



## Using PIX Firewall Failover

---

This chapter describes the PIX Firewall failover feature, which allows a secondary PIX Firewall to take over the functionality of a failed primary PIX Firewall. This chapter includes the following topics:

- [Failover System Requirements](#), page 10-2
- [Understanding Failover](#), page 10-3
- [Failover Configuration Prerequisites](#), page 10-8
- [Configuring Cable-Based Failover](#), page 10-9
- [Configuring LAN-Based Failover](#), page 10-11
- [Verifying the Failover Configuration](#), page 10-16
- [Forcing Failover](#), page 10-20
- [Disabling Failover](#), page 10-20
- [Monitoring Failover](#), page 10-21
- [Frequently Asked Failover Questions](#), page 10-22
- [Failover Configuration Examples](#), page 10-26



**Note**

---

For instructions about upgrading the failover feature from a previous version, see the “[Upgrading Failover Systems from a Previous Version](#)” section in [Chapter 11, “Changing Feature Licenses and System Software.”](#)”

---

# Failover System Requirements

Table 10-1 lists the system requirements for the failover feature.

**Table 10-1 Failover System Requirements**

Requirement	Description
Supported PIX Firewall models	<ul style="list-style-type: none"> <li>• PIX 515</li> <li>• PIX 515E</li> <li>• PIX 520</li> <li>• PIX 525</li> <li>• PIX 535</li> </ul> <p><b>Note</b> The PIX 501 and PIX 506E models do not support failover.</p>
Identical PIX Firewall hardware and software versions	<p>The failover feature requires two units that are identical in the following respects:</p> <ul style="list-style-type: none"> <li>• Model (a PIX 515E <i>cannot</i> be used with a PIX 515)</li> <li>• Same number and type of interfaces</li> <li>• Software version</li> <li>• Activation key type (DES or 3DES)</li> <li>• Flash memory</li> <li>• Amount of RAM</li> </ul> <p><b>Note</b> The PIX-4FE and PIX-4FE-66 cards are considered equivalent and interchangeable. You can install a PIX-4FE in the primary unit and a PIX-4FE-66 in the secondary unit, as long as you install them in the same slot number of each chassis. For example, if you install a PIX-4FE in Slot 1 of the primary unit, the PIX-4FE-66 must be installed in Slot 1 of the secondary unit.</p>
At least one unit with an Unrestricted (UR) license	<p>The other unit can have a Failover Only (FO) or another UR license. Units with a Restricted license cannot be used for failover, and two units with FO licenses cannot be used together as a failover pair.</p> <p>The PIX Firewall with the FO license is intended to be used solely for failover and not in standalone mode. If a failover unit is used in standalone mode, the unit will reboot at least once every 24 hours until the unit is returned to failover duty. When the unit reboots, the following message displays on the console:</p> <pre> =====NOTICE=====       This machine is running in secondary mode without       a connection to an active primary PIX. Please       check your connection to the primary system.                            REBOOTING... ===== </pre>

# Understanding Failover

This section describes how failover works, and includes the following topics:

- [Overview, page 10-3](#)
- [Network Connections, page 10-3](#)
- [Failover and State Links, page 10-4](#)
- [Primary and Secondary Vs. Active and Standby, page 10-6](#)
- [Configuration Replication, page 10-6](#)
- [Failover Triggers, page 10-7](#)

## Overview

The failover feature allows you to use a standby PIX Firewall to take over the functionality of a failed PIX Firewall. When the active unit fails, it changes to the standby state, while the standby unit changes to the active state. The unit that becomes active takes over the active unit's IP addresses and MAC addresses, and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network. (See the [“Primary and Secondary Vs. Active and Standby”](#) section for more information about MAC addresses).

The PIX Firewall supports two types of failover:

- **Regular Failover**—When a failover occurs, all active connections are dropped and clients need to reestablish connections when the new active unit takes over.
- **Stateful Failover**—During normal operation, the active unit continually passes per-connection stateful 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.

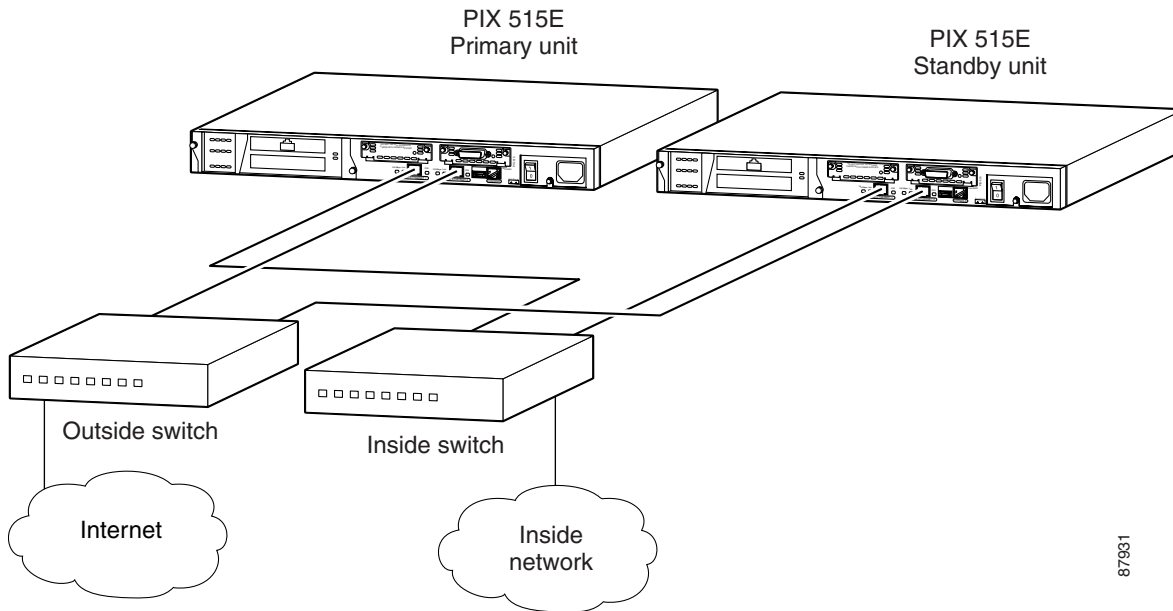
The state information passed to the standby unit includes:

- NAT translation table
- TCP connection states
- H.323, SIP, and MGCP UDP media connections

## Network Connections

Both units require the same access to the inside and outside networks. You must place them in parallel, as shown in [Figure 10-1](#). Because the standby unit does not pass traffic, only the active unit takes part in networking. The active and standby units must be on the same subnet, so there cannot be a router between the two units. However, you can place one or more switches between the two units.

