



### Lab 8.2.4 Configure LAN-Based Failover Between Two PIX Security Appliances (OPTIONAL)

#### Objectives:

This is a two part lab. In the first part, students will configure and test active/standby failover. In the second part of this lab, students will configure and test active/active failover.

In this lab exercise, the students will complete the following tasks:

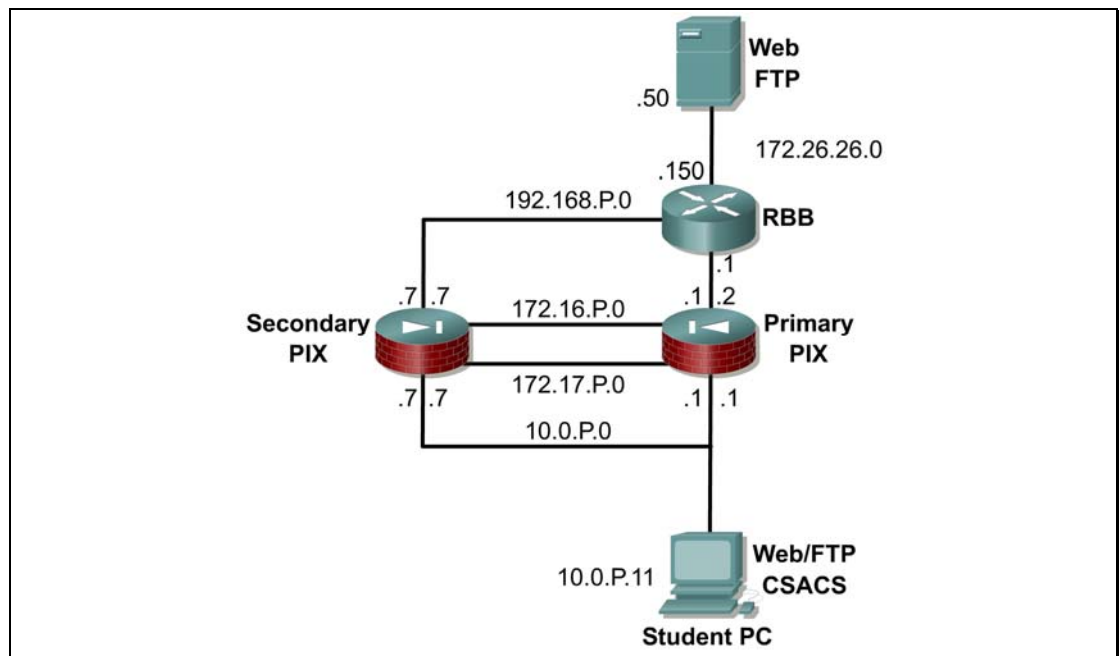
- Configure the primary PIX Security Appliance for LAN-based active/standby failover.
- Configure the secondary PIX Security Appliance for LAN-based active/standby failover.
- Test LAN-based active/standby failover.
- Configure the primary PIX Security Appliance for LAN-based active/active failover.
- Configure the secondary PIX Security Appliance for LAN-based active/active failover.
- Test LAN-based active/active failover.

#### Scenario

In an enterprise network, network outages are not an option. Many businesses and service providers must maintain continuous service, otherwise the monetary loss can be high. In addition to redundant routers, the PIX supports failover capabilities.

#### Topology

This figure illustrates the lab network environment used for the active/standby failover portion of this lab exercise:



## Preparation

Begin with the failover lab topology and verify the starting configuration on pod PIX Security Appliances. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

## Tools and Resources

In order to complete the lab, the following is required:

- One primary unrestricted(UR) PIX Security Appliance
- One secondary PIX Security Appliance (with a Failover Only (FO), Failover Only Active-Active (FO\_AA), or Unrestricted (UR) license.)
- Console cable
- HyperTerminal
- One student PC
- One Backbone Server

---

**Note** A least one of the PIX Security Appliance units must have an unrestricted (UR) license. The other unit can have a Failover Only (FO) license, a Failover Only Active-Active (FO\_AA) license, or another UR license. Units with a Restricted license cannot be used for failover, and two units with FO or FO\_AA licenses cannot be used together as a failover pair.

---

## Additional Materials

Student can use the following link for more information on the objectives covered in this lab:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/products\\_configuration\\_guide\\_chapter09186a008045247e.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008045247e.html)

## Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
<b>changeto</b> { <b>system</b>   <b>context</b> <i>name</i> }	To change between security contexts and the system, use the <b>changeto</b> command in privileged EXEC mode.
<b>clear configure failover</b>	To remove <b>failover</b> commands from the configuration and restore the defaults, use the <b>clear configure failover</b> command in global configuration mode.
<b>clear configure interface</b> [ <i>physical_interface</i> [. <i>subinterface</i> ]   <i>mapped_name</i>   <i>interface_name</i> ]	To clear the interface configuration, use the <b>clear configure interface</b> command in global configuration mode.
<b>failover</b>	To enable failover, use the <b>failover</b> command in global configuration mode.
<b>failover active</b>	To switch a standby security appliance or failover group to the active state, use the <b>failover active</b> command in privileged EXEC mode.
<b>failover group</b> [ <b>group</b> <i>group_id</i> ]	To configure an Active/Active failover group, use the <b>failover group</b> command in global configuration mode.
<b>failover interface ip</b> <i>if_name</i> <i>ip_address</i> <i>mask</i> <b>standby</b> <i>ip_address</i>	To specify the IP address and mask for the failover interface and the Stateful Failover interface, use the <b>failover interface ip</b> command in global configuration mode.
<b>failover lan enable</b>	To enable lan-based failover, use the <b>failover lan enable</b> command in global configuration mode.
<b>failover lan interface</b> <i>if_name</i> <i>phy_if</i>	To specify the interface used for failover communication, use the <b>failover lan interface</b> command in global configuration mode.
<b>failover key</b> <i>secret</i>	To specify the failover shared secret for encrypted and authenticated communication between failover pairs, use the <b>failover key</b> command in global configuration mode.
<b>failover lan unit</b> { <b>primary</b>   <b>secondary</b> }	To configure the PIX Security Appliance as either the primary or secondary unit in a LAN failover configuration, use the <b>failover lan unit</b> command in global configuration mode.
<b>failover link</b> <i>if_name</i> [ <i>phy_if</i> ]	To specify the Stateful Failover interface, use the <b>failover link</b> command in global configuration mode.

<b>mode</b> { <b>single</b>   <b>multiple</b> } <b>[noconfirm]</b>	To set the security context mode to single or multiple, use the <b>mode</b> command in global configuration mode.
<b>show context</b> [ <b>name</b>   <b>detail</b>   <b>count</b> ]	To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the <b>show context</b> command in privileged EXEC mode.
<b>show failover</b>	To display information about the failover status of the unit, use the <b>show failover</b> command in privileged EXEC mode.
<b>show mode</b>	To show the security context mode for the running software image and for any image in Flash memory, use the <b>show mode</b> command in privileged EXEC mode.

## Part I: Configure Active/Standby Failover

### Step 1 Configure the Primary PIX Security Appliance for LAN-Based Stateful Failover to the Secondary PIX Security Appliance

Complete the following steps to configure the primary PIX Security Appliance for failover to the secondary PIX Security Appliance:

- a. Save the current configuration

```
PixP(config)# write memory
```

- b. Step 2 IMPORTANT: Copy the current configuration to Flash: The same configuration will be reloaded at the end of this lab.

```
PixP(config)# copy running-config flash:/pre_fo_lab.cfg
```

- c. Step 3 Clear the existing configuration for the DMZ interface, interface ethernet2. In this lab, interface e2 will be used for the failover link.

```
PixP(config)# clear configure interface ethernet2
```

- d. Step 4 Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
```

```
PixP(config-if)# no shutdown
```

```
PixP(config-if)# exit
```

- e. Step 5 Assign a standby IP address for each interface:

```
PixP(config)# interface ethernet0
```

```
PixP(config-if)# ip address 192.168.P.2 255.255.255.0 standby  
192.168.P.7
```

```
PixP(config-if)# exit
```

```
PixP(config)# interface ethernet1
```

```
PixP(config-if)# ip address 10.0.P.1 255.255.255.0 standby 10.0.P.7
```

```
PixP(config-if)# exit
```

(where P = pod number)

- f. Step 6 Use the **failover lan interface** command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
```

INFO: Non-failover interface config is cleared on Ethernet2 and is sub-interfaces

(where P = pod number)

- g. Step 7 Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1  
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

- h. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

- i. Specify the primary PIX security Appliance to use for LAN-based failover:

```
PixP(config)# failover lan unit primary
```

(where P = pod number)

- j. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

- k. Enable failover:

```
PixP(config)# failover
```

- l. Save all changes to Flash memory:

```
PixP(config)# write memory
```

- m. Wait for the failover initialization process to complete. The following message will be displayed on the PIX Security Appliance console:

No Response from Mate

- n. Make sure that the primary PIX Security Appliance is enabled for failover by using the **show failover** command:

```
PixP(config)# show failover
```

Failover On

Cable status: N/A - LAN-based failover enabled

Failover unit Primary

Failover LAN Interface: myfailover Ethernet2 (up)

Unit Poll frequency 15 seconds, holdtime 45 seconds

Interface Poll frequency 15 seconds

Interface Policy 1

Monitored Interfaces 0 of 250 maximum

Last Failover at: 18:03:38 UTC Nov 12 2004

This host: Primary - Active

Active time: 30 (sec)

```

Interface outside (192.168.1.2): Normal (Waiting)
Interface inside (10.0.1.1): Normal (Waiting)
Other host: Primary - Failed
Active time: 0 (sec)
Interface outside (192.168.1.7): Unknown (Waiting)
Interface inside (10.0.1.7): Unknown (Waiting)
Stateful Failover Logical Update Statistics
Link : Unconfigured.

```

- o. Verify that the SuperServer can be pinged:

```
C:\> ping 172.26.26.50
```

- p. Verify that the backbone router is available by Telnet:

```
C:\> telnet 192.168.P.1
```

(where P = pod number)

## Step 2 Configure the Secondary PIX Security Appliance for LAN-Based Failover

Complete the following steps to prepare the secondary PIX Security Appliance for failover. The instructor will provide the instructions for accessing the secondary PIX.

