Managing Switch Stacks

This chapter provides the concepts and procedures to manage Catalyst 3750 switch stacks.

Note For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release.

This chapter consists of these sections:

- Understanding Switch Stacks, page 5-1
- Assigning Stack Member Information, page 5-17
- Accessing the CLI of a Specific Stack Member, page 5-19
- Displaying Switch Stack Information, page 5-20

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

Understanding Switch Stacks

A *switch stack* is a set of up to nine Catalyst 3750 switches connected through their StackWise 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 *stack members*. The stack members use the Cisco StackWise technology to behave and 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 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 the switch stack 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 uniquely identified by its own *stack member number*.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master from among themselves. A set of factors determine which switch is elected the stack master. One of the factors is the *stack member priority value*. The switch with the highest priority value becomes the stack master.

The system-level features supported on the stack master are supported on the entire switch stack. If the switch stack must have switches running both standard multilayer image (SMI) and enhanced multilayer image (EMI) software, we recommend that a switch running the EMI software be the stack master. EMI features are unavailable if the stack master is running the SMI software.

Similarly, we recommend that a switch running the cryptographic (that is, supports encryption) version of the SMI or EMI software be the stack master. Encryption features are unavailable if the stack master is running the noncryptographic version of the SMI or EMI software.

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:

- Cluster Management Suite (CMS) software through a supported browser session
- Command-line interface (CLI) over a serial connection to the console port of any stack member
- A network management application through the Simple Network Management Protocol (SNMP)
- CiscoWorks network management software

To manage switch stacks, you should understand:

- These concepts on how switch stacks are formed:
  - Switch Stack Membership, page 5-3
  - Stack Master Election and Re-Election, page 5-4
- These concepts on how switch stacks and stack members are configured:
  - Switch Stack Bridge ID and Router MAC Address, page 5-5
  - Stack Member Numbers, page 5-6
  - Stack Member Priority Values, page 5-7
  - Switch Stack Offline Configuration, page 5-7
  - Hardware Compatibility in Switch Stacks, page 5-10
  - Software Compatibility in Switch Stacks, page 5-10
  - Switch Stack Configuration Files, page 5-12
  - Additional Considerations for System-Wide Configuration on Switch Stacks, page 5-13
  - Switch Stack Management Connectivity, page 5-14
  - Switch Stack Configuration Scenarios, page 5-15

Note A switch stack is different from a *switch cluster.* A switch cluster is a set of switches connected through their LAN ports, such as the 10/100/1000 ports. For more information about how switch stacks differ from switch clusters, see the "Switch Clusters and Switch Stacks" section on page 6-14.

Switch Stack Membership

A switch stack has up to nine stack members connected through their StackWise 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 5-1 on page 5-4) to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack (Figure 5-2 on page 5-4) 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 5-7. For information about replacing a failed switch, refer to 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 the switches that you add to or remove from the switch stack are powered off.

After adding or removing stack members, make sure that the switch stack is operating at full bandwidth (32 Gbps). Press the Mode button on a stack member until the Stack mode LED is on. The last two port LEDs on all switches in the stack should be green. Depending on the switch model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module ports. If, on any of the switches, one or both of the last two port LEDs are not green, 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 newly created switch stacks.
  b. Reconnect them to the original switch stack through their StackWise ports.
  c. Power on the switches.

