This whitepaper describes security appliance failover options and how to configure them with Cisco Adaptive Security Device Manager (ASDM).

Understanding Failover

This topic describes what failover is and how it works.

**Hardware and Stateful Failover**

- **Hardware (Stateless) failover**: Hardware (Stateless) failover provides hardware redundancy. When the active security appliance fails, the standby security appliance becomes active. All connections are lost, and client applications must perform a new connection to restart communication through the security appliance. The client applications disconnection happens because the active security appliance does not pass the stateful connection information to the standby security appliance. Failover messages are exchanged over a LAN-based failover connection.

- **Stateful failover**: The stateful failover feature passes per-connection stateful information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Most end-user applications are not required to do a reconnect to keep the same communication session. The state information passed to the standby unit includes information such as the global pool addresses and status; connection and translation information and status; the negotiated H.323, session initiation protocol (SIP), and Media Gateway Control Protocol (MGCP) User Datagram Protocol (UDP) ports; the port allocation map for Port Address Translation (PAT); and other details necessary to let the standby unit take over processing if the primary unit fails.
Hardware failover protects the network should the primary go offline.

- Active/Standby: Only one unit can be actively processing traffic while the other is a hot standby.

The hardware (stateless) failover function for the security appliance provides a safeguard in case a security appliance fails. Specifically, when one security appliance fails, another immediately takes its place. In the failover process, there are two security appliances: the primary and the secondary. The primary security appliance functions as the active security appliance, performing normal network functions. The secondary security appliance functions as the standby security appliance, ready to take control should the active security appliance fail to perform. When the primary security appliance fails, the secondary security appliance becomes active while the primary security appliance enters the failed state. This entire process is called failover.

There are two types of hardware failover: active/standby and active/active. In active/standby, one security appliance is actively processing traffic while the other is a hot standby. All traffic flows through the active security appliance.

In the example in the figure, the active/standby scenario consists of two security appliances, the primary and secondary. In the example on the left, the primary unit is active and passing traffic. The secondary unit is functioning as the standby unit. In the example on the right in the figure, the primary failed. The secondary became active and passes the data.
Hardware Failover: Active/Active

- Hardware failover protects the network should the primary go offline.
- With active/active failover, both units can process traffic and serve as backup units.
- Active/active failover allows for load sharing of traffic on your network.

Active/Active hardware failover mode is only available on security appliances running in multiple contexts mode.

In active/active hardware failover, an administrator logically divides a security appliance into multiple contexts. Each security appliance can process traffic for a group of contexts and also serve as a backup unit for a different group of contexts at the same time. In the example on the left in the figure, each security appliance is composed of two contexts (context 1 and context 2). Under normal conditions, each security appliance has one active and one standby context. The security appliance on the left is actively processing traffic for context 1, and is in standby state for context 2. The security appliance on the right is actively processing traffic for context 2, and is in standby state for context 1.

In the active/active example on the right in the figure, the primary security appliance (on the left) failed. The former standby context (context 1) in the secondary security appliance (on the right) transitioned to the active state. Now both contexts in the secondary security appliance are active (active/active). The security appliance on the right now processes 100 percent of the traffic for both contexts.
Failover Requirements

Cisco ASA 5505, 5510, 5520, 5540, and 5550 Security Appliances and Cisco PIX 515E, 525, and 535 Security Appliances can be configured for failover support. For failover to work, a pair of security appliances must be identical in the following requirements:

- **Platform type**
- **Number and types of interfaces**
- **Software version**: For PIX Firewall Version 6.3 and earlier, software versions must be identical. Starting with Cisco ASA and PIX Security Appliance Software Version 7.0 and later, the versions between failover pairs do not need to be the same. This enables you to upgrade the operating software of the standby unit while the other member of the failover pair is active. Both security appliances must be a minimum of Version 7.0(1).
- **Operating mode**: Both security appliances must be in the same operating mode (routed or transparent, single or multiple context).
- **Licensed features**: Types of encryption, number of contexts, number of virtual private network (VPN) peers, and so on.
- **Flash memory**
- **Amount of RAM**
- **Proper licensing**:

  - **Cisco ASA security appliance**: The ASA 5505 and 5510 Security Appliances support failover only with a Security Plus license. With this license, the ASA 5505 Security Appliance supports stateless active/standby failover only; however, the ASA 5510 Security Appliance supports both active/standby and active/active failover. The ASA 5520, 5540, and 5550 Security Appliances support active/standby and active/active failover with the base license.
Failover Health Monitoring

Unit Health Monitoring:
- The security appliance determines the health of the other unit by monitoring the failover link

Interface Health 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:
- Link up/down test: Testing the network interface card itself
- Network activity test: Testing received network activity
- ARP test: Reading the security appliance ARP cache for the 10 most recently acquired entries
- Broadcast ping test: Sending out a broadcast ping request

Both the primary and secondary security appliances send special failover hello packets to each other over the LAN-based failover interface every second (the default), to make sure that everything is working. The hellos are also sent on all monitored interfaces so the security appliance can determine the health of each monitored interface.

Note
The Cisco ASA security appliance sends hello packets every second by default; the Cisco PIX security appliance sends hello packets every 15 seconds by default.

Unit Health Monitoring:
The security appliance 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 additional testing packets on all monitored interfaces, including the failover interface. The action the security appliance takes depends on the response from the other unit.

- If the security appliance receives a response on the failover interface, then it does not fail over.
- If the security appliance does not receive a response on the failover link, but receives a response on another monitored 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 security appliance does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed.

A configurable hold timer must expire before declaring the other unit failed. Default hold timer for PIX is 45 seconds and for the ASA is 15 seconds.
Interface Health Monitoring:

You can monitor up to 250 interfaces that are 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. At the start of each test, each security appliance clears its received packet count for its interfaces.

- **Link up/down**: This is a test of the network interface card (NIC) itself. If an interface card is not plugged into an operational network, it is considered failed; for example, the hub or switch has failed, the network has a failed port, or a cable is unplugged. If this test does not find anything, the network activity test begins.

- **Network activity**: This is a test of received network activity. The security appliance counts all received packets for an interval of 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 Address Resolution Protocol (ARP) test begins.

- **ARP**: The ARP test consists of reading the ARP cache of the security appliance for the 10 most recently acquired entries. The security appliance sends ARP requests one at a time to these machines, attempting to stimulate network traffic. After each request, the security appliance 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.

- **Broadcast ping**: The ping test consists of sending out a broadcast ping request. The security appliance 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 no traffic is received, the interface is considered failed.