- a. Ask the instructor to power up the secondary PIX Security Appliance.
- b. Complete the following substeps on the secondary PIX Security Appliance:
  - i. When prompted to configure the secondary PIX Security Appliance through interactive prompts, press **<Control Z>** to escape.
  - ii. Enter configuration mode.
- c. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
```

```
PixP(config-if)# no shutdown
```

```
PixP(config-if)# exit
```

- d. Use the failover lan interface command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
```

**Note:** Non-failover interface config is cleared on Ethernet2 and its sub-interfaces

(where P = pod number)

- e. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

- f. Enable encryption and authentication of LAN-based failover messages between PIX security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

- g. Specify the secondary PIX security Appliance to use for LAN-based failover:

```
PixP(config)# failover lan unit secondary
```

(where P = pod number)

- h. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

- i. Enable failover:

```
PixP(config)# failover
```

- j. Wait for the failover initialization process to complete. The following messages will be displayed on the secondary PIX Security Appliance console:

```
Detected an Active mate
```

```
Beginning configuration replication from mate.
```

```
End configuration replication from mate.
```

### Step 3 Test LAN-Based Stateful Failover

Complete the following steps to test LAN-based stateful failover:

- a. Switch to the primary PIX console. After the message “End Configuration Replication to mate” is displayed on the primary PIX Security Appliance console, verify that failover is running and the secondary failover device is recognized:

```
PixP(config)# show failover
```

```
Failover On
```

```
Cable status: N/A - LAN-based failover enabled
```

```
Failover unit Primary
```

```
Failover LAN Interface: myfailover Ethernet2 (up)
```

```
Unit Poll frequency 15 seconds, holdtime 45 seconds
```

```
Interface Poll frequency 15 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 0 of 250 maximum
```

```
Last Failover at: 18:03:38 UTC Nov 12 2004
```

```
This host: Primary - Active
```

```
Active time: 645 (sec)
```

```
Interface outside (192.168.1.2): Normal
```

```
Interface inside (10.0.1.1): Normal
```

```
Other host: Secondary - Standby Ready
```

```
Active time: 0 (sec)
```

```
Interface outside (192.168.1.7): Normal
```

```
Interface inside (10.0.1.7): Normal
```

```
Stateful Failover Logical Update Statistics
```

```
Link : Unconfigured.
```

- b. Start a continuous ping to 172.26.26.50:

```
C:\ ping 172.26.26.50 -t
```

- c. From the student PC open a telnet session to the backbone router

```
C:\>telnet 192.168.P.1
```

```
User Access Verification
```

```
Password: cisco
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
% Bad passwords
RBB>
```

- d. Reload the primary PIX security Appliance:

```
PixP(config)# reload
(where P = pod number)
```

- e. When asked to confirm the reload, press **Enter**.
- f. Notice the ping request times out and eventually resume after a configurable delay. After the successful pings return, try to access `rbb>enable`. The connection to `rbb>` should be lost. Stateful Failover is not enabled. Stop the pings `cntrl-C`
- g. After the primary PIX has completely rebooted, enter the `show failover` command on the primary Security Appliance and observe the new role and the new addresses displayed on the primary PIX:

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary - Standby Ready
Active time: 645 (sec)
Interface outside (192.168.P.7): Normal (waiting)
Interface inside (10.0.P.7): Normal (waiting)
Other host: Secondary - Active
Active time: 0 (sec)
Interface outside (192.168.P.2): Normal
Interface inside (10.0.P.1): Normal
Stateful Failover Logical Update Statistics
Link : Unconfigured.
```

- h. Make the primary PIX Security Appliance the active PIX Security Appliance by using the **failover active** command. Make sure to connect to the console port of the primary PIX Security Appliance.

```
PixP(config)# failover active
```



Switching to Active.

(where P = pod number)

- i. Step 9 Enable Stateful failover on the primary PIX.

```
PixP(config)# failover link myfailover
```

(where P = pod number)

- i. Save the configuration on the primary.
- ii. Verify that the stateful failover is enabled by using the **show failover** command. The stateful failover statistics should be present.

```
PixP(config)# show failover
```

Failover On

Cable status: N/A - LAN-based failover enabled

Failover unit Primary

Failover LAN Interface: myfailover Ethernet3 (up)

Unit Poll frequency 15 seconds, holdtime 45 seconds

Interface Poll frequency 15 seconds

Interface Policy 1

Monitored Interfaces 0 of 250 maximum

Last Failover at: 18:03:38 UTC Nov 12 2004

This host: Primary - Active

Active time: 140 (sec)

Interface outside (192.168.P.2): Normal

Interface inside (10.0.P.1): Normal

Other host: Secondary - Standby Ready

Active time: 3105 (sec)

Interface outside (192.168.P.7): Normal

Interface inside (10.0.P.7): Normal

Stateful Failover Logical Update Statistics

Link : myfailover Ethernet3 (up)

Stateful Obj xmit xerr rcv rerr

General 0 0 0 0

sys cmd 4 0 4 0

up time 0 0 0 0

RPC services 0 0 0 0

TCP conn 0 0 0 0

UDP conn 0 0 0 0

ARP tbl 0 0 8 0

Xlate\_Timeout 0 0 0 0

Logical Update Queue Information

Cur Max Total

```
Recv Q: 0 1 4
```

```
Xmit Q: 0 2 38
```

(where P = pod number)

- j. Start a continuous ping to 172.26.26.50:

```
C:\ ping 172.26.26.50 -t
```

- k. From the student PC, open a telnet session to the backbone router

```
C:\>telnet 192.168.P.1
```

```
User Access Verification
```

```
Password: cisco
```

```
RBB> enable
```

```
Password: <cr>
```

```
Password: <cr>
```

```
Password: <cr>
```

```
% Bad passwords
```

```
RBB>
```

- l. Reload the primary PIX Security Appliance:

```
PixP(config)# reload
```

(where P = pod number)

- m. When asked to confirm the reload, press **Enter**.

- n. Notice that the ping request times out and eventually resume after a delay.

- o. After the pings resume, try to access `rbb>enable` through the telnet session. The connection to `rbb>` should still be present. Stateful Failover is enabled.

```
RBB> enable
```

```
Password: <cr>
```

```
Password: <cr>
```

```
Password: <cr>
```

```
% Bad passwords
```

```
RBB>
```

- p. Stop the pings with **Ctrl-C**. Close the telnet session.

#### Step 4 Make the Primary PIX Security Appliance Active

Complete the following steps to make the primary PIX Security Appliance the active PIX Security Appliance:

- a. Make the primary PIX Security Appliance the active PIX Security Appliance by using the failover active command. Make sure to connect to the console port of the primary PIX Security Appliance.

```
PixP(config)# failover active
```

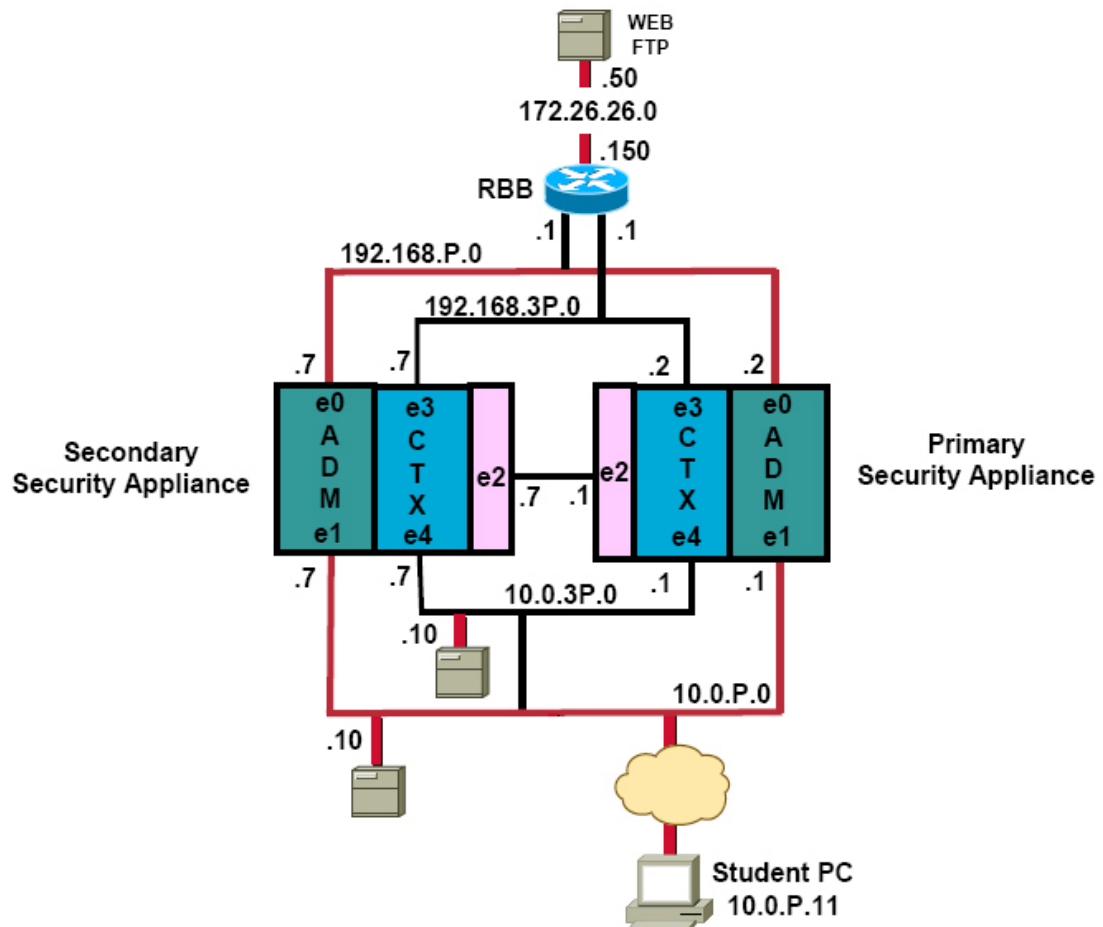
(where P = pod number)

- b. Verify that the failover active command worked by using the `show failover` command. The primary PIX Security Appliance should show that it is in active mode and the secondary PIX Security Appliance should show that it is in the standby mode.

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary - Active
Active time: 140 (sec)
Interface outside (192.168.P.2): Normal
Interface inside (10.0.P.1): Normal
Other host: Secondary - Standby Ready
Active time: 3105 (sec)
Interface outside (192.168.P.7): Normal
Interface inside (10.0.P.7): Normal
stateful Failover Logical Update Statistics
Link : myfailover Ethernet3 (up)
Stateful Obj xmit xerr rcv rerr
General 0 0 0 0
sys cmd 224 0 224 0
up time 0 0 0 0
RPC services 0 0 0 0
```

## Part II: Configure Active/Active Failover

The following figure displays the configuration that will be completed in the active/active failover portion of this lab exercise. There is a primary and secondary Security Appliance. Each Security Appliance is composed of two contexts, **admin** and **ctx1** contexts. In active/active failover, only one of the **admin** and one of the **ctx1** contexts will be active at any one time.



