



Using PIX Firewall Failover

This chapter describes the PIX Firewall failover feature, which lets you add a second PIX Firewall unit that takes control if the primary unit fails. It includes the following topics:

- [Failover Unit System Requirements](#)
- [Understanding Failover](#)
- [Configuring Failover with a Failover Cable](#)
- [Configuring LAN-Based Failover](#)
- [Changing from Cable-Based Failover to LAN-Based Failover](#)
- [Verifying Failover Configuration](#)
- [Additional Failover Information](#)
- [Failover Configuration Examples](#)



Note

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

Failover Unit System Requirements

Failover requires two units that are identical in the following respects:

- Platform type (a PIX 515E *cannot* be used with a PIX 515)
- Software version
- Activation key type (DES or 3DES)
- Flash memory
- Amount of RAM

One of the failover units must have an Unrestricted license (UR), while the other can have a Failover (FO) or UR license. Restricted units cannot be used for failover and two units with FO licenses cannot be used in a single failover pair. The PIX 515, PIX 515E, PIX 525, and PIX 535 can be used for failover if you have the optional Unrestricted (UR) license.



Note

Neither PIX 501 or PIX 506/506E units can be used for failover, either as the primary or secondary unit.

Understanding Failover

Failover lets you connect a second PIX Firewall unit to your network to protect your network should the first unit go off line. If you use Stateful Failover, you can maintain operating state for the TCP connection during the failover from the primary unit to the standby unit.

When failover occurs, each unit changes state. The unit that activates assumes the IP and MAC addresses of the previously active unit and begins accepting traffic. The new standby unit assumes the failover IP and MAC addresses of the unit that was previously the active unit. Because network devices see no change in these addresses, no ARP entries change or time out anywhere on the network.

Once you configure the primary unit and attach the necessary cabling, the primary unit automatically copies the configuration over to the standby unit.

The ACT indicator light on the front of the PIX 515, PIX 525, and PIX 535 is on when the unit is the active failover unit. If failover is not enabled, this light is on. If failover is present, the light is on when the unit is the active unit and off when the unit is the standby unit.

Failover works with all Ethernet interfaces.



Note

For Stateful Failover on a PIX 535, if you have Gigabit Ethernet (GE) interfaces, then the failover link must be GE.

Cabling two PIX Firewall units together for failover requires a high-speed serial cable when using cable-based failover, or a dedicated Ethernet connection to a dedicated switch (or VLAN) when using LAN-based failover. If you are using Stateful Failover, a separate dedicated connection is required when running cable-based failover and is recommended when running LAN-based failover. The minimum connection speed for a Stateful Failover link is 100 Mbps full-duplex.



Caution

You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports.

The failover feature causes the PIX Firewall to ARP for itself every 15 seconds (depending on the time set with the **failover poll** command). This ARPing can only be stopped by disabling failover.



Note

Improper use of the **static** command on an interface may prevent failover from functioning correctly.

The **static** command, used without a specific port, translates the address of any traffic received on an interface. However, a standby failover unit must be able to communicate with the active unit on each enabled interface to determine if the interface is still active.

For example, the following command would break failover communication between a pair of PIX Firewall units and should NOT be used:

```
static (inside,outside) interface 192.168.100.1
```

This command causes all traffic received on the outside interface to be translated and forwarded to IP address 192.168.100.1, including the failover messages sent by the standby unit. Because the standby unit does not receive a reply to these messages, it assumes that the interface is down and becomes the active unit.

To create a static translation without breaking failover, include a port number with the **static** command. When you specify the port number, only traffic to that port will be translated. Because failover uses a unique port number (port 105), it will not be translated. For example, the following command works properly with failover:

```
static (inside, outside) tcp interface 80 192.168.100.1 80
```

This use of the **static** command only translates HTTP traffic (port 80), so failover messages are not affected. If you need to translate other kinds of traffic, issue the **static** command for each port number.

Configuring the primary PIX Firewall for failover requires using the following commands:

- **failover** command to enable failover
- **failover ip address** command to assign IP addresses to the standby unit
- **failover link** command to enable Stateful Failover
- **failover lan** command to configure LAN-based failover

**Note**

See “[Additional Failover Information](#)” for information on Stateful Failover, how failover occurs, and frequently asked questions.

Configuring Failover with a Failover Cable

For failover, both PIX Firewall units should be the same model number, have at least as much RAM, have the same Flash memory size, and be running the same software version.

**Note**

If you have already powered on the standby unit, power it off and leave it off until instructed in the steps that follow.

Follow these steps to configure failover:

- Step 1** Because the PIX Firewall clock is stored in the CMOS, if you have not done so already, specify the **clock set time** command on the active PIX Firewall to synchronize the time on both PIX Firewall units.
- Step 2** Attach a network cable between the primary and secondary units for each network interface to which you have configured an IP address.
- Step 3** Connect the failover cable to the primary PIX Firewall unit ensuring that the end of the cable marked “Primary” attaches to the primary unit and that the end marked “Secondary” connects to the secondary unit.
- Step 4** *Only configure the primary unit.* Changes made to the standby unit are not copied to the primary unit and are lost during the next reboot. When you are done configuring the PIX Firewall and enter the **write memory** command to save the configuration to Flash memory, the primary unit automatically updates the secondary unit.

**Note**

Do not power on the secondary unit until prompted by the system. First configure the primary unit and then power on the secondary unit only when prompted to do so.

- Step 5** Enter configuration mode with the **configure terminal** command.

- Step 6** Ensure that you have not used the **auto** or the **1000auto** option in any **interface** command in your configuration. 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. Always specify the speed for the interface, such as **10baset** for 10 Mbps or **100basetx** for 100 Mbps. Ensure that the same speeds and duplexes are the same for any devices on the subnets including switches and routers.



Note If you are using Stateful Failover, set the Stateful Failover dedicate interface speed using the **100full** or **1000sxfull** option to the **interface** command. This is extremely important and should be performed even if you are using a crossover connector to connect the PIX Firewall units directly to each other. Also, the maximum transmission unit (MTU) size must be 1500 or larger on the Stateful Failover link.

You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports. For example, if the inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then the Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. In this case, you could not use a PIX-1GE or PIX-1FE card. Nor could you use any card installed in bus 2 or sharing bus 1 with a slower card.

- Step 7** Use the **clear xlate** command after changing the **interface** command.
- Step 8** If you have not done so already, use the **ip address** command statement to assign IP addresses to each interface on the primary unit. If you make a mistake while entering an **ip address** command, reenter the command again correctly.