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 security appliance returns to standby mode if the interface failure threshold is no longer met.
The security appliances communicate failover information between themselves. The communication identifies the unit as primary or secondary, identifies the power status of the other unit, and serves as a link for various failover communications between the two units. Most the failover communications are passed over dedicated failover links. The following are the two types of failover links for the ASA:

- **LAN-based failover**: With LAN-based failover, failover messages are transmitted over Ethernet connections. LAN-based failover provides message encryption and authentication using a manual pre-shared key for added security. LAN-based failover requires an additional Ethernet interface on each security appliance to be used exclusively for passing failover communications between two security appliance units. The LAN failover interface can be connected to either a 100BASE-TX or 1000BASE-TX full duplex on a dedicated switch or dedicated VLAN of a switch. In Cisco ASA and PIX Security Appliance Software Version 7.0, it can also be a crossover Ethernet cable on the Cisco PIX security appliance platform and straight or crossover cable on the Adaptive Security Algorithm (ASA) platform. Data is passed over the dedicated interface using IP protocol 105. No hosts or routers should be on this interface.

- **Stateful failover**: The stateful failover interface passes per-connection stateful information to the standby unit. Stateful failover requires an additional Ethernet interface on each security appliance with a minimum speed of 100-Mb/s full duplex to be used exclusively for passing state information between the two security appliance units. The stateful failover interface can be connected to either a 100BASE-T or 1000BASE-TX full duplex on a dedicated switch or dedicated VLAN of a switch. Starting with Version 7.0, the cable can also be a crossover Ethernet cable. The LAN-Based failover interface can also be used as the stateful failover interface.
Redundant Interfaces

- A redundant interface consists of a pair of physical interfaces.
- One physical interface serves as the active interface, and the other serves as a standby.
- If the active interface fails, the standby interface becomes active.
- Redundant interfaces can be used alone for increased reliability or along with device-level failover for an additional layer of redundancy.
- A redundant interface is considered in failure state only when both underlying physical interfaces fail.
- Redundant interface failure triggers device-level failover, if it is configured.

The redundant interface feature is separate from device-level failover, but you can use it alone or with device-level failover to increase the reliability of your security appliance. A redundant interface is a logical interface that is made up of two physical interfaces. One physical interface serves as the active interface while the other serves as the standby. When the active interface fails, the standby interface becomes active and starts passing traffic. It does not load-share across both interfaces at the same time. A redundant interface is considered in failure state only when both of the underlying physical interfaces fail.

You can configure up to eight redundant interface pairs. When you configure redundant interfaces, all security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.
Active/Standby LAN-Based Failover Configuration

This topic describes how to configure active/standby failover.

In active/standby failover, there are two security appliances that are interconnected with a failover cable: a primary unit and a secondary unit. In the top example in the figure, the primary security appliance is active and passing traffic. The IP addresses of the outside and inside interfaces are 192.168.1.2 and 10.0.1.1. The secondary unit is on standby and has interface IP addresses of 192.168.1.7 and 10.0.1.7. In the bottom example in the figure, the primary security appliance failed. In the active/standby application, the type of failover unit did not change; the primary unit is still the primary unit. What changed are the roles: active, standby, and failed. The secondary unit is now the active unit passing the traffic. The primary unit is now the failed unit. The interface IP addresses have also changed; they were swapped between the primary and secondary security appliances. The secondary unit inherited the IP addresses of the primary unit, 192.168.1.2 and 10.0.1.1. The secondary unit also inherited the MAC addresses of the primary unit.

Part of configuring active/standby failover is configuring standby IP addresses. These are the addresses used by the security appliance that is currently in the standby role. When configuring standby IP addresses, remember that both security appliances require the same access to all networks—inside, outside, Demilitarized Zone (DMZ), and so on. The primary and secondary security appliances must be on the same subnets for mutual networks (inside, outside, DMZ, and so on).
LAN-Based Active/Standby Failover Overview

LAN-based failover:
- Provides long-distance failover functionality
- Uses an Ethernet cable
- Requires a dedicated LAN interface, but the same interface can be used for stateful failover
- Enables you to use a dedicated switch, hub, or VLAN, or a crossover cable to connect the two security appliances
- Uses message encryption and authentication to secure failover transmissions

With LAN-based failover, an Ethernet cable can be used to replicate configuration from the primary security appliance to the secondary security appliance. LAN-based failover allows you to use a dedicated switch, hub, or VLAN, or a crossover cable to connect the two security appliances.

The same LAN interface that is used for LAN-based failover can also be used for stateful failover. However, the interface needs enough capacity to process both the LAN-based failover and stateful failover traffic. If the interface does not have the necessary capacity, use two separate, dedicated interfaces.

LAN-based failover allows traffic to be transmitted over Ethernet connections. To secure failover transmissions, LAN-based failover provides message encryption and authentication using a manual pre-shared key.

**Note**
Starting with Cisco ASA and PIX Security Appliance Software Version 7.0, a crossover Ethernet cable can be used for LAN-based failover cabling.
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 use 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.

If you use the LAN-Based failover interface 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.

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. Using a data interface as the stateful failover interface is only supported in single context, routed mode. 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.
In multiple context mode, the stateful failover link resides in the system context. This interface and the LAN-Based failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.

The state information that is passed to the standby unit includes the following:

- NAT translation table
- TCP connection states
- UDP connection states
- The ARP table
- The Layer 2 bridge table (when running in transparent firewall mode)
- The HTTP connection states (if HTTP replication is enabled)
- The ISAKMP and IPsec SA table
- GTP PDP connection database
- SIP signaling sessions

The information that is not passed to the standby unit when stateful failover is enabled includes the following:

- The HTTP connection table (unless HTTP replication is enabled).
- The user authentication (uauth) table.
- 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.
- State information for Security Service Modules.
- DHCP server address leases.

The following SSL VPN features are not supported with stateful failover:

- Smart tunnels
- Port forwarding
- Plug-ins
- Java applets
- IPv6 clientless or Anyconnect sessions
- Citrix authentication (Citrix users must reauthenticate after failover.)
Active/Standby Failover Configuration Tasks

Complete the following tasks to use ASDM to configure active/standby LAN-based failover:

1. Cable the interfaces on both security appliances.
2. Prepare both security appliances for configuration via ASDM.
3. Use the ASDM High Availability and Scalability Wizard to configure the primary security appliance.
4. Verify that ASDM configured the secondary security appliance.
5. Save the configuration of the secondary security appliance to flash memory.

