CONTENTS

Preface ix

Document Conventions ix
Related Documentation xi
Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

   Command Modes 1
   Using the Help System 3
   Understanding Abbreviated Commands 4
   No and Default Forms of Commands 5
   CLI Error Messages 5
   Configuration Logging 5

How to Use the CLI to Configure Features 6

   Configuring the Command History 6
      Changing the Command History Buffer Size 6
      Recalling Commands 6
      Disabling the Command History Feature 7
   Enabling and Disabling Editing Features 7
      Editing Commands Through Keystrokes 8
      Editing Command Lines That Wrap 9
   Searching and Filtering Output of show and more Commands 10
   Accessing the CLI on a Switch Stack 11
   Accessing the CLI Through a Console Connection or Through Telnet 11

CHAPTER 2

Using the Web Graphical User Interface 13

Prerequisites for Using the Web GUI 13

Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)
Information About Using The Web GUI 13
  Web GUI Features 13
Connecting the Console Port of the Switch 15
Logging On to the Web GUI 15
Enabling Web and Secure Web Modes 15
Configuring the Switch Web GUI 16

C H A P T E R  3
Managing Switch Stacks 21
  Finding Feature Information 21
  Prerequisites for Switch Stacks 21
  Restrictions for Switch Stacks 22
  Information About Switch Stacks 22
    Switch Stack Overview 22
      Supported Features in a Switch Stack 22
      Encryption Features 23
      StackWise-160 23
    Switch Stack Membership 23
      Changes to Switch Stack Membership 23
    Stack Member Numbers 24
    Stack Member Priority Values 25
    Switch Stack Bridge ID and MAC Address 25
      Persistent MAC Address on the Switch Stack 26
    Active and Standby Switch Election and Reelection 26
    Switch Stack Configuration Files 27
  Offline Configuration to Provision a Stack Member 28
    Effects of Adding a Provisioned Switch to a Switch Stack 28
    Effects of Replacing a Provisioned Switch in a Switch Stack 30
    Effects of Removing a Provisioned Switch from a Switch Stack 30
  Upgrading a Switch Running Incompatible Software 30
    Auto-Upgrade 30
    Auto-Advise 31
      Examples of Auto-Advise Messages 32
    SDM Template Mismatch in Switch Stacks 32
    Switch Stack Management Connectivity 32
      Connectivity to Specific Stack Members 33
<table>
<thead>
<tr>
<th>Chapter 5: Configuring Wireless High Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding Feature Information</td>
</tr>
<tr>
<td>Information about High Availability</td>
</tr>
<tr>
<td>Information About Redundancy</td>
</tr>
<tr>
<td>Configuring Redundancy in Access Points</td>
</tr>
<tr>
<td>Configuring Heartbeat Messages</td>
</tr>
<tr>
<td>Information about Access Point Stateful Switch Over</td>
</tr>
<tr>
<td>Initiating Graceful Switchover</td>
</tr>
<tr>
<td>Configuring EtherChannels for High Availability</td>
</tr>
<tr>
<td>Configuring LACP</td>
</tr>
<tr>
<td>Troubleshooting High Availability</td>
</tr>
<tr>
<td>Access the Standby Console</td>
</tr>
<tr>
<td>Before a Switchover</td>
</tr>
<tr>
<td>After a Switchover</td>
</tr>
<tr>
<td>Section</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Monitoring the Switch Stack</td>
</tr>
<tr>
<td>LACP Configuration: Example</td>
</tr>
<tr>
<td>Flex Link Configuration: Example</td>
</tr>
<tr>
<td>Viewing Redundancy Switchover History (GUI)</td>
</tr>
<tr>
<td>Viewing Switchover States (GUI)</td>
</tr>
</tbody>
</table>
Preface

- Document Conventions, page ix
- Related Documentation, page xi
- Obtaining Documentation and Submitting a Service Request, page xi

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in bold font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in courier font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td>Bold Courier font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
</tbody>
</table>
Document Conventions

### Convention | Description
--- | ---
\{x | y\} | Required alternative keywords are grouped in braces and separated by vertical bars.
\[x \{y \mid z\}\] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
\(< >\) | Nonprinting characters such as passwords are in angle brackets.
\[\] | Default responses to system prompts are in square brackets.
!, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

- **Note**
  Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

- **Tip**
  Means *the following information will help you solve a problem*.

- **Caution**
  Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

- **Timesaver**
  Means *the described action saves time*. You can save time by performing the action described in the paragraph.

- **Warning**
  IMPORTANT SAFETY INSTRUCTIONS
  This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071
  SAVE THESE INSTRUCTIONS
Related Documentation

Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Catalyst 3650 Switch documentation, located at:
  http://www.cisco.com/go/cat3650_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

- Error Message Decoder, located at:
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
CHAPTER 1

Using the Command-Line Interface

- Information About Using the Command-Line Interface, page 1
- How to Use the CLI to Configure Features, page 6

Information About Using the Command-Line Interface

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser. When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as show commands, which show the current configuration status, and clear commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.
### Table 1: Command Mode Summary

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
</table>
| User EXEC             | Begin a session using Telnet, SSH, or console.     | Switch>      | Enter `logout` or `quit` | Use this mode to  
• Change terminal settings.  
• Perform basic tests.  
• Display system information. |
| Privileged EXEC       | While in user EXEC mode, enter the `enable` command. | Switch#      | Enter `disable` to exit. | Use this mode to verify commands that you have entered. Use a password to protect access to this mode. |
| Global configuration  | While in privileged EXEC mode, enter the `configure` command. | Switch(config)# | To exit to privileged EXEC mode, enter `exit` or `end`, or press Ctrl-Z. | Use this mode to configure parameters that apply to the entire switch. |
| VLAN configuration    | While in global configuration mode, enter the `vlan vlan-id` command. | Switch(config-vlan)# | To exit to global configuration mode, enter the `exit` command.  
To return to privileged EXEC mode, press Ctrl-Z or enter `end`. | Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file. |
| Interface configuration | While in global configuration mode, enter the `interface` command (with a specific interface). | Switch(config-if)# | | Use this mode to configure parameters for the Ethernet ports. |
About This Mode

To exit to global configuration mode, enter `exit`.
To return to privileged EXEC mode, press `Ctrl-Z` or enter `end`.

To exit to global configuration mode, enter `exit`.
To return to privileged EXEC mode, press `Ctrl-Z` or enter `end`.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line configuration</td>
<td></td>
<td><code>Switch(config-line)#</code></td>
<td>To exit to global configuration mode, enter <code>exit</code>.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To return to privileged EXEC mode, press <code>Ctrl-Z</code> or enter <code>end</code>.</td>
<td></td>
</tr>
</tbody>
</table>

Using the Help System

You can enter a question mark (`?`) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

**SUMMARY STEPS**

1. `help`
2. `abbreviated-command-entry ?`
3. `abbreviated-command-entry <Tab>`
4. `?`
5. `command ?`
6. `command keyword ?`
## Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the `show configuration` privileged EXEC command in an abbreviated form:

```
Switch# show conf
```
No and Default Forms of Commands

Almost every configuration command also has a no form. In general, use the no form to disable a feature or function or reverse the action of a command. For example, the no shutdown interface configuration command reverses the shutdown of an interface. Use the command without the keyword no to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a default form. The default form of a command returns the command setting to its default. Most commands are disabled by default, so the default form is the same as the no form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the default command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

Table 2: Common CLI Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Meaning</th>
<th>How to Get Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Ambiguous command: &quot;show con&quot;</td>
<td>You did not enter enough characters for your switch to recognize the command.</td>
<td>Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.</td>
</tr>
<tr>
<td>% Incomplete command.</td>
<td>You did not enter all of the keywords or values required by this command.</td>
<td>Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.</td>
</tr>
<tr>
<td>% Invalid input detected at ‘^’ marker.</td>
<td>You entered the command incorrectly. The caret (^) marks the point of the error.</td>
<td>Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.</td>
</tr>
</tbody>
</table>

Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous
notification to registered applications whenever the configuration changes. You can choose to have the
notifications sent to the syslog.

**Note**
Only CLI or HTTP changes are logged.

---

### How to Use the CLI to Configure Features

#### Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature
is particularly useful for recalling long or complex commands or entries, including access lists. You can
customize this feature to suit your needs.

#### Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current
terminal session or for all sessions on a particular line. This procedure is optional.

**SUMMARY STEPS**

1. `terminal history [size number-of-lines]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>terminal history [size number-of-lines]</code></td>
<td>Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>terminal history size 200</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.

**Note**
The arrow keys function only on ANSI-compatible terminals such as VT100s.
SUMMARY STEPS

1. Ctrl-P or use the up arrow key
2. Ctrl-N or use the down arrow key
3. show history

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Ctrl-P or use the up arrow key</strong></td>
</tr>
<tr>
<td></td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Ctrl-N or use the down arrow key</strong></td>
</tr>
<tr>
<td></td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>show history</strong></td>
</tr>
<tr>
<td></td>
<td>Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.</td>
</tr>
</tbody>
</table>

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. terminal no history

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>terminal no history</strong></td>
</tr>
<tr>
<td></td>
<td>Disables the feature during the current terminal session in privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.
SUMMARY STEPS

1. terminal editing
2. terminal no editing

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# terminal editing</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# terminal no editing</td>
<td></td>
</tr>
</tbody>
</table>

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 3: Editing Commands

<table>
<thead>
<tr>
<th>Editing Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or use the left arrow key</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>Ctrl-F or use the right arrow key</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Esc B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc F</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Ctrl-T</td>
<td>Transposes the character to the left of the cursor with the character located at the cursor.</td>
</tr>
<tr>
<td>Key Combination</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete or Backspace key</td>
<td>Erases the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-U or Ctrl-X</td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Esc D</td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Esc C</td>
<td>Capitalizes at the cursor.</td>
</tr>
<tr>
<td>Esc L</td>
<td>Changes the word at the cursor to lowercase.</td>
</tr>
<tr>
<td>Esc U</td>
<td>Capitalizes letters from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Ctrl-V or Esc Q</td>
<td>Designates a particular keystroke as an executable command, perhaps as a shortcut.</td>
</tr>
<tr>
<td>Return key</td>
<td>Scrolls down a line or screen on displays that are longer than the terminal screen can display.</td>
</tr>
<tr>
<td>Note</td>
<td>The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.</td>
</tr>
<tr>
<td>Space bar</td>
<td>Scrolls down one screen.</td>
</tr>
<tr>
<td>Ctrl-L or Ctrl-R</td>
<td>Redisplays the current command line if the switch suddenly sends a message to your screen.</td>
</tr>
</tbody>
</table>

### Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press Ctrl-B or the left arrow key repeatedly. You can also press Ctrl-A to immediately move to the beginning of the line.
The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

**SUMMARY STEPS**

1. access-list
2. Ctrl-A
3. Return key

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> access-list</td>
<td>Displays the global configuration command entry that extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Ctrl-A</td>
<td>Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Return key</td>
<td>Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.</td>
</tr>
</tbody>
</table>

**Searching and Filtering Output of show and more Commands**

You can search and filter the output for `show` and `more` commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.
### SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 
{show | more} command | {begin | include | exclude} regular-expression | Searches and filters the output. Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output are not displayed, but the lines that contain output appear. |

**Example:**

Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up

---

### Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser. You manage the switch stack and the stack member interfaces through the active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.

**Note**

We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the `session standby ios` privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the `session switch stack-member-number` privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

### Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:
• Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.

• Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
  • The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
  • The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.
Using the Web Graphical User Interface

- Prerequisites for Using the Web GUI, page 13
- Information About Using The Web GUI, page 13
- Connecting the Console Port of the Switch, page 15
- Logging On to the Web GUI, page 15
- Enabling Web and Secure Web Modes, page 15
- Configuring the Switch Web GUI, page 16

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows XP SP1 (or later releases), or Windows 2000 SP4 (or later releases).
- The switch GUI is compatible with Microsoft Internet Explorer version 10.x, Mozilla Firefox 20.x, or Google Chrome 26.x.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each switch.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help.

You might need to disable your browser’s pop-up blocker to view the online help.