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

Figure 5-1 Creating a Switch Stack from Two Standalone Switches

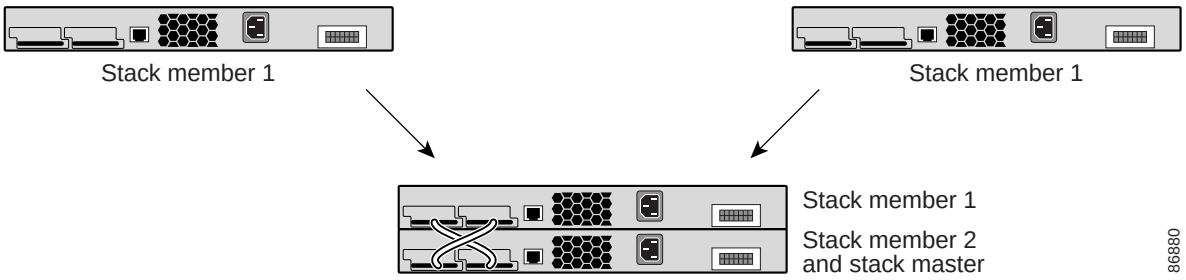
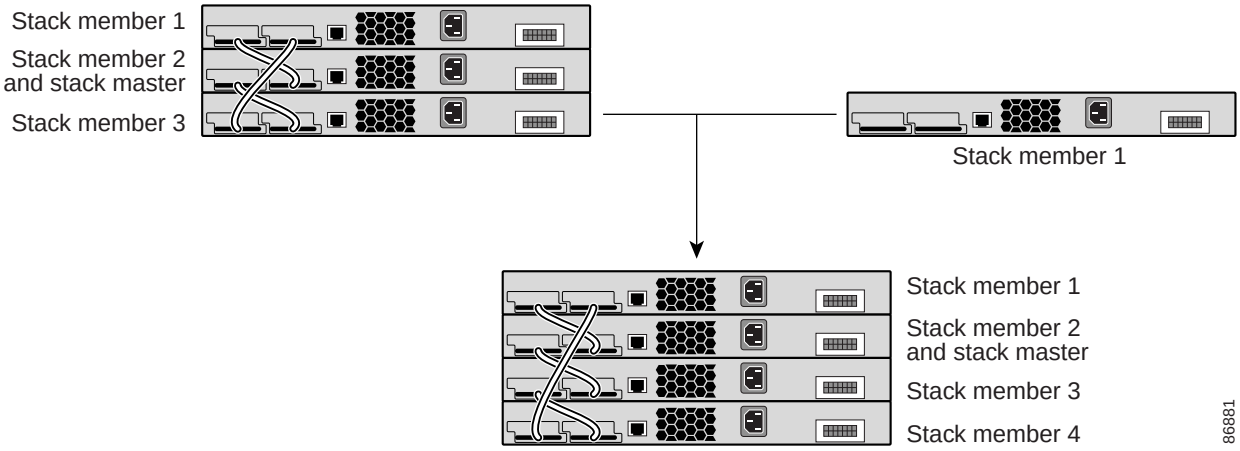


Figure 5-2 Adding a Standalone Switch to a Switch Stack



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 not using the default interface-level configuration.
4. The switch with the higher priority switch software version. These switch software versions are ordered from highest to lowest priority:
   1. Cryptographic EMI software
   2. Noncryptographic EMI software
   3. Cryptographic SMI software
   4. Noncryptographic SMI software

   The Catalyst 3750 EMI cryptographic image has a higher priority than the Catalyst 3750 SMI image during the master switch election in a stack. However, when two or more switches in the stack use different software images, such as the SMI image for Cisco IOS Release 12.1(11)AX and the

cryptographic EMI for Cisco IOS Release 12.1(19)EA1 or later, the switch running the SMI is selected as the stack master. This occurs because the switch running the cryptographic EMI takes 10 seconds longer to start than does the switch running the SMI. The switch running the EMI is excluded from the master election process that lasts 10 seconds. To avoid this problem, upgrade the switch running the SMI to a software release later than Cisco IOS Release 12.1(11)AX or manually start the master switch and wait at least 8 seconds before starting the new member switch.

5. The switch with the longest system up-time.
6. 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 has failed.
- 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 10-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 10-second time frame do not participate in this initial election and only become stack members. All stack members participate in re-elections. For all powering considerations that affect stack-master elections, refer to 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 while a new stack master is elected and is resetting.

If 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.

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 5-17. 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 4-14.

  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 5-12.

  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 by another member in the stack, 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 5-3).

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.

Stack Member Priority Values

A higher priority value for a stack member increases its likelihood to be elected stack master and to retain 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 if a re-election occurs.

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 5-18. 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 4-14.

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 will be 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 also is automatically created when a switch is added to a switch stack that is running Cisco IOS Release 12.2(20)SE or later 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 to it. Table 5-1 lists the events that occur when the switch stack compares the provisioned configuration with the provisioned switch:

Table 5-1 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.

Table 5-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch (continued)

Scenario		Result
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.
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) are executed. Depending on how different the actual switch type is from the previously provisioned switch type, some commands are rejected, and some commands are accepted.

For example, suppose the switch stack is provisioned for a 48-port switch with Power over Ethernet (PoE), the configuration is saved, and the stack is powered down. Then, a 24-port switch without PoE support is connected to the switch stack, and the stack is powered up. In this situation, the configuration for ports 25 through 48 is rejected, and error messages appear on the stack master switch console during initialization. In addition, any configured PoE-related commands that are valid only on PoE-capable interfaces are rejected, even for ports 1 through 24.

Note If the switch stack is running Cisco IOS Release 12.2(20)SE or later and 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 5-18.

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 5-8.

