CHAPTER 33

Configuring Active/Standby Failover

This chapter describes how to configure active/standby failover, and it includes the following sections:

Information About Active/Standby Failover

This section describes Active/Standby failover, and it includes the following topics:

Active/Standby Failover Overview

Active/Standby failover enables you to use a standby ASA to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

Note For multiple context mode, the ASA can fail over the entire unit (including all contexts) but cannot fail over individual contexts separately.

Primary/Secondary Status and Active/Standby Status

The main differences between the two units in a failover pair are related to which unit is active and which unit is standby, namely which IP addresses to use and which unit actively passes traffic.

However, a few differences exist between the units based on which unit is primary (as specified in the configuration) and which unit is secondary:

- The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).
- The primary unit MAC addresses are always coupled with the active IP addresses. The exception to this rule occurs when the secondary unit is active and cannot obtain the primary unit MAC addresses over the failover link. In this case, the secondary unit MAC addresses are used.

Device Initialization and Configuration Synchronization

Configuration synchronization occurs when one or both devices in the failover pair boot. Configurations are always synchronized from the active unit to the standby unit. When the standby unit completes its initial startup, it clears its running configuration (except for the failover commands needed to communicate with the active unit), and the active unit sends its entire configuration to the standby unit.

The active unit is determined by the following:

- If a unit boots and detects a peer already running as active, it becomes the standby unit.
- If a unit boots and does not detect a peer, it becomes the active unit.
- If both units boot simultaneously, then the primary unit becomes the active unit, and the secondary unit becomes the standby unit.

Note If the secondary unit boots without detecting the primary unit, the secondary unit becomes the active unit and uses its own MAC addresses, because it does not know the primary unit MAC addresses. However, when the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary unit, which can cause an interruption in your network traffic. Similarly, if you swap out the primary unit with new hardware, a new MAC address is used.

Virtual MAC addresses guard against this disruption because the active MAC addresses are known to the secondary unit at startup, and remain the same in the case of new primary unit hardware. In multiple context mode, the ASA generates virtual active and standby MAC addresses by default. See the "Information About MAC Addresses" section on page 5-21 for more information. In single context mode, you can manually configure virtual MAC addresses; see the "Configuring Virtual MAC Addresses" section on page 33-14 for more information.

If you do not configure virtual MAC addresses, you might need to clear the ARP tables on connected routers to restore traffic flow. The ASA does not send gratuitous ARPs for static NAT addresses when the MAC address changes, so connected routers do not learn of the MAC address change for these addresses.

When the replication starts, the ASA console on the active unit displays the message "Beginning configuration replication: Sending to mate," and when it is complete, the ASA displays the message "End Configuration Replication to mate." During replication, commands entered on the active unit may not replicate properly to the standby unit, and commands entered on the standby unit may be overwritten by the configuration being replicated from the active unit. Avoid entering commands on either unit in the failover pair during the configuration replication process. Depending upon the size of the configuration, replication can take from a few seconds to several minutes.

Note The **crypto ca server** command and related sub-commands are not synchronized to the failover peer.

On the standby unit, the configuration exists only in running memory. To save the configuration to Flash memory after synchronization, do the following:

- For single context mode, enter the **write memory** command on the active unit. The command is replicated to the standby unit, which proceeds to write its configuration to Flash memory.
- For multiple context mode, enter the **write memory all** command on the active unit from the system execution space. The command is replicated to the standby unit, which proceeds to write its configuration to Flash memory. Using the **all** keyword with this command causes the system and all context configurations to be saved.

Note Startup configurations saved on external servers are accessible from either unit over the network and do not need to be saved separately for each unit. Alternatively, you can copy the contexts on disk from the active unit to an external server, and then copy them to disk on the standby unit, where they become available when the unit reloads.

Command Replication

Command replication always flows from the active unit to the standby unit. As commands are entered on the active unit, they are sent across the failover link to the standby unit. You do not have to save the active configuration to Flash memory to replicate the commands.