Figure 10-1 Parallel Position in Network



## Failover and State Links

This section describes the failover link, and for Stateful Failover, the state link. This section includes the following topics:

- [Failover Link, page 10-4](#)
- [State Link, page 10-5](#)

### Failover Link

The two units constantly communicate over a failover link to determine each unit's operating status. Communications over the failover link include:

- The unit state (active or standby)
- The power status (cable-based failover only)
- Hello messages (also sent on all other interfaces)
- Configuration synchronization between the two units (see the [“Configuration Replication”](#) section for more information).

The failover link can be one of the following connections:

- Serial failover cable (“cable-based failover”)—If the two units are within six feet of each other, then we recommend that you use the serial failover cable. Using this cable allows the firewall to sense a power loss of the peer unit, and to differentiate a power loss from an unplugged cable. The cable is a modified RS-232 serial link cable that transfers data at 117,760 bps (115 Kbps). One end is labeled “Primary” and attaches to the primary unit, while the other end is labeled “Secondary” and attaches to the secondary unit. If you purchased a PIX Firewall failover bundle, this cable is included. To order a spare, use part number PIX-FO.
- Ethernet connection (“LAN-based failover”)—You can use any unused Ethernet interface on the device. If the units are further than six feet apart, use this method. We recommend that you connect this link through a dedicated switch. You *cannot* use a crossover Ethernet cable to link the units directly.

The disadvantages of using LAN-based failover include:

- The PIX Firewall cannot immediately detect the loss of power of a peer, so the PIX Firewall takes longer to fail over in this case.
- You need to configure the failover link on the standby unit before it can communicate with the active unit.

In cable-based failover, the standby unit can communicate directly with the active unit, and can receive the entire configuration before enabling any interfaces or setting IP addresses.

- The switch between the two units can be another point of hardware failure.
- You have to dedicate an Ethernet interface (and switch ports) to the failover link, and the interface cannot be used for regular traffic.

The benefits include:

- Separation of the units by more than 6 feet.
- Faster configuration replication.

## State Link

For Stateful Failover, you must use an Ethernet link to pass state information. The PIX Firewall supports the following Ethernet interface settings for the state link:

- Fast Ethernet (100BASE-T) full duplex
- Gigabit Ethernet (GE) (1000BASE-SX) full duplex



---

**Note**

On a PIX 535 with GE interfaces, you must use a GE interface as the state link.

---

We recommend that you use a crossover cable to directly connect the units. You can also use a switch between the units. No hosts or routers should be on this link.

If the two units are more than six feet apart, you can use the same Ethernet state link as the failover link, but we recommend that you use a separate Ethernet link if available. If they are closer than 6 feet, we recommend that you use the serial failover cable as the failover link.



---

**Note**

If you use the same link for both state and failover, you *cannot* use a crossover cable.

---

## Primary and Secondary Vs. Active and Standby

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

However, a few differences exist between the units based on which unit is *primary* and which unit is *secondary*:

- The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).
- The primary unit's MAC addresses are always coupled with the active IP addresses. The exception to this rule occurs when:
  - The secondary unit is active, and cannot obtain the primary's MAC addresses over the failover link.
  - If you hardcode them into the configuration (see the **failover mac address** command in the *Cisco PIX Firewall Command Reference* for more information about setting the MAC addresses).

In cable-based failover, the serial failover cable is marked with one end as “Primary” and the other as “Secondary.” The cable itself determines which unit is primary. In LAN-based failover, you must set the primary and secondary identification in the configuration.

## Configuration Replication

The two PIX Firewall units share the same configuration. The configuration can be the same because it includes both the *active* IP addresses and the *standby* IP addresses. When a unit is active, it uses the active IP addresses; when a unit is standby, it uses the standby IP addresses.



### Note

---

Because the configuration is the same on both units, the host names, usernames, and passwords are also the same.

---

For LAN-based failover, the configuration on the two units differs slightly, because you must set up the Ethernet link in advance. You must also define each unit as a primary or secondary unit within the configuration (as opposed to cable-based failover, where the serial failover cable itself defines these roles).

The active unit sends the configuration in running memory to the standby unit. On the standby unit, the configuration exists only in running memory. You can optionally save the configuration to Flash memory using the **write memory** command. If you save the configuration to Flash memory, and you reboot the standby unit when the active unit is unavailable, the standby unit can become the active unit because it has a valid configuration.



### Note

---

If you enter the **write memory** command on the active unit, the command is replicated to the standby unit, which proceeds to write its configuration to Flash memory.

---

Configuration replication from the active unit to the standby unit occurs in the following ways:

- When the standby unit completes its initial startup, it clears its running configuration using the **clear configure all** command (except for the LAN-based failover commands that are not replicated), and the active unit sends its entire configuration to the standby unit.
- As commands are entered on the active unit, they are sent across the failover link to the standby unit. You do not have to save the active configuration to Flash memory to replicate the commands.
- If you enter the **write standby** command on the active unit, the standby unit clears its running configuration using the **clear configure all** command (except for the LAN-based failover commands that are not replicated), and the active unit sends its entire configuration to the standby unit.

**Note**

---

Changes made on the standby unit are not replicated to the active unit.

---

When you use a serial failover cable, the replication can take a long time to complete with a large configuration.

When the replication starts, the PIX Firewall console displays the message “Sync Started,” and when complete, displays the message “Sync Completed.” During the replication, information cannot be entered on the PIX Firewall console.

## Failover Triggers

If the active unit fails, the standby unit takes over. The following situations cause a failover to occur if they affect the active unit, but not the standby unit:

- Network failure
- PIX Firewall hardware failure
- Power loss or reload

For power loss or reload using cable-based failover, the standby unit learns almost immediately if the active unit loses power or is reset. The other conditions listed previously are sensed when a given interface does not receive hello packets for two consecutive poll intervals. The poll interval is user configurable. The interface is then tested to determine which unit is at fault.

Initially, the PIX Firewall runs the Link Up/Down test, which is a test of the Ethernet card. If an interface card is not plugged into an operational network, it is also considered to be failed (for example, the upstream switch failed, has a failed port, or a cable is unplugged).