Web GUI Features

The switch web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial
wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of switch, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the switch for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the switch, WLAN, and radios.
- Enables you to configure and set security policies on your switch.
- Enables you to access the switch operating system software management commands.

The Administration tab enables you to configure system logs.
Connecting the Console Port of the Switch

**Before You Begin**

Before you can configure the switch for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

---

**Step 1**

Connect one end of a null-modem serial cable to the switch's RJ-45 console port and the other end to your PC's serial port.

**Step 2**

Plug the AC power cord into the switch and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the switch passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

**Step 3**

Enter yes. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.

After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the switch is configured with the IP address for service port.

---

Logging On to the Web GUI

Enter the switch IP address in your browser’s address bar. For a secure connection, enter https://ip-address. For a less secure connection, enter http://ip-address.

---

Enabling Web and Secure Web Modes

**Step 1**

Choose Configuration > Switch > Management > Protocol Management > HTTP-HTTPS.

The HTTP-HTTPS Configuration page appears.

**Step 2**

To enable web mode, which allows users to access the switch GUI using “http://ip-address,” choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.
Step 3  To enable secure web mode, which allows users to access the switch GUI using “https://ip-address,” choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.

Step 4  Choose to track the device in the IP Device Tracking check box.

Step 5  Choose to enable the trust point in the Enable check box.

Step 6  Choose the trustpoints from the Trustpoints drop-down list.

Step 7  Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box. The valid range is from 1 to 600 seconds.

Step 8  Enter the server life time in the Server Life Time (1 to 86400 sec) text box. The valid range is from 1 to 86400 seconds.

Step 9  Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box. The valid range is from 1 to 86400 connections.

Step 10  Click Apply.

Step 11  Click Save Configuration.

### Configuring the Switch Web GUI

The configuration wizard enables you to configure basic settings on the switch. You can run the wizard after you receive the switch from the factory or after the switch has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

---

**Step 1**  Connect your PC to the service port and configure an IPv4 address to use the same subnet as the switch. The switch is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.

**Step 2**  Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is admin and the password is cisco. You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.

When you log in for the first time, the **Accessing Cisco Switch** `<Model Number> <Hostname>` page appears.

**Step 3**  On the **Accessing Cisco Switch** page, click the **Wireless Web GUI** link to access switch web GUI **Home** page.

**Step 4**  Choose **Configuration > Wizard** to perform all steps that you need to configure the switch initially. The **Admin Users** page appears.

**Step 5**  On the **Admin Users** page, enter the administrative username to be assigned to this switch in the User Name text box and the administrative password to be assigned to this switch in the Password and Confirm Password text boxes. Click **Next**.

The default username is admin and the default password is cisco. You can also create a new administrator user for the switch. You can enter up to 24 ASCII characters for username and password.
The **SNMP System Summary** page appears.

**Step 6**  
On the **SNMP System Summary** page, enter the following SNMP system parameters for the switch, and click **Next**:

- Customer-definable switch location in the **Location** text box.
- Customer-definable contact details such as phone number with names in the **Contact** text box.
- Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the **SNMP Global Trap** drop-down list.
- Choose **enabled** to send system log messages or **disabled** not to send system log messages from the **SNMP Logging** drop-down list.

**Note**  
The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The **Management Port** page appears.

**Step 7**  
In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.

- Interface IP address that you assigned for the service port in the **IP Address** text box.
- Network mask address of the management port interface in the **Netmask** text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the **IPv4 DHCP Server** text box.

The **Wireless Management** page appears.

**Step 8**  
In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the **Select Interface** drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the **VLAN id** text box.
- IP address of wireless management interface where access points are connected in the **IP Address** text box.
- Network mask address of the wireless management interface in the **Netmask** text box.
- DHCP IPv4 IP address in the **IPv4 DHCP Server** text box.

When selecting VLAN as interface, you can specify the ports as —Trunk or Access ports from the selected list displayed in the **Switch Port Configuration** text box.

The **RF Mobility and Country Code** page appears.

**Step 9**  
In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

**Note**  
Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

**Step 10**  
In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Choose **Mobility Controller** or **Mobility Agent** from the Mobility Role drop-down list:
• If Mobility Agent is chosen, enter the mobility controller IP address in the Mobility Controller IP Address text box and mobility controller IP address in the Mobility Controller Public IP Address text box.

• If Mobility Controller is chosen, then the mobility controller IP address and mobility controller public IP address are displayed in the respective text boxes.

• Displays mobility protocol port number in the Mobility Protocol Port text box.

• Displays the mobility switch peer group name in the Mobility Switch Peer Group Name text box.

• Displays whether DTLS is enabled in the DTLS Mode text box.

  DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.

• Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.

• The amount of time (in seconds) between each ping request sent to an peer switch in the Mobility Keepalive Interval (1-30) sec text box.

  Valid range is from 1 to 30 seconds, and the default value is 10 seconds.

• Number of times a ping request is sent to an peer switch before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.

  The valid range is from 3 to 20, and the default value is 3.

• The DSCP value that you can set for the mobility switch in the Mobility Control Message DSCP Value (0-63) text box.

  The valid range is 0 to 63, and the default value is 0.

• Displays the number of mobility switch peer group member configured in the Switch Peer Group Members Configured text box.

The WLANs page appears.

**Step 11**

In the WLANs page, enter the following WLAN configuration parameters, and click Next.

• WLAN identifier in the WLAN ID text box.

• SSID of the WLAN that the client is associated with in the SSID text box.

• Name of the WLAN used by the client in the Profile Name text box.

The 802.11 Configuration page appears.

**Step 12**

In the 802.11 Configuration page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click Next.

The Set Time page appears.

**Step 13**

In the Set Time page, you can configure the time and date on the switch based on the following parameters, and click Next.

• Displays current timestamp on the switch in the Current Time text box.

• Choose either Manual or NTP from the Mode drop-down list.

  On using the NTP server, all access points connected to the switch, synchronizes its time based on the NTP server settings available.
Choose date on the switch from the Year, Month, and Day drop-down list.

Choose time from the Hours, Minutes, and Seconds drop-down list.

Enter the time zone in the Zone text box and select the offset setting required when compared to the current time configured on the switch from the Offset drop-down list.

The Save Wizard page appears.

**Step 14**

In the Save Wizard page, you can review the configuration settings performed on the switch using these steps, and if you wish to change any configuration value, click Previous and navigate to that page.

You can save the switch configuration created using the wizard only if a success message is displayed for all the wizards. If the Save Wizard page displays errors, you must recreate the wizard for initial configuration of the switch.
Managing Switch Stacks

- Finding Feature Information, page 21
- Prerequisites for Switch Stacks, page 21
- Restrictions for Switch Stacks, page 22
- Information About Switch Stacks, page 22
- How to Configure a Switch Stack, page 34
- Troubleshooting the Switch Stack, page 42
- Monitoring the Switch Stack, page 44
- Configuration Examples for Switch Stacks, page 45
- Additional References for Switch Stacks, page 52
- Feature History and Information for Switch Stacks, page 53

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Switch Stacks

All the switches in the switch stack need to be running the same license level as the active switch. For information about license levels, see the System Management Configuration Guide (Catalyst 3650 Switches).

All switches in the switch stack need to be running compatible software versions.
A StackWise adapter must be installed in the stacking port to enable stacking. For switch stack hardware considerations, see the *Catalyst 3650 Switch Hardware Installation Guide*.

**Restrictions for Switch Stacks**

The following are restrictions for your switch stack configuration:

- Switch stacks running the LAN Base license level do not support Layer 3 features.
- A switch stack can have up to nine stacking-capable switches connected through their StackWise-160 ports.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

**Related Topics**

- Supported Features in a Switch Stack, on page 22

**Information About Switch Stacks**

**Switch Stack Overview**

A switch stack can have up to nine stacking-capable switches connected through their StackWise-160 ports. The stack members work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

A switch stack always has one active switch and one standby switch. If the active switch becomes unavailable, the standby switch assumes the role of the active switch, and continues to keep the stack operational. The active switch controls the operation of the switch stack, and is the single point of stack-wide management. From the active switch, you configure:

- System-level (global) features that apply to all stack members
- Interface-level features for each stack member

The active switch contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for each stack member. Each stack member has a current copy of these files for back-up purposes.

**Supported Features in a Switch Stack**

The system-level features supported on the active switch are supported on the entire switch stack.

**Related Topics**

- Restrictions for Switch Stacks, on page 22
Encryption Features

If the active switch is running the cryptographic universal software image (supports encryption), the encryption features are available on the switch stack.

StackWise-160

The stack members use the StackWise-160 technology to work together as a unified system. Layer 2 and Layer 3 protocols support the entire switch stack as a single entity in the network.

Note

Switch stacks running the LAN Base image do not support Layer 3 features.

StackWise-160 has a stack bandwidth of 160 Gbps, and uses stateful switchover (SSO) to provide resiliency within the stack. The stack behaves as a single switching unit that is managed by an active switch elected by the member switches. The active switch automatically elects a standby switch within the stack. The active switch creates and updates all the switching, routing and wireless information and constantly synchronizes that information with the standby switch. Access points continue to remain connected during an active-to-standby switchover unless the access point is directly connected to the active switch. In this case the access point will lose power and reboot. A working stack can accept new members or delete old ones without service interruption.

Switch Stack Membership

A standalone switch is a switch stack with one stack member that also operates as the active switch. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them as the active switch. You can connect standalone switches to an existing switch stack to increase the stack membership.

Changes to Switch Stack Membership

If you replace a stack member with an identical model, the new switch functions with exactly the same configuration as the replaced switch, assuming that the new switch (referred to as the provisioned switch) is using the same member number as the replaced switch.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the active switch or you add powered-on standalone switches or switch stacks.

- Adding powered-on switches (merging) causes all switches to reload and elect a new active switch from among themselves. The newly elected active switch retains its role and configuration. All other switches retain their stack member numbers and use the stack configuration of the newly elected active switch.

- Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. This can cause:
  - An IP address conflict in your network. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.
  - A MAC address conflict between two members in the stack. You can use the `stack-mac update force` command to resolve the conflict.
If a newly created switch stack does not have an active switch or standby switch, the switch stack will reload and elect a new active switch.

**Note**

Make sure that you power off the switches that you add to or remove from the switch stack.

After adding or removing stack members, make sure that the switch stack is operating at full bandwidth (160 Gbps). Press the Mode button on a stack member until the Stack mode LED is on. The last two right port LEDs on all switches in the stack should be green. Depending on the switch model, the last two right ports are 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports (10/100/1000 ports). If one or both of these LEDs are not green on any of the switches, the stack is not operating at full bandwidth.

If you remove powered-on members but do not want to partition the stack:

- Power off the switches in the newly created switch stacks.
- Reconnect them to the original switch stack through their stack ports.
- Power on the switches.

For cabling and power considerations that affect switch stacks, see the *Catalyst 3650 Switch Hardware Installation Guide*.

**Related Topics**

- Assigning a Stack Member Number, on page 36
- Switch Stack Configuration Scenarios, on page 45

**Stack Member Numbers**

The stack member number (1 to 9) identifies each member in the Switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the `show switch` EXEC command.

A new, out-of-the-box Switch (one that has not joined a Switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a Switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same Switch stack cannot have the same stack member number. Every stack member, including a standalone Switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

- If you manually change the stack member number by using the `switch current-stack-member-number renumber new-stack-member-number` command, the new number goes into effect after that stack member resets (or after you use the `reload slot stack-member-number` privileged EXEC command) and only if that number is not already assigned to any other members in the stack. Another way to change the stack member number is by changing the Switch_NUMBER environment variable.

  If the number is being used by another member in the stack, the Switch selects the lowest available number in the stack.

  If you manually change the number of a stack member and no interface-level configuration is associated with that new member number, that stack member resets to its default configuration.
You cannot use the `switch current-stack-member-number renumber new-stack-member-number` command on a provisioned Switch. If you do, the command is rejected.

- If you move a stack member to a different Switch stack, the stack member retains its number only if the number is not being used by another member in the stack. If it is being used, the Switch selects the lowest available number in the stack.

- If you merge Switch stacks, the Switch that join the Switch stack of a new active switch select the lowest available numbers in the stack.