Table 33-1 lists the commands that are and are not replicated to the standby unit:

Table 33-1 Command Replication

Command Replicated to the Standby Unit	Commands Not Replicated to the Standby Unit
all configuration commands except for the **mode**, **firewall**, and **failover lan unit** commands	all forms of the **copy** command except for **copy running-config startup-config**
copy running-config startup-config	all forms of the **write** command except for **write memory**
delete	**crypto ca server** and associated sub-commands
mkdir	**debug**
rename	**failover lan unit**
rmdir	**firewall**
write memory	**mode**
—	**show**
—	**terminal pager** and **pager**

Note Changes made on the standby unit are not replicated to the active unit. If you enter a command on the standby unit, the ASA displays the message `**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit. Configurations are no longer synchronized.` This message displays even when you enter many commands that do not affect the configuration.

If you enter the **write standby** command on the active unit, the standby unit clears its running configuration (except for the failover commands used to communicate with the active unit), and the active unit sends its entire configuration to the standby unit.

For multiple context mode, when you enter the **write standby** command in the system execution space, all contexts are replicated. If you enter the **write standby** command within a context, the command replicates only the context configuration.

Replicated commands are stored in the running configuration. To save the replicated commands to the Flash memory on the standby unit, do the following:

- For single context mode, enter the **copy running-config startup-config** command on the active unit. The command is replicated to the standby unit, which proceeds to write its configuration to Flash memory.
- For multiple context mode, enter the **copy running-config startup-config** command on the active unit from the system execution space and within each context on disk. The command is replicated to the standby unit, which proceeds to write its configuration to Flash memory. Contexts with startup configurations on external servers are accessible from either unit over the network and do not need to be saved separately for each unit. Alternatively, you can copy the contexts on disk from the active unit to an external server, and then copy them to disk on the standby unit.

Failover Triggers

The unit can fail if one of the following events occurs:

- The unit has a hardware failure or a power failure.
- The unit has a software failure.
- Too many monitored interfaces fail.
- The **no failover active** command is entered on the active unit or the **failover active** command is entered on the standby unit.

Failover Actions

In Active/Standby failover, failover occurs on a unit basis. Even on systems running in multiple context mode, you cannot fail over individual or groups of contexts.

Table 33-2 shows the failover action for each failure event. For each failure event, the table shows the failover policy (failover or no failover), the action taken by the active unit, the action taken by the standby unit, and any special notes about the failover condition and actions.

Table 33-2 Failover Behavior

Failure Event	Policy	Active Action	Standby Action	Notes
Active unit failed (power or hardware)	Failover	n/a	Become active Mark active as failed	No hello messages are received on any monitored interface or the failover link.
Formerly active unit recovers	No failover	Become standby	No action	None.
Standby unit failed (power or hardware)	No failover	Mark standby as failed	n/a	When the standby unit is marked as failed, then the active unit does not attempt to fail over, even if the interface failure threshold is surpassed.
Failover link failed during operation	No failover	Mark failover interface as failed	Mark failover interface as failed	You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down.
Failover link failed at startup	No failover	Mark failover interface as failed	Become active	If the failover link is down at startup, both units become active.
Stateful Failover link failed	No failover	No action	No action	State information becomes out of date, and sessions are terminated if a failover occurs.
Interface failure on active unit above threshold	Failover	Mark active as failed	Become active	None.
Interface failure on standby unit above threshold	No failover	No action	Mark standby as failed	When the standby unit is marked as failed, then the active unit does not attempt to fail over even if the interface failure threshold is surpassed.

Optional Active/Standby Failover Settings

You can configure the following Active/Standby failover options when you initially configuring failover or after failover has been configured:

- HTTP replication with Stateful Failover—Allows connections to be included in the state information replication.
- Interface monitoring—Allows you to monitor up to 250 interfaces on a unit and control which interfaces affect your failover.
- Interface health monitoring—Enables the security appliance to detect and respond to interface failures more quickly.
- Failover criteria setup—Allows you to specify a specific number of interfaces or a percentage of monitored interfaces that must fail before failover occurs.
- Virtual MAC address configuration—Ensures that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit.