If the Link Up/Down test indicates that the Ethernet card is operational, then the firewall 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.

The PIX Firewall performs the following network tests:

1. 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.
2. ARP test—Reading the unit’s ARP cache for the 10 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.

3. Broadcast Ping test—The ping test 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 all network tests fail, then the interface is considered to be failed. If the standby unit has more operational interfaces, then a failover occurs. If both units have similar failures (for example, neither unit can receive upstream traffic), then no failover occurs.

## Failover Configuration Prerequisites

This section describes how to set up your network switches and your PIX Firewall to support failover. It includes the following topics:

- [Configuring Switches to Support Failover, page 10-8](#)
- [Preconfiguring the PIX Firewall for Failover, page 10-8](#)

## Configuring Switches to Support Failover

Perform the following steps on any Cisco switch ports that connect directly to the PIX Firewall:

- 
- Step 1** Enable PortFast.
- Step 2** Turn off trunking.
- Step 3** Turn off channeling.
- 



**Note**

In Cisco Catalyst operating system Version 5.4 and later, you can use the following command to perform steps 1 through 3:

```
set port host
```

The **set port host** command automatically executes the following commands:

```
spantree portfast enable
set trunk off
set port channel off
```

---

## Preconfiguring the PIX Firewall for Failover

This section includes steps that are not directly related to enabling failover, but that are required for failover to work. Follow these steps on the *primary* unit. Steps related only to Stateful Failover are preceded by “(Stateful Failover).”

- 
- Step 1** If you have not done so already, set the time.
- See the “[Managing the PIX Firewall Clock](#)” section in [Chapter 9, “Accessing and Monitoring PIX Firewall,”](#) to set the time.

**Step 2** If an interface is not going to be used, turn off the interface by entering:

```
primary(config)# interface hardware_id shutdown
```

Where *hardware\_id* is **ethernetn** or **gb-ethernetn**.

This step prevents the firewall from expecting hello packets on the interface.

**Step 3** Use the following Ethernet settings for your interfaces:

- **(Stateful Failover)** For the state link for Stateful Failover:

```
primary(config)# interface hardware_id {100full | 1000full}
```



**Note** The maximum transmission unit (MTU) size must be 1500 (the default) or larger on the state link. Use the **mtu** command if necessary.

- For all other Ethernet interfaces:

Any setting except the **auto** or the **1000auto** options. Auto detection is not always reliable, and PDM enforces this setting.

To view **interface** commands in your configuration, use the **write terminal** command. Reenter an interface with new information to correct a command you wish to change.

**Step 4** Take note of the IP addresses you configured on your interfaces using the **ip address** command.

These IP addresses are used by the active unit, but you should take note of them, because the failover IP addresses used on the standby unit must be on the same subnet.

## Configuring Cable-Based Failover

Follow these steps to configure failover using the serial failover cable as the failover link. The commands in this task apply to the *primary* unit. Steps related only to Stateful Failover are specified by “(Stateful Failover).”



**Note** At any time during the procedure, you can enter the **show failover** command to see the failover status. See the “[Using the Show Failover Command](#)” section for detailed information.

	Step/Command	Description
<b>Step 1</b>	Connect the failover cable to the PIX Firewall units.	Ensure that the end of the cable marked “Primary” attaches to the unit you want to use as the primary unit and that the end marked “Secondary” connects to the unit you want to use as the secondary unit.

	Step/Command	Description
<b>Step 2</b>	If you have not done so already, configure the Ethernet interface you are using for the Stateful Failover link:	(Stateful Failover)
<b>a.</b>	<pre>primary(config)# interface hardware_id hardware_speed</pre>	<p>Enables the interface.</p> <ul style="list-style-type: none"> <li>• <i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li>• <i>hardware_speed</i>—The hardware speed and duplex for the Ethernet interface. The state link must be at least 100 Mbps, full duplex: <ul style="list-style-type: none"> <li>– <b>100full</b>—100 Mbps full duplex</li> <li>– <b>1000full</b>—Auto negotiate, advertising 1000 Mbps full duplex</li> <li>– <b>1000full nonegotiate</b>—Force link to 1000 Mbps full duplex</li> </ul> </li> </ul> <p>For example:</p> <pre>primary(config)# interface ethernet3 100full</pre>
<b>b.</b>	<pre>primary(config)# nameif hardware_id interface_name securitylevel</pre>	<p>Names the interface and sets the security level.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• <i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li>• <i>interface_name</i>—A string describing the interface.</li> <li>• <i>securitylevel</i>—A number between 1 and 99. 0 and 100 are reserved for the inside and outside interfaces. Because this interface is a dedicated link, the security level can be any number.</li> </ul> <p>For example:</p> <pre>primary(config)# nameif ethernet3 state security80</pre>
<b>c.</b>	<pre>primary(config)# ip address interface_name ip_address [netmask]</pre>	<p>Sets the IP address.</p> <p>For example:</p> <pre>primary(config)# ip address state 192.168.2.1 255.255.255.0</pre>

	Step/Command	Description
Step 3	<code>primary(config)# failover ip address interface_name ip_address</code>	<p>For each interface that has an IP address, this command identifies the failover IP address. This IP address is used on the standby unit.</p> <p>This IP address must be in the same subnet as the active IP address. You do not need to identify the subnet mask. To check the current IP address settings, enter the <b>show ip address</b> command.</p> <p>You must use static IP addresses with failover configurations; you cannot use IP addresses obtained through DHCP or PPPoE.</p> <p>The following example sets the IP addresses for the active unit and for the standby unit:</p> <pre>primary(config)# ip address inside 10.1.1.1 255.255.255.0 primary(config)# failover ip address inside 10.1.1.2 primary(config)# ip address outside 192.168.1.1 255.255.255.0 primary(config)# failover ip address outside 192.168.1.2 primary(config)# ip address state 192.168.2.1 255.255.255.0 primary(config)# failover ip address state 192.168.2.2</pre>
Step 4	<code>primary(config)# failover link interface_name</code>	<p><b>(Stateful Failover)</b> Specifies the state link interface.</p> <p>For example, to set the “state” interface as the state link, enter:</p> <pre>primary(config)# failover link state</pre>
Step 5	<code>primary(config)# failover poll seconds</code>	<p>(Optional) Sets a time shorter than 15 seconds for the units to exchange “hello” packets.</p> <p>Where <i>seconds</i> is an integer between 3 and 15. The default is 15 seconds.</p> <p>You might want to set a lower value for Stateful Failover, to make sure that the state information is up to date. With a faster poll time, the PIX Firewall can detect failure faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.</p>
Step 6	<code>primary(config)# failover</code>	Enables failover.
Step 7	If you have not already done so, power on the secondary unit.	The active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages “Sync Started” and “Sync Completed” appear on the primary console.
Step 8	<code>primary(config)# write memory</code>	Saves the primary configuration to Flash memory. Because this command is replicated to the standby unit, the standby unit also saves its configuration to Flash memory.