As described in the hardware installation guide, you can use the Switch port LEDs in Stack mode to visually determine the stack member number of each stack member.

**Related Topics**
- Assigning a Stack Member Number, on page 36
- Switch Stack Configuration Scenarios, on page 45

### Stack Member Priority Values

A higher priority value for a stack member increases the probability of it being elected active switch and retaining its stack member number. The priority value can be 1 to 15. The default priority value is 1. You can display the stack member priority value by using the `show switch` EXEC command.

---

**Note**

We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as the active switch if a reelection occurs.

To change the priority value for a stack member, use the `switch stack-member-number priority new priority-value` command. For more information, see the “Setting the Stack Member Priority Value” section.

The new priority value takes effect immediately but does not affect the current active switch. The new priority value helps determine which stack member is elected as the new active switch when the current active switch or the switch stack resets.

**Related Topics**
- Setting the Stack Member Priority Value, on page 37

### Switch Stack Bridge ID and MAC Address

A switch stack is identified in the network by its `bridge ID` and, if it is operating as a Layer 3 device, its router MAC address. The bridge ID and router MAC address are determined by the MAC address of the active switch.

If the active switch changes, the MAC address of the new active switch determines the new bridge ID and router MAC address.

If the entire switch stack reloads, the switch stack uses the MAC address of the active switch.
Persistent MAC Address on the Switch Stack

You can use the persistent MAC address feature to set a time delay before the stack MAC address changes. During this time period, if the previous active switch rejoins the stack, the stack continues to use its MAC address as the stack MAC address, even if the switch is now a stack member and not an active switch. If the previous active switch does not rejoin the stack during this period, the switch stack takes the MAC address of the new active switch as the stack MAC address. By default, the stack MAC address will be the MAC address of the first active switch, even if a new active switch takes over.

You can also configure stack MAC persistency so that the stack MAC address never changes to the new active switch MAC address.

Related Topics

- Enabling the Persistent MAC Address Feature, on page 34
- Enabling the Persistent MAC Address Feature: Example, on page 47

Active and Standby Switch Election and Reelection

All stack members are eligible to be the active switch or the standby switch. If the active switch becomes unavailable, the standby switch becomes the active switch.

An active switch retains its role unless one of these events occurs:

- The switch stack is reset.
- The active switch is removed from the switch stack.
- The active switch is reset or powered off.
- The active switch fails.
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks.

The active switch is elected or reelected based on one of these factors and in the order listed:

1. The switch that is currently the active switch.
2. The switch with the highest stack member priority value.
3. The switch with the shortest start-up time.
4. The switch with the lowest MAC address.

Note

We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as active switch if a reelection occurs.

Note

The factors for electing or reelecting a new standby switch are same as those for the active switch election or reelection, and are applied to all participating switches except the active switch.
After election, the new active switch becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected during a new active switch election and reset.

When the previous active switch becomes available, it does not resume its role as the active switch.

If you power on or reset an entire switch stack, some stack members might not participate in the active switch election. Stack members that are powered on within the same 2-minute timeframe participate in the active switch election and have a chance to become the active switch. Stack members that are powered on after the 120-second timeframe do not participate in this initial election and become stack members. For powering considerations that affect active-switch elections, see the switch hardware installation guide.

As described in the hardware installation guide, you can use the ACTV LED on the switch to see if the switch is the active switch.

**Switch Stack Configuration Files**

The active switch has the saved and running configuration file for the switch stack. The standby switch automatically receives the synchronized running configuration file. Stack members receive synchronized copies when the running configuration file is saved into the startup configuration file. If the active switch becomes unavailable, the standby switch takes over with the current running configuration.

The configuration files record these settings:

- System-level (global) configuration settings such as IP, STP, VLAN, and SNMP settings that apply to all stack members
- Stack member interface-specific configuration settings that are specific for each stack member

---

**Note**

The interface-specific settings of the active switch are saved if the active switch is replaced without saving the running configuration to the startup configuration.

A new, out-of-box switch joining a switch stack uses the system-level settings of that switch stack. If a switch is moved to a different switch stack before it is powered on, that switch loses its saved configuration file and uses the system-level configuration of the new switch stack. If the switch is powered on as a standalone switch before it joins the new switch stack, the stack will reload. When the stack reloads, the new switch may become the active switch, retain its configuration and overwrite the configuration files of the other stack members.

The interface-specific configuration of each stack member is associated with the stack member number. Stack members retain their numbers unless they are manually changed or they are already used by another member in the same switch stack. If the stack member number changes, the new number goes into effect after that stack member resets.

- If an interface-specific configuration does not exist for that member number, the stack member uses its default interface-specific configuration.
- If an interface-specific configuration exists for that member number, the stack member uses the interface-specific configuration associated with that member number.

If you replace a failed member with an identical model, the replacement member automatically uses the same interface-specific configuration as the failed switch. You do not need to reconfigure the interface settings. The replacement switch (referred to as the provisioned switch) must have the same stack member number as the failed switch.
You back up and restore the stack configuration in the same way as you would for a standalone switch configuration.

**Related Topics**
- Assigning a Stack Member Number, on page 36
- Switch Stack Configuration Scenarios, on page 45

### Offline Configuration to Provision a Stack Member

You can use the offline configuration feature to provision (to supply a configuration to) a new switch before it joins the switch stack. You can configure the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack. The configuration that you create on the switch stack is called the **provisioned configuration**. The switch that is added to the switch stack and that receives this configuration is called the **provisioned switch**.

You manually create the provisioned configuration through the `switch stack-member-number provision type` global configuration command. You must change the `stack-member-number` on the provisioned switch before you add it to the stack, and it must match the stack member number that you created for the new switch on the switch stack. The switch type in the provisioned configuration must match the switch type of the newly added switch. The provisioned configuration is automatically created when a switch is added to a switch stack and when no provisioned configuration exists.

When you configure the interfaces associated with a provisioned switch, the switch stack accepts the configuration, and the information appears in the running configuration. However, as the switch is not active, any configuration on the interface is not operational and the interface associated with the provisioned switch does not appear in the display of the specific feature. For example, VLAN configuration information associated with a provisioned switch does not appear in the `show vlan` user EXEC command output on the switch stack.

The switch stack retains the provisioned configuration in the running configuration whether or not the provisioned switch is part of the stack. You can save the provisioned configuration to the startup configuration file by entering the `copy running-config startup-config` privileged EXEC command. The startup configuration file ensures that the switch stack can reload and can use the saved information whether or not the provisioned switch is part of the switch stack.

**Related Topics**
- Removing Provisioned Switch Information, on page 39
- Provisioning a New Member for a Switch Stack: Example, on page 47

### Effects of Adding a Provisioned Switch to a Switch Stack

When you add a provisioned Switch to the switch stack, the stack applies either the provisioned configuration or the default configuration. This table lists the events that occur when the switch stack compares the provisioned configuration with the provisioned switch.
### Table 4: Results of Comparing the Provisioned Configuration with the Provisioned Switch

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>The stack member numbers and the Switch types match.</td>
<td>1 If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and&lt;br&gt;2 If the Switch type of the provisioned switch matches the Switch type in the provisioned configuration on the stack.</td>
</tr>
<tr>
<td>The stack member numbers match but the Switch types do not match.</td>
<td>1 If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but&lt;br&gt;2 The Switch type of the provisioned switch does not match the Switch type in the provisioned configuration on the stack.</td>
</tr>
<tr>
<td>The stack member number is not found in the provisioned configuration.</td>
<td></td>
</tr>
<tr>
<td>The stack member number of the provisioned switch is not found in the provisioned configuration.</td>
<td></td>
</tr>
</tbody>
</table>

If you add a provisioned switch that is a different type than specified in the provisioned configuration to a powered-down switch stack and then apply power, the switch stack rejects the (now incorrect) `switch stack-member-number provision type` global configuration command in the startup configuration file. However, during stack initialization, the nondefault interface configuration information in the startup configuration file for the provisioned interfaces (potentially of the wrong type) is executed. Depending on the differences between the actual Switch type and the previously provisioned switch type, some commands are rejected, and some commands are accepted.
Effects of Replacing a Provisioned Switch in a Switch Stack
When a provisioned switch in a switch stack fails, it is removed from the stack, and is replaced with another switch. The stack applies either the provisioned configuration or the default configuration to it. The events that occur when the switch stack compares the provisioned configuration with the provisioned switch are the same as those when you add a provisioned switch to a stack.

Effects of Removing a Provisioned Switch from a Switch Stack
If you remove a provisioned switch from the switch stack, the configuration associated with the removed stack member remains in the running configuration as provisioned information. To completely remove the configuration, use the `no switch stack-member-number provision` global configuration command.

Upgrading a Switch Running Incompatible Software
The auto-upgrade and auto-advise features enable a switch with software packages that are incompatible with the switch stack to be upgraded to a compatible software version so that it can join the switch stack.

Auto-Upgrade
The purpose of the auto-upgrade feature is to allow a switch to be upgraded to a compatible software image, so that the switch can join the switch stack.

When a new switch attempts to join a switch stack, each stack member performs compatibility checks with itself and the new switch. Each stack member sends the results of the compatibility checks to the active switch, which uses the results to determine whether the switch can join the switch stack. If the software on the new switch is incompatible with the switch stack, the new switch enters version-mismatch (VM) mode.

If the auto-upgrade feature is enabled on the new switch, the active switch automatically upgrades the new switch with the same software image running on a compatible stack member. Auto-upgrade starts a few minutes after the mismatched software is detected before starting.

Auto-upgrade is disabled by default.

Auto-upgrade includes an auto-copy process and an auto-extract process.

- Auto-copy automatically copies the software image running on any stack member to the new switch to automatically upgrade it. Auto-copy occurs if auto-upgrade is enabled, if there is enough flash memory in the new switch, and if the software image running on the switch stack is suitable for the new switch.
A switch in VM mode might not run all released software. For example, new switch hardware is not recognized in earlier versions of software.

- Automatic extraction (auto-extract) occurs when the auto-upgrade process cannot find the appropriate software in the stack to copy to the new switch. In that case, the auto-extract process searches all switches in the stack for the bin file needed to upgrade the switch stack or the new switch. The bin file can be in any flash file system in the switch stack or in the new switch. If a bin file suitable for the new switch is found on a stack member, the process extracts the file and automatically upgrades the new switch.

The auto-upgrade feature is not available in bundle mode. The switch stack must be running in installed mode. If the switch stack is in bundle mode, use the `software expand` privileged EXEC command to change to installed mode.

You can enable auto-upgrade by using the `software auto-upgrade enable` global configuration command on the new switch. You can check the status of auto-upgrade by using the `show running-config` privileged EXEC command and by checking the `Auto upgrade` line in the display.

You can configure auto-upgrade to upgrade the new switch with a specific software bundle by using the `software auto-upgrade source url` global configuration command. If the software bundle is invalid, the new switch is upgraded with the same software image running on a compatible stack member.

When the auto-upgrade process is complete, the new switch reloads and joins the stack as a fully functioning member. If you have both stack cables connected during the reload, network downtime does not occur because the switch stack operates on two rings.

For more information about upgrading a switch running incompatible software see the Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE (Catalyst 3650 Switches).

**Auto-Advise**

The auto-advise feature is triggered when:

- The auto-upgrade feature is disabled.
- The new switch is in bundle mode and the stack is in installed mode. Auto-advise displays syslog messages about using the `software auto-upgrade` privileged EXEC command to change the new switch to installed mode.
- The stack is in bundle mode. Auto-advise displays syslog messages about booting the new switch in bundle mode so that it can join the stack.
- An auto-upgrade attempt fails because the new switch is running incompatible software. After the switch stack performs compatibility checks with the new switch, auto-advise displays syslog messages about whether the new switch can be auto-upgraded.