Licensing Requirements for Active/Standby Failover

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5505	Security Plus License. (Stateful failover is not supported).
ASA 5510	Security Plus License.
All other models	Base License.

Prerequisites for Active/Standby Failover

Active/Standby failover has the following prerequisites:

- Both units must be identical security appliances that are connected to each other through a dedicated failover link and, optionally, a Stateful Failover link.
- Both units must have the same software configuration and the proper license.
- Both units must be in the same mode (single or multiple, transparent or routed).

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- Supported in single and multiple context mode.
- For multiple context mode, perform all steps in the system execution space unless otherwise noted.

Firewall Mode Guidelines

- Supported in transparent and routed firewall mode.

IPv6 Guidelines

- IPv6 failover is supported.

Model Guidelines

- Stateful failover is not supported on the Cisco ASA 5505 adaptive security appliance.

Additional Guidelines and Limitations

Configuring port security on the switch(es) connected to an ASA failover pair can cause communication problems when a failover event occurs. This is because if a secure MAC address configured or learned on one secure port moves to another secure port, a violation is flagged by the switch port security feature.

ASA failover replication fails if you try to make a configuration change on two or more contexts at the same time. The workaround is to make configuration changes on each unit sequentially.

The following guidelines and limitations apply for Active/Standby failover:

- To receive packets from both units in a failover pair, standby IP addresses need to be configured on all interfaces.
- The standby IP addresses are used on the security appliance that is currently the standby unit, and they must be in the same subnet as the active IP address on the corresponding interface on the active unit.
- If you enter the **terminal pager** or **pager** commands on the active unit in a failover pair, the active console terminal pager settings change, but the standby unit settings do not. A default configuration issued on the active unit does affect behavior on the standby unit.
- When you enable interface monitoring, you can monitor up to 250 interfaces on a unit.
- By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The failover replication http command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but it could have a negative impact upon system performance.

Configuring Active/Standby Failover

This section describes how to configure Active/Standby failover and includes the following topics:

Task Flow for Configuring Active/Standby Failover

Follow these steps to configure Active/Standby Failover:

Step 1 Configure the primary unit, as shown in the "Configuring the Primary Unit" section on page 33-8.

Step 2 Configure the secondary unit, as shown in the "Configuring the Secondary Unit" section on page 33-10.

Step 3 (Optional) Configure optional Active/Standby failover settings, as shown in the "Configuring Optional Active/Standby Failover Settings" section on page 33-12.

Configuring the Primary Unit

Follow the steps in this section to configure the primary unit in a LAN-based, Active/Standby failover configuration. These steps provide the minimum configuration needed to enable failover on the primary unit.

Restrictions

Do not configure an IP address in interface configuration mode for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the **failover interface ip** command to configure a dedicated Stateful Failover interface in a later step.

Detailed Steps

	Command	Purpose

Step 1	**ip address** *active_addr netmask* **standby** *standby_addr*
	
	ipv6 address {**autoconfig** | *ipv6-prefix/prefix-length* [**eui-64**] [**standby** *ipv6-prefix*] | *ipv6-address* **link-local** [**standby** *ipv6-address*]}
	
	Example:
	`hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2`
	
	`hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64 standby 3ffe:c00:0:1::575`
		Configures the active and standby IP addresses for each data interface (routed mode), for the management IP address (transparent mode), or for the management-only interface.
		
		In routed firewall mode and for the management-only interface, enter this command in interface configuration mode for each interface.
		
		In transparent firewall mode, enter the command in global configuration mode.
		
		In multiple context mode, configure the interface addresses from within each context. Use the **change to context** command to switch between contexts. The command prompt changes to `hostname/`*`context`*`(config-if)#`, where *context* is the name of the current context. You must enter a management IP address for each context in transparent firewall multiple context mode.
		
		Each data interface can have an IPv4 address and one or more IPv6 addresses. For IPv6 addresses that use the **eui-64** option, you do not need to specify a standby address—one will be created automatically.

Step 2	**failover lan unit primary**	Designates the unit as the primary unit.

