CHAPTER 7

Managing Switch Stacks

This chapter provides the concepts and procedures to manage switch stacks.

Note The switch command reference has command syntax and usage information.

For other switch stack-related information, such as cabling the switches through their StackWise Plus ports and using the LEDs to display switch stack status, see the hardware installation guide.

Caution The Cisco Catalyst Blade Switch 3120 for HP does not support switch stacks with different types of blade switches as members. Combining the Cisco Catalyst Blade Switch 3120 for HP with other types of blade switches in a switch stack might cause the switch to work improperly or to fail.

Understanding Switch Stacks

A *switch stack* is a set of up to nine stacking-capable switches connected through their StackWise Plus ports.

One of the switches controls the operation of the stack and is called the *stack master*. The stack master and the other switches in the stack are all *stack members*. The stack members use the Cisco StackWise Plus technology to work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. The stack members can be in different enclosures.

The stack master is the single point of stack-wide management. From the stack master, you configure:

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

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 stack master. Every stack member is identified by its own *stack member number*.

All stack members are eligible to be stack masters. If the stack master becomes unavailable, the remaining stack members elect a new stack master from among themselves. The switch with the highest *stack member priority value* becomes the new stack master.

The system-level features supported on the stack master are supported on the entire switch stack. If a switch in the stack is running the IP base or IP services feature set and the cryptographic (that is, supporting encryption) universal software image, we recommend that this switch be the stack master. Encryption features are unavailable if the stack master is running the IP base or IP services feature set and the noncryptographic software image.

The stack master 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.

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

You can use these methods to manage switch stacks:

- Network Assistant (available on Cisco.com)
- Command-line interface (CLI) over a serial connection to the console port of any stack member or the Ethernet management port of a stack member
- A network management application through the Simple Network Management Protocol (SNMP)

  Use SNMP to manage network features across the switch stack that are defined by supported MIBs. The switch does not support MIBs to manage stacking-specific features such as stack membership and election.
- CiscoWorks network management software

To manage switch stacks, you should understand:

- These concepts on how switch stacks are formed:
  - Switch Stack Membership, page 7-3
  - Stack Master Election and Re-Election, page 7-6
- These concepts on how switch stacks and stack members are configured:
  - Switch Stack Bridge ID and Router MAC Address, page 7-8
  - Stack Member Numbers, page 7-8
  - Stack Member Priority Values, page 7-9
  - Switch Stack Offline Configuration, page 7-9
  - Hardware Compatibility and SDM Mismatch Mode in Switch Stacks, page 7-11
  - Switch Stack Software Compatibility Recommendations, page 7-12
  - Stack Protocol Version Compatibility, page 7-12
  - Major Version Number Incompatibility Among Switches, page 7-12
  - Minor Version Number Incompatibility Among Switches, page 7-12
  - Incompatible Software and Stack Member Image Upgrades, page 7-16
  - Switch Stack Configuration Files, page 7-16
  - Additional Considerations for System-Wide Configuration on Switch Stacks, page 7-17

Switch Stack Membership

A switch stack has up to nine stack members connected through their StackWise Plus ports. A switch stack always has one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another (Figure 7-1 on page 7-4 and Figure 7-2 on page 7-5) to create a switch stack containing two stack members, with one of them as the stack master. You can connect standalone switches to an existing switch stack (Figure 7-3 on page 7-6) to increase the 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 is using the same member number as the replaced switch. For information about the benefits of provisioning a switch stack, see the "Switch Stack Offline Configuration" section on page 7-9. For information about replacing a failed switch, see the "Troubleshooting" chapter in the hardware installation guide.

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

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 (64 Gb/s). 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.

- Adding powered-on switches (merging) causes the stack masters of the merging switch stacks to elect a stack master from among themselves. The re-elected stack master retains its role and configuration and so do its stack members. All remaining switches, including the former stack masters, reload and join the switch stack as stack members. They change their stack member numbers to the lowest available numbers and use the stack configuration of the re-elected stack master.
- 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 configuration 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. If you did not intend to partition the switch stack:
  a. Power off the switches in the newly created switch stacks.
  b. Reconnect them to the original switch stack through their StackWise Plus ports.
  c. Power on the switches.

For more information about cabling and powering switch stacks, see the "Switch Installation" chapter in the hardware installation guide.

Figure 7-1 Creating a Switch Stack from Two Standalone Switches in Two Enclosures