Auto-advise cannot be disabled. It does not give suggestions when the switch stack software and the software of the switch in version-mismatch (VM) mode do not contain the same license level.
Examples of Auto-Advise Messages

**Auto-Upgrade Is Disabled and Incompatible Switch Attempting to Join: Example**

This sample auto-advise output shows the system messages displayed when the auto-upgrade feature is disabled and an incompatible switch 1 tries to join the switch stack:

```
*Oct 18 08:36:19.379: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer: Auto advise
   initiated for switch 1
*Oct 18 08:36:19.380: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: Searching stack for software
to upgrade switch 1
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: Switch 1 with incompatible
   software has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: added to the stack. The
   software running on
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: all stack members was
   scanned and it has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: determined that the 'software
   auto-upgrade'
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: command can be used to
   install compatible
```

**Auto-Upgrade is Disabled and New Switch is in Bundle Mode: Example**

This sample auto-advise output shows the system messages displayed when auto-upgrade is disabled and a switch running in bundle mode tries to join the stack that is running in installed mode:

```
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer: Auto advise
   initiated for switch 1
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: Switch 1 running bundled
   software has been added
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: to the stack that is running
   installed software.
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: The 'software auto-upgrade'
   command can be used to
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: convert switch 1 to the
   installed running mode by
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer: installing its running
   software.
```

**SDM Template Mismatch in Switch Stacks**

All stack members use the Switch Database Management (SDM) template configured on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

You can use the `show switch` privileged EXEC command to see if any stack members are in SDM-mismatch mode.

Version-mismatch (VM) mode has priority over SDM-mismatch mode. If a VM-mode condition and an SDM-mismatch mode exist, the switch stack first attempts to resolve the VM-mode condition.

**Switch Stack Management Connectivity**

You manage the switch stack and the stack member interfaces through the active switch. You can use the CLI, SNMP, and supported network management applications such as CiscoWorks. You cannot manage stack members on an individual Switch basis.
Use SNMP to manage network features across the stack that are defined by supported MIBs. The switch does not support MIBs to manage stacking-specific features such as stack membership and election.

**Connectivity to Specific Stack Members**

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, you can access it from the active switch using the `session standby ios privileged EXEC` command. To debug a specific stack member, use the `session switch stack-member-number privileged EXEC` command from the active switch to access the diagnostic shell of the stack member. Only the `show` and `debug` commands are available in a CLI session to a specific stack member.

**Connectivity to the Switch Stack Through an IP Address**

The switch stack is managed through a single IP address. The IP address is a system-level setting and is not specific to the active switch or to any other stack member. You can still manage the stack through the same IP address even if you remove the active switch or any other stack member from the stack, provided there is IP connectivity.

Stack members retain their IP addresses when you remove them from a switch stack. To avoid a conflict by having two devices with the same IP address in your network, change the IP addresses of any Switch that you remove from the switch stack.

For related information about switch stack configurations, see the *Switch Stack Configuration Files section*.

**Connectivity to the Switch Stack Through Console Ports or Ethernet Management Ports**

You can connect to the active switch by using one of these methods:

- You can connect a terminal or a PC to the active switch through the console port of one or more stack members.

- You can connect a PC to the active switch through the Ethernet management ports of one or more stack members. For more information about connecting to the switch stack through Ethernet management ports, see the *Using the Ethernet Management Port section*.

Be careful when using multiple CLI sessions to the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.

We recommend using only one CLI session when managing the switch stack.
How to Configure a Switch Stack

Default Switch Stack Configuration

The following table shows the default switch stack configuration settings:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack MAC address timer</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Stack member number</td>
<td>1</td>
</tr>
<tr>
<td>Stack member priority value</td>
<td>1</td>
</tr>
<tr>
<td>Offline configuration</td>
<td>The switch stack is not provisioned.</td>
</tr>
<tr>
<td>Persistent MAC address</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Enabling the Persistent MAC Address Feature

When you enter the command to configure this feature, a warning message appears with the consequences of your configuration. You should use this feature cautiously. Using the old active switch MAC address elsewhere in the same domain could result in lost traffic.

Follow these steps to enable persistent MAC address:

SUMMARY STEPS

1. enable
2. configure terminal
3. stack-mac persistent timer [0 | time-value]
4. end
5. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 stack-mac persistent timer [0</td>
<td>$time-value$]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# stack-mac persistent timer ?</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**What to Do Next**

Use the **no stack-mac persistent timer** global configuration command to disable the persistent MAC address feature.

**Related Topics**

Persistent MAC Address on the Switch Stack, on page 26

Enabling the Persistent MAC Address Feature: Example, on page 47
Assigning a Stack Member Number

This optional task is available only from the active switch.

Follow these steps to assign a member number to a stack member:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `switch current-stack-member-number renumber new-stack-member-number`
4. `end`
5. `reload slot stack-member-number`
6. `show switch`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switch current-stack-member-number renumber new-stack-member-number</code></td>
<td>Specifies the current stack member number and the new stack member number for the stack member. The range is 1 to 9. You can display the current stack member number by using the <code>show switch</code> user EXEC command.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# switch 3 renumber 4</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>reload slot stack-member-number</code></td>
<td>Resets the stack member.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# reload slot 4</code></td>
<td></td>
</tr>
</tbody>
</table>
### Setting the Stack Member Priority Value

This optional task is available only from the active switch.

Follow these steps to assign a priority value to a stack member:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. switch stack-member-number priority new-priority-number
4. end
5. show switch stack-member-number
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>switch stack-member-number priority new-priority-number</td>
<td>Specifies the stack member number and the new priority for the stack member. The stack member number range is 1 to 9. The priority value range is 1 to 15. You can display the current priority value by using the <code>show switch</code> user EXEC command. The new priority value takes effect immediately but does not affect the current active switch. The new priority value helps determine which stack member is elected as the new active switch when the current active switch or switch stack resets.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# switch 3 priority 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>show switch stack-member-number</td>
<td>Verify the stack member priority value.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# show switch</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Stack Member Priority Values, on page 25

### Provisioning a New Member for a Switch Stack

This optional task is available only from the active switch.
SUMMARY STEPS

1. show switch
2. configure terminal
3. switch stack-member-number provision type
4. end
5. copy running-config startup-config

DETAILLED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show switch</td>
<td>Displays summary information about the switch stack.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show switch</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>switch stack-member-number provision type</td>
<td>Specifies the stack member number for the preconfigured switch. By default, no switches are provisioned. For stack-member-number, the range is 1 to 9. Specify a stack member number that is not already used in the switch stack. See Step 1. For type, enter the model number of a supported switch that is listed in the command-line help strings.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# switch 3 provision WS-xxxx</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Removing Provisioned Switch Information

Before you begin, you must remove the provisioned switch from the stack. This optional task is available only from the active switch.
SUMMARY STEPS

1. configure terminal
2. no switch stack-member-number provision
3. end
4. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>no switch stack-member-number provision</td>
<td>Removes the provisioning information for the specified member.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# no switch 3 provision</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
</tbody>
</table>

If you are removing a provisioned switch in a stack with this configuration:

- The stack has four members
- Stack member 1 is the active switch
- Stack member 3 is a provisioned switch

and want to remove the provisioned information and to avoid receiving an error message, you can remove power from stack member 3, disconnect the StackWise-160 cables between the stack member 3 and switches to which it is connected, reconnect the cables between the remaining stack members, and enter the no switch stack-member-number provision global configuration command.

Related Topics:

- Offline Configuration to Provision a Stack Member, on page 28
- Provisioning a New Member for a Switch Stack: Example, on page 47
Displaying Incompatible Switches in the Switch Stack

SUMMARY STEPS

1. show switch

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>show switch</td>
<td>Displays any incompatible switches in the switch stack (indicated by a 'Current State' of 'V-Mismatch'). The V-Mismatch state identifies the switches with incompatible software. The output displays Lic-Mismatch for switches that are not running the same license level as the active switch. For information about managing license levels, see the System Management Configuration Guide (Catalyst 3650 Switches).</td>
</tr>
</tbody>
</table>

Upgrading an Incompatible Switch in the Switch Stack

SUMMARY STEPS

1. software auto-upgrade
2. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>software auto-upgrade</td>
<td>Upgrades incompatible switches in the switch stack, or changes switches in bundle mode to installed mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# software auto-upgrade</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Troubleshooting the Switch Stack

Accessing the Diagnostic Console of a Stack Member

Before You Begin
This optional task is available only from the active switch.

SUMMARY STEPS

1. session switch stack-member-number
2. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>session switch stack-member-number</td>
<td>Accesses the diagnostic shell of the stack member from the active switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# session switch 2</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Returns to the CLI session on the active switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(diag)&gt; exit</td>
<td></td>
</tr>
</tbody>
</table>

Temporarily Disabling a Stack Port

If a stack port is flapping and causing instability in the stack ring, to disable the port, enter the switch stack-member-number stack port port-number disable privileged EXEC command. To reenable the port, enter the switch stack-member-number stack port port-number enable command.

Note
Be careful when using the switch stack-member-number stack port port-number disable command. When you disable the stack port, the stack operates at half bandwidth.

A stack is in the full-ring state when all members are connected through the stack ports and are in the ready state.

The stack is in the partial-ring state when the following occurs:

• All members are connected through their stack ports but some are not in the ready state.
Some members are not connected through the stack ports.

**SUMMARY STEPS**

1. `switch stack-member-number stack port port-number disable`
2. `switch stack-member-number stack port port-number enable`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>switch stack-member-number stack port port-number disable</code></td>
<td>Disables the specified stack port.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch 2 stack port 1 disable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>switch stack-member-number stack port port-number enable</code></td>
<td>Reenables the stack port.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>switch 2 stack port 1 enable</code></td>
<td></td>
</tr>
</tbody>
</table>

When you disable a stack port and the stack is in the full-ring state, you can disable only one stack port. This message appears:

`Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]`

When you disable a stack port and the stack is in the partial-ring state, you cannot disable the port. This message appears:

`Disabling stack port not allowed with current stack configuration.`

**Reenabling a Stack Port While Another Member Starts**

Stack Port 1 on Switch 1 is connected to Port 2 on Switch 4. If Port 1 is flapping, you can disable Port 1 with the `switch 1 stack port 1 disable` privileged EXEC command. While Port 1 on Switch 1 is disabled and Switch 1 is still powered on, follow these steps to reenable a stack port:

**Step 1** Disconnect the stack cable between Port 1 on Switch 1 and Port 2 on Switch 4.
**Step 2** Remove Switch 4 from the stack.
**Step 3** Add a switch to replace Switch 4 and assign it switch-number 4.
**Step 4** Reconnect the cable between Port 1 on Switch 1 and Port 2 on Switch 4 (the replacement switch).
**Step 5** Reenable the link between the switches. Enter the `switch 1 stack port 1 enable` privileged EXEC command to enable Port 1 on Switch 1.
**Step 6** Power on Switch 4.
Powering on Switch 4 before enabling the Port 1 on Switch 1 might cause one of the switches to reload. If Switch 4 is powered on first, you might need to enter the `switch 1 stack port 1 enable` and the `switch 4 stack port 2 enable` privileged EXEC commands to bring up the link.

### Monitoring the Switch Stack

**Table 6: Commands for Displaying Stack Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show switch</code></td>
<td>Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.</td>
</tr>
<tr>
<td><code>show switch stack-member-number</code></td>
<td>Displays information about a specific member.</td>
</tr>
<tr>
<td><code>show switch detail</code></td>
<td>Displays detailed information about the stack.</td>
</tr>
<tr>
<td><code>show switch neighbors</code></td>
<td>Displays the stack neighbors.</td>
</tr>
<tr>
<td><code>show switch stack-ports [summary]</code></td>
<td>Displays port information for the stack.</td>
</tr>
<tr>
<td><code>show redundancy</code></td>
<td>Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, the uptime in the current state and so on.</td>
</tr>
<tr>
<td><code>show redundancy state</code></td>
<td>Displays all the redundancy states of the active and standby switches.</td>
</tr>
</tbody>
</table>
Configuration Examples for Switch Stacks

Switch Stack Configuration Scenarios

Most of these switch stack configuration scenarios assume that at least two switch are connected through their StackWise-160 ports.

