboot. If you want to witness the key generation after the specified interval has expired, then you must login via SSH at least once during each expiration interval.

Spanning Tree Configuration Tips

To ensure proper operation with switches that use Cisco Per VLAN Spanning Tree (PVST+), you must do one of the following:

- Create a separate Spanning Tree Group for each VLAN.

- Manually add all associated VLANs into a single Spanning Tree Group.

When using Layer 2 Trunk Failover, disable Spanning Tree Protocol on external ports.

Syslog Configuration Tip

The *facility* parameter traditionally is used to correlate services (such as IP, CLI, etc.) to messages. This is done to distinguish between the different services that are running in the network/device. However, for the SI4093, there is a single configured facility value (0-7) used on all messages. By configuring a unique facility value for each switch, a single SYSLOG server can distinguish between the various SI4093s in the network. Refer to "System Host Log Configuration" in the *Command Reference.*

Trunk Group Configuration Tips

Please be aware of the following information when you configure trunk groups:

- Always configure trunk groups first, on both ends, before you physically connect the links.

- Configure all ports in a trunk group to the same speed (you cannot aggregate 1Gb ports with 10GBASE-SFP+ ports).

- Configure all ports in a trunk group with the same duplex.

- Configure all ports in a trunk group with the same flow control.

vCenter Synchronization

When applying distributed VM group configuration changes, the switch will attempt to synchronize settings with the VMware vCenter for virtualization management. If the vCenter is unavailable, an error message will be displayed on

the switch. Be sure to evaluate all error message and take the appropriate actions to ensure the expected changes are properly applied. If corrective actions are not taken, synchronization may remain incomplete when connection with the vCenter is restored.

Solution: When the switch connection with the vCenter is restored, use the following operational command to force synchronization:

```
SI4093(config)# virt vmware scan
```

VRRP Configuration

Although the Virtual Router Redundancy Protocol (VRRP) standard permits up to 255 virtual router instances, the N/OS 8.2 implementation only allows up to 128 virtual router instances (corresponding to the number of supported IP interfaces). Each virtual router instance can be assigned a unique Virtual Router ID (VRID) between 1 and 255.

New and Updated Features

N/OS 8.2 for SI4093 System Interconnect Module (SI4093) has been updated to include several new features, summarized in the following sections. For more detailed information about configuring SI4093 features and capabilities, refer to the complete N/OS 8.2 documentation as listed on .

Auto VLAN Tagging on Trunk Ports

This speeds up the process of adding trunk ports in VLANs by automatically adding them to all VLANs in their allowed ranges. By default, all VLANs are allowed on each port.When you configure a port as a trunk port, it is automatically added to all VLANs in its allowed range. When a new VLAN is created, all trunk ports with that VLAN in their allowed ranges are automatically added to it.

Backdoor PSIRT Fix

Certain login username/password combinations used for development debugging were hard-coded on the switches and were not changeable. These were a cause of potential security vulnerability. Access to these login username/password combinations has been removed.

CEE Command Enhancement

The command:

```
SI4093(config)# cee gloobal ets priority-group <priority group>
```

allows configuration of all eight priority groups at the same time.

Flexible Port Mapping

This feature allows flexible remapping of ports. You can map and unmap ports and see the current saved port configuration.The Flexible Port Mapping feature also warns you when a reboot is needed.

MTM and ESN Through the CLI

You can now get information on the chassis Machine Type Model as well as the Equipment Serial Number through the switch CLI.

NETCONF Support

The NETCONF (RFC4741) protocol defines a mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated.

Password Fix-Up Mode

Password Fix-Up Mode enables admin user account recovery if administrator access is lost. This feature adds the option to disable password fix-up functionality, letting the switch administrator decide whether or not to enable Fix-Up mode to cover security concerns.

Private VLAN in Stacked mode

The release supports the use of Private VLANs with switches in a stacked configuration as described in RFC 5517.

RMON Support (RFC1757, RFC2819)

Remote network monitoring (RMON) devices, often called monitors or probes, are instruments that exist for the purpose of managing a network. This release supports RMON for Ethernet statistics, Ethernet history, and Alarm and Event groups.

Secure Image Signing

This release adds a signature to the header of the image to ensure that the image loaded onto the switch is a genuine Lenovo official image.

Security Audit Log

This release supports Audit log with SNMPv3 credential configuration from the CMM through the EHCM MIB interface. It also introduces audit log access privileges for SNMPv3.

Sensor Parameter Temperatures Changed

The temperature at which the sensor parameters will trigger a shutdown or recovery have been increased.

Old Temperatures:

Temperature Shutdown : Shutdown at 75 C / Recover at 70 C

New Temperatures:

Temperature Shutdown : Shutdown at 82 C / Recover at 77 C

SNMP Trap Host

This feature implements the SNMP interface for getting and setting SNMP host configuration for traps.

SSLv3 Disabled in vmReady

The weaker SSLv3 used for vmReady SSL and TLS transactions with the server has been disabled.

Syslog Enhancements

The following syslog enhancements have been made to the Browser-Based Interface:

- The syslog page has been enhanced to show the latest log entries first.
- You can now configure the page refresh interval.

TACACS+ Enhancement

When a TACACS+ server is configured to provide authentication, authorization, and accounting (AAA) services but is unavailable, you will be prompted for a username and password.

Time and DST for EHCM 1.02g

This feature adds an interface in the EHCM MIB for the Chassis Management Module (CMM) to configure the time zone and DST settings.

Trial Feature-on-Demand Keys

This release provides support for trial Feature-on-Demand keys that last up to 90 days.

UFP Trunk Mode Supports 1024 VLANs in Standalone Mode

The maximum number of VLANs a UFP port can support in standalone mode has been increased to 1024 VLANs per vPort. These VLANs are distributed dynamically amongst the enabled vPorts of the UFP port. The number of VLANs a UFP can support in stacking mode is 256.

Use SSH Public Keys for up to 20 Local Switch Users

The feature allows users to login to a switch via SSH using public key authentication instead of password authentication. When SSH is enabled the switch supports both password and public key authentication. The switch now supports up to 20 SSH public key users.

VLAG and MSTP Enhancement

This enhancement removes STP configuration restrictions when vLAG and MSTP are both enabled, such as changing the MSTP instance and VLAN associations. The vLAG interswitch link ports now send a recurring warning message when there's an MSTP region mismatch between the vLAG switches.

VPD and image attributes for EHCM 1.02g

This release implements Enhanced Configuration and Management for I/O Modules (EHCM) 1.02g, which provides enhancements such as delayed image activation and more detailed OID descriptions.