Use the **show ip address** command to view the addresses you specified:

```
show ip address
System IP Addresses:
  ip address outside 192.168.1.1 255.255.255.0
  ip address inside 10.1.1.1 255.255.255.0
  ip address intf2 192.168.2.1 255.255.255.0
  ip address intf3 192.168.3.1 255.255.255.0
  ip address 4th 172.16.1.1 255.255.255.0
Current IP Addresses:
  ip address outside 192.168.1.1 255.255.255.0
  ip address inside 10.1.1.1 255.255.255.0
  ip address intf2 192.168.2.1 255.255.255.0
  ip address intf3 192.168.3.1 255.255.255.0
  ip address 4th 172.16.1.1 255.255.255.0
```

The Current IP Addresses are the same as the System IP Addresses on the failover active unit. When the primary unit fails, the Current IP Addresses become those of the standby unit.

- Step 9** Use the **failover** command statement to enable failover on the primary unit.

- Step 10** Use the **show failover** command to verify that the primary unit is enabled by checking for the following statement:

This host: primary - Active

Sample output from the **show failover** command follows:

```
show failover
Failover On
Cable status: Other side powered off
Reconnect timeout 0:00:00
Poll frequency 15 seconds
  This host: primary - Active
    Active time: 225 (sec)
    Interface 4th (172.16.1.1): Normal (Waiting)
    Interface intf3 (192.168.3.1): Normal (Waiting)
    Interface intf2 (192.168.2.1): Normal (Waiting)
    Interface outside (192.168.1.1): Normal (Waiting)
    Interface inside (10.1.1.1): Normal (Waiting)
  Other host: secondary - Standby
    Active time: 0 (sec)
    Interface 4th (0.0.0.0): Unknown (Waiting)
    Interface intf3 (0.0.0.0): Unknown (Waiting)
    Interface intf2 (0.0.0.0): Unknown (Waiting)
    Interface outside (0.0.0.0): Unknown (Waiting)
    Interface inside (0.0.0.0): Unknown (Waiting)
```

The Cable Status that displays with the **show failover** command has these values:

- My side not connected—Indicates that the serial cable is not connected to the unit on which you entered the **show failover** command.
- Normal—Indicates that the active unit is working and that the standby unit is ready.
- Other side is not connected—Indicates that the serial cable is not connected to the other unit (the unit *opposite* from where you entered the **show failover** command).
- Other side powered off—Indicates that the unit not shown as active is powered off.

The failover interface flags appear to the right of each interface's IP address in the **show failover** command display. The failover flags indicate the following:

- Failed—The interface has failed.
- Link Down—The interface line protocol is down.
- Normal—The interface is working correctly.
- Shut Down—The interface has been administratively shut down (the **shutdown** option is enabled in the **interface** command statement in the configuration).
- Unknown—The IP address for the interface has not been configured and failover cannot determine the status of the interface.
- Waiting—Monitoring of the other unit's network interface has not yet started.

- Step 11** Enter a **failover ip address** command statement for each interface to specify the standby unit's interface addresses. It is *not* necessary for the two units to be configured for this command to work correctly. The IP addresses on the standby unit are different from the active unit's addresses, but should be in the same subnet for each interface. The following example sets the IP addresses for the interfaces on the standby unit.

```
failover ip address inside 10.1.1.2
failover ip address outside 192.168.1.2
failover ip address intf2 192.168.2.2
failover ip address intf3 192.168.3.2
failover ip address 4th 172.16.1.2
```

Sample output from the **show failover** command shows that the secondary unit now has IP addresses for each interface:

```
show failover
Failover On
Cable status: Other side powered off
Reconnect timeout 0:00:00
Poll frequency 15 seconds
  This host: primary - Active
    Active time: 510 (sec)
    Interface 4th (172.16.1.1): Normal (Waiting)
    Interface intf3 (192.168.3.1): Normal (Waiting)
    Interface intf2 (192.168.2.1): Normal (Waiting)
    Interface outside (192.168.1.1): Normal (Waiting)
    Interface inside (10.1.1.1): Normal (Waiting)
  Other host: secondary - Standby
    Active time: 0 (sec)
    Interface 4th (172.16.1.2): Unknown (Waiting)
    Interface intf3 (192.168.3.2): Unknown (Waiting)
    Interface intf2 (192.168.2.2): Unknown (Waiting)
    Interface outside (192.168.1.2): Unknown (Waiting)
    Interface inside (10.1.1.2): Unknown (Waiting)
```

Step 12 If you are configuring Stateful Failover, use the **failover link** command to specify the name of the dedicated interface you are using. For example, assume the “4th” interface will be used for Stateful Failover and enter the following command.

```
failover link 4th
```

Step 13 After enabling Stateful Failover, use the **show failover** command and additional information is provided as follows:

```
show failover
Failover On
Cable status: Other side powered off
Reconnect timeout 0:00:00
Poll frequency 15 seconds
  This host: primary - Active
    Active time: 510 (sec)
    Interface 4th (172.16.1.1): Normal (Waiting)
    Interface intf3 (192.168.3.1): Normal (Waiting)
    Interface intf2 (192.168.2.1): Normal (Waiting)
    Interface outside (192.168.1.1): Normal (Waiting)
    Interface inside (10.1.1.1): Normal (Waiting)
  Other host: secondary - Standby
    Active time: 0 (sec)
    Interface 4th (172.16.1.2): Unknown (Waiting)
    Interface intf3 (192.168.3.2): Unknown (Waiting)
    Interface intf2 (192.168.2.2): Unknown (Waiting)
    Interface outside (192.168.1.2): Unknown (Waiting)
    Interface inside (10.1.1.2): Unknown (Waiting)

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

```

The items in the top row of the “Stateful Failover Logical Update Statistics” section of the **show failover** command are as follows:

- Stateful Obj—PIX Firewall stateful object
- xmit—Number of transmitted packets to the other unit
- xerr—Number of errors that occurred while transmitting packets to the other unit
- rcv—Number of received packets
- rerr—Number of errors that occurred while receiving packets from the other unit

The items in the first column provide an object static count for each statistic:

- 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—CTCP connection information
- udp conn—Dynamic UDP connection information
- ARP tbl—Dynamic ARP table information
- RIF Tbl—Dynamic router table information

The items in the “Logical Update Queue Information” list the current, maximum, and total number of packets in the receive (Recv) and transmit (Xmit) queues.