	Command	Purpose
Step 3	**failover lan interface** *if_name phy_if* **Example:** `hostname(config)# failover lan interface folink GigabitEthernet0/3`	Specifies the interface to be used as the failover interface. The *if_name* argument assigns a name to the interface specified by the *phy_if* argument. The *phy_if* argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. On the ASA 5505 adaptive ASA, the *phy_if* specifies a VLAN. This interface should not be used for any other purpose (except, optionally, the Stateful Failover link).

Step 4	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]
	
	Example:
	`hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2`
	
	`hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71`
		Assigns the active and standby IP addresses to the failover link. You can assign either an IPv4 or an IPv6 address to the interface. You cannot assign both types of addresses to the failover link.
		
		The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask.
		
		The failover link IP address and MAC address do not change at failover. The active IP address for the failover link always stays with the primary unit, while the standby IP address stays with the secondary unit.

Step 5	**interface** *phy_if*
	
	Example:
	`hostname(config)# interface vlan100`
	`hostname(config-if)# no shutdown`
		Enables the interface.

Step 6	**failover link** *if_name phy_if* **Example:** `hostname(config)# failover link statelink GigabitEthernet0/2`	(Optional) Specifies the interface to be used as the Stateful Failover link. **Note** If the Stateful Failover link uses the failover link or a data interface, then you only need to supply the *if_name* argument. The *if_name* argument assigns a logical name to the interface specified by the *phy_if* argument. The *phy_if* argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. This interface should not be used for any other purpose (except, optionally, the failover link).

	Command	Purpose

Step 7	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address/prefix* **standby***ipv6_address*]
	
	Example:
	`hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2`
	
	`hostname(config)# failover interface ip statelink 2001:a1a:b00::a0a:a70/64 standby 2001:a1a:b00::a0a:a71`
		(Optional) Assigns an active and standby IP address to the Stateful Failover link. You can assign either an IPv4 or an IPv6 address to the interface. You cannot assign both types of addresses to the Stateful Failover link.
		
		Note If the stateful Failover link uses the failover link or data interface, skip this step. You have already defined the active and standby IP addresses for the interface.
		
		The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask.
		
		The Stateful Failover link IP address and MAC address do not change at failover unless it uses a data interface. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit.

Step 8	**interface** *phy_if*
	no shutdown
	
	Example:
	`hostname(config)# interface vlan100`
	`hostname(config-if)# no shutdown`
		(Optional) Enables the interface.
		
		If the Stateful Failover link uses the failover link or a data interface, skip this step. You have already enabled the interface.

Step 9	**failover** **Example:** `hostname(config)# failover`	Enables failover.
Step 10	**copy running-config startup-config** **Example:** `hostname(config)# copy running-config startup-config`	Saves the system configuration to Flash memory.

Configuring the Secondary Unit

The only configuration required on the secondary unit is for the failover interface. The secondary unit requires these commands to communicate initially with the primary unit. After the primary unit sends its configuration to the secondary unit, the only permanent difference between the two configurations is the **failover lan unit** command, which identifies each unit as primary or secondary.

Prerequisites

When configuring LAN-based failover, you must bootstrap the secondary device to recognize the failover link before the secondary device can obtain the running configuration from the primary device

Detailed Steps

	Command	Purpose
Step 1	**failover lan interface** *if_name phy_if* **Example:** `hostname(config)# failover lan interface folink vlan100`	Specifies the interface to be used as the failover interface. (Use the same settings that you used for the primary unit.) The *if_name* argument assigns a name to the interface specified by the *phy_if* argument.

Step 2	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]
	
	Example:
	`hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2`
	
	`hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71`
		Assigns the active and standby IP addresses to the failover link. You can assign either an IPv4 or an IPv6 address to the interface. You cannot assign both types of addresses to the failover link.
		
		To receive packets from both units in a failover pair, standby IP addresses need to be configured on all interfaces.
		
		Note Enter this command exactly as you entered it on the primary unit when you configured the failover interface on the primary unit (including the same IP address).