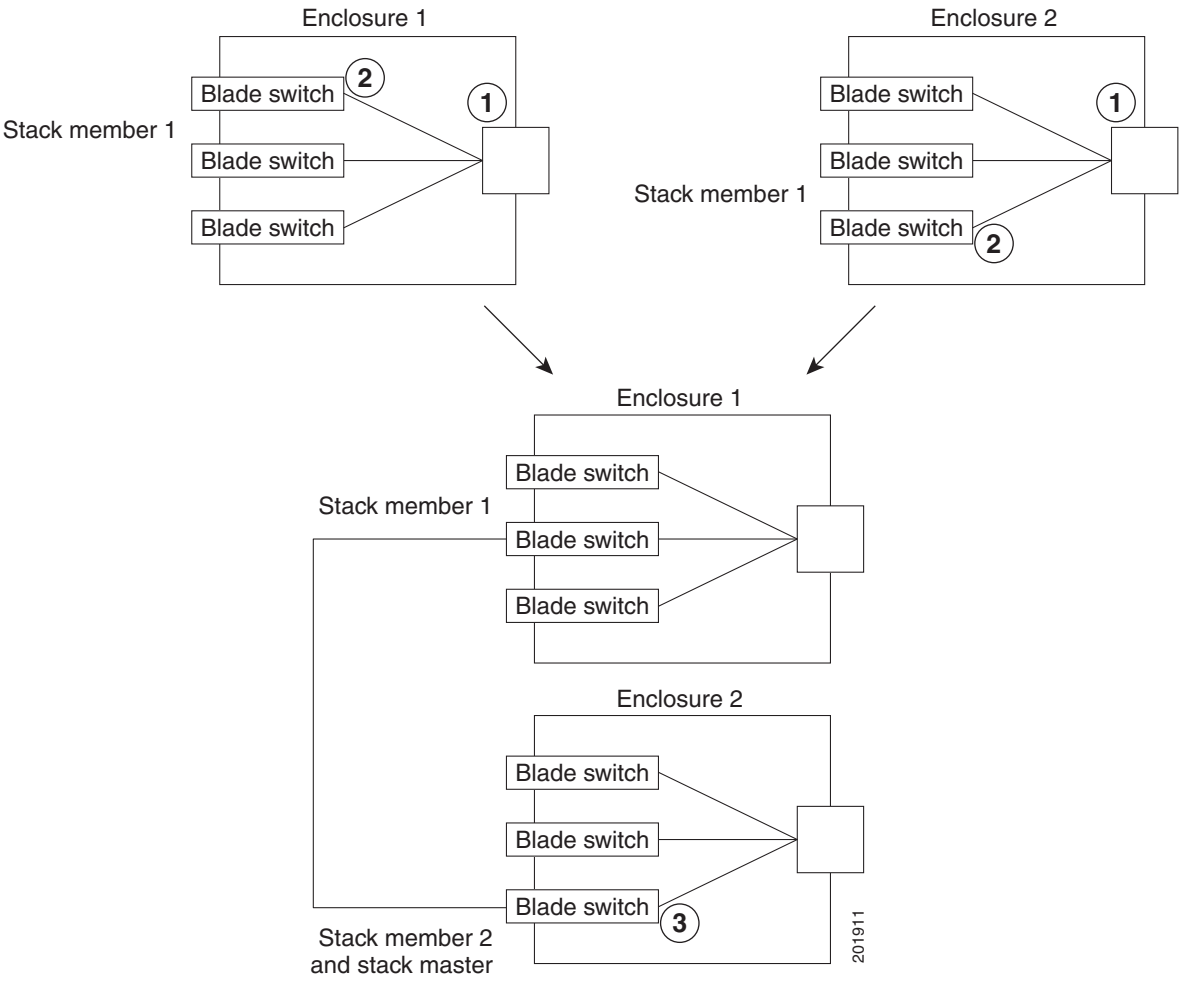


Figure 7-2 Creating a Switch Stack from Two Standalone Switches in the Same Enclosures

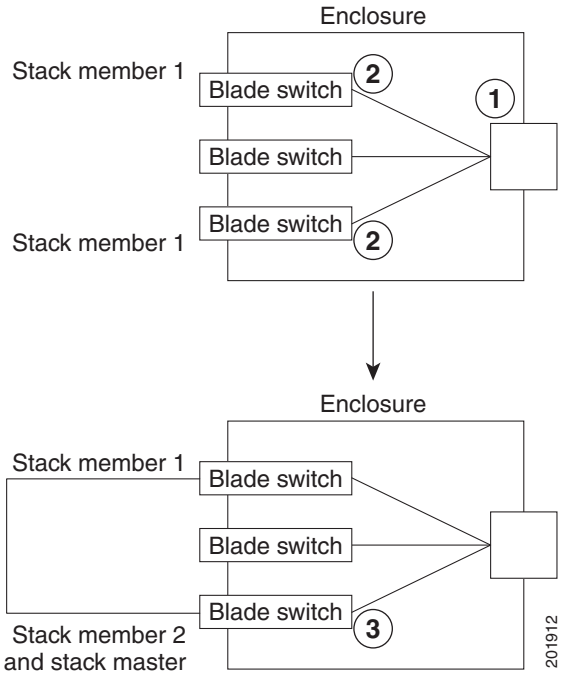
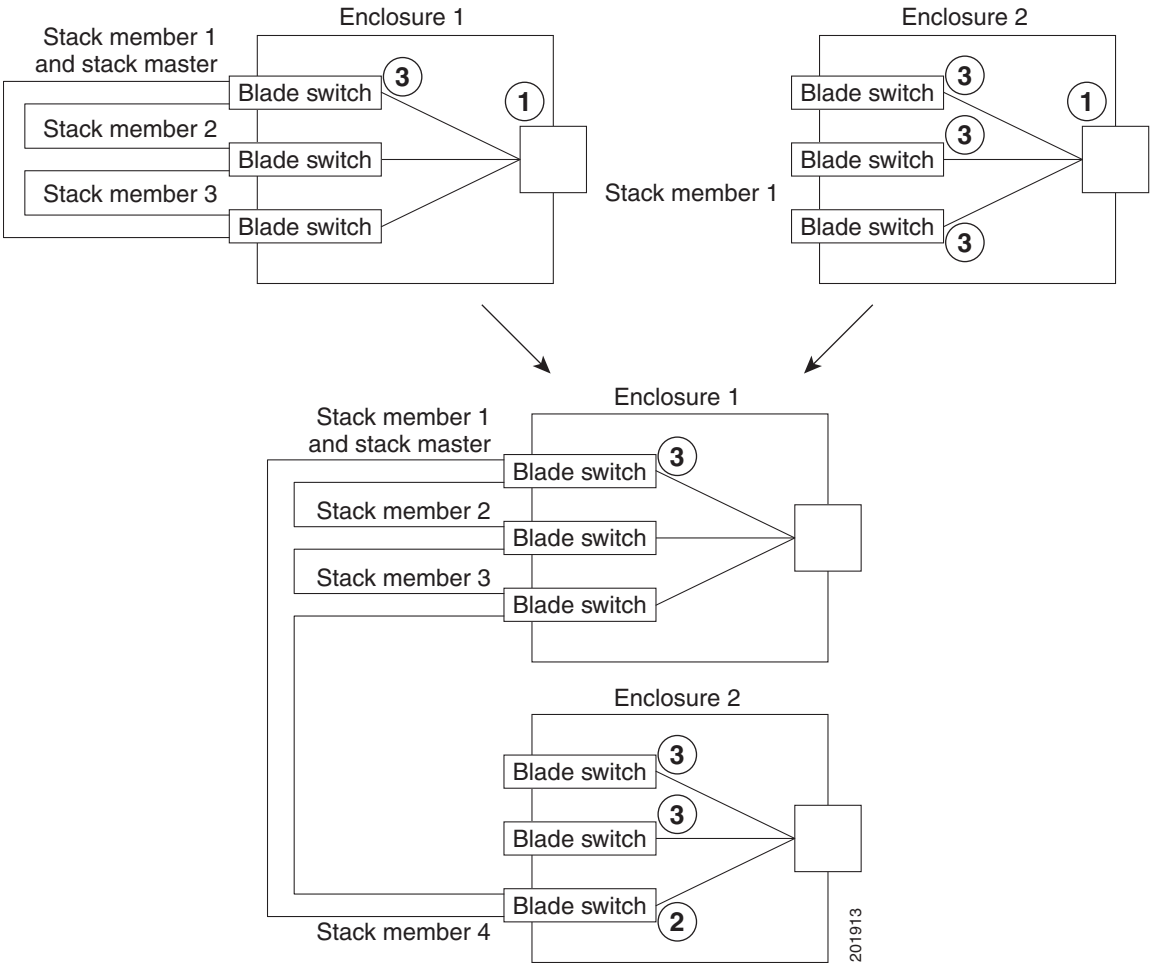