- Step 14** If you want to set a time shorter than 15 seconds for the units to exchange “hello” packets to ensure each unit is available, use the **failover poll seconds** command. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds. Set to a lower value for Stateful Failover. With a faster poll time, PIX Firewall 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.
- Step 15** Power on the secondary unit. As soon as the secondary unit starts, the primary unit recognizes it and starts synchronizing the configurations. As the configurations synchronize, the messages “Sync Started” and “Sync Completed” appear.
- Step 16** After the standby unit comes up, use the **show failover** command on the primary unit to verify status:

```

show failover
Failover On
Cable status: Other side powered off
Reconnect timeout 0:00:00
Poll frequency 15 seconds
  This host: primary - Active
    Active time: 510 (sec)
    Interface 4th (172.16.1.1): Normal
    Interface intf3 (192.168.3.1): 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 intf3 (192.168.3.2): 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

```

- Step 17** Use the **write memory** to save the configuration to Flash memory and to synchronize the configuration on the standby unit with the primary unit.

Configuring LAN-Based Failover

PIX Firewall version 6.2 introduces support for LAN-based failover so a special Failover cable is no longer required to connect the primary and secondary PIX Firewalls. LAN-based failover overcomes the distance limitations imposed by the six-foot length of the Failover cable.



Note

A dedicated LAN interface and a dedicated switch (or VLAN) is required to implement LAN-based failover. You cannot use a crossover Ethernet cable to connect the two PIX Firewalls.

With LAN-based failover, failover messages may be transmitted over Ethernet connections that are relatively less secure than the dedicated Failover cable used in previous versions of the PIX Firewall. For LAN-based failover, PIX Firewall version 6.2 provides message encryption and authentication using a manual pre-shared key.

For failover, both PIX Firewall units should be the same model number, have at least as much RAM, have the same Flash memory size, and be running the same software version.

Follow these steps to configure failover:

- Step 1** Because the PIX Firewall clock is stored in the CMOS, if you have not done so already, specify the **clock set time** command on the active PIX Firewall to synchronize the time on both PIX Firewall units.
- Step 2** Attach a network cable between the primary and secondary units for each network interface to which you have configured an IP address, except for the interface to be used for LAN-based failover.
- Step 3** If the Failover cable is connected to the PIX Firewall, disconnect it.
- Step 4** *Only configure the primary unit.* Changes made to the standby unit are not copied to the primary unit and are lost during the next reboot. When you are done configuring the PIX Firewall and enter the **write memory** command to save the configuration to Flash memory, the primary unit automatically updates the secondary unit.
- Step 5** Enter configuration mode with the **configure terminal** command.

- Step 6** Ensure that you have not used the **auto** or the **1000auto** option in any **interface** command in your configuration. 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. Always specify the speed for the interface, such as **10baset** for 10 Mbps or **100basetx** for 100 Mbps. Ensure that the same speeds and duplexes are the same for any devices on the subnets including switches and routers.
- Step 7** If you are using Stateful Failover, set the Stateful Failover dedicated interface speed using the **100full** or **1000sxfull** option to the **interface** command. This is extremely important and should be performed even if you are using a crossover connector to connect the PIX Firewall units directly to each other.

**Caution**

You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports.

- Step 8** Use the **clear xlate** command after changing the **interface** command.
- Step 9** If you have not done so already, use the **ip address** command statement to assign IP addresses to each interface on the primary unit. If you make a mistake while entering an **ip address** command, reenter the command again correctly.

Use the **show ip address** command to view the addresses you specified:

```
show ip address
System IP Addresses:
  ip address outside 192.168.1.1 255.255.255.0
  ip address inside 10.1.1.1 255.255.255.0
  ip address intf2 192.168.2.1 255.255.255.0
  ip address intf3 192.168.3.1 255.255.255.0
  ip address 4th 172.16.1.1 255.255.255.0
Current IP Addresses:
  ip address outside 192.168.1.1 255.255.255.0
  ip address inside 10.1.1.1 255.255.255.0
  ip address intf2 192.168.2.1 255.255.255.0
  ip address intf3 192.168.3.1 255.255.255.0
  ip address 4th 172.16.1.1 255.255.255.0
```

The Current IP Addresses are the same as the System IP Addresses on the failover active unit. When the primary unit fails, the Current IP Addresses become those of the standby unit.

- Step 10** Use the **failover** command statement to enable failover on the primary unit.
- Step 11** Use the **show failover** command to verify that the primary unit is enabled by checking for the following statement:

```
This host: primary - Active
```

Sample output from the **show failover** command follows:

```
show failover
Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
This host: primary - Active
Active time: 225 (sec)
Interface 4th (172.16.1.1): Normal (Waiting)
Interface intf3 (192.168.3.1): Link Down
Interface intf2 (192.168.2.1): Normal (Waiting)
Interface outside (192.168.1.1): Normal (Waiting)
Interface inside (10.1.1.1): Normal (Waiting)
Other host: secondary - Standby
Active time: 0 (sec)
Interface 4th (0.0.0.0): Unknown (Waiting)
```

```
Interface intf3 (0.0.0.0): Unknown (Waiting)
Interface intf2 (0.0.0.0): Unknown (Waiting)
Interface outside (0.0.0.0): Unknown (Waiting)
Interface inside (0.0.0.0): Unknown (Waiting)
```

The Cable Status that displays with the **show failover** command has these values:

- My side not connected—Indicates that the serial cable is not connected to the unit on which you entered the **show failover** command.
- Normal—Indicates that the active unit is working and that the standby unit is ready.
- Other side is not connected—Indicates that the serial cable is not connected to the other unit (the unit *opposite* from where you entered the **show failover** command).
- Other side powered off—Indicates that the unit not shown as active is powered off.

The failover interface flags appear to the right of each interface's IP address in the **show failover** command display. The failover flags indicate the following:

- Failed—The interface has failed.
- Link Down—The interface line protocol is down.
- Normal—The interface is working correctly.
- Shut Down—The interface has been administratively shut down (the **shutdown** option is enabled in the **interface** command statement in the configuration).
- Unknown—The IP address for the interface has not been configured and failover cannot determine the status of the interface.
- Waiting—Monitoring of the other unit's network interface has not yet started.