## Configuring LAN-Based Failover

This section describes how to configure failover using an Ethernet failover link. This section includes the following topics:

- [Configuring the Primary Unit, page 10-12](#)
- [Configuring the Secondary Unit, page 10-15](#)

**Note**

If you are changing from cable-based failover to LAN-based failover, complete all the steps in the following procedures that you did not already complete when you initially set up cable-based failover. For example, you might need to configure the **failover ip address** command for the failover link, but you do not need to reconfigure all the other failover IP addresses.

## Configuring the Primary Unit

Follow these steps to configure the primary unit for LAN-based failover. Steps related only to Stateful Firewall are preceded by “(Stateful Failover).”

**Note**

At any time during the procedure, you can enter the **show failover** command to see the failover status. See the “[Using the Show Failover Command](#)” section for detailed information.

	Step/Command	Description
<b>Step 1</b>	If you have not done so already, configure the Ethernet interface you are using for the failover link:	Note these settings because you must use the same settings on the secondary unit.
<b>a.</b>	<pre>primary(config)# interface hardware_id hardware_speed</pre>	<p>Enables the interface.</p> <ul style="list-style-type: none"> <li>• <i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li>• <i>hardware_speed</i>—The hardware speed and duplex for the Ethernet interface. Do not use <b>auto</b> or <b>1000auto</b>. Auto detection is not always reliable, and PDM enforces this setting. <ul style="list-style-type: none"> <li>– <b>10baseT</b>—10 Mbps half duplex</li> <li>– <b>10full</b>—10 Mbps full duplex</li> <li>– <b>100baseTX</b>—100 Mbps half duplex</li> <li>– <b>100full</b>—100 Mbps full duplex</li> <li>– <b>1000full</b>—Auto negotiate, advertising 1000 Mbps full duplex</li> <li>– <b>1000full nonegotiate</b>—Force link to 1000 Mbps full duplex</li> </ul> </li> </ul> <p>For example:</p> <pre>primary(config)# interface ethernet2 100full</pre>

	Step/Command	Description
b.	<pre>primary(config)# nameif hardware_id interface_name securitylevel</pre>	<p>Names the interface and sets the security level.</p> <p>Where:</p> <ul style="list-style-type: none"> <li><i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li><i>interface_name</i>—A string describing the interface.</li> <li><b>securitylevel</b>—A number between 1 and 99. 0 and 100 are reserved for the inside and outside interfaces. Because this interface is a dedicated link, the security level can be any number.</li> </ul> <p>For example:</p> <pre>primary(config)# nameif ethernet2 faillink security90</pre>
c.	<pre>primary(config)# ip address interface_name ip_address [netmask]</pre>	<p>Sets the IP address. This address is used on the primary unit even when it changes to standby state.</p> <p>For example:</p> <pre>primary(config)# ip address faillink 192.168.2.1 255.255.255.0</pre>
<b>Step 2</b>	If you have not done so already, configure the Ethernet interface you are using for the Stateful Failover link:	<b>(Stateful Failover)</b>
a.	<pre>primary(config)# interface hardware_id hardware_speed</pre>	<p>Enables the interface.</p> <ul style="list-style-type: none"> <li><i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li><i>hardware_speed</i>—The hardware speed and duplex for the Ethernet interface. The state link must be at least 100 Mbps, full duplex: <ul style="list-style-type: none"> <li><b>100full</b>—100 Mbps full duplex</li> <li><b>1000full</b>—Auto negotiate, advertising 1000 Mbps full duplex</li> <li><b>1000full nonegotiate</b>—Force link to 1000 Mbps full duplex</li> </ul> </li> </ul> <p>For example:</p> <pre>primary(config)# interface ethernet3 100full</pre>
b.	<pre>primary(config)# nameif hardware_id interface_name securitylevel</pre>	<p>Names the interface and sets the security level.</p> <p>Where:</p> <ul style="list-style-type: none"> <li><i>hardware_id</i>—<b>ethernetn</b> or <b>gb-ethernetn</b>.</li> <li><i>interface_name</i>—A string describing the interface.</li> <li><b>securitylevel</b>—A number between 1 and 99. 0 and 100 are reserved for the inside and outside interfaces. Because this interface is a dedicated link, the security level can be any number.</li> </ul> <p>For example:</p> <pre>primary(config)# nameif ethernet3 state security80</pre>

	Step/Command	Description
c.	<pre>primary(config)# ip address interface_name ip_address [netmask]</pre>	<p>Sets the IP address.</p> <p>For example:</p> <pre>primary(config)# ip address state 192.168.3.1 255.255.255.0</pre>
Step 3	<pre>primary(config)# failover ip address interface_name ip_address</pre>	<p>For each interface that has an IP address, this command identifies the failover IP address. This IP address is used on the standby unit.</p> <p>This IP address must be in the same subnet as the active IP address. You do not need to identify the subnet mask. To check the current IP address settings, enter the <b>show ip address</b> command.</p> <p>You must use static IP addresses with failover configurations; you cannot use IP addresses obtained through DHCP or PPPoE.</p> <p><b>Note</b> You must set the failover IP address for the failover link, even though the failover link IP address and MAC address <i>do not</i> change at failover. The active IP address always stays with the primary unit, while the failover IP address stays with the secondary unit.</p> <p>The following example sets the IP addresses for the active unit and for the standby unit:</p> <pre>primary(config)# ip address inside 10.1.1.1 255.255.255.0 primary(config)# failover ip address inside 10.1.1.2 primary(config)# ip address outside 192.168.1.1 255.255.255.0 primary(config)# failover ip address outside 192.168.1.2 primary(config)# ip address faillink 192.168.2.1 255.255.255.0 primary(config)# failover ip address faillink 192.168.2.2 primary(config)# ip address state 192.168.3.1 255.255.255.0 primary(config)# failover ip address state 192.168.3.2</pre>
Step 4	<pre>primary(config)# failover link interface_name</pre>	<p><b>(Stateful Failover)</b> Specifies the state link interface.</p> <p>For example, to set the “state” interface as the state link, enter:</p> <pre>primary(config)# failover link state</pre>
Step 5	<pre>primary(config)# failover poll seconds</pre>	<p>(Optional) Sets a time shorter than 15 seconds for the units to exchange “hello” packets.</p> <p>Where <i>seconds</i> is an integer between 3 and 15. The default is 15 seconds.</p> <p>You might want to set a lower value for Stateful Failover, to make sure that the state information is up to date. With a faster poll time, the PIX Firewall can detect failure faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.</p>
Step 6	<pre>primary(config)# failover lan unit primary</pre>	<p>Sets this PIX Firewall as the primary unit.</p>