To configure active-standby LAN-based failover, complete the following tasks:

1. Cable the interfaces on both security appliances.
2. Prepare both security appliances for configuration via Cisco ASDM.
3. Use the Cisco ASDM High Availability and Scalability Wizard to configure the primary security appliance for failover.
4. Verify that Cisco ASDM configured the secondary security appliance with the LAN-based failover command set.
5. Save the configuration of the secondary security appliance to flash memory.
The following steps provide more details about configuring LAN-based failover:

**Step 1** Complete the following substeps to cable the interfaces of both security appliances:

1. Attach a network cable for each network interface that you plan to use.

2. Install a LAN-based failover connection between the primary and secondary security appliances. If you plan to use stateful failover, one interface must be dedicated to this function, unless you configure stateful failover to share the LAN-based failover connection.

3. Perform the following on any switch port that connects to the security appliances:
   - Enable PortFast
   - Turn off Ether-channeling
Preparing to Use ASDM for Configuring LAN Failover

Step 2  Complete the following substeps to prepare the security appliances for failover configuration via Cisco ASDM:

1. Enable one interface on the secondary security appliance and assign it an IP address that is reachable from the primary security appliance.

2. Configure the secondary security appliance to accept HTTP connections from the host running Cisco ASDM in its browser. This is the host from which you plan to configure failover via Cisco ASDM.

3. Configure the primary security appliance to accept HTTP connections from the IP address you assigned to the secondary security appliance.

4. Verify that you have not used the auto or the 1000auto option in any interface command in your configuration. If you have used one of these options, change it by re-entering the command with the correct information. Always specify the speed for the interface, such as 10BASE-T for 10 Mb/s or 100BASE-TX for 100 Mb/s. Ensure that the speeds and duplexes are the same for any devices on the subnets, including switches and routers. For stateful failover, set the stateful failover dedicated interface speed to “100full” or “1000full.”
Using ASDM to Configure LAN Failover

Step 3  Complete the following substeps to configure the primary security appliance for failover:

1. Click **Wizards** in the ASDM menu bar.

2. Choose **High Availability and Scalability Wizard**. The High Availability and Scalability Wizard opens.
Specify the Configuration Type

On the first wizard page, specify the failover configuration type.

3. Click the **Configure Active/Standby Failover** radio button.

4. Click Next. The Failover Peer Connectivity and Compatibility Check page is displayed.
Checking Failover Peer Connectivity and Compatibility

On this wizard page, specify the IP address of the failover peer to verify that the peer is reachable and that it is compatible peer for the primary security appliance.

5. Enter the IP address of the failover peer in the Peer IP Address field. This is the IP address you assigned to the secondary security appliance in Step 2. In the figure, 10.0.1.7 is entered.

Note This address does not have to be the failover link address, but it must be an interface that has Cisco ASDM access enabled on it.

6. Click Next. Cisco ASDM performs the following tests to determine if the security appliance at the IP address that you entered is a compatible failover peer for the security appliance that you are configuring:

- Connectivity test from this Cisco ASDM to the peer security appliance (secondary unit)
- Connectivity test from this security appliance (primary unit) to the peer security appliance (secondary unit)
- Hardware compatibility test
- Software version compatibility test
- Failover license compatibility test
- Routed or transparent firewall mode compatibility test
- Single or multiple context mode compatibility test

7. If all compatibility tests are passed, the LAN Link Configuration page is displayed.
On this wizard page, configure the failover interface for communications between this security appliance and its failover peer.

8. Choose the interface that you want to use as the failover interface from the Interface drop-down list. In the figure, GigabitEthernet0/2 is chosen.

9. Enter a name for the failover interface in the Logical Name field. In the figure, LANFAIL is entered.

10. Enter an IP address for the failover interface in the Active IP Address field. In the figure, 172.17.1.1 is entered.

11. In the Standby IP Address field, enter a standby IP address for the failover interface. This is the IP address that is to be used for the failover interface on the security appliance that is in the standby state. In the figure, 172.17.1.7 is entered.

12. Choose a subnet mask for the active and standby IP addresses from the Subnet Mask drop-down list. In the figure, 255.255.255.0 is chosen.

13. (Optional) Specify the key that is used to encrypt failover communication by using one of the following options. If you leave the Secret Key field blank, failover communications are sent in cleartext. Transmitting this sensitive data in cleartext could pose a significant security risk; therefore, securing the failover communication with a failover key is highly recommended.

- Enter an alphanumeric shared-secret in the Secret Key field. The secret can be from 1 to 63 characters. Valid characters are any combination of numbers, letters, or punctuation. The shared-secret is used to generate the encryption key. In the figure, the key is 1234567.

- Check the Use 32 Hexadecimal Characters check box, and enter a hexadecimal value for the encryption key in the Secret Key field. The key must be 32 hexadecimal characters (0-9, a-f).

14. Click Next. The State Link Configuration page is displayed.
This wizard page enables you to enable stateful failover and define the stateful failover link.

**Note** The State Link Configuration page does not appear in the wizard for Cisco ASDM running on the Cisco ASA 5505 platform.

15. Click one of the following radio buttons:

- **Disable Stateful Failover**: Choose this option to disable stateful failover.
- **Use the LAN Link as the State Link**: Choose this option to pass state information across the LAN-based failover link.
- **Configure Another Interface for Stateful Failover**: Choose this option to configure an unused interface as the stateful failover interface. If you choose this option, use the drop-down lists and fields to configure the following parameters:
  - **State Interface**: The interface that you want to use for stateful failover communication
  - **Logical Name**: A name for the stateful failover interface
  - **Active IP Address**: An IP address for the stateful failover link
  - **Standby IP**: A standby IP address for the stateful failover link
  - **Subnet Mask**: The subnet mask for the active IP and standby IP addresses

16. Click **Next**. The Standby Address Configuration page is displayed.
This wizard page enables you to configure standby IP addresses for each interface that has an active IP address.

17. Double-click the Standby IP Address field for each interface to add a standby IP address for the interface. These IP addresses are used by the standby security appliance and are different from the active security appliance addresses, but they should be in the same subnet for each interface.

18. Press the Enter key or the Tab key after entering the standby IP address.

19. (Optional) Deselect the Monitored check box for an interface to disable health monitoring for that interface. By default, health monitoring of physical interfaces is enabled and health monitoring of virtual interfaces is disabled.

20. Click **Next**. The Summary page is displayed.
21. Review your configuration on the Summary screen. If necessary, use the Back button to go to a previous screen and make changes.

22. When you are satisfied with your configuration, click Finish. The failover configuration is sent to the security appliance and to the failover peer.

23. After you click Finish, the Waiting for Config Sync window is displayed. Wait until this window automatically closes and another (Information) dialog box displays the following message:

   Failover configuration is complete. Configuration synchronization between the pair may take up to a few minutes. During that time, Cisco ASDM may lose connectivity to the device. After a few minutes, click on the Refresh button on the toolbar to regain connection.