Step 12 Enter a **failover ip address** command statement for each interface to specify the standby unit's interface addresses. It is not necessary for the two units to be configured for this command to work correctly. The IP addresses on the standby unit are different from the active unit's addresses, but should be in the same subnet for each interface. The following example sets the IP addresses for the interfaces on the standby unit.

```
failover ip address inside 10.1.1.2
failover ip address outside 192.168.1.2
failover ip address intf2 192.168.2.2
failover ip address intf3 192.168.3.2
failover ip address 4th 172.16.1.2
```

To use these commands to configure your PIX Firewall, replace **intf3** with the interface name on the primary PIX Firewall used to connect to the secondary unit. Replace the IP addresses with the values appropriate for your network.

The following sample output from the **show failover** command shows that the secondary unit now has IP addresses for each interface:

```
show failover
Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
This host: primary - Active
Active time: 510 (sec)
Interface 4th (172.16.1.1): Normal (Waiting)
Interface intf3 (192.168.3.1): Link Down
Interface intf2 (192.168.2.1): Normal (Waiting)
Interface outside (192.168.1.1): Normal (Waiting)
Interface inside (10.1.1.1): Normal (Waiting)
Other host: secondary - Standby
```

```

Active time: 0 (sec)
Interface 4th (172.16.1.2): Unknown (Waiting)
Interface intf3 (192.168.3.2): Unknown (Waiting)
Interface intf2 (192.168.2.2): Unknown (Waiting)
Interface outside (192.168.1.2): Unknown (Waiting)

```

- Step 13** Connect the LAN failover interface to the network and enter the following commands to configure LAN-based failover on the primary unit:

```

no failover
failover lan unit primary
failover lan interface intf3
failover lan key 1234567
failover lan enable
failover

```

Replace **intf3** with the interface used for the failover connection. Replace **1234567** with the key used for encrypting traffic over the failover interface.

- Step 14** If you are configuring Stateful Failover, use the **failover link** command to specify the name of the dedicated interface you are using. For example, assume the “4th” interface will be used for Stateful Failover and enter the following command.

```
failover link 4th
```

- Step 15** After enabling Stateful Failover, use the **show failover** command and additional information is provided as shown in the following example:

```

show failover
Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
  This host: primary - Active
    Active time: 510 (sec)
    Interface 4th (172.16.1.1): Normal (Waiting)
    Interface intf2 (192.168.2.1): Normal (Waiting)
    Interface outside (192.168.1.1): Normal (Waiting)
    Interface inside (10.1.1.1): Normal (Waiting)
  Other host: secondary - Standby
    Active time: 0 (sec)
    Interface 4th (172.16.1.2): Unknown (Waiting)
    Interface intf2 (192.168.2.2): Unknown (Waiting)
    Interface outside (192.168.1.2): Unknown (Waiting)
    Interface inside (10.1.1.2): Unknown (Waiting)

```

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) Unknown
```

The items in the top row of the “Stateful Failover Logical Update Statistics” section of the show failover command are as follows:

- Stateful Obj—PIX Firewall stateful object
- xmit—Number of transmitted packets to the other unit
- xerr—Number of errors that occurred while transmitting packets to the other unit
- rcv—Number of received packets
- rerr—Number of errors that occurred while receiving packets from the other unit

The items in the first column provide an object static count for each statistic:

- 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—CTCP connection information
- udp conn—Dynamic UDP connection information
- ARP tbl—Dynamic ARP table information
- RIF Tbl—Dynamic router table information

The items in the “Logical Update Queue Information” list the current, maximum, and total number of packets in the receive (Recv) and transmit (Xmit) queues.

- Step 16** Power on the secondary unit (without the LAN-based failover interface connected) and enter the following commands:

```
nameif ethernet3 intf3 security40
interface ethernet3 100full
ip address intf3 192.168.3.1 255.255.255.0
failover ip address intf3 192.168.3.2
failover lan unit secondary <--optional
failover lan interface intf3
failover lan key 1234567
failover lan enable
failover
wr mem
reload
```

These are the commands necessary to configure the secondary unit to connect to the primary unit through the interface chosen for LAN-based failover. Once this connection is made, the rest of the configuration is replicated from the primary unit over the failover connection.

To use these commands to configure your PIX Firewall, replace **intf3** with the interface name on the secondary PIX Firewall used to connect to the primary unit. Replace the IP addresses and the subnetwork mask with the values appropriate for your network. Replace **1234567** with the string that you want to use to establish security over the LAN-based failover connection.

- Step 17** After the secondary unit boots, connect the LAN-based failover interface to the network and use the **show failover** command to verify LAN-based failover status:

```
show failover
Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
```

```

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
```



Note The display in this example is only for illustration and is not complete.

- Step 18** Use the **write memory** command to save the configuration to Flash memory and to synchronize the configuration on the secondary unit with the primary unit.

Changing from Cable-Based Failover to LAN-Based Failover

- Step 1** Shut down failover by entering the following command:
- ```
no failover
```
- Step 2** On the primary unit, enter the following commands:
- ```
failover lan unit primary
failover lan interface intf3
failover lan key 12345678
failover lan enable
failover
```
- Step 3** Use the **show failover** command to verify that LAN-based failover is running on the primary unit, as shown in the following example:
- ```
show failover
Failover On
```

```

Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
This host: primary - Active
Active time: 510 (sec)
Interface 4th (172.16.1.1): Normal (Waiting)
Interface intf2 (192.168.2.1): Normal (Waiting)
Interface outside (192.168.1.1): Normal (Waiting)
Interface inside (10.1.1.1): Normal (Waiting)
Other host: secondary - Standby
Active time: 0 (sec)
Interface 4th (172.16.1.2): Unknown (Waiting)
Interface intf2 (192.168.2.2): Unknown (Waiting)
Interface outside (192.168.1.2): Unknown (Waiting)
Interface inside (10.1.1.2): Unknown (Waiting)

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) Down

```

**Step 4** On the secondary unit, enter the following commands:

```

failover lan unit secondary <--- optional
failover lan interface intf3
failover lan key 12345678
failover lan enable
failover
wr mem
reload

```

After the secondary unit finishes reloading, use the **show failover** command to verify that LAN-based failover is running correctly, as shown in the following example:

```

show failover

Failover On
Cable status: Unknown
Reconnect timeout 0:00:00
Poll frequency 15 seconds
This host: primary - Active
Active time: 510 (sec)
Interface 4th (172.16.1.1): Norml
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

