



CHAPTER 32

Information About High Availability

This chapter provides an overview of the failover features that enable you to achieve high availability on the Cisco 5500 series adaptive security appliances. For information about configuring high availability, see [Chapter 34, “Configuring Active/Active Failover”](#) or [Chapter 33, “Configuring Active/Standby Failover.”](#)

This chapter includes the following sections:

- [Information About Failover and High Availability, page 32-1](#)
- [Failover System Requirements, page 32-2](#)
- [Failover and Stateful Failover Links, page 32-3](#)
- [Active/Active and Active/Standby Failover, page 32-9](#)
- [Stateless \(Regular\) and Stateful Failover, page 32-10](#)
- [Transparent Firewall Mode Requirements, page 32-11](#)
- [Auto Update Server Support in Failover Configurations, page 32-12](#)
- [Failover Health Monitoring, page 32-14](#)
- [Failover Feature/Platform Matrix, page 32-16](#)
- [Failover Times by Platform, page 32-16](#)
- [Failover Messages, page 32-17](#)

Information About Failover and High Availability

Configuring high availability requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a Stateful Failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The ASA supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover.

With Active/Active failover, both units can pass network traffic. This also lets you configure traffic sharing on your network. Active/Active failover is available only on units running in multiple context mode.

With Active/Standby failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either single or multiple context mode.

Both failover configurations support stateful or stateless (regular) failover.

**Note**

When the security appliance is configured for Active/Active stateful failover, you cannot enable IPsec or SSL VPN. Therefore, these features are unavailable. VPN failover is available for Active/Standby failover configurations only.

Failover System Requirements

This section describes the hardware, software, and license requirements for ASAs in a failover configuration.

This section contains the following topics:

- [Hardware Requirements, page 32-2](#)
- [Software Requirements, page 32-2](#)
- [Licensing Requirements, page 32-3](#)

Hardware Requirements

The two units in a failover configuration must be the same model, have the same number and types of interfaces, and the same SSMs installed (if any). Both units must have the same amount of RAM memory installed.

If you are using units with different Flash memory sizes in your failover configuration, make sure the unit with the smaller Flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger Flash memory to the unit with the smaller Flash memory will fail.

Software Requirements

The two units in a failover configuration must be in the same operating modes (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version. However, you can use different versions of the software during an upgrade process; for example, you can upgrade one unit from Version 7.0(1) to Version 7.0(2) and have failover remain active. We recommend upgrading both units to the same version to ensure long-term compatibility.

See [“Performing Zero Downtime Upgrades for Failover Pairs” section on page 78-5](#) for more information about upgrading the software on a failover pair.

Licensing Requirements

The licensed features (such as SSL VPN peers or security contexts, for example) on both units participating in failover must be identical.

Failover and Stateful Failover Links

This section describes the failover and the Stateful Failover links, which are dedicated connections between the two units in a failover configuration. This section includes the following topics:

- [Failover Link, page 32-3](#)
- [Stateful Failover Link, page 32-4](#)
- [Avoiding Interrupted Failover Links, page 32-5](#)

Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization



Caution

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

You can use any unused Ethernet interface on the device as the failover link; however, you cannot specify an interface that is currently configured with a name. The LAN failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface should only be used for the LAN failover link (and optionally for the Stateful Failover link).

Connect the LAN failover link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the LAN failover interfaces of the ASA.
- Using a crossover Ethernet cable to connect the appliances directly, without the need for an external switch.



Note

When you use a crossover cable for the LAN failover link, if the LAN interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which interface failed and caused the link to come down.

**Note**

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

Stateful Failover Link

To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- You can use a dedicated Ethernet interface for the Stateful Failover link.
- If you are using LAN-based failover, you can share the failover link.
- You can share a regular data interface, such as the inside interface. However, this option is not recommended.

If you are using a dedicated Ethernet interface for the Stateful Failover link, you can use either a switch or a crossover cable to directly connect the units. If you use a switch, no other hosts or routers should be on this link.

**Note**

Enable the PortFast option on Cisco switch ports that connect directly to the ASA.