24. Click OK.
show failover Command with LAN-Based Failover

```
as1(config)# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: LANFAIL GigabitEthernet0/2 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 500 milliseconds, holdtime 5 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 18:03:38 UTC Dec 12 2007
  This host: Secondary – Standby Ready
    slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
    Interface outside (192.168.1.7): Normal (Waiting)
    Interface inside (10.0.1.7): Normal (Waiting)
  Other host: Primary – Active
    slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
    Interface outside (192.168.1.2): Normal (Waiting)
    Interface inside (10.0.1.1): Normal (Waiting)
```

Use the `show failover` CLI command to view the failover status. The `show failover` command provides the following information:

- Status of failover
- Unit poll frequency
- Interface poll frequency
- Interface (failure) policy
- Monitored interfaces
- Software version
- Primary and secondary unit status
- Primary and secondary interface status

The figure shows the output of the `show failover` command after replication. In this example, failover is on, this is the secondary security appliance, and the software version of both security appliances is Version 8.0(2). The name of the interface that is used for LAN-based failover is LANFAIL. Notice that this interface does not appear in the interface list that displays the status of the interfaces.

The security appliances are using LAN-based failover with a unit poll interval of 200 ms and a hold time of 800 ms. The interface policy is set to one; one failed interface causes a failover. The number of monitored interfaces is two: inside and outside interfaces.

In the bottom half of the example, notice the types of failover units and their status. This security appliance is the secondary unit and its status is standby-ready. Notice the IP addresses of the primary and secondary units. The outside interface address on the primary unit is 192.168.1.2, and the address of the outside interface of the secondary unit is 192.168.1.7. The interfaces on the primary and secondary units are all normal (waiting).
The following table provides a description of the **show failover** command statistics:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>- On</td>
</tr>
<tr>
<td></td>
<td>- Off</td>
</tr>
<tr>
<td>Failover unit</td>
<td>Primary or secondary.</td>
</tr>
<tr>
<td>Failover LAN interface</td>
<td>Displays the logical and physical name of the failover link.</td>
</tr>
<tr>
<td>Unit poll frequency</td>
<td>Displays the number of seconds or milliseconds between hello messages that are sent to the peer unit and the number of seconds or milliseconds during which the unit must receive a hello message on the failover link before declaring that the peer failed.</td>
</tr>
<tr>
<td>Interface poll frequency</td>
<td>The number of seconds or milliseconds between hello messages that are sent to the peer interface and the number of seconds during which the interface must receive a hello message before declaring that the peer interface failed.</td>
</tr>
<tr>
<td>Interface policy</td>
<td>Displays the number or percentage of interfaces that must fail to trigger failover.</td>
</tr>
<tr>
<td>Monitored interfaces</td>
<td>Displays the number of interfaces monitored out of the maximum possible.</td>
</tr>
<tr>
<td>failover replication http</td>
<td>Displays if HTTP state replication is enabled for stateful failover. To enable HTTP (port 80) connection replication, use the <code>failover replication http</code> command in global configuration mode. The default is disabled.</td>
</tr>
<tr>
<td>Last failover at:</td>
<td>The date and time of the last failover in the following form: hh:mm:ss UTC Month day yyyy Coordinated Universal Time (UTC) is equivalent to Greenwich Mean Time (GMT).</td>
</tr>
<tr>
<td>This host:</td>
<td>For each host, the display shows the following information:</td>
</tr>
<tr>
<td>Other host:</td>
<td>- The role (primary or secondary) that the host plays in the failover configuration.</td>
</tr>
<tr>
<td></td>
<td>- The current status (active or standby) of the host.</td>
</tr>
<tr>
<td></td>
<td>- The amount of time, in seconds, that the host has been active. This time is cumulative; therefore, if the standby unit was active in the past, it will also show a value.</td>
</tr>
<tr>
<td></td>
<td>- The name, IP address, and status of each interface currently being used. The status may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Failed:</strong> The interface has failed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No link:</strong> The interface line protocol is down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normal:</strong> The interface is working correctly.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Link down:</strong> The interface has been administratively shut down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown:</strong> The security appliance cannot determine the status of the interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Waiting:</strong> Monitoring of the network interface on the other unit has not yet started.</td>
</tr>
<tr>
<td>Stateful Failover Logical Update Statistics</td>
<td>The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled.</td>
</tr>
</tbody>
</table>
Forcing Control Back

Use the `failover active` command when you need to force control of the connection back to the unit that you are accessing, such as when you want to switch control back from a unit after you have fixed a problem and want to restore service to the primary unit. Enter either the `no failover active` command on the secondary unit to switch service to the primary or the `failover active` command on the primary unit.

The `failover reset` command allows you to change the failed unit to an unfailed state. This command can be entered from either security appliance, but it is best to always enter commands at the active security appliance. Entering the `failover reset` command at the active firewall unfails the standby firewall.
Defining Failover Criteria

- **Failover unit poll time:** Amount of time between hello messages
- **Failover unit hold time:** Amount of time to wait (after 3 consecutive poll failures) before triggering failover
- **Failover interface poll time:** Poll time for interface monitoring
- **Failover interface hold time:** Hold time for interface monitoring
- **Failover interface policy:** Number of failed interfaces that triggers failover

If you want failover to occur faster, decrease the failover unit poll time, which specifies how often hello messages are sent on the failover link. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly. The default failover poll time for the Cisco ASA is 1 second; for Cisco PIX Security Appliances, it is 15 seconds. The minimum unit poll time value is 200 ms.

You can specify the amount of time that the security appliance will wait (after three consecutive poll failures) before declaring the peer unit failed and triggering a failover. This time duration is called the failover unit hold time. The default hold timer for the PIX security appliance is 45 seconds; for the ASA, it is 15 seconds.

You can also configure failover poll times and hold times for monitored interfaces. The security appliance sends hello packets out of each monitored data interface to monitor interface health. If the security appliance does not receive a hello packet from the corresponding interface on the peer unit for over half of the hold time, 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. By default, a single interface failure causes failover, but you can change the number of interfaces that must fail before a failover occurs. Decreasing the poll and hold times enables the security appliance to detect and respond to interface failures more quickly, but may consume more system resources.

