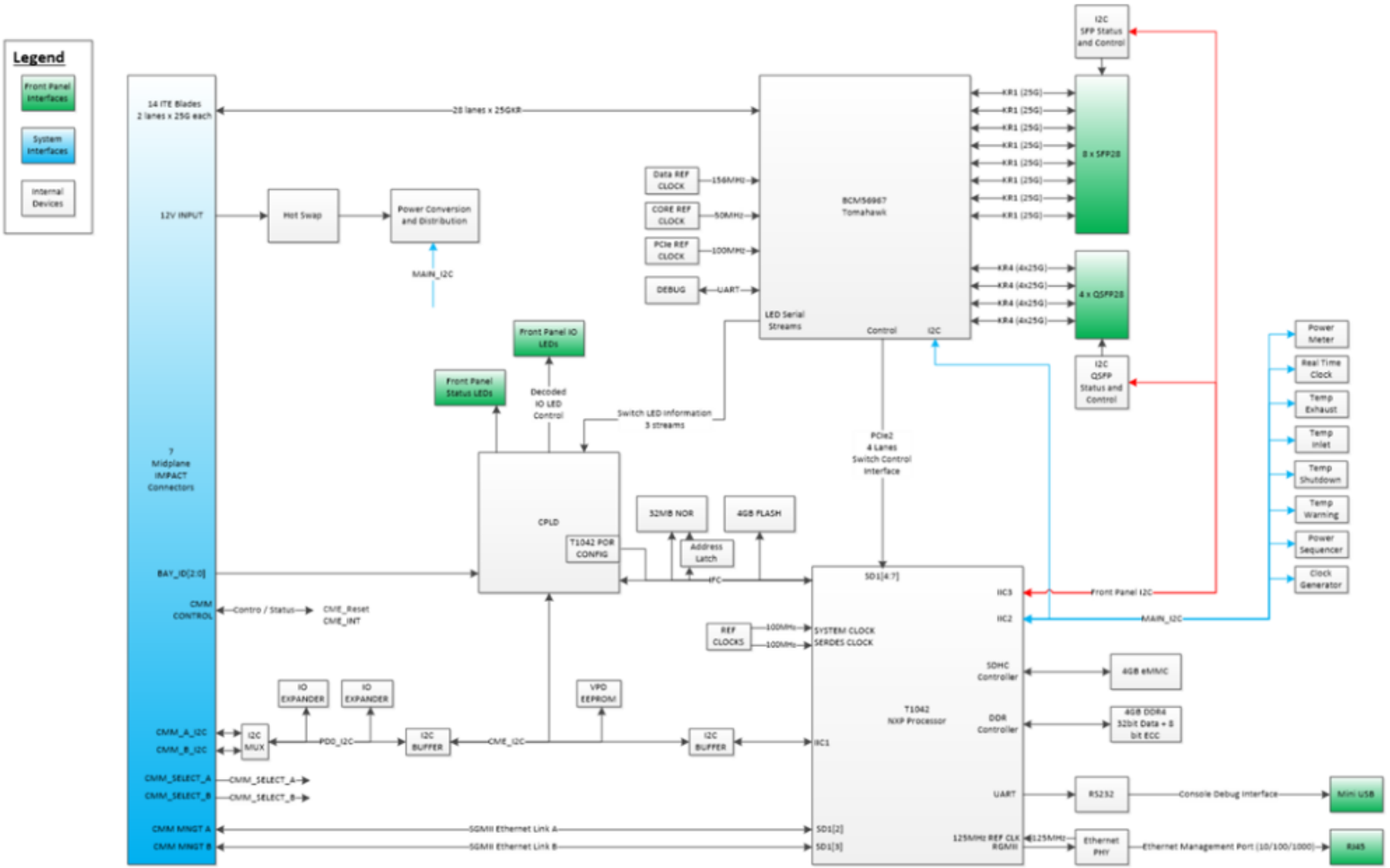
System configurations and diagrams

Block diagram, port configurations, switch management, firmware upgrade

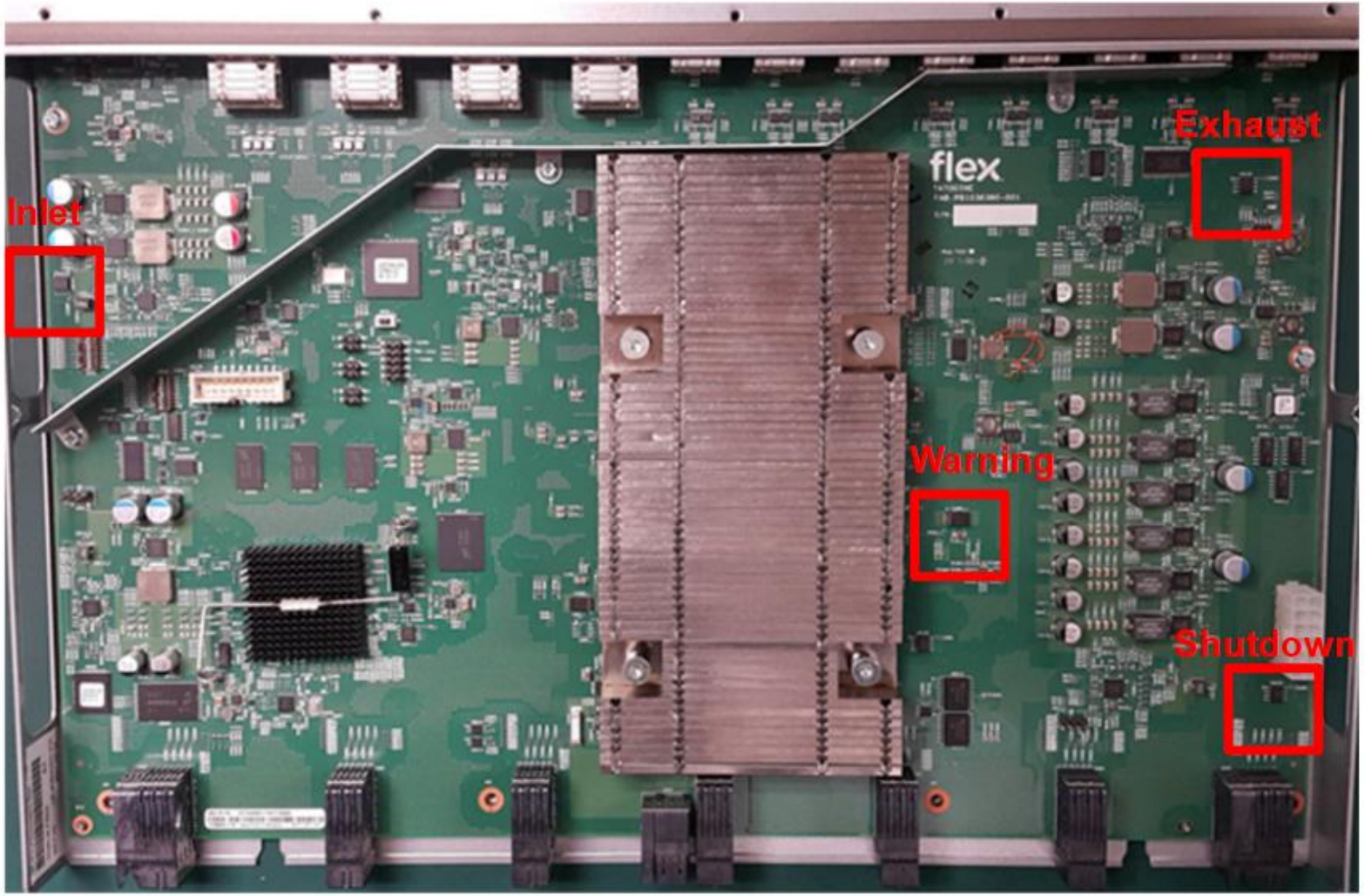
NE2552E Flex Switch block diagram



Flex switch thermal sensor locations

The NE2552E Flex switch comes with four I2C-based temperature sensors:

- One thermal sensor to measure the switch inlet air temperature.
- Two sensors to implement a warning and shutdown on the switch.
- One thermal sensor to measure the switch exhaust air temperature.



Management and configuration

The switch has an internal Ethernet path to the CMM, the external Ethernet data ports, an external management port, and a serial console port. The switch supports two remote-access modes for management through Ethernet connections:

- Default mode: The default mode uses the internal path to the CMM only. Refer to “Establishing an interface through the CMM” for more information.
- External management mode: The external management mode allows for the use of alternate entities to control and manage the switch. Refer to “Enabling management through data ports” for more information.