Effects of Removing a Provisioned Switch from a Switch Stack

If a switch stack is running Cisco IOS Release 12.2(20)SE or later and 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 in Switch Stacks

The Catalyst 3750-12S switch supports desktop and aggregator Switch Database Management (SDM) templates. All other Catalyst 3750 switches support only the desktop SDM templates.

All stack members use the SDM template configured on the stack master. If the stack master is using an aggregator template, only Catalyst 3750-12S switches can be stack members. All other switches attempting to join this switch stack enter SDM mismatch mode. These switches can join the stack only when the stack master is running a desktop SDM template.

We recommend that your stack master use an aggregator template only if you plan to create a switch stack of Catalyst 3750-12S switches. If you plan to have a switch stack with different Catalyst 3750 switch models, configure the stack master to use one of the desktop templates.

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

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."

Software Compatibility in Switch Stacks

This section describes how to ensure software compatibility between stack members:

- Compatibility Recommendations, page 5-11
- Incompatible Software and Stack Member Image Upgrades, page 5-11
- Stack Protocol Version Compatibility, page 5-11

To ensure complete compatibility between stack members, use the information in this section and in the "Hardware Compatibility in Switch Stacks" section on page 5-10.

Compatibility Recommendations

All stack members must run the same Cisco IOS software version to ensure compatibility between stack members.

Follow these recommendations:

- The Cisco IOS software version on all stack members, including the stack master, should be the same. This helps ensure full compatibility in the stack protocol version among the stack members. For example, all stack members should have the EMI Cisco IOS Release 12.1(14)EA1 installed.
- If your switch stack must have switches running SMI and EMI software, the switch running the EMI software should be the stack master. EMI features become unavailable to all stack members if the stack master is running the SMI software.
- At least two stack members should have the EMI software installed to ensure redundant support of the EMI features. The EMI has precedence over the SMI during stack master election, assuming that the priority value of the stack members are the same. If the EMI stack master fails, the other stack member running the EMI software becomes the stack master.
- When a switch running the EMI joins a switch stack running the SMI of the same version, the EMI switch does not automatically become the stack master. If you want the EMI switch to become the stack master, reset the current SMI stack master by using the **reload slot** *stack-member-number* privileged EXEC command. The EMI switch is elected the stack master, assuming its priority value is higher or the same as the other stack members.

Incompatible Software and Stack Member Image Upgrades

You can upgrade a switch that has an incompatible 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 B-34.

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. 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 incompatible 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.

These sections provide more detail about incompatibility in switch stacks:

- Major Incompatibility Between Switches, page 5-12
- Minor Incompatibility Between Switches, page 5-12

Major Incompatibility Between Switches

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

Minor Incompatibility Between Switches

Switches with the same major version number but a different minor version number as the stack master are considered partially compatible. When connected to a switch stack, partially compatible switches enter into version mismatch (VM) mode and cannot join the stack. The stack master downloads the software version it is using to any switch in VM mode.

- If there is a stack member that is not in VM mode and is running software that can also run on the switch in VM mode, the stack master uses that software to upgrade (or downgrade) the software on the switch in VM mode. The switch in VM mode automatically reloads and joins the stack as a fully functioning member.

  The stack master does not automatically install EMI software on an SMI-running switch or SMI software on an EMI-running switch.

- If none of the stack members are running software that can be installed on the switch in VM mode, the stack master scans the switch stack to see if there are any other recommended actions. Recommended actions appear in the system message log. If there are no other actions to try, the stack master displays the recommended action to upgrade the software running on the switch stack.

The port LEDs on switches in VM mode remain off and pressing the Mode button does not change the LED mode.

You can also use the **show switch** user EXEC command to see if any stack members are in VM mode.

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, which 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 are installed with Cisco IOS Release 12.1(14)EA1 or later to ensure that the interface-specific settings of the stack master are saved, in case 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 5-6, 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 5-7.

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 B, "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:

- "Switch Clusters and Switch Stacks" section on page 6-14
- "MAC Addresses and Switch Stacks" section on page 7-22
- "Setting the SDM Template" section on page 8-4
- "802.1x and Switch Stacks" section on page 10-10
- "VTP and Switch Stacks" section on page 14-6
- "Private VLANs and Switch Stacks" section on page 15-5
- "Spanning Tree and Switch Stacks" section on page 17-12
- "MSTP and Switch Stacks" section on page 18-6
- "DHCP Snooping and Switch Stacks" section on page 21-6
- "IGMP Snooping and Switch Stacks" section on page 23-6
- "Port Security and Switch Stacks" section on page 24-14
- "CDP and Switch Stacks" section on page 25-2
- "SPAN and RSPAN and Switch Stacks" section on page 27-10
- "ACLs and Switch Stacks" section on page 31-6
- "EtherChannel and Switch Stacks" section on page 33-9
- "IP Routing and Switch Stacks" section on page 34-3
- "HSRP and Switch Stacks" section on page 35-2
- "Multicast Routing and Switch Stacks" section on page 36-8
- "Fallback Bridging and Switch Stacks" section on page 38-3