Step 3	**interface** *phy_if*
	
	no shutdown
	
	Example:
	`hostname(config)# interface vlan100`
	`hostname(config-if)# no shutdown`
		Enables the interface.

Step 4	**failover lan unit secondary** **Example:** `hostname(config)# failover lan unit secondary`	(Optional) Designates this unit as the secondary unit: **Note** This step is optional because, by default, units are designated as secondary unless previously configured.
Step 5	**failover** **Example:** `hostname(config)# failover`	Enables failover. After you enable failover, the active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages "Beginning configuration replication: Sending to mate" and "End Configuration Replication to mate" appear on the active unit console.
Step 6	**copy running-config startup-config** **Example:** `hostname(config)# copy running-config startup-config`	Saves the configuration to Flash memory. Enter the command after the running configuration has completed replication.

Configuring Optional Active/Standby Failover Settings

This section includes the following topics:

You can configure the optional Active/Standby failover settings when initially configuring the primary unit in a failover pair (see Configuring the Primary Unit, page 33-8) or on the active unit in the failover pair after the initial configuration.

Enabling HTTP Replication with Stateful Failover

To allow HTTP connections to be included in the state information replication, you need to enable HTTP replication. Because HTTP connections are typically short-lived, and because THTTP clients typically retry failed connection attempts, HTTP connections are not automatically included in the replicated state information.

Enter the following command in global configuration mode to enable HTTP state replication when Stateful Failover is enabled.

Command	Purpose
failover replication http **Example:** `hostname (config)# failover replication http`	Enables HTTP state replication.

Disabling and Enabling Interface Monitoring

You can control which interfaces affect your failover policy by disabling the monitoring of specific interfaces and enabling the monitoring of others. This feature enables you to exclude interfaces attached to less critical networks from affecting your failover policy.

You can monitor up to 250 interfaces on a unit. By default, monitoring physical interfaces is enabled and monitoring subinterfaces is disabled.

Hello messages are exchanged during every interface poll frequency time period between the security appliance failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.

- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

For units in single configuration mode, enter the following commands to enable or disable health monitoring for specific interfaces. For units in multiple configuration mode, you must enter the commands within each security context.

Do one of the following:	
no monitor-interface *if_name* **Example:** `hostname(config)# no monitor-interface lanlink`	Disables health monitoring for an interface.
monitor-interface *if_name* **Example:** `hostname(config)# monitor-interface lanlink`	Enables health monitoring for an interface.

Configuring the Interface Health Poll Time

The ASA sends hello packets out of each data interface to monitor interface health. If the ASA does not receive a hello packet from the corresponding interface on the peer unit for over half of the hold time, then the additional interface testing begins. If a hello packet or a successful test result is not received within the specified hold time, the interface is marked as failed. Failover occurs if the number of failed interfaces meets the failover criteria.

Decreasing the poll and hold times enables the ASA to detect and respond to interface failures more quickly, but may consume more system resources.

Command	Purpose
failover polltime interface [**msec**] *time* [**holdtime** *time*] **Example:** `hostname (config): failover polltime interface msec 500 holdtime 5`	Changes the interface poll time. Valid values for poll time are from 1 to 15 seconds or, if the optional **msec** keyword is used, from 500 to 999 milliseconds. The hold time determines how long it takes from the time a hello packet is missed to when the interface is marked as failed. Valid values for the hold time are from 5 to 75 seconds. You cannot enter a hold time that is less than 5 times the poll time. If the interface link is down, interface testing is not conducted and the standby unit could become active in just one interface polling period if the number of failed interfaces meets or exceeds the configured failover criteria.

Configuring Failover Criteria

You can specify a specific number of interface or a percentage of monitored interfaces that must fail before failover occurs. By default, a single interface failure causes failover.

To the change the default failover criteria, enter the following command in global configuration mode:

Command	Purpose
failover interface-policy *num*[%] **Example:** `hostname (config)# failover interface-policy 20%`	Changes the default failover criteria. When specifying a specific number of interfaces, the *num* argument can be from 1 to 250. When specifying a percentage of interfaces, the *num* argument can be from 1 to 100.