For specific details about configuring the switch and preparing for system installation, go to the Lenovo Support Web site at http://support.Lenovo.com.

You can manage and configure the NE2552E through the following interfaces:

- A Secure Shell (SSH) version 2 or Telnet connection to the embedded Command-line interface (CLI).
- A terminal emulation program connection to the serial port interface.
- A network management application using Simple Network Management Protocol (SNMP).

Establishing an interface through the CMM (1 of 2)

For remote management functions, the switch requires a TCP/IP interface. This can be configured through the CMM as follows:

1. Log on to the CMM CLI. If necessary, obtain the IP address of the CMM from your system administrator.

Note: The default User ID for the CMM is **USERID**, and the default password is **PASSW0RD** where the sixth character is the number zero. The User ID and password fields are case-sensitive.

2. Set the environment to the bay where you installed the switch:
   ```
   system> env -T system:switch[1]
   ```
3. Run the `ifconfig` command to configure the IP parameters you wish to use for remote switch management. For example,
   ```
   ifconfig -i 192.168.70.1 -s 255.255.255.0 -g 192.168.70.100
   ```

   where the `-i` parameter is the IPv4 address, `-s` is the subnet mask, and `-g` is the default gateway.

Establishing an interface through the CMM (2 of 2)

4. Ping the switch from the CMM using this address:

```
system:switch[1]> ping -i 192.168.70.1
Reply from 192.168.70.1: bytes=64 time=0.198ms
Reply from 192.168.70.1: bytes=64 time=0.213ms
Reply from 192.168.70.1: bytes=64 time=0.228ms
Reply from 192.168.70.1: bytes=64 time=0.168ms
```

   After the switch management address is configured, you can use it to establish a SSH/Telnet session.

Note: SSH is enabled by default. Telnet can be enabled once you have initially logged into the switch.

The SSHv2 / Telnet client software provides different ways to access the same internal-switching firmware and configure it.

If your system application requires that you use the SSHv2 / Telnet client software, see “Accessing the Switch Through the SSHv2/Telnet Interface” for additional information.

Accessing the switch through the SSHv2 / Telnet interface

To connect to the switch through the SSHv2 / Telnet interface, refer to your client software for specific instructions on how to invoke a session. For example, using the Microsoft Telnet Client, you would complete the following steps:

1. From a DOS command-line prompt, type `telnet` <*switch IP address*> and press **Enter**.
2. When prompted, enter your **user name** and **password**.

Note: When you log into the switch for the first time, The default switch administrative user ID is **USERID**, and the default password is **PASSW0RD** where the sixth character is the number zero. The User ID and password fields are case-sensitive.

Any configuration changes made using the management interface will be lost during the next switch restart. Be sure to make a copy your configuration.

3. To copy your configuration, at the command prompt, enter the following command:

```
Copy running-config startup-config
```

This command stores the current switch configuration and all changes in nonvolatile memory. For more information about configuring through the CLI, see the *Application Guide* and *Command Reference* for your specific switch and its installed firmware.

Enabling management through data ports

To access and manage the switch through external interfaces, you must enable the data non-management ports and the ability to manage the switch through them. Use the information in the following table to configure your ports.

Data ports (`-ep` option)	External management (`-em` option)	Description
Disabled	Disabled	The switch must be managed through the CMM. No traffic is allowed on internal or external switch ports.
Enabled	Disabled	The switch must be managed through the CMM. Data traffic is allowed on internal and external switch ports.
Disabled	Enabled	The switch can be managed through the CMM or a compute node. No traffic is allowed on internal or external switch ports.
Enabled	Enabled	The switch can be manage through the CMM, a compute node, or a management station that is connected through the switch. Data traffic is allowed on internal and external switch ports.

Data port configuration

To enable management through data ports, complete the following steps.

1. Log on to the CMM CLI. If necessary, obtain the IP address of the CMM from your system administrator.
2. Run the following command to set the environment to the bay where you installed the switch:
   ```
   system> env -T system:switch[1]
   ```
3. Run the `ifconfig` command to enable data ports and external management:
   ```
   ifconfig -ep enabled -em enabled
   ```

You can now manage the switch using its data ports or external management port.