Figure 7-3 Adding a Standalone Switch to a Switch Stack



1	Onboard Administrator (OA)
2	Internal Ethernet management port that is not active
3	Active internal Ethernet management port on the stack master **Note** The internal Ethernet management ports on the stack members are disabled.

Stack Master Election and Re-Election

The stack master is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack master.
2. The switch with the highest stack member priority value.

Note We recommend assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch that is not using the default interface-level configuration.

4. The switch with the higher priority feature set and software image combination. These combinations are listed from highest to lowest priority:
   - IP services feature set and the cryptographic software image
   - IP services feature set and the noncryptographic software image
   - IP base feature set and the cryptographic software image
   - IP base feature set and the noncryptographic software image

   During the stack master switch election, differences in start-up times between the feature sets determine the stack master. The switch with the shorter start-up time becomes the stack master.

   For example, a switch running the IP services feature set and the cryptographic software image has a higher priority than the switch running the IP base feature set and the noncryptographic image, but the switch running the IP base feature set becomes the stack master because the other switch takes 10 seconds longer to start. To avoid this problem, upgrade the switch running the IP base feature set to same feature set and software image as the other switch, or manually start the master switch and wait at least 8 seconds before starting the new member switch that running the IP base feature set.
5. The switch with the lowest MAC address.

A stack master retains its role unless one of these events occurs:

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

In the events marked by an asterisk (*), the current stack master *might* be re-elected based on the listed factors.

When you power on or reset an entire switch stack, some stack members *might not* participate in the stack master election. Stack members that are powered on within the same 20-second time frame participate in the stack master election and have a chance to become the stack master. Stack members that are powered on after the 20-second time frame do not participate in this initial election and become stack members. All stack members participate in re-elections. For all powering considerations that affect stack-master elections, see the “Switch Installation” chapter in the hardware installation guide.

The new stack master 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 stack master election and reset.

After a new stack master is elected and the previous stack master becomes available, the previous stack master *does not* resume its role as stack master.

As described in the hardware installation guide, you can use the Master LED on the switch to see if the switch is the stack master.

Switch Stack Bridge ID and Router MAC Address

The bridge ID and router MAC address identify the switch stack in the network. When the switch stack initializes, the MAC address of the stack master determines the bridge ID and router MAC address.

If the stack master changes, the MAC address of the new stack master determines the new bridge ID and router MAC address. However, when the persistent MAC address feature is enabled, the stack MAC address changes in approximately 4 minutes. During this time period, if the previous stack master 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 a stack master. If the previous stack master does not rejoin the stack during this period, the switch stack takes the MAC address of the new stack master as the stack MAC address. See the "Enabling Persistent MAC Address" section on page 7-22 for more information.

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** user 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* global configuration 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. For more information, see the "Assigning a Stack Member Number" section on page 7-24. Another way to change the stack member number is by changing the SWITCH_NUMBER environment variable, as explained in the "Controlling Environment Variables" section on page 3-22.

  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. For more information about stack member numbers and configurations, see the "Switch Stack Configuration Files" section on page 7-16.

  You cannot use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration 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 switches that join the switch stack of a new stack master select the the lowest available numbers in the stack. For more information about merging switch stacks, see the "Switch Stack Membership" section on page 7-3.

Stack Member Priority Values

A higher priority value for a stack member increases its likelihood of being elected stack master 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** user EXEC command.

Note We recommend assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master.

You can change the priority value for a stack member by using the **switch** *stack-member-number* **priority** *new-priority-value* global configuration command. For more information, see the "Setting the Stack Member Priority Value" section on page 7-24. Another way to change the member priority value is by changing the SWITCH_PRIORITY environment variable, as explained in the "Controlling Environment Variables" section on page 3-22.

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

Switch Stack Offline Configuration

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 in advance 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. 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 (for example, as part of a VLAN), the switch stack accepts the configuration, and the information appears in the running configuration. The interface associated with the provisioned switch is not active, operates as if it is administratively shut down, and the **no shutdown** interface configuration command does not return it to active service. The interface associated with the provisioned switch does not appear in the display of the specific feature; for example, it does not appear in the **show vlan** user EXEC command output.

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.

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. Table 7-1 lists the events that occur when the switch stack compares the provisioned configuration with the provisioned switch.

Table 7-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch

Scenario		Result
The stack member numbers and the switch types match.	1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and 2. If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack.	The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack.
The stack member numbers match but the switch types do not match.	1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but 2. The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack.	The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
The stack member number is not found in the provisioned configuration.		The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
The stack member number of the provisioned switch is in conflict with an existing stack member.	The stack master assigns a new stack member number to the provisioned switch. The stack member numbers and the switch types match: 1. If the new stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and 2. If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack.	The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
	The stack member numbers match, but the switch types do not match: 1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but 2. The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack.	The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.

Table 7-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch (continued)

Scenario		Result
The stack member number of the provisioned switch is not found in the provisioned configuration.		The switch stack applies the default configuration to the provisioned switch and adds it to the stack.

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.

Note If the switch stack does not contain a provisioned configuration for a new switch, the switch joins the stack with the default interface configuration. The switch stack then adds to its running configuration a **switch** *stack-member-number* **provision** *type* global configuration command that matches the new switch.

For configuration information, see the "Provisioning a New Member for a Switch Stack" section on page 7-25.

Effects of Replacing a Provisioned Switch in a Switch Stack

When a provisioned switch in a switch stack fails, 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 described in the "Effects of Adding a Provisioned Switch to a Switch Stack" section on page 7-10.