	Step/Command	Description
Step 7	<code>primary(config)# failover lan interface interface_name</code>	Identifies the Ethernet interface for the failover link. For example, enter: <code>primary(config)# failover lan interface faillink</code>
Step 8	<code>primary(config)# failover lan key string</code>	(Optional) Encrypts the failover communications over the Ethernet link. If you do not enter this command, all failover communications are sent in clear text. Where <i>string</i> is a shared key.
Step 9	<code>primary(config)# failover lan enable</code>	Enables the LAN-based failover link, instead of the default serial failover cable link.
Step 10	<code>primary(config)# failover</code>	Enables failover.
Step 11	<code>primary(config)# write memory</code>	Saves the configuration to Flash memory.

## Configuring the Secondary Unit

Follow these steps to configure the secondary unit for LAN-based failover. The only configuration required for the secondary unit is for the failover interface and for LAN failover parameters. The secondary unit requires these commands to initially communicate with the primary unit. After the primary unit sends its configuration to the secondary unit, the only permanent difference between the two configurations is the **failover lan unit** command, which identifies each unit as primary or secondary. Although all other **failover lan** commands are the same on both units, these commands are not replicated from the active unit to the standby unit and must be saved in Flash memory.



**Note** At any time during the procedure, you can enter the **show failover** command to see the failover status. See the [“Using the Show Failover Command”](#) section for detailed information.

	Step/Command	Description
Step 1	Configure the Ethernet interface you are using for the failover link:	Use the same settings as the primary unit. See <a href="#">“Configuring the Primary Unit”</a> for details about the following commands.
a.	<code>secondary(config)# interface hardware_id hardware_speed</code>	Enables the interface. For example: <code>secondary(config)# interface ethernet2 100full</code>
b.	<code>secondary(config)# nameif hardware_id interface_name securitylevel</code>	Names the interface and sets the security level. For example: <code>secondary(config)# nameif ethernet2 faillink security90</code>

	Step/Command	Description
c.	<code>secondary(config)# ip address interface_name ip_address [netmask]</code>	Set the IP address to match the IP address on the primary unit. The secondary unit does not use this IP address, but instead uses the failover IP address you set in the next step. However, you must still set the primary IP address.  For example:  <code>secondary(config)# ip address faillink 192.168.2.1 255.255.255.0</code>
Step 2	<code>secondary(config)# failover ip address interface_name ip_address</code>	Set the failover IP address to match the failover IP address on the primary unit. You do not need to identify the subnet mask. This secondary unit always uses this IP address for the failover link.  For example:  <code>secondary(config)# failover ip address faillink 192.168.2.2</code>
Step 3	<code>secondary(config)# failover lan unit secondary</code>	(Optional) Sets this PIX Firewall as the secondary unit. If you do not enter this command, the default is secondary.
Step 4	<code>secondary(config)# failover lan interface interface_name</code>	Identifies the Ethernet interface for the failover link.  For example, enter:  <code>secondary(config)# failover lan interface faillink</code>
Step 5	<code>secondary(config)# failover lan key string</code>	(Optional) Encrypts the failover communications over the Ethernet link. Use the same key as the one you set for the primary unit.  Where <i>string</i> is a shared key.
Step 6	<code>secondary(config)# failover lan enable</code>	Enables the LAN-based failover link.
Step 7	<code>secondary(config)# write memory</code>	Because the <b>failover lan</b> commands are not replicated from the active unit to the standby unit, you should save them in Flash memory.
Step 8	<code>secondary(config)# failover</code>	Enables failover. After you enable failover, the active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages “Sync Started” and “Sync Completed” appear on the active unit’s console.
Step 9	<code>secondary(config)# write memory</code>	(Optional) After the “Sync Completed” message appears on the active unit, you can save the entire configuration on the standby unit to Flash memory (in addition to the <b>failover lan</b> commands you saved in Step 7).

## Verifying the Failover Configuration

This section describes how to verify your failover configuration. This section includes the following topics:

- [Using the Show Failover Command, page 10-17](#)
- [Testing the Failover Functionality, page 10-20](#)

See the “[Monitoring Failover](#)” section for other troubleshooting tools.

## Using the Show Failover Command

On each unit, you can verify the failover status by entering:

```
primary(config)# show failover
```

This command shows:

- Whether failover is on or off
- Which unit is active
- The IP addresses assigned for the active and standby units
- The serial cable status
- The LAN cable status
- Stateful Failover statistics



### Note

The **show interface** display on the standby unit shows the active IP addresses associated with each interfaces, even though the unit is using the failover IP addresses. Use the **show failover** command to view the actual IP addresses being used.

See the following sample **show failover** command output. A description of each field follows.

```
pix(config)# show failover
Failover On
Serial Failover Cable status: My side not connected
Reconnect timeout 0:00:00
Poll frequency 15 seconds
Last Failover at: 18:32:16 UTC Mon Apr 7 2003
  This host: Primary - Active
    Active time: 510 (sec)
    Interface 4th (172.16.1.1): Normal
    Interface intf2 (192.168.2.1): Normal
    Interface outside (192.168.1.1): Normal
    Interface inside (10.1.1.1): Normal
  Other host: Secondary - Standby
    Active time: 0 (sec)
    Interface 4th (172.16.1.2): Normal
    Interface intf2 (192.168.2.2): Normal
    Interface outside (192.168.1.2): Normal
    Interface inside (10.1.1.2): Normal
Stateful Failover Logical Update Statistics
Link : 4th
Stateful Obj   xmit   xerr   rcv    rerr
General        0       0       0      0
sys cmd        0       0       0      0
up time        0       0       0      0
xlate          0       0       0      0
tcp conn       0       0       0      0
udp conn       0       0       0      0
ARP tbl        0       0       0      0
RIP Tbl        0       0       0      0
```

```

Logical Update Queue Information
          Cur      Max      Total
Recv Q:   0        0        0
Xmit Q:   0        0        0