If you use a data interface as the Stateful Failover link, you receive the following warning when you specify that interface as the Stateful Failover link:

```
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
Sharing Stateful failover interface with regular data interface is not
a recommended configuration due to performance and security concerns.
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
```

Sharing a data interface with the Stateful Failover interface can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment.

**Note**

Using a data interface as the Stateful Failover interface is supported in single context, routed mode only.

In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.

**Note**

The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.

**Caution**

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords, and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

Failover Interface Speed for Stateful Links

If you use the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.

Use the following failover interface speed guidelines for the adaptive security appliances:

- Cisco ASA 5510
 - Stateful link speed can be 100 Mbps, even though the data interface can operate at 1 Gigabit due to the CPU speed limitation.
- Cisco ASA 5520/5540/5550
 - Stateful link speed should match the fastest data link.
- Cisco ASA 5580/5585
 - Use only non-management 1 Gigabit ports for the stateful link because management ports have lower performance and cannot meet the performance requirement for stateful failover.

For optimum performance when using long distance LAN failover, the latency for the failover link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than 10 milliseconds, some performance degradation occurs due to retransmission of failover messages.

All platforms support sharing of failover heartbeat and stateful link, but we recommend using a separate heartbeat link on systems with high Stateful Failover traffic.

Avoiding Interrupted Failover Links

Because adaptive security appliances use failover LAN interfaces to transport messages between primary and secondary units, if a failover LAN interface is down (that is, the physical link is down or the switch used to connect the LAN interface is down), then the adaptive security appliance failover operation is affected until the health of the failover LAN interface is restored.

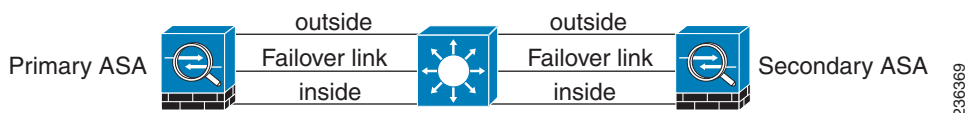
In the event that all communication is cut off between the units in a failover pair, both units go into the active state, which is expected behavior. When communication is restored and the two active units resume communication through the failover link or through any monitored interface, the primary unit remains active, and the secondary unit immediately returns to the standby state. This relationship is established regardless of the health of the primary unit.

Because of this behavior, stateful flows that were passed properly by the secondary active unit during the network split are now interrupted. To avoid this interruption, failover links and data interfaces should travel through different paths to decrease the chance that all links fail at the same time. In the event that only one failover link is down, the adaptive security appliance takes a sample of the interface health, exchanges this information with its peer through the data interface, and performs a switchover if the active unit has a greater number of down interfaces. Subsequently, the failover operation is suspended until the health of the failover link is restored.

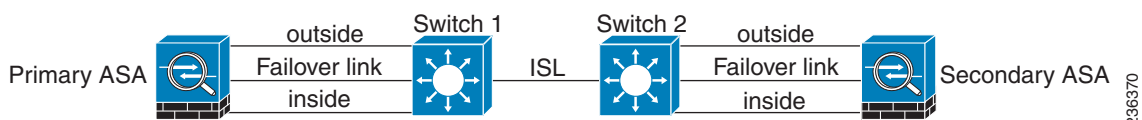
Depending upon their network topologies, several primary/secondary failure scenarios exist in adaptive security appliance failover pairs, as shown in the following scenarios.

Scenario 1—Not Recommended

If a single switch or a set of switches are used to connect both failover and data interfaces between two adaptive security appliances, then when a switch or inter-switch-link is down, both adaptive security appliances become active. Therefore, the following two connection methods shown in [Figure 32-1](#) and [Figure 32-2](#) are NOT recommended.