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.

Hardware Compatibility and SDM Mismatch Mode in Switch Stacks

The switch supports only the desktop Switch Database Management (SDM) templates.

All stack members use the SDM template configured on the stack master.

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.

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

For more information about SDM templates and SDM-mismatch mode, see Chapter 8, "Configuring SDM Templates."

Switch Stack Software Compatibility Recommendations

To ensure complete compatibility between stack members, use the information in this section and also in the "Hardware Compatibility and SDM Mismatch Mode in Switch Stacks" section on page 7-11.

All stack members must run the same Cisco IOS software image and feature set to ensure compatibility between stack members. For example, all stack members should run the cryptographic universal software image and have the IP services feature set enabled for Cisco IOS Release 12.2(40)EX or later.

For more information, see the "Stack Protocol Version Compatibility" section on page 7-12.

Stack Protocol Version Compatibility

Each software image includes a *stack protocol version*. The stack protocol version has a *major* version number and a *minor* version number (for example 1.4, where 1 is the major version number and 4 is the minor version number). Both version numbers determine the level of compatibility among the stack members. You can display the stack protocol version by using the **show platform stack-manager all** privileged EXEC command.

Switches with the same Cisco IOS software version have the same stack protocol version. Such switches are fully compatible, and all features function properly across the switch stack. Switches with the same Cisco IOS software version as the stack master immediately join the switch stack.

If an incompatibility exists, the fully functional stack members generate a system message that describes the cause of the incompatibility on the specific stack members. The stack master sends the message to all stack members. For more information, see the "Major Version Number Incompatibility Among Switches" procedure on page 7-12 and the "Minor Version Number Incompatibility Among Switches" procedure on page 7-12.

Major Version Number Incompatibility Among Switches

Switches with different major Cisco IOS software versions usually have different stack protocol versions. Switches with different major version numbers are incompatible and cannot exist in the same switch stack.

Minor Version Number Incompatibility Among Switches

Switches with the same major version number but with a different minor version number are considered partially compatible. When connected to a switch stack, a partially compatible switch enters version-mismatch (VM) mode and cannot join the stack as a fully functioning member. The software detects the mismatched software and tries to upgrade (or downgrade) the switch in VM mode with the switch stack image or with a tar file image from the switch stack flash memory. The software uses the automatic upgrade (auto-upgrade) and the automatic advise (auto-advise) features. For more information, see the "Understanding Auto-Upgrade and Auto-Advise" section on page 7-13.

To see if there are switches in VM mode, use the **show switch** user EXEC command. The port LEDs on switches in VM mode stay off. Pressing the Mode button does not change the LED mode.

You can use the **boot auto-download-sw** global configuration command to specify a URL pathname for the master switch to use to get an image in case of version mismatch.

Understanding Auto-Upgrade and Auto-Advise

When the software detects mismatched software and tries to upgrade the switch in VM mode, two software processes are involved: automatic upgrade and automatic advise.

- The automatic upgrade (auto-upgrade) process includes an auto-copy process and an auto-extract process. By default, auto-upgrade is enabled (the **boot auto-copy-sw** global configuration command is enabled). You can disable auto-upgrade by using the **no boot auto-copy-sw** global configuration command on the stack master. You can check the status of auto-upgrade by using the **show boot** privileged EXEC command and by checking the *Auto upgrade* line in the display.
  - Auto-copy automatically copies the software image running on any stack member to the switch in VM mode to upgrade (auto-upgrade) it. Auto-copy occurs if auto-upgrade is enabled, if there is enough flash memory in the switch in VM mode, and if the software image running on the switch stack is suitable for the switch in VM mode.

  Note 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 switch in VM mode. In that case, the auto-extract process searches all switches in the stack, whether they are in VM mode or not, for the tar file needed to upgrade the switch stack or the switch in VM mode. The tar file can be in any flash file system in the switch stack (including the switch in VM mode). If a tar file suitable for the switch in VM mode is found, the process extracts the file and automatically upgrades that switch.

  The auto-upgrade (auto-copy and auto-extract) processes wait for a few minutes after the mismatched software is detected before starting.

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

Note Auto-upgrade performs the upgrade only when the two feature sets are the same type. For example, it does not automatically upgrade a switch in VM mode from IP services feature set to IP base feature set (or the reverse) or from cryptographic universal software image to noncryptographic universal software image (or the reverse).

- Automatic advise (auto-advise) occurs when the auto-upgrade process cannot find appropriate stack member software to copy to the switch in VM mode. This process tells you the command (**archive copy-sw** or **archive download-sw** privileged EXEC command) and the image name (tar filename) needed to manually upgrade the switch stack or the switch in VM mode. The recommended image can be the running switch stack image or a tar file in any flash file system in the switch stack (including the switch in VM mode). If an appropriate image is not found in the stack flash file systems, the auto-advise process tells you to install new software on the switch stack. Auto-advise cannot be disabled, and there is no command to check its status.

The auto-advise software does *not* give suggestions when the switch stack software and the software of the switch in VM mode do not contain the same feature sets. For example, if the switch stack is running the IP base image and you add a switch that is running the IP services image, the auto-advise software does not provide a recommendation. The same events occur when cryptographic and noncryptographic images are running.

You can use the **archive-download-sw /allow-feature-upgrade** privileged EXEC command to allow installing an different software image.

Auto-Upgrade and Auto-Advise Example Messages

When you add a switch that has a different minor version number to the switch stack, the software displays messages in sequence (assuming that there are no other system messages generated by the switch).