Note: External management refers to a process by which configuration is performed by a method other than using the CMM. To externally manage the switch, additional IP interfaces must be configured. For more information, see the *Application Guide* for your specific switch and its installed firmware.

External management port

The management port is used only for switch management and is not used for data traffic. Before you use this port to configure your switch, the port must be enabled by using the following administrative login credentials:

Note: The user ID for the CMM is **USERID**, and the default password is **PASSW0RD** where the sixth character is the number zero. The User ID and password fields are case-sensitive.

The initial configuration of this management port is completed by logging in to the switch from the CMM only. A reserved IP address must be configured connecting to this port from a managing device other than the CMM.

To configure an IP address for the management port, log in to the switch from the CMM and run the following command sequence:

```
env -T system:switch[x]
ifconfig -i [ip address of port]
Ifconfig -s [subnet mask]
Ifconfig -g [ip address of gateway]
```

Accessing the switch through the RS-232 port

Messages from the POST and all initialization information are transmitted through the serial port. You can use the serial port to log in to the switch to access and configure the internal switching firmware. The serial port is compatible with the standard 16550 Universal Asynchronous Receiver/Transmitter (UART) protocol. The RS-232 serial port is enabled by default.

To log in to the switch, complete the following steps:

1. Connect one end of the serial cable that comes with your device into the RS-232 port and connect the other end to the management station.
2. On the management station, open a console window and make sure that the serial port is configured with the following settings:
   - 9600 baud
   - 8 data bits
   - No parity
   - 1 stop bit
   - No flow control
3. When prompted, enter your user name and password. The default administrator user ID is **USERID**, and the default password is **PASSW0RD** where the sixth character is the number zero. The User ID and password fields are case-sensitive.

Initial switch configuration

The *Lenovo ThinkSystem NE2552E Flex Switch Application Guide* describes how to configure and use the Lenovo ENOS 8.4 software on the Lenovo ThinkSystem NE2552E Flex Switch.

The switch software image is the executable code running on the NE2552E. A version of the setup utility 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 NE2552E, go to http://www.ibm.com/support/

The Setup utility prompts you step-by-step to enter all the necessary information for basic configuration of the switch. To access setup from the Command-line interface after login, enter the following command:

```
NE2552E(config)# setup
```

To determine the software version of the switch, enter the following command:

```
NE2552E# show boot
```

Switch firmware update

The *Lenovo ThinkSystem NE2552E Flex Switch Application Guide* describes how to update the Lenovo ENOS 8.4 software on the Lenovo ThinkSystem NE2552E Flex Switch.

The operating firmware on the switch contains default configuration files that are installed during the firmware installation. These initial configuration settings are not in a separate configuration file but are components of the firmware. When you restore the switch to factory defaults, the original configuration is restored. After you log on to the switch, you must perform basic configuration tasks.

Configuration settings may be lost during some firmware updates. Before updating the firmware, save a copy of the configuration on a separate device. In the event of a failed update, the saved configuration can be restored.

To copy your configuration, at the command prompt, enter the following command:

```
Copy running-config startup-config
```

Determining the level of switch firmware

To determine the level of the firmware that is installed, complete the following steps.

1. Log on to the Lenovo Flex System CMM CLI. If necessary, obtain the Internet Protocol (IP) address of the CMM from your system administrator.
2. Set the environment to the bay where you installed the switch. For example:

   ```
   system> env -T system:switch[1]
   ```

3. Run the info command to display switch firmware information as follows:

   ```
   system:switch[1]> info ...
   Boot ROM
         Rel date: 04/02/2013
         Version: 7.7.1.12
         Status: Active
   Main application
         Rel date: 04/02/2013
         Version: 7.7.1.12
         Status: Active
   Main application
         Rel date: 03/22/2013
         Version: 7.7.1.12
         Status: Inactive
   ```

Obtaining the latest switch firmware

If firmware updates are available, you can download them from the Lenovo Web site at http://support.lenovo.com/. Changes are made periodically to the Lenovo Web site. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

Attention: Installing the incorrect firmware might cause the switch to malfunction. Before you install firmware, read any release notes, readme files and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure or requirements for updating from an early firmware version to the latest version.

Before you install new software to the switch

The NE2552E can store up to two different switch software images (called image1 and image2) as well as special boot software (called boot). When you install new software, you must specify where it is placed: either into image1, image2, or boot. For example, if your active image is currently loaded into image1, you would load the new image software into image2. This allows you to test the new software and reload the original active image (stored in image1), if needed.