```

```

Lan Based Failover is Active
  interface intf3 (192.168.3.1): Normal, peer (192.168.3.2) Normal

```

**Table 10-2 Show Failover Display Description**

Field	Options
Failover	<ul style="list-style-type: none"> <li>On</li> <li>Off</li> </ul>
Serial Failover Cable status:	<ul style="list-style-type: none"> <li>Normal—The cable is connected to both units, and they both have power.</li> <li>My side not connected—The serial cable is not connected to this unit. It is unknown if the cable is connected to the other unit.</li> <li>Other side is not connected—The serial cable is connected to this unit, but not to the other unit.</li> <li>Other side powered off—The other unit is turned off.</li> </ul>
Reconnect timeout	Not used.
Poll frequency	<i>n</i> seconds The number of seconds you set with the <b>failover poll</b> command. The default is 15 seconds.
Last Failover at:	The date and time of the last failover in the following form: <i>hh:mm:ss UTC DayName Month Day yyyy</i> UTC (Coordinated Universal Time) is equivalent to GMT (Greenwich Mean Time).
This host:	For each host, the display shows the following information.
Other host:	
Primary or Secondary	<ul style="list-style-type: none"> <li>Active</li> <li>Standby</li> </ul>
Active time:	<i>n</i> (sec) The amount of time the unit has been active. This time is cumulative, so the standby unit, if it was active in the past, will also show a value.

**Table 10-2 Show Failover Display Description (continued)**

Field	Options
Interface name (n.n.n.n):	<p>For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions:</p> <ul style="list-style-type: none"> <li>Failed—The interface has failed.</li> <li>Link Down—The interface line protocol is down.</li> <li>Normal—The interface is working correctly.</li> <li>Shutdown—The interface has been administratively shut down (<b>interface hardware_id shutdown</b>).</li> <li>Unknown—The firewall cannot determine the status of the interface.</li> <li>Waiting—Monitoring of the other unit's network interface has not yet started.</li> </ul> <p>The LAN failover interface is not included in this list, but is shown at the bottom of the display.</p>
Stateful Failover Logical Update Statistics	<p>The following fields relate to the Stateful Failover feature. If the Link field shows an interface name, the Stateful Failover statistics are shown.</p>
Link	<ul style="list-style-type: none"> <li><i>interface_name</i>—The interface used for the Stateful Failover link.</li> <li>Unconfigured—You are not using Stateful Failover.</li> </ul>
Stateful Obj	<p>For each field type, the following statistics are used:</p> <ul style="list-style-type: none"> <li>xmit—Number of transmitted packets to the other unit</li> <li>xerr—Number of errors that occurred while transmitting packets to the other unit</li> <li>rcv—Number of received packets</li> <li>rerr—Number of errors that occurred while receiving packets from the other unit</li> </ul>
General	Sum of all stateful objects.
sys cmd	Logical update system commands; for example, LOGIN and Stay Alive.
up time	Up time, which the active unit passes to the standby unit.
xlate	Translation information.
tcp conn	TCP connection information.
udp conn	Dynamic UDP connection information.
ARP tbl	Dynamic ARP table information.
RIP Tbl	Dynamic router table information.
Logical Update Queue Information	<p>For each field type, the following statistics are used:</p> <ul style="list-style-type: none"> <li>Cur—Current number of packets</li> <li>Max—Maximum number of packets</li> <li>Total—Total number of packets</li> </ul>
Recv Q	The status of the receive queue.

**Table 10-2 Show Failover Display Description (continued)**

Field	Options
Xmit Q	The status of the transmit queue.
Lan-based Failover is Active	This field appears only when LAN-based failover is enabled.
interface <i>name</i> ( <i>n.n.n.n</i> ): peer ( <i>n.n.n.n</i> ):	For the LAN failover link, the display shows the IP address currently being used on each unit, as well as the condition of the link. See the preceding <b>interface</b> description for a description of each condition.

## Testing the Failover Functionality

Follow these steps to ensure failover works:

- 
- Step 1** Power up the standby unit.
  - Step 2** Test that your primary (active) unit is passing traffic as expected by using FTP (for example) to send a file between hosts on different interfaces.
  - Step 3** Power up the standby unit, and wait for the configuration to sync.
  - Step 4** Power down the active unit to force a failover to the standby unit.
  - Step 5** Use FTP to send another file between the same two hosts.
  - Step 6** If the network test was successful, power on the primary unit. If the test was not successful, enter the **show failover** command to check the failover status.
  - Step 7** When you are finished, you can leave the secondary unit as active, or force the primary unit to be active again by entering:

```
primary(config)# failover active
```

---

## Forcing Failover

To force the standby unit to become active, enter:

- On the active unit:  

```
primary(config)# no failover active
```
- On the standby unit:  

```
secondary(config)# failover active
```

## Disabling Failover

You can disable failover by entering the following command on the active unit:

```
primary(config)# no failover
```

This command is replicated to the standby unit, so that it also has failover disabled. To verify that failover is off, enter the **show failover** command:

```
primary(config)# show failover
```

```
Failover Off  
...
```

To disable the LAN failover link, disable failover and then disable the LAN failover link:

```
primary(config)# no failover  
primary(config)# no failover lan enable
```

When you enable failover again, the firewall uses the serial failover cable if connected.

## Monitoring Failover

When a failover occurs, both PIX Firewalls send out syslog messages, and the ACTIVE light on the front of the devices indicate the current state. This section includes the following topics:

- [Failover Syslog Messages, page 10-21](#)
- [SNMP, page 10-21](#)
- [Debugging Command, page 10-21](#)
- [ACTIVE Light, page 10-21](#)

## Failover Syslog Messages

The PIX Firewall issues a number of syslog messages related to failover at priority level 2, which indicates a critical condition. To view these messages, see the *Cisco PIX Firewall System Log Messages* to enable logging and to see descriptions of the syslog messages. If you search for “failover” on the following web page, you can easily find related messages:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_sw/v\\_63/63syslog/pixemsgs.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63syslog/pixemsgs.htm)

## 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** command in the *Cisco PIX Firewall Command Reference* for more information.

