Lenovo Flex System SI4093 System Interconnect Module

Release Notes

for Lenovo Network OS 8.4

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 (January 2017)

Release Notes

This release supplement provides the latest information regarding Lenovo Network OS 8.4 for the SI4093 System Interconnect Module.

This supplement modifies and extends the following Lenovo N OS documentation for use with N/OS 8.4:

- *SI4093 System Interconnect Module Application Guide for Lenovo Network OS 8.4*
- *SI4093 System Interconnect Module Command Reference for Lenovo Network OS 8.4*
- *SI4093 System Interconnect Module Installation Guide*

The publications listed are available at the following address:

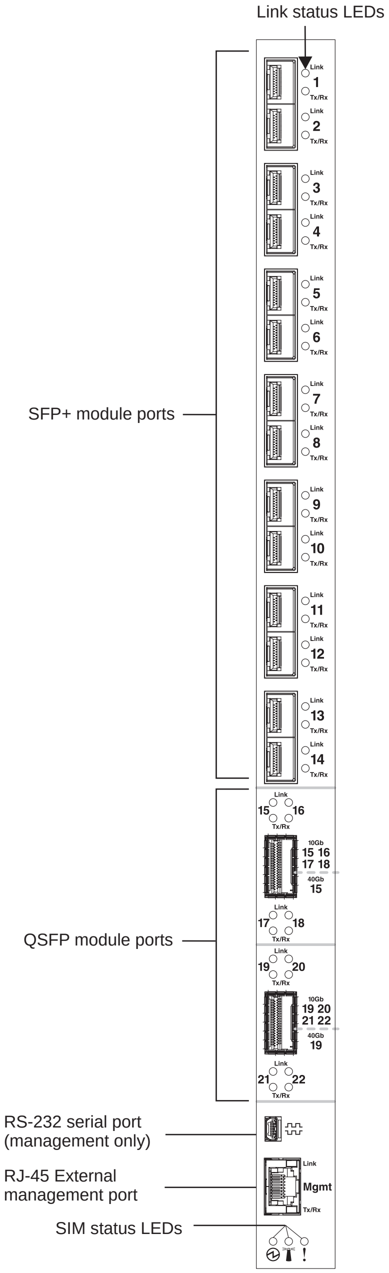
http://flexsystem.lenovofiles.com/help/index.jsp

Please keep these release notes with your product manuals.

Hardware Support

Lenovo Network OS 8.4 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 Installation 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://support.lenovo.com

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

For instructions on the typical upgrade process, see "Loading New Software to Your Switch" on page 7.

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 Image Upgrade" on page 10).

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

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

  Note: Be sure to download both the new boot file and the new image file.
- The hostname or IP address of the SFTP, FTP, or TFTP server.

  Note: The DNS parameters must be configured if specifying hostnames.
- The name of the new software image or boot file.

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

Loading Software via the Command Line Interface

Follow these steps to load software onto your switch:

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

```
SI4093# copy {sftp|tftp|ftp} {image1|image2|boot-image}
```

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

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

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

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

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

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

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

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

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

```
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.

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

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.

```
Resetting the System ...
Memory Test ................................

Boot Management Menu
        1 - Change booting image
        2 - Change configuration block
        3 - Boot in recovery mode (tftp and xmodem download of images to 
recover switch)
        5 - Reboot
        6 - Exit
Please choose your menu option:
```

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 a software image recovery, press **3** and follow the screen prompts.
- To reboot the switch press **5** and follow the screen prompts.
- To exit the Boot Management menu, press **6**. The booting process continues.

Recovering from a Failed Image Upgrade

The Boot Management menu allows you to perform fundamental device management operations, such as selecting which software image will be loaded, resetting the SI4093 to factory defaults or recovering from a failed image download.

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

1. Connect a PC to the serial Console port of the SI4093.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, SecureCRT or PuTTY) and select the following port characteristics:

● Speed:	9,600 bps
● Data Bits:	8
● Stop Bits:	1
● Parity:	None
● Flow Control:	None

3. To access the Boot Management menu, you must interrupt the boot process from the Console port. Boot the SI4093, and when the system begins displaying Memory Test progress (a series of dots), press **<Shift + B>**.

   The Boot Management menu will appear:

```
Resetting the System ...
Memory Test ................................

Boot Management Menu
        1 - Change booting image
        2 - Change configuration block
        3 - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        5 - Reboot
        6 - Exit
Please choose your menu option:
```

4. Select **3** to boot in recovery mode. The following menu will appear:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        R) Reboot
        E) Exit

Option? :
```

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

If you choose option **T** (TFTP download), go to Step 6.

5. **Xmodem download:** When you see the following message, change the serial port characteristics to 115,200 bps:

```
Change the baud rate to 115200 bps and hit the ENTER key before
initiating the download.
```

   a. Press **<Enter>** to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator. You will see a display similar to the following:

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

   b. When you see the following message, change the serial port characteristics to 9,600 bps:

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

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

```
install software image 1 or 2 (hit return to just boot image):
```

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

```
Extracting images ... Do *NOT* power cycle the switch.
Installing Root Filesystem:
Image signature verified.  100%
Installing Kernel:
Image signature verified.  100%
Installing Device Tree:
Image signature verified.  100%
Installing Boot Loader:  100%
Updating install log. File image installed from xmodem at 18:06:02 on
13-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        R) Reboot
        E) Exit

Option? :
```

   Continue to Step 7.

6. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter ‘q’
to quit):
IP Addr    :
Server Addr:
Netmask    :
Gateway    :
Image Filename:
```

a. Enter the required information and press **<Enter>**. You will see a display similar to the following:

```
         Host IP    : 10.10.98.110
         Server IP  : 10.10.98.100
         Netmask    : 255.255.255.0
         Broadcast  : 10.10.98.255
         Gateway    : 10.10.98.254
Installing image 8.4.0_OS.img from TFTP server 10.10.98.100
```

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

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

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

```
Image2 updated succeeded
Updating install log. File 8.4.0_OS.img installed from 10.10.98.100 at
15:29:30 on 12-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        R) Reboot
        E) Exit

Option? :
```

Continue to Step 7.

7. Image recovery is complete. Perform one of the following steps:

- Press **R** to reboot the switch.
- Press **E** to exit the Boot Management menu.
- Press the Escape key (**<Esc>**) to re-display the Boot Management menu.

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 that the interface dedicated to the external management port (EXTM, IF127) 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 must 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)
- VLAN 4095
- IP interface 128
- Gateway 4
- STG 128

For more information about remotely managing the SI4093 through the external ports, see "Accessing the Switch" in the *Lenovo Network OS 8.4 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 8.4 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

Lenovo Network OS 8.4 for 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 8.4 documentation as listed on page 3.

ACL Enhancements

Syslog messages generated by Access Control Lists (ACLs) are now logged by the switch. If ACL logging is enabled on the switch, then packet samples that match the ACL filter will be forwarded to the CPU.

Metering is now supported for IPv6 ACLs.

Certificate Signing Request (CSR)

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

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 (for example, hostname, netmask, uplink ports, or vLAG) and the tool automatically configures the switch accordingly.

Feature on Demand

When performing Feature on Demand (FoD) upgrades or downgrades, a switch reload is no longer needed for the changes to take effect if the FoD modifications are performed using the default (factory) switch configuration.

Network Mask Enhancement

Adds support for /31 network mask for point-to-point configurations involving class B and class C IP addresses.

Password Encryption

All passwords configured on the switch are encrypted using industry-standard encryption methods.

SIOM

Secure Input/Output Module (SIOM) is a feature that ensures a high security level on the switch as required by the Chassis Management Module (CMM). The CMM pushes necessary configurations to the I/O Module (switch) using the secure connection channel established between the CMM and the IOM.

The switch can be in two operating modes in regards to SIOM:

- Secure I/O Module (SIOM) mode - the CMM successfully configures the switch and imposes the security policy
- Legacy I/O Module (LIOM) mode - the switch operates with its own security setting

If the switch and the CMM are both running firmware versions that support SIOM, then by default both the switch and the CMM will operate in SIOM mode.

If either the switch or the CMM is running a firmware version that does not support SIOM, then by default both the switch and the CMM will operate in LIOM mode.

In SIOM mode, a secure version of LDAP using StartTLS and LDAPS is supported. Cryptographic provisioning is also supported.

In SIOM mode, the switch will be fully provisioned by the CMM.

One of the things provisioned by the CMM is SNMPv3 user accounts with customized attributes. For each SNMPv3 user account, the IOM will create a local SNMPv3 user account. When SNMPv3 accounts are centrally managed by the CMM:

- SNMP v1/v2 access is disabled
- the factory default and user configured local SNMPv3 accounts are disabled. Only CMM provisioned accounts are allowed to access the switch via SNMPv3.

TACACS+ Two Level Authentication

This feature enables the TACACS+ server to request a second level of authentication when a user attempts to access the switch’s Privileged EXEC command mode. The feature is active only if TACACS+ is used to control access to the switch and Privileged EXEC command mode is configured to require a password.

Known Issues

This section describes known issues for N/OS 8.4 on the SI4093 System Interconnect Module.

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.

Statistics

The unicast traffic counter is not incremented for member unit port when sending tagged traffic. (ID: 37800)

- o Packets that have invalid length in EtherType/Length field from Ethernet header are counted as multicast packets even though they are unicast packets (invalid means that the length specified is not the same as packet length).

SIOM

- To ensure that the Secure Input/Output Module (SIOM) works correctly, the Chassis Management Module (CMM) needs to use a digest algorithm that is supported by the switch. If the switch has cryptographic mode enabled and the CMM uses a weak digest algorithm that is not supported under cryptographic mode (for example, SHA-1), then cryptographic mode needs to be disabled on the switch or the digest algorithm needs be changed on the CMM (for example, to SHA-256). (ID: 59962)
- When establishing an HTTPS connection, the certificate used by the switch to identify itself will use only the static IPv4 and IPv6 addresses that are configured on the Chassis Management Module (CMM) as the IP address of the switch's internal management port. If the IP addresses are changed from the CMM, the certificate used by the HTTPS server will be regenerated using the new IP addresses after the switch is restarted. (ID: 63118)

UFP

Traffic behavior when having ETS and Bandwidth mode enabled on different ports. (ID: 5706)

- o The bandwidth ratios of PGs for ETS can't be guaranteed when running traffic between ETS UFP-enabled port and Bandwidth mode UFP-enabled port. Based on the current implementation of UFP VLAN, for ingress traffic into UFP-enabled port, it won't copy the inner priority to outer priority. For UFP QoS Bandwidth mode port, all the traffic sent from the server is assigned to PG0, regardless of the priority set in the inner TAG. As a result, for PFC priority and ETS it's only guaranteed minimum bandwidth for PGs.
- o Also, when a vPort is expected to be lossless, it should be configured with FCoE network mode.