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

```

- Step 5** Use the **write memory** command to save the configuration to Flash memory and to synchronize the configuration on the secondary unit with the primary unit.

## Verifying Failover Configuration

Follow these steps to verify that the configuration was successful:

- Step 1** If you have access to a syslog server, such as a UNIX system, enable logging so you can view the syslog messages as you proceed with the steps that follow. For information on syslog messages, refer to *Cisco PIX Firewall System Log Messages*, which is available online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_62/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/index.htm)

Additional information on syslog is available on the **logging** command page in the *Cisco PIX Firewall Command Reference*.

To enable logging to a server with the example address 10.1.1.5 on the inside interface, use the following commands:

```

logging host inside 10.1.1.5
logging trap debugging
logging on

```

The **logging trap debugging** command statement lets all levels of syslog messages be sent, which can produce a large number of messages on a system in production, but is very helpful for debugging. When you are done testing failover, use the **logging trap error** command to reduce the number of syslog messages to only those messages displaying an alert, critical condition, or error.

- Step 2** Test the secondary unit by powering off the primary unit.
- Step 3** Use the **show failover** command to verify that the secondary unit is now active.
- Step 4** Use FTP to send a file between hosts on different interfaces.
- Step 5** Use the **show interface** command to verify that traffic is being processed.
- Step 6** You can also use the **debug fover option** command. Choose an option from the following table.

| Option        | Description                                   |
|---------------|-----------------------------------------------|
| <b>cable</b>  | Failover cable status                         |
| <b>fail</b>   | Failover internal exception                   |
| <b>fmsg</b>   | Failover message                              |
| <b>get</b>    | IP network packet received                    |
| <b>ifc</b>    | Network interface status trace                |
| <b>open</b>   | Failover device open                          |
| <b>put</b>    | IP network packet transmitted                 |
| <b>rx</b>     | Failover cable receive                        |
| <b>rxdump</b> | Cable rcv message dump (serial console only)  |
| <b>rxip</b>   | IP network failover packet received           |
| <b>tx</b>     | Failover cable transmit                       |
| <b>txdump</b> | Cable xmit message dump (serial console only) |
| <b>txip</b>   | IP network failover packet transmit           |
| <b>verify</b> | Failover message verify                       |
| <b>switch</b> | Failover Switching status                     |

- Step 7** When ready, power on the primary unit and it will take over automatically as the active unit. The system will display the following message:

```
"Verifying LAN-Based Failover Configuration:"
```

In PIX Firewall version 6.2, the **show failover** command provides additional information about the status of LAN-based failover if it is implemented. [Example 10-1](#) shows the output from this command when LAN-based failover is enabled.

#### **Example 10-1** *show failover Command Output—LAN-Based Failover Enabled*

```
pix(config)# show failover
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
 This host: Primary - Active
 Active time: 253515 (sec)
```

```

Interface faillink (192.168.3.1): Normal
Interface outside (172.23.58.70): Normal
Interface inside (192.168.2.1): Normal
Other host: Secondary - Standby
Active time: 0 (sec)
Interface faillink (192.168.3.2): Normal
Interface outside (172.23.58.71): Normal
Interface inside (192.168.2.2): Normal

```

#### Stateful Failover Logical Update Statistics

```

Link : faillink
Stateful Obj xmit xerr rcv rerr
General 34177 0 34183 0
sys cmd 34175 0 34173 0
up time 2 0 2 0
xlate 0 0 0 0
tcp conn 0 0 8 0
udp conn 0 0 0 0
ARP tbl 0 0 0 0
RIP Tbl 0 0 0 0

```

&gt;

```

Logical Update Queue Information
 Cur Max Total
Recv Q: 0 1 34184
Xmit Q: 0 1 34179

```

&gt;

LAN-based Failover is Active

```

interface dmz (171.69.39.200) Normal, peer (171.69.39.201): Normal:

```



**Note** Some of the output has been omitted from this example.

A new command, **show failover lan** shows only the status of LAN-based failover.

The command **show failover lan detail** command provides information for debugging purposes.

[Example 10-2](#) shows the output from this command.

#### Example 10-2 show failover lan detail Command Output