This example shows that the switch stack detected a new switch that is running a different minor version number than the switch stack. Auto-copy starts, finds suitable software to copy from a stack member to the switch in VM mode, upgrades the switch in VM mode, and then reloads it:

```
*Mar 11 20:31:19.247:%STACKMGR-6-STACK_LINK_CHANGE:Stack Port 2 Switch 2 has changed to
state UP
*Mar 11 20:31:23.232:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
*Mar 11 20:31:23.291:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH) (Stack_1-3)
*Mar 11 20:33:23.248:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED:Auto-copy-software process
initiated for switch number(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Searching for stack member to act
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:as software donor...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Found donor (system #2) for
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:member(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System software to be uploaded:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System Type:            0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving cbs31x0-universal-mz.122-40.EX
(directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving
cbs31x0-universal-mz.122-40.EX/cbs31x0-universal-mz.122-40.EX.bin (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving
cbs31x0-universal-mz.122-40.EX/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:examining image...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting
cbs31x0-universal-mz.122-40.EX/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Stacking Version Number:1.4
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System Type:            0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Ios Image File Size:  0x004BA200
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Total Image File Size:0x00818A00
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Minimum Dram required:0x08000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Suffix:ipservices-122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image
Directory:cbs31x0-universal-mz.122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image Name:cbs31x0-universal-mz.122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Image
Feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
```

```
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Old image for switch
1:flash1:cbs31x0-universal-mz.122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:  Old image will be deleted after download.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Extracting images from archive into flash on
switch 1...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: cbs31x0-universal-mz.122-0.0.313.EX
(directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting
cbs31x0-universal-mz.122-0.0.313.EX/cbs31x0-universal-mz.122-40.EX (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting
cbs31x0-universal-mz.122-40.EX/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Installing
(renaming):`flash1:update/cbs31x0-universal-mz.122-0.0.313.EX' ->
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
`flash1:cbs31x0-universal-mz.122-40.EX'
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:New software image installed in
flash1:cbs31x0-i5-mz.122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Removing old
image:flash1:cbs31x0-universal-mz.122-40.EX
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:All software images installed.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Requested system reload in progress...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Software successfully copied to
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:system(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Done copying software
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Reloading system(s) 1
```

This example shows that the switch stack detected a new switch that is running a different minor version number than the switch stack. Auto-copy starts but cannot find software in the switch stack to copy to the VM-mode switch to make it compatible with the switch stack. The auto-advise process starts and recommends that you download a tar file from the network to the switch in VM mode:

```
*Mar  1 00:01:11.319:%STACKMGR-6-STACK_LINK_CHANGE:Stack Port 2 Switch 2 has changed to
state UP
*Mar  1 00:01:15.547:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
stack_2#
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED:Auto-copy-software process
initiated for switch number(s) 1
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:Searching for stack member to act
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:as software donor...
*Mar  1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:Software was not copied
*Mar  1 00:03:15.562:%IMAGEMGR-6-AUTO_ADVISE_SW_INITIATED:Auto-advise-software process
initiated for switch number(s) 1
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:Systems with incompatible software
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:have been added to the stack.  The
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:storage devices on all of the stack
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:members have been scanned, and it has
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:been determined that the stack can be
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:repaired by issuing the following
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:command(s):
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:    archive download-sw /force-reload
/overwrite /dest 1 flash1:cbs31x0-universal-mz.122-40.EX.tar
*Mar  1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
```

For information about using the **archive download-sw** privileged EXEC command, see the "Working with Software Images" section on page A-25.

Note Auto-advise and auto-copy identify which images are running by examining the info file and by searching the directory structure on the switch stack. If you download your image by using the **copy tftp:** boot loader command instead of the **archive download-sw** privileged EXEC command, the proper directory structure is not created. For more information about the info file, see the "File Format of Images on a Server or Cisco.com" section on page A-26.

Incompatible Software and Stack Member Image Upgrades

You can upgrade a switch that has an incompatible universal software image by using the **archive copy-sw** privileged EXEC command. It copies the software image from an existing stack member to the one with incompatible software. That switch automatically reloads and joins the stack as a fully functioning member. For more information, see the "Copying an Image File from One Stack Member to Another" section on page A-40.

Switch Stack Configuration Files

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

The stack master has the saved and running configuration files for the switch stack. All stack members periodically receive synchronized copies of the configuration files from the stack master. If the stack master becomes unavailable, any stack member assuming the role of stack master has the latest configuration files.

Note We recommend that all stack members run Cisco IOS Release 12.2(40)EX or later. The interface-specific settings of the stack master are saved if the stack master is replaced without saving the running configuration to the startup configuration.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that switch stack. If a switch is moved to a different switch stack, that switch loses its saved configuration file and uses the system-level configuration of the new switch stack.

The interface-specific configuration of each stack member is associated with the stack member number. As mentioned in the "Stack Member Numbers" section on page 7-8, stack members retain their numbers unless they are manually changed or they are already used by another member in the same switch stack.

- 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 a stack member fails and you replace with it with an identical model, the replacement switch automatically uses the same interface-specific configuration as the failed switch. Hence, you do not need to reconfigure the interface settings. The replacement switch must have the same stack member number as the failed switch. For information about the benefits of provisioning a switch stack, see the "Switch Stack Offline Configuration" section on page 7-9.

You back up and restore the stack configuration in the same way as you would for a standalone switch configuration. For more information about file systems and configuration files, see Appendix A, "Working with the Cisco IOS File System, Configuration Files, and Software Images."

Additional Considerations for System-Wide Configuration on Switch Stacks

These sections provide additional considerations for configuring system-wide features on switch stacks:

- "Planning and Creating Clusters" chapter in the *Getting Started with Cisco Network Assistant*, available on Cisco.com
- "MAC Addresses and Switch Stacks" section on page 5-15
- "Setting the SDM Template" section on page 8-5
- "802.1x Authentication and Switch Stacks" section on page 9-12
- "VTP and Switch Stacks" section on page 14-8
- "Private VLANs and Switch Stacks" section on page 16-6
- "Spanning Tree and Switch Stacks" section on page 18-12
- "MSTP and Switch Stacks" section on page 19-8
- "DHCP Snooping and Switch Stacks" section on page 22-9
- "IGMP Snooping and Switch Stacks" section on page 24-7
- "Port Security and Switch Stacks" section on page 26-19
- "CDP and Switch Stacks" section on page 27-2
- "SPAN and RSPAN and Switch Stacks" section on page 30-11
- "ACLs and Switch Stacks" section on page 35-7
- "EtherChannel and Switch Stacks" section on page 38-9
- "IP Routing and Switch Stacks" section on page 39-3
- "IPv6 and Switch Stacks" section on page 40-10
- "HSRP and Switch Stacks" section on page 41-5
- "Multicast Routing and Switch Stacks" section on page 45-10
- "Fallback Bridging and Switch Stacks" section on page 47-3

Switch Stack Management Connectivity

You manage the switch stack and the stack member interfaces through the stack master. You can use the CLI, SNMP, Network Assistant, and CiscoWorks network management applications. You cannot manage stack members on an individual switch basis.