Figure 32-1 Connecting with a Single Switch—Not Recommended

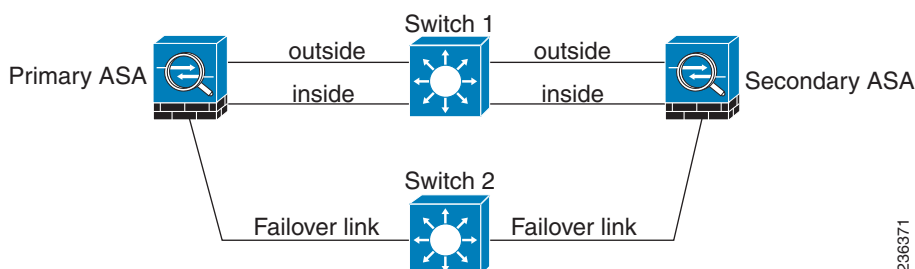
236369

Figure 32-2 Connecting with a Double Switch—Not Recommended

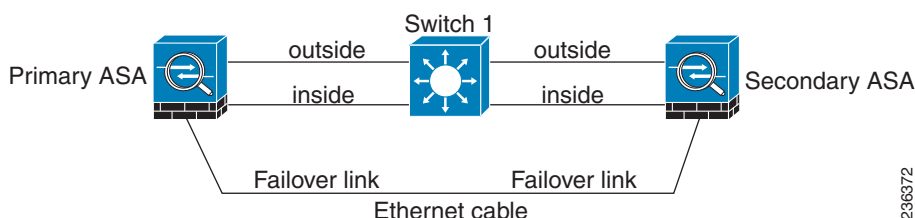
236370

Scenario 2—Recommended

To make the ASA failover pair resistant to failover LAN interface failure, we recommend that failover LAN interfaces NOT use the same switch as the data interfaces, as shown in the preceding connections. Instead, use a different switch or use a direct cable to connect two adaptive security appliance failover interfaces, as shown in [Figure 32-3](#) and [Figure 32-4](#).

Figure 32-3 Connecting with a Different Switch

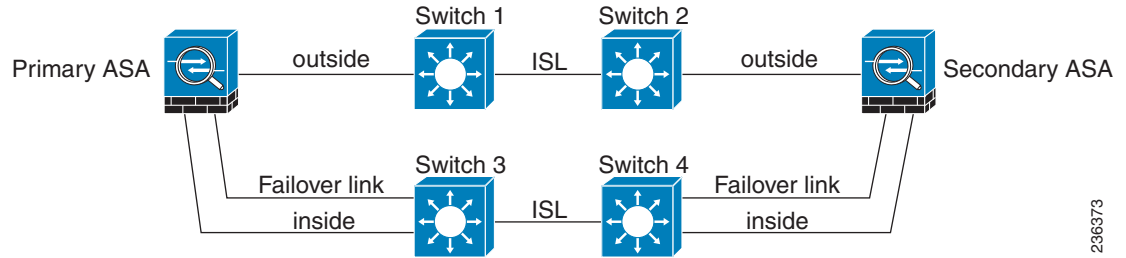
236371

Figure 32-4 Connecting with a Cable

236372

Scenario 3—Recommended

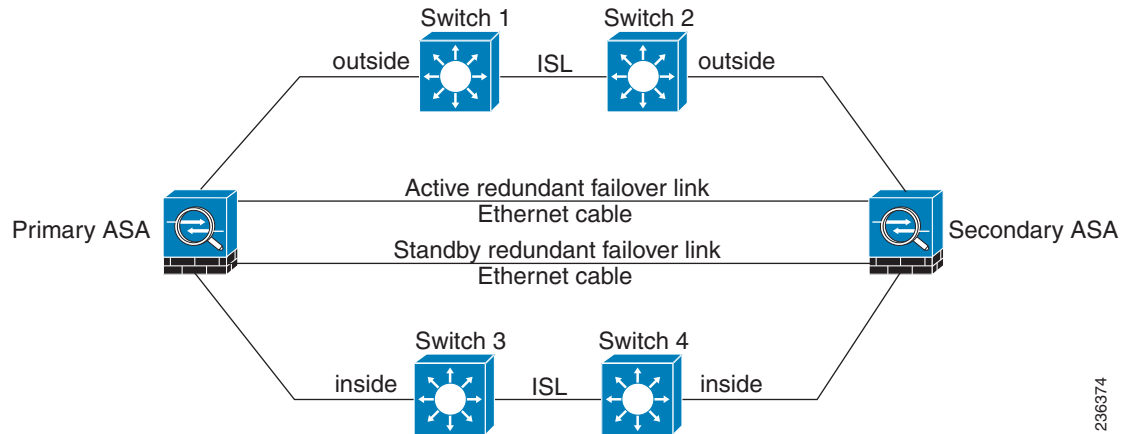
If the adaptive security appliance data interfaces are connected to more than one set of switches, then a failover LAN interface can be connected to one of the switches, preferably the switch on the secure side of network, as shown in [Figure 32-5](#).