Configuring Virtual MAC Addresses

In Active/Standby failover, the MAC addresses for the primary unit are always associated with the active IP addresses. If the secondary unit boots first and becomes active, it uses the burned-in MAC address for its interfaces. When the primary unit comes online, the secondary unit obtains the MAC addresses from the primary unit. The change can disrupt network traffic.

You can configure virtual MAC addresses for each interface to ensure that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit. If you do not specify virtual MAC addresses the failover pair uses the burned-in NIC addresses as the MAC addresses.

Note You cannot configure a virtual MAC address for the failover or Stateful Failover links. The MAC and IP addresses for those links do not change during failover.

Enter the following command on the active unit to configure the virtual MAC addresses for an interface:

Command	Purpose
failover mac address *phy_if active_mac standby_mac* **Example:** `hostname (config): failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8`	Configures the virtual MAC address for an interface. The *phy_if* argument is the physical name of the interface, such as Ethernet1. The *active_mac* and *standby_mac* arguments are MAC addresses in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. The *active_mac* address is associated with the active IP address for the interface, and the *standby_mac* is associated with the standby IP address for the interface. There are multiple ways to configure virtual MAC addresses on the ASA. When more than one method has been used to configure virtual MAC addresses, the ASA uses the following order of preference to determine which virtual MAC address is assigned to an interface: 1. The **mac-address** command (in interface configuration mode) address. 2. The **mac-address auto** command generated address. 3. The **failover mac address** command address. 4. The burned-in MAC address. Use the **show interface** command to display the MAC address used by an interface.

Controlling Failover

This sections describes how to control and monitor failover. This section includes the following topics:

Forcing Failover

To force the standby unit to become active, enter one of the following commands:

Command	Purpose
failover active **Example:** hostname# **failover active**	Forces a failover when entered on the standby unit in a failover pair. The standby unit becomes the active unit.
no failover active **Example:** hostname# **no failover active**	Forces a failover when entered on the active unit in a failover pair. The active unit becomes the standby unit.

Disabling Failover

To disable failover, enter the following command:

Command	Purpose
no failover **Example:** hostname(config)# **no failover**	Disables failover. Disabling failover on an Active/Standby pair causes the active and standby state of each unit to be maintained until you restart. For example, the standby unit remains in standby mode so that both units do not start passing traffic. To make the standby unit active (even with failover disabled), see the "Forcing Failover" section on page 33-16.

Restoring a Failed Unit

To restore a failed unit to an unfailed state, enter the following command:

Command	Purpose
failover reset **Example:** hostname(config)# **failover reset**	Restored a failed unit to an unfailed state. Restoring a failed unit to an unfailed state does not automatically make it active; restored units remain in the standby state until made active by failover (forced or natural).

Testing the Failover Functionality

To test failover functionality, perform the following steps:

Step 1 Test that your active unit is passing traffic as expected by using FTP (for example) to send a file between hosts on different interfaces.

Step 2 Force a failover by entering the following command on the active unit:

```
hostname(config)# no failover active
```

Step 3 Use FTP to send another file between the same two hosts.

Step 4 If the test was not successful, enter the **show failover** command to check the failover status.

Step 5 When you are finished, you can restore the unit to active status by enter the following command on the newly active unit:

```
hostname(config)# no failover active
```

Monitoring Active/Standby Failover

To monitor Active/Standby failover, enter one of the following commands:

Command	Purpose
`show failover`	Displays information about the failover state of the unit.
`show monitor-interface`	Displays information about the monitored interface.
`show running-config failover`	Displays the failover commands in the running configuration.

For more information about the output of the monitoring commands, refer to the *Cisco ASA 5500 Series Command Reference*.

Feature History for Active/Standby Failover

Table 33-3 lists the release history for this feature.

Table 33-3 Feature History for Optional Active/Standby Failover Settings

Feature Name	Releases	Feature Information
This feature was introduced.	7.0	This feature was introduced.
IPv6 support for failover added.	8.2(2)	The following commands were modified: **failover interface ip**, **show failover**, **ipv6 address**, **show monitor-interface**.