## Debugging Command

To see debugging messages, enter the **debug fover** command. See the *Cisco PIX Firewall Command Reference* for more information, or see the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_sw/v\\_63/cmdref/df.htm#94643](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/df.htm#94643)

## ACTIVE Light

The ACTIVE light on the front of the firewall indicates the unit’s failover state, either active (light is on) or standby (light is off). If you do not enable failover, the ACTIVE light remains on.

# Frequently Asked Failover Questions

This section contains some frequently asked questions about the failover features and includes the following topics:

- [Configuration Replication Questions, page 10-23](#)
- [Basic Failover Questions, page 10-23](#)
- [Cable-Based Failover Questions, page 10-24](#)
- [LAN-Based Failover Questions, page 10-25](#)
- [Stateful Failover Questions, page 10-25](#)

## Configuration Replication Questions

- Does configuration replication save the configuration to Flash memory on the standby unit?  
No, the configuration is only in running memory.
- How can both units be configured the same without manually entering the configuration twice?  
Commands entered on the active unit are automatically replicated to the standby unit.
- What happens if I enter commands on the standby unit?  
You will see an error message telling you that the configurations are out of sync.  
If you enter individual commands on the active unit that are replicated to the standby unit, your alterations are preserved.  
If you use the **write standby** command on the active unit, it will erase any new commands you entered on the standby unit.
- What happens if I enter the **write memory** command on the active unit?  
The **write memory** command is replicated to the standby unit, which proceeds to write its configuration to Flash memory.
- What happens if the configuration in Flash memory on the secondary unit differs from the configuration on the primary unit?  
After startup, the primary unit sends its configuration to the secondary unit, and erases the secondary unit's running configuration. However, the secondary unit's configuration remains unaltered in Flash memory.
- How can I view the running configuration and the Flash memory configuration?
  - **show running**—Shows the running configuration. You can also enter **write terminal**.
  - **show config**—Shows the configuration in Flash memory.

## Basic Failover Questions

- Which unit becomes active if you restart both units?  
The primary unit.
- What happens if the active unit has a power failure?
  - Cable-based—The standby unit learns immediately of the active power failure, and becomes active.
  - LAN-based—After hello packets are not acknowledged, the standby unit becomes active. There is a slight delay compared to cable-based failover.
- What happens when the formerly active unit comes online again?  
No failover occurs. It remains in standby mode.

- How long does it take to detect a failure?
  - Network errors are detected within two consecutive polling intervals (by default, 15 second intervals). The polling interval is user-configurable using the **failover poll** command.
  - (Cable-based only) Power failure and cable failure is detected immediately.
  - Failover communication errors are detected within two consecutive polling intervals.
- What maintenance is required?
 

Syslog messages are generated when any errors or switches occur. Evaluate the failed unit and fix or replace it.
- Can you put a router between the PIX Firewall units?
 

No, all interfaces of the two units must be on the same subnet.
- Is it possible to have both PIX Firewall units become active at the same time?
 

Yes, in the following rare circumstances:

  - Cable-based failover only
  - The failover link is unplugged at startup
  - Both units have configurations in Flash memory
  - Both units have failover enabled
  - Both units have the UR license

In LAN-based failover, if the failover link is down, the secondary unit uses other interfaces to detect if the primary unit is active, and does not become active itself.
- What prevents the standby unit from passing traffic?
 

The PIX Firewall failover feature ensures that only traffic aimed *to* the standby unit (hello packets, Telnet if enabled) is successful, while traffic aimed *through* the unit is dropped.

## Cable-Based Failover Questions

- What happens if the cable is disconnected at startup?
 

The primary unit becomes active. If the primary unit fails, the secondary unit does not become active until the cable is reconnected.

Note that both units can become active in the following rare circumstances:

  - Both units have configurations in Flash memory
  - Both units have failover enabled
  - Both units have the UR license
- What happens if the cable becomes unplugged after startup?
 

The firewall generates a syslog message but no switching occurs. No failover can occur until the cable is reconnected.

## LAN-Based Failover Questions

- What happens if the failover link is disconnected at startup?

The primary unit becomes active. The secondary unit uses other interfaces to detect if the primary unit is active, and does not become active itself. If the primary unit is not active, then the secondary unit waits a brief period before becoming active.

- What happens if the link goes down between the firewall and the switch after startup?
  - If the active unit's failover interface goes down, it will failover to the standby unit. No additional failovers can occur until the failover interface comes back up again.
  - If the standby unit's failover interface goes down, an error message displays, but no failover occurs. No failover can occur until the cable is reconnected.
- What happens if the failover link is not down, but does not pass traffic (for example, each PIX Firewall is connected to a separate switch and the link between the two switches is down)?

The PIX Firewalls use other interfaces to poll the peer status, but a failover is not triggered. If the units detect other failover triggers, and a failover occurs, no additional failovers can occur until the failover interface comes back up again.

- Can I use a crossover cable?

No, you must use a switch between the two units. We recommend that if your units are closer than 6 feet (which is when you would use a crossover cable), then you should use the serial failover cable. You can use a crossover cable for the state link for Stateful Failover.

## Stateful Failover Questions

- What information is *not* replicated to the standby PIX Firewall on Stateful Failover?
  - The user authentication (uauth) table.
  - The ISAKMP and IPSec SA table.
  - The ARP table.
  - Routing information.
  - Other UDP connections.
- What are Stateful Failover hardware requirements?
  - An Ethernet link dedicated to Stateful Failover.
  - Minimum 100 Mbps full duplex. On a PIX 535 with GE interfaces, you must use a GE interface for the state link.
  - A connection using a crossover cable or a switch.
- Can I share the state link Ethernet interface with the failover link?

Yes, if you are connecting to a switch, and not using a crossover cable. However, we recommend that you use a separate connection.