Figure 32-5 Connecting with a Secure Switch

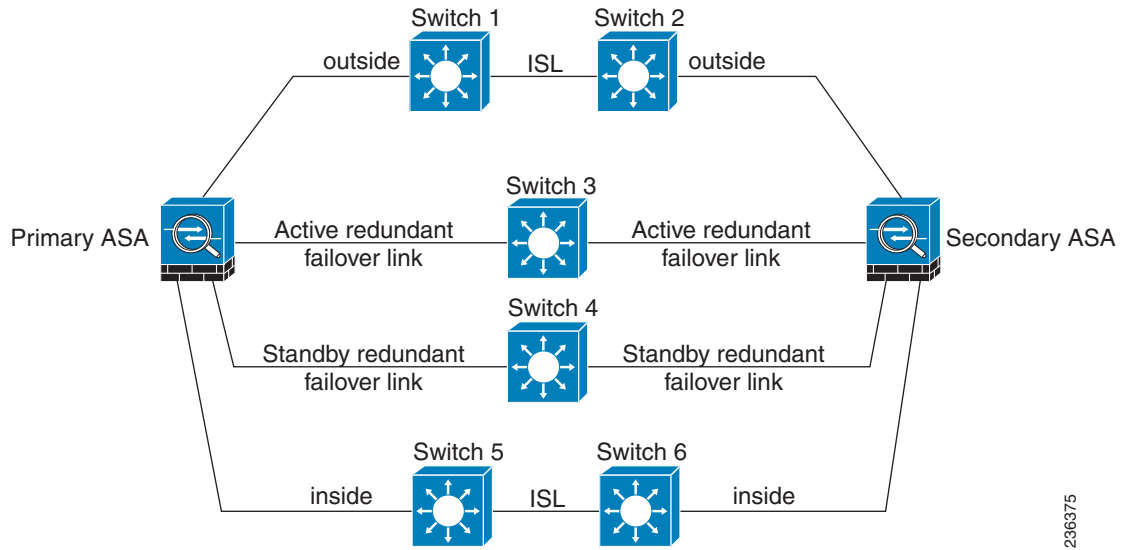
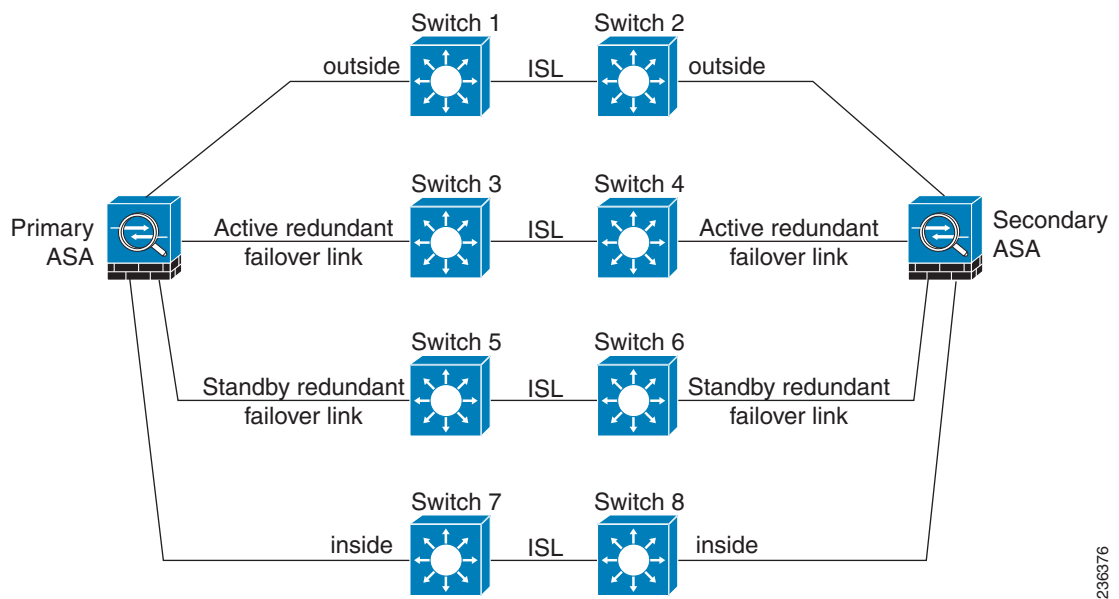
236373