### Step 1 Enable Multiple Context Mode

By default, a PIX Security Appliance operates in single mode. Active/active failover requires the PIX Security Appliance to operate with multiple mode with virtual security contexts. Complete the following steps to enable multiple context mode.

- On the primary PIX Security Appliance, verify security context is a licensed feature of this PIX Security Appliance.

```
PixP(config)# show version
.....
License Feature of this Platform:
.....
Security Contexts :5
```

- Check the current mode of the PIX Security Appliance:

```
PixP(config)# show mode
```

```
Security appliance mode: single
```

c. Enable Multiple Context mode:

```
PixP(config)# mode multiple  
WARNING: This command will change the behavior of the device  
WARNING: This command will initiate a Reboot  
Proceed with change mode? [confirm] <Enter>  
Convert the system configuration? [confirm] <Enter>  
The old running configuration file will be written to flash  
The admin context configuration will be written to flash  
The new running configuration file was written to flash
```

## Step 2 Confirm Multiple Context Mode

When a PIX Security Appliance changes to a multiple mode configuration, the default multiple mode configuration is two security contexts, system and admin contexts. The PIX Security Appliance boots into the system context. In the system context, the administrator can view and create contexts. They can also allocate system resources and configure failover links. Complete the following steps to examine the default multiple mode environment:

a. After the primary PIX Security Appliance re-boots, confirm the PIX Security Appliance is in multiple context mode:

```
PixP# show mode  
  
Security context mode: multiple
```

b. Confirm the PIX Security Appliance saved the original configuration as `old_running.cfg`:

```
PixP# show flash  
  
Directory of flash:/  
  
 3 -rw- 5031936 08:30:41 Aug 12 2004 pix_7_82.bin  
 8 -rw- 2028 08:30:41 Aug 12 2004 old_running.cfg  
 9 -rw- 1682 08:30:41 Aug 12 2004 admin.cfg
```

c. Examine the current security contexts.

```
PixP# show context  
  
Context Name Interfaces URL  
*admin Ethernet0, Ethernet1 flash:/admin.cfg  
Total active Security Contexts: 1  
  
PixP# show context detail  
  
Context "system", is a system resource  
Config URL: startup-config  
Real Interfaces:  
Mapped Interfaces: Ethernet0, Ethernet1, Ethernet2, Ethernet3,  
Ethernet4, Ethernet5  
Flags: 0x00000019, ID: 0  
  
Context "admin", has been created, but initial ACL rules not  
complete  
Config URL: flash:/admin.cfg
```

```
Real Interfaces: Ethernet0, Ethernet1
Mapped Interfaces: Ethernet0, Ethernet1
Flags: 0x00000013, ID: 1
Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 257
```

### Step 3 Configure the Failover Link

A failover link can only be configured in system context. In this task, remove the previous active/standby failover configuration on interface Ethernet 2. Re-configure it as an active/active failover link. Complete the following steps to configure the failover link in the system context:

- a. Clear the existing failover configuration

```
PixP(config)# clear configure failover
```

- b. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
PixP(config-if)# no shutdown
PixP(config-if)# exit
```

- c. Use the failover lan interface command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
INFO: Non-failover interface config is cleared on Ethernet3 and its
sub-interfaces
(where P = pod number)
```

- d. Enable LAN-based failover:

```
PixP(config)# failover lan enable
(where P = pod number)
```

- e. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
(where P = pod number)
```

- f. Enable stateful failover:

```
PixP(config)# failover link MYFAILOVER ethernet2
(where P = pod number)
```

- g. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
(where P = pod number)
```

- h. Configure this device as the primary failover unit:

```
PixP(config)# failover lan unit primary
(where P = pod number)
```

- i. Configure failover group 1 to be active on the primary:  

```
PixP(config)# failover group 1
```

```
PixP(config-fover-group)# exit
```

(where P = pod number)
- j. Configure failover group 2 to be active on the secondary:  

```
PixP(config)# failover group 2
```

```
PixP(config-fover-group)# exit
```
- k. Save all changes to Flash memory:
- l. Show the failover status  

```
PixP# show failover
```

Failover Off

Cable status: N/A - LAN-based failover enabled

Failover unit Primary

Failover LAN Interface: myfailover Ethernet2 (up)

Unit Poll frequency 15 seconds, holdtime 45 seconds

Interface Poll frequency 15 seconds

Interface Policy 1

Monitored Interfaces 2 of 250 maximum

#### Step 4 Allocate Interfaces and Failover Groups by Context

The system context has no physical connections of its own other than the failover link. The system context is used to create other contexts and allocate resources to each context. In this task, create a ctx1 context and allocate resources to both the admin and ctx1 contexts. Complete the following steps to allocate interfaces and a failover group to each context:

- a. Access the admin context configuration commands:  

```
PixP(config)# context admin
```
- b. Allocate interfaces to the admin context:  

```
PixP(config-ctx)# allocate-interface ethernet0
```

```
PixP(config-ctx)# allocate-interface ethernet1
```
- c. Configure a URL for admin context configuration:  

```
PixP(config-ctx)# config-url flash:/admin.cfg
```
- d. Allocate a failover group to the admin context:  

```
PixP(config-ctx)# failover group 1
```

```
PixP(config-if)# exit
```
- e. Create the 'ctx1' context:  

```
PixP(config)# context ctx1
```

Creating context 'ctx1' . . Done.
- f. Allocate interfaces to the ctx1 context:  

```
PixP(config-ctx)# allocate-interface ethernet3
```

```
PixP(config-ctx)# allocate-interface ethernet4
```

- g. Configure a new URL for ctx1 context configuration:

```
PixP(config-ctx)# config-url flash:/ctx1.cfg  
WARNING: Could not fetch the URL flash:/ctx1.cfg  
INFO: Creating context with default config
```

- h. Allocate a failover group to the ctx1 context:

```
PixP(config-ctx)# failover group 2  
PixP(config-fover-group)# exit
```

- i. Enable interfaces Ethernet3 and Ethernet4

```
PixP(config)# interface ethernet3  
PixP(config-if)# no shutdown  
PixP(config-if)# exit  
PixP(config)# interface ethenet4  
PixP(config-if)# no shut  
PixP(config-if)# exit
```

- j. Verify the context allocation configuration:

```
PixP# show context  
  
Context Name Interfaces URL  
*admin Ethernet0, Ethernet1 flash:/admin.cfg  
ctx1 Ethernet3, Ethernet4 flash:/ctx1.cfg  
Total active Security Contexts: 2
```

## Step 5 Configure the admin and ctx1 Context

In this task, configure a virtual security context. Use the “changeto” command to navigate between each context. Complete the following steps to configure the ctx1 context:

- a. From the primary PIX Security Appliance console, access the admin context configuration commands:

```
PixP(config)# changeto context admin  
PixP/admin(config)#
```

Notice the prompt has changed. Admin was added to the hostname. You are now administratively located in the admin context.

- b. Notice the configuration from the interfaces still exists.

```
PixP/admin(config)# show running-config interface
```

- c. Notice that if the commands **show running-config failover** or **configure failover** parameters are used while in the admin context, an error message is displayed.

```
PixP/admin(config)# show running-config failover  
ERROR: % Invalid input detected at marker  
Failover is configured in the system context only.
```

- d. Access the ctx1 context configuration commands:

```
PixP(config)# changeto context ctx1  
PixP/ctx1(config)#
```



Notice the prompt has changed. Ctx1 was added to the hostname. You are now administratively located in the ctx1 context.

- e. View the interface configuration. The context ctx1 interfaces are available but not configured.

```
PixP/ctx1(config)# show interface  
Interface Ethernet2 " " is up, line protocol is up  
Available but not configured via nameif  
Interface Ethernet3 " " is up, line protocol is up  
Available but not configured via nameif
```

- f. Step 6 Configure context ctx1 interfaces:

```
PixP/ctx1(config)# interface ethernet3  
PixP/ctx1(config-if)# nameif ctxout  
Info: Security level for "ctxout" set to 0 by default.  
PixP/ctx1(config-if)# ip address 192.168.30+P.2 255.255.255.0  
standby 192.168.30+P.7  
PixP/ctx1(config-if)# no shutdown  
PixP/ctx1(config-if)# exit  
PixP/ctx1 config)# interface e4  
PixP/ctx1(config-if)# nameif ctxin  
Info: Security level for "ctxin" set to 0 by default.  
PixP/ctx1(config-if)# ip address 10.0.30+P.1 255.255.255.0 standby  
10.0.30+P.7  
PixP/ctx1(config-if)# security-level 100  
PixP/ctx1(config-if)# no shutdown  
PixP/ctx1(config-if)# exit
```

- g. Add a default route.

```
PixP/ctx1(config)# route ctxout 0 0 192.168.31.1
```

- h. Add a static route from super server to outside network

```
PixP/ctx1(config)# static (ctxin,ctxout) 192.168.31.10 10.0.31.10
```

- i. Add an access-list for allow outside access to super server.

```
PixP/ctx1(config)# access-list ctxin permit tcp any host  
192.168.31.10
```

- j. Add an access-list to allow ICMP.

```
PixP/ctx1(config)# access-list ctxin permit icmp any any
```

- k. Bind the access-list to the outside interface

```
PixP/ctx1(config)# access-group ctxin in interface outside
```

- l. Save the changes.

```
PixP/ctx1(config)# write memory
```

- m. From the student PC, try to ping the backbone router:

```
C:\ ping 172.26.26.50
```

- n. From the student PC, try to ping the context ctx1 outside interface:

```
C:\ ping 192.168.31.2
```

- o. From the student PC, try to ping the context ctx1 inside host:

```
C:\ ping 192.168.31.10 (translated address for the inside host)
```

Connectivity should be present from the student PC through context admin to the backbone, 172.26.26.50, and back through context ctx1, 192.168.31.2 to the inside host, 192.168.31.10.