Table 7: Configuration Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active switch election specifically determined by existing active switches</td>
<td>Connect two powered-on switch stacks through the StackWise-160 ports. Only one of the two active switches becomes the new active switch.</td>
</tr>
</tbody>
</table>
| Active switch election specifically determined by the stack member priority value | 1 Connect two switches through their StackWise-160 ports. The stack member with the higher priority value is elected active switch.  
2 Use the `switch stack-member-number priority new-priority-number global configuration command to set one stack member with a higher member priority value.  
3 Restart both stack members at the same time.                                                                 |
| Active switch election specifically determined by the configuration file | Assuming that both stack members have the same priority value:  
1 Make sure that one stack member has a default configuration and that the other stack member has a saved (nondefault) configuration file.  
2 Restart both stack members at the same time. The stack member with the saved configuration file is elected active switch. |
<p>| Active switch election specifically determined by the MAC address       | Assuming that both stack members have the same priority value, configuration file, and feature set, restart both stack members at the same time. The stack member with the lower MAC address is elected active switch. |</p>
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member number conflict</td>
<td>The stack member with the higher priority value retains its stack member number. The other stack member has a new stack member number.</td>
</tr>
<tr>
<td></td>
<td>Assuming that one stack member has a higher priority value than the other stack member:</td>
</tr>
<tr>
<td></td>
<td>1 Ensure that both stack members have the same stack member number. If necessary, use the switch current-stack-member-number renumber new-stack-member-number global configuration command.</td>
</tr>
<tr>
<td></td>
<td>2 Restart both stack members at the same time.</td>
</tr>
<tr>
<td>Add a stack member</td>
<td>The active switch is retained. The new switch is added to the switch stack.</td>
</tr>
<tr>
<td></td>
<td>1 Power off the new switch.</td>
</tr>
<tr>
<td></td>
<td>2 Through their StackWise-160 ports, connect the new switch to a powered-on switch stack.</td>
</tr>
<tr>
<td></td>
<td>3 Power on the new switch.</td>
</tr>
<tr>
<td>Active switch failure</td>
<td>One of the remaining stack members becomes the new stack master. All other stack members in the stack remain as stack members and do not reboot.</td>
</tr>
<tr>
<td></td>
<td>Remove (or power off) the active switch.</td>
</tr>
<tr>
<td>Add more than nine stack members</td>
<td>Two switch become active switches. One active switch has nine stack members. The other active switch remains as a standalone switch.</td>
</tr>
<tr>
<td></td>
<td>Use the Mode button and port LEDs on the switch to identify which switch are active switches and which switch belong to each active switch.</td>
</tr>
<tr>
<td></td>
<td>1 Through their StackWise-160 ports, connect ten switch.</td>
</tr>
<tr>
<td></td>
<td>2 Power on all switch.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Assigning a Stack Member Number](#), on page 36
- [Changes to Switch Stack Membership](#), on page 23
- [Stack Member Numbers](#), on page 24
- [Switch Stack Configuration Files](#), on page 27
Enabling the Persistent MAC Address Feature: Example

This example shows how to configure the persistent MAC address feature for a 7-minute time delay and to verify the configuration:

```
Switch(config)# stack-mac persistent timer 7
WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack MAC after a master switchover until the MAC
WARNING: persistency timer expires. During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain. If it does,
WARNING: user traffic may be blackholed.
Switch(config)# end
Switch# show switch
Switch/Stack Mac Address : 0016.4727.a900
Mac persistency wait time: 7 mins
```

```
Switch# Role Mac Address Priority Version State
*1 Active 0016.4727.a900 1 P2B Ready
```

Related Topics

- Enabling the Persistent MAC Address Feature, on page 34
- Persistent MAC Address on the Switch Stack, on page 26

Provisioning a New Member for a Switch Stack: Example

This example shows how to provision a switch with a stack member number of 2 for the switch stack. The `show running-config` command output shows the interfaces associated with the provisioned switch:

```
Switch(config)# switch 2 provision
Switch(config)# end
Switch# show running-config | include switch 2
! interface GigabitEthernet2/0/1
! interface GigabitEthernet2/0/2
! interface GigabitEthernet2/0/3
<output truncated>
```

Related Topics

- Removing Provisioned Switch Information, on page 39
- Offline Configuration to Provision a Stack Member, on page 28

show switch stack-ports summary Command Output: Example

Only Port 1 on stack member 2 is disabled.

```
Switch# show switch stack-ports summary
Switch/# Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
-------- ------ -------- -------- ---- -------- ----------
1/1 OK 3 50 cm Yes Yes Yes 1 No
```
Table 8: show switch stack-ports summary Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch#/Port#</td>
<td>Member number and its stack port number.</td>
</tr>
</tbody>
</table>
| Stack Port Status | Status of the stack port.  
  • Absent—No cable is detected on the stack port.  
  • Down—A cable is detected, but either no connected neighbor is up, or the stack port is disabled.  
  • OK—A cable is detected, and the connected neighbor is up. |
| Neighbor       | Switch number of the active member at the other end of the stack cable.     |
| Cable Length   | Valid lengths are 50 cm, 1 m, or 3 m. If the switch cannot detect the cable length, the value is no cable. The cable might not be connected, or the link might be unreliable. |
| Link OK        | Whether the stack cable is connected and functional. There may or may not be a neighbor connected on the other end.  
  The link partner is a stack port on a neighbor switch.  
  • No—There is no stack cable connected to this port or the stack cable is not functional.  
  • Yes—There is a functional stack cable connected to this port. |
| Link Active    | Whether a neighbor is connected on the other end of the stack cable.  
  • No—No neighbor is detected on the other end. The port cannot send traffic over this link.  
  • Yes—A neighbor is detected on the other end. The port can send traffic over this link. |
### Field | Description
--- | ---
Sync OK | Whether the link partner sends valid protocol messages to the stack port.
  - No—The link partner does not send valid protocol messages to the stack port.
  - Yes—The link partner sends valid protocol messages to the port.

# Changes to LinkOK | The relative stability of the link. If a large number of changes occur in a short period of time, link flapping can occur.

In Loopback | Whether a stack cable is attached to a stack port on the member.
  - No—At least one stack port on the member has an attached stack cable.
  - Yes—None of the stack ports on the member has an attached stack cable.

---

### Software Loopback: Examples

In a stack with three members, stack cables connect all the members:

```
Switch# show switch stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor</th>
<th>Cable Length</th>
<th>Link OK</th>
<th>Link Active</th>
<th>Sync OK</th>
<th>#Changes to LinkOK</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>OK</td>
<td>3</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>1/2</td>
<td>OK</td>
<td>2</td>
<td>3 m</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/1</td>
<td>OK</td>
<td>1</td>
<td>3 m</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/2</td>
<td>OK</td>
<td>3</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/1</td>
<td>OK</td>
<td>2</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/2</td>
<td>OK</td>
<td>1</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

If you disconnect the stack cable from Port 1 on Switch 1, these messages appear:

```
01:09:55: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 3 has changed to state DOWN
01:09:56: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state DOWN
```

```
Switch# show switch stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor</th>
<th>Cable Length</th>
<th>Link OK</th>
<th>Link Active</th>
<th>Sync OK</th>
<th>#Changes to LinkOK</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Absent</td>
<td>None</td>
<td>No cable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>1/2</td>
<td>OK</td>
<td>2</td>
<td>3 m</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/1</td>
<td>OK</td>
<td>1</td>
<td>3 m</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/2</td>
<td>OK</td>
<td>3</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/1</td>
<td>OK</td>
<td>2</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/2</td>
<td>Down</td>
<td>None</td>
<td>50 cm</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>
If you disconnect the stack cable from Port 2 on Switch 1, the stack splits.

Switch 2 and Switch 3 are now in a two-member stack connected through stack cables:

```
Switch# show sw stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor Status</th>
<th>Cable Length</th>
<th>OK</th>
<th>Active</th>
<th>Sync</th>
<th>#Changes</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>Down</td>
<td>None</td>
<td>3 m</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/2</td>
<td>OK</td>
<td>3</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/1</td>
<td>OK</td>
<td>2</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>3/2</td>
<td>Down</td>
<td>None</td>
<td>50 cm</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

Switch 1 is a standalone switch:

```
Switch# show switch stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor Status</th>
<th>Cable Length</th>
<th>OK</th>
<th>Active</th>
<th>Sync</th>
<th>#Changes</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Absent</td>
<td>None</td>
<td>No cable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>1/2</td>
<td>Absent</td>
<td>None</td>
<td>No cable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Software Loopback with Connected Stack Cables: Examples

- On Port 1 on Switch 1, the port status is Down, and a cable is connected.
  
On Port 2 on Switch 1, the port status is Absent, and no cable is connected.

```
Switch# show switch stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor Status</th>
<th>Cable Length</th>
<th>OK</th>
<th>Active</th>
<th>Sync</th>
<th>#Changes</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Down</td>
<td>None</td>
<td>50 cm</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>1/2</td>
<td>Absent</td>
<td>None</td>
<td>No cable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

- In a physical loopback, a cable connects both stack ports on a switch. You can use this configuration to test
  
  * Cables on a switch that is running properly
  * Stack ports with a cable that works properly

```
Switch# show switch stack-ports summary
```

<table>
<thead>
<tr>
<th>Sw#/Port#</th>
<th>Port Status</th>
<th>Neighbor Status</th>
<th>Cable Length</th>
<th>OK</th>
<th>Active</th>
<th>Sync</th>
<th>#Changes</th>
<th>In Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>OK</td>
<td>2</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2/2</td>
<td>OK</td>
<td>2</td>
<td>50 cm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

The port status shows that
  
  * Switch 2 is a standalone switch.
  * The ports can send and receive traffic.
Software Loopback with no Connected Stack Cable: Example

Switch# show switch stack-ports summary

Switch# show switch stack-ports summary

Finding a Disconnected Stack Cable: Example

Stack cables connect all stack members. Port 2 on Switch 1 connects to Port 1 on Switch 2.

This is the port status for the members:

Switch# show switch stack-ports summary

If you disconnect the cable from Port 2 on Switch 1, these messages appear:

%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state DOWN
%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DOWN

This is now the port status:

If only one end of the cable connects to a stack port, Port 1 on Switch 2.

- The Stack Port Status value for Port 2 on Switch 1 is Absent, and the value for Port 1 on Switch 2 is Down.

- The Cable Length value is No cable.

Diagnosing the problem:

- Verify the cable connection for Port 2 on Switch 1.

- Port 2 on Switch 1 has a port or cable problem if
  - The In Loopback value is Yes.
or

- The Link OK, Link Active, or Sync OK value is No.

Fixing a Bad Connection Between Stack Ports: Example

Stack cables connect all members. Port 2 on Switch 1 connects to Port 1 on Switch 2.

This is the port status:

```
Switch# show switch stack-ports summary
Switch# Sw#/Port# Port Neighbor Cable Link Link Sync #Changes In
Status Length OK Active OK To LinkOK Loopback
-------- ------ -------- -------- ---- ------ ---- --------- --------
1/1 OK 2 50 cm Yes Yes Yes 1 No
1/2 Down None 50 cm No No No 2 No
2/1 Down None 50 cm No No No 2 No
2/2 OK 1 50 cm Yes Yes Yes 1 No
```

Diagnosing the problem:

- The Stack Port Status value is Down.
- Link OK, Link Active, and Sync OK values are No.
- The Cable Length value is 50 cm. The switch detects and correctly identifies the cable.

The connection between Port 2 on Switch 1 and Port 1 on Switch 2 is unreliable on at least one of the connector pins.

Additional References for Switch Stacks

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabling and powering on a switch stack.</td>
<td>Catalyst 3650 Switch Hardware Installation Guide</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>
### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and , use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

---

### Feature History and Information for Switch Stacks

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 4

Configuring Cisco NSF with SSO

- Finding Feature Information, page 55
- Prerequisites for NSF with SSO, page 55
- Restrictions for NSF with SSO, page 56
- Information About NSF with SSO, page 56
- How to Configure Cisco NSF with SSO, page 61
- Additional References for NSF with SSO, page 68
- Feature History and Information for NSF with SSO, page 69

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for NSF with SSO

The following are prerequisites and considerations for configuring NSF with SSO.

- Use of the routing protocols requires the IP Services license level. EIGRP-stub and OSPF for routed access are supported on IP Base license level.

- BGP support in NSF requires that neighbor networking devices be NSF-aware; that is, the devices must have the graceful restart capability and advertise that capability in their OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have graceful restart capability, it does not establish an NSF-capable session with that neighbor. All other neighbors
that have graceful restart capability continue to have NSF-capable sessions with this NSF-capable networking device.

• OSPF support in NSF requires that all neighbor networking devices be NSF-aware. If an NSF-capable router discovers that it has non-NSF-aware neighbors on a particular network segment, it disables NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware routers continue to provide NSF capabilities.

Restrictions for NSF with SSO

The following are restrictions for configuring NSF with SSO:

• NSF capability is supported for IPv4 routing protocols only. NSF capability is not supported for IPv6 routing protocols.

• NSF does not support IP Multicast Routing, as it is not SSO-aware.

• NSF is not supported if the IOS-XE software is running in the LAN Base mode.

• For NSF operation, you must have SSO configured on the device.

• NSF with SSO supports IP Version 4 traffic and protocols only; NSF with SSO does not support IPv6 traffic.

• All Layer 3 neighboring devices must be NSF Helper or NSF-capable to support graceful restart capability.

• For IETF, all neighboring devices must be running an NSF-aware software image.

Information About NSF with SSO

Overview of NSF with SSO

The switch supports fault resistance by allowing a standby switch to take over if the active switch becomes unavailable. Cisco nonstop forwarding (NSF) works with stateful switchover (SSO) to minimize the amount of time a network is unavailable.

NSF provides these benefits:

• Improved network availability—NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.

• Overall network stability—Network stability may be improved with the reduction in the number of route flaps, which were created when routers in the network failed and lost their routing tables.

• Neighboring routers do not detect a link flap—Because the interfaces remain up during a switchover, neighboring routers do not detect a link flap (the link does not go down and come back up).

• Prevents routing flaps—Because SSO continues forwarding network traffic during a switchover, routing flaps are avoided.

• Maintains user sessions established prior to the switchover.
SSO Operation

When a standby switch runs in SSO mode, the standby switch starts up in a fully-initialized state and synchronizes with the persistent configuration and the running configuration of the active switch. It subsequently maintains the state on the protocols listed below, and all changes in hardware and software states for features that support stateful switchover are kept in synchronization. Consequently, it offers minimum interruption to Layer 2 sessions in a redundant active switch configuration.

If the active switch fails, the standby switch becomes the active switch. This new active switch uses existing Layer 2 switching information to continue forwarding traffic. Layer 3 forwarding will be delayed until the routing tables have been repopulated in the newly active switch.

---

**Note**

SSO is not supported if the IOS-XE software is running the LAN Base license level.

The state of these features is preserved between both the active and standby switches:

- 802.3
- 802.3u
- 802.3x (Flow Control)
- 802.3ab (GE)
- 802.3z (Gigabit Ethernet including CWDM)
- 802.3ad (LACP)
- 802.1p (Layer 2 QoS)
- 802.1q
- 802.1X (Authentication)
- 802.1D (Spanning Tree Protocol)
- 802.3af (Inline power)
- PAgP
- VTP
- Dynamic ARP Inspection
- DHCP snooping
- IP source guard
- IGMP snooping (versions 1 and 2)
- DTP (802.1q and ISL)
- MST
- PVST+
- Rapid-PVST
- PortFast/UpLinkFast/BackboneFast
SSO is compatible with the following list of features. However, the protocol database for these features is not synchronized between the standby and active switches:

- 802.1Q tunneling with Layer 2 Protocol Tunneling (L2PT)
- Baby giants
- Jumbo frame support
- CDP
- Flood blocking
- UDLD
- SPAN/RSPAN
- NetFlow

All Layer 3 protocols on a switch are learned on the standby switch if SSO is enabled.

### NSF Operation

Cisco IOS Nonstop Forwarding (NSF) always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic. NSF is supported by the BGP, OSPF, and EIGRP routing protocols and is supported by Cisco Express Forwarding (CEF) for forwarding. The routing protocols have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. After the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF then updates the hardware with the new FIB information.

If the active switch is configured for BGP (with the graceful-restart command), OSPF, or EIGRP routing protocols, routing updates are automatically sent during the active switch election.

The switch supports NSF-awareness and NSF-capability for the BGP, OSPF, and EIGRP protocols in IP Services license level and NSF-awareness for the EIGRP-stub in IP Base license level.

NSF has two primary components:

- NSF-awareness
  
  A networking device is NSF-aware if it is running NSF-compatible software. If neighboring router devices detect that an NSF router can still forward packets when an active switch election happens, this capability is referred to as NSF-awareness. Cisco IOS enhancements to the Layer 3 routing protocols...
(BGP, OSPF, and EIGRP) are designed to prevent route-flapping so that the CEF routing table does not time out or the NSF router does not drop routes. An NSF-aware router helps to send routing protocol information to the neighboring NSF router. NSF-awareness is enabled by default for EIGRP-stub, EIGRP, and OSPF protocols. NSF-awareness is disabled by default for BGP.

• NSF-capability

A device is NSF-capable if it has been configured to support NSF; it rebuilds routing information from NSF-aware or NSF-capable neighbors. NSF works with SSO to minimize the amount of time that a Layer 3 network is unavailable following an active switch election by continuing to forward IP packets. Reconvergence of Layer 3 routing protocols (BGP, OSPFv2, and EIGRP) is transparent to the user and happens automatically in the background. The routing protocols recover routing information from neighbor devices and rebuild the Cisco Express Forwarding (CEF) table.

Cisco Express Forwarding

A key element of Cisco IOS Nonstop Forwarding (NSF) is packet forwarding. In a Cisco networking device, packet forwarding is provided by Cisco Express Forwarding (CEF). CEF maintains the FIB and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active supervisor switch synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby switch. Upon switchover, the standby switch initially has FIB and adjacency databases that are mirror images of those that were current on the active switch. CEF keeps the forwarding engine on the standby switch current with changes that are sent to it by CEF on the active switch. The forwarding engine can continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates cause prefix-by-prefix updates to CEF, which it uses to update the FIB and adjacency databases. Existing and new entries receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the forwarding engine during convergence. The switch signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

BGP Operation

When an NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a statement that the NSF-capable device has “graceful” restart capability. Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable router and its BGP peers need to exchange the graceful restart capability in their OPEN messages at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be capable of a graceful restart.

If the BGP session is lost during the active switch switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable router as stale; however, it continues to use these routes to make forwarding
decisions for a set period of time. This functionality prevents packets from being lost while the newly active
switch is waiting for convergence of the routing information with the BGP peers.

After an active switch switchover occurs, the NSF-capable router reestablishes the session with the BGP peer.
In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable router
as having restarted.

At this point, the routing information is exchanged between the two BGP peers. After this exchange is complete,
the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding
information. The NSF-aware device uses the network information to remove stale routes from its BGP table;
the BGP protocol then is fully converged.

If a BGP peer does not support the graceful restart capability, it ignores the graceful restart capability in an
OPEN message but establishes a BGP session with the NSF-capable device. This function allows interoperability
with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware
BGP peers is not capable of a graceful restart.

Note
BGP support in NSF requires that neighbor networking devices be NSF-aware; that is, the devices must
have the graceful restart capability and advertise that capability in their OPEN message during session
establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have graceful
restart capability, it does not establish an NSF-capable session with that neighbor. All other neighbors
that have graceful restart capability continue to have NSF-capable sessions with this NSF-capable
networking device.

OSPF Operation

When an OSPF NSF-capable router performs an active switch switchover, it must perform the following tasks
in order to resynchronize its link state database with its OSPF neighbors:

- Relearn the available OSPF neighbors on the network without causing a reset of the neighbor relationship
- Reacquire the contents of the link state database for the network

As quickly as possible after an active switch switchover, the NSF-capable router sends an OSPF NSF signal
to neighboring NSF-aware devices. Neighbor networking devices recognize this signal as an indicator that
the neighbor relationship with this router should not be reset. As the NSF-capable router receives signals from
other routers on the network, it can begin to rebuild its neighbor list.

After neighbor relationships are reestablished, the NSF-capable router begins to resynchronize its database
with all of its NSF-aware neighbors. At this point, the routing information is exchanged between the OSPF
neighbors. Once this exchange is complete, the NSF-capable device uses the routing information to remove
stale routes, update the RIB, and update the FIB with the new forwarding information. The OSPF protocols
are then fully converged.

Note
OSPF support in NSF requires that all neighbor networking devices be NSF-aware. If an NSF-capable
router discovers that it has non-NSF-aware neighbors on a particular network segment, it disables NSF
capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware
routers continue to provide NSF capabilities.
EIGRP Operation

When an EIGRP NSF-capable router initially re-boots after an NSF restart, it has no neighbor and its topology table is empty. The router is notified by the standby (now active) switch when it needs to bring up the interfaces, reacquire neighbors, and rebuild the topology and routing tables. The restarting router and its peers must accomplish these tasks without interrupting the data traffic directed toward the restarting router. EIGRP peer routers maintain the routes learned from the restarting router and continue forwarding traffic through the NSF restart process.

To prevent an adjacency reset by the neighbors, the restarting router uses a new Restart (RS) bit in the EIGRP packet header to indicate a restart. The RS bit is set in the hello packets and in the initial INIT update packets during the NSF restart period. The RS bit in the hello packets allows the neighbors to be quickly notified of the NSF restart. Without seeing the RS bit, the neighbor can only detect an adjacency reset by receiving an INIT update or by the expiration of the hello hold timer. Without the RS bit, a neighbor does not know if the adjacency reset should be handled using NSF or the normal startup method.

When the neighbor receives the restart indication, either by receiving the hello packet or the INIT packet, it recognizes the restarting peer in its peer list and maintains the adjacency with the restarting router. The neighbor then sends it topology table to the restarting router with the RS bit set in the first update packet indicating that it is NSF-aware and is helping out the restarting router. The neighbor does not set the RS bit in their hello packets, unless it is also a NSF restarting neighbor.

Note

A router may be NSF-aware but may not be helping the NSF restarting neighbor because booting from a cold start.

If at least one of the peer routers is NSF-aware, the restarting router would then receive updates and rebuild its database. The restarting router must then find out if it had converged so that it can notify the routing information base (RIB). Each NSF-aware router is required to send an end of table (EOT) marker in the last update packet to indicate the end of the table content. The restarting router knows it has converged when it receives the EOT marker. The restarting router can then begin sending updates.

An NSF-aware peer would know when the restarting router had converged when it receives an EOT indication from the restarting router. The peer then scans its topology table to search for the routes with the restarted neighbor as the source. The peer compares the route timestamp with the restart event timestamp to determine if the route is still available. The peer then goes active to find alternate paths for the routes that are no longer available through the restarted router.

When the restarting router has received all EOT indications from its neighbors or when the NSF converge timer expires, EIGRP notifies the RIB of convergence. EIGRP waits for the RIB convergence signal and then floods its topology table to all awaiting NSF-aware peers.

How to Configure Cisco NSF with SSO

Configuring SSO

You must configure SSO in order to use NSF with any supported protocol.
SUMMARY STEPS

1. redundancy
2. mode sso
3. end
4. show running-config
5. show redundancy states

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# redundancy</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>mode sso</td>
<td>Configures SSO. When this command is entered, the standby switch is reloaded and begins to work in SSO mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-red)# mode sso</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-red)# end</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
<td>Verifies that SSO is enabled.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show redundancy states</td>
<td>Displays the operating redundancy mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# show redundancy states</td>
<td></td>
</tr>
</tbody>
</table>

Configuring SSO Example

This example shows how to configure the system for SSO and display the redundancy state:

```
Switch(config)# redundancy
Switch(config)# mode sso
Switch(config)# end
Switch# show redundancy states
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 5
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
```
Configuring CEF NSF

The CEF NSF feature operates by default while the networking device is running in SSO mode. No configuration is necessary.

Verifying CEF NSF

To verify CEF NSF, use the `show cef state` privileged EXEX command.