Scenario 4—Recommended

The most reliable failover configurations use a redundant interface on the failover LAN interface, as shown in [Figure 32-6](#), [Figure 32-7](#), and [Figure 32-8](#).

Figure 32-6 Connecting with Ethernet Cables

236374

Figure 32-7 Connecting with Redundant Interfaces**Figure 32-8 Connecting with Inter-switch Links**

Active/Active and Active/Standby Failover

Two types of failover configurations are supported by the ASA: Active/Standby and Active/Active.

In Active/Standby failover, one unit is the active unit. It passes traffic. The standby unit does not actively pass traffic. When a failover occurs, the active unit fails over to the standby unit, which then becomes active. You can use Active/Standby failover for ASAs in single or multiple context mode, although it is most commonly used for ASAs in single context mode.

Active/Active failover is only available to ASAs in multiple context mode. In an Active/Active failover configuration, both ASAs can pass network traffic. In Active/Active failover, you divide the security contexts on the ASA into *failover groups*. A failover group is simply a logical group of one or more security contexts. Each group is assigned to be active on a specific ASA in the failover pair. When a failover occurs, it occurs at the failover group level.

For more detailed information about each type of failover, refer the following information:

- [Chapter 33, “Configuring Active/Standby Failover”](#)
- [Chapter 34, “Configuring Active/Active Failover”](#)

Determining Which Type of Failover to Use

The type of failover you choose depends upon your ASA configuration and how you plan to use the ASAs.

If you are running the ASA in single mode, then you can use only Active/Standby failover. Active/Active failover is only available to ASAs running in multiple context mode.

If you are running the ASA in multiple context mode, then you can configure either Active/Active failover or Active/Standby failover.

- To allow both members of the failover pair to share the traffic, use Active/Active failover. Do not exceed 50% load on each device.
- If you do not want to share the traffic in this way, use Active/Standby or Active/Active failover.

[Table 32-1](#) provides a comparison of some of the features supported by each type of failover configuration:

Table 32-1 Failover Configuration Feature Support

Feature	Active/Active	Active/Standby
Single Context Mode	No	Yes
Multiple Context Mode	Yes	Yes
Traffic Sharing Network Configurations	Yes	No
Unit Failover	Yes	Yes
Failover of Groups of Contexts	Yes	No
Failover of Individual Contexts	No	No

Stateless (Regular) and Stateful Failover

The ASA supports two types of failover, regular and stateful. This section includes the following topics:

- [Stateless \(Regular\) Failover, page 32-10](#)
- [Stateful Failover, page 32-10](#)

Stateless (Regular) Failover

When a failover occurs, all active connections are dropped. Clients need to reestablish connections when the new active unit takes over.



Note

In Release 8.0 and later, some configuration elements for WebVPN (such as bookmarks and customization) use the VPN failover subsystem, which is part of Stateful Failover. You must use Stateful Failover to synchronize these elements between the members of the failover pair. Stateless (regular) failover is not recommended for WebVPN.

Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

[Table 32-2](#) list the state information that is and is not passed to the standby unit when Stateful Failover is enabled.

