CHAPTER 21

failover through fallback Commands

failover

To enable failover, use the **failover** command in global configuration mode. To disable failover, use the **no** form of this command.

failover

no failover

Syntax Description

This command has no arguments or keywords.

Defaults

Failover is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was limited to enable or disable failover in the configuration (see the **failover active** command).

Usage Guidelines

Use the **no** form of this command to disable failover.

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

The ASA 5505 device allows only Stateless Failover, and only while not acting as an Easy VPN hardware client.

Examples

The following example disables failover:

```
hostname(config)# no failover
hostname(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover active

To switch a standby ASA or failover group to the active state, use the **failover active** command in privileged EXEC mode. To switch an active ASA or failover group to standby, use the **no** form of this command.

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

Syntax Description

group *group_id*	(Optional) Specifies the failover group to make active.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include failover groups.

Usage Guidelines

Use the **failover active** command to initiate a failover switch from the standby unit, or use the **no failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit offline for maintenance. If you are not using Stateful Failover, all active connections are dropped and must be reestablished by the clients after the failover occurs.

Switching for a failover group is available only for Active/Active failover. If you enter the **failover active** command on an Active/Active failover unit without specifying a failover group, all groups on the unit become active.

Examples

The following example switches the standby group 1 to active:

```
hostname# failover active group 1
```

Related Commands

Command	Description
failover reset	Moves an ASA from a failed state to standby.

failover exec

To execute a command on a specific unit in a failover pair, use the **failover exec** command in privileged EXEC or global configuration mode.

failover exec {**active** | **standby** | **mate**} *cmd_string*

Syntax Description

active	Specifies that the command is executed on the active unit or failover group in the failover pair. Configuration commands entered on the active unit or failover group are replicated to the standby unit or failover group.
cmd_string	The command to be executed. **Show**, configuration, and EXEC commands are supported.
mate	Specifies that the command is executed on the failover peer.
standby	Specifies that the command is executed on the standby unit or failover group in the failover pair. Configuration commands executed on the standby unit or failover group are not replicated to the active unit or failover group.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **failover exec** command to send commands to a specific unit in a failover pair.

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the **failover exec** command to enter configuration commands on the correct unit, no matter which unit you are logged in to. For example, if you are logged in to the standby unit, you can use the **failover exec active** command to send configuration changes to the active unit. Those changes are then replicated to the standby unit. Do not use the **failover exec** command to send configuration commands to the standby unit or context; those configuration changes are not replicated to the active unit and the two configurations will no longer be synchronized.

Output from configuration, exec, and **show** commands is displayed in the current terminal session, so you can use the **failover exec** command to issue **show** commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

Command Modes

The **failover exec** command maintains a command mode state that is separate from the command mode of your terminal session. By default, the **failover exec** command mode is global configuration mode for the specified device. You can change that command mode by sending the appropriate command (such as the **interface** command) using the **failover exec** command.

Changing **failover exec** command modes for the specified device does not change the command mode for the session that you are using to access the device. For example, if you are logged in to the active unit of a failover pair, and you issue the following command in global configuration mode, you will remain in global configuration mode, but any commands sent using the **failover exec** command will be executed in interface configuration mode:

```
hostname(config)# failover exec interface GigabitEthernet0/1
hostname(config)#
```

Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command. For example, if you are in interface configuration mode on the active unit, and you have not changed the **failover exec** command mode, the following command would be executed in global configuration mode:

```
hostname(config-if)# failover exec active router ospf 100
hostname(config-if)#
```

Use the **show failover exec** command to display the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Security Considerations

The **failover exec** command uses the failover link to send commands to and receive the output of the command execution from the peer unit. You should use the **failover key** command to encrypt the failover link to prevent eavesdropping or man-in-the-middle attacks.

Limitations

- If you upgrade one unit using the zero-downtime upgrade procedure and not the other, both units must be running software that supports the **failover exec** command for the command to work.
- Command completion and context help are not available for the commands in the *cmd_string* argument.
- In multiple context mode, you can only send commands to the peer context on the peer unit. To send commands to a different context, you must first change to that context on the unit you are logged in to.
- You cannot use the following commands with the **failover exec** command:
  - **changeto**
  - **debug** (**undebug**)
- If the standby unit is in the failed state, it can still receive commands from the **failover exe**c command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot use the **failover exec** command to switch from privileged EXEC mode to global configuration mode on the failover peer. For example, if the current unit is in privileged EXEC mode, and you enter the **failover exec mate configure terminal** command, the **show failover exec**

mate command output will show that the failover exec session is in global configuration mode. However, entering configuration commands for the peer unit using the **failover exec** command will fail until you enter global configuration mode on the current unit.

- You cannot enter recursive **failover exec** commands, such as the **failover exec mate failover exec mate** *command.*
- Commands that require user input or confirmation must use the **/nonconfirm** option.

Examples

The following example shows how to use the **failover exec** command to display failover information on the active unit. The unit on which the command is executed is the active unit, so the command is executed locally.