To load a new software image to your switch, obtain the following:

- The image and boot software loaded on an FTP, SFTP, or TFTP server on your network. Be sure to download both the new boot file and the new image file.
- The hostname or IP address of the FTP, SFTP, or TFTP server. The DNS parameters must be configured if specifying host names.
- 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.

Installing the software image using ISCLI (1 of 2)

1. FTP is disabled by default, you need to enable it. In Privileged EXEC mode, enter the following command:

   ```
   NE2552E# access ftp enable
   ```

2. Copy the image to your switch, specifying the method for loading the software (FTP, SFTP, or TFTP) and the NE2552E destination (image1, image2, or boot-image) by entering the following command:

   ```
   NE2552E# copy {tftp|ftp|sftp} {image1|image2|boot-image}
   ```

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

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

4. 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, SFTP, or TFTP directory (for example, `tftpboot`).

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

Installing the software image using ISCLI (2 of 2)

6. Confirm your request at the prompt. After the confirmation, the software begins the installation into the switch. Allow the installation to complete.
7. To enter the Global Configuration mode and to select either software **image1** or **image2** to run in switch memory for the next restart, enter the following commands:

```
Router# 14
Router(config)# boot image {image1|image2}
```

The system verifies the image that is installed during the next restart and displays a confirmation message:

```
Next boot will use switch software image1 instead of image2.
```

8. Restart the switch to run the new software. Enter the following command:

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

The system prompts you to confirm your request. Once confirmed, the switch restarts an uses the new software.

Installing the software image using a Browser-Based Interface

To install the switch software using a Browser-Based Interface (BBI), the software image you will install must reside in one of the following locations:

- FTP server
- TFTP server
- SFTP server
- Local system

After you log in to the BBI, complete the following steps to install the 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 displays.
3. If you are installing software from your computer (HTTP client), skip this step and go to the next. Otherwise, if you are loading software from an FTP, SFTP, or TFTP server, enter the server's information in the FTP, SFTP, or 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 an FTP, SFTP, or 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 is installed, the page refreshes to show the new software.

Before updating software on vLAG switches

When you update the software and boot images for switches configured with vLAG, ensure the following:

- Make sure that the spanning tree root switch is not one of the vLAG switches
- Shut down of ports should done under the port configuration
- Follow the shut down order of the ports as follows:
    a. ISL links
    b. vLAG links
    c. vLAG health check (MGT port)

Then follow this procedure to update the software on vLAG switches:

1. On Switch 2 (the original Secondary switch), shut down all links ISL, vLAG links, and vLAG HC. This is equivalent to powering off Switch 2.
   – All the traffic will failover to Switch 1 (the original Primary switch.).
   – After the shutdown of links on Switch 2, there will be N-S traffic loss of around ~0.16 seconds.

Updating software on vLAG switches (1 of 2)

2. Upgrade Switch 2 with the new image. Use FTP, STFP, or TFTP to copy the new ENOS and boot images onto the switch. Refer to “Before you install new software to the switch”.
   - After Switch 2 comes up, vLAG HC will be up and vLAG mismatch will happen with vLAG ports down (since it is still Secondary).
   - The traffic will still be forwarding via Switch 1 (the original Primary switch).
3. On Switch 1 (the original Primary switch), shut down all links ISL, vLAG links, and vLAG HC. This is equivalent to powering off Switch 1 (the original Primary switch)
   - All the traffic will failover to Switch 2, which will assume the vLAG operation role of Primary.
   - After all the links are up on Switch 2, there will be N-S traffic loss of around ~70 seconds due to spanning trees reconverging.