Table 32-2 State Information

State Information Passed to Standby Unit	State Information Not Passed to Standby Unit
NAT translation table	The HTTP connection table (unless HTTP replication is enabled).
TCP connection states	The user authentication (uauth) table. Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
UDP connection states	The routing tables. After a failover occurs, some packets may be lost or routed out of the wrong interface (the default route) while the dynamic routing protocols rediscover routes.
The ARP table	State information for Security Service Modules.
The Layer 2 bridge table (when running in transparent firewall mode)	DHCP server address leases.

Table 32-2 State Information

State Information Passed to Standby Unit	State Information Not Passed to Standby Unit
The HTTP connection states (if HTTP replication is enabled)	Stateful failover for phone proxy. When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and reregister with the active unit. The call must be re-established.
The ISAKMP and IPsec SA table	—
GTP PDP connection database	—
SIP signalling sessions	—

The following WebVPN features are not supported with Stateful Failover:

- Smart Tunnels
- Port Forwarding
- Plugins
- Java Applets
- IPv6 clientless or Anyconnect sessions
- Citrix authentication (Citrix users must reauthenticate after failover)

**Note**

If failover occurs during an active Cisco IP SoftPhone session, the call remains active because the call session state information is replicated to the standby unit. When the call is terminated, the IP SoftPhone client loses connection with the Cisco CallManager. This occurs because there is no session information for the CTIQBE hangup message on the standby unit. When the IP SoftPhone client does not receive a response back from the Call Manager within a certain time period, it considers the CallManager unreachable and unregisters itself.

For VPN failover, VPN end-users should not have to reauthenticate or reconnect the VPN session in the event of a failover. However, applications operating over the VPN connection could lose packets during the failover process and not recover from the packet loss.

Transparent Firewall Mode Requirements

When the active unit fails over to the standby unit, the connected switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss while the port is in a blocking state, you can configure one of the following workarounds depending on the switch port mode:

- Access mode—Enable the STP PortFast feature on the switch:

```
interface interface_id
spanning-tree portfast
```

The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

- Trunk mode—Block BPDUs on the ASA on both the inside and outside interfaces:

```
access-list id ethertype deny bpdud
access-group id in interface inside_name
access-group id in interface outside_name
```

Blocking BPDUs disables STP on the switch. Be sure not to have any loops involving the ASA in your network layout.

If neither of the above options are possible, then you can use one of the following less desirable workarounds that impacts failover functionality or STP stability:

- Disable failover interface monitoring.
- Increase failover interface holdtime to a high value that will allow STP to converge before the ASAs fail over.
- Decrease STP timers to allow STP to converge faster than the failover interface holdtime.

Auto Update Server Support in Failover Configurations

You can use Auto Update Server to deploy software images and configuration files to ASAs in an Active/Standby failover configuration. To enable Auto Update on an Active/Standby failover configuration, enter the Auto Update Server configuration on the primary unit in the failover pair. See the [“Configuring Auto Update Support” section on page 78-19](#), for more information.

The following restrictions and behaviors apply to Auto Update Server support in failover configurations:

- Only single mode, Active/Standby configurations are supported.
- When loading a new platform software image, the failover pair stops passing traffic.
- When using LAN-based failover, new configurations must not change the failover link configuration. If they do, communication between the units will fail.
- Only the primary unit will perform the call home to the Auto Update Server. The primary unit must be in the active state to call home. If it is not, the ASA automatically fails over to the primary unit.
- Only the primary unit downloads the software image or configuration file. The software image or configuration is then copied to the secondary unit.
- The interface MAC address and hardware-serial ID is from the primary unit.
- The configuration file stored on the Auto Update Server or HTTP server is for the primary unit only.

Auto Update Process Overview

The following is an overview of the Auto Update process in failover configurations. This process assumes that failover is enabled and operational. The Auto Update process cannot occur if the units are synchronizing configurations, if the standby unit is in the failed state for any reason other than SSM card failure, or if the failover link is down.