To specify the policy for failover when monitoring detects an interface failure, use the `failover interface-policy num[\%]` command in global configuration mode. For the `num` value, use a number from 1 to 100 if you specify a percentage; use a number from 1 to the maximum number of interfaces if you specify a number. The defaults are as follows:

- One interface
- Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.
**Note**  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 interface meets or exceeds the configured failover criteria.
Complete the following optional steps to configure failover criteria:

**Step 1** Click the Configuration button in the ASDM toolbar.

**Step 2** Choose Device Management from the navigation pane.

**Step 3** Expand the High Availability menu.

**Step 4** Choose Failover from the High Availability menu.

**Step 5** Click the Criteria tab.

**Step 6** To specify the number of failed interfaces that triggers failover, enter a value from 1 to 250 in the Number of Failed Interfaces that Triggers Failover field. In the figure, the failure of one interface triggers failover.

**Step 7** To specify the number of failed interfaces that triggers failover as a percentage of the monitored interfaces, click the Percentage of Failed Interfaces That Triggers Failover radio button, and enter the percentage in the corresponding field.

**Step 8** To specify the amount of time between hello messages among units, do one of the following:

- Choose milliseconds from the Unit Failover drop-down list and enter a value from 200 to 999 in the Unit Failover field. In the figure, 200 is entered.
- Choose seconds from the Unit Failover drop-down list and enter a value from 1 to 15 in the Unit Failover field.
Step 9  To specify the amount of time that the security appliance will wait (after three consecutive poll failures) before declaring the peer unit failed and triggering a failover, do one of the following:

- Choose milliseconds from the Unit Hold Time drop-down list and enter a value from 800 to 999 in the Unit Hold Time field. You cannot enter a value that is less than 3 times the unit poll time. In the figure, 800 is entered.
- Choose seconds from the Unit Hold Time drop-down list and enter a value from 3 to 45 in the Unit Hold Time field. You cannot enter a value that is less than 3 times the unit poll time.

Step 10  To specify the poll time for interface monitoring, do one of the following:

- Choose milliseconds from the Monitored Interfaces drop-down list and enter a value from 500 to 999 in the Monitored Interfaces field. In the figure, 500 is entered.
- Choose seconds from the Monitored Interfaces drop-down list and enter a value from 3 to 15 in the Monitored Interfaces field.

Step 11  To specify the hold time for interface monitoring, enter a value from 5 to 75 (seconds) in the Interface Hold Time field. You cannot enter a hold time that is less than 5 times the poll time. In the figure, 5 is entered.

Step 12  Click **Apply**.
You can use the Setup tab within the Failover panel to enable failover on the security appliance. You also designate the failover link and the stateful failover link on this tab.
You can use the Interfaces tab within the Failover panel to define the standby IP address for each interface on the security appliance and to specify whether the status of the interface should be monitored.

By default, monitoring of physical interfaces is enabled and monitoring of subinterfaces is disabled. You can monitor up to 250 interfaces on a unit. You can control which interfaces affect your failover policy by disabling the monitoring of specific interfaces and enabling the monitoring of others. This lets you exclude interfaces that are attached to less critical networks from affecting your failover policy.

The other two tabs in the Failover panel include the following:

- **Criteria tab**: Enables you to set the interface policy, the unit, and interface poll and hold times.
- **MAC Addresses tab**: Enables you to set the virtual active and standby MAC addresses for the physical interfaces.
Active/Active Failover Configuration

This topic describes how active/active failover works and how to configure it.

**Active/Active Failover**

Traffic

<table>
<thead>
<tr>
<th>g0/1</th>
<th>m0/0</th>
<th>g0/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTX1 Active</td>
<td>CTX2 Standby</td>
<td>g0/2</td>
</tr>
<tr>
<td>g0/0 g0/3</td>
<td>g0/1 m0/0</td>
<td>g0/2</td>
</tr>
</tbody>
</table>

Unit A
Active (CTX1)/Standby (CTX2)

Unit B
Active (CTX2)/Standby (CTX1)

Active/active failover requires the use of contexts. For example, you could have two security appliances with two contexts each:
- CTX1
- CTX2

Under normal conditions, each security appliance has one active and one standby context:
- The active context processes traffic.
- The standby context is located in the peer security appliance.

Under the active/standby failover model, only one security appliance actively processes user traffic while the other unit acts as a hot standby, prepared to take over if the active unit fails. Starting with Cisco ASA and PIX Security Appliance Software Version 7.0, the security appliance is capable of active/active failover. When two security appliances are configured to function in active/active failover, both units can actively process security appliance traffic while serving as a backup for their peer unit.

The active/active failover feature leverages the virtual context feature. In the example in the figure, there are two security appliances configured for active/active failover: Unit A and Unit B. Each security appliance is partitioned into two contexts: CTX1 and CTX2. In the security appliance active/active scenario, under normal conditions, there is one active context and one standby context per unit. In Unit A, CTX1 is active and passing traffic. CTX1 in Unit B is in standby state. In Unit B, CTX2 is active and passing traffic while CTX2 in Unit A is in standby state.
In the previous example, in Unit A, CTX1 was active while CTX2 was standby. In Unit B, CTX1 was standby while CTX2 was active. Active/active failover logic enables each security appliance to determine whether a failure is context-based or unit-based.

If an active context fails, the active context transitions to a failed state. In the peer security appliance, the standby context transitions from standby to active. For example, in the figure, if Unit A interface g0/0 fails, Unit A can determine that the failure is a context-based failure. Unit A places CTX1 in a failed state. Unit A can communicate with Unit B about the change in state of CTX1. Unit B changes the state of its CTX1 to active. After the state change, both of the Unit B contexts are active and passing traffic.

Unit-based failover occurs when a failure affects the whole unit and the peer unit can take over by activating any standby contexts and start processing 100 percent of the traffic.
The Failover Link

- Used to communicate unit health, interface health, and switchover messages
- Used for configuration resynchronization
- Configured in the system configuration of the primary failover unit

The figure illustrates the g0/2 interface on the security appliances are being used as the LAN-Based failover link. The failover link is used to communicate unit health, interface health, switchover messages, configuration resynchronization, and so on. Keep the following important points in mind when configuring the failover link for active/active failover:

- The failover link is configured in the system configuration of the primary failover unit.
- The failover link interface must be enabled.
- The failover link must be assigned a name, an active IP address, and a standby IP address.
- You can use the failover link as the stateful failover interface. If you use the LAN-Based failover interface 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.
Failover Groups

- Active/active failover requires the use of failover groups to manage contexts.
- A group is comprised of one or more contexts.
- Each security appliance supports up to two failover groups.
- Each failover group contains separate state machines to keep track of the group failover state.
- Active/active failover can occur on a group or system basis.

In active/standby failover, failover is performed on a unit basis. One unit is active while the other unit is a standby unit.

In active/active failover, one context is active while the same context in the other security appliance is in standby state.