Switch Stack Management Connectivity

You manage the switch stack and the stack member interfaces through the stack master. You can use the CMS, the CLI, and SNMP 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, page 5-14
- Connectivity to the Switch Stack Through an SSH Session, page 5-14
- Connectivity to the Switch Stack Through Console Ports, page 5-14
- Connectivity to Specific Stack Members, page 5-14

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 address or addresses of the switch that you removed from the switch stack.

For related information about switch stack configurations, see the "Switch Stack Configuration Files" section on page 5-12.

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 version of the SMI or EMI software, fails and is replaced by a switch that is running a noncryptographic version of the software. We recommend that a switch running the cryptographic version of the SMI or EMI software be the stack master. Encryption features are unavailable if the stack master is running the noncryptographic version of the SMI or EMI software.

Connectivity to the Switch Stack Through Console Ports

You can connect to the stack master through the console port of one or more stack members.

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 11-7.

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 5-2 provides switch stack configuration scenarios. Most of the scenarios assume at least two switches are connected through their StackWise ports.

Table 5-2 Switch Stack Configuration Scenarios

Scenario		Result
Stack master election specifically determined by existing stack masters	Connect two powered-on switch stacks through the StackWise 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 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.
Stack master election specifically determined by the cryptographic EMI software	Assuming that all stack members have the same priority value: 1. Make sure that one stack member has the cryptographic EMI software installed and that the other stack member has the noncryptographic EMI software installed. 2. Restart both stack members at the same time.	The stack member with the cryptographic EMI software is elected stack master.

Table 5-2 Switch Stack Configuration Scenarios (continued)

Scenario		Result
Stack master election specifically determined by the EMI software	Assuming that all stack members have the same priority value: 1. Make sure that one stack member has the noncryptographic EMI software installed and that the other stack member has the cryptographic SMI software installed. 2. Restart both stack members at the same time.	The stack member with the noncryptographic EMI software is elected stack master.
Stack master election specifically determined by the cryptographic SMI software	Assuming that all stack members have the same priority value: 1. Make sure that one stack member has the cryptographic SMI software installed and that the other stack member has the noncryptographic SMI software installed. 2. Restart both stack members at the same time.	The stack member with the cryptographic SMI software 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 software image, 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 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 5-2 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 5-4, 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 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 which stack master. For information about using the Mode button and the LEDs, refer to the hardware installation guide.

Assigning Stack Member Information

These sections describe how to assign stack member information:

- Default Switch Stack Configuration, page 5-17
- Assigning a Stack Member Number, page 5-17 (optional)
- Setting the Stack Member Priority Value, page 5-18 (optional)
- Provisioning a New Member for a Switch Stack, page 5-18 (optional)

Default Switch Stack Configuration

Table 5-3 shows the default switch stack configuration.

Table 5-3 Default Switch Stack Configuration

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

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, and apply this configuration change.
Step 5	**show switch**	Verify the stack member number.
Step 6	**copy running-config startup-config**	(Optional) 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.
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 2.
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.

This example shows how to provision a Catalyst 3750G-12S 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-C3750G-12S
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 available only from the stack master. This task is only for debugging purposes.

You can access all or specific stack 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 stack members by using the **session** *stack-member-number* privileged EXEC command. The stack member number range is 1 to 9. 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`. Enter **exit** to return to the CLI session on the stack master. Only the **show** and **debug** commands are available in a CLI session to a specific stack member.

Displaying Switch Stack Information

To display configuration changes that you save after you reset a specific stack member or the switch stack, use the privileged EXEC commands listed in Table 5-4.

Table 5-4 Commands for Displaying Switch Stack Information

Command	Description
show platform stack-manager all	Displays all switch stack information.
show switch	'Displays summary information about the switch stack, including the status of provisioned switches.
show switch *stack-member-number*	Displays information about a specific member.
show switch detail	Displays detailed information about the stack ring.
show switch neighbors	Display the neighbors for the entire switch stack.
show switch stack-ports	Displays port information for the entire switch stack.
show switch stack-ring activity [**detail**]	Displays the number of frames per stack member that are sent to the stack ring. Use the **detail** keyword to display the ASIC, the receive queues, and the number of frames per stack member that are sent to the stack ring.