```

pix(config)# show failover lan detail
Lan Failover is Active
This Pix is Primary
Command Interface is dmz
Peer Command Interface IP is 171.69.39.201
My interface status is 0x1
Peer interface status is 0x1
Peer interface downtime is 0x0
Total msg send: 103093, rcvd: 103031, dropped: 0, retrans: 13, send_err: 0
Total/Cur/Max of 51486:0:5 msgs on retransQ
msgs on retransQ if any
LAN FO cmd queue, count: 0, head: 0x0, tail: 0x0
Failover config state is 0x5c
Failover config poll cnt is 0
Failover pending tx msg cnt is 0
Failover Fmsg cnt is 0

```

PIX Firewall version 6.2 also provides four new debug options for debugging LAN-based failover:

- **lanrx**—Display debug messages on LAN-based failover receive process
- **lanretx**—Display debug messages on LAN-based failover retransmit process
- **lantx**—Display debug messages on LAN-based failover transmit process
- **lancmd** —Display debug messages on LAN-based failover main thread

## Additional Failover Information

This section includes the following topics:

- [Failover Communication](#)
- [What Causes Failover?](#)
- [Configuration Replication](#)
- [Stateful Failover](#)
- [Disabling Failover](#)
- [Failover Usage Notes](#)
- [Frequently Asked Failover Questions](#)
- [Stateful Failover Questions](#)

## Failover Communication

Both units in a failover pair communicate through either a dedicated LAN connection or a special Failover cable. The Failover cable is a modified RS-232 serial link cable that transfers data at 117,760 baud (115 K). The data provides the unit identification of primary or secondary, the power status of the other unit, and serves as a communication link for various failover communications between the two units.

The two units send special failover “hello” packets to each other over all network interfaces and the failover connection every 15 seconds. The **failover poll seconds** command lets you determine how long failover waits before sending special failover “hello” packets between the primary and secondary units over all network interfaces and the failover connection. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds. Set to a lower value for Stateful Failover. With a faster poll time, PIX Firewall 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 failover feature in PIX Firewall monitors failover communication, the power status of the other unit, and hello packets received at each interface. If two consecutive hello packets are not received within a time determined by the failover feature, failover starts testing the interfaces to determine which unit has failed, and transfers active control to the secondary unit.

You can choose the Stateful Failover option if you have interfaces with a minimum connection speed of 100 Mbps full-duplex. If you are using Stateful Failover, connection states are relayed from the primary unit to the secondary unit. Without Stateful Failover, the standby unit does not maintain the state information of each connection. This means that all active connections will be dropped when failover occurs and that client systems should reestablish connections.

You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports. For example, if the inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then the Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. In this case, you could not use a PIX-1GE or PIX-1FE card. Nor could you use any card installed in bus 2 or sharing bus 1 with a slower card.

## What Causes Failover?

If a failure is due to a condition other than a loss of power on the other unit, failover will begin a series of tests to determine which unit failed. This series of tests will begin when “hello” messages are not heard for two consecutive 15-second intervals (the interval depends on how you set the **Failover poll** command). Hello messages are sent over both network interfaces and the failover connection.

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 go to the next test.

**Note**

---

If the failover IP address has not been set, failover does not work, and the Network Activity, ARP, and Broadcast ping tests are not performed.

---

Failover uses the following tests to determine if the other unit is available:

- **Link Up/Down test**—This is a test of the NIC card itself. If an interface card is not plugged into an operational network, it is considered failed (for example, a switch failed, has a failed port, or a cable is unplugged).
- **Network Activity test**—This is a received network activity test. The unit will count 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.
- **ARP test**—The ARP test consists of 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.
- **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 no traffic is received, the testing starts over again with the ARP test.

**Note**

---

When running LAN-based failover, then loss of power on the peer unit cannot be detected by the PIX Firewall.

---

## Configuration Replication

The two PIX Firewall units should be configured exactly the same and running the same software release. Configuration replication occurs over the failover connection from the active unit to the secondary unit in three ways:

- When the standby unit completes its initial bootup, the active unit replicates its entire configuration to the standby unit.
- As commands are entered on the active unit they are sent across the failover connection to the standby unit.
- Entering the **write standby** command on the active unit forces the entire configuration in memory to be sent to the standby unit.

The configuration replication only occurs from memory to memory. After replication, use the **write memory** command to write the configuration into Flash memory. When a Failover cable is used, the replication can take a long time to complete with a large configuration. If a switchover occurs during the replication, the new active unit will have a partial configuration. The unit will reboot itself to recover the configuration from the Flash memory or re-synchronize with the other unit. 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.

## 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. 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 the global pool addresses and status, connection and translation information and status, the negotiated H.323 UDP ports, the port allocation bit map for PAT, and other details necessary to let the standby unit take over processing if the primary unit fails.

Depending on the failure, the PIX Firewall takes from 15 to 45 seconds to cause a switchover. Applications not handled by Stateful Failover will then require time to reconnect before the active unit becomes fully functional.

Stateful Failover requires an interface with a minimum connection speed of 100 Mbps full-duplex that can be used exclusively for passing state information between the two PIX Firewall units.

The Stateful Failover interface can be connected to any of the following:

- Cat 5 crossover cable directly connecting the primary unit to the secondary unit.
- 100BaseTX full duplex on a dedicated switch or dedicated VLAN of a switch.
- 1000BaseTX full duplex on a dedicated switch or dedicated VLAN of a switch.



### Caution

---

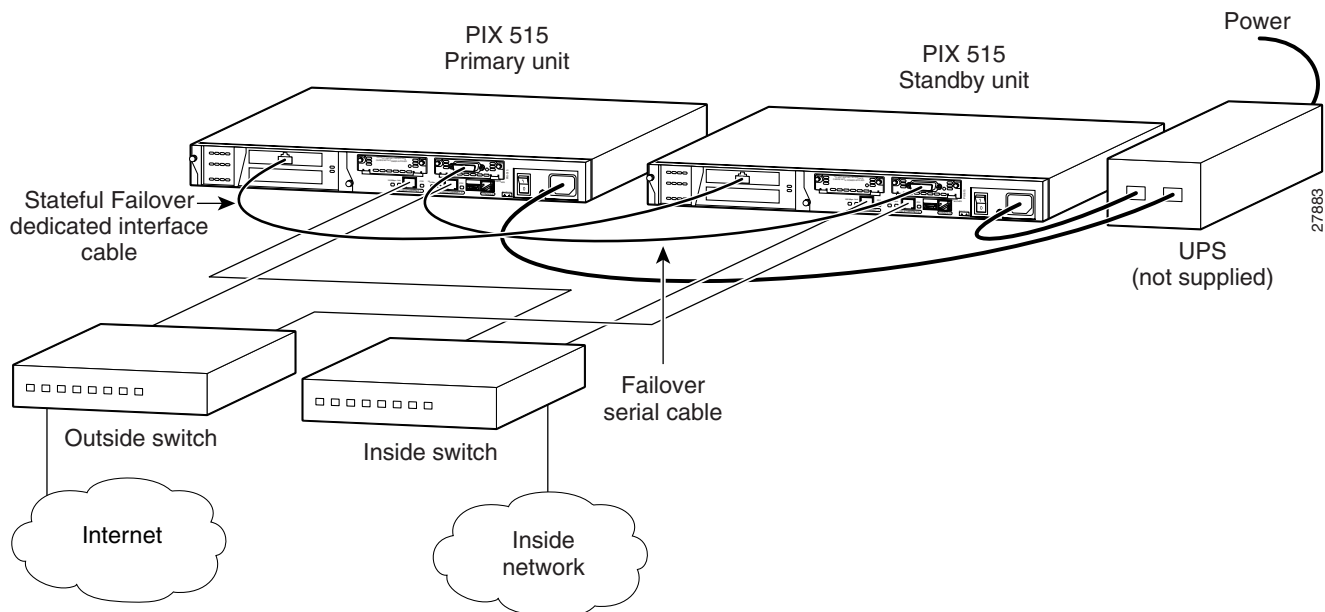
You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports.

---

Data is passed over the dedicated interface using IP protocol 105. No hosts or routers should be on this interface.

Figure 10-1 shows two PIX Firewall units connected for use with Stateful Failover.

Figure 10-1 Stateful Failover Minimum Setup



**Note**

All enabled interfaces should be connected between the active and standby units. If an interface is not in use, use the **shutdown** option to the **interface** command to disable the interface.

## Disabling Failover

You can disable failover with the **no failover** command. If failover is disabled, the following messages display when you enter the **show failover** command.

```
show failover
Failover Off
Cable Status: My side not connected
Reconnect timeout: 0:00:00
```

## Failover Usage Notes

The following notes apply to the use of failover on the PIX Firewall:

1. Perform the following on any switch that connects to the PIX Firewall:
  - a. Enable portfast on all ports on the switch that connect directly to the PIX Firewall.
  - b. Turn off trunking on all ports on the switch that connect directly to the PIX Firewall.
  - c. Turn off channeling on all ports on the switch that connect directly to the PIX Firewall.
  - d. Ensure the MSFC is not running a deferred Cisco IOS software version.



**Note** In CAT OS 5.4 a new command was added: **set port host**. This command executes the following commands: **spantree portfast enable**, **set trunk off**, and **set port channel off**. This command provides a convenient way to configure host/access ports to a mode that allows the port to forward traffic in less than one second from link up.

- The PIX Firewall failover unit 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 at the console.