Cisco ASA and PIX Security Appliance Software Version 7.0 introduced the concept of the failover group. Each security appliance supports up to two failover groups. You can join one or more contexts to a failover group. For example, context CTX1, CTX2, and CTX3 can join group 1 while context CTX4 and CTX5 can join group 2. The security appliance uses failover groups to manage contexts. Each failover group contains separate state machines to keep track of their context failover states. Failover can occur on a failover group or system basis.

In the example in the figure, there are two failover groups: group 1 and group 2. Context CTX1 joins group 1 and CTX2 joins group 2. Group 1 monitors the health of CTX1 and group 2 monitors the health of CTX2 across both security appliances.

Once the failover groups are defined, you can assign contexts to failover groups and allocate context interfaces in the system configuration. In the example in the figure, the administrator allocated security appliance interfaces g0/0 and g0/1 to context CTX1, and interfaces g0/3 and m0/0 to context CTX2. The administrator assigned CTX1 to failover group 1 and CTX2 to failover group 2.

With active/active failover, you can control the distribution of active contexts between the two security appliances by controlling each context’s membership in a failover group. Some contexts might be heavily loaded, while others are not. Therefore, simply dividing the contexts evenly between the two failover groups does not always result in an even distribution of the traffic load between the two security appliances.
Active/Active Failover IP Addressing

- Active and standby IP addresses must be assigned to each interface that is allocated to a context.
- The active and standby IP addresses must be configured on the unit where the context is active.

Each allocated interface within the context is configured with an active and standby IP address. For example, in the figure, context CTX1 interface g0/0 is assigned an active IP address of 192.168.1.2 and a standby IP address of 192.168.1.7. The standby IP address is used on the security appliance that is currently the standby unit for that context. It must be in the same subnet as the active IP address.
Active/Active Failover Configuration
Overview

Complete the following tasks to use the ASDM High Availability and Scalability Wizard to configure active/active failover:
- Cable the interfaces on both security appliances.
- Ensure that both security appliances are in multiple context mode.
- Configure contexts and allocate interfaces to contexts.
- Enable and assign an IP address to each interface that is allocated to a context.
- Prepare both security appliances for configuration via ASDM.
- Use the ASDM High Availability and Scalability Wizard to configure the primary security appliance.
- Verify that ASDM configured the secondary security appliance.
- Save the configuration of the secondary security appliance to flash memory.

To configure active/active failover, complete the following tasks:
1. Cable the interfaces on both security appliances.
2. Ensure that both security appliances are in multiple context mode.
3. Configure contexts and allocate interfaces to contexts.
4. Enable and assign an IP address to each interface that is allocated to a context.
5. Prepare both security appliances for configuration via Cisco ASDM.
6. Use the Cisco ASDM High Availability and Scalability Wizard to configure the primary security appliance for failover.
7. Verify that Cisco ASDM configured the secondary security appliance with the LAN-based failover command set.
8. Save the configuration of the secondary security appliance to flash memory.
Complete the following steps to use the Cisco ASDM High Availability and Scalability Wizard to configure active/active failover:

**Step 1**  
From the system context, click **Wizards** in the ASDM menu bar.

**Step 2**  
Choose **High Availability and Scalability Wizard**. The High Availability and Scalability Wizard opens.
Specifying the Configuration Type

On the first wizard page, specify the failover configuration type.

**Step 3**  Click the **Configure Active/Active Failover** radio button.

**Note**  If your security appliances are not in multiple context mode, the Wrong Firewall Mode window opens, asking you if you would like to allow Cisco ASDM to convert both security appliances to multiple context mode.

**Step 4**  Click **Next**. The Failover Peer Connectivity and Compatibility Check page is displayed.
Checking Failover Peer Connectivity and Compatibility

On this wizard page, specify the IP address of the failover peer to verify that the peer is reachable and that it is compatible peer for the primary security appliance.

**Step 5** Enter the IP address of the failover peer in the Peer IP Address field. In the figure, 10.0.1.7 is entered.

**Note** This address does not have to be the failover link address, but it must be an interface that has Cisco ASDM access enabled on it.

**Step 6** Click **Next**. Cisco ASDM performs the following tests to determine if the security appliance at the IP address you entered is a compatible failover peer for the security appliance that you are configuring:

- Connectivity test from this Cisco ASDM to the peer security appliance
- Connectivity test from this security appliance to the peer security appliance
- Hardware compatibility test
- Software version compatibility test
- Failover license compatibility test
- Routed or transparent firewall mode compatibility test
- Single or multiple context mode compatibility test

**Step 7** If all compatibility tests are passed, the Security Context Configuration page is displayed.
Configuring Contexts and Failover Groups

On this wizard page, assign security contexts to failover groups. The page displays the security contexts currently configured on the security appliance along with the failover group each context belongs to. By default, both contexts are assigned to group 1.

Step 8  To assign a context to a different failover group, select the failover group for the corresponding context.

Step 9  Select the new failover group number from the drop-down list.

Step 10  Click **Next**. The LAN Link Configuration page is displayed.
On this wizard page, configure the failover interface for communications between this security appliance and its failover peer.

**Step 11** Choose the interface that you want to use as the failover interface from the Interface drop-down list. In the figure, GigabitEthernet0/2 is chosen.

**Step 12** Enter a name for the failover interface in the Logical Name field. In the figure, LANFAIL is entered.

**Step 13** Enter an IP address for the failover interface in the Active IP Address field. In the figure, 172.17.1.1 is entered.

**Step 14** In the Standby IP Address field, enter a standby IP address for the failover interface. This is the IP address to be used for the failover interface on the security appliance that is in the standby state. In the figure, 172.17.1.7 is entered.

**Step 15** Choose a subnet mask for the active and standby IP addresses from the Subnet Mask drop-down list. In the figure, 255.255.255.0 is chosen.

**Step 16** (Optional) Specify the key that is used to encrypt failover communication by using one of the following options. If you leave the Secret Key field blank, failover communications are sent in cleartext. Transmitting this sensitive data in cleartext could pose a significant security risk; therefore, securing the failover communication with a failover key is highly recommended.

- Enter an alphanumeric shared-secret in the Secret Key field. The secret can be from 1 to 63 characters. Valid characters are any combination of numbers, letters, or punctuation. The shared-secret is used to generate the encryption key. In the figure, the key is 1234567.

- Check the Use 32 Hexadecimal Characters check box, and enter a hexadecimal value for the encryption key in the Secret Key field. The key must be 32 hexadecimal characters (0-9, a-f).

**Step 17** Click **Next**. The State Link Configuration page is displayed.
This wizard page enables you to enable stateful failover and define the stateful failover link.