# Failover Configuration Examples

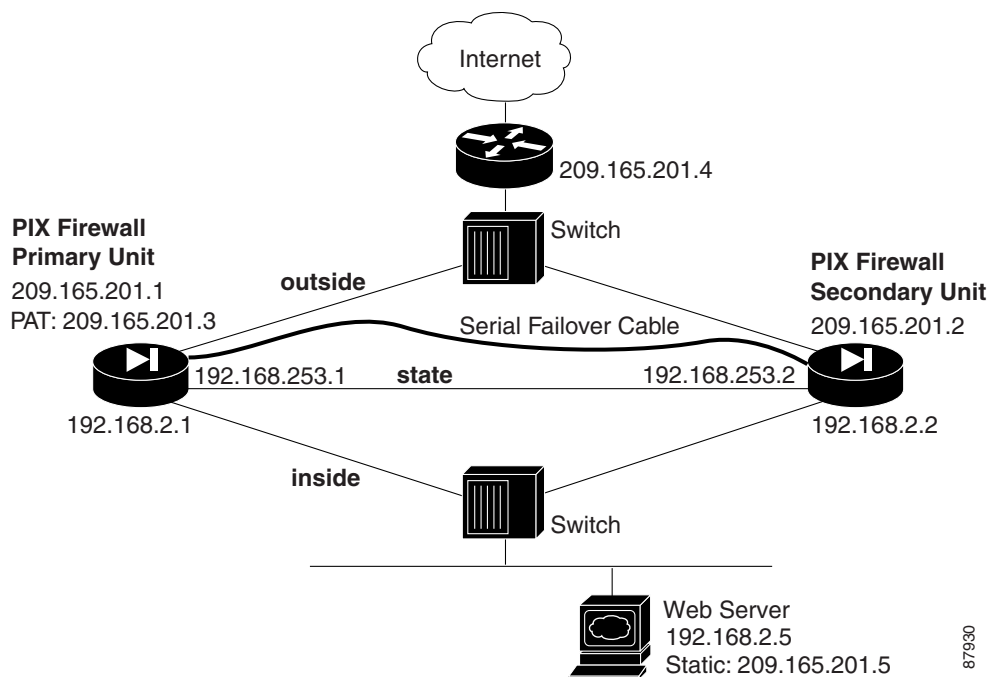
This section includes sample configurations and network diagrams, and includes the following topics:

- [Cable-Based Failover Example, page 10-26](#)
- [LAN-Based Failover Example, page 10-27](#)

## Cable-Based Failover Example

Figure 10-2 shows the network diagram for a failover configuration using a serial failover cable.

**Figure 10-2 Cable-Based Failover Configuration**



Example 10-1 lists the typical commands in a cable-based failover configuration.

**Example 10-1 Cable-Based Failover Configuration**

```
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shutdown
interface ethernet3 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet3 state security20
enable password farscape encrypted
password crichton encrypted
telnet 192.168.2.45 255.255.255.255
hostname pixfirewall
ip address outside 209.165.201.1 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address state 192.168.253.1 255.255.255.252
```

87930

```

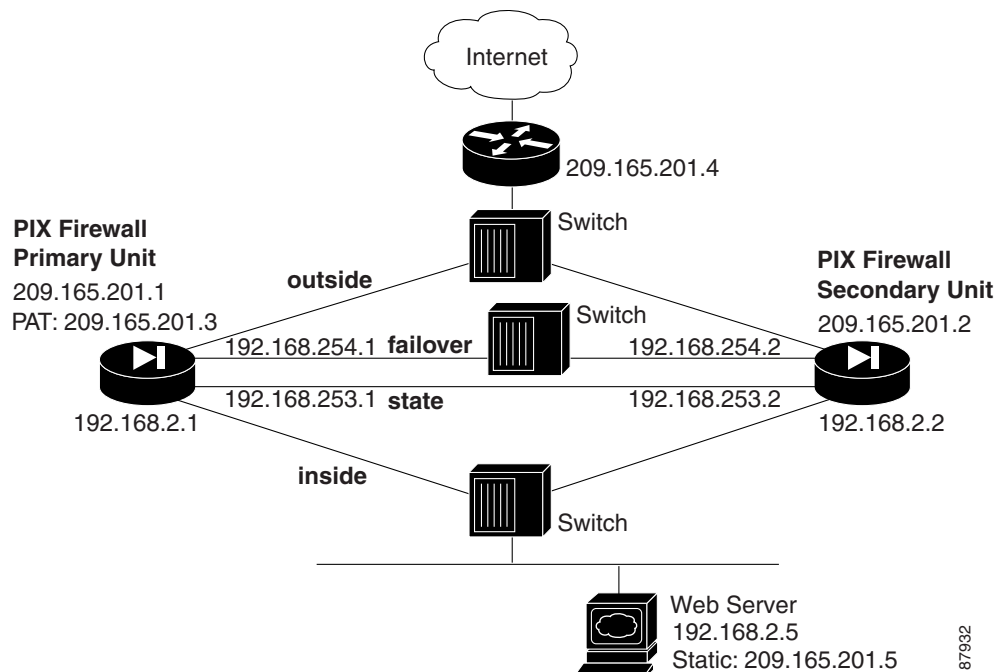
failover ip address outside 209.165.201.2
failover ip address inside 192.168.2.2
failover ip address state 192.168.253.2
failover link state
failover
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-list acl_out permit tcp any 209.165.201.5 eq 80
access-group acl_out in interface outside
route outside 0 0 209.165.201.4 1

```

## LAN-Based Failover Example

Figure 10-3 shows the network diagram for a failover configuration using an Ethernet failover link.

**Figure 10-3 LAN-Based Failover Configuration**



Example 10-2 (primary unit) and Example 10-3 (secondary unit) list the typical commands in a LAN-based failover configuration.

### Example 10-2 LAN-Based Failover Configuration: Primary Unit

```

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 failover security10
nameif ethernet3 state security20
enable password farscape encrypted
password crichton encrypted

```

```

telnet 192.168.2.45 255.255.255.255
hostname pixfirewall
ip address outside 209.165.201.1 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address failover 192.168.254.1 255.255.255.0
ip address state 192.168.253.1 255.255.255.252
failover ip address outside 209.165.201.2
failover ip address inside 192.168.2.2
failover ip address failover 192.168.254.2
failover ip address state 192.168.253.2
failover link state
failover lan unit primary
failover lan interface failover
failover lan key 12345678
failover lan enable
failover
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-list acl_out permit tcp any host 209.165.201.5 eq 80
access-group acl_out in interface outside
route outside 0 0 209.165.201.4 1

```

[Example 10-3](#) shows the configuration for the secondary unit.

### **Example 10-3 LAN-Based Failover Configuration: Secondary Unit**

```

interface ethernet2 100full
nameif ethernet2 failover security10
ip address failover 192.168.254.1 255.255.255.0
failover ip address failover 192.168.254.2
failover lan unit secondary
failover lan interface failover
failover lan key 12345678
failover lan enable
failover

```