1. Both units exchange the platform and ASDM software checksum and version information.
2. The primary unit contacts the Auto Update Server. If the primary unit is not in the active state, the ASA first fails over to the primary unit and then contacts the Auto Update Server.
3. The Auto Update Server replies with software checksum and URL information.
4. If the primary unit determines that the platform image file needs to be updated for either the active or standby unit, the following occurs:

- a. The primary unit retrieves the appropriate files from the HTTP server using the URL from the Auto Update Server.
 - b. The primary unit copies the image to the standby unit and then updates the image on itself.
 - c. If both units have new image, the secondary (standby) unit is reloaded first.
 - If hitless upgrade can be performed when secondary unit boots, then the secondary unit becomes the active unit and the primary unit reloads. The primary unit becomes the active unit when it has finished loading.
 - If hitless upgrade cannot be performed when the standby unit boots, then both units reload at the same time.
 - d. If only the secondary (standby) unit has new image, then only the secondary unit reloads. The primary unit waits until the secondary unit finishes reloading.
 - e. If only the primary (active) unit has new image, the secondary unit becomes the active unit, and the primary unit reloads.
 - f. The update process starts again at step 1.
5. If the ASA determines that the ASDM file needs to be updated for either the primary or secondary unit, the following occurs:
 - a. The primary unit retrieves the ASDM image file from the HTTP server using the URL provided by the Auto Update Server.
 - b. The primary unit copies the ASDM image to the standby unit, if needed.
 - c. The primary unit updates the ASDM image on itself.
 - d. The update process starts again at step 1.
 6. If the primary unit determines that the configuration needs to be updated, the following occurs:
 - a. The primary unit retrieves the configuration file from the using the specified URL.
 - b. The new configuration replaces the old configuration on both units simultaneously.
 - c. The update process begins again at step 1.
 7. If the checksums match for all image and configuration files, no updates are required. The process ends until the next poll time.

Monitoring the Auto Update Process

You can use the **debug auto-update client** or **debug fover cmd-exe** commands to display the actions performed during the Auto Update process. The following is sample output from the **debug auto-update client** command.

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
  Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
  Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
  Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
```