Updating software on vLAG switches (2 of 2)

4. Upgrade Switch 1 (the original Primary switch with the new ENOS image. Use FTP, STFP, or TFTP to copy the new ENOS and boot images onto the switch. Refer to “Before you install new software to the switch”.
   - After Switch 1 comes up, vLAG HC, ISL, and vLAG links will be up, and Switch 1 will assume the vLAG operation role of Secondary.
   - All the traffic will now follow the hash and load balance settings between Switch 1 and Switch 2.
   - There will be N-S traffic loss of around ~0.05 seconds.
5. Change the operational role of the vLAG switches to match the final topology by reloading Switch 2.
   - There will be N-S traffic loss of around ~0.102 seconds.
   - Switch 1 will reassume the vLAG primary role and switch 2 will reassume the vLAG secondary role.
6. Make sure that switch 1 is now the vLAG primary switch and switch 2 is now the vLAG secondary switch. Enter the following command:

```
NE2552E> show vlag information
```

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 displays.

```
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:
```

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 boot in recovery mode, press **R**. For more information, refer to “Boot Recovery Mode”.
- To restart the boot process from the beginning, press **Q**.
- To exit the Boot Management menu, press **E**. The booting process continues.

Boot Recovery Mode

The Boot Recovery Mode allows you to recover from a failed software or boot image upgrade using TFTP or XModem download.

To enter Boot Recovery Mode you must select the **Boot in recovery mode** option from the Boot Management Menu by pressing **R**. The entering rescue mode screen displays.

```
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? :
```

Boot Recovery Mode actions

The Boot Recovery Mode allows you to perform the following actions:

- To recover from a failed software or boot image upgrade using TFTP, press **T** and follow the screen prompts.
- To recover from a failed software or boot image upgrade using Xmodem download, press **X** and follow the screen prompts.
- To enable the loading of an unofficial image, press **P** and follow the screen prompts.
- To restart the boot process from the beginning, press **R**.
- To exit Boot Recovery Mode menu, press **E**. The boot process continues.

Upgrading the switch firmware

You can upgrade the switch firmware by using an FTP, TFTP, or SFTP file server. To transfer the switch firmware image files from the FTP, TFTP, or SFTP file server to the switch, you can establish a SSHv2 or Telnet session through the CMM. Ping the file server to make sure that you have a connection. The session performs optimally if all three network entities (file server, CMM, and switch IP addresses) are on the same subnet. Otherwise, you must use a router and configure a gateway address on the switch. Use the management-module interface to configure the IP addresses of the CMM external interface (eth0) and the switch to ensure that they are both on the same subnet as the file server.

Examples of IP addresses and masks are described in the following table.

Network entity	IP address	Subnet mask
FTP, TFTP or SFTP file server	192.168.2.178	255.255.255.0
CMM (eth0)	192.168.2.237	255.255.255.0
Switch-module current IP configuration (IF 128)	192.168.2.51	255.255.255.0

Switch firmware upgrade example

To upgrade the switch firmware, complete the following steps.

1. Log in to the switch.
2. At the switch CLI prompt, run the following commands to upload the firmware image to the switch.

   ```
   NE2552E> enable
   NE2552E# copy {ftp|tftp|sftp} {image1|image2} addr <server address> file
   <image file> {dataport|extmport|mgtport}
   ```

   Where *server address* is the IP address of file server, and *image file* is the file name of the firmware image as it appears in the file server operating-system.
3. Run the following command to upload the boot image to the switch.

   ```
   NE2552E# copy {ftp|tftp|sftp} boot addr <server address> file <boot file>
   {dataport|extmport|mgtport}
   ```

   Where *boot file* is the file name of the boot image as it appears in the file server operating-system.
4. Reset and restart the switch as described in “Resetting and restarting the switch”.

Resetting and restarting the switch

To activate the new image or images, you must reset the switch. To reset the switch, complete the following steps:

1. Log on to the CMM CLI. If necessary, obtain the IP address of the CMM from your system administrator.
2. Set the environment to the bay where you installed the switch. For example:

   ```
   system> env T system:switch[1]
   ```

3. Enter the reset command to restart the switch.

   ```
   System:switch[1]> reset
   ```

4. Wait for the POST to complete. POST may take up to two minutes.
5. Enter the `info` command for the switch that was just restarted and note the corresponding level of the firmware for the switch. Confirm that the firmware build number reflects the correct firmware release. Refer to “Switch build number example” for more information.

Switch build number example

To confirm that the firmware build number reflects the correct firmware release, refer to the following example:

```
system:switch[1]> info ...
Boot ROM
     Rel date: 01/18/2015
     Version: 7.11.0.0
     Status: Active
Main application
     Rel date: 01/18/2015
     Version: 7.11.0.0
     Status: Active
Main application
     Rel date: 01/18/2015
     Version: 7.11.0.0
     Status: Inactive
```