Note The State Link Configuration page does not appear in the wizard for Cisco ASDM running on the Cisco ASA 5505 platform.

Step 18 Click one of the following radio buttons:

- **Disable Stateful Failover**: Choose this option to disable stateful failover.

- **Use the LAN Link as the State Link**: Choose this option to pass state information across the LAN-based failover link.

- **Configure Another Interface for Stateful Failover**: Choose this option to configure an unused interface as the stateful failover interface. If you choose this option, use the drop-down lists and fields to configure the following parameters:
  
  — **State Interface**: The interface that you want to use for stateful failover communication
  
  — **Logical Name**: A name for the stateful failover interface
  
  — **Active IP Address**: An IP address for the stateful failover link
  
  — **Standby IP**: A standby IP address for the stateful failover link
  
  — **Subnet Mask**: The subnet mask for the active IP and standby IP addresses

Step 19 Click Next. The Standby Address Configuration page is displayed.
Configuring Standby Addresses

This wizard page enables you to configure standby IP addresses for each interface that has an active IP address.

Step 20 Double-click the Standby IP Address field for each interface to add a standby IP address for the interface. These IP addresses are used by the standby security appliance and are different from the active security appliance addresses, but they should be in the same subnet for each interface.

Step 21 Press the Enter key or the Tab key after entering the standby IP address.

Step 22 (Optional) Deselect the Monitored check box for an interface to disable health monitoring for that interface. By default, health monitoring of physical interfaces is enabled and health monitoring of virtual interfaces is disabled.

Step 23 Click Next. The Summary page is displayed.

From this page, you can also determine which contexts are in each of the failover group and which interfaces are allocated to each context. For example, in the figure, you can determine that the failover group GROUP1, has the admin context assigned to it and the admin context has two allocated interfaces (inside and outside). The failover group GROUP2, has the CTX2 context assigned to it and the CTX2 context has two allocated interfaces (dmz and mgmt).
Step 24  Review your configuration on the Summary screen. If necessary, use the Back button to go to a previous screen and make changes.

Step 25  When you are satisfied with your configuration, click Finish. The active/active failover configuration is sent to the security appliance and to the failover peer, and After you click Finish, the Waiting for Config Sync window is displayed. Wait until this window automatically closes and another (Information) dialog box displays the following message:

Step 26  Failover configuration is complete. Configuration synchronization between the pair may take up to a few minutes. During that time, Cisco ASDM may lose connectivity to the device. After a few minutes, click on the Refresh button on the toolbar to regain connection.

Step 27  Click OK.
The `show failover` command statistics can be broken down into three logical sections: failover LAN, primary unit, and secondary unit. The example in the figure displays the failover LAN statistics. The table shows some of the available failover statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>On or off.</td>
</tr>
<tr>
<td>Failover Unit</td>
<td>Primary or secondary.</td>
</tr>
<tr>
<td>Failover LAN Interface</td>
<td>Displays the logical and physical name of the failover link.</td>
</tr>
<tr>
<td>Unit Poll Frequency</td>
<td>Displays the number of seconds between hello messages that are sent to the peer unit and the number of seconds during which the unit must receive a hello message on the failover link before it declares that the peer has failed.</td>
</tr>
<tr>
<td>Interface Poll Frequency</td>
<td>Displays the values that you set for interface monitoring.</td>
</tr>
<tr>
<td>Interface Policy</td>
<td>Displays the number or percentage of interfaces that must fail before failover is triggered.</td>
</tr>
<tr>
<td>Monitored Interfaces</td>
<td>Displays the number of interfaces monitored, out of the maximum possible.</td>
</tr>
<tr>
<td>Group 1 Last Failover at:</td>
<td>The date and time of the last failover for each group in the following form:</td>
</tr>
<tr>
<td>Group 2 Last Failover at:</td>
<td><code>hh:mm:ss UTC DayName Month Day yyyy</code></td>
</tr>
<tr>
<td></td>
<td>UTC is equivalent to GMT.</td>
</tr>
</tbody>
</table>
The second logical section of the `show failover` command shows statistics of the primary failover unit. In the primary security appliance, the command displays the state of each group, such as active, standby, or failed. For example, the figure shows that Group 1 is active on the primary unit and Group 2 is standby on the primary unit. The command also details the interface information by context.
The table shows some of the available failover statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This host:</td>
<td>Shows the information for each host.</td>
</tr>
<tr>
<td>Other host:</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Primary or secondary.</td>
</tr>
<tr>
<td>System State</td>
<td>- Active or standby ready</td>
</tr>
<tr>
<td></td>
<td>- Active time in seconds</td>
</tr>
<tr>
<td>Group 1 State</td>
<td></td>
</tr>
<tr>
<td>Group 2 State</td>
<td></td>
</tr>
<tr>
<td><code>context Interface name (n.n.n.n):</code></td>
<td>For each interface, the display shows the IP address currently being used on each unit, in addition to one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Failed</strong>: The interface has failed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No link</strong>: The interface line protocol is down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normal</strong>: The interface is working correctly.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Link down</strong>: The interface has been administratively shut down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown</strong>: The security appliance cannot determine the status of the interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Waiting</strong>: Monitoring of the network interface on the other unit has not yet started.</td>
</tr>
</tbody>
</table>
The third logical section of the `show failover` command shows statistics of the peer failover unit, the secondary unit. This section of the command displays the state of the peer, such as active, standby, or failed. For example, the figure shows that Group 1 is standby on the secondary unit and Group 2 is active on the secondary unit. The command also details the interface information by context.
The table shows some of the available failover statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This host:</td>
<td>Shows the information for each host.</td>
</tr>
<tr>
<td>Other host:</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Primary or secondary.</td>
</tr>
<tr>
<td>System State</td>
<td>■ Active or standby ready</td>
</tr>
<tr>
<td></td>
<td>■ Active time in seconds</td>
</tr>
<tr>
<td>Group 1 State</td>
<td>■ Active or standby ready</td>
</tr>
<tr>
<td>Group 2 State</td>
<td>■ Active time in seconds</td>
</tr>
<tr>
<td>context Interface name (n.n.n.n):</td>
<td>For each interface, the display shows the IP address currently being used on each unit and one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Failed</strong>: The interface has failed.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>No link</strong>: The interface line protocol is down.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Normal</strong>: The interface is working correctly.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Link down</strong>: The interface has been administratively shut down.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Unknown</strong>: The security appliance cannot determine the status of the interface.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Waiting</strong>: Monitoring of the network interface on the other unit has not yet started.</td>
</tr>
</tbody>
</table>
You can also view the statistics for a specific failover group via the `show failover group` command. With the `show failover group` command, the administrator can display the state of the failover group and the interfaces on the unit. For example, the figure shows that Group 1 is active on the primary unit.
You can activate a unit by using the `failover active` command. You can activate a group by adding the `group` keyword to the command string, as in the `failover active group` command. In the example in the figure, the administrator wants to activate standby CTX2 in the primary unit. To activate CTX2, enter the `failover active group 2` command in the primary unit. To deactivate a context, you can use the `no` version of the command. For example, to deactivate the admin context in the figure, the administrator enters `no failover active group 1` command to force the switchover.