```
hostname(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        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          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
hostname(config)#
```

The following example uses the **failover exec** command to display the failover status of the peer unit. The command is executed on the the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show failover
```

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        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          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

The following example uses the **failover exec** command to display the failover configuration of the failover peer. The command is executed on the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

The following example uses the **failover exec** command to create a context on the active unit from the standby unit. The command is replicated from the active unit back to the standby unit. Note the two “Creating context…” messages. One is from the **failover exec** command output from the peer unit when the context is created, and the other is from the local unit when the replicated command creates the context locally.

```
hostname(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

hostname(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

hostname(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

The following example shows the warning that is returned when you use the **failover exec** command to send configuration commands to a failover peer in the standby state:

```
hostname# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

        **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
hostname(config)#
```

The following example uses the **failover exec** command to send the **show interface** command to the standby unit:

```
hostname(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
```

```
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

The following example shows the error message returned when issuing an illegal command to the peer unit:

```
hostname# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

The following example shows the error message that is returned when you use the **failover exec** command when failover is disabled:

```
hostname(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

Command	Description
debug fover	Displays failover-related debugging messages.
debug xml	Displays debugging messages for the XML parser used by the **failover exec** command.
show failover exec	Displays the **failover exec** command mode.

failover group

To configure an Active/Active failover group, use the **failover group** command in global configuration mode. To remove a failover group, use the **no** form of this command.

failover group *num*

no failover group *num*

Syntax Description

num	Failover group number. Valid values are 1 or 2.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can define a maximum of two failover groups. The **failover group** command can only be added to the system context of devices configured for multiple context mode. You can create and remove failover groups only when failover is disabled.

Entering this command puts you in the failover group command mode. The **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, **mac address**, and **polltime interface** commands are available in the failover group configuration mode. Use the **exit** command to return to global configuration mode.

Note The **failover polltime interface**, **failover interface-policy**, **failover replication http**, and **failover mac address** commands have no affect in Active/Active failover configurations. They are overridden by the following failover group configuration mode commands: **polltime interface**, **interface-policy**, **replication http**, and **mac address**.

When removing failover groups, you must remove failover group 1 last. Failover group 1 always contains the admin context. Any context not assigned to a failover group defaults to failover group 1. You cannot remove a failover group that has contexts explicitly assigned to it.

Note If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address using the **mac address** command.

Examples

The following partial example shows a possible configuration for two failover groups:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
asr-group	Specifies an asymmetrical routing interface group ID.
interface-policy	Specifies the failover policy when monitoring detects interface failures.
join-failover-group	Assigns a context to a failover group.
mac address	Defines virtual mac addresses for the contexts within a failover group.
polltime interface	Specifies the amount of time between hello messages sent to monitored interfaces.
preempt	Specifies that a unit with a higher priority becomes the active unit after a reboot.
primary	Gives the primary unit higher priority for a failover group.
replication http	Specifies HTTP session replication for the selected failover group.
secondary	Gives the secondary unit higher priority for a failover group.

failover interface ip

To specify the IPv4 address and mask or IPv6 address and prefixfor the failover interface and the Stateful Failover interface, use the **failover interface ip** command in global configuration mode. To remove the IP address, use the **no** form of this command.

failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address***/***prefix* **standby***ipv6_address*]

no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address***/***prefix* **standby***ipv6_address*]

Syntax Description

if_name	Interface name for the failover or Stateful Failover interface.
ip_address mask	Specifies the IP address and mask for the failover or Stateful Failover interface on the primary device.
ipv6_address	Specifies the IPv6 address fore the failover or Stateful Failover interface on the primary device.
prefix	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
standby *ip_address*	Specifies the IP address used by the secondary device to communicate with the primary device.
standby*ipv6_address*	Specifies the IPv6 address used by the secondary device to communicate with the primary device.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(2)	IPv6 address support was added to the command.