```
Switch# show cef state
CEF Status:
RP instance
common CEF enabled
IPv4 CEF Status:
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
universal per-destination load sharing algorithm, id DEA83012
IPv6 CEF Status:
CEF disabled/not running
dCEF disabled/not running
universal per-destination load sharing algorithm, id DEA83012
RRP state:
I am standby RRP: no
RF Peer Presence: yes
RF PeerComm reached: yes
RF Progression blocked: never
Redundancy mode: rpr(1)
CEF NSF sync: disabled/not running
CEF ISSU Status:
FIBHWIDB broker
No slots are ISSU capable.
FIBIDB broker
No slots are ISSU capable.
FIBHWIDB Subblock broker
No slots are ISSU capable.
FIBIDB Subblock broker
No slots are ISSU capable.
Adjacency update
No slots are ISSU capable.
IPv4 table broker
No slots are ISSU capable.
CEF push
No slots are ISSU capable.
```

Configuring BGP for NSF

You must configure BGP graceful restart on all peer devices participating in BGP NSF.
### SUMMARY STEPS

1. configure terminal
2. router bgp as-number
3. bgp graceful-restart

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# configure</td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 router bgp as-number</td>
<td>Enables a BGP routing process, which places the switch in switch</td>
</tr>
<tr>
<td>Example:</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# router</td>
<td></td>
</tr>
<tr>
<td>bgp 300</td>
<td></td>
</tr>
<tr>
<td>Step 3 bgp graceful-restart</td>
<td>Enables the BGP graceful restart capability, starting BGP NSF. If you</td>
</tr>
<tr>
<td>Example:</td>
<td>enter this command after the BGP session has been established, you</td>
</tr>
<tr>
<td>Switch(config)# bgp</td>
<td>must restart the session for the capability to be exchanged with the</td>
</tr>
<tr>
<td>graceful-restart</td>
<td>BGP neighbor. Use this command on the restarting switch and all of its</td>
</tr>
<tr>
<td>peers.</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying BGP NSF

To verify BGP NSF, you must check that BGP graceful restart is configured on the SSO-enabled networking device and on the neighbor devices. To verify, follow these steps:

#### Step 1

Verify that "bgp graceful-restart" appears in the BGP configuration of the SSO-enabled switch by entering the `show running-config` command:

Example:
```
Switch# show running-config
...  
router bgp 120
...  
bgp graceful-restart
neighbor 192.0.2.0 remote-as 300
...  
```
Step 2 Repeat Step 1 on each of the BGP neighbors.
Step 3 On the SSO device and the neighbor device, verify that the graceful restart function is shown as both advertised and received, and confirm the address families that have the graceful restart capability. If no address families are listed, BGP NSF does not occur either:

Example:
Switch# show ip bgp neighbors
BGP neighbor is 192.0.2.3, remote AS 1, internal link
BGP version 4, remote router ID 192.0.2.4
BGP state = Established, up for 00:02:38
Last read 00:00:38, last write 00:00:35, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0
Sent Rcvd
Opens: 1 1
Notifications: 0 0
Updates: 0 0
Keepalives: 4 4
Route Refresh: 0 0
Total: 5 5
Default minimum time between advertisement runs is 0 seconds
............................................................
(Remaining output deleted)

Configuring OSPF NSF

All peer devices participating in OSPF NSF must be made OSPF NSF-aware, which happens automatically when you install an NSF software image on the device.

SUMMARY STEPS

1. configure terminal
2. router ospf processID
3. nsf

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Cisco NSF with SSO

### Verifying OSPF NSF

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td><code>router ospf processID</code></td>
<td>Enables an OSPF routing process, which places the switch in router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# router ospf processID</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>nsf</code></td>
<td>Enables NSF operations for OSPF.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# nsf</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Step 1
Verify that ‘nsf’ appears in the OSPF configuration of the SSO-enabled device by entering the `show running-config` command:

**Example:**
```
Switch(config)# show running-config
route ospf 120
log-adjacency-changes
nsf
network 192.0.2.0 192.0.2.255 area 0
network 192.0.2.1 192.0.2.255 area 1
network 192.0.2.2 192.0.2.255 area 2
```

#### Step 2
Enter the `show ip ospf` command to verify that NSF is enabled on the device:

**Example:**
```
Switch show ip ospf
Routing Process "ospf 1" with ID 192.0.2.1
Start time: 00:02:07.532, Time elapsed: 00:39:05.052
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
transit capable is 0
External flood list length 0
IETF Non-Stop Forwarding enabled
restart-interval limit: 120 sec
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
Number of interfaces in this area is 3 (1 loopback)
Area has no authentication
SPF algorithm last executed 00:08:53.760 ago
SPF algorithm executed 2 times
Area ranges are
Number of LSA 3. Checksum Sum 0x025BE0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
```
Configuring EIGRP NSF

**SUMMARY STEPS**

1. `configure terminal`
2. `router eigrp as-number`
3. `nsf`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Enables an EIGRP routing process, which places the switch in router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>router eigrp as-number</strong>&lt;br&gt;Enables EIGRP NSF.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# router eigrp as-number</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>nsf</code>&lt;br&gt;Use this command on the &quot;restarting&quot; switch and all of its peers.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-router)# nsf</code></td>
</tr>
</tbody>
</table>

**Verifying EIGRP NSF**

**Step 1**

Verify that “nsf” appears in the EIGRP configuration of the SSO-enabled device by entering the `show running-config` command:

```bash
Switch show running-config
```

Example:
```
Switch show running-config
.
router eigrp 100
auto-summary
nsf
```
Step 2

Enter the `show ip protocols` command to verify that NSF is enabled on the device:

**Example:**

```
Switch# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.0.2.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 1
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
Loopback0
GigabitEthernet5/3
TenGigabitEthernet3/1
Routing Information Sources:
Gateway Distance Last Update
192.0.2.1 110 00:01:02
Distance: (default is 110)
Routing Protocol is "bgp 601"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Automatic route summarization is disabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.0.2.0 110 00:01:02
```

### Additional References for NSF with SSO

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errors/index.cgi">https://www.cisco.com/cgi-bin/Support/Errors/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and , use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for NSF with SSO

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>

Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)
| Cisco IOS XE 3.3SE | This feature was introduced. |
Configuring Wireless High Availability

- Finding Feature Information, page 71
- Information about High Availability, page 71
- Information About Redundancy, page 72
- Information about Access Point Stateful Switch Over, page 74
- Initiating Graceful Switchover, page 74
- Configuring EtherChannels for High Availability, page 74
- Configuring LACP, page 75
- Troubleshooting High Availability, page 76

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about High Availability

The high availability feature is enabled by default when the switches are connected using the stack cable and the Cisco StackWise-160 technology is enabled. You cannot disable it; however, you can initiate a manual graceful-switchover using the command line interface to use the high availability feature enabled in the switch.

In Cisco Wireless LAN Controllers, high availability is achieved with redundancy.

In Cisco Wireless LAN Controllers, redundancy is achieved in two ways—n+1 and AP SSO redundancy.
Information About Redundancy

In case of n+1 redundancy, access points are configured with primary, secondary, and tertiary controllers. When the primary controller fails, depending upon the number of access points managed by a controller, the access point fails over to the secondary controller. In case of AP SSO redundancy, once the primary controller is unavailable, the access points re-discovers the controller and reestablishes the CAPWAP tunnel with the secondary controller. However, all clients must disconnect and a re-authentication is performed to rejoin the controller.

You can configure primary, secondary, and tertiary controllers for a selected access point and a selected controller.

In an ideal high availability deployment, you can have access points connected to primary and secondary controllers and one controller can remain with out connection to any access points. This way the controller that does not have any access points can take over when a failure occurs and resume services of active controller.

Configuring Redundancy in Access Points

You must use the commands explained in this section to configure primary, secondary, or tertiary controllers for a selected access point.

Before You Begin

SUMMARY STEPS

1. conf t
2. ap capwap backup primary
3. ap capwap backup secondary
4. ap capwap backup tertiary

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>conf t</td>
<td>Configures the terminal</td>
</tr>
</tbody>
</table>
|  | Example:  
Controller # conf t | |
| Step 2 | ap capwap backup primary | Configures the primary controller for the selected access point. |
|  | Example:  
Controller # ap capwap backup primary  
WLAN-Controller-A | |
| Step 3 | ap capwap backup secondary | Configures the secondary controller for the selected access point. |
|  | Example:  
Controller # ap capwap backup secondary  
WLAN-Controller-B | |
## Configuring Heartbeat Messages

Hearbeat messages enable you to reduce the controller failure detection time. When a failure occurs, a switchover from active to hot standby happens after the controller waits for the heartbeat timer. If the controller does not function within the heartbeat time, then the standby takes over as the active controller. Ideally the access point generates three heartbeat messages within the timeout value specified, and when the controller does not respond within the timeout value, the standby controller takes over as active. You can specify the timeout value depending on your network. Ideally the timer value is not a higher value as some chaos will occur while performing a switchover. This section explains on how to configure heartbeat interval between the controller and the access points using a timeout value to reduce the controller failure detection time.

### Before You Begin

**SUMMARY STEPS**

1. `conf t`
2. `ap capwap timers heartbeat-timeout`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>conf t</code></td>
<td>Configures the terminal.</td>
</tr>
</tbody>
</table>

Example:

```
controller # conf t
```
### Step 2

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap capwap timers heartbeat-timeout</td>
<td>Configures the heartbeat interval between the controller and access points. The timeout value ranges from 1 to 30.</td>
</tr>
</tbody>
</table>

#### Example:

```
controller # ap capwap timers heartbeat-timeout
```

---

### Information about Access Point Stateful Switch Over

An Access Point Stateful Switch Over (AP SSO) implies that all the access point sessions are switched over state-fully and the user session information is maintained during a switchover, and access points continue to operate in network with no loss of sessions, providing improved network availability. The active switch in the stack is equipped to perform all network functions, including IP functions and routing information exchange. The switch supports 1000 access points and 12000 clients.

However, all the clients are de-authenticated and need to be re-associated with the new active switch except for the locally switched clients in FlexConnect mode when a switchover occurs.

Once a redundancy pair is formed while in a stack, high availability is enabled, which includes that access points continue to remain connected during an active-to-standby switchover.

#### Note

You can not disable AP SSO while in a switch stack once the switches form a redundant pair.

### Initiating Graceful Switchover

To perform a manual switchover and to use the high availability feature enabled in the switch, execute the `redundancy force-switchover` command. This command initiates a graceful switchover from the active to the standby switch.