In active/active failover, failover can be triggered at the unit level if one of the following events occurs:

- The unit has a hardware failure.
- The unit has a power failure.
- The unit has a software failure.
- The `no failover active` command is entered in the system execution space.

Failover is triggered at the failover group level when one of the following events occurs:

- Too many monitored interfaces in the group fail.
- The `no failover active group group_id` command is entered.

Configure the failover threshold for each failover group by specifying the number or percentage of interfaces within the failover group that must fail before the group fails. Because a failover group can contain multiple contexts, and each context can contain multiple interfaces, it is possible for all interfaces in a single context to fail without causing the associated failover group to fail.
Configuring Redundant Interfaces

This topic explains how to configure redundant interfaces to increase the adaptive security appliance reliability.

Using a Redundant Interface as a Failover Link

- If you use a redundant interface for the failover link, configure the redundant interface as part of the basic configuration on both security appliances.
- If you use a redundant interface for the failover link, you must put a switch or hub between the two security appliances.
- When the active interface fails over to the standby interface, the redundant interface does not appear to be failed when being monitored for device-level failover.

Follow these guidelines when using redundant interface for the LAN-Based failover or stateful failover link:

- If you want to use a redundant interface for the LAN-Based failover or stateful failover link, you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.

Note
A redundant interface that is used by failover also performs member switchover upon missing a threshold number of hello messages, provided the link status of the standby member interface is up.

- If you use a redundant interface for the LAN-Based failover or stateful failover link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
- When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.
- You can monitor redundant interfaces for failover using the monitor-interface command; be sure to reference the logical redundant interface name.
Physical Interface Considerations

<table>
<thead>
<tr>
<th>Redundant Interface</th>
<th>Member Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Same physical type</td>
</tr>
<tr>
<td>IP addresses</td>
<td>No names</td>
</tr>
<tr>
<td>Security level</td>
<td>No IP addresses</td>
</tr>
<tr>
<td></td>
<td>No security level</td>
</tr>
</tbody>
</table>

To add a physical interface that is already in your configuration to a redundant interface pair, you must remove its name; removing the name clears any configuration that refers to the interface.

When configuring redundant interfaces, keep in mind the following important points regarding physical interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name. Removing the name clears any configuration that refers to the interface.
- The only configurations available to physical interfaces that are part of a redundant interface pair are physical parameters (such as speed and duplex), the `description` command, and the `shutdown` command. You can also enter runtime commands such as `default` and `help`. When a physical interface is assigned as a member of a redundant interface, you can no longer assign an IP address, security level, or name to that physical interface.
- If you shut down the active interface, the standby interface becomes active.
When you add a redundant interface using Cisco ASDM, it is enabled by default. However, the member interfaces must also be enabled to pass traffic.

Complete the following steps to create a logical redundant interface:

1. **Step 1** Click the Configuration button in the ASDM toolbar.
2. **Step 2** Choose **Device Setup** from the navigation pane.
3. **Step 3** Choose **Interfaces** from the Device Setup menu. The Interfaces panel is displayed.
4. **Step 4** Click **Add**.
5. **Step 5** Choose **Redundant Interface** from the drop-down list. The Add Redundant Interface window opens.
In the Add Redundant Interface window, you can configure such settings as the redundant interface ID, the redundant interface name, and the member interfaces.

**Step 6** Enter an integer from 1 to 8 in the Redundant ID field. In the figure, 1 is entered.

**Step 7** From the Primary Interface drop-down list, choose the first member interface. In the figure, GigabitEthernet0/2 is chosen.

**Step 8** From the Secondary Interface drop-down list, choose the second member interface. In the figure, GigabitEthernet0/3 is chosen.

**Note** After you add a physical interface to the interface pair, any configuration for it, such as an IP address, is removed.

**Step 9** Enter a name for the redundant interface in the Interface Name field. The name can be up to 48 characters in length and is not case-sensitive. In the figure, DMZ is entered.

**Step 10** Enter a security level for the redundant interface in the Security Level field. Enter an integer from 1 to 100. In the figure, 50 is entered.

**Step 11** Verify that the Enable Interface check box is checked. This should be checked by default. If it is not, check it.

**Step 12** Choose one of the following IP Address radio buttons to specify an IP addressing method. The remaining configuration depends on your choice. In the figure, Use Static IP is chosen.

- Use Static IP
- Obtain Address via DHCP
- Use PPPoE
Step 13  Configure the IP address parameters for the addressing method that you chose in the previous step. In the figure, the static IP address 172.18.1.1 is entered in the IP Address field, and 255.255.255.0 is entered in the Subnet Mask field.

Step 14  Click OK.

Step 15  Click Apply in the Interfaces panel.

The redundant interface uses the MAC address of the first physical interface that you add. This is the interface chosen from the Primary Interface drop-down list. If you change the order of the member interfaces in the configuration, the MAC address changes to match the MAC address of the interface that is now listed first.

You can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses using the MAC address cloning option from the Advanced window. When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.
Changing the Active Interface

```plaintext
ciscoasa(config)# show interface redundant number detail | grep member
```
- Shows which interface in a redundant interface pair is active

```plaintext
ciscoasa(config)# show interface redundant1 detail | grep member
Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```
- Shows that GigabitEthernet0/3 is the active interface

```plaintext
ciscoasa(config)# redundant-interface redundant number active-member physical_interface
```
- Changes the active interface

```plaintext
ciscoasa(config)# redundant-interface redundant1 active-member
GigabitEthernet0/2
```
- Sets GigabitEthernet0/2 as the active interface

To view which interface is active, use the `show interface` command with the `redundant number` argument. In the example in the figure, the command output shows that GigabitEthernet0/3 is the active interface. You can change the active interface by using the `redundant-interface` command.

The syntax for the `redundant-interface` command is as follows:

```
redundant-interface redundant number active-member physical_interface
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redundant number</code></td>
<td>Specifies the redundant interface ID, such as redundant1.</td>
</tr>
<tr>
<td><code>active-member physical_interface</code></td>
<td>Sets the active member. Both member interfaces must be the same physical type.</td>
</tr>
</tbody>
</table>