Usage Guidelines

The standby address must be in the same subnet as the primary address.

You can only have one **failvover interface ip** command in the configuration. Therefore, your failover interface can have either an IPv6 or an IPv4 address; you cannot assign both an IPv6 and an IPv4 address to the interface.

Failover and Stateful Failover interfaces are functions of Layer 3, even when the ASA is operating in transparent firewall mode, and are global to the system.

In multiple context mode, you configure failover in the system context (except for the **monitor-interface** command).

This command must be part of the configuration when bootstrapping an ASA for LAN failover.

Examples

The following example shows how to specify an IPv4 address and mask for the failover interface:

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

The following example shows how to specify an IPv6 address and prefix for the failover interface:

```
hostname(config)# failover interface ip lanlink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover lan interface	Specifies the interface used for failover communication.
failover link	Specifies the interface used for Stateful Failover.
monitor-interface	Monitors the health of the specified interface.
show running-config failover	Displays the **failover** commands in the running configuration.

failover interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **failover interface-policy** command in global configuration mode. To restore the default, use the **no** form of this command.

failover interface-policy *num*[%]

no failover interface-policy *num*[%]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces when used as a number.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

The defaults are as follows:

- *num* is 1.
- Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional % keyword.

If the number of failed interfaces meets the configured policy and the other ASA is functioning correctly, the ASA marks itself as failed and a failover might occur (if the active ASA is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the interface policy for each failover group with the **interface-policy** command in failover group configuration mode.

Examples

The following examples show two ways to specify the failover policy:

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit and interface poll times.
failover reset	Restores a failed unit to an unfailed state.
monitor-interface	Specifies the interfaces being monitored for failover.
show failover	Displays information about the failover state of the unit.

failover ipsec pre-shared-key

To establish IPsec LAN-to-LAN tunnels on the failover and state links between the units to encrypt all failover communications, use the **failover ipsec pre-shared-key** command in global configuration mode To remove the key, use the **no** form of this command.

failover ipsec pre-shared-key *key*

no failover ipsec pre-shared-key

Syntax Description

0	Specifies an unencrypted password. This is the default.
8	Specifies an encrypted password. If you use a master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), then the key is encrypted in the configuration. If you are copying from the configuration (for example, from **more system:running-config** output), specify that the key is encrypted by using the **8** keyword. **Note** The **failover ipsec pre-shared-key** shows as ***** in **show running-config** output; this obscured key is not copyable.
key	A *key* that you specify on both units that is used by IKEv2 to establish the tunnels, up to 128 characters in length.

Command Default

0 (unencrypted) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
9.1(2)	We introduced this command.

Usage Guidelines

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

We recommend using the **failover ipsec pre-shared-key** method of encryption over the legacy **failover key** method.

You cannot use both IPsec encryption and the legacy **failover key** encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), you must first remove the failover key using the **no failover key** command before you configure IPsec encryption.

Note Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.

Examples

The following example configures an IPsec pre-shared key:

```
hostname(config)# failover ipsec pre-shared-key a3rynsun
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.
show vpn-sessiondb	Shows information about VPN tunnels, including the failover IPsec tunnels.

failover key

To specify the key for encrypted and authenticated communication between units in a failover pair (over the failover and state links), use the **failover key** command in global configuration mode. To remove the key, use the **no** form of this command.

failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

no failover key

Syntax Description

0	Specifies an unencrypted password. This is the default.
8	Specifies an encrypted password. If you use a master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), then the shared secret is encrypted in the configuration. If you are copying from the configuration (for example, from **more system:running-config** output), specify that the shared secret is encrypted by using the **8** keyword. **Note** The **failover key** shared secret shows as ***** in **show running-config** output; this obscured key is not copyable.
hex *key*	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0-9, a-f).
shared_secret	Specifies an alphanumeric shared secret. The secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

Defaults

0 (unencrypted) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified from **failover lan key** to **failover key**.
7.0(4)	This command was modified to include the **hex** *key* keyword and argument.
8.3(1)	This command was modified to support the master passphrase with the **0** and **8** keywords.

Usage Guidelines

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

We recommend using the **failover ipsec pre-shared-key** method of encryption over the legacy **failover key** method.