```
Switch# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration ...
Preparing for switchover ...
Compressed configuration from 14977 bytes to 6592 bytes[OK]This will reload the active unit and force switchover to standby[confirm] : y
```

### Configuring EtherChannels for High Availability

The LAG, or an EtherChannel, bundles all the existing ports in both the standby and active units into a single logical port to provide an aggregate bandwidth of 60 Gbps. The creation of an EtherChannel enables protection against failures. The EtherChannels or LAGs created are used for link redundancy to ensure high availability of access points.
For more details on configuring EtherChannel, and Etherchannel modes, see the Layer 2 (Link Aggregation) Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

---

**Step 1**
Connect two switches that are in powered down state using the stack cable.

**Step 2**
Power up and perform a boot on both switches simultaneously or power and boot one switch. The switches boot up successfully, and form a high availability pair.

**Step 3**
Configure EtherChannel or LAG on the units.

**Step 4**
Use the `show etherchannel summary` command to view the status of the configured EtherChannel. On successful configuration, all the specified ports will be bundled in a single channel and listed in the command output of `show etherchannel summary`.

**Step 5**
Execute the `show ap uptime` command to verify the connected access points.

---

**Configuring LACP**

**SUMMARY STEPS**

1. `configure terminal`
2. `interface port-channel number`
3. `lacp max-bundle number`
4. `lacp port-priority number`
5. `switchport backup interface po2`
6. `end`
7. `show etherchannel summary`
8. `show interfaces switchport backup`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface port-channel number</td>
<td>Enters port-channel interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface Port-channel Po2</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>lacp max-bundle number</code></td>
<td>Defines the maximum number of active bundled LACP ports allowed in a port channel. The value ranges from 1 to 8.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# lacp max-bundle 6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>lacp port-priority number</code></td>
<td>Specifies port priority to be configured on the port using LACP. The value ranges from 0 to 65535.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# lacp port-priority 4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>switchport backup interface po2</code></td>
<td>Specifies an interface as the backup interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport backup interface Po2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exits the interface and configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>show etherchannel summary</code></td>
<td>Displays a summary of EtherChannel properties.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show etherchannel summary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>show interfaces switchport backup</code></td>
<td>Displays summary of backup EtherChannel properties.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show interfaces switchport backup</code></td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting High Availability**

**Access the Standby Console**

You can only access the console of the active switch in a stack. To access the standby switch, use the following commands.

**Before You Begin**

Use this functionality only under supervision of Cisco Support.
SUMMARY STEPS

1. configure terminal
2. service internal
3. redundancy
4. main-cpu
5. standby console enable
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>service internal</td>
<td>Enables Cisco IOS debug commands.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# service internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>redundancy</td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# redundancy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>main-cpu</td>
<td>Enters the redundancy main configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# main-cpu</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>standby console enable</td>
<td>Enables the standby console.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# standby console enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Before a Switchover

A switchover happens when the active switch fails; however, while performing a manual switchover, you can execute these commands to initiate a successful switchover:
SUMMARY STEPS

1. show redundancy states  
2. show switch detail  
3. show platform ses states  
4. show ap summary  
5. show capwap detail  
6. show dtls database-brief  
7. show power inline

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>show redundancy states</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show redundancy states</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show switch detail</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show switch detail</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show platform ses states</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show platform ses states</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show ap summary</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show ap summary</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show capwap detail</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show capwap detail</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show dtls database-brief</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show dtls database-brief</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show power inline</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show power inline</td>
</tr>
</tbody>
</table>
After a Switchover

This section defines the steps that you must perform to ensure that successful switchover from the active to standby switch is performed. On successful switchover of the standby switch as active, all access points connected to the active need to re-join the standby (then active) switch.

**SUMMARY STEPS**

1. show ap uptime
2. show wireless summary
3. show wcdb database all
4. show power inline

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify if the uptime of the access point after the switchover is large enough.</td>
</tr>
<tr>
<td>show ap uptime</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show ap uptime</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Display the clients connected in the active switch.</td>
</tr>
<tr>
<td>show wireless summary</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show wireless summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Display if the client has reached the uptime.</td>
</tr>
<tr>
<td>show wcdb database all</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show wcdb database all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Display the power over Ethernet power state.</td>
</tr>
<tr>
<td>show power inline</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show power inline</td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring the Switch Stack**

*Table 9: Commands for Displaying Stack Information*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show switch</td>
<td>Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.</td>
</tr>
</tbody>
</table>
### Command | Description
--- | ---
**show switch stack-member-number** | Displays information about a specific member.
**show switch detail** | Displays detailed information about the stack.
**show switch neighbors** | Displays the stack neighbors.
**show switch stack-ports [summary]** | Displays port information for the stack.
**show redundancy** | Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, the uptime in the current state and so on.
**show redundancy state** | Displays all the redundancy states of the active and standby switches.

### LACP Configuration: Example

This example shows how to configure LACP and to verify creation of the LACP bundle and the status:

```
Switch(config)# !
interface TenGigabitEthernet1/0/1
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
```
interface TenGigabitEthernet2/0/1
    switchport mode trunk
    channel-group 1 mode active
    lacp port-priority 10
    ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
    switchport mode trunk
    channel-group 1 mode active
    lacp port-priority 10
    ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
    switchport mode trunk
    channel-group 1 mode active
    lacp port-priority 10
    ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
    switchport mode trunk
    channel-group 1 mode active
    ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
    switchport mode trunk
    channel-group 1 mode active
    ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
    switchport mode trunk
    channel-group 1 mode active
    ip dhcp snooping trust
!
interface Vlan1
    no ip address
    ip igmp version 1
    shutdown
!
Switch# show etherchannel summary

Flags: D - down                  P - bundled in port-channel
       I - stand-alone               S - suspended
       H - Hot-standby (LACP only)  R - Layer3
       L - Layer2                   S - Layer2
       U - in use                    f - failed to allocate aggregator

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----------+----------------+-----------+-----------------------------------------------
1  Po1(SU)  LACP      Tel1/0/1(P) Tel1/0/2(P) Tel1/0/3(P)
       Tel1/0/4(H) Tel1/0/5(H) Tel1/0/6(H)
       Te2/0/1(P) Te2/0/2(P) Te2/0/3(P)
       Te2/0/4(H) Te2/0/5(H) Te2/0/6(H)

This example shows the switch backup interface pairs:

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
-----------------------------------------------
This example shows the summary of the EtherChannel configured in the switch:

Switch# show ethernet summary

Flags: D - down     P - bundled in port-channel
I - stand-alone    s - suspended
H - Hot-standby    L - Layer3
R - Layer2         S - Layer2
U - in use        f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 2
Number of aggregators: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>LACP</td>
<td>Te1/0/1(P) Te1/0/2(P) Te1/0/3(P) Te1/0/4(P) Te1/0/5(P) Te1/0/6(P)</td>
</tr>
<tr>
<td>2</td>
<td>Po2(SU)</td>
<td>LACP</td>
<td>Te2/0/1(P) Te2/0/2(P) Te2/0/3(P) Te2/0/4(P) Te2/0/5(P) Te2/0/6(P)</td>
</tr>
</tbody>
</table>

**Flex Link Configuration: Example**

This example shows how to configure flex link and to verify creation and the status of the created link:

Switch(config)# !
interface Port-channel1
description Ports 1-6 connected to NW-55-SW
switchport mode trunk
switchport backup interface Po2
switchport backup interface Po2 preemption mode forced
switchport backup interface Po2 preemption delay 1
ip dhcp snooping trust
!
interface Port-channel2
description Ports 7-12 connected to NW-55-SW
switchport mode trunk
ip dhcp snooping trust
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
no ip address
 negotiation auto
!
interface TenGigabitEthernet1/0/1
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
```
! interface TenGigabitEthernet1/0/5
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
  switchport mode trunk
  channel-group 2 mode on
  ip dhcp snooping trust
!
interface Vlan1
  no ip address

Switch# show etherchannel summary
Flags:  D = down         P = bundled in port-channel
        I = stand-alone  s = suspended
        H = Hot-standby (LACP only)
        R = Layer3      S = Layer2
        U = in use       f = failed to allocate aggregator
        M = not in use, minimum links not met
        u = unsuitable for bundling
        w = waiting to be aggregated
        d = default port

Number of channel-groups in use: 2
Number of aggregators: 2

Group   Port-channel  Protocol    Ports
--------+-------------------+-------------------+-----------------------------------------------
1       Po1(SU)       -     Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)  Te1/0/4(P)  Te1/0/5(P)  Te1/0/6(P)  
2       Po2(SU)       -     Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(D)  Te2/0/4(P)  Te2/0/5(P)  Te2/0/6(P)
```
Viewing Redundancy Switchover History (GUI)

**Step 1**
Click Monitor > Controller > Redundancy > States.
The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Displays the index number of the redundant unit.</td>
</tr>
<tr>
<td>Previous Active</td>
<td>Displays the Switches that was active before.</td>
</tr>
<tr>
<td>Current Active</td>
<td>Displays the Switches that is currently active.</td>
</tr>
<tr>
<td>Switch Over Time</td>
<td>Displays the system time when the switchover occurs.</td>
</tr>
<tr>
<td>Switch Over Reason</td>
<td>Displays the cause of the switchover.</td>
</tr>
</tbody>
</table>

**Step 2**
Click Apply.

Viewing Switchover States (GUI)

**Step 1**
Click Monitor > Controller > Redundancy > States.
The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My State</td>
<td>Shows the state of the active CPU Switch module. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Standby HOT</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td>Peer State</td>
<td>Displays the state of the peer (or standby) CPU Switch module. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Standby HOT</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the current state of the redundancy peer. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Simplex— Single CPU switch module</td>
</tr>
<tr>
<td></td>
<td>• Duplex— Two CPU switch modules</td>
</tr>
<tr>
<td>Unit ID</td>
<td>Displays the unit ID of the CPU switch module.</td>
</tr>
<tr>
<td>Redundancy Mode (Operational)</td>
<td>Displays the current operational redundancy mode supported on the unit.</td>
</tr>
<tr>
<td>Redundancy Mode (Configured)</td>
<td>Displays the current configured redundancy mode supported on the unit.</td>
</tr>
<tr>
<td>Redundancy State</td>
<td>Displays the current functioning redundancy state of the unit. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• SSP</td>
</tr>
<tr>
<td></td>
<td>• Not Redundant</td>
</tr>
<tr>
<td>Manual SWACT</td>
<td>Displays whether manual switchovers have been enabled without the force option.</td>
</tr>
<tr>
<td>Communications</td>
<td>Displays whether communications are up or down between the two CPU Switch modules.</td>
</tr>
<tr>
<td>Client Count</td>
<td>Displays the number of redundancy subsystems that are registered as RF clients.</td>
</tr>
<tr>
<td>Client Notification TMR</td>
<td>Displays, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.</td>
</tr>
<tr>
<td>Keep Alive TMR</td>
<td>Displays, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby CPU switch module.</td>
</tr>
<tr>
<td>Keep Alive Count</td>
<td>Displays the number of keep-alive messages sent without receiving a response from the standby CPU Switch module.</td>
</tr>
<tr>
<td>Keep Alive Threshold</td>
<td>Displays the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).</td>
</tr>
<tr>
<td>RF Debug Mask</td>
<td>Displays an internal mask used by the RF to keep track of which debug modes are on.</td>
</tr>
</tbody>
</table>

**Step 2**

Click **Apply**.
Viewing Switchover States (GUI)
INDEX

A
assigning information 36, 37, 38
  member number 36
  priority value 37
  provisioning a new member 38
auto-advise 30
auto-copy 30
auto-extract 30
auto-upgrade 30
automatic advise (auto-advise) in switch stacks 30
automatic copy (auto-copy) in switch stacks 30
automatic extraction (auto-extract) in switch stacks 30
automatic upgrades (auto-upgrade) in switch stacks 30
automatic upgrades with auto-upgrade 30

N
Network Assistant 32
  managing switch stacks 32

O
offline configuration 28, 38
  provisioned configuration, defined 28
  provisioned switch, defined 28
  provisioning a new member 38

P
partitioned 23
  priority value 37
  provisioned configuration, defined 28
  provisioned switch, defined 28
  provisioning a new member 38
  provisioning new members for a switch stack 28

R
removing a provisioned member 39
  replacing 27
  replacing a failed member 27

S
SDM 32
  switch stack consideration 32
  stack member 27, 36, 37, 38, 39
  configuring 36, 37
    member number 36
    priority value 37
    provisioning a new member 38
    removing a provisioned member 39
  managing switch stacks 32
  merged 23
  member number 36
  priority value 37
  provisioning a new member 38
  provisioning a new member 38

C
configuring 36, 37
  member number 36
  priority value 37

D
desktop template 32

M
MAC address of 34
  managing switch stacks 32
  manual upgrades with auto-advise 30
  member number 36
  merged 23

Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)
stack member (continued)
    replacing 27
stacks switch 27
    replacing a failed member 27
stacks, switch 28, 30, 34, 37, 38
    assigning information 37, 38
        priority value 37
        provisioning a new member 38
    auto-advise 30
    auto-extract 30
    auto-upgrade 30
    MAC address of 34
    offline configuration 28, 38
        provisioned configuration, defined 28
        provisioned switch, defined 28
        provisioning a new member 38
    version-mismatch (VM) mode 30
        automatic upgrades with auto-upgrade 30
        upgrades with auto-extract 30
stacks, switch version-mismatch (VM) mode 30
    manual upgrades with auto-advise 30
stacks, switch 23, 30, 36, 39
    assigning information 36
        member number 36
    auto-copy 30
    merged 23
    offline configuration 39
        removing a provisioned member 39
        partitioned 23
switch stack consideration 32

U

upgrades with auto-extract 30

V

version-mismatch (VM) mode 30
    automatic upgrades with auto-upgrade 30
    manual upgrades with auto-advise 30
    upgrades with auto-extract 30