## Step 6 Enable Failover on the Primary Failover Device

Once connectivity with failover disabled has been established, enable failover on the primary failover device.

- a. Change to the system context

```
PixP/ctx1(config)# changeto system
```

- b. Show the failover status of the primary failover device

```
PixP(config)# show failover
```

```
Failover Off
```

```
Cable status: N/A - LAN-based failover enabled
```

```
Failover unit Primary
```

```
Failover LAN Interface: myfailover Ethernet2 (up)
```

```
Unit Poll frequency 15 seconds, holdtime 45 seconds
```

```
Interface Poll frequency 15 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 4 of 250 maximum
```

- c. Enable failover

```
PixP(config)# failover
```

After a pause, the following message should be displayed on the console:

```
No response from Mate
```

```
Group 1 No response from Mate, Switch to Active
```

```
Group 2 No response from Mate, Switch to Active
```

- d. Show the new failover status of the primary failover device

```
PixP# show failover
```

```
Failover On
```

```
Cable status: N/A - LAN-based failover enabled
```

```
Failover unit Primary
```

```
Failover LAN Interface: myfailover Ethernet2 (up)
```

```
Unit Poll frequency 15 seconds, holdtime 45 seconds
```

```
Interface Poll frequency 15 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 4 of 250 maximum
```

```
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
```

```
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
```

```
This host: Primary
```

```

Group 1 State: Active
Active time: 6135 (sec)
Group 2 State: Active
Active time: 0 (sec)
admin Interface outside (192.168.P.2): Normal (Waiting)
admin Interface inside (10.0.P.1): Normal (Waiting)
cxl Interface outside (192.168.3P.2): Normal (Waiting)
cxl Interface inside (10.0.3P.1): Normal (Waiting)
Other host: Primary
Group 1 State: Failed
Active time: 0 (sec)
Group 2 State: Failed
Active time: 0 (sec)
admin Interface outside (192.168.P.7): Unknown (Waiting)
admin Interface inside (10.0.P.7): Unknown (Waiting)
cxl Interface outside (192.168.31.7): Unknown (Waiting)
cxl Interface inside (10.0.31.7): Unknown (Waiting)
Configure the Secondary Failover Security Device

```

## Step 7 Enable Multiple Context Mode

Once the primary PIX Security Appliance is configured, the next task is to prepare the secondary PIX Security Appliance for active/active failover. Complete the following steps to enable multiple mode on the secondary PIX Security Appliance.

- Ask the instructor how to access the console port of the secondary failover device.
- Once the console of the secondary PIX Security Appliance is accessed, verify that this PIX Security Appliance is licensed to support security contexts.

```
PixP(config)# show version
```

- Check the current mode of the secondary PIX Security Appliance:

```
PixP(config)# show mode
```

```
Security appliance mode: single
```

```
The flash mode is the SAME as the running mode.
```

- Enable Multiple Context mode:

```
PixP(config)# mode multiple
```

```
WARNING: This command will change the behavior of the device
```

```
WARNING: This command will initiate a Reboot
```

```
Proceed with change mode? [confirm] <Enter>
```

```
Convert the system configuration? [confirm] <Enter>
```

```
The old running configuration file will be written to flash
```

```
The admin context configuration will be written to flash
```

```
The new running configuration file was written to flash
```

- e. After the secondary Security Appliance re-boots, confirm the PIX Security Appliance is in multiple context mode:

```
PixP# show mode  
Security context mode: multiple
```

- f. Confirm the PIX Security Appliance saved the original configuration as `old_running.cfg`:

```
PixP# show flash  
Directory of flash:/  
 3 -rw- 4810752 08:30:41 Aug 12 2004 pix_7_82.bin  
 8 -rw- 2028 08:30:41 Aug 12 2004 old_running.cfg  
 9 -rw- 1682 08:30:41 Aug 12 2004 admin.cfg
```

- g. Examine the current security contexts.

```
PixP# show context  
Context Name Interfaces URL  
*admin Ethernet0,Ethernet1 flash:/admin.cfg  
Total active Security Contexts: 1  
PixP# show context detail  
Context "system", is a system resource  
Config URL: startup-config  
Real Interfaces:  
Mapped Interfaces: Ethernet0, Ethernet1, Ethernet2,  
Ethernet3, Ethernet4, Ethernet5  
Flags: 0x00000019, ID: 0  
Context "admin", has been created, but initial ACL rules not  
complete  
Config URL: flash:/admin.cfg  
Real Interfaces: Ethernet0, Ethernet1  
Mapped Interfaces: Ethernet0, Ethernet1  
Flags: 0x00000013, ID: 1  
Context "null", is a system resource  
Config URL: ... null ...  
Real Interfaces:  
Mapped Interfaces:  
Flags: 0x00000009, ID: 257
```

## Step 8 Configure the Failover Link

Complete the following steps to add a failover link to the system context:

- a. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2  
PixP(config-if)# no shutdown  
PixP(config-if)# exit
```

- b. Use the **failover lan interface** command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
```

INFO: Non-failover interface config is cleared on Ethernet3 and its sub-interfaces

(where P = pod number)

- c. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

- d. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1  
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

- e. Enable stateful failover:

```
PixP(config)# failover link MYFAILOVER ethernet2
```

(where P = pod number)

- f. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

- g. Configure this device as the secondary failover device:

```
PixP(config)# failover lan unit secondary
```

- h. Enable failover on the secondary failover device:

```
PixP(config)# failover
```

After a pause, from the secondary device console the following messages should be displayed:

```
Detected an active mate
```

```
Beginning configuration replication from mate
```

```
Creating context 'admin'. . . Done
```

```
Creating context 'ctx1'. . . Done
```

```
End configuration replication
```

```
Group 1 detected active mate
```

```
Group 2 detected active mate
```

```
End configuration replication from mate.
```

- i. Return to the console of the primary failover device.