```

=====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...
=====

```

- If a failover-only PIX Firewall is not attached to a failover connection or is attached to the primary end of a Failover cable, then it will hang at boot time. It should be a secondary unit.
- Changes made on the standby unit are not replicated on the active unit.

Failover messages always have a syslog priority level of 2, which indicates a critical condition. Refer to the **logging** command in the *Cisco PIX Firewall Command Reference* for more information on syslog messages. For a complete list of messages, refer to *Cisco PIX Firewall System Log Messages*. PIX Firewall documentation is available at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_62/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/index.htm)

To receive SNMP syslog traps (SNMP failover traps), 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.

## Frequently Asked Failover Questions

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

- [Cable-Based Failover](#)
- [LAN-Based Failover](#)
- [Stateful Failover Questions](#)

### Cable-Based Failover

- What happens when failover is triggered?

A switch can be initiated by either unit. When a switch takes place, each unit changes state. The newly active unit assumes the IP address and MAC address of the previously active unit and begins accepting traffic for it. The new standby unit assumes the IP address and MAC address of the unit that was previously the standby unit.

- How is startup initialization accomplished between two units?

When a unit boots up, it defaults to Failover Off and secondary, unless the failover connection is present or failover has been saved in the configuration. The configuration from the active unit is also copied to the standby unit. If the cable is not present, the unit automatically becomes the active unit. If a connection is present, the unit that has the primary end of the failover connection plugged into it becomes the primary unit by default.

- How can both units be configured the same without manually entering the configuration twice?

Commands entered on the active unit are automatically replicated on the standby unit.

- What happens if a primary unit has a power failure?

When the primary PIX Firewall unit experiences a power failure, the standby PIX Firewall comes up in active mode. If the primary unit is powered on again it will become the standby unit.

- What constitutes a failure?

Fault detection is based on the following:

- Failover hello packets are received on each interface. If hello packets are not heard for two consecutive 15-second intervals, the interface will be tested to determine which unit is at fault. (You can change this duration with the **failover poll** command.)
- Cable errors. The cable is wired so that each unit can distinguish between a power failure in the other unit, and an unplugged cable. If the standby unit detects that the active unit is turned off (or resets), it will take active control.

If the cable is unplugged, a syslog is generated but no switching occurs. An exception to this is at bootup, at which point an unplugged cable will force the unit active. If both units are powered on without the failover connection installed they will both become active creating a duplicate IP address conflict on your network. The failover connection has to be installed for failover to work correctly.

- Failover communication. The two units share information every 15 seconds, but you can change this duration with the **failover poll** command. If the standby unit does not hear from the active unit in two communication attempts (and the cable status is OK) the standby unit will take over as active.
- How long does it take to detect a failure?
  - Network errors are detected within 30 seconds (two consecutive 15-second intervals).
  - Power failure (and cable failure) is detected within 15 seconds.
  - Failover communications errors are detected within 30 seconds (two consecutive 15-second intervals).

- What maintenance is required?

Syslog messages will be generated when any errors or switches occur. Evaluate the failed unit and fix or replace it.

## LAN-Based Failover

- What is the advantage of using LAN-based failover?
  - Using LAN-based failover, the distance between PIX Firewall units can be longer than 6 feet (the maximum Failover Cable length).
- What is the disadvantage of using LAN-based failover?
  - PIX Firewall cannot detect peer failure due to loss of power or reload, so it will take longer for a PIX Firewall unit to fail over if that happens.
  - User need to configure the secondary PIX Firewall unit before it can communicate with the primary unit.
- Can users put a router between the PIX Firewall units when running LAN-based failover?
  - No, only a switch or VLAN is allowed. All interfaces of the two units still need to be on the same subnet.
- What happen if the interface for LAN-based failover is down?
  - If the LAN-based failover command interface link goes down, then the PIX Firewall notifies the peer through “other” interfaces, and if the active PIX Firewall’s interface goes down, then the standby unit will take over.




---

**Note** When the command interface goes down and the PIX Firewall becomes a standby unit, the PIX Firewall cannot become active until the interface comes back up again.

---

- What happens if the connectivity of LAN-based failover command interface is down due to reasons other than the link down (for example, each PIX is connected to a separate switch and two switches are connected using ISL).
  - The PIX Firewall will try to use “other” interfaces to poll the peer status, and then failover if necessary.
- Is it possible to have both PIX Firewall unites become active at the same time?
  - If all connectivity between the two PIX Firewall units is lost, then this can happen. Therefore, it is best to use a separate switch for the LAN-based failover command interface, so a failed switch will not cause all connectivity to be lost between the two PIX Firewall units.

## Stateful Failover Questions

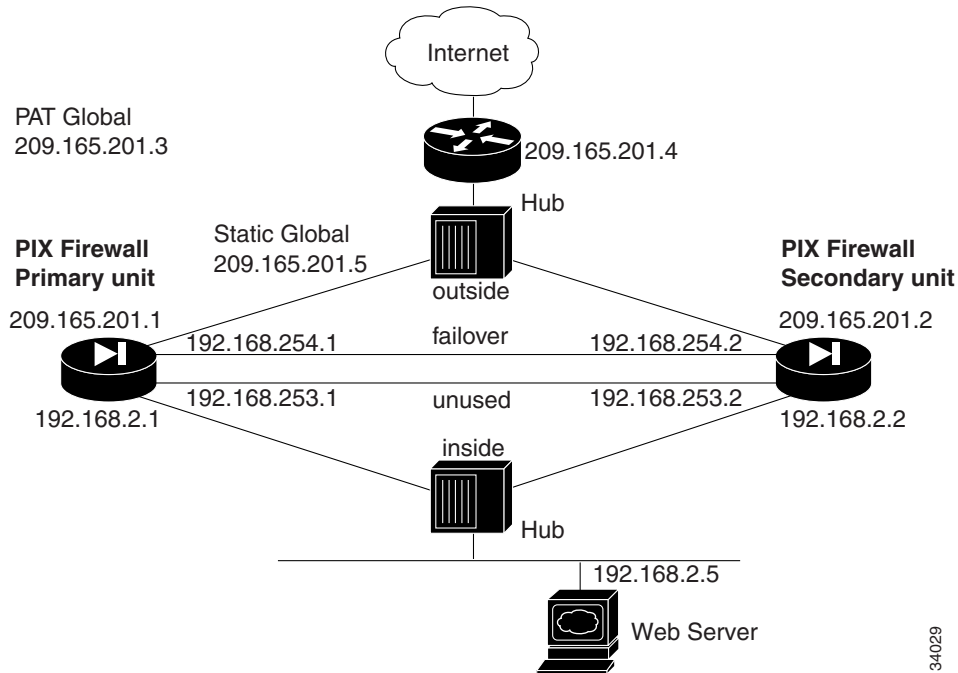
- What causes Stateful Failover to occur?
  - A power off or a power down condition on the active PIX Firewall.
  - Reboot of the active PIX Firewall.
  - A link goes down on the active PIX Firewall for more than twice the configured poll time or a maximum of 30 seconds.
  - “Failover active” on the standby PIX Firewall.
  - Block memory exhaustion for 15 consecutive seconds or more on the active unit.
- What information is replicated to the standby PIX Firewall on Stateful Failover?
  - The configuration.
  - TCP connection table including timeout information of each connection.

- Translation (xlate) table.
  - System up time; that is, the system clock is synchronized on both PIX Firewall units.
- 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.
- What are Stateful Failover hardware requirements?
  - Two identical PIX Firewall units, with a minimum connection speed of 100 Mbps full-duplex, are required. Connect the LAN ports for Stateful Failover on both PIX Firewall units with a crossover cable or through a switch.
  - For better performance, a PIX 520 or later model of PIX Firewall is recommended.
  - You need a dedicated LAN connection or a Failover cable to connect the two failover ports on both PIX Firewall units.
- What are Stateful Failover hardware restrictions?
  - The dedicated LAN connection or Failover cable should be installed and be working correctly.
  - The dedicated failover ports on both PIX Firewall units that use Tera Term Pro with SSH must be connected and fully functional.
  - You must use an interface card and bus for a Stateful Failover LAN port that is at least as fast as the fastest card used for the network interface ports.
- What are Stateful Failover software requirements?
  - PIX Firewall version 5.1 or later is required for Stateful Failover.
  - Both PIX Firewall units should run the same version of PIX Firewall software.
- What are Stateful Failover license requirements?
  - Stateful Failover requires a feature-based license key with failover feature support or connection-based license key.

# Failover Configuration Examples

Figure 10-2 lists the network diagram for a failover configuration using a Failover cable.

Figure 10-2 Failover Configuration



Follow these steps to configure the PIX Firewall units for use with failover:

- 
- Step 1** Set up the PIX Firewall without failover information.
  - Step 2** Add the **failover ip address** command for all interfaces including the one for the dedicated failover interface but not for unused interfaces.  
If there are any interfaces that have not been configured in the non-failover setup, configure them at this time with an IP address and a failover IP address. Also leave the unused interfaces unconnected.
  - Step 3** If you want to configure Stateful Failover, add the **failover link** command and specify the interface the Stateful Failover will be using. For Stateful Failover, you should have a dedicated 100BaseTX Stateful Failover interface in addition to all other interfaces.
  - Step 4** Use the **write memory** command on the primary unit to save the new configuration.
  - Step 5** Plug the Failover cable into the primary unit and then power on the secondary unit.



**Note** If the secondary unit has been previously configured, before you connect it to the Failover cable to the primary unit, boot it up, and enter the **write erase** command to remove any configuration. This will ensure a smooth synchronization.

---

- Step 6** Enter the **write standby** command from the active unit to synchronize the current configuration to the Flash memory on the standby unit.

---

In the example configuration illustrated in [Figure 10-2](#), the Ethernet2 interface (labeled “failover”) is used as the dedicated interface for Stateful Failover. The Ethernet3 interface is a previously unconfigured interface and is currently not connected to any active network. There is a cross-over Ethernet cable connecting the unused interface so that the failover check up messages can be sent and received.

**Note**

PIX Firewall requires that unused interfaces be connected to the standby unit and that each unused interface be assigned an IP address. Even if an interface is administratively shut down, the PIX Firewall will try to send the failover check up messages to *all* internal interfaces.

---

[Example 10-3](#) lists the failover configuration.

**Example 10-3 Failover Configuration**

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 failover security10
nameif ethernet3 unused security20
enable password xxx encrypted
passwd xxx encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 20
no logging timestamp
no logging standby
logging console errors
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 10baset
interface ethernet2 100full
interface ethernet3 10baset
mtu outside 1500
mtu inside 1500
mtu failover 1500
mtu unused 1500
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 unused 192.168.253.1
 255.255.255.252
failover
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 unused 192.168.253.2
failover link failover
arp timeout 14400
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-list acl_out permit icmp any any
access-group acl_out in interface outside
access-list acl_ping permit icmp any any
access-group acl_ping in interface inside
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip failover passive
no rip failover default
route outside 0 0 209.165.201.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80