These sections provide switch stack connectivity information:

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 stack master or to any other stack member. You can still manage the stack through the same IP address even if you remove the stack master or any other stack member from the stack, provided there is IP connectivity.

Note 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 switches that you remove from the switch stack.

For related information about switch stack configurations, see the "Switch Stack Configuration Files" section on page 7-16.

Connectivity to the Switch Stack Through an SSH Session

The Secure Shell (SSH) connectivity to the switch stack can be lost if a stack master running the cryptographic software image and the IP base or IP services feature set fails and is replaced by a switch that is running the noncryptographic image and the same feature set. We recommend that a switch running the cryptographic software image and the IP base or IP services feature set be the stack master. Encryption features are unavailable if the stack master is running the noncryptographic software image.

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

You can connect to the stack master by using one of these methods:

- You can connect a terminal or a PC to the stack master through the console port of one or more stack members.
- You can connect a PC to the stack master 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 Internal Ethernet Management Port" section on page 11-13.

Be careful when using multiple CLI sessions to the stack master. 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.

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. For more information, see the "Using Interface Configuration Mode" section on page 11-8.

To debug a specific stack member, you can access it from the stack master by using the **session** *stack-member-number* privileged EXEC command. The stack member number is appended to the system prompt. For example, `Switch-2#` is the prompt in privileged EXEC mode for stack member 2, and the system prompt for the stack master is `Switch`. Only the **show** and **debug** commands are available in a CLI session to a specific stack member.

Switch Stack Configuration Scenarios

Table 7-2 provides switch stack configuration scenarios. Most of the scenarios assume that at least two switches are connected through their StackWise Plus ports.

Table 7-2 Switch Stack Configuration Scenarios

Scenario		Result
Stack master election specifically determined by existing stack masters	Connect two powered-on switch stacks through the StackWise Plus ports.	Only one of the two stack masters becomes the new stack master. None of the other stack members become the stack master.
Stack master election specifically determined by the stack member priority value	1. Connect two switches through their StackWise Plus ports. 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.	The stack member with the higher priority value is elected stack master.
Stack master 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 stack master.

Table 7-2 Switch Stack Configuration Scenarios (continued)

Scenario		Result
Stack master election specifically determined by the cryptographic software image and the IP services feature set and the IP services feature set	Assuming that all stack members have the same priority value: 1. Make sure that one stack member has the cryptographic image installed and the IP services feature set enabled and that the other stack member has the noncryptographic image installed and the IP services feature set enabled. 2. Restart both stack members at the same time.	The stack member with the cryptographic image and the IP services feature set is elected stack master.
Stack master election specifically determined by the cryptographic software image and the IP base feature set	Assuming that all stack members have the same priority value: 1. Make sure that one stack member has the cryptographic image installed and the IP base feature set enabled and that the other stack member has the noncryptographic image installed and the IP base feature set enabled. 2. Restart both stack members at the same time.	The stack member with the cryptographic image and the IP base feature set is elected stack master.
Stack master 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 stack master.
Stack member number conflict	Assuming that one stack member has a higher priority value than the other stack member: 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. 2. Restart both stack members at the same time.	The stack member with the higher priority value retains its stack member number. The other stack member has a new stack member number.
Add a stack member	1. Power off the new switch. 2. Through their StackWise Plus ports, connect the new switch to a powered-on switch stack. 3. Power on the new switch.	The stack master is retained. The new switch is added to the switch stack.

Table 7-2 Switch Stack Configuration Scenarios (continued)

Scenario		Result
Stack master failure	Remove (or power off) the stack master.	Based on the factors described in the "Stack Master Election and Re-Election" section on page 7-6, 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.
Add more than nine stack members	1. Through their StackWise Plus ports, connect ten switches. 2. Power on all switches.	Two switches become stack masters. One stack master has nine stack members. The other stack master remains as a standalone switch. Use the Mode button and port LEDs on the switches to identify which switches are stack masters and which switches belong to each stack master. For information about using the Mode button and the LEDs, see the hardware installation guide.

Configuring the Switch Stack

These sections contain this configuration information:

Default Switch Stack Configuration

Table 7-3 shows the default switch stack configuration.

Table 7-3 Default Switch Stack Configuration

Feature	Default Setting
Stack MAC address timer	Disabled.
Stack member number	1
Stack member priority value	1
Offline configuration	The switch stack is not provisioned.

Enabling Persistent MAC Address

The switch stack MAC address is determined by the MAC address of the stack master. When a stack master is removed from the stack and a new stack master takes over, the default is for the MAC address of the new stack master to immediately become the new stack MAC router address. However, you can enable the persistent MAC address feature to allow a time delay before the stack MAC address changes. During this time period, if the previous stack master 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 a stack master. If the previous stack master does not rejoin the stack during this period, the switch stack takes the MAC address of the new stack master as the stack MAC address.You can also configure stack MAC persistency so that the stack never switches to the MAC address of the new stack master.

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

You can configure the time period as 0 to 60 minutes.

- If you enter the command with no value, the default delay is 4 minutes. We recommend that you always enter a value. If the command is entered without a value, the time delay appears in the running-config file with an explicit timer value of 4 minutes.
- If you enter **0**, the stack MAC address of the previous stack master is used until you enter the **no stack-mac persistent timer** command, which immediately changes the stack MAC address to that of the current stack master. If you do not enter the **no stack-mac persistent timer** command, the stack MAC address never changes.
- If you enter a time delay of 1 to 60 minutes, the stack MAC address of the previous stack master is used until the configured time period expires or until you enter the **no stack-mac persistent timer** command.

Note If the entire switch stack reloads, it uses with the MAC address of the stack master as the stack MAC address.