## Task 9 Exercise Active/Active Failover

Complete the following steps to exercise active/active failover:

- a. From the primary device console, verify that you are in the system context.
- b. View the failover statistics. Notice the primary group 1 and group 2 are both active.

Notice the secondary group 1 and group 2 are in standby ready state. Also notice the host addresses of each interface. The standby interface addresses end in .7

```

PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
This host: Primary
Group 1 State: Active
Active time: 765 (sec)
Group 2 State: Active
Active time: 765 (sec)
admin Interface outside (192.168.1.2): Normal
admin Interface inside (10.0.1.1): Normal
ctx1 Interface outside (192.168.31.2): Normal
ctx1 Interface inside (10.0.31.1): Normal
Other host: Secondary
Group 1 State: Standby Ready
Active time: 0 (sec)
Group 2 State: Standby Ready
Active time: 0 (sec)
admin Interface outside (192.168.1.7): Normal
admin Interface inside (10.0.1.7): Normal
ctx1 Interface outside (192.168.31.7): Normal
ctx1 Interface inside (10.0.31.7): Normal

```

- c. From the student PC, perform a continuous ping to host 172.26.26.50

```

C:\>ping 172.26.26.50 -t

```

- d. From the student PC open a telnet session to the backbone router

```

C:\>telnet 192.168.P.1
User Access Verification
Password: Cisco
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>

```

```
% Bad passwords
```

```
RBB>
```

- e. Force the peer PIX Security Appliance to become active.

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

- f. After the failover, verify the ping is still active and the telnet session is still open.

From the telnet session type the following:

```
RBB> enable
```

```
Password: <cr>
```

```
Password: <cr>
```

```
Password: <cr>
```

```
% Bad passwords
```

```
RBB>
```

- g. Close the telnet session and stop the pings.

- h. From the primary failover device console, view failover statistics:

```
PixP(config)# show failover
```

```
Failover On
```

```
Cable status: N/A - LAN-based failover enabled
```

```
Failover unit Primary
```

```
Failover LAN Interface: myfailover Ethernet2 (up)
```

```
Unit Poll frequency 15 seconds, holdtime 45 seconds
```

```
Interface Poll frequency 15 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 4 of 250 maximum
```

```
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
```

```
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
```

```
This host: Primary
```

```
Group 1 State: Standby Ready
```

```
Active time: 765 (sec)
```

```
Group 2 State: Standby Ready
```

```
Active time: 765 (sec)
```

```
admin Interface outside (192.168.1.7): Normal
```

```
admin Interface inside (10.0.1.7): Normal
```

```
ctx1 Interface outside (192.168.31.7): Normal
```

```
ctx1 Interface inside (10.0.31.7): Normal
```

```
Other host: Secondary
```

```
Group 1 State: Active
```

```
Active time: 240 (sec)
```

```
Group 2 State: Active
```

```
Active time: 240 (sec)
```

```
admin Interface outside (192.168.1.2): Normal
admin Interface inside (10.0.1.1): Normal
ctx1 Interface outside (192.168.31.2): Normal
ctx1 Interface inside (10.0.31.1): Normal
```

Notice after the failover, the host address of the primary interfaces end in .7 while the standby secondary interfaces end in .2. The interface addresses switched between primary and secondary units due to the failover.

## Step 10 Return the Failover Devices to Single Mode

Complete the following steps to return the failover devices to single mode:

- a. From the primary failover device console, disable failover:

```
PixP(config)# no failover
```

- b. Return the failover device to single mode

```
PixP(config)# mode single
```

WARNING: This command will change the behavior of the device

WARNING: This command will initiate a Reboot

Proceed with change mode? [confirm] <Enter>

- c. After the primary device reboots, erase the configuration.

```
PixP # write erase
```

Erase configuration in flash memory? [confirm] <Enter>

```
PixP # reload
```

Proceed with reload? [confirm] <Enter>

- d. After the primary Security Appliance reloads, copy the configuration that was saved at the beginning of this lab to the running-config.

```
pixfirewall(config)# copy flash:/pre_fo_lab.cfg running-config
```

- e. Save the configuration.

- f. From the secondary failover device console:

```
PixP(config)# no failover
```

- g. Return the failover device to single mode

```
PixP(config)# mode single
```

WARNING: This command will change the behavior of the device

WARNING: This command will initiate a Reboot

Proceed with change mode? [confirm] <Enter>

- h. After the secondary device reboots, erase the configuration.

```
PixP # write erase
```

Erase configuration in flash memory? [confirm] <Enter>

```
PixP # reload
```