```

**Example 10-4** shows the configuration listing for the primary unit when implementing LAN-based failover.

#### **Example 10-4 LAN-Based Failover Primary Unit Configuration**

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 stateful security10
nameif ethernet3 lanfover security20
enable password xxx encrypted
passwd xxx encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 20
no logging timestamp
no logging standby
logging console errors
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 100full
interface ethernet1 100full

```

```
interface ethernet2 100full
interface ethernet3 100full
mtu outside 1500
mtu inside 1500
mtu failover 1500
mtu unused 1500
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 unused 192.168.253.1 255.255.255.252
failover
failover ip address outside 209.165.201.2
failover ip address inside 192.168.2.2
failover ip address stateful 192.168.254.2
failover ip address lanfover 192.168.253.2
failover link stateful
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
arp timeout 14400
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-list acl_out permit icmp any any
access-group acl_out in interface outside
access-list acl_ping permit icmp any any
access-group acl_ping in interface inside
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip failover passive
no rip failover default
route outside 0 0 209.165.201.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80
```

[Example 10-5](#) shows the configuration listing for the secondary unit with LAN-based Failover.

**Example 10-5 LAN-Based Failover Secondary Unit Configuration**

```
nameif ethernet3 stateful security20
interface ethernet3 100full
ip address lanfover 192.168.253.1 255.255.255.252
failover ip address lanfover 192.168.254.2
failover lan unit primary
failover lan interface lanfover
failover lan key 12345678
failover lan enable
failover
```