Beginning in privileged EXEC mode, follow these steps to enable persistent MAC address. This procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**stack-mac persistent timer** [**0** | *time-value*]	Enable a time delay after a stack-master change before the stack MAC address changes to that of the new stack master. If the previous stack master rejoins the stack during this period, the stack uses that MAC address as the stack MAC address. • Enter the command with no value to set the default delay of approximately 4 minutes. We recommend that you always configure a value. • Enter **0** to continue using the MAC address of the current stack master indefinitely. • Enter a *time-value* from 1 to 60 minutes to configure the time period before the stack MAC address changes to the new stack master. **Note** When you enter this command, a warning states that traffic might be lost if the old master MAC address appears elsewhere in the network domain. If you enter the **no stack-mac persistent timer** command after a new stack master takes over, before the time expires, the switch stack moves to the current stack master MAC address.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config** or	Verify that the stack MAC address timer is enabled. If enabled, the output shows `stack-mac persistent timer` and the time in minutes.
Step 5	**show switch**	If enabled, the display includes: `Mac persistency wait time`, the number of minutes configured, and the current stack MAC address.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

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
                                           H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0016.4727.a900     1      0       Ready
```

Assigning Stack Member Information

These sections describe how to assign stack member information:

- Assigning a Stack Member Number, page 7-24 (optional)
- Setting the Stack Member Priority Value, page 7-24 (optional)
- Provisioning a New Member for a Switch Stack, page 7-25 (optional)

Assigning a Stack Member Number

Note This task is available only from the stack master.

Beginning in privileged EXEC mode, follow these steps to assign a member number to a stack member. This procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**switch** *current-stack-member-number* **renumber** *new-stack-member-number*	Specify 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 **show switch** user EXEC command.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload slot** *stack-member-number*	Reset the stack member.
Step 5	**show switch**	Verify the stack member number.
Step 6	**copy running-config startup-config**	Save your entries in the configuration file.

Setting the Stack Member Priority Value

Note This task is available only from the stack master.

Beginning in privileged EXEC mode, follow these steps to assign a priority value to a stack member: This procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command	Purpose
Step 2	**switch** *stack-member-number* **priority** *new-priority-number*	Specify 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 **show switch** user EXEC command. The new priority value takes effect immediately but does not affect the current stack master. The new priority value helps determine which stack member is elected as the new stack master when the current stack master or switch stack resets.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload slot** *stack-member-number*	Reset the stack member, and apply this configuration change.
Step 5	**show switch** *stack-member-number*	Verify the stack member priority value.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Provisioning a New Member for a Switch Stack

Note This task is available only from the stack master.

Beginning in privileged EXEC mode, follow these steps to provision a new member for a switch stack. This procedure is optional.

	Command	Purpose
Step 1	**show switch**	Display summary information about the switch stack.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**switch** *stack-member-number* **provision** *type*	Specify 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.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify the correct numbering of interfaces in the running configuration file.
Step 6	**show switch** *stack-member-number*	Verify the status of the provisioned switch. For *stack-member-number*, enter the same number as in Step 1.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove provisioned information and to avoid receiving an error message, remove the specified switch from the stack before you use the **no** form of this command.

For example, if you are removing a provisioned switch in a stack with this configuration:

- The stack has four members
- Stack member 1 is the master
- 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 Plus 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.

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 WS-CBS3120G
Switch(config)# end
Switch# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

Accessing the CLI of a Specific Stack Member

Note This task is only for debugging purposes, and is only available from the master.

You can access all or specific members by using the **remote command** {**all** | *stack-member-number*} privileged EXEC command. The stack member number range is 1 to 9.

You can access specific members by using the **session** *stack-member-number* privileged EXEC command. The member number is appended to the system prompt. For example, the prompt for member 2 is `Switch-2#`, and system prompt for the master is `Switch#`. Enter exi**t** to return to the CLI session on the master. Only the **show** and **debug** commands are available on a specific member.

Displaying Switch Stack Information

To display saved configuration changes after resetting a specific member or the stack, use these privileged EXEC commands:

Table 7-4 Commands for Displaying Stack Information

Command	Description
show platform stack manager all	Display all stack information, such as the stack protocol version.
show platform stack ports {**buffer** | **history**}	Display the stack port events and history.

Table 7-4 Commands for Displaying Stack Information (continued)

Command	Description
show switch	Display summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.
show switch *stack-member-number*	Display information about a specific member.
show switch detail	Display detailed information about the stack ring.
show switch neighbors	Display the stack neighbors.
show switch stack-ports [**summary**]	Display port information for the stack. Use the **summary** keyword to display the stack cable length, the stack link status, and the loopback status.
show switch stack-ring activity [**detail**]	Display the number of frames per member that are sent to the stack ring. The **detail** keyword displays the number of frames per member that are sent to the stack ring, the receive queues, and the ASIC.

Troubleshooting Stacks

Manually 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 re-enable 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
  - All members are connected through the stack ports, but some all are not in the ready state.
  - Some members are not connected through the stack ports.

When you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command 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]
  ```

- 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.
  ```

Re-Enabling 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, 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:

1. Disconnect the stack cable between Port 1 on Switch 1 and Port 2 on Switch 4.
2. Remove Switch 4 from the stack.
3. Add a switch to replace Switch 4 and assign it switch-number 4.
4. Reconnect the cable between Port 1 on Switch 1 and Port 2 on Switch 4 (the replacement switch).
5. Re-enable the link between the switches. Enter the **switch 1 stack port 1 enable** privileged EXEC command to enable Port 1 on Switch 1.
6. Power on Switch 4.

Caution 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.

Understanding the show switch stack-ports summary Output

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
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     OK         3      50 cm     Yes    Yes    Yes        1        No
  1/2     Down      None    3 m       Yes    No     Yes        1        No
  2/1     Down      None    3 m       Yes    No     Yes        1        No
  2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
  3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
  3/2     OK         1      50 cm     Yes    Yes    Yes        1        No
```

Table 7-5 show switch stack-ports summary Command Output

Field	Description
Switch#/Port#	Member number and its stack port number.
Stack Port Status	• 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	This shows if the link is stable. The *link partner* is a stack port on a neighbor switch. • No—The link partner receives invalid protocol messages from the port. • Yes—The link partner receives valid protocol messages from the port.
Link Active	This shows if the stack port is in the same state as its link partner. • No—The port cannot send traffic to the link partner. • Yes—The port can send traffic to the link partner.
Sync OK	• 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	This shows 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	• 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.