```

auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419

```

The following system log message is generated if the Auto Update process fails:

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

The *file* is “image”, “asdm”, or “configuration”, depending on which update failed. The *version* is the version number of the update. And the *reason* is the reason the update failed.

Failover Health Monitoring

The ASA monitors each unit for overall health and for interface health. See the following sections for more information about how the ASA performs tests to determine the state of each unit:

- [Unit Health Monitoring, page 32-15](#)
- [Interface Monitoring, page 32-15](#)

Unit Health Monitoring

The ASA determines the health of the other unit by monitoring the failover link. When a unit does not receive three consecutive hello messages on the failover link, the unit sends interface hello messages on each interface, including the failover interface, to validate whether or not the peer interface is responsive. The action that the ASA takes depends upon the response from the other unit. See the following possible actions:

- If the ASA receives a response on the failover interface, then it does not fail over.
- If the ASA does not receive a response on the failover link, but it does receive a response on another interface, then the unit does not failover. The failover link is marked as failed. You should restore the failover link as soon as possible because the unit cannot fail over to the standby while the failover link is down.
- If the ASA does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed.

**Note**

If a failed unit does not recover, and you believe it should not be failed, you can reset the state by entering the **failover reset** command. If the failover condition persists, however, the unit will fail again.

You can configure the frequency of the hello messages and the hold time before failover occurs. A faster poll time and shorter hold time speed the detection of unit failures and make failover occur more quickly, but it can also cause “false” failures due to network congestion delaying the keepalive packets.

Interface Monitoring

You can monitor up to 250 interfaces divided between all contexts. You should monitor important interfaces. For example, you might configure one context to monitor a shared interface. (Because the interface is shared, all contexts benefit from the monitoring.)

When a unit does not receive hello messages on a monitored interface for half of the configured hold time, it runs the following tests:

1. **Link Up/Down test**—A test of the interface status. If the Link Up/Down test indicates that the interface is operational, then the ASA performs network tests. The purpose of these tests is to generate network traffic to determine which (if either) unit has failed. At the start of each test, each unit clears its received packet count for its interfaces. At the conclusion of each test, each unit looks to see if it has received any traffic. If it has, the interface is considered operational. If one unit receives traffic for a test and the other unit does not, the unit that received no traffic is considered failed. If neither unit has received traffic, then the next test is used.
2. **Network Activity test**—A received network activity test. The unit counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the ARP test begins.
3. **ARP test**—A reading of the unit ARP cache for the 2 most recently acquired entries. One at a time, the unit sends ARP requests to these machines, attempting to stimulate network traffic. After each request, the unit counts all received traffic for up to 5 seconds. If traffic is received, the interface is considered operational. If no traffic is received, an ARP request is sent to the next machine. If at the end of the list no traffic has been received, the ping test begins.
4. **Broadcast Ping test**—A ping test that consists of sending out a broadcast ping request. The unit then counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops.

If an interface has IPv4 and IPv6 addresses configured on it, the ASA uses the IPv4 addresses to perform the health monitoring.

If an interface has only IPv6 addresses configured on it, then the ASA uses IPv6 neighbor discovery instead of ARP to perform the health monitoring tests. For the broadcast ping test, the ASA uses the IPv6 all nodes address (FE02::1).

If all network tests fail for an interface, but this interface on the other unit continues to successfully pass traffic, then the interface is considered to be failed. If the threshold for failed interfaces is met, then a failover occurs. If the other unit interface also fails all the network tests, then both interfaces go into the “Unknown” state and do not count towards the failover limit.

An interface becomes operational again if it receives any traffic. A failed ASA returns to standby mode if the interface failure threshold is no longer met.

**Note**

If a failed unit does not recover and you believe it should not be failed, you can reset the state by entering the **failover reset** command. If the failover condition persists, however, the unit will fail again.

Failover Feature/Platform Matrix

Table 32-3 shows the failover features supported by each hardware platform.

Table 32-3 Failover Feature Support by Platform

Platform	LAN-Based Failover	Stateful Failover	Active/Standby Failover	Active/Active Failover
Cisco ASA 5505 ASA	Yes	No	Yes	No
Cisco ASA 5500 series ASA (other than the ASA 5505)	Yes	Yes	Yes	Yes

Failover Times by Platform

Table 32-4 shows the minimum, default, and maximum failover times for the Cisco ASA 5500 series ASA.

Table 32-4 Cisco ASA 5500 Series Adaptive Security Appliance Failover Times

Failover Condition	Minimum	Default	Maximum
Active unit loses power or stops normal operation.	800 milliseconds	15 seconds	45 seconds
Active unit main board interface link down.	500 milliseconds	5 seconds	15 seconds
Active unit 4GE card interface link down.	2 seconds	5 seconds	15 seconds
Active unit IPS or CSC card fails.	2 seconds	2 seconds	2 seconds
Active unit interface up, but connection problem causes interface testing.	5 seconds	25 seconds	75 seconds

Failover Messages

When a failover occurs, both ASAs send out system messages. This section includes the following topics:

- [Failover System Messages, page 32-17](#)
- [Debug Messages, page 32-17](#)
- [SNMP, page 32-17](#)

Failover System Messages

The ASA issues a number of system messages related to failover at priority level 2, which indicates a critical condition. To view these messages, see the *Cisco ASA 5500 Series System Log Messages* to enable logging and to see descriptions of the system messages.

**Note**

During switchover, failover logically shuts down and then bring up interfaces, generating syslog 411001 and 411002 messages. This is normal activity.

Debug Messages

To see debug messages, enter the **debug fover** command. See the *Cisco ASA 5500 Series Command Reference* for more information.

**Note**

Because debugging output is assigned high priority in the CPU process, it can drastically affect system performance. For this reason, use the **debug fover** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC.

SNMP

To receive SNMP syslog traps for failover, configure the SNMP agent to send SNMP traps to SNMP management stations, define a syslog host, and compile the Cisco syslog MIB into your SNMP management station. See the **snmp-server** and **logging** commands in the *Cisco Security Appliance Command Reference* for more information.