You cannot use both IPsec encryption (the **failover ipsec pre-shared-key** command) and the legacy **failover key** encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), you must first remove the failover key using the **no failover key** command before you configure IPsec encryption.

Examples

The following example shows how to specify a shared secret for securing failover communication between units in a failover pair:

```
hostname(config)# failover key abcdefg
```

The following example shows how to specify a hexadecimal key for securing failover communication between two units in a failover pair:

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

The following example shows an encrypted password copied and pasted from **more system:running-config** output:

```
hostname(config)# failover key 8 TPZCVNgdegLhWMa
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.

failover lan interface

To specify the interface used for failover communication, use the **failover lan interface** command in global configuration mode. To remove the failover interface, use the **no** form of this command.

failover lan interface *if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}]

Syntax Description

if_name	Specifies the name of the ASA interface dedicated to failover.
phy_if	Specifies the physical interface.
sub_if	(Optional) Specifies a subinterface number.
vlan_if	Used on the ASA 5505 to specify a VLAN interface as the failover link.

Defaults

Not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include the *phy_if* argument.
7.2(1)	This command was modified to include the *vlan_if* argument.

Usage Guidelines

LAN failover requires a dedicated interface for passing failover traffic. However you can also use the LAN failover interface for the Stateful Failover link.

Note If you use the same interface for both LAN failover and Stateful Failover, the interface needs enough capacity to handle both the LAN-based failover and Stateful Failover traffic.

You can use any unused Ethernet interface on the device as the failover interface. You cannot specify an interface that is currently configured with a name. The failover interface is not configured as a normal networking interface; it exists only for failover communications. This interface should only be used for the failover link (and optionally for the state link). You can connect the LAN-based failover link by using a dedicated switch with no hosts or routers on the link or by using a crossover Ethernet cable to link the units directly.

Note When using VLANs, use a dedicated VLAN for the failover link. Sharing the failover link VLAN with any other VLANs can cause intermittent traffic problems and ping and ARP failures. If you use a switch to connect the failover link, use dedicated interfaces on the switch and ASA for the failover link; do not share the interface with subinterfaces carrying regular network traffic.

On systems running in multiple context mode, the failover link resides in the system context. This interface and the state link, if used, are the only interfaces that you can configure in the system context. All other interfaces are allocated to and configured from within security contexts.

Note The IP address and MAC address for the failover link do not change at failover.

The **no** form of this command also clears the failover interface IP address configuration.

This command must be part of the configuration when bootstrapping an ASA for LAN failover.

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

Examples

The following example configures the failover LAN interface using a subinterface on an ASA 5500 series (except for the ASA 5505):

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

The following example configures the failover LAN interface on the ASA 5505:

```
hostname(config)# failover lan interface folink Vlan6
```

Related Commands

Command	Description
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
failover link	Specifies the Stateful Failover interface.

failover lan unit

To configure the ASA as either the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

Syntax Description

primary	Specifies the ASA as a primary unit.
secondary	Specifies the ASA as a secondary unit.

Defaults

Secondary.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

For Active/Standby failover, the primary and secondary designation for the failover unit refers to which unit becomes active at boot time. The primary unit becomes the active unit at boot time when the following occurs:

- The primary and secondary unit both complete their boot sequence within the first failover poll check.
- The primary unit boots before the secondary unit.

If the secondary unit is already active when the primary unit boots, the primary unit does not take control; it becomes the standby unit. In this case, you need to enter the **no failover active** command on the secondary (active) unit to force the primary unit back to active status.

For Active/Active failover, each failover group is assigned a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover group become active at startup when both units start simultaneously (within the failover polling period).

This command must be part of the configuration when bootstrapping an ASA for LAN failover.

Examples

The following example sets the ASA as the primary unit in LAN-based failover:

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

Related Commands

Command	Description
failover lan interface	Specifies the interface used for failover communication.

failover link

To specify the Stateful Failover interface, use the **failover link** command in global configuration mode. To remove the Stateful Failover interface, use the **no** form of this command.

failover link *if_name* [*phy_if*]

no failover link

Syntax Description

if_name	Specifies the name of the ASA interface dedicated to Stateful Failover.
phy_if	(Optional) Specifies the physical or logical interface port. If the Stateful Failover interface is sharing the interface assigned for failover communication or sharing a standard firewall interface, then this argument is not required.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include the *phy_if* argument.
7.0(4)	This command was modified to accept standard firewall interfaces.

Usage Guidelines

This command is not available on the ASA 5505, which does not support Stateful Failover.

The physical or logical interface argument is required when not sharing the failover communication or a standard firewall interface.

The **failover link** command enables Stateful Failover. Enter the **no failover link** command to disable Stateful Failover. If you are using a dedicated Stateful Failover interface, the **no failover link** command also clears the Stateful Failover interface IP address configuration.

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

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to specify a dedicated interface as the Stateful Failover interface. The interface in the example does not have an existing configuration.

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

Related Commands

Command	Description
failover interface ip	Configures the IP address of the **failover** command and Stateful Failover interface.
failover lan interface	Specifies the interface used for failover communication.

failover mac address

To specify the failover virtual MAC address for a physical interface, use the **failover mac address** command in global configuration mode. To remove the virtual MAC address, use the **no** form of this command.

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

Syntax Description

active_mac	The MAC address assigned to the specified interface the active ASA. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
phy_if	The physical name of the interface to set the MAC address.
standby_mac	The MAC address assigned to the specified interface of the standby ASA. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Defaults

Not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **failover mac address** command lets you configure virtual MAC addresses for an Active/Standby failover pair. If virtual MAC addresses are not defined, then when each failover unit boots it uses the burned-in MAC addresses for its interfaces and exchanges those addresses with its failover peer. The MAC addresses for the interfaces on the primary unit are used for the interfaces on the active unit.

However, if both units are not brought online at the same time and the secondary unit boots first and becomes active, it uses the burned-in MAC addresses for its own interfaces. When the primary unit comes online, the secondary unit will obtain the MAC addresses from the primary unit. This change can disrupt network traffic. Configuring virtual MAC addresses for the interfaces ensures that the secondary unit uses the correct MAC address when it is the active unit, even if it comes online before the primary unit.

The **failover mac address** command is unnecessary (and therefore cannot be used) on an interface configured for LAN-based failover because the **failover lan interface** command does not change the IP and MAC addresses when failover occurs. This command has no affect when the ASA is configured for Active/Active failover.

When adding the **failover mac address** command to your configuration, it is best to configure the virtual MAC address, save the configuration to flash memory, and then reload the failover pair. If the virtual MAC address is added when there are active connections, then those connections stop. Also, you must write the complete configuration, including the **failover mac address** command, to the flash memory of the secondary ASA for the virtual MAC addressing to take effect.

If the **failover mac address** is specified in the configuration of the primary unit, it should also be specified in the bootstrap configuration of the secondary unit.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the virtual MAC address for each interface in a failover group with the **mac address** command in failover group configuration mode.

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

Examples

The following example configures the active and standby MAC addresses for the interface named intf2:

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

Related Commands

Command	Description
show interface	Displays interface status, configuration, and statistics.

failover polltime

To specify the failover unit poll and hold times, use the **failover polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values are from 3 to 45 seconds or from 800 to 999 milliseconds if the optional **msec** keyword is used.
msec	(Optional) Specifies that the given time is in milliseconds.
poll_time	Sets the amount of time between hello messages. Valid values are from 1 to 15 seconds or from 200 to 999 milliseconds if the optional **msec** keyword is used.
unit	(Optional) Indicates that the command is used for unit poll and hold times. Adding this keyword to the command does not have any affect on the command, but it can make it easier to differentiate this command from the **failover polltime interface** commands in the configuration.

Defaults

The default values on the ASA are as follows:

- The *poll_time* is 1 second.
- The **holdtime** *time* is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and now includes **unit** and **holdtime** keywords.
7.2(1)	The **msec** keyword was added to the **holdtime** keyword. The **polltime** minimum value was reduced to 200 milliseconds from 500 milliseconds. The **holdtime** minimum value was reduced to 800 milliseconds from 3 seconds.

Usage Guidelines

You cannot enter a **holdtime** value that is less than three times the unit poll time. With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switch overs when the network is temporarily congested.

If a unit does not hear hello packet on the failover communication interface or cable for one polling period, additional testing occurs through the remaining interfaces. If there is still no response from the peer unit during the hold time, the unit is considered failed and, if the failed unit is the active unit, the standby unit takes over as the active unit.

You can include both **failover polltime** [**unit**] and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through an ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example changes the unit poll time frequency to 3 seconds:

```
hostname(config)# failover polltime 3
```

The following example configures the ASA to send a hello packet every 200 milliseconds and to fail over in 800 milliseconds if no hello packets are received on the failover interface within that time. The optional **unit** keyword is included in the command.

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

Related Commands

Command	Description
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.
polltime interface	Specifies the interface poll and hold times for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover polltime interface

To specify the data interface poll and hold times in an Active/Standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 seconds.
interface *time*	Specifies the poll time for interface monitoring. Valid values range from 1 to 15 seconds. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Defaults

The default values are as follows:

- The poll *time* is 5 seconds.
- The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and includes **unit**, **interface**, and **holdtime** keywords.
7.2(1)	The optional **holdtime** *time* and the ability to specify the poll time in milliseconds was added.

Usage Guidelines

Use the **failover polltime interface** command to change the frequency that hello packets are sent out on data interfaces. This command is available for Active/Standby failover only. For Active/Active failover, use the **polltime interface** command in failover group configuration mode instead of the **failover polltime interface** command.

You cannot enter a **holdtime** value that is less than five times the unit poll time. With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested. Interface testing begins when a hello packet is not heard on the interface for over half the hold time.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through an ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example sets the interface poll time frequency to 15 seconds:

```
hostname(config)# failover polltime interface 15
```

The following example sets the interface poll time frequency to 500 milliseconds and the hold time to 5 seconds:

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit failover poll and hold times.
polltime interface	Specifies the interface polltime for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover reload-standby

To force the standby unit to reboot, use the **failover reload-standby** command in privileged EXEC mode.

failover reload-standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command when your failover units do not synchronize. The standby unit restarts and resynchronizes to the active unit after it finishes booting.

Examples

The following example shows how to use the **failover reload-standby** command on the active unit to force the standby unit to reboot:

```
hostname# failover reload-standby
```

Related Commands

Command	Description
write standby	Writes the running configuration to the memory on the standby unit.

failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command in global configuration mode. To disable HTTP connection replication, use the **no** form of this command.

failover replication http

no failover replication http

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from **failover replicate http** to **failover replication http**.

Usage Guidelines

By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **failover replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative affect on system performance.

In Active/Active failover configurations, you control HTTP session replication per failover group using the **replication http** command in failover group configuration mode.

Examples

The following example shows how to enable HTTP connection replication:

```
hostname(config)# failover replication http
```

Related Commands

Command	Description
replication http	Enables HTTP session replication for a specific failover group.
show running-config failover	Displays the **failover** commands in the running configuration.

failover replication rate

To configure the bulk-sync connection replication rate, use the **failover replication rate** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover replication rate *rate*

no failover replication rate

Syntax Description

rate	Sets the number of connections per second. Values and the default setting depend on your model's maximum connections per second.

Command Default

Varies depending on your model.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.4(4.1)/8.5(1.7)	We introduced this command.

Usage Guidelines

You can configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASASM is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced.

Examples

The following example sets the failover replication rate to 20000 connections per second:

```
hostname(config)# failover replication rate 20000
```

Related Commands

Command	Description
failover rate http	Enables HTTP connection replication.

failover reset

To restore a failed ASA to an unfailed state, use the **failover reset** command in privileged EXEC mode.

failover reset [**group** *group_id*]

Syntax Description

group	(Optional) Specifies a failover group. The **group** keyword applies to Active/Active failover only.
group_id	Failover group number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to add the optional failover group ID.

Usage Guidelines

The **failover reset** command allows you to change the failed unit or group to an unfailed state. The **failover reset** command can be entered on either unit, but we recommend that you always enter the command on the active unit. Entering the **failover reset** command at the active unit will “unfail” the standby unit.

You can display the failover status of the unit with the **show failover** or **show failover state** commands.

There is no **no** form of this command.

In Active/Active failover, entering **failover reset** resets the whole unit. Specifying a failover group with the command resets only the specified group.

Examples

The following example shows how to change a failed unit to an unfailed state:

```
hostname# failover reset
```

Related Commands

Command	Description
failover interface-policy	Specifies the policy for failover when monitoring detects interface failures.
show failover	Displays information about the failover status of the unit.

failover timeout

To specify the failover reconnect timeout value for asymmetrically routed sessions, use the **failover timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

Syntax Description

hh	Specifies the number of hours in the timeout value. Valid values range from -1 to 1193. By default, this value is set to 0. Setting this value to -1 disables the timeout, allowing connections to reconnect after any amount of time. Setting this value to 0, without specifying any of the other timeout values, sets the command back to the default value, which prevents connections from reconnecting. Entering **no failover timeout** command also sets this value to the default (0). **Note** When set to the default value, this command does not appear in the running configuration.
mm	(Optional) Specifies the number of minutes in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.
ss	(Optional) Specifies the number of seconds in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.

Defaults

By default, *hh*, *mm*, and *ss* are 0, which prevents connections from reconnecting.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to appear in the command listing.

Usage Guidelines

This command is used in conjunction with the **static** command with the **nailed** option. The **nailed** option allows connections to be reestablished in a specified amount of time after bootup or a system goes active. The **failover timeout** command specifies that amount of time. If not configured, the connections cannot be reestablished. The **failover timeout** command does not affect the **asr-group** command.

Note Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection.

Entering the **no** form of this command restores the default value. Entering **failover timeout 0** also restores the default value. When set to the default value, this command does not appear in the running configuration.

Examples

The following example switches the standby group 1 to active:

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

Related Commands

Command	Description
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

fallback

To configure the fallback timers that the Cisco Intercompany Media Engine uses to fallback from VoIP to PSTN when connection integrity degrades, use the **fallback** command in uc-ime configuration mode. To remove the fallback settings, use the **no** form of this command.

fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

no fallback fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

Syntax Description

filename	Specifies the filename of the sensitivity file. Enter the name of a file on disk that includes the .fbs file extension. To specify the filename, you can include the path on the local disk, for example `disk0:/file001.fbs`.
hold-down timer	Sets the amount of time that ASA waits before notifying Cisco UCM whether to fall back to PSTN.
monitoring timer	Sets the time between which the ASA samples the RTP packets received from the Internet. The ASA uses the data sample to determine if fallback to the PSTN is needed for a call.
sensitivity-file	Specifies the file to use for mid-call PSTN fallback. The sensitivity file is parsed by the ASA and entered in the RMA library.
timer_millisec	Specifies the length of the monitoring timer in milliseconds. Enter an integer within the range 10-600. By default, the length of the monitoring timer is 100 milliseconds.
timer_sec	Secifies the length of the hold-down timer in seconds. Enter an integer within the range 10-360. By default, the length of the hold-down timer is 20 seconds.

Defaults

By default, the length of the monitoring timer is 100 milliseconds.

By default, the length of the hold-down timer is 20 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Uc-ime configuration	•	—	•	—	—

Command History

Release	Modification
8.3(1)	The command was introduced.

Usage Guidelines

Specifies the fallback timer for the Cisco Intercompany Media Engine.

Internet connections can vary wildly in their quality and vary over time. Therefore, even if a call is sent over VoIP because the quality of the connection was good, the connection quality might worsen mid-call. To ensure an overall good experience for the end user, Cisco Intercompany Media Engine attempts to perform a mid-call fallback.

Performing a mid-call fallback requires the ASA to monitor the RTP packets coming from the Internet and send information into an RTP Monitoring Algorithm (RMA) API, which will indicates to the ASA whether fallback is required. If fallback is required, the ASA sends a REFER message to Cisco UCM to tell it that it needs to fallback the call to PSTN.

Note You cannot change the fallback timer when the Cisco Intercompany Media Engine proxy is enabled for SIP inspection. Remove the Cisco Intercompany Media Engine proxy from SIP inspection before changing the fallback timer.

Examples

The following example shows how to configure the Cisco Intercompany Media Engine while specifying the fallback timers:

```
hostname(config)# uc-ime local_uc-ime_proxy
hostname(config-uc-ime)# media-termination ime-media-term
hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
hostname(config-uc-ime)# ticket epoch 1 password password1234
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

The following example shows how to configure the Cisco Intercompany Media Engine while specifying a sensitivity file:

```
hostname(config)# uc-ime local_uc-ime_proxy
hostname(config-uc-ime)# media-termination ime-media-term
hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
hostname(config-uc-ime)# ticket epoch 1 password password1234
hostname(config-uc-ime)# fallback sensitivity-file local_uc-ime_fallback_policy
```

Related Commands

Command	Description
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
show uc-ime	Displays statistical or detailed information about fallback notifications, mapping service sessions, and signaling sessions.
uc-ime	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.