Identifying Loopback Problems

Software Loopback

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

```
Switch# show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     OK         3      50 cm     Yes    Yes    Yes        1        No
  1/2     OK         2      3 m       Yes    Yes    Yes        1        No
  2/1     OK         1      3 m       Yes    Yes    Yes        1        No
  2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
  3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
  3/2     OK         1      50 cm     Yes    Yes    Yes        1        No
```

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
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Absent     None    No cable  No     No     No         1        No
  1/2     OK         2       3 m       Yes    Yes    Yes        1        No
  2/1     OK         1       3 m       Yes    Yes    Yes        1        No
  2/2     OK         3       50 cm     Yes    Yes    Yes        1        No
  3/1     OK         2       50 cm     Yes    Yes    Yes        1        No
  3/2     Down       None    50 cm     No     No     No         1        No
```

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
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  2/1     Down       None    3 m       No     No     No         1        No
  2/2     OK         3       50 cm     Yes    Yes    Yes        1        No
  3/1     OK         2       50 cm     Yes    Yes    Yes        1        No
  3/2     Down       None    50 cm     No     No     No         1        No
```

Switch 1 is a standalone switch.

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

Software Loopback Example: No Connected Stack Cable

Port status:

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

Software Loopback Examples: Connected Stack Cables

- 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
  Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
   Port#     Port              Length    OK   Active   OK    Changes   Loopback
            Status                                          To LinkOK
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Down      None    50 Cm      No     No     No       1          No
    1/2     Absent    None    No cable   No     No     No       1          No
  ```

- 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
  Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
   Port#     Port              Length    OK   Active   OK    Changes   Loopback
            Status                                          To LinkOK
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    2/1       OK       2      50 cm     Yes    Yes    Yes       1          No
    2/2       OK       2      50 cm     Yes    Yes    Yes       1          No
  ```

  The port status shows that
  - Switch 2 is a standalone switch.
  - The ports can send and receive traffic.

Hardware Loopback

The **show platform stack ports buffer** privileged EXEC command output shows the hardware loopback values.

```
Switch# show platform stack ports buffer
              Stack Debug Event Data Trace
============================================================
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
============================================================

  Event    Stack           Stack PCS Info              Ctrl-Status  Loopback   Cable
  Count    Port                                                     IOS / HW   length
=========  =====  ==================================  ===========  ========  ========
Event type: LINK OK Stack Port 1
0000000011   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000011   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
Event type: LINK OK Stack Port 2
0000000012   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000012   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
Event type: RAC
0000000013   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000013   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
```

On a member,

- If a stack port has an connected stack cable, the *Loopback HW* value for the stack port is *No*.
- If the stack port does not have an connected stack cable, the *Loopback HW* value for the stack port is *Yes*.

Hardware Loopback Example: LINK OK event

```
Switch# show platform stack ports buffer

              Stack Debug Event Data Trace
============================================================
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
============================================================

  Event    Stack           Stack PCS Info              Ctrl-Status  Loopback   Cable
  Count    Port                                                     IOS / HW   length
=========  =====  ==================================  ===========  ========  ========
Event type: LINK OK Stack Port 1
0000000153   1    FF01FF00 860351A5 55A5FFFF FFFFFFFF   0CE60C10     No /No   50 cm
0000000153   2    FF01FF00 00017C07 00000000 0000FFFF   0CE60C10     No /No   3 m
Event type: RAC
0000000154   1    FF01FF00 860351A5 55A5FFFF FFFFFFFF   0CE60C10     No /No   50 cm
0000000154   2    FF01FF00 00017C85 00000000 0000FFFF   0CE60C10     No /No   3 m
```

Hardware Loop Example: LINK NOT OK Event

```
Switch# show platform stack ports buffer
Stack Debug Event Data Trace
============================================================
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
============================================================

  Event    Stack           Stack PCS Info              Ctrl-Status  Loopback   Cable
  Count    Port                                                     IOS / HW   length
=========  =====  ==================================  ===========  ========  ========
Event type: LINK OK Stack Port 1
0000000014   1    FF01FF00 860204A7 5555FFFF 00000000   0CE60CA6     No /No   50 cm
0000000014   2    FF01FF00 85020823 AAAAFFFF 00000000   0CE60CA6     No /No   3 m
Event type: RAC
0000000015   1    FF01FF00 860204A7 5555FFFF 00000000   0CE60CA6     No /No   50 cm
0000000015   2    FF01FF00 85020823 AAAAFFFF 00000000   0CE60CA6     No /No   3 m
Event type: LINK OK Stack Port 2
0000000029   1    FF01FF00 860204A7 5555FFFF 00000000   1CE61CE6     No /No   50 cm
0000000029   2    FF01FF00 86020823 AAAAFFFF 00000000   1CE61CE6     No /No   3 m
Event type: RAC
0000000030   1    FF01FF00 860204A7 5555FFFF 00000000   1CE61CE6     No /No   50 cm
0000000030   2    FF01FF00 86020823 AAAAFFFF 00000000   1CE61CE6     No /No   3 m
Event type: LINK NOT OK Stack Port 1
0000009732   1    FF01FF00 00015B12 5555FFFF A49CFFFF   0C140CE4     No /No   50 cm
0000009732   2    FF01FF00 86020823 AAAAFFFF 00000000   0C140CE4     No /No   3 m
Event type: RAC
0000009733   1    FF01FF00 00015B4A 5555FFFF A49CFFFF   0C140CE4     No /No   50 cm
0000009733   2    FF01FF00 86020823 AAAAFFFF 00000000   0C140CE4     No /No   3 m
Event type: LINK NOT OK Stack Port 2
0000010119   1    FF01FF00 00010E69 25953FFF FFFFFFFF   0C140C14     No /Yes  No cable
0000010119   2    FF01FF00 0001D98C 81AAC7FF 0300FFFF   0C140C14     No /No   3 m
Event type: RAC
0000010120   1    FF01FF00 00010EEA 25953FFF FFFFFFFF   0C140C14     No /Yes  No cable
0000010120   2    FF01FF00 0001DA0C 81AAC7FF 0300FFFF   0C140C14     No /No   3 m
```

Finding a Disconnected Stack Cable

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
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     OK         2      50 cm     Yes    Yes    Yes        0        No
  1/2     OK         2      50 cm     Yes    Yes    Yes        0        No
  2/1     OK         1      50 cm     Yes    Yes    Yes        0        No
  2/2     OK         1      50 cm     Yes    Yes    Yes        0        No
```

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:

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

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

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#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  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.